Network Working Group
Internet Draft
Expires: December, 2009
Intended Status: Standards Track

Hing-Kam Lam
Alcatel-Lucent
Scott Mansfield
Eric Gray
Ericsson

June 24, 2009

MPLS TP Network Management Requirements
draft-ietf-mpls-tp-nm-req-02.txt

Status of this Memo

Abstract

This document specifies the requirements for the management of equipment used in networks supporting an MPLS Transport Profile (MPLS-TP). The requirements are defined for specification of network management aspects of protocol mechanisms and procedures that constitute the building blocks out of which the MPLS transport profile is constructed. That is, these requirements indicate what management capabilities need to be available in MPLS for use in managing the MPLS-TP. This document is intended to identify essential network management capabilities, not to specify what functions any particular MPLS implementation supports.

Table of Contents

1. Introduction

This document specifies the requirements for the management of equipment used in networks supporting an MPLS Transport Profile (MPLS-TP). The requirements are defined for specification of network management aspects of protocol mechanisms and procedures that constitute the building blocks out of which the MPLS transport profile is constructed. That is, these requirements indicate what management capabilities need to be available in MPLS for use in managing the MPLS-TP. This document is intended to identify essential network management capabilities, not to specify what functions any particular MPLS implementation supports.

This document also leverages management requirements specified in ITU-T G.7710/Y.1701 [1] and RFC 4377 [2], and attempts to comply with best common practice as defined in [18].

ITU-T G.7710/Y.1701 defines generic management requirements for transport networks. RFC 4377 specifies the OAM requirements, including OAM-related network management requirements, for MPLS networks.

This document is a product of a joint ITU-T and IETF effort to include an MPLS Transport Profile (MPLS-TP) within the IETF MPLS and PWE3 architectures to support capabilities and functionality of a transport network as defined by ITU-T.

The requirements in this document derive from two sources:

1) MPLS and PWE3 architectures as defined by IETF, and

2) packet transport networks as defined by ITU-T.

Requirements for management of equipment in MPLS-TP networks are defined herein. Related functions of MPLS and PWE3 are defined elsewhere (and are out of scope in this document).

This document expands on the requirements in [1] and [2] to cover fault, configuration, performance, and security management for MPLS-TP networks, and the requirements for object and information models needed to manage MPLS-TP Networks and Network Elements.

In writing this document, the authors assume the reader is familiar with references [19] and [20].

1.1. Terminology

Although this document is not a protocol specification, 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 [6] and are to be interpreted as instructions to protocol designers producing solutions that satisfy the requirements set out in this document.

Anomaly: The smallest discrepancy which can be observed between actual and desired characteristics of an item. The occurrence of a single anomaly does not constitute an interruption in ability to perform a required function. Anomalies are used as the input for the Performance Monitoring (PM) process and for detection of defects ([27], 3.7).

Communication Channel (CCh): A logical channel between network elements (NEs) that can be used - e.g. - for management or control plane applications. The physical channel supporting the CCh is technology specific. See APPENDIX A.~~:~~

Data Communication Network (DCN): A network that supports Layer 1 (physical layer), Layer 2 (data-link layer), and Layer 3 (network layer) functionality for distributed management communications related to the management plane, for distributed signaling communications related to the control plane, and other operations communications (e.g., order-wire/voice communications, software downloads, etc.).

Defect: The density of anomalies has reached a level where the ability to perform a required function has been interrupted. Defects are used as input for performance monitoring, the control of consequent actions, and the determination of fault cause ([27], 3.24).

Failure: The fault cause persisted long enough to consider the ability of an item to perform a required function to be terminated. The item may be considered as failed; a fault has now been detected ([27], 3.25).

Fault: A fault is the inability of a function to perform a required action. This does not include an inability due to preventive maintenance, lack of external resources, or planned actions ([27], 3.26).

Fault Cause: A single disturbance or fault may lead to the detection of multiple defects. A fault cause is the result of a correlation process which is intended to identify the defect that is representative of the disturbance or fault that is causing the problem ([27], 3.27).

Fault Cause Indication (FCI): An indication of a fault cause.

Management Communication Channel (MCC): A CCh dedicated for management plane communications.

Management Communication Network (MCN): A DCN supporting management plane communication is referred to as a Management Communication Network (MCN).

MPLS-TP NE: A network element (NE) that supports the functions of MPLS necessary to participate in an MPLS-TP based transport service. See [24] for further information on functionality required to support MPLS-TP.

MPLS-TP network: A network in which MPLS-TP NEs are deployed.

OAM, On-Demand and Proactive: One feature of OAM that is largely a management issue is control of OAM; on-demand and proactive are modes of OAM mechanism operation defined - for example - in Y.1731 ([28] - 3.45 and 3.44 respectively) as:

- On-demand OAM - OAM actions which are initiated via manual intervention for a limited time to carry out diagnostics. On-demand OAM can result in singular or periodic OAM actions during the diagnostic time interval.

- Proactive OAM - OAM actions which are carried on continuously to permit timely reporting of fault and/or performance status.

(Note that it is possible for specific OAM mechanisms to only have a sensible use in either on-demand or proactive mode.)

Operations System (OS): A system that performs the functions that support processing of information related to operations, administration, maintenance, and provisioning (OAM&P) for the networks, including surveillance and testing functions to support customer access maintenance.

Signaling Communication Channel (SCC): A CCh dedicated for control plane communications. The SCC may be used for GMPLS/ASON signaling and/or other control plane messages (e.g., routing messages).

Signaling Communication Network (SCN): A DCN supporting control plane communication is referred to as a Signaling Communication Network (SCN).

2. Management Interface Requirements

This document does not specify which management interface protocol should be used as the standard protocol for managing MPLS-TP networks. Managing an end-to-end connection across multiple operator domains where one domain is managed (for example) via NETCONF/XML ([21]) or SNMP/SMI ([22]), and another domain via CORBA/IDL ([23]), is allowed.

For the management interface to the management system, an MPLS-TP NE MAY actively support more than one management protocol in any given deployment. For example, an MPLS-TP NE may use one protocol for configuration and another for monitoring. The protocols to be supported are at the discretion of the operator.

3. Management Communication Channel (MCC) Requirements

Specifications SHOULD define support for management connectivity with remote MPLS-TP domains and NEs, as well as with termination points located in NEs under the control of a third party network operator. See ITU-T G.8601 [8] for example scenarios in multi-carrier multi-transport-technology environments.

For management purpose, every MPLS-TP NE MUST connect to an OS. The connection MAY be direct (e.g. - via a software, hardware or proprietary protocol connection) or indirect (via another MPLS-TP NE). In this document, any management connection that is not via another MPLS-TP NE is a direct management connection. When an MPLS-TP NE is connected indirectly to an OS, an MCC MUST be supported between that MPLS-TP NE and any MPLS-TP NE(s) used to provide the connection to an OS.

4. Management Communication Network (MCN) Requirements

Entities of the MPLS-TP management plane communicate via a DCN, or more specifically via the MCN. The MCN connects management systems with management systems, management systems with MPLS-TP

NEs, and (in the indirect connectivity case discussed in section 3) MPLS-TP NEs with MPLS-TP NEs.

RFC 5586 ([10]) defines a Generic Associated Channel (G-ACh) to enable the realization of a communication channel (CCh) between adjacent MPLS-TP NEs for management and control. Reference [11] describes how the G-ACh may be used to provide infrastructure that forms part of the MCN and ~~a~~ SCN. It also explains how MCN and SCN messages are encapsulated, carried on the G-ACh, and decapsulat~~multiplex~~ed for delivery to management or signaling/routing control plane components on a label switching router (LSR).

ITU-T G.7712/Y.1703 [7], section 7, describes the transport DCN architecture and requirements. The MPLS-TP MCN MUST support the requirements (in reference [7]) for:

- CCh access functions specified in section 7.1.1;

- MPLS-TP SCC data-link layer termination functions specified in section 7.1.2.3;

- MPLS-TP MCC data-link layer termination functions specified in section 7.1.2.4;

- Network layer PDU into CCh data-link frame encapsulation functions specified in section 7.1.3;

- Network layer PDU forwarding (7.1.6), interworking (7.1.7) and encapsulation (7.1.8) functions, as well as tunneling (7.1.9) and routing (7.1.10) functions specified in [7].

As a practical matter, MCN connections will typically have addresses. See the section on addressing in [15] for further information.

In order to have the MCN operate properly, a number of management functions for the MCN are needed, including:

- Retrieval of DCN network parameters to ensure compatible functioning, e.g. packet size, timeouts, quality of service, window size, etc.;

- Establishment of message routing between DCN nodes;

- Management of DCN network addresses;

- Retrieval of operational status of the DCN at a given node;

- Capability to enable/disable access by an NE to the DCN. Note that this is to allow isolating a malfunctioning NE from impacting the rest of the network.

5. Fault Management Requirements

The Fault Management functions within an MPLS-TP NE enable the supervision, detection, validation, isolation, correction, and reporting of abnormal operation of the MPLS-TP network and its environment.

5.1. Supervision Function

The supervision function analyses the actual occurrence of a disturbance or fault for the purpose of providing an appropriate indication of performance and/or detected fault condition to maintenance personnel and operations systems.

The MPLS-TP NE MUST support supervision of the OAM mechanisms that are deployed for supporting the OAM requirements defined in [3].

The MPLS-TP NE MUST support the following data-plane forwarding path supervision functions:

- Supervision of loop-checking functions used to detect loops in the data-plane forwarding path (which result in non-delivery of traffic, wasting of forwarding resources and unintended self-replication of traffic);

- Supervision of failure detection;

The MPLS-TP NE MUST support the capability to configure data-plane forwarding path related supervision mechanisms to perform on-demand or proactively.

The MPLS-TP NE MUST support supervision for software processing e.g., processing faults, storage capacity, version mismatch, corrupted data and out of memory problems, etc.

The MPLS-TP NE MUST support hardware-related supervision for interchangeable and non-interchangeable unit, cable, and power problems.

The MPLS-TP NE SHOULD support environment-related supervision for temperature, humidity, etc.

5.2. Validation Function

Validation is the process of integrating Fault Cause indications into Failures. A Fault Cause Indication (FCI) indicates a limited interruption of the required transport function. A Fault Cause is not reported to maintenance personnel because it might exist only for a very short time. Note that some of these events are summed up in the Performance Monitoring process (see section 7), and when this sum exceeds a configured value, a threshold crossing alert (report) can be generated.

When the Fault Cause lasts long enough, an inability to perform the required transport function arises. This failure condition is subject to reporting to maintenance personnel and/or an OS because corrective action might be required. Conversely, when the Fault Cause ceases after a certain time, clearing of the Failure condition is also subject to reporting.

The MPLS-TP NE MUST perform persistency checks on fault causes before it declares a fault cause a failure.

The MPLS-TP NE SHOULD provide a configuration capability for control parameters associated with performing the persistency checks described above.

An MPLS-TP NE MAY provide configuration parameters to control reporting, and clearing, of failure conditions.

A data-plane forwarding path failure MUST be declared if the fault cause persists continuously for a configurable time (Time-D). The failure MUST be cleared if the fault cause is absent continuously for a configurable time (Time-C).

Note: As an example, the default time values might be as follows:

Time-D = 2.5 +/- 0.5 seconds

Time-C = 10 +/- 0.5 seconds

These time values are as defined in G.7710 [1].

MIBs - or other object management semantics specifications - defined to enable configuration of these timers SHOULD explicitly provide default values and MAY provide guidelines on ranges and value determination methods for scenarios where the default value chosen might be inadequate. In addition, such specifications SHOULD define the level of granularity at which tables of these values are to be defined. Examples of levels of granularity MAY include per-failure-cause and per-deduced-fault.

Implementations MUST provide the ability to configure the preceding set of timers, and SHOULD provide default values to enable rapid configuration. Suitable default values, timer ranges, and level of granularity are out of scope in this document and form part of the specification of fault management details. Timers SHOULD be configurable per NE for broad categories of failure causes and deduced faults, and MAY be configurable per-interface on an NE or per individual failure cause or deduced fault.

The failure declaration and clearing MUST be time stamped. The time-stamp MUST indicate the time at which the fault cause is activated at the input of the fault cause persistency (i.e. defect-to-failure integration) function, and the time at which the fault cause is deactivated at the input of the fault cause persistency function.

5.3. Alarm Handling Function

5.3.1. Alarm Severity Assignment

Failures can be categorized to indicate the severity or urgency of the fault.

An MPLS-TP NE SHOULD support the ability to assign severity (e.g., Critical, Major, Minor, Warning) to alarm conditions via configuration.

See G.7710 [1], section 7.2.2 for more detail on alarm severity assignment.

5.3.2. Alarm Suppression

Alarms can be generated from many sources, including OAM, device status, etc.

An MPLS-TP NE MUST support suppression of alarms based on configuration.

5.3.3. Alarm Reporting

Alarm Reporting is concerned with the reporting of relevant events and conditions, which occur in the network (including the NE, incoming signal, and external environment).

Local reporting is concerned with automatic alarming by means of audible and visual indicators near the failed equipment.

An MPLS-TP NE MUST support local reporting of alarms.

The MPLS-TP NE MUST support reporting of alarms to an OS. These reports are either autonomous reports (notifications) or reports on request by maintenance personnel. The MPLS-TP NE SHOULD report local (environmental) alarms to a network management system.

An MPLS-TP NE supporting one or more other networking technologies (e.g. - Ethernet, SDH/SONET, MPLS) over MPLS-TP MUST be capable of translating an MPLS-TP defects into failure conditions that are meaningful to the client layer, as described in RFC 4377 [2], section 4.7.

5.3.4. Alarm Reporting Control

Alarm Reporting Control (ARC) supports an automatic in-service provisioning capability. Alarm reporting can be turned off on a per-managed entity (e.g., LSP) basis to allow sufficient time for customer service testing and other maintenance activities in an "alarm free" state. Once a managed entity is ready, alarm reporting is automatically turned on.

An MPLS-TP NE SHOULD support the Alarm Reporting Control function for controlling the reporting of alarm conditions.

See G.7710 [1] (section 7.1.3.2) and RFC 3878 [9] for more information about ARC.

6.Configuration Management Requirements

Configuration Management provides functions to identify, collect data from, provide data to and control NEs. Specific configuration tasks requiring network management support include hardware and software configuration, configuration of NEs to support transport paths (including required working and protection paths), and configuration of required path integrity/connectivity and performance monitoring (i.e. - OAM).

6.1. System Configuration

The MPLS-TP NE MUST support the configuration requirements specified in G.7710 [1] section 8.1 for hardware.

The MPLS-TP NE MUST support the configuration requirements specified in G.7710 [1] section 8.2 for software.

The MPLS-TP NE MUST support the configuration requirements specified in G.7710 [1] section 8.13.2.1 for local real time clock functions.

The MPLS-TP NE MUST support the configuration requirements specified in G.7710 [1] section 8.13.2.2 for local real time clock alignment with external time reference.

The MPLS-TP NE MUST support the configuration requirements specified in G.7710 [1] section 8.13.2.3 for performance monitoring of the clock function.

6.2. Control Plane Configuration

If a control plane is supported in an implementation of MPLS-TP, the MPLS-TP NE MUST support the configuration of MPLS-TP control plane functions by the management plane. Further detailed requirements will be provided along with progress in defining the MPLS-TP control plane in appropriate specifications.

6.3. Path Configuration

In addition to the requirement to support static provisioning of transport paths (defined in [24], section 2.1 - General Requirements - requirement 18), an MPLS-TP NE MUST support the configuration of required path performance characteristic thresholds (e.g. - Loss Measurement [LM], Delay Measurement [DM] thresholds) necessary to support performance monitoring of the MPLS-TP service(s).

In order to accomplish this, an MPLS-TP NE MUST support configuration of LSP information (such as an LSP identifier of some kind) and/or any other information needed to retrieve LSP status information, performance attributes, etc.

If a control plane is supported, and that control plane includes support for control-plane/management-plane hand-off for LSP setup/maintenance, the MPLS-TP NE MUST support management of the hand-off of Path control. See, for example, references [25] and [26].

Further detailed requirements will be provided along with progress in defining the MPLS-TP control plane in appropriate specifications.

If MPLS-TP transport paths cannot be statically provisioned using MPLS LSP and pseudo-wire management tools (either already defined in standards or under development), further management specifications MUST be provided as needed.

6.4. Protection Configuration

The MPLS-TP NE MUST support configuration of required path protection information as follows:

- designate specifically identified LSPs as working or protecting~~on~~ LSPs;

- define associations of working and protecting~~on~~ paths;

- operate/release manual protection switching;

- operate/release force protection switching;

- operate/release protection lockout;

- set/retrieve Automatic Protection Switching (APS) parameters, including -

    o Wait to Restore time,

    o Protection Switching threshold information.

6.5. OAM Configuration

The MPLS-TP NE MUST support configuration of the OAM entities and functions specified in [3].

The MPLS-TP NE MUST support the capability to choose which OAM functions to use and which maintenance entity will apply to them.

The MPLS-TP NE MUST support the capability to configure the OAM entities/functions as part of LSP setup and tear-down, including co-routed bidirectional point-to-point, associated bidirectional point-to-point, and uni-directional (both point-to-point and point-to-multipoint) connections.

The MPLS-TP NE MUST support the configuration of maintenance entity identifiers (e.g. MEP ID, ~~and ~~MIP ID and ME(G) ID) for the purpose of LSP connectivity checking.

The MPLS-TP NE MUST support configuration of OAM parameters to meet their specific operational requirements, such as whether -

1) one-time on-demand immediately or

2) one-time on-demand pre-scheduled or

3) on-demand periodically based on a specified schedule or

4) proactive on-going.

The MPLS-TP NE MUST support the enabling/disabling of the connectivity check processing. The connectivity check process of the MPLS-TP NE MUST support provisioning of the identifiers to be transmitted and the expected identifiers.

7. Performance Management Requirements

Performance Management provides functions for the purpose of Maintenance, Bring-into-service, Quality of service, and statistics gathering.

This information could be used, for example, to compare behavior of the equipment, MPLS-TP NE or network at different moments in time to evaluate changes in network performance.

ITU-T Recommendation G.7710 [1] provides transport performance monitoring requirements for packet-switched and circuit-switched transport networks with the objective of providing coherent and consistent interpretation of the network behavior in a multi-technology environment. The performance management requirements specified in this document are driven by such an objective.

7.1. Path Characterization Performance Metrics

It MUST be possible to determine when an MPLS-TP based transport service is available and when it is unavailable.

From a performance perspective, a service is unavailable if there is an indication that performance has degraded to the extent that a configurable performance threshold has been crossed and the degradation persists long enough (i.e. - the indication persists for some amount of time - which is either configurable, or well-known) to be certain it is not a measurement anomaly.

Methods, mechanisms and algorithms for exactly how unavailability is to be determined - based on collection of raw performance data - are out of scope for this document.

<<Comment start>>

Old:

For the purposes of this document, it is sufficient to state that an MPLS-TP NE MUST support collection, and reporting, of raw performance data that MAY be used in determining availability of a transport service, and that implementations SHOULD support some as yet to be defined mechanism for determining service availability.

New:

~~For the purposes of this document, it is sufficient to state that an~~The MPLS-TP NE MUST support collection~~,~~ and reporting~~,~~ of raw performance data that MAY be used in determining unavailability of a transport service.~~, and that implementations SHOULD support some as yet to be defined mechanism for determining service availability.~~

The MPLS-TP NE MUST support the determination of the unavailability of the transport service. This determination MUST be supported within the MPLS-TP NE.

Note that for the Ethernet transport network, unavailability is determined based on Severely Errored Seconds (SES). SES and Unavailable Seconds (UAS) are defined for Ethernet transport networks in ITU-T Recommendation Y.1563 [29]. ITU-T is currently extending these definitions to apply them to the packet transport technology in general. Once these definitions are available, they should be used for the MPLS-TP NE.

<<Comment end>>

The MPLS-TP NE MUST support collection of loss measurement (LM) statistics.

The MPLS-TP NE MUST support collection of delay measurement (DM) statistics.

The MPLS-TP NE MUST support reporting of Performance degradation via fault management for corrective actions. "Reporting" in this context could mean:

- reporting to an autonomous protection component to trigger protection switching,

- reporting via a craft interface to allow replacement of a faulty component (or similar manual intervention),

- etc.

The MPLS-TP NE MUST support reporting of performance statistics on request from a management system.

7.2. Performance Measurement Instrumentation

7.2.1. Measurement Frequency

For performance measurement mechanisms that support both proactive and on-demand modes, the MPLS-TP NE MUST support the capability to be configured to operate on-demand or proactively.

7.2.2. Measurement Scope

On measurement of packet loss and loss ratio:

- For bidirectional (both co-routed and associated) P2P connections -

  o on-demand measurement of single-ended packet loss, and loss ratio, measurement is REQUIRED;

  o proactive measurement of packet loss, and loss ratio, measurement for each direction is REQUIRED.

- for unidirectional (P2P and P2MP) connection, proactive measurement of packet loss, and loss ratio, is REQUIRED.

On Delay measurement:

- for unidirectional (P2P and P2MP) connection, on-demand measurement of delay measurement is REQUIRED.

- for co-routed bidirectional (P2P) connection, on-demand measurement of one-way and two-way delay is REQUIRED.

- for associated bidirectional (P2P) connection, on-demand measurement of one-way delay is REQUIRED.

8. Security Management Requirements

The MPLS-TP NE MUST support secure management and control planes.

8.1. Management Communication Channel Security

Secure communication channels MUST be supported for all network traffic and protocols used to support management functions. This MUST include, at least, protocols used for configuration, monitoring, configuration backup, logging, time synchronization, authentication, and routing. The MCC MUST support application protocols that provide confidentiality and data integrity protection.

The MPLS-TP NE MUST support the following:

- Use of open cryptographic algorithms (See RFC 3871 [5])

- Authentication - allow management connectivity only from authenticated entities.

- Authorization - allow management activity originated by an authorized entity, using (for example) an Access Control List (ACL).

- Port Access Control - allow management activity received on an authorized (management) port.

8.2.Signaling Communication Channel Security

Security requirements for the SCC are driven by considerations similar to MCC requirements described in section 8.1.

Security Requirements for the control plane are out of scope for this document and are expected to be defined in the appropriate control plane specifications.

Management of control plane security MUST also be defined at that time.

8.3. Distributed Denial of Service

A Denial of Service (DoS) attack is an attack that tries to prevent a target from performing an assigned task, or providing its intended service(s), through any means. A Distributed DoS (DDoS) can multiply attack severity (possibly by an arbitrary amount) by using multiple (potentially compromised) systems to act as topologically (and potentially geographically) distributed attack sources. It is possible to lessen the impact and potential for DoS and DDoS by using secure protocols, turning off unnecessary processes, logging and monitoring, and ingress filtering. RFC 4732 [4] provides background on DOS in the context of the Internet.

An MPLS-TP NE MUST support secure management protocols and SHOULD do so in a manner the reduce potential impact of a DoS attack.

An MPLS-TP NE SHOULD support additional mechanisms that mitigate a DoS (or DDoS) attack against the management component while allowing the NE to continue to meet its primary functions.

9. Security Considerations

Section 8 includes a set of security requirements that apply to MPLS-TP network management.

Solutions MUST provide mechanisms to prevent unauthorized and/or unauthenticated access to management capabilities and private information by network elements, systems or users.

Performance of diagnostic functions and path characterization involves extracting a significant amount of information about network construction that the network operator might consider private.

10. IANA Considerations

There are no IANA actions associated with this document.

11. Acknowledgments

The authors/editors gratefully acknowledge the thoughtful review, comments and explanations provided by Adrian Farrel, Alexander Vainshtein, Andrea Maria Mazzini, Ben Niven-Jenkins, Bernd Zeuner, Dan Romascanu, Daniele Ceccarelli, Diego Caviglia, Dieter Beller, He Jia, Leo Xiao, Maarten Vissers, Neil Harrison, Rolf Winter, Yoav Cohen and Yu Liang.

12. References

12.1. Normative References

[1] ITU-T Recommendation G.7710/Y.1701, "Common equipment management function requirements", July, 2007.

[2] Nadeau, T., et al, "Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks", RFC 4377, February 2006.

[3] Vigoureux, M., et al, "Requirements for OAM in MPLS Transport Networks", work in progress.

[4] Handley, M., et al, "Internet Denial-of-Service Considerations", RFC 4732, November 2006.

[5] Jones, G., "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure", RFC 3871, September 2004.

[6] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[7] ITU-T Recommendation G.7712/Y.1703, "Architecture and Specification of Data Communication Network", June 2008.

[8] ITU-T Recommendation G.8601, "Architecture of service management in multi bearer, multi carrier environment", June 2006.

[9] Lam, H., et al, "Alarm Reporting Control Management Information Base (MIB)", RFC 3878, September 2004.

[10] Bocci, M., et al, "MPLS Generic Associated Channel", RFC 5586, June 2009.

[11] Beller, D., et al, "An Inband Data Communication Network For the MPLS Transport Profile", draft-ietf-mpls-tp-gach-dcn, work in progress.

12.2. Informative References

[12] Chisholm, S. and D. Romascanu, "Alarm Management Information Base (MIB)", RFC 3877, September 2004.

[13] ITU-T Recommendation M.20, "Maintenance Philosophy for Telecommunication Networks", October 1992.

[14] Telcordia, "Network Maintenance: Network Element and Transport Surveillance Messages" (GR-833-CORE), Issue 5, August 2004.

[15] Bocci, M. et al, "A Framework for MPLS in Transport Networks", Work in Progress, November 27, 2008.

[16] ANSI T1.231-2003, "Layer 1 In-Service Transmission Performance Monitoring", American National Standards Institute, 2003.

[17] Vigoureux, M. et al, "MPLS Generic Associated Channel", draft-ietf-mpls-tp-gach-gal, work in progress.

[18] Harrington, D., "Guidelines for Considering Operations and Management of New Protocols and Protocol Extensions", draft-ietf-opsawg-operations-and-management, work in progress.

[19] Mansfield, S. et al, "MPLS-TP Network Management Framework", draft-ietf-mpls-tp-nm-framework, work in progress.

[20] Bocci, M. et al, "A Framework for MPLS in Transport Networks", draft-ietf-mpls-tp-framework, work in progress.

[21] Enns, R. et al, "NETCONF Configuration Protocol", draft-ietf-netconf-4741bis, work in progress.

[22] McCloghrie, K. et al, "Structure of Management Information Version 2 (SMIv2)", RFC 2578, April 1999.

[23] OMG Document formal/04-03-12, "The Common Object Request Broker: Architecture and Specification", Revision 3.0.3. March 12, 2004.

[24] Niven-Jenkins, B. et al, "MPLS-TP Requirements", draft-ietf-mpls-tp-requirements, work in progress.

[25] Caviglia, D. et al, "Requirements for the Conversion between Permanent Connections and Switched Connections in a Generalized Multiprotocol Label Switching (GMPLS) Network", RFC 5493, April 2009.

[26] Caviglia, D. et al, "RSVP-TE Signaling Extension For The Conversion Between Permanent Connections And Soft Permanent Connections In A GMPLS Enabled Transport Network", draft-ietf-ccamp-pc-spc-rsvpte-ext, work in progress.

[27] ITU-T Recommendation G.806, "Characteristics of transport equipment - Description methodology and generic functionality", January, 2009.

[28] ITU-T Recommendation Y.1731, "OAM Functions and Mechanisms for Ethernet Based Networks", February, 2008.

[29] ITU-T Recommendation Y.1563, "Ethernet frame transfer and availability performance ", January 2009.

Author's Addresses

Editors:

Eric Gray
Ericsson
900 Chelmsford Street
Lowell, MA, 01851
Phone: +1 978 275 7470
Email: Eric.Gray@Ericsson.com

Scott Mansfield
Ericsson
250 Holger Way
San Jose CA, 95134
+1 724 931 9316
EMail: Scott.Mansfield@Ericsson.com

Hing-Kam (Kam) Lam
Alcatel-Lucent
600-700 Mountain Ave
Murray Hill, NJ, 07974
Phone: +1 908 582 0672
Email: hklam@Alcatel-Lucent.com

Author(s):

Contributor(s):

Adrian Farrel
Old Dog Consulting
Email: adrian@olddog.co.uk

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

APPENDIX A: Communication Channel (CCh) Examples

A CCh may be realized in a number of ways.

1. The CCh may be provided by a link in a physically distinct network. That is, a link that is not part of the transport network that is being managed. For example, the nodes in the transport network may be interconnected in two distinct physical networks: the transport network and the DCN.

This is a "physically distinct out-of-band CCh".

2. The CCh may be provided by a link in the transport network that is terminated at the ends of the DCC and which is capable of encapsulating and terminating packets of the management protocols. For example, in MPLS-TP a~~n~~ single-hop LSP might be established between two adjacent nodes, and that LSP might be capable of carrying IP traffic. Management traffic can then be inserted into the link in an LSP parallel to the LSPs that carry user traffic.

This is a "physically shared out-of-band CCh."

3. The CCh may be supported as its native protocol on the interface alongside the transported traffic. For example, if an interface is capable of sending and receiving both MPLS-TP and IP, the IP-based management traffic can be sent as native IP packets on the interface.

This is a "shared interface out-of-band CCh".

4. The CCh may use overhead bytes available on a transport connection. For example, in TDM networks there are overhead bytes associated with a data channel, and these can be used to provide a CCh. It is important to note that the use of overhead bytes does not reduce the capacity of the associated data channel.

This is an "overhead-based CCh".

This alternative is not available in MPLS-TP because there is no overhead available.

5. The CCh may provided by a dedicated channel associated with the data link. For example, the generic associated label (GAL) [17] may be used to label DCC traffic being exchanged on a data

link between adjacent transport nodes, potentially in the absence of any data LSP between those nodes.

This is a "data link associated CCh".

It is very similar to case 2, and by its nature can only span a single hop in the transport network.

6. The CCh may be provided by a dedicated channel associated with a data channel. For example, in MPLS-TP the GAL [17] may be imposed under the top label in the label stack for an MPLS-TP LSP to create a channel associated with the LSP that may carry management traffic. This CCh requires the receiver to be capable of demultiplexing management traffic from user traffic carried on the same LSP by use of the GAL.

This is a "data channel associated CCh".

7. The CCh may be provided by mixing the management traffic with the user traffic such that is indistinguishable on the link without deep-packet inspection. In MPLS-TP this could arise if there is a data-carrying LSP between two nodes, and management traffic is inserted into that LSP. This approach requires that the termination point of the LSP is able to demultiplex the management and user traffic. Such might be possible in MPLS-TP if the MPLS-TP LSP was carrying IP user traffic.

This is an "in-band CCh".

These realizations may be categorized as:

A. Out-of-fiber, out-of-band (types 1 and 2)
B. In-fiber, out-of-band (types 2, 3, 4, and 5)
C. In-band (types 6 and 7)

The MCN and SCN are logically separate networks and may be realized by the same DCN or as separate networks. In practice, that means that, between any pair of nodes, the MCC and SCC may be on the same link or separate links.

It is also important to note that the MCN and SCN do not need to be categorised as in-band, out-of-band, etc. This definition only applies to the individual links, and it is possible for some nodes to be connected in the MCN or SCN by one type of link, and other nodes by other types of link. Furthermore, a pair of adjacent nodes may be connected by multiple links of different types.

Lastly note that the division of DCN traffic between links between a pair of adjacent nodes is purely an implementation choice. Parallel links may be deployed for DCN resilience or load sharing. Links may be designated for specific use. For example, so that some links carry management traffic and some carry control plane traffic, or so that some links carry signaling protocol traffic while others carry routing protocol traffic.

It should be noted that the DCN may be a routed network with forwarding capabilities, but that this is not a requirement. The ability to support forwarding of management or control traffic within the DCN may substantially simplify the topology of the DCN and improve its resilience, but does increase the complexity of operating the DCN.

See also RFC 3877 [12], ITU-T M.20 [13], and Telcordia document GR-833-CORE [14] for further information.