Network Working Group   Hing-Kam Lam
Internet Draft   Alcatel-Lucent
Expires: October, 2009   Scott Mansfield
Intended Status: Informational   Eric Gray
                                                       Ericsson
                                                 April 15, 2009

MPLS TP Network Management Requirements
draft-ietf-mpls-tp-nm-req-01.txt

Status of this Memo

Abstract

   This document specifies the requirements necessary to manage the
   elements and networks that support an MPLS Transport Profile
   (MPLS-TP). This document is a product of a joint International
   Telecommunications Union - Telecommunications Standardization
   Sector (ITU-T) and Internet Engineering Task Force (IETF) effort
   to include a MPLS Transport Profile within the IETF MPLS
   architecture. The requirements are driven by the management
   functionality needs defined by ITU-T for packet transport
   networks.

Table of Contents

1. Introduction

This document describes the requirements necessary to manage the elements and networks that support an MPLS Transport Profile (MPLS-TP). It leverages the management requirements specified in ITU-T G.7710/Y.1701 [1] and RFC 4377 [2]. ITU-T G.7710/Y.1701 [1] specifies generic management requirements for transport (including packet-based and circuit-based) networks. RFC 4377 specifies the OAM requirements, including OAM-related network management requirements, for MPLS networks. 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.

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.

MPLS-TP NE: a network element (NE) that supports MPLS-TP functions

MPLS-TP network: a network in which MPLS-TP NEs are deployed

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.).

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

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

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

Management Communication Channel (MCC): a CC dedicated for management plane communications.

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

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.

2. Management Interface Requirements

This document does not specify which management interface protocol should be 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 or SNMP/SMI, and another domain via CORBA/IDL, 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

An MPLS-TP management network SHOULD support seamless management connectivity with remote MPLS-TP domains and NEs as well as with termination points located in NEs under control by 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 either directly or indirectly via another MPLS-TP NE. When an MPLS-TP NE is connected indirectly to an OS, an MCC MUST be supported between the MPLS-TP NE and the other MPLS-TP NE.

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 MPLS-TP NEs
   with management systems, NEs with NEs, and management systems
   with management systems. Transport DCN architecture and
   requirements are specified in ITU-T G.7712/Y.1703 [7], including
   network layer protocols and their interworking.

   As a practical requirement, MCN connections require addressing.
   See the section on addressing in [13] for further information.

   In order to have the MCN operate properly, a number of
   management functions for the MCN are required, 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 to the DCN.

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 transmission
supervision functions:

   . Supervision of looping check 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 the detection of failure in the sequence of
     a protocol exchange (e.g. automatic protection switching
     protocol);

The MPLS-TP NE transmission-related supervision mechanisms MUST
support the flexibility to be configured to perform on-demand or
proactively.

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

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

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

5.2. Validation Function

Validation is concerned with the integration of Fault Causes
into Failures. A Fault Cause indicates a limited interruption of
the required transport function. A Fault Cause is not reported
to maintenance personnel because it could exist only for a very
short time. Note that some of these events however are summed up
in the Performance Monitoring process, and when this sum exceeds
a certain value, a Threshold 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.

A transmission failure SHALL be declared if the fault cause
persists continuously for a configurable time (Time-D). The
failure SHALL be cleared if the fault cause is absent
continuously for a configurable time (Time-C). Typically the
default time values would 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].

The failure declaration and clearing MUST be time stamped. The
time-stamp SHALL 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 might be categorized to indicate the severity or
urgency of the fault.

An MPLS-TP NE SHOULD support the flexibility of assignment of
severity (e.g., Critical, Major, Minor, Warning) by the
management system.

See G.7710 [1] for more description about alarm severity
assignment.

5.3.2. Alarm Suppression

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

An MPLS-TP NE MUST provide alarm suppression functionality that
prevents the generation of superfluous alarms.

Examples of alarm suppression mechanisms include simply
discarding the alarms (or not generating them in the first
place), or aggregating the alarms together, thereby greatly
reducing the number of alarm notifications to be emitted.

Note: An MPLS-TP NE supporting the inter-working of one or more
networking technologies (e.g., Ethernet, SDH/SONET, MPLS) with
MPLS-TP needs to translate an MPLS-TP fault into an existing
transport technology failure condition for reporting to the
management system.

See RFC 4377 [2] for more description.

5.3.3. Alarm Reporting Control

Alarm Reporting Control (ARC) supports an automatic in-service
provisioning capability. Alarm reporting MAY 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] and RFC 3878 [9] for more description of ARC.

5.3.4. 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.

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] for hardware, software, and date/time.

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 might be provided along with progress in defining
the MPLS-TP control plane in appropriate specifications.

6.3. **Path Configuration**

The MPLS-TP NE MUST support the capability of configuring
required path performance characteristic thresholds (e.g. - Loss
Measurement [LM], Delay Measurement [DM] thresholds).

The MPLS-TP NE MUST support the capability of configuring
required LSPs as follows:

    . configure LSP indentifier and/or other information
       necessary to retrieve LSP status information.

6.4. **Protection Configuration**

The MPLS-TP NE MUST support the capability of configuring
required path protection as follows:

    . Designate specifically identified LSPs as working or
       protection LSPs;
    . define associations of working and protection paths;
    . operate/release manual protection switching;
    . operate/release force protection switching;
    . operate/release protection lockout;
    . set/retrieve Automatic Protection Switching (APS)
       parameters, including -
          . Wait to Restore time,
          . Protection Switching threshold information.

6.5. OAM Configuration

   The MPLS-TP NE MUST provide the capability to configure 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 to apply 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) for the purpose of
   LSP connectivity checking.

   The MPLS-TP NE MUST have the flexibility to configure 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 to evaluate and report
   upon the behavior of the equipment, NE, and network for the
   purpose of Maintenance, Bring-into-service, Quality of service,
   and Performance monitoring for signal degradation. 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 particular
   for hybrid network which consists of multiple transport
   technologies. The performance management requirements specified
   in this document are driven by such an objective.

7.1. Path Characterization Performance Metrics

   The MPLS-TP NE MUST support collection of loss measurement (LM)
   so that they can be used to detect performance degradation.

The MPLS-TP NE MUST support collection of delay measurement (DM)
so that they can be used to detect performance degradation.

The MPLS-TP NE MUST support reporting of Performance degradation
via fault management for corrective actions (e.g. protection
switching).

The MPLS-TP NE MUST support collection of loss ratio measurement
so that they can be used to determine Severely Errored Second
(SES).

A SES is declared for a one second interval when the ratio of
lost packets to total transmitted packets in that one second
interval exceeds a predetermined threshold.

The packet lost threshold for declaring SES MUST be
configurable.

The number of SESs MUST be collected per configurable intervals
(e.g. 15-minute and 24-hour).

The MPLS-TP NE MUST support collection of SES measurement so
that they can be used to determine service unavailable time.

A period of unavailable time (UAT) begins at the onset of 10
consecutive SES events. These 10 seconds are considered to be
part of unavailable time. A new period of available time begins
at the onset of 10 consecutive non-SES events. These 10 seconds
are considered to be part of available time.

The MPLS-TP NE MUST support collection of Unavailable Seconds
(UAS) so that they can be used to determine service
availability.

The number of UAS MUST be collected per configurable intervals
(e.g. 15-minute and 24-hour).

SES and UAS history (the number of readings to be retained and
available) is as defined in ITU and ANSI documents associated
with specific transport technologies (for instance, ITU-T
G.7710, and ANSI T1.231-2003 [T1.231.01-2003 for DSL,.02 for
DS1,.03 for DS3 and T1.231.04-2003 for SONET] - see [1] and [14]
respectively), however these are fairly consistently defined as
follows:

   - Current and previous 1-day statistics

       - Current and 16 recent 15-minute statistics (ITU-T)

       - Current, previous and 31 recent 15-minute statistics (ANSI)

    Note that - worst case (ANSI) requires 2 copies of 1-day
    statistics (current and previous) and 33 copies of 15-minute
    statistics (current, previous and 31 recent).

7.2. Performance Measurement Instrumentation

7.2.1. Measurement Frequency

    The performance measurement mechanisms MUST support the
    flexibility to be configured to operate on-demand or proactively
    (i.e. continuously over a period of time).

7.2.2. Measurement Scope

    On measurement of packet loss and loss ratio:

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

            . on-demand measurement of single-ended packet loss,
              and loss ratio, measurement are required;

            . proactive measurement of packet loss, and loss
              ratio, measurement for each direction are required.

    Note: for associated bidirectional P2P connections, this data
    can only be measured at end-points.

      - For unidirectional (P2P and P2MP) connection, proactive
        measurement of packet loss, and loss ratio, are 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 are 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 channels MUST be provided 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.

If management communication security is provided, 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 considerations for the SCC are similar to the considerations driving the 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 the control plane security must also be defined at that time.

8.3. Distributed Denial of Service

Denial of Service (DoS) attack is an attack which 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 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.

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 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 MAY 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,
Andrea Maria Mazzini, Ben Niven-Jenkins, Bernd Zeuner, Diego
Caviglia, Dieter Beller, He Jia, Leo Xiao, Maarten Vissers, Neil
Harrison and Rolf Winter.

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]   Vigoureus, 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.

12.2. Informative References

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

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

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

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

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

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

[13]. Author's Addresses

Editors:

Scott Mansfield
Ericsson
5000 Ericsson Drive
Warrendale, PA, 15086
Phone: +1 724 742 6726
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

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

Author(s):

Contributor(s):

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

Copyright Statement

Acknowledgment

APPENDIX A: Communication Channel (CC) Examples

A CC may be realized in a number of ways.

1. The CC 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 CC".

2. The CC 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 an 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 CC."

3. The CC 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 CC".

4. The CC 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 CC. 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 CC".

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

5. The CC may provided by a dedicated channel associated with
the data link. For example, the generic associated label (GAL)
[15] 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 CC".

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

6. The CC may be provided by a dedicated channel associated with
a data channel. For example, in MPLS-TP the GAL [15] 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 CC 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 CC".

7. The CC 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 CC".

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 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 [10], ITU-T M.20 [11], and Telcordia document
GR-833-CORE [12] for further information.