SIF-029-1999

(SIF Document #SIF-IM-9712-097 R3)

SIF APPROVED DOCUMENT

WORK GROUP: Information Modeling

TITLE: Implementers Agreement on Connection Management and Fault Management for EMS to NMS

DATE: April 29th, 1999

EDITOR: **Name: Jean Lawlis**
Voice: 1-978-960-6314
email: jlawlis@lucent.com

ABSTRACT: This Implementers Agreement covers the Interface between a SONET NMS and a SONET EMS exchanging information for the purposes of managing SONET connections. It assumes the use of CMISE.

This document has received the approval of the SONET Interoperability Forum (SIF).

April 29, 1999

Table of Contents

....

1. Introduction

1.1 Intent

The intent of this document is to provide specific requirements and procedures for implementing interoperable Connection Management and Fault Management Information Models for use between NMSs and EMSs.

1.2 Scope

The SIF Network Management Information Model Group has defined an information model for use between the TMN NM and EM Layers that is documented in ***Information Model for Connection Management and Fault Management at the EMS/NMS Interface***. It is the function of the SIF Network Management Information Model Implementers Group to create an Implementers Agreement for that Information model that provides all of the necessary information for two or more vendors to successfully implement that model and interoperate. This document contains that information including the specific parts of the Information Model that must be implemented, the suggested process for reaching agreement, the verification process to be followed, the communications infra-structure to be supported, and the Conformance Statements to be used.

This Implementors Agreement addresses the following functional areas of SONET network management:

- Transport network connection management (including set-up/ modification for subnetwork connection, link connection, and trails.)
- Transport network configuration provisioning (including subnetwork provisioning, and link provisioning)
- Network fault management (a reduced set)

This agreement and the Information Model on which it is based address the network-view aspects of the NMS/EMS (Network Management System/Element Management System) interface needed to support SONET network management, i.e. the management of aggregates of Network Elements such as subnetworks. Note that the network-view is intended as an aggregate view to provide additional value.

This agreement focuses on what is considered to be the initial functionality of SONET network view management. It is understood that this initial set of functions, managed entities, and scenarios will be enhanced in subsequent versions as the Information Model and OS Platform are further refined.

This agreement focuses on the interface functionality to manage the subnetwork, and does not provide requirements on the management systems themselves. Only Public Data Networks are addressed in this specification, the management of a Private Data Network is not included.

1.3 Guide to Contents

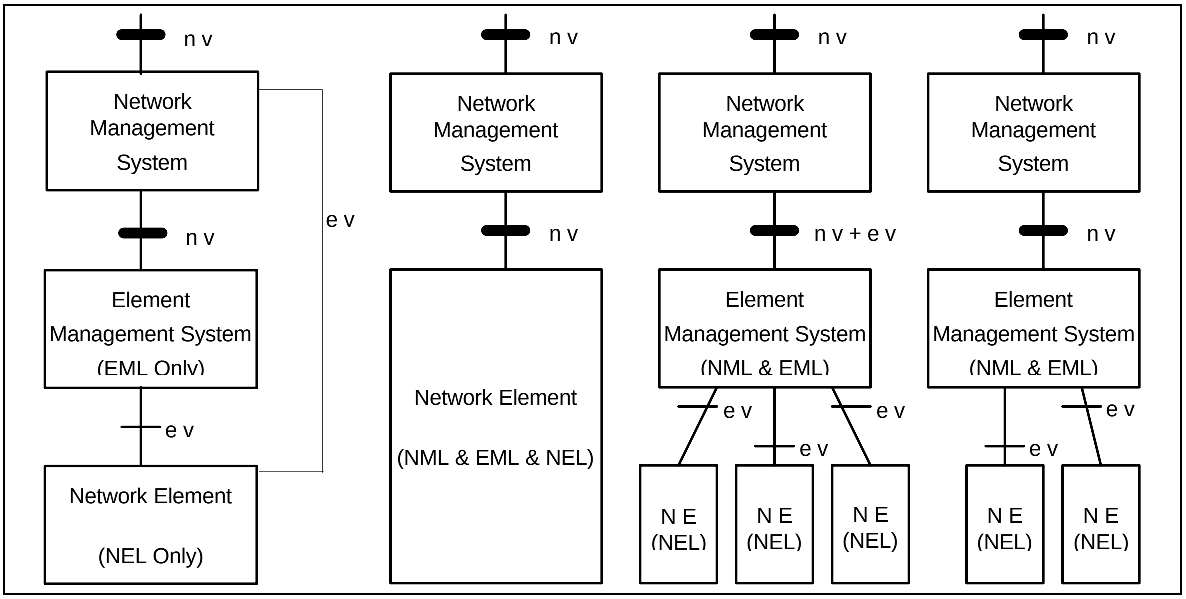
The document is divided into six sections. This section covers introductory information. Section 2 covers the required communication Infrastructure. Section 3 covers security. Section 4 covers the Information Model(s). Section 5 contains the Conformance Requirements. Section 6 contains the Testing and Conflict Resolution Procedures. Section 7 provides a suggested sequence of events and timetable. For a definitions of terms used see Annex A. A filled out MOCS (Managed Object Conformance Statement) Pro Forma, provides a profile of the model – indicating which parts of the model form the base set that is needed to be implemented for interoperability.

1.4 History of the Development Process and Methodology

This document was developed by SIF member companies who are SONET OS and NE providers with help from SIF members who are service providers or who offer consulting services or testing services and tools that are envisioned as being helpful in this process. It represents a consensus on the features and procedures to be followed for the implementation of EMS and NMS connection management and fault management functions. An initial draft was produced in February of 1998. Subsequent discussions of Implementors lead to changes in the SIF model. This agreement is based on the Information Model described in "Network View Model for Connection and Fault Management" (SIF-IM-9810-146R2), and should be regarded as a companion document for Implementors.

1.5 Network Management Architecture: Scope of Agreement

In order to understand which functions are implementers are agreeing to implement, it is necessary to review the philosophy for the network management architecture. One can view the network with its associated network management layers as shown in the figure below. We show here the Network Elements (NEs), EMSs and NMSs, but none of the higher layer management systems. The EMS may address Network Management Layer (NML) and Network Element Layer (NEL) functions along with Element Management Layer (EML) functions. The Network-view (nv) and the NE-view (ev) between the individual management systems are also shown.


n v
Network Management System
n v
e v
Element Management System (EML Only)
e v
Network Element (NEL Only)
n v
Network Management System
n v
Network Element (NML & EML & NEL)
n v
Network Management System
n v + e v
Element Management System (NML & EML)
e v
e v
e v
N E (NEL)
N E (NEL)
N E (NEL)
n v
Network Management System
n v
Element Management System (NML & EML)
e v
e v
N E (NEL)
N E (NEL)

ev - network element view
nv - network view

To support the multiple architectures described in the figure, the SONET NE-view and the SONET Network-view MIBs can be combined in multiple fashions. The SONET network management interface requirements in this document address the EMS/NMS interface, regardless of the functional layers addressed by the individual EMS or NMS. The focus of these requirements is the NMS to EMS interaction needed to support SONET subnetwork management for connection and fault management services.

This document has received the approval of the SONET Interoperability Forum (SIF).

1.6 RELATIONSHIP WITH OTHER SIF DOCUMENTS

This agreement is based on the Information Model described in “Network View Model for Connection and Fault Management” (SIF-IM-9810-146R2), and should be regarded as a companion document for Implementors.

The communications protocol and infrastructure employed by implementers using this will be based on the work of the SIF DNME (Distributed Network Management Environment) group as documented in “Requirements for SIF OS Platforms*”* (SIF-NM-9606-6501). See Section 2.0 which follows for more details.

2. COMMUNICATIONS PROTOCOL AND INFRASTRUCTURE

2.1 Primary Reference

The communications protocol and infrastructure employed by implementers of the Information Model Defined in *Information Model for Connection Management and Fault Management at the EMS/NMS Interface* will be based on the work of the SIF DNME (Distributed Network Management Environment) group as documented in "*Requirements for SIF OS Platforms"* (SIF-NM-9606-6501). The information below has been extracted from that document and modified as noted.

2.2 Scope

OS Platform requirements to support application implementations of TMN layers EML and NML within a TMN are within the scope of this specification. Communications Protocol Requirements for network elements and craft interface terminals are outside of the scope.

The following definition comes from the DNME document:

A SIF OS Platform is defined as a set of components (e.g. communications stacks, tools, management services, security services, etc.) that can be purchased from a single supplier or piece-part from multiple suppliers, and can be used as a uniform environment for the execution of SONET applications... These services are primarily for a CMISE environment.

2.3 Communications Requirements, CMISE Profile

NMF OMNIpoint CMIP Communications Component Set (supplemented by Q.812 [1]***)***, which specifies **-**

- ISP 11183-1: 1992, Specification of ACSE, Presentation and Session Protocols for use by ROSE and CMISE, and
- ISP 11183-2: 1992, AOM12 **-** Enhanced Management Communications.

2.4 Communications Stacks

2.4.1 GENERAL

Communicating applications should agree on which stack will be used for an interface, so that mediation functions within the DCN are minimized.

2.4.2 CMISE

For CMISE communications, it is an objective that the SIF OS Platform shall support the following profile for TP4/CLNP over LAN. While not the preferred choice, TP4 over X.25 and CMISE over

[1] AOM12 is supplemented by Q.812 as follows: "Applications may override the APDU size of 10K specified in AOM12 if a larger size is needed."

RFC1006 [2] with TCP/IP [3] are also allowed. Vendors intending to interoperate need to agree on the stack to be used. It is expected that the NMS will support all three stacks, but undertake interoperability with an EMS using one selected stack**. It is a requirement for interoperability that one of the following three stacks be employed when CMISE is used.**

- ***ITU-T Q.811 CLNS1 (LAN) Protocol Profiles***, which specifies - ISP 10608-1 and ISP 10608-2:1992, Connection-mode Transport Service over Connectionless-mode Network Service - Part 2: TA51 Profile including Subnetwork-dependent Requirements for CSMA/CD LANs. (TP4/CLNS over CSMA/CD LAN)
- ***ITU-T Q.811 CLNS2 (X.25) Protocol Profiles***, which specifies - ISP 10608-1 and ISP 10608-5:1992, Connection-mode Transport Service over Connectionless-mode Network Service - Part 5: TA1111/TA1121 Profile including Subnetwork-dependent Requirements for X.25 Packet Switched Data Networks using Virtual Calls. (TP4/CLNS over X.25)
- ***ITU-T Q.811 RFC1006 with TCP/I***P

2.5 System Management Functions

2.5.1 CMISE

System Management Functions discussed here are application functions common to all TMN (CMISE) applications.

A SIF OS Platform shall support the following Management Function Profiles and standards :

NMF TMN Basic Management Platform Component Set, which specifies -

- ISP 12060-1:1994, AOM211 - General Management Capabilities,
- ISP 12060-4: 1994, AOM221, General Event Report Management,
- ISP 12060-5: 1994, AOM231 - General Log Control,
- NMF 021, Managed Object Naming, Issue 2, 10/95, and
- NMF 015, Shared Management Knowledge, Issue 1, 10/92 + Errata, Issue 1, 10/95, or draft X.750/DIS 10164-16, Management Knowledge Management Function.

[2] RFC1006 is being revised by IETF. The draft RFC is called "ISO Transport Service on top of TCP (ITOT)". The goal is to provide enhancements without introducing interoperability issues with existing RFC1006 implementations.

[3] TCP/IP is not supported on the SONET DCC. Interworking of CLNP and IP is an open issue which the SIF Architecture subgroup is investigating.

3.0 Security

3.1 When 7-layer OSI Stack is Employed

Proposal for securing the SIF EMS-NMS interface (SIF-IM-9802-015 - on the server) requires some assurance from middleware providers that they will really implement the proposed security based on the ACSE Authentication FU in their middleware products - before it can be included in this agreement. This is under study in the Distributed Network Management Group.

3.2 When TCP/IP is Employed as Stack

SSL for CMIP with TCP/IP can be used as agreed by the cooperating vendors.

4.0 MANAGEMENT INFORMATION MODEL PROFILE (based on SIF IM Model)

4.1 Operations Supported in Implementers Agreement

Connection Management

Connection Management Function	Supported in IM Model	Supported in IMPL agreement
Network Topology		
Partitioning	Yes	Yes
A & Z End Points	Yes	Yes
Geographic Location	Yes	Yes
Route selection	Yes	
Rates	Yes	Yes
Protection Schemes		
Subnetwork Protection	No	No
Path Protection	No	No
NMSinitiated Connection Restoration	Not applicable at this interface.	Not applicable at this interface.
Drops Available	Yes	Yes
Scheduling and Reservation	No	No
Bandwidth Availability	Sufficient information is available to calculate route capacity	Sufficient information is available to calculate route capacity
Subnetwork Pools of unused facilities	No	No
Establish Primary and Secondary Connections		
Establish Connection	Yes	Yes
Establish Monitored Connection	No	No
Release Connection	Yes	Yes
Mark TPs and Links as IN-SERVICE	No	No
Notify Connection SUCCESS or FAILURE	Yes	Yes

Fault Management

Fault Management Operations	Supported in IM model	Supported in IMP Agreement
Set Parameters		
* Establish criteria for reliability, availability and survivability. As defined in GR-2869-CORE Generic Requirements for Operations Based on the TMN Architecture:	No	No
* Reliability refers to measures of the mean time between failure and the mean time to repair equipment.	No	No
* Availability refers to the percentage of time services and resources are ready for use.	No	No
* Survivability refers to the robustness of the network in the presence of faults.	No	No
* Register facilities for monitoring	No	No
* Define alarm types to be screened	No	No
* Set up alarm/event thresholds and other event criteria	No	No
* Assign priorities to circuits/components/sessions	No	No
* Set up rule base	No	No
Monitor Network Status		
* Monitoring events and alarms	Yes	Yes
* Maintain log of events and alarms	Yes	Yes
* Status request of any component on the network (automated and manual)	No	No
* Collect/poll for prescreened system events or alarms	Yes	Not covered
* Collect performance information	Yes	Not covered
* Filter duplicate and informational messages	Yes	Yes
* Suppress recurring messages	Yes	Yes
* Suppress minor or informational alarms	Yes	Yes
* Archive events	Yes	Yes
* Continual data analysis and results review	Yes	Not Covered
* Generate event and alarm reports	Yes	Not Covered
Detect Network Deficiencies		
* Update the user interface (network topology)	No	No
* Retrieve alarms	Yes	Yes
* Reformat alarms	Yes	Not covered
* Identify alarms	Yes	Yes
* Identify alarm implications	Yes	Not covered
* Archive alarms	Yes	Not covered
Receive notification of a fault condition from alarms, from the Performance Management System (e.g., exceeding thresholds for PM triggers), or from a customer (via a trouble report or a Customer Network Management system).	Yes for fault conditions from alarms, no for other conditions	Yes for fault conditions from alarms, no for other conditions
Isolate Trouble		
* Heuristic (methodical and intuitive) analysis of alarms	Yes	Not covered
* Correlate alarms	Yes	Not covered
* Review correlation results	Yes	Not covered
* Determine source alarms	Yes	Not covered
* Suppress related alarms	Yes	Not covered

* Test to further isolate trouble and recommend further action for problem resolution.	No	No
Diagnose Fault		
* Analyze event log	Yes	Not covered
* Perform root cause analysis	Yes	Not covered
* Make an informed hypothesis concerning the source of the trouble	Yes	Not covered
* Determine condition severity	Yes	Not covered
* Suggest tests	No	No
* Utilize remote test access and local diagnostic tools to test resources and provide multiple test points along the circuit path	No	No
* Analyze test results	No	No
* Suggest appropriate actions based upon diagnostic results	No	No
Resolve Trouble		
* Initiate the fault resolution process	No	No
* Maintain connectivity to production applications	No	No
* Automatically generate trouble ticket request	No	No
* Track status of the trouble	No	No
* Escalate as necessary	No	No
* Send requests to:	No	No
* Reconfiguration Management to reconfigure network or reroute traffic	No	No
* Connection Management to order new services where required	No	No
Restore Service		
* Initiate full backup, recovery and restore procedures	No	No
* Test the end-to-end connections to assure they work.	No	No
* Clear alarms	No	No
* Modify alarm status indicators	No	No
* Update user interface	No	No
* Mark inventories with failed resources and new routes, all nodes with pertinent state information, etc.		
* Notify all downstream OSS that reconfiguration has occurred.	No	No
* Notify users of reconfiguration, reroute or restoral.	No	No
* Verify restoral of service.	No	No
* Close trouble log and archive	No	No
Restore Original Configuration	No	No

4.2 Profile Overview

This section is intended to show the specific way in which SIF Information Model is adapted for use by Implementors. The model is a rich model, and not all of its features and options are covered by this agreement. In particular:

The focus of this agreement is on:

- Allowing the NMS to discover topological information from the EMS,
- Allowing the NMS to make requests for the addition and deletion of subnetwork connections,
- Supporting fault management so that the NMS can receive autonomously fault notifications and can query the EMS for alarm information.

The following agreements have been made in order to simplify the basic Interoperability agreement. Vendors are free to add additional functionality by agreement. However, having a base set increases the ease and rapidity of integrating SONET operations systems.

1. While the Information Model supports the partitioning of Subnetworks, it is assumed that partitioning is not employed in the basic interface In other words: an EMS manages a set of subnetworks. Subnetworks do not contain other subnetworks.
2. Fault management as covered in this Implementors agreement simply consists of the passing of fault notifications from the EMS to the NMS. The EMS may filter redundant alarms and lower level alarms, but Root Cause Analysis is not implemented.
3. It is assumed that the topology of subnetworks and links is managed by the EMS and discovered by the NMS. The NMS knows of links between Subnetworks managed by different EMSs through provisioning.
4. UserLabels will not be required to be unique and may be used by the NMS to provide additional information (e.g. the customer associated with a subNetworkConnection).
5. Subnetworks can be viewed as being connected by topological links. Link capacity is not managed.
6. Link Connections are covered in the Information Model, but are not used in the basic Implementors agreement.

4.3 Role of the MOCS Pro Forma Profile

The details of exactly what parts of the information model “Network View Model for Connection and Fault Management” (SIF-IM-9810-146R2), are spelled out in the filled out MOCS Pro Forma attached as Appendix A of this document.

Please note that when something is optional in the interface (e.g. routing parameters are optional when setting up an SNC) and the MOCS Pro Forma has been filled in to indicate "yes", what is meant is that the feature is supported by both systems but continues to be optional (not always used).

5. Testing and Conflict Resolution

Although the SIF tries to foresee potential shortcomings of standard or in this case of an implementation agreement, there is room for error. This contribution sets guidelines to use when, in testing two implementations of the SIF Information Model together (NMS and EMS), there comes to light an interoperability issue. This is not to say that the only possibilities for conflict resolution reside in this document, but this is an attempt to create a SIF procedure for resolution.

This document is meant for use with the SIF document entitled “Implementers Agreement on Connection Management and Fault Management for EMS to NMS.” However it can generically apply to other scenarios where SONET interoperability is a concern.

Testing:

Interoperability testing of SONET systems is often referred to as an art. This is because there are no well-defined interoperability tests. Typically, interoperability is tested by brute force (i.e., interconnecting systems and observing operation). This approach is limited in that it generally fails to apply real-world stresses. Therefore, this type of testing only reveals the level of interoperability under “sunny day” scenarios.

Figure 2, below, expresses interoperability testing in the form of a flow chart:

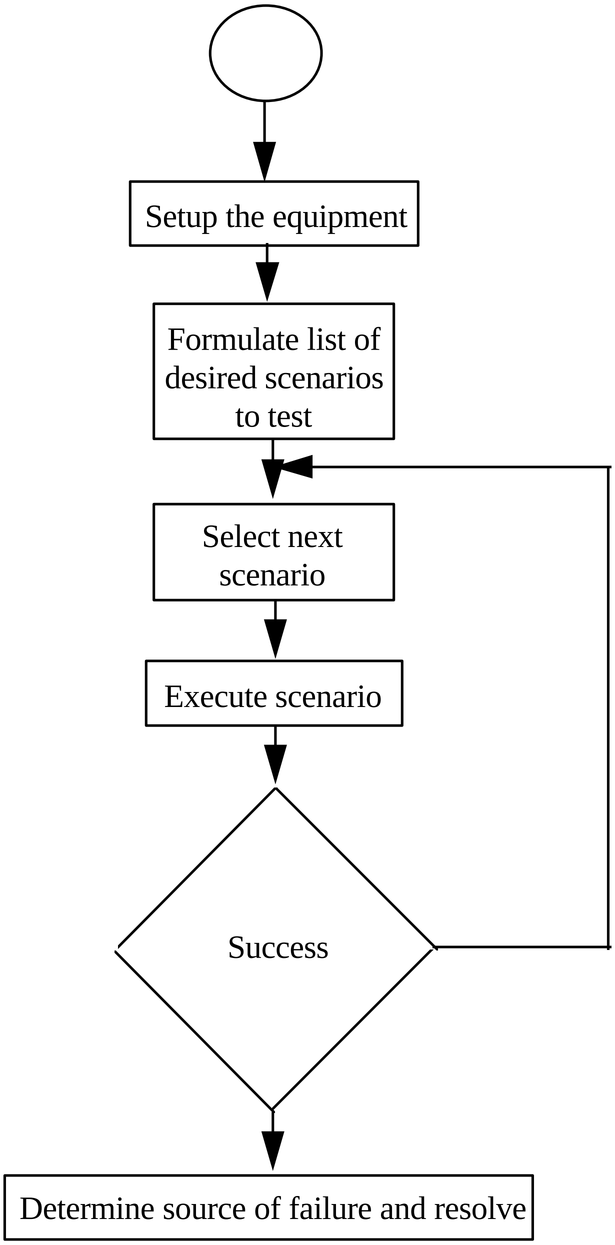

Setup the equipment
Formulate list of desired scenarios to test
Select next scenario
Execute scenario
Success
Determine source of failure and resolve

Figure 2

The scenarios for use with the SIF Information Model can be found in the SIF Implementers Agreement document. The most difficult part of interoperability testing is referred to in the above figure as "Determine source of failure and resolve." This most often requires a human to analyze data captured while running the scenario and determining where the disconnect in the communications occurred. For testing of the Information Model there are two basic conclusions to come from such an analysis. Either the problem is in the transport of the application data (i.e., the OSI stack or CMOT) or in the application itself.

As an overview, interoperability testing should be done following stand-alone conformance testing. Clearly, the majority of interoperability issues are in reality, stand-alone conformance issues. Potential interoperability issues include: differences in features supported, provisionable vs. non-provisionable options, and conflicting criteria interpretation. Often, a paper analysis comparing the results of two stand-alone analyses will reveal interoperability issues. The best approach to hands-on testing allows the analyst the ability to see inside the black box of communications between the systems. To do this one must have the ability to monitor and decode the operations traffic among the systems under test. This traffic is segmented into the protocols used for transport (7-layer OSI, CMOT, etc.) and the application (e.g., the SIF Information Model). By decoding each protocol and PDU in the data stream, an analyst can compare the traffic to the published standards and identify issues.

In the event that an interoperability issue is encountered, there are a few steps that should be taken before bringing it in for resolution by the SIF. It should be certain that it is not a nonconformance on the part of one or more of the products involved. This should have been addressed in the stand-alone conformance phase of the testing, but there are no guarantees that 100% of all conformance issues are captured in a conformance analysis. Once the issue is determined to be one of conflicting standards interpretation, then it should be brought to SIF for resolution.

Conflict Resolution:

In the absence of a more structured approach to interoperability testing, or in the event where the brute force method reveals issues. It is essential to have a means of resolution. The issue of conflicting criteria interpretation creates the need for resolving conflicts. The parties involved may include the suppliers, the service provider, the suppliers' sub-contractors, and the testing agency. Any of these groups may seek conflict resolution.

When, during interoperability trials, an issue that cannot be resolved among the involved parties is encountered, there needs to be a procedure in place for correction of the standards or implementation agreements. The procedure has the following objectives:

- Provide a rapid response,
- Unbiased and focused on the overall good of the industry,
- Protect parties from industry-wide embarrassment and protection of proprietary information.

The simplest approach may be for the involved parties to collaborate and provide a clear overview of the issue to the SIF body via an exploder. This approach has an advantage of meeting the objective for rapidly getting information to the SIF body. However, it does not provide for the third objective. So, this approach should be considered the first option if all of the involved parties agree to the approach and content.

However, in the case where all parties cannot agree and keeping the above guidelines in mind, the following conflict resolution procedure is proposed. When an organization discovers an interoperability issue that it feels needs to be addressed in the SIF for updates to the Implementers Agreements, they should do the following.

- Bring the problem to a neutral third party (e.g., ATIS) to be presented to the SIF Information Model Implementation subgroup (IMI SG) in such a manor as not to disclose the identities of the parties involved unless consent is granted.

- Details of the issue will be placed on the general SIF email exploder for all of the SIF members to see and bring the appropriate personnel to the next meeting of the IMI SG.

- The IMI SG will place the issue on its agenda and either achieve resolution at its next meeting to be brought for vote at the following meeting's plenary session, or announce a schedule for the resolution of the issue. The hope is that no company will have to wait more than 4 months before resolution of their issue is attained.

- Once resolution of the issue is achieved, the new information necessary to conform to it will be placed in the SIF Implementers Agreements document.

- The Implementation Workgroup will then be responsible for identifying and industry liaison that may be required to obtain resolution through other non-SIF bodies.

....

6.0 References

The following two SIF documents form a core part of this recommendation:

“Network View Model for Connection and Fault Management” (SIF-IM-9810-146R2),.

“Requirements for SIF OS Platforms” (SIF-NM-9606-6501.

The following standards contain information used while defining the information model used in this agreement.

ITU-T Recommendation G.774 (09/92), *Synchronous Digital Hierarchy (SDH) Management Information Model for the Network Element View*.

ITU-T Recommendation G.774.01 (11/94), *Synchronous Digital Hierarchy (SDH) Performance Monitoring for the Network Element View*.

ITU-T Recommendation G.774.02 (11/94), *Synchronous Digital Hierarchy (SDH) Configuration of the Payload Structure for the Network Element View*.

ITU-T Recommendation G.774.03 (11/94), *Synchronous Digital Hierarchy (SDH) Management of Multiplex-Section Protection for the Network Element View*.

ITU-T Recommendation G.774.04 (07/95), *Synchronous Digital Hierarchy (SDH) Management of the Subnetwork Connection Protection for the Network Element View*.

ITU-T Recommendation G.774.05 (07/95), *Synchronous Digital Hierarchy (SDH) Management of Connection Supervision Functionality (HCS/LCS) for the Network Element View*.

ITU-T Recommendation G.805 (11/95), *Generic Functional Architecture of Transport Networks*.

ITU-T Draft Recommendation G.853-01, *Common Elements of the Information Viewpoint for the Management of a Transport Network*.

ITU-T Draft Recommendation G.853-02, *Subnetwork Connection Management Information Viewpoint*.

ITU-T Draft Recommendation G.855-01.

ITU-T Recommendation M.3100 (07/95), *Generic Network Information Model*.

ITU-T Recommendation X.710 (03/91), *Common management information service definition for CCITT applications*.

ITU-T Recommendation X.721 (02/92), *Information Technology - Open Systems Interconnection - Structure of Management Information: Definition of Management Information*.

ITU-T Recommendation X.733 (02/92), *Information technology – Open Systems Interconnection – Systems Management: Alarm reporting function*.

ITU-T Recommendation X.734 (09/92), *Information technology – Open Systems Interconnection – Systems Management: Event report management function*.

ITU-T Recommendation X.735 (09/92), *Information technology – Open Systems Interconnection – Systems Management: Log control function*.

AF-NM-0058.000, *NMS/EMS Network View Interface Requirements, and Logical MIB*, (ATM Forum Technical Committee)

AF-NM-0073-000 Letter Ballot, *M4 Network View CMIP MIB Specification* Version 1.0, November 1996.

GR-253-CORE (December 1995), *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria (A Module of TSGR, FR-NWT-000440)*, Issue 2, (Bellcore)

TR-NWT-000496 (May 1992), *SONET Add-Drop Multiplex Equipment (SONET ADM) Generic Criteria*, Issue 3, (Bellcore).

GR-1042 (September 1997), *Generic Requirements for Operations Interfaces Using OSI Tools - Information Model Overview: Synchronous Optical Network (SONET) Transport Information Model*, Issue 2, (Bellcore)

SR-TSV-002671 (June 1993), *EML Applications for Fault Management: Subnetwork Root Cause Alarm Analysis*, Issue 1 (Bellcore).

SR-TSV-002672 (March 1994), *EML Applications for Fault Management: Intelligent Alarm Filtering for SONET*, Issue 1 (Bellcore).

GR-2869-CORE (October 1996), *Generic Requirements for Operations Based on the TMN Architecture*, Issue 2 (Bellcore).

ANNEX A Definitions (note that this is reproduced from the IM document)

This section lists the terms and definitions used in this document. Many of these terms have different definitions in other standards documents. Attempts were made to adopt the most common definition of each term. The definition includes the context in which the term is used. Where possible, the relationship between a term and the real world is provided.

KEY:

- "double quotes" **-** term is defined elsewhere in this glossary
- *italics* **-** element of the SIF Information Model (e.g., object, attribute, etc.)

access group

A group of co-located "network trail termination points" within a "layer network domain." The *sonetAccessGroup* managed object class is used to represent an access group in the model.

administrative domain

A set of network and administrative resources grouped for management purposes. For the NMS/EMS interface, the grouping of managed objects corresponds to the resources managed by an EMS agent. An administrative domain will typically encompass a number of "layer network domains" associated with distinct transport layers. The *networkR1* managed object class is used to represent an administrative domain in the model.

Client/Server (C/S) Pointers

The client pointer attribute (clientLayerNCTP) identifies the object instances of the related sonetNetworkCTP (and subclasses) in the clientserver layer. The
sonetNetworkCTPs may belong to multiple sonetLayerNetworkDomains. The server pointer attribute (serverLayerNTTP) identifies the object instance of the related networkTTP (and subclasses) in the server layer.

characteristic information

A signal with a specific rate and format, which is transferred on "network connections"[G.853-01]. Characteristic information is also associated with termination points independent of whether or not they are supporting connections. The potential signal formats include signals of the SONET hierarchy (VT/STS/OC) and digital tributary signal formats (DS1, DS3).

connection management

A management application designed to manage the set-up, release, and modification of subnetwork connections and trails in a layer network. Connection management will generally require application functions in multiple TMN management layers (i.e., SML, NML, EML, and NEL). Although the focus is on configuration management, functions in other functional areas (e.g., fault, performance management) may be included in the application. SIF functional requirements for a SONET connection management application are described in G.805.

Connection Termination Point (CTP)

A Connection Termination Point is a managed object that terminates a link connection. See M.3100.

Downstream Connectivity Pointer (DCP)

Defined in M.3100, the downstream connectivity pointer attribute points to the termination point managed object, within the same managed element, that receives information (traffic) to this termination point at the same layer, or is null.

drop

The port on a SONET network element where the service to an end customer may be connected, e.g., a tributary card on a SONET ADM. For example, a drop for a DS1 customer service may be provided by a VT1.5 card terminating a VT1.5 trail.

drop and continue

The ability of a SONET add-drop multiplex to pass the same signal (STS/VT) that is being dropped onto the outgoing OC-N signal[SR-2672].

dynamic subnetworks

A management capability that allows modification of a subnetwork's properties in terms of termination points or contained subnetworks and links under partitioning. A typical modification would be the reallocation of sNTPs.

Element Management Layer (EML)

An abstraction of the functions provided by systems which manage each network element on an individual basis.

Element Management System (EMS)

A management system, which provides functions at the Element Management Layer, and could also include functions at the Network Management Layer. The "administrative domain" associated with the EMS agent could be delimited by geographical area, topology, or supplier product (as examples) within the provider's network.

hardwired multiplex

An add-drop multiplex configuration in which specific VT/STS-1 time-slots are dedicated to specific low-speed ports[SR-2672].

layer network

A "topological component" that includes other topological components, transport entities, and transport processing functions that describes the generation, transport and termination of a particular characteristic information[G.853-01].
As an example, a layer network may be associated with SONET STS-1 transport.

layer network domain

The part of a layer network which is managed by a management system[G.853-01]. For the NMS/EMS interface, the relevant management system is the EMS. The *sonetLayerNetworkDomain* managed object class is used to represent a layer network domain in the model.

link

A “topological component” that provides transport capacity between two endpoints in different subnetworks via a fixed (i.e., inflexible routing) relationship[4]. The endpoints are “subnetwork termination point pools.” Multiple links may exist between a pair of subnetworks. A link also represents a set of “link connections.” The *sonetLink* managed object class is used to represent a link in the model.

link connection

A “transport entity” that represents the fixed capacity of transfer of “characteristic information” transparently across a link. A link connection is delineated by “network connection termination points” or “NE-view connection termination points.” The “network connection termination points” can be associated with “subnetwork termination points” by relationship. The *sonetLinkConnection* managed object class is used to represent a link connection in the model.

Management Applications Function (MAF)

An application process participating in system management. The management application function includes an agent (being managed) and/or manager[G.784].

multiple partitioning views

A management capability that supports more than one scheme of partitioning subnetworks. This allows the use of different partitioning schemes for different functional areas or different management systems.

network connection

A “transport entity” formed by a series of contiguous "link connections" and/or "subnetwork connections" between subnetwork termination points. A network connection may extend across “layer network domains” associated with more than one “administrative domain.” A network connection is not represented by an object class in the model.

network connection termination point

An extremity of a “link connection”[G.855-01]. It is also a network level abstraction of a nodal (NE) view connection termination point. The *networkCTP* managed object class is used to represent a network connection termination point in the model.

network connection termination point bidirectional

A network connection termination point that represents the functionalities of both a network connection termination point source and network connection termination point sink in the model.

network connection termination point sink

A unidirectional network connection termination point that is intended to be bound to the output of a unidirectional “link connection.” The *sonetNetworkCTPSink* managed object class is used to represent a network connection termination point sink in the model.

network connection termination point source

A unidirectional network connection termination point that is intended to be bound to the input of a unidirectional “link connection.” The *sonetNetworkCTPSource* managed object class is used to represent a network connection termination point source in the model.

[4] An exception to the “fixed” relationship is when protection mechanisms are applied.

Network Element (NE)

A system that supports at least “NEFs” and may also support “Element Management Layer” Functions/Mediation Functions. It cannot be further decomposed into managed elements in the context of a given management function.

Network Element Function (NEF)

A function within a SONET entity that supports the SONET based network transport services, e.g. cross-connections.

Network Element Layer (NEL)

An abstraction of functions related specifically to the technology, vendor, and the network resources or network elements that provide basic communications services.

network element view (NE view)

The network element view is the network view representing information received directly from network elements which is defined in other information models such as GR-1042.

Network Management Layer (NML)

An abstraction of the functions provided by systems which manage network elements on a collective basis as subnetworks, and/or as individual entities.

Network Management System (NMS)

An entity which implements functions at the Network Management Layer. It may also include Element Management Layer functions.

NMS Environment - *under study*

A set of Network Management Systems (NMS) which cooperate to manage one or more subnetworks.

network trail termination point

An extremity of a “trail”[G.855-01]. It is also a network level abstraction of a nodal (NE) view trail termination point. A network trail termination point includes trail termination functions that ensure integrity of information transport on an end-to-end basis (see Figure I.2 in [G.855-01] for a mapping between termination point managed objects[G.855-01] and termination functions and access points in a functional network architecture[G.853-01]). The *sonetNetworkTTP* managed object class is used to represent a network trail termination point in the model.

network trail termination point bidirectional

A network trail termination point that represents the functionalities of both a network trail termination point source and network trail termination point sink in the model.

network trail termination point sink

A network trail termination point that is intended to be bound to the output of a unidirectional trail. The *sonetNetworkTTPSink* managed object class is used to represent a network trail termination point sink in the model.

network trail termination point source

A network trail termination point that is intended to be bound to the input of a unidirectional trail. The *sonetNetworkTTPSource* managed object class is used to represent a network trail termination point source in the model.

network view

The network view is an abstracted view of the network which would include some level of NE connectivity.

NE-view connection termination point

A managed object class defined in an information model for network elements which represents the termination of a link connection.

NE-view trail termination point

A managed object class defined in an information model for network elements which represents the termination of a trail.

partitioning

The decomposition of a “subnetwork” into its component “subnetworks” and “links” in a way that reflects the internal structure (topology) of that “subnetwork” or the way that it will be managed. Partitioning may be based on a variety of factors including architecture (e.g., BLSR), supplier product line, or administrative considerations.

point-to-point route

A point-to-point route consists of two end points and, optionally, intermediate points in a layer network. Each end point or intermediate point will consist of a set of sNTPs in the same layer network.

protection

In the network view, protection refers to the ability to switch service from a primary “transport entity” to a preconfigured backup “transport entity” in response to a detected failure on the primary “transport entity.” Protection mechanisms may be entirely within a “layer network” or may involve a server layer mechanism supporting client transport services, and may be activated on the basis of a variety of monitoring. Trail protection is a protection method applied in a “layer network” when a defect condition is detected in the same “layer network.” Subnetwork connection protection is applied in the client layer network when a defect condition is detected in a server layer network, sub-layer or other transport layer network.

restoration

In the network view, restoration refers to an application in which the NMS responds to a confirmed failure by requesting a new connection. This action may be viewed by the EMS as a release of the failed connection and the set-up of a new connection.

route

A sequence of geographical or topological points or components through which “transport entities” may be established. “Transport entities” within a route have common endpoints and common intermediate points (if intermediate points are specified). The role of route endpoint may be played by a “subnetwork” or “access group;” an intermediate point may be associated with a “subnetwork,” or “subnetwork termination point pool.” In an unpartitioned subnetwork view, the route includes all potential connections in the “subnetwork” between “access groups;” in a fully-partitioned subnetwork view, the route may include all available connections supported by a specific set of paths (links) and NEs (fabrics).

route capacity

A measure of the transport capacity available on an end-to-end basis on a specific “route” within a “layer network domain.”

route separation

A qualitative measure of the relationship between “routes” assigned to primary and protection connections.

service

Service or transport service is the communications product purchased by a customer, represented by a “subnetwork connection.” Services come in many forms, including switched services, data services, and private line services. See “Service Characterics” for additional details.

state

State is an attribute type representing the condition or an object instance. See X.721.

subnetwork

A “topological component” used to effect routing of a specific “characteristic information”[G.853-01]. A subnetwork is associated with a specific “layer network.” Within a given layer, “partitioning” may be applied to decompose a subnetwork into its component subnetworks and links. The *sonetSubnetwork* managed object class is used to represent a subnetwork in the model.

subnetwork connection (SNC)

A “transport entity” that transfers information across a subnetwork[G.853-01]. A point-to-point subnetwork connection connects two “subnetwork termination points.” An SNC may be either a stand-alone SNC, or a concatenation of SNCs and link connections. The *sonetSubnetworkConnection* managed object class is used to represent a subnetwork connection in the model.

Subnetwork Management System (subNMS) - *under study*

A Network Management System, which is managing one or more subnetworks, and which is managed by one or more Network Management Systems.

subnetwork termination point

An abstraction that represents the binding between a “subnetwork” and either a “network connection termination point” or a “network trail termination point.” It also represents the potential for connection across a subnetwork[G.855-01]. A subnetwork termination point is represented in the model by the *sonetSNTP* object class.

subnetwork termination point bidirectional

An abstraction that represents both a sink and a source subnetwork termination point. An *sonetSNTPBidirectional* object class represents this abstraction in the model.

subnetwork termination point pool

A set (possibly empty) of subnetwork termination points at the frontier of a given subnetwork[G.855-01]. In SONET, a subnetwork termination point pool is used to terminate a link. An *sonetSNTPPool* object class represents this abstraction in the model.

subnetwork termination point sink

A subnetwork termination point that represents the potential binding of the output of a unidirectional “subnetwork connection” and either a “network connection termination point source” or a “network trail termination point sink.” The *sonetSNTPSink* object class represents this abstraction in the model.

subnetwork termination point source

A subnetwork termination point that represents the potential binding of the output of either a unidirectional “link connection” or a “network trail termination point source” and the input of a unidirectional “subnetwork connection.” The *sonetSNTPSource* object class represents this abstraction in the model.

subnetwork capacity

A measure of the total/available transport capacity within a subnetwork. This measure may be useful in planning for network topology changes. (See “route capacity.”)

Termination Point (TP)

A Termination Point is a managed object that terminates “transport entites” such as “trails” and connections. See M.3100.

Time-Slot Assignment (TSA)

The capability to flexibly assign add-dropped signals, but not through signals. Through signals maintain the same time-slots on the incoming and outgoing signals[SR-2671].

Time-Slot Interchange (TSI)

The capability to flexibly assign both add-dropped signals and through signals[SR-2671].

topological component

An architectural component, used to describe the transport network in terms of the topological relationships between sets of points within the same “layer network”[G.853-01]. Examples of topological components include “layer network,” “subnetwork,” and “link.”

trail

A "transport entity" which consists of an associated pair of "unidirectional trails" capable of simultaneously transferring information in opposite directions between their respective inputs and outputs[G.853-01]. A trail also represents the transfer of “characteristic information” between “network trail termination points” or “NE-view trail termination points.” A trail is supported by a “subnetwork connection” or “network connection” and in addition includes trail termination functions that ensure integrity of information transport (i.e., via monitoring) on an end-to-end basis. A trail may be established to directly support an end-to-end network service or to provide “link connections” within the client layer. A trail is represented in the model by the *sonetTrail* managed object class.

trail termination function

A transport processing function that allows the monitoring of information transport on trails on an end-to-end basis. Two types of trail termination functions are defined: a trail termination source adds monitoring information to the “characteristic information” input at one end; a trail termination sink removes the monitoring information and presents the “characteristic information” at the other end.

Trail Termination Point(TTP)

A Trail Termination Point is a managed object that terminates a trail. It represents the access point to a subnetwork. See M.3100.

transport entity

An architectural component which transfers information between its inputs and outputs within a “layer network”[G.853-01]. Examples of transport entities include “subnetwork connection,” “link connection,” and “trail.”

Upstream Connectivity Pointer (UCP)

Defined in M.3100, the upstream connectivity pointer attribute points to the termination point managed object, within the same managed element, that sends information (traffic) to this termination point at the same layer, or is null.

Acronyms

ADM	Add Drop Multiplexer
AIS	Alarm Indication Signal
APS	Automatic Protection System
ATMF	Asynchronous Transfer Mode Forum
BLSR	BiDirectional Line Switched Ring
BML	Business Management Layer
C/S	Client/Server
CMISE	Common Management Information Service Element
CTP	Connection Termination Point
DCN	Digital Communication Network
DCP	Downstream Connectivity Pointer
DCS	Digital Cross-connect System
DSn	Digital Signal hierarchy, layer n
EFD	Event Forwarding Discriminator
EML	Element Management Layer
EMS	Element Management System
E-R	Entity-Relationship
ETSI	European Telecommunications Standards Institute
GDMO	Guidelines for the Definition of Managed Objects
ITU-T	International Telecommunications Union
LOF	Loss of Frame
LOP	Loss Of Pointer
LOS	Loss of Signal
MAF	Management Application Function
MIB	Management Information Base
NE	Network Element
NEF	Network Element Function

NEL	Network Element Layer
NMF	Network Management Forum
NML	Network Management Layer
NMS	Network Management System
NSA	Non-Service-Affecting
OC-N	Optical Carrier - level N
OOF	Out Of Frame
OS	Operating System
OSI	Open Systems Interconnection
OTDR	Optical Time Delayed Reflectometry
QOS	Quality Of Service
PM	Performance Monitoring
RCAA	Root Cause Alarm Analysis
RDI	Remote Defect Indication
RFI	Remote Failure Indication
SA	Service-Affecting
SLM	Signal Label Mismatch
SML	Service Management Layer
SNC	SubNetwork Connection
SOA	Statement Of Application
STS-N	Synchronous Transport Signal level N
STS-Nc	Synchronous Transport Signal level N, concatenated
TCA	Threshold Crossing Alarm
TMN	Telecommunications Management Network
TP	Termination Point
TSA	Time-Slot Assignment
TSI	Time-Slot Interchange
TTP	Trail Termination Point
UCP	Upstream Connectivity Pointer
UPSR	UniDirectional Path Switched Ring
VT	Virtual Tributary

....