SONET Interoperability Forum

NE-NE Remote Login

Initial Solution Evaluation Criteria

This document is a working draft which does not represent a consensus of the SONET Interoperability Forum (SIF).

Document Number: **SIF-RL-9605-043-R4**

Issue Date : **6/12/96**

TABLE OF CONTENTS

LIST OF FIGURES

REVISION HISTORY

ISSUE	DATE	SUMMARY OF CHANGES
R1	5/28/96	initial release
R2	6/4/96	revised per comment by Mark Jones (Sprint) and Brett Hammond (GRCI). These communications were made available on the sif-rlogin mail exploder.
R3	6/7/96	revised per agreements of review held by conference call on 6/4/96.
R4	6/12/96	revised per agreements during SIF meeting on 6/12/96.

1. Introduction

The SONET Interoperability Forum (SIF) has identified a need to provide a multi-vendor solution for network element to network element (NE-NE) remote login. An 'NE-NE Remote Login Sub-group' has been formed by the SIF to address this need. The charter of the sub-group is

> To define the communications architecture and interfaces necessary to allow a craftsperson at a craft inteface terminal to manage a network element at a remote site without the mediation of an intermediate management system. The communciations architecture and interface definitions must promote interoperability in a multivendor environment.

The Sub-group has defined remote login as:

Definition of NE-NE Remote Login: 'craft access to network elements from a remote site for the purpose of managing that network element'

1.1 Purpose of this document

The purpose of this document is to define the "user" requirements (see Section 1.4 for definition of "user" for NE-NE remote login in a multi-vendor environment). That is, this document defines the user expectations for the behavior and features of remote login.

This document will be used to validate proposals for the solutions proposed for the NE-NE remote login. As such, this document will describe requirements for the proposed solutions.

1.2 Purpose of the SIF Project on NE-NE Remote Login

The purpose of NE-NE remote login as defined in Section 1 is to provide remote access to management functionality of a network element. This document is intended to define user requirements incremental necessary for this remote access.

The following list identifies possible network provider applications for NE-NE remote login:

- initial turn–up of network elements and/or systems (e.g., test the operation of a SONET ring)
- trouble verification
- repair verification
- monitor NE performance (e.g., query PM data)
- update NE software and hardware
- manual control of NE (e.g., protection inhibit/restore, manual protection)
- remote inventory

1.3 Scope

User requirements for craft interface terminals, network elements, and networking are within the scope of this specification. These will typically be described in terms of requirements for the solution to NE-NE remote login.

1.4 Definitions

Craft Interface The connection between a network element and the terminal.

Craft Interface Terminal The laptop or computer terminal ("dumb" terminal) used by the craftsperson.

Craftsperson Network service provider personnel.

DCN The Data Communications Network (DCN) can consist of a wide area network, local communications network, data communications channel(s), or any combination thereof.

Intermediate NE A network element on the communication path between the local NE (NE_A) and the remote NE (NE_Z). NE_A and NE_Z are not considered to be intermediate NEs.

Laptop A portable computer carried by the craftsperson.

1.5 Acronyms and Abbreviations

CIT Craft inteface terminal

DCN Data communications network

GUI Graphical user interface

LCN Local communications network

NE Network element

WAN Wide area network

1.6 References

1) ”User Interface Generic Requirements for Supporting Network Element Operations,” Bellcore GR–826–CORE, Issue 1, June 1994, Section 10.2 of OTGR.

2. User Requirements

The following sub–sections define the key areas of user requirements for NE-NE remote login.

2.1 Formatting Key

The following designation will be used throughout this section.

(R-n) identifies a requirement

(O-n) identifies an objective

2.2 Architecture

Figure I shows the NE-NE Remote Login Architecture Model. The CIT connects to the Local NE (NE_A) to gain access to the Remote/Target NE (NE_Z). NE-NE Remote Login traffic between NE_A and NE_Z is sent over the DCN.

DCN is shown here as a generic Data Communications Network and, depending on the implementation, would consist of any combinations of SONET DCC or Local Area Network in the central office (i.e., LCN). Thus, in addition to SONET NEs, the DCN would involve Routers, Hubs, and other Switching Elements of the LCN.

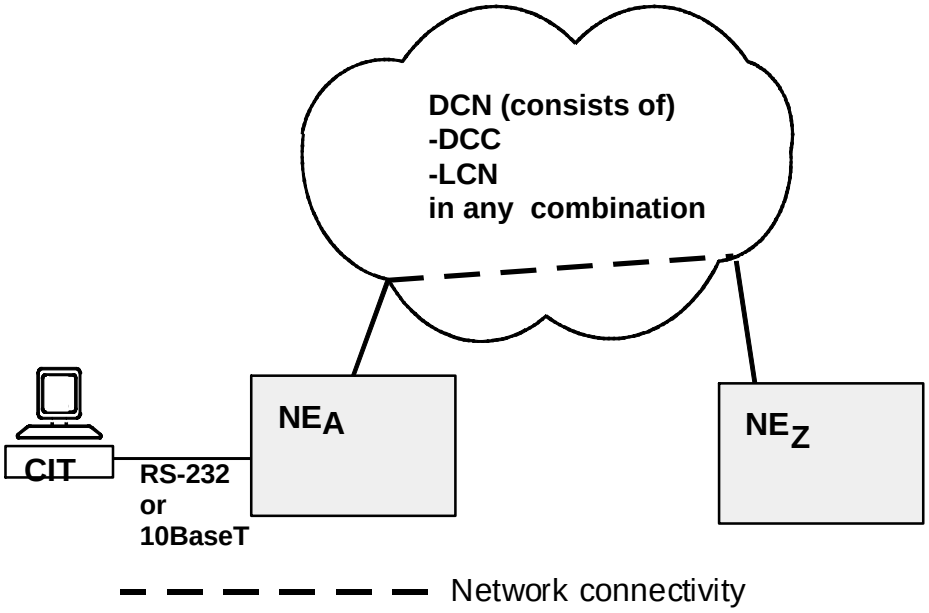

Figure I. Architecture Model Model for Remote Login to Far End NE

(R-1) Remote login shall follow the architecture defined in Figure I.

(R-2) The DCN shall be based on CLNP, ES-IS and IS-IS as specified in GR-253-CORE.

(R-3) The solution shall not require intermediate NEs to perform functions other than routing (i.e. process CLNP, ES-IS, IS-IS) as specified in GR-253-CORE.

2.3 Craft Interface Device

2.3.1 Physical Connector(s)

2.3.1.1 Connection to NE

(R-4) The primary connection between the CIT and the local NE shall be either:

- 10BaseT or
- RS–232

but not both. An optional secondary connection may be proposed and shall be:

- 10BaseT or
- RS–232

Primary and Secondary connections shall not be used simultaneously. A solution shall specify which type of interface shall be used.

(R-5) If a 10BaseT connection is used between the CIT and the local NE, it shall use 802.3 LLC1 at layer2 and CLNP at layer 3 per GR-253-CORE.

2.3.2 Minimum Processing Capacity

(R-6) The solution shall support a laptop as the craft interface device, a dumb terminal as the craft interface device, or both.

(R-7) If a laptop is used for the craft interface device, the laptop shall not be required to have more than the equivalent processing capacity of an 80486 CPU based computer.

2.3.3 Software Administration

2.3.3.1 Vendor Dependent Software

Users are willing to support different software modules on the CIT that are specific to different network management systems. This would include the distribution and synchronization of the different software modules. However, one goal should be to minimize the need for managing vendor specific software on the CIT.

(O-8) The need for managing (i.e. distributing, installing, configuring, maintaining, configuration managing, updating, etc.) vendor specific software on the CIT shall be minimized.

2.3.3.2 CIT Operating Environment

Any vendor specific software shall be developed to a common CIT operating environment.

(R-9) If a laptop is used for the CIT, the solution shall allow the laptop to be the NE-NMS remote login remote CIT.

(R-10) If a laptop is used for the CIT, the laptop shall be an IBM-PC compatible computer.

(R-11) If a laptop is used for the CIT, the solution shall specify the required operating environment.

2.3.3.3 Support for Multi–vendor Network Elements

(R-12) The solution shall support the ability to login to different vendors network elements from a single CIT.

2.3.4 Sessions

(O-13) The craftsperson shall be able to login to multiple network elements simultaneously.

(R-14) If multiple simultaneous sessions are supported, the user interface shall clearly identify the target network element of the management operations.

2.3.5 Network Element

See Section 2.2.1.1 for a description of the physical connection between the NE and the CIT.

2.4 Remote Network Element

2.4.1 Physical Connector(s)

(R-15) The physical connectors between the remote network element and the DCN shall be as defined in GR-253-CORE.

2.4.2 Layer 2 and Layer 3 connections

(R-16) Layer 2 and Layer 3 connections shall use 802.3 LLC1 at layer2 and CLNP at layer 3 per GR-253-CORE.

2.4.3 Sessions

(O-17) Mutiple simultaneous NE-NE rlogin sessions into a single remote NE shall be supported.

2.5 User Interface

2.5.1 User Interface Display Mode

Although it is not a requirement that a GUI be supported, the solution shall not prevent NE vendors from placing a GUI over the solution recommended by SIF.

(R-18) If a laptop is used for the CIT, the solution shall not preclude the use of a GUI on the laptop.

(O-19) The solution shall use a GUI.

2.5.2 Response time

(O-20) If a standard typing mode is used, under normal operating conditions the time between a keystroke and the character being displayed on the terminal shall be less than 100ms.

2.5.3 Synchronization of Operation

(R-21) The acknowledgment of a completed operation at the CIT user interface shall occur only after the entity responsible for completing the requested operation has done so.

2.6 Name Resolution

(R-22) The solution shall not preclude the use of any name resolution conventions adopted by SIF.

2.7 Network Bandwidth Constraints

(R-23) The solution shall work within the bandwidth constraints of the SONET section DCC.[1]

2.8 Availability

The availability of NE-NE remote login depends on the availability and performance of the network.

(O-24) The NE-NE remote login solution shall maximize the availability of NE-NE remote login functions during periods of network stress and/or disaster and/or turn-up.

2.9 Security

(R-25) The solution shall use an authorization and authentication scheme, which at a minimum may use clear-text transfers.

2.10 Time to Market

(O-26) The solution shall be immediately implementable by network element vendors.

[1] Not all of this bandwidth will be available for NE-NE remote login (the bandwidth is shared).

2.11 Reuse

(O-27) The solution shall employ existing standards as much as possible.

3. Bibliography

1) ”Remote Login User Requirements,” SIF–95/001, SONET Interoperability Forum, April 18, 1995.