SIF-Approved document #: SIF-009-1997
(SIF Contribution #: SIF-RL-9611-088R2)

Contribution to

SONET Interoperability Forum

PROJECT: **Remote Login**

TITLE: **NE-NE Remote Login Implementation Requirements Specification**

SOURCE: **SIF NE-NE Remote Login Subgroup**

CONTACT: **Ed Snyder**
Lucent Technologies
Room 21-3C41
1600 Osgood St.
North Andover, Ma. 01845
508-960-4362
ecs@mvjok.lucent.com

DATE: **February 13, 1997**

ABSTRACT: **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. This document defines the implementation requirements for this feature in such a way as to allow implementors to satisfy the needs of users.**

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

February 13, 1997

TABLE OF CONTENTS

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

February 13, 1997

REVISION HISTORY

ISSUE	DATE	SUMMARY OF CHANGES
First Draft	11/11/96	
Second Draft	12/3/96	Incorporated comments from 11/18 conference call; added more detail
Release 1	12/5/96	Incorporated comments and agreements from 12/4 meeting.
Release 2	02/13/97	Approved version.

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 interface terminal to manage a network element at a remote site without the mediation of an intermediate management system. The communications architecture and interface definitions must promote interoperability in a multivendor environment.

The SIF had previously produced a recommendation in support of remote login to an NMS [1]. The current work is intended to complement this earlier effort.

The present Sub-group has produced evaluation criteria for NE-NE Remote Login [2] that were used to bound the various proposals and to shape the solution documented here. This solution has also been heavily influenced by the results of a survey completed by service providers within SIF [3].

1.1 Purpose of this document

The purpose of this document is to define the "implementation" requirements for NE-NE remote login. The requirements in this document are intended to allow implementors to satisfy the needs of users as documented in [2] and [3].

1.2 Scope

Implementation requirements for craft interface terminals, network elements, and networking are within the scope of this specification.

1.3 Definitions

Craft Interface Terminal The laptop or computer 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.

Laptop A portable computer carried by the craftsperson.

1.4 Acronyms and Abbreviations

ACSE Association Control Service Element

AETitle Application Entity Title

API Application Programming Interface

CIT Craft Interface Terminal

CMISE Common Management Information Service Element

DCN Data Communications Network

DSA (ITU-T X.500) Directory System Agent

DUA (ITU-T X.500) Directory User Agent

ES (OSI) End System

FTAM File Transfer & Access Method

GUI Graphical User Interface

IS (OSI) Intermediate System

LAN Local Area Network

LCN Local Communications Network

NARSE Name Address Resolution Service Element

NSAP Network Service Access Point

PSAP Presentation Service Access Point

NE Network Element

RA (ANSI T1.245) Registration Agent

ROSE Remote Operations Service Element

RRP (ANSI T1.245) Registration Request Protocol

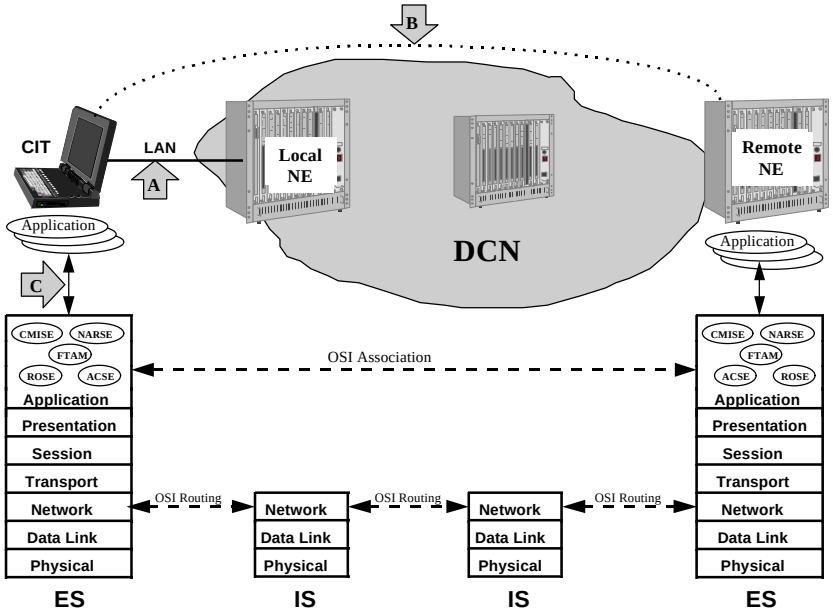
TARP TID Address Resolution Protocol

TL1 Transaction Language 1

WAN Wide Area Network

2. Architecture Overview

The architecture for SIF NE-NE Remote Login is shown below.



NE-NE Remote Login Architecture

It has the following characteristics:

- Like the WS-DCN interface specified in the SIF recommendation for NE-to-NMS remote login [1], the interface between the CIT and the DCN (reference point A above) is 10BASE-T LAN and uses OSI Network Layer Protocols.
- The CIT may be connected to the DCN via an existing LAN or directly to a local NE. The CIT dynamically discovers its own NSAP.
- The CIT performs name/address resolution and establishes an application association to the remote NE, over which management information is exchanged. The interface between the CIT and the remote NE is denoted as reference point B in this architecture.
- The CIT and remote NE act as OSI End Systems (ESs). The local NE and other systems within the DCN involved in routing messages between the CIT and the remote NE play OSI Intermediate System (IS) roles.
- While NE software is normally provided solely by the NE vendor, CIT software is expected to consist of both platform components and vendor-specific components from one or more NE

vendors. A given CIT implementation will include the appropriate set of Application Service Elements (ASEs), as part of the platform, needed to support its vendor-specific applications. The interface between vendor-specific applications and platform components is shown as reference point C.

3. Craftsperson to CIT Interface

The interface between the craftsperson and the CIT may be graphical or non-graphical and is expected to be provided on a vendor-specific basis. The format is outside the scope of this recommendation.

The CIT must, however, be capable of supporting multiple simultaneous login sessions.

4. CIT to DCN Interface

This section defines the physical, link and network layer interfaces for reference point A, at which the CIT attaches to the DCN. As previously mentioned the CIT may be connected via an existing LAN or, alternatively, directly to a local NE via its LAN interface. As such this section places requirements on both the CIT and the local NE.

4.1 Physical Layer

The physical interface for connecting a CIT to an existing LAN or a local NE for the purposes of remote login shall be as follows (applies to both CIT and NE sides of the interface):

·The interface shall follow the requirements for a 10BASE-T Medium Attachment Unit (MAU) connection as specified in ISO/IEC 8802-3:1993 (E) ANSI/IEEE Std 802.3 1993 Edition.

·The medium utilized is twisted-pair wire (26 AWG to 22 AWG) unshielded in a multipair cable.

·A RJ-45 jack shall be provided for physical connection.

Pin	Signal
1	TD+
2	TD-

3 RD+

6 RD-

·This interface shall support message traffic at a preferred data rate of 10 Mb/s.

·The MAU will provide for operating from 0 meters to 100 meters (328 feet) of twisted pair without the use of a repeater.

If the CIT is to be connected via an existing 10BASE-T LAN, the network provider will need to insure that the signal connections are compatible with the local LAN wiring plan.

If the CIT and the local NE are to be connected in a point-to-point configuration, then the transmit data pins of one device must be wired to the receive data pins of the other device, and vice versa. The signal crossover may be provided by a special crossover cable, with the transmit pins on the RJ-45 plug at one end of the cable wired to the receive data pins on the RJ-45 plug at the other end of the crossover cable and vice versa.

Pin	Signal	routed to Pin	Signal
1	TD+	3	RD+
2	TD-	6	RD-
3	RD+	1	TD+
6	RD-	2	TD-

4.2 Data Link Layer

The Data Link Layer interface shall be Logical Link Control (LLC1) over Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as specified in Section 8.3.2.2 of Bellcore GR-253-CORE, Issue 2.

4.3 Network Layer

The Network Layer interface shall be Connectionless Network Layer Protocol (CLNP) including End System to Intermediate System (ES-IS) as specified in Section 8.3.3.2 of Bellcore GR-253-CORE, Issue 2. The CIT shall support the End System role, and the local NE shall support the Intermediate System role.

Dynamic discovery by the CIT of its own NSAP is discussed in section 6.

5. CIT to Remote NE Interface

In the SIF NE-NE remote login architecture, exchange of management information occurs over an application association between the CIT and the remote NE through the intervening DCN. The interface between the CIT and the remote NE is reference point B in this architecture.

This section specifies requirements on both the CIT and the remote NE to support TL1 and/or CMISE associations between the CIT and the remote NE. TL1 or CMIP can be used for transaction-oriented exchange of management information. Other proprietary application protocols might be used as well without violating the conformance requirements specified herein.

This section also specifies requirements on both the CIT and the remote NE to support FTAM associations between the CIT and the remote NE. FTAM is used for file-oriented exchange and can supplement the use of a transaction-oriented protocol to provide software management capabilities.

Name/address resolution mechanisms used to support association establishment are discussed in section 7.

5.1 Transport Layer

The profile for the Transport and underlying services shall be that specified in Appendix C of Bellcore GR-253-CORE, Issue 2.

5.2 Session Layer

The profile for the Session Layer shall be that specified in Section D.8 of Bellcore GR-253-CORE, Issue 2.

5.3 Presentation Layer

The profile for the Presentation Layer shall be that specified in Section D.7 of Bellcore GR-253-CORE, Issue 2.

The presentation selectors (P-SEL) for CMISE, FTAM and TL1 PDUs shall be initialized and configurable as specified in Section 8.3.6 of Bellcore GR-253-CORE, Issue 2.

It should be noted that if multiple application entities provide responder services (e.g. FTAM), it is possible for more than one application to register against the same P-SEL. This would cause any incoming ACSE requests to fail. Thus, this problem gives rise to the requirement for the P-SEL to be configurable on a per application entity responder basis. This requirement goes beyond the basic configuration requirement stated in Section 8.3.6 of Bellcore GR-253-CORE, Issue 2.

5.4 Application Layer

This section specifies requirements on ACSE, CMISE/ROSE, and FTAM for conforming CIT and remote NE implementations.

5.4.1 ACSE Requirements

The profile for ACSE shall be that specified in Section D.6 of Bellcore GR-253-CORE, Issue 2, including requirements specific to the CMISE and FTAM Application Service Elements (ASEs).

The CIT must be capable of acting in the role of association-initiator for transaction-oriented message exchange, and the association-responder role for the file-oriented exchange. Conversely, a remote NE is required to support the association-responder role for purposes of transaction-oriented exchange; and the association-initiator role for file-oriented exchange, if supported.

5.4.2 CMISE/ROSE Requirements

If provided, the CIT and the remote NE shall support CMISE/ROSE in accordance with the SIF SONET CMISE Profile [5]. The CIT shall support the roles of invoker and responder for CMISE operations and notifications, respectively. The remote NE shall support the roles of responder and invoker for CMISE operations and notifications, respectively.

5.4.3 FTAM Requirements

If provided, the CIT shall support the role of responder and the remote NE shall support the role of initiator in accordance with the SIF SONET Operations Communications FTAM Profile [6].

6. Dynamic NSAP Assignment for CIT

It is expected that the CIT will frequently be attached and re-attached to the DCN at different points in the network. Hence it

will need to have an NSAP assigned to it on a temporary basis. This section specifies a procedure for dynamic NSAP assignment for the CIT that is similar to the procedure specified in the previous SIF recommendation for NE-to-NMS remote login [1].

6.1 CIT Requirements

Each time a CIT is rebooted or explicitly initiated (a local matter), the CIT shall determine its NSAP value(s) via the following procedure:

> After the CIT is connected to the NE LAN port (or the LCN) and layer 3 is initialized, the CIT inserts its MAC address into the System Identifier field. Next, the CIT waits to receive an "Intermediate System Hello Protocol Data Unit" (ISH PDU). After receiving the first ISH PDU, the CIT copies the Area Address from this ISH PDU for use in "End System Hello Protocol Data Units" (ESH PDU's). The CIT then generates its NSAP or NSAPs using N-selectors specified in GR-253-CORE [4], Section 8.3.3. All CITs will generate an NSAP for OSI transport layer; CITs that support TARP will also generate an NSAP for TARP. The CIT will then transmit the NSAP or NSAPs on each ESH PDU it transmits according to ISO 9542 [7]; to announce its addition to the network.

7. Name/Address Resolution

Name/address resolution must be performed at the CIT before it establishes an application association to the remote NE. TARP or ANSI T1.245 directory services may be used for this purpose. It is expected that TL1 NEs will support TARP and that CMISE NEs will support T1.245 directory services. This section specifies requirements on the CIT, NEs and the network in support of these mechanisms.

Manual provisioning of name/address pairs at the CIT can also be used in lieu of TARP or T1.245.

7.1 TARP

TARP can be used to translate a Target Identifier (TID) to a corresponding Network Service Access Point (NSAP). This can be useful, for example, when establishing a TL1 association from the CIT to the remote NE.

If TARP is used then the following requirements apply:

7.1.1 CIT Requirements

Using the TID of the remote NE, the CIT needs to originate (Type 1/2) TARP PDUs. It must also process the Type 3 TARP PDU returned to it by the remote NE. The Type 3 PDU contains the NSAP of the remote NE. As such it must satisfy all requirements pertaining to origination and processing of TARP requests, including management of the TARP processor, as specified in Bellcore GR-253-CORE [4].

7.1.2 Remote NE Requirements

The remote NE can satisfy the name/address resolution request made by the CIT directly. As such it should provide full TARP support as specified in Bellcore GR-253-CORE [4].

Alternatively, a T5GW NE can satisfy the name/address resolution request made by the CIT on behalf of the remote NE as described in the SIF TARP/X.500 Interworking Specification [8].

7.1.3 Networking Requirements

To satisfy a TARP request there needs to be some path from either the CIT to the remote NE, or from the CIT to a T5GW NE. The local NE and other intermediate NEs along this path should satisfy requirements for receipt, loop detection and propagation of TARP PDUs as per Bellcore GR-253-CORE [4]. If some non-SONET intermediate NE (e.g., a router) along this path does not provide TARP capabilities, then manual TARP adjacencies should be set up as described in [4].

7.2 ANSI T1.245

ANSI T1.245 Directory Services [9] can be used to translate an Application Entity title (AEtitle) to a corresponding Presentation Service Access Point (PSAP). This can be useful, for example, when establishing a CMISE association from the CIT to the remote NE.

If T1.245 Directory Services is used then the following requirements apply:

7.2.1 CIT Requirements

To perform name/address resolution the CIT must conform to the T1.245 DUA role as specified in [9].

Addressing information for primary and shadowing Directory System Agents (DSAs) must be auto-learned by a T1.245 Registration Agent

(RA) residing on the CIT using the Registration Request Protocol (RRP), as specified in [9].

7.2.2 Remote NE Requirements

Directory objects (tmnNE, applicationProcess, applicationEntity) for the remote NE must obviously exist in order for the CIT to perform name/address resolution using T1.245 Directory Services. This information may be placed in a T1.245 Directory in several ways:

1) Auto-populated by the remote NE itself.

2) Auto-populated by a T5GW NE on its behalf.

3) Manually, by a directory administrator.

In case 1) above the remote NE must conform to auto-population requirements, including RRP support, as specified in [9].

In the other cases there are no requirements, per se, on the remote NE. In case 2) the T5GW NE must conform to requirements as specified in [8].

7.2.3 Networking Requirements

By definition, if name/address resolution is satisfied via T1.245 Directory Services, then the presence and availability of a T1.245 DSA is required somewhere in the network.

8. Security

For a remote login session it is recommended that strong user authentication be provided as specified in Bellcore GR-1469-CORE [10]. The choice of the particular security mechanism to be used is at the discretion of an individual NE vendor and should be supported by NE and CIT software provided by that vendor.

In addition to the above, security of the CIT itself needs to be addressed. At a minimum, the remote login application on the CIT should be password protected.

9. CIT Configuration

This section covers hardware configuration, and required and optional platform components for the CIT.

9.1 Hardware Configuration

The SIF recognizes the need for a specification for a common hardware platform which significantly increases the usefulness and application of a NE-to-NE Remote Login solution for the SONET telecommunications industry. Specifying a hardware platform allows network providers to purchase no more than one single CIT per craftsperson, and allows vendors of CIT software to concentrate their efforts on enhancing their software rather than porting and maintaining the software for different hardware platforms.

To this end, the hardware platform for the CIT shall be an IBM-PC compatible computer, and (as a minimum) capable of running the Microsoft Windows NT operating system.

9.2 Platform Components

The following components are considered part of the platform. They provide services that NE vendor specific applications on the CIT use. Detailed service specifications for these components will be provided in another document, the SIF OS/CIT software platform architecture [11]. Additional CIT platform components may also be identified and specified in that document.

- Windows NT operating system - The SIF has recognized the need to specify an operating system to facilitate the ability of OSI stack vendors and application software vendors to supply components that can be integrated on a single CIT. Specifying a single operating system environment also allows CIT software vendors (OSI stack and applications vendors) to eliminate the need to develop different versions of a software product for various operating systems. This economy in software development can be passed on to the network providers and will benefit the SONET telecommunications industry in general. SIF believes specifying an operating system to be paramount in this specification, enabling the solution to be widely accepted and deployed in the industry, as well as creating a more open market for CIT software.
- OSI stack including ACSE
- Name Address Resolution Service Element (NARSE) - This service element is used to satisfy application requests for name/address resolution using TARP,

T1.245 Directory Services, or information configured locally on the CIT.

- CMISE ASE (optional)
- FTAM ASE (optional)

9.3 Application Programming Interfaces

To facilitate development and deployment of NE vendor-specific applications for the CIT, the SIF has determined the need to specify APIs for CIT-resident platform components. These specifications are included in the SIF OS/CIT software platform architecture [11]. The SIF recommends that these APIs be provided in such a way to allow dynamic linking of application modules.

10. References

1) ”NE-NE Remote Login Initial Solution Evaluation Criteria”, SIF–9605-043-R4, SONET Interoperability Forum, June 12, 1996.

2) ”Results of Service Providers’ Responses to NE-NE Remote Login Survey”, SIF–RL-9609-076, SONET Interoperability Forum, September 23, 1996.

3) ”Remote Login Implementation Requirements Specification”, SIF–116-0895-R3, SONET Interoperability Forum, April 26, 1995.

4) Bellcore GR-253-CORE, "SONET Transport Systems: Common Generic Criteria”, Issue 2, December 1995.

5) “Third Draft of a SONET CMISE Profile”, SIF-TA-9601-006-R2, SONET Interoperability Forum, June 10, 1996.

6) “SONET Operations Communications FTAM Profile”, SIF-95/002, SONET Interoperability Forum, April 11, 1995.

7) ISO/IEC 8473, “Information technology - End system to intermediate system routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service”, 1994.

8) “TARP/500: The TARP and X.500 Directory Services Interworking Specification”, SIF-TA-9604-034, SONET Interoperability Forum, April 17, 1996.

9)“Directory Service for Telecommunications Management Network (TMN) and Synchronous Optical Network (SONET)”, ANSI T1.245, 1995.

10) Bellcore GR-1469-CORE, "Generic Requirements on Security for OSI-Based Telecommunications Management Network Interfaces”, Issue 1, December 1994.

11) “SIF OS/CIT Software Platform Architecture Specification”, SONET Interoperability Forum, To be published.