Last Modified Date 10/2/01 9:16:09 AM

ISIS-700

ATM Signaling External Functional Specification

1000-SPC-0137-01.D08

Primary Author(s): Nilan Naidoo, Vladimir Rakocevic

Key Contributors: Shuchi Chawla,

Normative References:

[1] G.Shenoda et al, ISIS-700 Product Requirements Version R1.0, Oresis internal document

[2] The ATM Forum, Private Network-Network Interface Specification Version 1.0 (PNNI 1.0), af-pnni-0055.000, March 1996

[3] The ATM Forum, PNNI V1.0 Errata and PICS, af-pnni-0081.000, May 1997

[4] The ATM Forum, ATM User-Network Interface (UNI) Signalling Specification Version 4.0, af-sig-0061.000, July 1996

[5] The ATM Forum, Addendum to PNNI Version 1.0 for ABR parameter negotiation, af-pnni-0075.000, January 1997

[6] The ATM Forum, PNNI Addendum for Generic Application Transport Version 1.0, af-cs-0126.000

[7] The ATM Forum, PNNI SPVC Addendum Version 1.0, af-cs-0127.000

[8] The ATM Forum, User-Network Interface Signaling Specification, Version 3.1, 1994

[9] ITU-T, B-ISDN AAL Service Specific Connection Oriented Protocol (SSCOP), Q.2110, July 1994

[10] ITU-T, B-ISDN SAAL Service Specific Coordination Function (SSCF) at the UNI, Q.2130, July 1994

[11] ITU-T, B-ISDN DSS 2 UNI Layer 3 Specification for Basic Call/Connection Control , Q.2931, February 1995

[12] D. Thomas, ISIS-700 Connections External Functional Specification, Oresis Internal Document, 1000-SPC-0055-XX

[13] D. Thomas, ISIS-700 Usage Measurement and Statistics Functional Specification, Oresis Internal Document, 1000-SPC-0009-XX

[14] N. Naidoo, ISIS-700 Soft Permanent Connections External Functional Specification, Oresis Internal Document, 1000-EFS-0194-XXS-0194-01.

[15] THE ATM FORUM, NETWORK CALL CORRELATION IDENTIFIER V1.0, AF-CS-0140.000, MARCH 2000.

[16] A. ALLEMAN, ISIS-700 SCM REDUNDANCY EXTERNAL FUNCTIONAL SPECIFICATION, ORESIS INTERNAL DOCUMENT, 1000-EFS-0125-XX

[17] THE ATM FORUM, PNNI ADDENDUM FOR PATH AND CONNECTION TRACE BTD-CS-PNNI-TRAC -01.01

Informative References:

[18] A. ALLEMAN, ISIS-700 TOP LEVEL ARCHITECTURE OVERVIEW, ORESIS INTERNAL DOCUMENT, 1000-ARC-0088-XX

[19] S. CHAWLA AND P. IYER, ISIS-700 CHASSIS INTERFACE CONFIGURATION MANAGEMENT FUNCTIONAL SPECIFICATION, ORESIS INTERNAL DOCUMENT 1000-SPC-0016-XX

[20] J. JIANG, ISIS-700 PNNI ROUTING AND SIGNALING FUNCTIONAL SPECIFICATION, ORESIS INTERNAL DOCUMENT, 1000-SPC-0081-11

[21] P. SHARMA, ISIS-700 ADDRESSING MODEL FUNCTIONAL SPECIFICATION, ORESIS INTERNAL DOCUMENT, 1000-SPC-0097-02

[22] THE ATM FORUM, PRIVATE NETWORK-NETWORK INTERFACE SPECIFICATION VERSION 1.0 ADDENDUM (SOFT PVC MIB), AF-PNNI-0066.000

[23] *BELLCORE, GENERIC REQUIREMENTS FOR OPERATIONS OF ATM NES, GR-1248-CORE, 1998*

Documents for which this document is a Normative Reference:

[24] *V. RAKOCEVIC, ISIS-700 EXTERNAL INTERFACE FUNCTIONAL SPECIFICATION – PROGRAMMATIC ATM SIGNALING, ORESIS INTERNAL DOCUMENT, 1000-EISP-0198-XX*

Documents which are obsolete by this document:

Notification List:

System Architecture Team
Connections Team
Stats team
Embedded and GUI NM teams
Product Verification

Reviewers:

Official Review Team:

- Mike Ott (PM)
- Andrew Alleman (SAT)
- Kenith Mann (PV)
- Bharath Belagodu (NM)
- Nilan Naidoo (Content Expert)

- Vladimir Rakocevic (Content Expert)

Other recommended reviewers / notification list members:
Shuchi Chawla, Padmini Iyer, Parag Sharma, Visweswar Javangula,

Approvals:

Version -01

Role	Signature	Date
SAT representative	Andrew Alleman	20-Sep-01
PV representative	Kenith Mann	20-Sep-01
PM representative	Mike Ott	28-Sep-01
NM representative	Bharath Belagodu	01-Oct-01

REVISION HISTORY

Date	Revision	Author	Description
05-Oct-00	A00	Nnaidoo	**Initial version**
12-Dec-00	B01	Nnaidoo	**Updates after internal review**
30-Jan-01	B02	Nnaidoo	**Updates after external review**
25-May-01	B03	Nnaidoo	**Added more requirements to most sections. Major rework of the document for R1.5**
20-Aug-01	B04	nnaidoo	**Updates after walkthrough and moved to B level document.**
31-Aug-01	B05	vrakocevic	**Some minor updates. Added requirements for Switched Virtual Connections.**
13-Sep-01	B06	vrakocevic	**Updates after first formal review.**
21-Sep-01	D07	vrakocevic	**Updates after the second formal review**
02-Oct-01	D08	vrakocevic	**Updates after B. Belagodu's comments.**

TABLE OF CONTENTS

FIGURES

TABLES

1. INTRODUCTION

1.1. PURPOSE

This document describes the external functional specification for ATM Signaling. ATM Signaling is used to setup and tear down Switched Virtual Connections (SVCs). The external functional specification includes requirements for supporting SVC capabilities at the user-network interface (UNI) and private network-network interface (PNNI). SVCs provide for the dynamic establishment and release of calls/connections across the ATM network. The requirements cover the switch functions, messages, procedures, and parameters which are necessary to support SVC capabilities at the UNI and NNI of the ISIS-700. Thus, not only are signaling aspects covered, but also other switch requirements needed in conjunction with signaling are detailed.

This document is intended to be the sole authority on the contents of the external functional specification for Switched Virtual Connections. All behaviors as specified in this document should appear in the implementation of ATM Signaling. This is a controlled NPI document, and must follow the procedures set forth in the *Engineering NPI Document Lifecycle* specification.

1.2. SCOPE

This external functional specification, along with the architecture specification(s) and external interface specification(s), are the authorities for the specification of the external functional interface of the ATM Signaling feature. The external functional specification is the “most senior” of the three, but it does not specify interface details or architecture. This document shall serve as both requirements for design and implementation of the functionality described and for subsequent formal verification of the feature.

The target product release for the functionality specified in this document is Release 1.5

1.3. ASSUMPTIONS

Although not specifically required, it is assumed that the reader is familiar with ISIS700, its hardware and software architecture and their components. The reader is also assumed to be familiar with the ATM Signaling.

The existence of approved normative documents is assumed.

1.4. DOCUMENT FORMAT

Requirements can be classified into three categories: those that are required for the current release, those that are not required for any release, and those that may be required in future releases. The sets of features are distinguished based on the requirement designation:

R1-1[0]: Features required for release 1.5 shall be stated using this requirement specification.

N1-2[0]: Features not required for any release shall be stated using this requirement specification.

F1-3[0]: Requirements for future consideration shall be stated using this requirement specification.

2. FUNCTIONALITY OVERVIEW

2.1. OPERATIONAL DESCRIPTION

ATM signaling allows Switched Virtual Connections (SVC) to be setup on demand by users equipment connecting through the ISIS-700. These connections can be used to carry voice, video or data traffic. The signaling messages used to setup and tear down these SVCs are exchanged over a separate permanent virtual connection between the user equipment and the ISIS700, called the signaling virtual channel. The SVCs that a user is allowed to make via a signaling channel are restricted to the set of endpoints on the service interface(s) associated with the signaling channel at provisioning time.

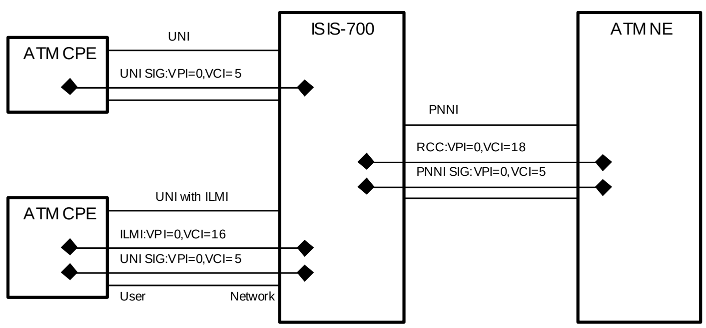

Figure 2-1 ~~2-1~~ ATM Signaling Model

Figure 2-1 shows the general model for signaling between customer premise equipment (CPE) and the ISIS-700, and between the ISIS-700 and other network elements. Three types of signaling interfaces are supported: UNI, UNI with ILMI and PNNI.

In the case of the UNI signaling interface, the ATM CPE is physically connected to the ISIS-700 through an ATM interface, e.g. OC3c, DS1. A signaling channel PVC (e.g. VPI=0, VCI=5) is setup between the ATM CPE and the ISIS700 to carry the signaling messages exchanged between the ATM CPE and the ISIS-700. The signaling protocols supported on this interface are ATM Forum UNI3.1 and UNI4.0.

The UNI with ILMI signaling interface is the same as the UNI signaling interface, except that it has an ILMI channel configured on a particular VP/VCI (e.g. VPI=0,VCI=16). The ILMI channel is used by the CPE to register user addresses and exchange status.

The PNNI signaling interface is used between the ISIS-700 and another ISIS-700 or other vendors network elements. A signaling channel is setup on VPI=0,VCI=5 to exchange signaling messages. The signaling protocol supported is PNNI. A route control channel is setup on VPI=0, VCI=18 to exchange PNNI Topology State Elements (PTSE) which are used to compute routes through the network.

2.1.1. Typical Application

This section describes some typical ATM signaling applications.

2.1.1.1. IAD to IAD Voice Call through the ISIS-700

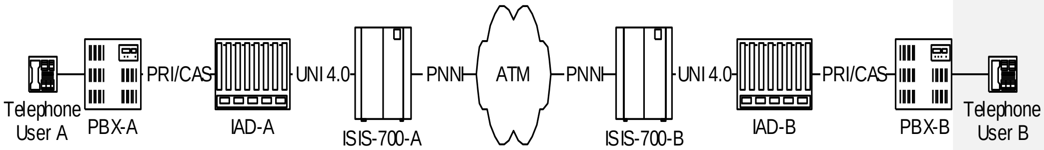

Figure 2-2 ~~2-2~~Network Architecture for IAD to IAD Voice Call

Figure 2-2 shows an application where a voice call is made through an IAD attached to the ISIS-700. The example demonstrates the use of both PNNI and UNI signaling. PNNI signaling is used between the ISIS-700 and the network, and UNI signaling is used between the user devices and the ISIS-700.

User A wants to call User B. User A's telephone is attached to a PBX which is connected to an Integrated Access Device (IAD). The IAD is connected to the ISIS-700 via an ATM UNI. A signaling channel is provisioned between the IAD and the ISIS-700 on the ATM UNI. Similarly User B is attached to another ISIS-700 through its own IAD.

UserA will pick up his telephone and dial the number of UserB. PBX-A will initiate PRI signaling. IAD-A will initiate two SVC calls to tunnel the N-ISDN signaling and to carry the voice data.

IAD A receives a N-ISDN SETUP message from a PRI interface that is connected to PBX-A, and there is no previous signaling channel that has been established. The IAD will map the called party number in the N-ISDN SETUP message to the ATM address of IAD-B and initiate an SVC. IAD-A initiates the SVC call by sending a UNI 4.0 SETUP message across the signaling channel to ISIS-700-A. When ISIS-700-A receives the SETUP it uses PNNI routing to determine if the call can be supported to the destination address and to compute a route to the destination IAD. The ISIS-700 will select a VPCI/VCI for the call and send it in the CALL PROCEEDING message to IAD-A. ISIS-700-A will then forward the PNNI SETUP message into the ATM network towards ISIS-700-B. When ISIS-700-B receives the SETUP message and determines that it is destined for IAD, it converts the SETUP message to UNI 4.0 SETUP message and sends it across the signaling channel connected to IAD-B. IAD-B responds with a CONNECT message when it receives the SETUP message. ISIS-700-B forwards the CONNECT message towards ISIS-700-A and cuts-through the connection for the N-ISDN signaling channel. When ISIS-700-A receives the CONNECT message it forwards the message to IAD-A and cuts-through the connection for the N-ISDN signaling channel. At this point the SVC used to tunnel N-ISDN messages is established between IAD-A and IAD-B.

A similar procedure is used to setup the VCC for bearer channels between IAD-A and IAD-B. Once this VCC is setup, the N-ISDN SETUP is sent to PBX-B across the N-ISDN signaling channel. PBX-B responds with a N-ISDN CONNECT, and the two phones are connected.

The message sequence to setup these connections is shown in Figure 2-3.

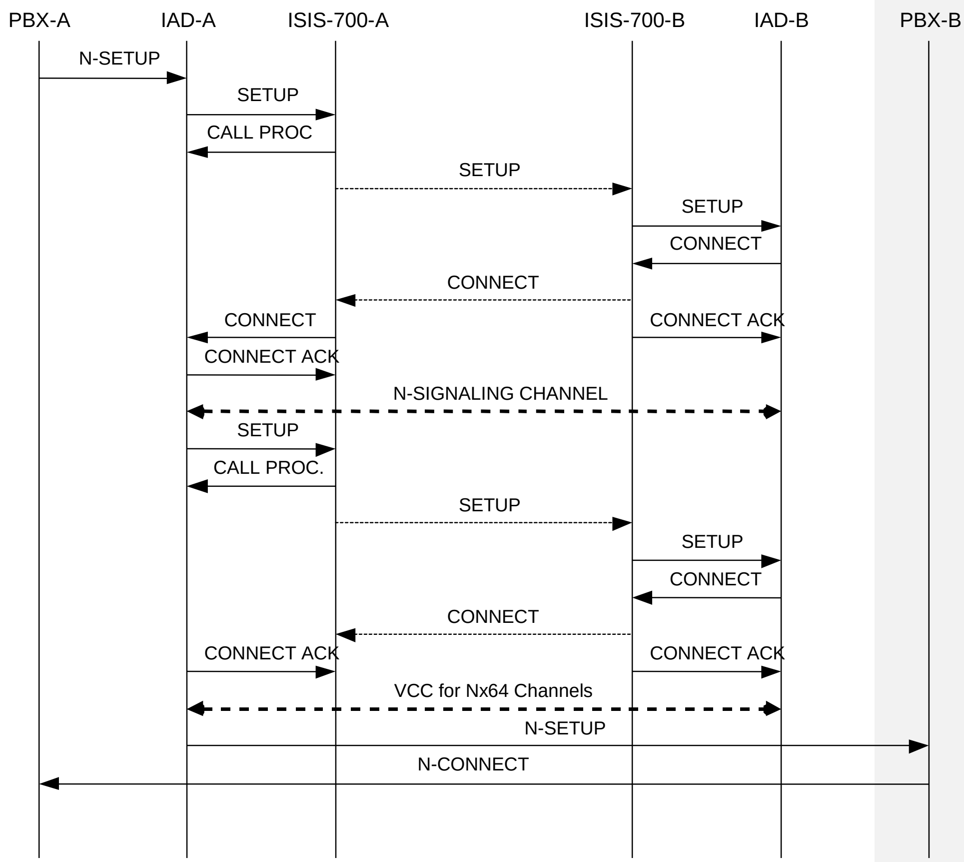

Figure 2-3 ~~2-3~~ Message Sequence for IAD to IAD Voice Call

3. FEATURE REQUIREMENTS

This section provides sufficient details about the ATM Signaling features to help readers understand the ISIS-700 ATM Signaling functionality in order to produce design, test, and customer documentation. The ATM forum document name and revision is stated for features or functionality that will be supported. The requirements also include an exception list for specific items covered by the ATM forum specifications that are not supported.

In the context of this document the term UNI Signaling shall mean UNI 3.1 Network Side or UNI 4.0 Network Side, unless otherwise noted. The term NNI signaling shall mean PNNI signaling unless otherwise noted.

3.1. PHYSICAL, ATM AND ADAPTATION LAYERS

3.1.1. Physical Layer

The ISIS-700 supports many physical interfaces and modules, but not all of them are able to provide SVC services. The signaling channels may reside on the same physical interface as the connections they control, or they may reside on another interface in the case of proxy signaling.

R3-1[1]: The ISIS-700 *shall* support facility associated NNI signaling on the 4 x OC3 Physical Module (PM).

R3-2[2]: The ISIS-700 *shall* support facility associated NNI signaling on the 12 x DS3 PM.

R3-3[3]: The ISIS-700 *shall* support facility associated NNI signaling on the 12 x E3 PM.

R3-4[4]: The ISIS-700 *shall* support facility associated NNI signaling on the 1 x OC12 PM.

F3-5[5]: The ISIS-700 *shall* support facility associated UNI signaling on the 4 x OC3 PM.

F3-6[6]: The ISIS-700 *shall* support facility associated UNI signaling on the 12 x DS3 PM.

F3-7[7]: The ISIS-700 *shall* support facility associated UNI signaling on the 12 x E3 PM.

F3-8[8]: The ISIS-700 *shall* support facility associated UNI signaling on the 1 x OC12 PM.

F3-9[9]: The ISIS-700 shall support facility associated UNI on any DS1 interface provided to a USM100.

F3-10[10]: The ISIS-700 shall support facility associated UNI on any E1 interface provided to a USM100.

Table 3-1 shows a summary of the physical interface and the SVC services that are supported on the interfaces.

Physical Interface	UNI	NNI
OC3	F	R
DS3	F	R
E3	F	R
DS1	F	N
E1	F	N
OC12	F	R

Table 3-1 Summary of Physical Interfaces for SVC Services

3.1.2. ATM Layer

This section describes ATM layer generic requirements specific to SVC signaling.

R3-11[11]: The ISIS-700 *shall* use VPI=0, VCI=5 as the default for the point-to-point signaling channel.

R3-12[12]: The ISIS-700 *shall* support management requests to change the VPI and VCI of the point-to-point signaling channel.

Traffic controls are applied to the signaling virtual channel. The traffic characteristics of the signaling channel are configurable, with defaults being applied in the absence of configuration. The specification of standard defaults means that degradation of signaling performance due to cell loss can be avoided without requiring configuration. The signaling virtual channel traffic requirements and recommendations is described in section 4.2 of ATM Forum UNI 4.0 specification.

R3-13[13]: The default ATM layer service category for the signaling VCC shall be rt-VBR.

R3-14[14]: The ISIS-700 *shall* support management requests to change the default ATM Layer service category of the signaling VCC.

The output of the signaling VCC should be shaped to conform to the traffic contract. If shaping is not performed then during periods of congestion, or when connected to networks that do not perform tagging for the VBR.3 traffic contract definition, degraded signaling performance will be experienced due to cell loss. Degradation might take the form of excessive delay in establishment or clearing of connections, or a signaling VCC outage.

R3-15[15]: Signaling and routing protocol VCCs for ATM Signaling Applications shall be traffic shaped and policed as possible on the service module on which they reside.

R3-16[16]: The default traffic contract for the signaling virtual channel is as follows:

- PCR = the payload rate of the interface. The payload rate is the ATM cell rate of the interface, excluding any physical layer overhead. The values for each interface are shown in Table 3-2.
- SCR shall be as shown in Table 3-2.
- MBS = 16 cells.

R3-17[17]: The ISIS-700 *shall* support management requests to change the default traffic contract of the signaling VCC.

Physical Interface	PCR (cells/s)	SCR (cells/s)
DS1	3500	42
E1	4700	42
E3	72000	500
DS3	96000	500
OC3	365000	2000
OC12	1466000	8000

Table 3-2 Default PCR and SCR for Signaling VCC

3.1.3. Signaling ATM Adaptation Layer (SAAL)

The SAAL protocol defines the transfer of signaling information for call/connection control on the signaling virtual channel. It supports assured, message mode transfer through the SAAL service access point. The SAAL includes AAL5 Common Part (CP), Service Specific, Connection Oriented Protocol (SSCOP), and Service Specific Coordination Function (SSCF). There are two types of SSCF: SSCF-UNI and SSCF-NNI 2 . The ATM Forum's UNI and PNNI specification requires the use of SSCOP as defined in Q.2110 [9] , and SSCF-UNI as defined in Q.2130 [8].

In order to understand the SSCOP protocol, Q.2110 should be consulted. However, at a high level, SSCOP has PDUs that are used for various tasks. SD PDUs are used to transport data for the user of the SSCOP connection. Periodically, one connection endpoint will check on the status of the other end by issuing a POLL PDU, and wait for a STAT PDU in reply. In addition, there are PDUs (e.g., BGN, END) that are used in the establishment and release of the SSCOP connection, PDUs (e.g., RS) that are used to resynchronize the connection, and PDUs (e.g.,ER) used for error recovery.

SSCOP configurable parameters are captured in ATM Signaling EIS-P document [24].

R3-18[18]: Upon management request, the ISIS-700 shall configure the SSCOP parameters and timers for signaling channel. Refer to ATM Signaling EIS-P [24] for the parameters values.

The default SSCOP parameters and timers for UNI and NNI signaling channels are specified in ATM Signaling EIS-P [24].

3.2. SWITCHED VIRTUAL CONNECTIONS (SVC) GENERAL REQUIREMENTS

This section specifies requirements which describe Switched Virtual Connections and their handling on the ISIS-700.

R3-19[19]: The ISIS-700 shall reject an SVC call setup request if the egress SVC endpoint is on an interface not in the active state.

R3-20[20]: The ISIS-700 shall release all Switched Virtual Connections on a interface when the interface state changes to Unavailable.

R3-21[21]: The ISIS-700 shall release all Switched Virtual Connections on a slot when slot is being shutdown.

R3-22[22]: The ISIS-700 shall release all Switched Virtual Connections on a slot when slot is being set to factory defaults (purged).

R3-23[23]: The ISIS-700 shall maintain the following status for each Switched Virtual Connection and shall support requests to retrieve this information.

- The Operational State of a Switched Virtual Connection is always Active.
- The NCCI value assigned to an SVC. If the NCCI is not available then a “Null” value is returned.

R3-24[24]: The ISIS-700 shall support management request to release a specific Switched Virtual Connection.

R3-25[25]: The ISIS-700 shall support management request to retrieve all Switched Virtual Connections per interface.

R3-26[26]: The ISIS-700 shall support all monitoring statistics for Signaled Virtual Connections which are supported for Permanent Virtual Connections as described in ISIS-700 Connections EFS [12] and in ISIS-700 Usage Measurement and Statistics EFS [13].

~~3.2.~~3.3. CALL PROCESSING

Formatted: Bullets and Numbering

This section describes the requirements to establish, maintain, and clear point-to-point, switched virtual channel connections.

3.3.1. UNI 3.1

F3-27[27]: The ISIS-700 *shall* support the network-side call/connection procedures for point-to-point calls as described in Section 5.5 of the ATM Forum User Network Interface Specification, Version 3.1 [8], with the following modifications:

— The sending of a CALL PROCEEDING message is mandatory at the originating interface of a call/connection.

F3-28[28]: The ISIS-700 *shall* support the user-side call/connection procedures for point-to-point calls as described in Section 5.5 of the ATM Forum User Network Interface Specification, Version 3.1 [8].

3.3.2. UNI 4.0

F3-29[29]: The ISIS-700 *shall* support the network-side call/connection procedures for point-to-point calls as described in Section 2.0 of the ATM Forum UNI 4.0 Signaling specification [4], with the following modifications:

— Virtual UNIs are not supported (F)

— ABR Signaling for point-to-point calls is not supported (N)

— Frame discard is not supported (F)

F3-30[30]: The ISIS-700 *shall* support the Signaling of Individual QOS Parameters procedure as described in Section 9.0 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-31[31]: The ISIS-700 *shall* support the user-side of the UNI 4.0 signaling capabilities specified in Section 5 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-32[32]: The ISIS-700 *shall* support UNI 4.0 Point-to-multipoint calls specified in Section 5 of the ATM Forum UNI 4.0 Signaling specification [4].

N3-33[33]: The ISIS-700 *shall* not support UNI 4.0 procedures for Leaf initiated join calls specified in Section 6 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-34[34]: The ISIS-700 *shall* support UNI 4.0 ATM anycast capability specified in Section 7 of the ATM Forum UNI 4.0 specification Signaling specification [4].

F3-35[**35**]:The ISIS-700 *shall* not support UNI 4.0 ABR Signaling for Point-to-point calls specified in Section 10 of the ATM Forum UNI 4.0 specification [4].

F3-36[**36**]:The ISIS-700 *shall* support UNI 4.0 Generic Identifier Transport Information Element described in Section 2.1.1 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-37[**37**]:The ISIS-700 *shall* support use of Virtual UNIs as specified in Annex 8 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-38[38]: The ISIS-700 *shall* support Switched Virtual Path (VP) Services as specified in Section 2 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-39[39]: The ISIS-700 *shall* support Proxy Signaling as specified in Annex 2 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-40[40]: The ISIS-700 *shall* support Frame Discard procedures as specified in Section 2 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-41[41]: The ISIS-700 *shall* support Traffic Parameter Negotiation capability as specified in Section 8 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-42[42]: The ISIS-700 *shall* support Direct Dialing In (DDI) service as specified in Section Annex 4 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-43[43]: The ISIS-700 *shall* support Multiple Subscriber Number (MSN) service as specified in Annex 4 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-44[44]: The ISIS-700 *shall* support Calling Line Identification Presentation (CLIP) service as specified in Annex 4 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-45[45]: The ISIS-700 *shall* support Calling Line Identification Restriction (CLIR) service as specified in Annex 4 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-46[46]: The ISIS-700 *shall* support Connected Line Identification Presentation (COLP) service as specified in Annex 4 of the ATM Forum UNI 4.0 Signaling specification [4].

F3-47[47]: The ISIS-700 *shall* support Connected Line Identification Restriction (COLR) service as specified in Annex 4 of the ATM Forum UNI 4.0 specification [4].

F3-48[48]: The ISIS-700 *shall* support Subaddressing (SUB) service as specified in Annex 4 of the ATM Forum UNI 4.0 specification [4].

F3-49[49]: The ISIS-700 *shall* support User-user Signaling (UUS) as specified in Annex 4 of the ATM Forum UNI 4.0 Signaling specification [4].

Table 3-3 summarizes the UNI 4.0 capabilities supported by the ISIS-700.

The UNI 4.0 signaling capability types are as follows:

M: Required for minimum functionality
O: Optional for all categories of switching systems

The Reference indicates the section(s) in the UNI 4.0 Specification [4] where the corresponding UNI 4.0 capabilities are described in details. The UNI 4.0 capabilities marked "R" are required in Release 1.5 of the ISIS-700. Those marked "F" are required in a future release. Those marked "N" are not required.

No	UNI 4.0 Capability	Reference	Type	ISIS-700 Support
1	Point-to-point calls	2	M	F
2	Point-to-multi point calls	5	M	F
3	Signaling of individual Qos parameters	9	M	F
4	Leaf initiated join	6	O	N
5	ATM anycast	7	M	F
6	ABR signaling for point-to-point calls	10	O	N
7	Generic identifier transport	2.1.1	O	F
8	Virtual UNIs	Annex 8	O	F
9	Switched virtual path (VP) service	2	O	F
10	Proxy signaling	Annex 2	O	F
11	Frame discard	2	O	F
12	Traffic parameter negotiation	8	O	F
13.1	Direct dialing in (DDI)	Annex 4	O	F
13.2	Multiple subscriber number (MSN)	Annex 4	O	F
13.3	Calling line identification presentation (CLIP)	Annex 4	O	F
13.4	Calling line identification restriction (CLIR)	Annex 4	O	F
13.5	Connected line identification presentation (COLP)	Annex 4	O	F
13.6	Connected line identification restriction (COLR)	Annex 4	O	F
13.7	Sub-addressing (SUB)	Annex 4	O	F

No	UNI 4.0 Capability	Reference	Type	ISIS-700 Support
13.8	User-user signaling (UUS)	Annex 4	O	F
Notes:				

Table 3-3 Summary of ISIS-700 UNI 4.0 Signaling Capabilities

3.3.3. PNNI

R3-50[50]: The ISIS-700 *shall* support the call/connection procedures for point-to-point calls as described in Section 6.3.1 and 6.5 of the ATM Forum PNNI Specification, Version 1.0 [2].

F3-51[51]: The ISIS-700 *shall* support the call/connection procedures for point-to-multi point calls as described in Section 6.3.4 and 6.6 of the ATM Forum PNNI Specification, Version 1.0 [2].

R3-52[52]: The ISIS-700 *shall* support the Signaling of Individual QoS Parameters as described in 6.5.2.3.5 of the ATM Forum PNNI specification, Version 1.0 [2].

F3-53[53]: The ISIS-700 *shall* support ATM anycast capability specified in Section 4.8 of the ATM Forum PNNI specification, Version 1.0 [2].

R3-54[54]: The ISIS-700 *shall* support Crankback procedure for Point-to-Point calls as specified in Annex B of the ATM Forum PNNI specification, Version 1.0 [2].

F3-55[55]: The ISIS-700 *shall* support Associated Signaling as specified in section 6.5.2.2.1 of the ATM Forum PNNI specification, Version 1.0 [2].

F3-56[56]: The ISIS-700 *shall* support Negotiation of ATM Traffic Descriptors as specified in section 6.5.2.3.4 and 6.5.2.6.2 of the ATM Forum PNNI specification, Version 1.0 [2].

R3-57[57]: The ISIS-700 *shall* support PNNI Switched Virtual Path (VP) Service.

R3-58[58]: The ISIS-700 *shall* support Soft PVPC and PVCC connections as specified in Soft Permanent Connections External Interface Specification [14].

N3-59[59]: The ISIS-700 *shall* not support PNNI ABR Signaling for Point-to-point calls specified in Section 6.4.5.5 and 6.4.5.6 of the ATM Forum PNNI specification, Version 1.0 [2].

R3-60[60]: The ISIS-700 *shall* support Generic Identifier Transport Information Element described in Section 6.4.5.31 of the ATM Forum PNNI specification, Version 1.0 [2].

F3-61[61]: The ISIS-700 *shall* support Frame Discard procedures as specified in Section 5.5.4.1.2 the ATM Forum PNNI specification, Version 1.0 [2].

F3-62[62]: The ISIS-700 *shall* support ILMI functionality over PNNI Links.

R3-63[63]: The ISIS-700 *shall* support the following NCCI features as described in *THE ATM FORUM, NETWORK CALL CORRELATION IDENTIFIER V1.0, AF-CS-0140.000, MARCH 2000.*[15]:

- AESA based NCCI format as defined in section 2.
- NCCI procedures for Point-to-Point PNNI calls as specified in section 3.2 and 7.
- Interaction with Soft PVC as described in section 6.1

All other features are not supported.

F3-64[64]: The ISIS-700 *shall* support PNNI Path and Connection Tracing as specified in PNNI addendum for Path and Connection Trace BTD-CS-PNNI-TRAC -01.01.

Table 3-4 summarizes the PNNI signaling capabilities supported by the ISIS-700.

The PNNI signaling capability types are as follows:

M: Required for minimum functionality
O: Optional for all categories of switching systems

The Reference indicates the section(s) in the PNNI Specification [2] where the corresponding PNNI signaling capabilities are described in details. The PNNI signaling capabilities marked "R" are required in Release 1.5 of the ISIS-700. Those marked "F" are required in a future release. Those marked "N" are not required.

No	PNNI Signaling Capability	Reference	Type	ISIS-700 Support
1	Point-to-point calls	6.3.1,6.5	M	R
2	Point-to-multi point calls	6.3.4,6.6	M	F
3	Signaling of Individual QOS parameters	6.5.2.3.5	M	R
5	ATM Anycast	4.8	M	F
6	Crankback	Annex B	M	R
7	Associated Signaling	6.5.2.2.1	O	F
8	Negotiation of ATM traffic descriptors	6.5.2.3.4 and 6.5.2.6.2	O	F
9	Switched Virtual Path (VP) service		O	R
10	Soft PVPC and PVCC support	Annex C	O	R
11	ABR Signalling for Point-to-point Calls	6.4.5.5 and 6.4.5.6	O	N
12	Generic Identifier Transport	6.4.5.31	O	R
13	Frame Discard	5.5.4.1.2	O	F

No	PNNI Signaling Capability	Reference	Type	ISIS-700 Support
14	ILMI over PNNI links		O	F
15	NCCI support	*THE ATM FORUM, NETWORK CALL CORRELATION IDENTIFIER V1.0, AF-CS-0140.000, MARCH 2000.*	O	R
16	Path and Connection Trace	Af-cs-0141.000	O	F

Table 3-4 Summary of ISIS-700 PNNI Signaling Capabilities

3.3.4. Call Release requirements

If no RELEASE COMPLETE message is received from the user before timer T308 expires the second time, the signaling specifications state that the equipment shall perform implementation dependant recovery.

R3-65[65]: The ISIS-700 *shall* initiate the restart procedures if no RELEASE COMPLETE message is received on a UNI or NNI signaling channel before T308 expires a second time. Note that restarting the signaling channel will clear all calls on the signaling channel.

The restart procedures are used to return a virtual channel, all virtual channels in a virtual path, or all virtual channels controlled by the signaling channel to the idle condition. The procedure is usually invoked when the other side of the interface does not respond to other control messages or failure has occurred. It may also be initiated as a result of local failure, maintenance action or mis-operation.

R3-66[66]: The ISIS-700 shall support the restart procedure in section 5.5.1 of Q.2931 [11] with the following modifications:

- The number of consecutive unsuccessful restart attempts in 5.5.1.2 in Q.2931 shall be limited to 2.
- When the restart limit is reached, an event will be sent to the management entity. All virtual channels that are in the out-of-service condition shall be unavailable until the signaling channel is disabled or removed.

~~3.3.~~3.4. SIGNALING INTERWORKING

Formatted: Bullets and Numbering

When a signaling message transits an ISIS-700 chassis, the ingress signaling channel and the egress signaling channel may not run the same variant of ATM signaling protocol, e.g. the ingress may be using UNI3.1 and the egress may be using PNNI. In this case a protocol interworking function may take place

F3-67[67]: The ISIS-700 *shall* support the interworking between the following ATM signaling protocols. The interworking features marked “R” are be supported in the current release, and those marked “F” shall be supported in a future release. Those marked “N” are not required.

Interworking Protocols	Point-to-Point	Point-to-Multipoint (root initiated join)	Point-to-Multipoint (leaf initiated join)
UNI 3.1 ↔ UNI 4.0	F	F	N
UNI 3.1 ↔ PNNI	F	F	N
UNI 4.0 ↔ PNNI	F	F	N

Table 3-5 ISIS-700 Signaling Protocol Support

4. FUNCTIONAL REQUIREMENTS

4.1. MANAGEMENT REQUIREMENTS

4.1.1. Configuration Requirements

4.1.1.1. Signaling Application Types

A signaling channel carries signaling messages between two signaling entities. A signaling channel must be provisioned before SVCs can be setup. The signaling channel is normally configured as VCC on the interface that it controls, but in the case of Proxy signaling the signaling channel can be on a different interface.

A Route Control Channel (RCC) is used by the PNNI protocol to exchange routing information between the adjacent nodes. The RCC must be provisioned on an interface running the PNNI signaling protocol so that PNNI routing information can be exchanged between the nodes.

An ILMI channel is normally used to register addresses on CPE, and is used mainly on interfaces running the UNI signaling protocol. The ILMI channel can also be configured on interfaces running the PNNI signaling protocol. ILMI is described in the ILMI External Functional Specification.

Signaling channels, RCC and ILMI channels on the ISIS-700 are configured using internally terminated connections. Internally terminated connections are described in the Connections External Functional Specification [12].

Not all combinations of signaling channels, RCC and ILMI channels can be configured on an interface. On the ISIS-700 the valid combinations are grouped into ATM Signaling applications that can be configured on an ATM Service interface. The following ATM Signaling applications can be configured on an ATM Service interface on the ISIS-700.

- **PNNI** – This type of ATM signaling application can only be configured on an ATM NNI service interface and requires that a PNNI signaling channel and a RCC to be configured on the service interface. The signaling channel controls all the SVC endpoints on the service interface.
- **UNI** – This type of ATM signaling application can only be configured on an ATM UNI service interface and requires that a UNI signaling channel be configured on the service interface. The signaling channel controls the SVC endpoints on the service interface.
- **UNI with ILMI** – This type of ATM signaling application is the same as the UNI signaling application, except that an IMLI channel is also required to be configured on the service interface.
- **Proxy UNI** – This type of ATM signaling application can be configured on an ATM UNI service interface, and in the case of remote proxy can also be configured on an

ATM NNI interface. Proxy ATM signaling application requires that a UNI 4.0 signaling channel be configured on the ATM service interface. This signaling channel normally controls SVC endpoints on other service interfaces that are associated to this signaling channel.

R4-1[68]: The ISIS-700 *shall* support management requests to configure an ATM NNI service interface to support the PNNI signaling application.

F4-2[69]: The ISIS-700 *shall* support management requests to configure an ATM UNI service interface to support the UNI signaling application.

F4-3[70]: The ISIS-700 *shall* support management requests to configure an ATM UNI service interface to support the UNI with IMLI signaling application.

F4-4[71]: The ISIS-700 *shall* support management requests to configure an ATM service interface to support the Proxy signaling application, and allow other ATM Service interfaces to be controlled by the proxy signaling channel.

R4-5[72]: The ISIS-700 *shall* allow one and only one of PNNI, UNI or UNI with IMLI signaling applications to be configured on the ATM service interface at the same time.

R4-6[73]: The ISIS-700 shall assign a unique application alias to a configured ATM Signaling application.

An ATM Signaling application has a strong association with an interface it is providing service for, and therefore cannot be configured without the existence of the ATM service interface.

R4-7[74]: The ISIS-700 shall not allow creation of a PNNI application for an ATM Service Interface if the interface is not configured.

F4-8[75]: The ISIS-700 shall not allow creation of an ATM UNI Signaling application for an ATM Service Interface if the interface is not configured.

Several attributes of a PNNI link which are used for PNNI routing, are also configured as a part of PNNI application configuration.

R4-9[76]: The ISIS-700 shall support management requests to configure the following routing attributes for a PNNI link when configuring a PNNI Signaling application as described in Atm Signaling EIS-P [24]:

- Administrative weight for Constant Bit Rate traffic
- Administrative weight for Real Time Variable Bit Rate traffic
- Administrative weight for Non Real Time Variable Bit Rate traffic
- Administrative weight for Unspecified Bit Rate traffic
- Virtual Path capability which indicates if a VPC can be establish within the link.

Signaling channels have a number of configuration options and tuning parameters. The ISIS-700 shall allow the management system to configure these parameters when the signaling channels are created. Some parameters will be fixed depending on the signaling application, and some of the configured parameters can be modified without disrupting the signaling application.

R4-10[77]: The ISIS-700 shall support management requests to configure each ATM Signaling channel with any of the following parameters that are applicable to the type of signaling application that the channel is providing (as described in Atm Signaling EIS-P [24]):

— Signaling protocol (e.g. UNI 3.1, UNI 4.0 or PNNI)

— Interface type (e.g. User or Network)

— Layer 2 protocol timers

— Layer 3 protocol Timers

4.1.1.2. UNI Signaling Application Subscription Parameters

Once a UNI is configured to be controlled by a UNI Signaling application, several subscription parameters need to be specified. In the UNI Signaling specification, there are several features that are not necessarily required to be supported on a public UNI, regarding which information in a SETUP message is to be forwarded and which is not. Support of these features is determined by subscription, and so these subscription values must be configured.

The following subscription parameters may need to be specified at the User-Network Interface:

1. Calling Party Number delivery feature: This parameter indicates whether the Calling Party Number (CgPN) is delivered to the user equipment at the called address.

2. Calling Party Subaddress transfer feature: This parameter indicates whether to accept and transfer Calling Party Subaddress information from the calling user on call/ connection origination. Calling Party Subaddress information is only delivered to the called user if CgPN information is delivered.
3. AESA for Calling Party transfer feature: This parameter indicates whether to accept and transfer the AESA for Calling Party information from the calling user on call/ connection origination. AESA for Calling Party information is only delivered to the called user if CgPN information is delivered.
4. Calling Party Number screening feature: This parameter indicates whether screening of a user-provided CgPN is supported at the originating UNI. With screening, the originating ATM NE checks the user-provided CgPN to make sure it is one of the allowable numbers. (This list of allowable numbers is discussed below.) If the number fails screening, the switch will replace the user provided CgPN with the default number for the interface in the SETUP message. This will result in a completed call, but the number used for signaling will not be the number requested by the calling customer.
5. The list of allowable calling numbers for screening must be configured if screening is active. One number is identified as the “default number” for the UNI.
6. Called Party Subaddress transfer feature: This parameter indicates whether to accept, transfer, and deliver Called Party Subaddress information from the calling user on call/connection origination.

The next two items refer to Broadband High- and Low- Layer Information transfer features. The ability to disable their transfer is designed to allow carriers to protect themselves against customers using the unused octets of signaling messages for free information transfer.

7. Broadband High Layer Information (BHLI) transfer feature: This parameter indicates whether to accept, transfer, and deliver high layer information from the calling user to the called user on call/connection origination.
8. Broadband Low Layer Information (BLLI) transfer feature: This parameter indicates whether to accept, transfer, and deliver low layer information from the calling user to the called user on call/connection origination.
9. Broadband Low Layer Information selection feature: This parameter indicates whether to accept, transfer, and deliver up to three instances of the low layer

information parameter(s) for low layer information selection in a single message. This parameter may be supplied only if the BLLI transfer feature is “yes”.

10. AAL Parameters transfer feature: This parameter indicates whether to accept, transfer, and deliver ATM adaptation layer parameter information from the calling user to the called user on call/connection origination.

Table 4-1clarifies which subscription parameters apply at the originating UNI and which one at the terminating UNI, according to ATM UNI Signaling specifications.

Subscription Feature	**Originating UNI**	**Terminating UNI**
CgPN Delivery	N/A	Yes
CgPN Subaddress Transfer	Yes	N/A
AESA for CgP Transfer	Yes	N/A
CgPN Screening	Yes	N/A
CdPN Subaddress Transfer	Yes	N/A
BHLI Transfer	Yes	N/A
BLLI Transfer	Yes	N/A
BLLI Selection	Yes	N/A
AAL Parameters Transfer	Yes	N/A

Table 4-1 Locations at Which Subscription Features Apply

F4-11[78]: The ISIS-700 shall support Management system requests to configure each ATM UNI service interface that is controlled by a UNI Signaling application with any of the following signaling subscription features that are applicable on a per-subscriber basis:

- Calling Party Number delivery
- Calling Party Subaddress transfer
- AESA for Calling Party transfer the ATM NE will replace the user-provided CgPN with the default number for the
- Calling Party Number screening feature: When this value is ‘yes’, a list of valid numbers is supplied by the management system. One of these values is specified as the “default” number.
- Called Party Subaddress transfer
- Broadband High Layer Information transfer
- Broadband Low Layer Information transfer

— Broadband Low Layer Information selection

— AAL Parameters information transfer.

4.1.1.3. Virtual User-Network Interfaces

NOTE: !!!TBD: Review and clarify this section later, once virtual UNIs are clearly defined.

At the UNI, each VPC that is controlled by the signaling entity is assigned a VPCI. This may be done in one of several ways:

- The Management Plane can configure these VPCs with the associated VPCIs.
- The Management Plane can configure the range of VPIs and VPCIs that are used by the Control Plane, and which are under the control of the Management Plane. Note that UNI 3.1 does not include provisions to negotiate or modify allowed ranges for VPCIs and/or VCIs.

Note also that in UNI 3.1, there is a restriction on the UNI that there is a one-to-one mapping between the VPCI and VPI (i.e., VPI =VPCI). In UNI 4.0, this is not always required, although it is the default case.

F4-12[79]: The ISIS-700 shall support Management system requests to configure the VPCIs of a UNI/V-UNI. Such configuration should be undertaken consistent with the constraints of the version of the signaling channel that controls the VPCIs.

VPCIs are identifiers used by the signaling layer to identify VPCs. They are distinct from VPI values, which are identifiers used by the ATM layer to identify VPLs. In many cases the VPCI and VPI are assigned the same value (in fact, VPIs and VPCIs are often mistakenly considered to be identical).

In the ATM Forum's UNI 3.1 specification, VPCIs are configured on a UNI so that the VPCI always has the same value as the VPI. In UNI Signaling 4.0, the VPCI value does not have to equal the VPI value, although it is assumed that many customers will use VPCI =VPI at their interface. Thus, VPCI =VPI should be the default relationship to minimize unnecessary Management System interactions.

When V-UNIs are supported, the VC Switch interfaces to the VP multiplexer via the Vb Interface. For the VC Switch side of the Vb interface, the VPI space must be shared among V-UNIs, and each V-UNI that supports signaling requires a signaling access point. See Figure 4-1 . For each VPI used for signaling bearer channels at the switch, there must be a relationship established to a VPCI and to a V-UNI. At the VP multiplexer, there is a mapping between the VPIs used by the customer and VPIs used by the VC Switch.

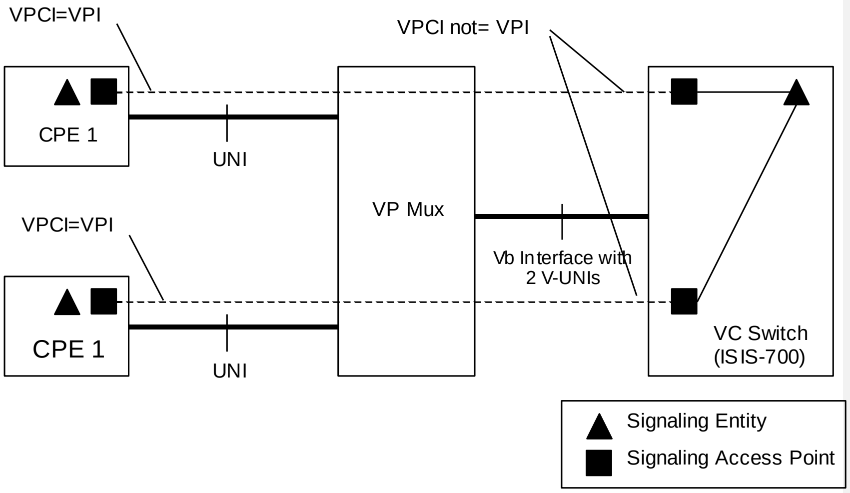

Figure 4-1 ~~4-1~~Example Signaling Configuration of Two Virtual UNIs

The specification allows for any arbitrary mapping of VPCIs to VPIs at the Vb interface. It would be desirable if there could be a simple formula to map VPIs from the Customers' UNIs to VPIs on the Vb interface, such as dividing the Vb interface's VPI space into contiguous ranges for each V-UNI. This is possible if it can be known in advance, once and for all, how many VPIs each UNI will require. However, a requirement that a UNI's VPIs be contiguous can cause problems, particularly where there are many V-UNIs that share the same VPI space of a Vb interface. For example, if 4 VPIs are assigned to each V-UNI, but later it is determined that one customer needs 5 VPIs, then many other customers will need to have their VPCs reconfigured at the VP multiplexer in order to keep that customer's 5 VPIs contiguous. This would result in service outage, and a great deal of effort.

Consequently, a table approach is appropriate. At the VC Switch side of the Vb interface, the VPI value is associated with a V-UNI (e.g., by using the VP multiplexer's interface ID for the UNI), and a VPCI value. Table 4-2 shows an example. The following constraints apply in all cases:

- All values in the "VPI at Vb" column must be unique
- For a given V-UNI ID, a VPCI value must be unique.

The following are allowed:

- Any "VPI at Vb" value may be associated with any V-UNI
- Different V-UNIs may use the same VPCI value.

VPI at Vb	V-UNI ID	VPCI
0	1	0
1	1	1
2	2	0
3	1	3
4	2	2
5	2	3
6	1	4

Table 4-2 An Example of VPI Mapping at the Vb Interface

For UNIs (as opposed to V-UNIs), it may be possible to always assume that the VPCI =VPI, so it is not necessary to explicitly configure the VPCI via the Management System in this case. However, if they may differ, then configuration is required.

F4-13[80]: For VPIs that can be used to support SVC bearer channels on a UNI, a default VPCI value equal to the VPI value shall be assumed. However, the ISIS-700 shall support Management System requests of associating a different VPCI to a VPI.

For V-UNIs, it is necessary to associate the information such as that shown in Table 4-2 with a VPI.

F4-14[81]: To support configuration of a V-UNI, based on information provided by the management system, the ISIS-700 shall associate the following with each VPI that supports SVCC bearer channels on the Vb interface:

- V-UNI ID
- VPCI. (For any given V-UNI, a VPCI must be unique.)

4.1.1.4. Handling of Physical Port failures

It takes between 15 to 30 seconds to detect a signaling channel failure after an ATM service interface has gone down. SVC call clearing is normally initiated when the signaling channel failure is detected. This length of time may not be acceptable, and the user should be given the ability to initiate call clearing much sooner after the ATM service interface has gone down.

F4-15[82]: The ATM service interface that is controlled by an ATM signaling channel *shall* have the following additional attributes that are provisioned:

— ATM Signaling Hold down timer. This is the number of seconds to wait before the ISIS-700 initiates SVC clearing when the interface has gone down. A value of 0 shall result in the ISIS-700 clearing the SVCs immediately upon detection of the interface outage.

NOTE: When this future requirement becomes a requirement then R3-21 should be modified.

Disabling the ATM Signaling application shall disable all contained signaling, RCC and ILMI channels. Disabling signaling channel causes Layer 2 disconnect message to go out on the channel and the channel goes to operationally ~~u~~Unavailable state ~~status down~~. All the calls controlled by the signaling channel are cleared. The administrative ~~state~~ mode is set to ~~unavailable~~Unavailable. Any further attempts at bringing up the channel will be ignored until the channel is made active. Enabling a channel sets the administrative ~~state~~ mode to be ~~active~~Active. An attempt will be made to bring the channel operationally up. Attempts by attached equipment to bring the channel up will succeed.

R4-16[83]: The ISIS-700 *shall* allow the management system requests to change the administrative ~~state~~ mode of the ATM signaling application. Note that the channels contained within the signaling application will change their administrative mode accordingly regardless in what mode they were individually set before. In the case of PNNI Signaling application, refer to the ATM Routing and Addressing EFS for behavior specific to the RCC and Hello Protocol running over the associated PNNI Link.

R4-17[84]: The ISIS-700 *shall* allow the management system requests to change the administrative mode~~state~~ of a signaling channel. All calls controlled by the signaling channel shall be cleared when the administrative mode is set to U~~u~~navailable and no new calls shell be accepted on that channel. In the case of PNNI application, the corresponding Rcc channel will not change its administrative mode.

R4-18[85]: The ISIS-700 *shall* allow the management system requests to change the administrative mode of a Routing Control channel of the PNNI application. If the Rcc Admin mode is changed to Unavailable, the Hello protocol will be stopped on a service interface carrying the Rcc channel. The corresponding ATM signaling channel will not change its administrative mode.

Restarting (or resetting) the ATM signaling application shall restart all contained signaling, RCC and ILMI channels. When a signaling channel is restarted, a Layer 3 message is sent over the signaling channel to restart all calls controlled by the signaling channel. All calls controlled by the signaling channels are cleared and the signaling channel is brought to a known state.

R4-19[86]: The ISIS-700 *shall* allow management requests to restart an ATM signaling application~~up~~. This operation will result in restart of all its contained channels.

R4-20[87]: The ISIS-700 *shall* allow management requests to restart an ATM signaling channel.

R4-21[88]: The ISIS-700 *shall* allow management requests to restart Routing Control Channel.

R4-22[89]: The ISIS-700 *shall* not allow management requests to delete an ATM service interface if an ATM Signaling application is configured on that interface.

For an ATM signaling application to be fully functional, all the channels (i.e. signaling and routing channels) that are required for that application must be configured and fully operational. The channel can go into the operationally unavailable state if the channel's internally terminated connection is removed or if the protocol at peer is not operational.

R4-23[90]: The ATM Signaling application *shall* be placed in the operationally unavailable state, if one or more of its channels is operationally unavailable.

The ATM Signaling Channels are attached to internally terminated Permanent Virtual Connection carrying the signaling traffic. Internally terminated Permanent Virtual Connections (ITC) are described in "ISIS-700 SAS Internally Terminated Connections, 1000-SAS-0185-xx" specification and Connections External Functional Specification [12]. ISIS-700 makes association of internally terminated PVCs with configured ATM Signaling Channels. The association is done by using a unique Signaling application Identifier representing the ATM Signaling Application.

The ISIS-700 discovers and informs management when invalid association of internally terminated Permanent Connection with ATM Signaling Channel occurs as a result of invalid PNNI or UNI Signaling application Id, i.e. unknown Application Id. The alarm will exist until the Internally Terminated Connection is not delete.

NOTE: Association will not happen even if the Signaling application Id becomes valid, i.e. user later configures PNNI or UNI Signaling Application.

Also, the ISIS-700 discovers and informs management when invalid association of internally terminated Permanent Connection with PNNI Rcc Channel occurs as a result of invalid PNNI application Id. The alarm will exist until the Internally Terminated Connection is not delete.

4.1.1.5. Other ATM Signaling Application Configuration Parameters

It is desirable to limit the range of VPI/VCI used for SVCs within the full range allowed for PVCs. By creating two separate address ranges, you can use one VPI/VCI range for PVCs on the ATM service interface, and different (smaller) VPI/VCI range for SVCs on the same ATM service interface. This addressing scheme also allows the ISIS-700 to inter-operate with an SVC capable CPE that only supports VPI 0 for SVCs. You can set the VPI/VCI range to limit SVCs to VPI 0, while allowing PVCs to utilize the full VPI range.

R4-24[91]: The ATM service interface *shall* have the following additional attributes that are provisioned:

- Minimum VCI for SVCs. If an ATM Signaling application is provided on that interface then this value shall be between the minimum VCI value for PVC and the maximum VCI value for PVCs. If the minimum VCI value for PVC is less than 32, then the minimum VCI value for SVC shall be 32.
- Maximum VCI for SVC. If an ATM Signaling application is provided on that interface then this value shall be between the minimum VCI value for PVC and the maximum VCI value for PVCs.
- Minimum VPI for SVC. If an ATM Signaling application is provided on that interface then this value shall be between the minimum VPI value for PVC and the maximum VPI value for PVCs.
- Maximum VPI for SVC. If an ATM Signaling application is provided on that interface then this value shall be between the minimum VPI value for PVC and the maximum VPI value for PVCs.

It is also desirable to limit the percentage of ATM service interface bandwidth that SVCs are allowed to consume. This is useful in cases when you want to offer both SVC and PVC services on an ATM Service interface yet limit the amount of a bandwidth available for SVCs. When an ATM service interface is configured for use with SVCs, you should have the ability to set the bandwidth available for SVCs for each supported class of service (CBR, VBR-RT, VBR-NRT, UBR).

Note that a transit SPVC at a UNI or NNI endpoint is treated as a SVC endpoint and is subject to the entered SVC allowed bandwidth. An originating or terminating SPVC a UNI or NNI is treated as a PVC and is not subject to the entered SVC allowed bandwidth.

F4-25[92]: The ATM service interface that is controlled by an ATM signaling application *shall* have the following additional attributes that are provisioned:

- The bandwidth for Constant Bit Rate (CBR) traffic that is available to SVCs
- The bandwidth for Variable Bit Rate Real Time (VBR-RT) traffic that is available to SVCs
- The bandwidth for Variable Bit Rate Non-Real Time (VBR-NRT) traffic that is available to SVCs
- The bandwidth for Unspecified Bit Rate (UBR) traffic that is available to SVCs

Transit delay is the end-to-end delay of user information transferred between a calling an called user. It includes the following components:

- Processing time in the end-user systems, e.g., AAL handling and cell assembly
- The network transfer delay which includes propagation delay, ATM layer transfer delay, and network processing delays.

Section 4.5.17 and Annex K of ITU-T Recommendation Q.2931 [11] require that signaling entities support the accumulation of an end-to-end transit delay measure on a per call basis.

The maximum acceptable delay may be indicated by a user in the call SETUP message along with the cumulative value for the transit delay from the calling user to the network boundary. If the delay measure is greater than the user's maximum acceptable value, the call will be cleared. The use of this feature is optional to the user, but the network must support it. In order to implement this feature the switch must have an expected value for its transfer delay. It is expected that this value could be independently determined, e.g., by testing, and then be configured by a management system.

R4-26[93]: The ISIS-700 shall support configuration of its expected ATM cell transfer delay.

4.1.2. Status Requirements

The ISIS-700 shall maintain status on the ATM signaling application and on the channels configured for the signaling application.

R4-27[94]: The ISIS-700 *shall* maintain the following status for each ATM signaling application, and shall support requests to retrieve this information:

— Operational state

R4-28[95]: The ISIS-700 *shall* maintain the following status for each ATM signaling channel, and shall support requests to retrieve this information:

— Assigning mode of the signaling channel. The assigning mode of the signaling channels is determined using the configured protocol and interface type.

— Operational state

— Connection state indicating if the channel is connected or disconnected.

R4-29[96]: The ISIS-700 *shall* maintain the following status for each RCC channel, and shall support requests to retrieve this information:

— Operational state

— Connection state indicating if the channel is connected or disconnected.

4.1.3. Statistics and Counters

SAAL Performance Monitoring Counters

As with any other protocol, the approach is one of protocol observation to identify protocol abnormalities and to maintain a time-sequential history of PDU activity or a subset of it. These events may reflect various types of problems in the network, ranging from facility failures that cause an SSCOP link failure, to malfunctions in the software implementing the protocol.

There are two main activities associated with the maintenance function:

- Protocol monitoring - for detecting undesired abnormality levels
- Protocol data capture - for logging protocol abnormalities.

SSCOP protocol abnormalities include SSCOP PDU retransmission and errored PDU received. The errored PDUs include unexpected PDUs, invalid PDUs (as defined in SSCOP) and PDUs with sequence number errors or list element errors. The SSCOP monitoring functions count the SSCOP protocol abnormalities. For SSCOP performance monitoring, the following events are counted:

- SSCOP connection disconnect (i.e., loss of SSCOP connection). The SSCOP connection between signaling entities is a rather critical resource since it carries signaling traffic. The significance of losing the SSCOP connection is relative (it may be used for interoffice signaling, or it may be used for access signaling for a single video terminal), so there will be cases when it is critical to monitor this event and cases when it is desirable but not essential.
- Inability to establish an SSCOP connection
- Reestablishment or resynchronization of the SSCOP link connection. This usually indicates lack of synchronization between the two ends.

In most cases, the above abnormalities are communicated to layer management through an MAA-ERROR indication. A list of the error codes can be found in Annex A of the SSCOP standard (see Q.2110 [9] and T1.637).

R4-30[97]: The ISIS-700 shall count a *sum of errors* counter to monitor the receive side of each signaling channel that it supports. This *SSCOP Connection Monitoring Counter* is incremented when any of the following events occurs:

— SSCOP connection disconnect - The abnormal occurrence of this event is characterized by the expiry of Timer_NO_RESPONSE. This event is communicated to the layer management with MAA-ERROR code P.

— SSCOP connection initiation failure - This condition indicates the inability to establish an SSCOP connection. This event occurs whenever the number of expiries of the connection control Timer_CC exceeds MaxCC (communicated to layer management with MAA-ERROR code O) or upon receipt of a connection reject message BGREJ PDU.

— SSCOP connection re-establishment/resynchronization - This event occurs upon receipt of a BGN PDU or RESYNC PDU.

R4-31[98]: The ISIS-700 shall count a *sum of errors SSCOPErrored PDUs* counter of errored PDUs to monitor the receive side of each signaling channel that it supports. This counter is incremented when any of the following events occurs:

— Unexpected PDUs (MAA-ERRORS A-M).

— Invalid PDUs. These are defined in SSCOP and consist of PDUs with incorrect length (MAA-ERROR code U), undefined PTU type code (i.e., ‘0000’) or “not 32-bit aligned”.

— Unexpected PDU Values. PDU N(S), N(PS), N(R) errors or list elements error in STAT/USTAT PDUs. These events are communicated to layer management with MAA-ERRORs Q-T.

These counters shall be used on all PNNI and UNI signaling channels. For UNI channels, the ISIS-700 shall allow the Management System to activate/deactivate the protocol monitoring capability for a given channel.

F~~R~~4-32[99]: For ATM signaling channels, the ISIS-700 should count an additional SSCOP performance monitoring parameter to monitor the transmit (network to user) side of the UNI Signaling channel:

SSCOP Network Monitoring Counter - This counter is incremented upon the occurrence of any of the following events:

— SSCOP connection initiation failure - This event occurs when issuing a connection reject message BGREJ PDU.

— SSCOP connection establishment - This event occurs when issuing a BGN PDU or RESYNC PDU.

— Monitoring of the transmit side should be activated/deactivated independently from monitoring of the receive side.

ATM Signaling Performance Monitoring Counters

Performance monitoring activities for the ATM signaling protocol include monitoring and data capture of ATM Signaling Layer 3 PDUs at both the receive side and the transmit side. This allows an ISIS-700 to detect and diagnose problems associated with an improper protocol implementation or unusual behavior. The following abnormalities can occur:

- Abnormal call/connection termination - A call/connection can be abnormally terminated by unrecoverable conditions that cause termination of the call/connection, or dropping of one of its parties, by issuing a RELEASE, RELEASE COMPLETE, ADD PARTY REJECT or DROP PARTY messages. These messages contain a Cause field that indicates the condition causing the termination (including timer expiries) and are issued either in response to an offending message or as a result of a problem in the network or at the other end of the call/connection.
- *Status errors* - In some instances, a message with errors is received that does not cause termination of the call/connection. In these cases, a STATUS message with a cause field is used to respond to the offending message.

Protocol monitoring of the signaling channel is achieved by classifying abnormalities into the following categories,

1. **Route Unavailability counter -** This counter is incremented when a route is not available. It is incremented when a RELEASE, RELEASE COMPLETE, ADD PARTY REJECT or DROP PARTY message is transmitted or received, that contain any of the Cause values from Table 4-3. Note that these Cause values apply to both UNI 3.1 and UNI 4.0.

Cause value	Meaning	Result
Cause #1	Unallocated (Unassigned) number	Clear
Cause #2	No route to specified transit network	Clear
Cause #3	No route to destination	Clear
Cause #88	Incompatible destination	Clear
Cause #128	Next Node Unreachable	Clear
Cause #160	DTL Not my Node ID	Clear

Table 4-3 Cause Values for Unavailable Routes

2. **Resource Unavailability counter -** This counter reflects network, service and user resource unavailability. This corresponds to RELEASE, RELEASE COMPLETE, ADD PARTY REJECT or DROP PARTY messages transmitted or received, that contain any of the Cause values from Table 4-4.

Cause value	Meaning	Result
Cause #34	No Circuit/Channel Available	Clear
Cause #35	Requested VPCI/VCI unavailable	Clear
Cause #37	User cell rate not available (UNI 3.1 only)	Clear
Cause #38	Network out of order Clear	Clear

Cause value	Meaning	Result
Cause #41	Temporary failure	Clear
Cause #42	Switching System Congestion	Clear
Cause #45	No VPCI/VCI available	Clear
Cause #47	Resource unavailable, unspecified	Clear
Cause #49	Quality of Service unavailable	Clear
Cause #58	Bearer capability not presently available	Clear
Cause #63	Service or option not available, unspecified	Clear
Cause #92	Too many pending add party requests	Clear

Table 4-4 Cause Values for Resource Unavailability

3. **Called Party Responsible for Unsuccessful Call counter -** This counter is incremented when the call/connection cannot be completed because of the Called Party. It is incremented when a RELEASE, RELEASE COMPLETE, ADD PARTY REJECT or DROP PARTY message is transmitted or received, that contain any of the Cause values from Table 4-5. Note that these Cause values apply to both UNI 3.1, and UNI 4.0.

Cause value	Meaning	Result
Cause #17	User busy	Clear
Cause #18	No user responding	Clear
Cause #21	Call rejected	Clear
Cause #22	Number changed	Clear
Cause #23	User rejects all calls with Calling Line ID Restriction (CLIR)	Clear
Cause #27	Destination out of order	Clear
Cause #31	Normal, unspecified	Clear

Table 4-5 Cause Values for Called Party Events

4. **Incorrect Messages counter -** A count that reflects any sort of incorrect information in a message. This includes:

— RELEASE, RELEASE COMPLETE, ADD PARTY REJECT, DROP PARTY and STATUS messages transmitted or received, that contain any of the Cause values from Table 4-6.

— Ignored messages. These messages are ignored because the message was so damaged that it could not be further processed. A list of the “ignored messages” is compiled below:

1. Message with invalid protocol discriminator
2. Message with errors in the call reference Information Element
    - Bits 5-8 of the first octet not equal to ‘0000’
    - Bits 1-4 of the first octet indicating a length other than 3 octets
    - RELEASE COMPLETE message received with a call reference that does not relate to a call active or in progress
    - SETUP message received with call reference flag incorrectly set to 1
    - SETUP message received with a call reference for a call that is already active or in progress.
3. Message too short.

Cause value	Meaning	Result
Cause #6	Channel unacceptable	Clear
Cause #36	VPCI/VCI assignment failure (UNI 3.1, 4.0 and DSS2)	Clear
Cause #81	Invalid call reference value	Clear
Cause #82	Identified channel does not exist	Clear
Cause #89	Invalid endpoint reference	Clear
Cause #95	Invalid message, unspecified	Clear
Cause #96	Mandatory information element missing	Clear

Cause value	Meaning	Result
Cause #97	Message type non-existent or not implemented	STATUS
Cause #99	Information Element non-existent or not implemented	STATUS
Cause #100	Invalid information element contents	[1]
Cause #101	Message not compatible with call state	STATUS
Cause #104	Incorrect message length	Clear
Cause #111	Protocol error, unspecified	Clear

Table 4-6 Cause Values for Incorrect Messages

5. **Calling Party Events counter -** This counter monitors error events caused by the originating user doing something wrong. It is incremented when a RELEASE, RELEASE COMPLETE, ADD PARTY REJECT, DROP PARTY or STATUS messages transmitted or received that contains any of the Cause Values from Table 4-7.

Cause value	Meaning	Result
Cause #28	Invalid number format	Clear
Cause #29	Facility rejected	Clear
Cause #43	Access information discarded	Clear
Cause #50	Requested facility not subscribed	Clear
Cause #57	Bearer capability not authorized	Clear
Cause #65	Bearer capability not implemented	Clear
Cause #73	Unsupported combination of traffic parameters	Clear
Cause #78	AAL Parameters cannot be supported (UNI 3.1, 4.0 and DSS2)	STATUS
Cause #79	Service Option not Implemented	Clear
Cause #91	Invalid transit network selection	Clear

Table 4-7 Cause Values for Calling Party Events

[1] Clear for Mandatory IEs; STATUS for optional IEs.

6. **Timer Expiries counter -** A count of network timers expiries and, to some extent, user timers expiries. The conditions for incrementing this counter are

   — Expiry of any network timer

   — Receipt of a RELEASE or RELEASE COMPLETE message with Cause #102, “recovery on timer expiry.”

7. **Restart Activity counter -** A counter that reflects user and network restart activity. This counter is incremented when receiving or transmitting a RESTART message.

NOTE: For any of the counters above, RELEASE COMPLETE messages that are a reply to a previous RELEASE message and contain the same Cause value, are redundant (for counting purposes) and should not be counted.

R4-33[100]: The ISIS-700 shall count ~~and threshold~~the following sum of errors counters for a ATM (UNI and PNNI) ~~n UNI~~ signaling channel when requested by the Management System. Separate counts shall be made for the transmit direction (i.e., away from the ISIS-700) and receive direction (i.e., into the ISIS-700) for each parameter.

— Route Unavailability (i.e., messages RELEASE, RELEASE COMPLETE, ADD PARTY REJECT, DROP PARTY and STATUS with Cause codes shown in Table 4-3)

— Resource Unavailability (i.e., messages RELEASE, RELEASE COMPLETE, ADD PARTY REJECT, DROP PARTY and STATUS with Cause codes shown in Table 4-4)

— Called Party Responsible for Unsuccessful Call (i.e., messages RELEASE, RELEASE COMPLETE, ADD PARTY REJECT, DROP PARTY and STATUS with Cause codes shown in Table 4-5)

— Incorrect Messages (i.e., messages RELEASE, RELEASE COMPLETE, ADD PARTY REJECT, DROP PARTY and STATUS with cause codes shown in Table 4-6)

— Calling Party Events (i.e., messages RELEASE, RELEASE COMPLETE, ADD PARTY REJECT, DROP PARTY and STATUS with cause codes shown in Table 4-7)

Commented [sc1]: Page: 1
I assume thresholding is Future.

— Timer Expiries (i.e., expiry of any network timer, or receipt of a RELEASE or RELEASE COMPLETE message with Cause #102, “recovery on timer expiry”)

— ATM Signaling Layer 3 Restart activity counter.

SVC network data collection requirements at the UNI/V-UNI support NDC requirements relating to call/connection traffic load monitoring. It is desirable for the ISIS-700 to count the total number of successful and unsuccessful call/connection attempts at the access interface. This includes intra-switch calls and calls involving more than one ISIS-700. Note that for calls/connections involving more than one switch, counts of call/connection completion problems at the interoffice signaling points where problems occur are more useful to the network, because this provides information about where there is a problem.

In addition, a measure is needed of call/connections that are successfully established.

Both parameters should be counted separately for the incoming (i.e., coming into the ISIS-700 performing the counting) and outgoing (i.e., out of the ISIS-700) directions. The count of call/connection attempts, when combined with the counts of call/connection completions, provides a measure of the completion success being experienced by the user.

R4-34[101]: The ISIS-700 *shall* count the number of call/connection attempts (regardless of whether they are successful or not) and successful call/ connection completions ~~for a UNI/V-UNI,~~ on a per ATM (PNNI and UNI) signaling channel basis. These counts shall be made separately for the incoming and outgoing directions.

R4-35[102]: The ISIS-700 *shall* keep a count of the following messages transmitted and received by the signaling channel:

— Setup

— Call proceeding

— Connect

— Alerting

— Notify

— Progress

— Release

— Release Complete

— Restart

— Restart Acknowledge

— Status

4.2. MAINTENANCE AND DIAGNOSTICS

SSCOP PDU Data Capture

The data capture activity applies to both the receive and transmit side of the signaling channel, and it consists of maintaining a log of SSCOP PDUs. Such a log may be activated for an SSCOP connection to gather diagnostic information about SSCOP PDUs. It may be activated once protocol-monitoring counters have crossed a threshold, or, more pro-actively, a log may be activated on selected signaling channels on an ongoing basis so LEC personnel will have immediate access to diagnostic information when an error is suspected.

Some PDUs contain a sequence number, and there is a running counter for these counts. Other PDUs contain no sequence number. POLL PDUs contain their own sequence numbers, with a different running counter.

In order to fully understand a sequence of states at one end of an SSCOP connection to diagnose problems, it is important to know the order in which PDUs were sent, received, and when timers expired. This allows analysis of the state transitions that occurred. Thus, a single log is indicated.

F4-36[103]: The ISIS-700 shall be capable of supporting an SSCOP log that monitors both the transmit and receive direction of a signaling channel. The ISIS-700 shall allow a Management System to activate/deactivate the logging capability. The logging capability shall be activated/deactivated independently from the protocol monitoring activities. When the log is full, new information shall replace the oldest information in the log. The ISIS-700 shall be capable of logging SSCOP PDUs and timer expires for at least 10% of its access signaling channels at any given time, and for at least 5 separate interoffice signaling channels at a given time.

— The SSCOP log shall maintain entries for the most recent SSCOP PDUs or timer expiries of a connection. For access signaling channels, the log needs to be capable of storing 100 large SSCOP PDUs. For interoffice signaling channels, the log needs to be capable of storing

1000 large SSCOP PDUs. Log information from one SSCOP connection shall not overwrite information from another connection.

— An entry in the SSCOP log shall be made upon the transmission of an SSCOP PDU, upon the receipt of any SSCOP PDU, or upon expiry of any local SSCOP timer.

— There are two types of log entries: SSCOP PDUs and local SSCOP timer expiries. When PDUs are logged, entries shall contain the following:

- Timestamp (time of log entry, accurate to the nearest ms, according to the local clock)
- PDU. For data PDUs (SD PDU, UD PDU and MD PDU), only the last 32 octets of the information field would need to be logged to get information about SSCOP operation. However, the entire PDU shall be logged in order to support analysis of the operation of higher-layer PDUs within the SSCOP PDUs (e.g., DSS2).
- Whether PDU was sent or received.

— The log entry for a timer expiry event shall be as follows:

- Timestamp (time of log entry, accurate to the nearest ms, according to the local clock)
- SSCOP timer identifier
- SSCOP timer value.

ATM Signaling Layer 3 PDU Data Capture

The logging activity applies to both the receive and transmit side of the UNI. Note that *all* ATM Signaling layer 3 messages on a signaling channel are logged when logging is activated, so that the sequence of events can be reconstructed.

F4-37[104]: The ISIS-700 shall be capable of supporting, for each UNI signaling channel, one ATM Signaling protocol log of layer 3 timers. The ISIS-700 shall allow a Management System to activate/deactivate the logging capability for a given UNI signaling channel. The logging capability shall be activated/deactivated independently from the protocol monitoring activities. The ISIS-700 shall be capable of logging all of its UNI signaling channels. It shall be capable of logging at least 100 timer expiries, and when full, the oldest entry shall be replaced by the newest.

— The log entry for a timer expiry event shall be as follows:

- Call Reference ID for the timer that expired

- Timestamp (time the expiry is logged, accurate to the nearest ms, according to the local clock)
- ATM Signaling layer 3 timer identifier
- ATM Signaling layer 3 timer value.

4.3. BILLING

An ISIS-700 chassis shall generate raw call data for each switched call. The call data records (CDR) shall be stored in a file on the local disk and periodically transferred to an offline billing mediation system, where the records will be analyzed and used for customer billing. The billing requirements supported by the ISIS-700 are described in the ATM Forum ATM Usage Measurement Requirements document.

F4-38[105]: The ISIS-700 shall support the usage measurements for billing purposes as described in Section 4 of the ATM Forum ATM Usage Measurement Requirements, af-nm-0154.000, with the following modifications:

— *<< Add modifications >>*

4.4. FAULT TOLERANCE

4.4.1. SCM Redundancy

SCM Redundancy support provides support for a warm Standby SCM. The datapath is kept hot; however, the control path is lost during the time of the switchover. The Signaling Stacks and associated functional entities are not going to be kept hot on the Standby SCM with the FSO functionality In Release 1.5. What this implies is that on a switchover to the Standby, although the signaled connections may be kept up (that is, the datapath may be up), state information associated with those connections is lost. Hence, after a switchover, it is necessary to release signaled connections and reconfigure the ATM Signaling application so as to get to a known state. Hence, the functionality associated with Switched Connections in the presence of FSO may be worse than that associated with Permanent Connections. In a best case SCM switchover, the Permanent

Connections datapath does not get impacted (very minimal impact); however, the Switched Connections datapath shall always be impacted.

The datapath associated with the Switched Connections is taken down towards the tail end of the Switchover process, so as to minimize the impact to these connections. However, since Layer 3 of the protocol is unavailable during the time of the switchover (it resides on the SCM), the ISIS-700 will lose the ability to handle incoming messages that need to be processed by this layer. This may lead to the end, on not receiving a response to a Release message, for example, restarting the Signaling Channel, which will result in the release of ALL calls associated with the channel. However, on the ISIS-700 end, the hardware is configured with those connections since the Restart message won't get processed during the time of the switchover.

There are a few enhancements that may be possible to help minimize the impact of the switchover. For example, on an SM, a Layer 3 protocol may be faked to respond with a release to all messages received so the other end does not perceive the link to be down. However, the impact of this addition needs further investigation, and hence will be marked as Future functionality.

Refer to Figure 4-2 Partial SCM Switchover Sequence with ATM Signaling Functionality for ATM Signaling behavior within the SCM Switchover sequence.

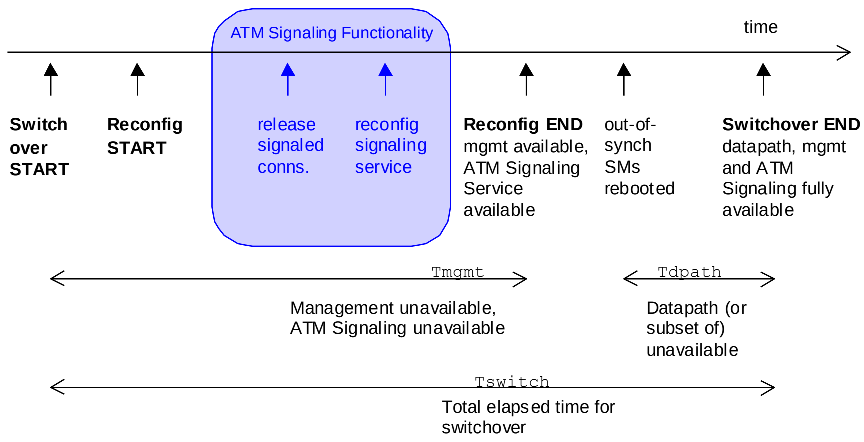

Figure 4-2 Partial SCM Switchover Sequence with ATM Signaling Functionality

R4-39[106]: The ISIS-700 shall not be required to process requests for the setup of new connections or release of existing connections (that is, process Layer 3 ATM Signaling messages) from the time of (Forced or Controlled) SCM Switchover initiation until the management plane is restored as per SCM Redundancy EFS [16].

R4-40[107]: The ISIS-700 shall process requests for the setup of new Switched Virtual Connections after management plane is restored as per SCM Redundancy EFS [16].

R4-41[108]: It shall be permissible for the ISIS-700 to release all signaled connections on a Forced or Controlled SCM Switchover. The release of signaled connections shall be initiated after the switchover is initiated. Refer to the SCM Redundancy External Functional Specification for details associated with the switchover timing sequence [16].

NOTE: Until the Signaling Stacks and associated functional entities are kept hot on the Standby SCM, the intent is to always force release of all signaled connections so as to restore Signaling application to a known state.

R4-42[109]: The ISIS-700 shall reconfigure ATM Signaling application after the signaled connections are released. For those (out-of-sync) SMs that are rebooted as a result of the switchover, the reconfiguration of ATM Signaling application on the rebooted SMs shall occur. Refer to the SCM Redundancy External Functional Specification for details associated with the switchover timing sequence.

R4-43[110]: The configuration of signaled connections on an SM shall not be taken into account when determining the configuration consistency of an SM after a Forced or Controlled SCM Switchover. Signaled Connection information is not stored in PDB, and hence does not qualify to be included as part of this check.

F4-44[111]: After a Switch Over Start, the ISIS-700 shall respond to the Far-End with a RELEASE message for all Layer 3 messages received. This may prevent the Far-End attempting to release a call and receiving no response, for example, to restart of the ATM Signaling Channel, which will result in all calls being released. Note that, eventually, the ISIS-700 will still be forced to release all calls prior to reconfiguring the Signaling application. The addition of this functionality may help reduce potential downtime for these calls.

~~Describe requirements for SCM FSO: all Calls dropped after switchover, but links reconfigured and restored. – reason SVC state is in RAM and not preserved on a SCM FSO.~~

4.5. PERFORMANCE

The ISIS-700 will be used in a number of different networks and must be able to meet the demands to which it will be subjected. Many factors can influence the measured performance of the network and characterization of the signaling performance is important to understanding how the switch will perform under realistic traffic situations.

The ATM Forum has defined a uniform set of signaling performance measurements which both the service providers and vendors can use to gauge the performance of network elements under “real” world signaling traffic. This section describes the requirements for signaling performance on the ISIS-700.

The ATM signaling protocol stack consists of the following protocol layers, Call Control, Q.93b and the Signaling ATM Adaptation Layer (SAAL). The Call Control and Q.93b layers are primarily responsible for call establishment. The SAAL maintains the signaling channel and provides robust transmission of signaling messages between peer signaling entities.

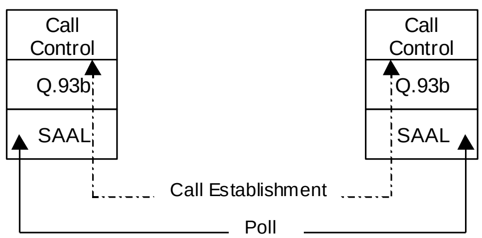

Figure 4-3~~4-2~~ Signaling Message Flow

Call Establishment

The following illustrates the process of Connection Establishment. A Setup message containing the traffic descriptor and QoS requirements is transmitted from the Source to the Destination. If the network can guarantee the requested QoS, it will forward the Setup message to its Destination.

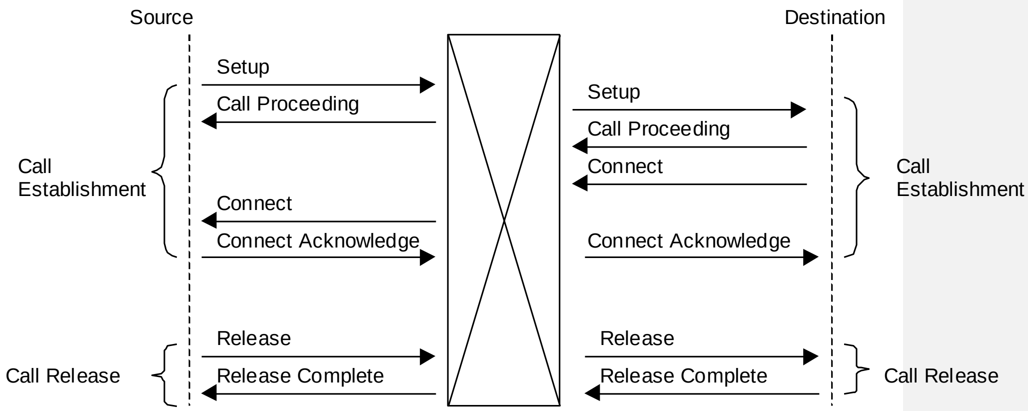

Figure 4-4~~4-3~~ Connection Establishment and Tear down

The destination processes the Setup message and responds with a Connect message that is eventually forwarded to the Source. Either the Source or the Destination can release the call by generating a Release message.

The setup rate refers to the rate at which connections are requested from the network. Since a Setup message is used to request a connection, Setup rate is the rate at which Setup messages are transmitted from the Source. In the same way, Connect rate is the rate at which Connect messages are received by the Source.

Signaling Performance Metrics

The Performance metrics currently being standardized by the ATM Forum for Point-to-point and Point-to-Multipoint calls are as follows,

- Burst Throughput Rate,
- Latency,
- Sustained Throughput Rate, and
- Simultaneous Active Call Capacity (SAC).

4.5.1. Burst Throughput Rate

The purpose of the burst throughput rate is to indicate how a network will perform when it is bombarded with a burst of connection or disconnection requests (setup/ release messages). A burst of Setup messages simulates a number of users simultaneously accessing the network, while a burst of Release messages can occur in cases of network link failure.

Burst throughput rates are measured by generating a ‘short’ burst of messages. The messages are generated by the tester to the switch at the maximum generation rate of the tester. The time to establish ‘N’ calls, release ‘N’ calls, or perform ‘N’ call cycles through the switch is measured, and then divided by ‘N’. The burst throughput rate is the inverse of this value. For example, if the time to establish 100 calls is 2 seconds, then the burst throughput rate is 50 calls/second.

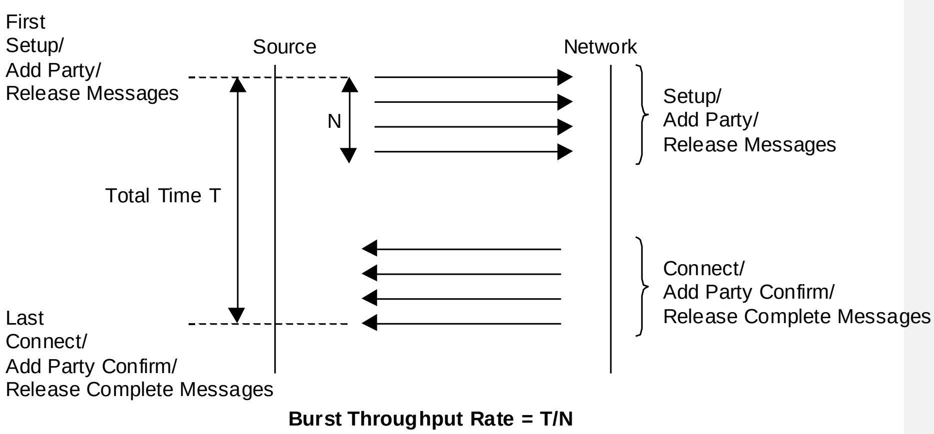

Figure 4-5~~4-4~~ Burst Throughput Rate Measurement

By increasing the burst size, a characteristic curve of the switch can be plotted. At burst sizes less than or equal to an optimum burst size, the measured Burst Throughput rate will remain constant. Beyond this point, the network signaling performance will begin to degrade.

R4-45[112]: The ISIS-700 shall support a burst setup rate of 200 calls per second on cell relay interfaces.

R4-46[113]: The ISIS-700 shall support a burst release rate of 200 calls per second on cell relay interfaces.

R4-47[114]: The ISIS-700 shall support a connection burst rate of 200 calls per second on cell relay interfaces.

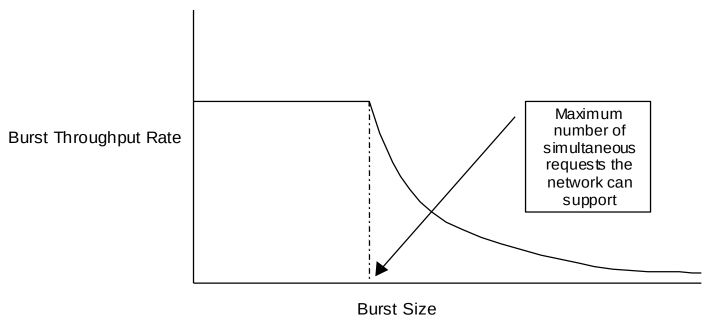

Figure 4-6~~4-5~~ Burst Throughput Rate Characterization

In the event of signaling storms, the ISIS-700 discards new setups once the number of outstanding setups has exceeded a fixed threshold. Setups will only be allowed once the backlog has been cleared, i.e. the number of outstanding setups is below the threshold. Even though the ISIS-700 may discard setups, it will still accept call clearing and call progress messages. The ISIS-700 depends on the other side to re-signal messages that were dropped after the protocol timer expires.

4.5.2. Message Latency

Latency measures the propagation delay of messages across a network. It is the time it takes a network to receive, process and propagate messages across its interfaces. To measure latency, the message is transmitted by the source to the switch and the corresponding entry (A) and exit (B) times are noted. The message latency is the difference between these times. (B-A).

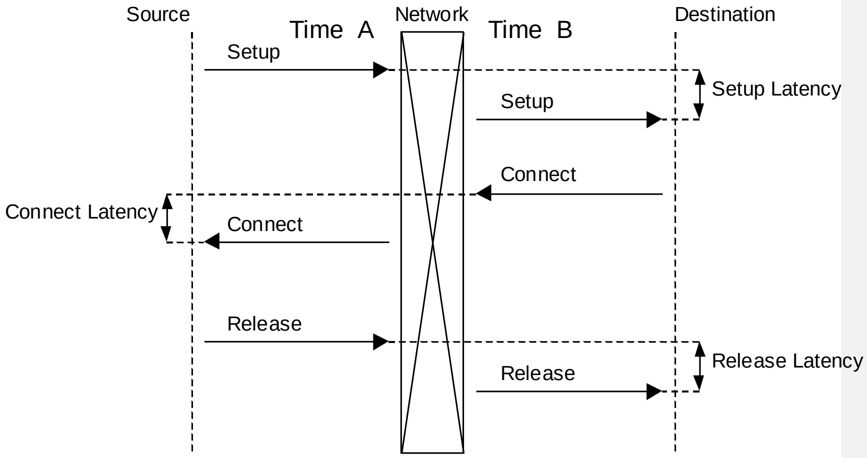

Figure 4-7~~4-6~~ Latency Measurements

For example, the Setup latency is the time that a Setup message spends in the Network. A Setup message is transmitted to the network and the corresponding entry and exit times are noted. The Setup Latency is the difference between these times.

Latency measurement is important since it will ultimately influence the time it takes the network to establish a connection. High latencies will cause calls to remain in the initiated state for extended periods. Since Service Providers start their billing process only after the connection is established, latency can have negative impact on the bottom line.

Release Latency measures the time it takes the switch to release the resources allocated for a call, after the source or destination has released it. It is a measure of how effective the network manages its resources.

Call Establishment Latency is the sum of the Setup and Connect Latencies. This is an indication of how much delay was introduced by the network during the establishment of a call.

The traffic conditions and the Message contents can influence the latency of a network. For example, Setup messages with different traffic parameters will require different processing to be performed by the network. So it is important to measure Latency under different traffic types and network conditions.

R4-48[115]: The setup message latency shell be no more than 30 mili seconds on ISIS-700.

R4-49[116]: The connect message latency shell be no more than 30 mili seconds on ISIS-700.

R4-50[117]: The release message latency shell be no more than 20 mili seconds on ISIS-700.

R4-51[118]: The mean setup delay shell be 80 mili sec. and 95 percentile shell be 125 mili sec.

4.5.3. Sustained Throughput Rate

The Sustained Throughput rate gives an indication of the long-term performance of a network under different signaling traffic. It allows Service Providers to test the ability of their networks to reliably process connections over extended periods.

The Sustained Throughput rate is an extension of the Burst Throughput rate, except that this measurement is performed over an extended period, typically forty-eight hours. Setup messages are generated to the network at a defined rate for an extended period. Once the calls become active, they are released. The average Connect rate is the average number of Connect messages per second that is received by the test application from the network. If the network can successfully handle the offered Setup rate, the average Connect rate will be equivalent to the average rate Setup rate. Otherwise, the average Connect rate will be less than the average Setup rate.

To measure the maximum sustained throughput rate of a network, the setup rate is incremented to the point where the average connect rate is less than the average setup rate. The maximum sustained throughput rate of the network is at the rate which setup and connect times are equivalent.

The maximum rate at which both the Setup and Connect rates are equivalent, is the sustained throughput rate.

R4-52[119]: The ISIS-700 shall support minimum sustained throughput rate of 100 calls per second.

R4-53[120]: The ISIS-700 shall support maximum sustained throughput rate of 150 calls per second.

4.5.4. Simultaneous Active Call Capacity (SAC)

As its name suggests, the Simultaneous Active Capacity (SAC) is the number of simultaneous Connections that a Network can support. Service providers can use this number to compute the maximum number of users they should add to their network.

The Capacity (SAC) is measured by making a number of Connection requests to destinations across the network until release messages are received from the network. Because SAC is not a rate measurement, the calls are generated at a very low rate. The number of successful calls will increase until the Network reaches its maximum SAC. Beyond this point, the network will reject all incoming connection requests.

R4-54[121]: The number of Simultaneous Active SVC Calls on the ISIS-700 shall be equal to number of cross connection available on a chassis [12].

APPENDIX A DEFINITIONS AND ACRONYMS

ATM Anycast	The ability to allow an application to request a point-to-point connection to a single ATM end system that is part of an ATM group.
CDV	*Cell Delay Variation*.
CLP	*Cell Loss Priority* – A bit in the ATM cell header to indicate two levels of priority for discarding ATM cells.
CLR	*Cell Loss Ratio* – define as Lost Cells/Total Transmitted Cells, this is a QoS parameter that the network agrees to offer as an objective over the lifetime of the connection. It is expressed as an order of magnitude, having a range of 10-1 to 10-15 and unspecified.
CPCS	*Common Part Convergence Sublayer* – The portion of the convergence sublayer of an AAL that remains the same regardless of the traffic type
Crankback	A mechanism for partially releasing a PNNI connection setup in progress which has encountered a failure.
CTD	*Cell Transfer Delay* – The elapsed time between a cell exit event at the source UNI and the corresponding cell entry event at the destination UNI for a particular connection. The cell transfer delay between two measurement points is the sum of the total inter-ATM node transmission delay and the total ATM node processing delay.
DTL	*Designated Transit List* – A list of node and optionally link Ids that completely specify path across a single PNNI peer group.
ILMI	*Integrated Local Management Interface* – An ATM Forum defined interim specification for network management functions between an end user and a public or private network and between a public network and a private network. This is based on a limited subset of SNMP capabilities.
Logical Link	An abstract representation of the connectivity between two logical nodes. This includes individual physical links, individual virtual

path connections, and parallel physical links and/or virtual path connections.

Native Address An address or address prefix that matches one of a given node's summary addresses.

NSAP *Network Service Access Point* – OSI generic standard for a network address consisting of 20 octets. ATM has specified E.164 for public network addressing and the NSAP address structure for private network addresses.

PDU *Protocol Data Unit.*

PVCC *Permanent Virtual Channel Connection* –An ATM connection where switching is performed on the VPI/VCI fields of each cell, and one which is provisioned through some network management function and left up indefinitely.

PVPC *Permanent Virtual Path Connection* – An ATM connection where switching is performed on the VPI field only of each cell and one which is provisioned through some network management function and left up indefinitely

S-PVC *Soft Permanent Virtual Connection* – A PVCC or PVPC that is established using the ATM signaling procedure.

QoS *Quality of Service* – Defined on an end-to-end basis in terms of the following attributes of the end-to-end ATM connection:

- Cell Loss Ratio
- Cell Transfer Delay
- Cell Delay Variation

SAAL *Signaling ATM Adaptation Layer* – A layer that resides between the ATM layer and the Q.2931 function. The SAAL provides reliable transport of Q.2931 messages between Q.2931 entities (e.g., ATM switch and host) over the ATM layer; two sublayers: common part and service specific part

SSCOP *Service Specific Connection Oriented Protocol* – The common part of SAAL for connection-oriented traffic as specified in ITU-T Q.2110

SSCS-UNI *Service Specific Convergence Sublayer at the UNI* – The service specific part of SAAL as defined in ITU-T Q.2130.

APPENDIX B RATIONALE & NOTES

~~A.1~~B.1 ISSUE NUMBER 1

~~A.1.1~~B.1.1 Sub Issue Number 1

~~A.1.2~~B.1.2 Sub Issue Number 2

Formatted: Bullets and Numbering

APPENDIX C REQUIREMENTS CHANGE LOG

Table C-1: Requirements Change Log

Date	Author	Requirement Number	Description

Last Immutable Requirement Number ever used in this document is: 121.