NIST Special Publication 823-5

Computer Systems Technology

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology

NIST

North American ISDN Users' Forum Agreements on Integrated Services Digital Network

NORTH AMERICAN ISDN USERS' FORUM

The National Institute of Standards and Technology was established in 1988 by Congress to "assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries."

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering and performs related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Public Inquiries Desk, 301-975-3058.

Technology Services
- Manufacturing Technology Centers Program
- Standards Services
- Technology Commercialization
- Measurement Services
- Technology Evaluation and Assessment
- Information Services

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Electromagnetic Fields[1]
- Electromagnetic Technology[1]

Chemical Science and Technology Laboratory
- Biotechnology
- Chemical Engineering[1]
- Chemical Kinetics and Thermodynamics
- Inorganic Analytical Research
- Organic Analytical Research
- Process Measurements
- Surface and Microanalysis Science
- Thermophysics[2]

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Molecular Physics
- Radiometric Physics
- Quantum Metrology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Automated Production Technology
- Robot Systems
- Factory Automation
- Fabrication Technology

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- Reactor Radiation

Building and Fire Research Laboratory
- Structures
- Building Materials
- Building Environment
- Fire Science and Engineering
- Fire Measurement and Research

Computer Systems Laboratory
- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

Computing and Applied Mathematics Laboratory
- Applied and Computational Mathematics[2]
- Statistical Engineering[2]
- Scientific Computing Environments[2]
- Computer Services[2]
- Computer Systems and Communications[2]
- Information Systems

---

[1] At Boulder, CO 80303.

[2] Some elements at Boulder, CO 80303.

North American ISDN Users' Forum Agreements on Integrated Services Digital Network

Daniel P. Stokesberry and Tish A. Antonishek, Editors

Advanced Systems Division
Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-0001

March 1994

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

TECHNOLOGY ADMINISTRATION
Mary L. Good, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Arati Prabhakar, Director

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) has a unique responsibility for computer systems technology within the Federal government. NIST's Computer Systems Laboratory (CSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. CSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. CSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 823 series reports CSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

National Institute of Standards and Technology Special Publication 823-5
Natl. Inst. Stand. Technol. Spec. Publ. 823-5, 351 pages (March 1994)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1994

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

North American ISDN Users' Forum Agreements
on Integrated Services Digital Network

ABSTRACT

This document compiles the existing North American Integrated Services Digital Network (ISDN) Users' Forum (NIUF) agreements for an ISDN developed and approved in the NIUF as of October 1992. New agreements superseded or added during 1992 cover Layer 1 BRI at the U, and S/T reference points. In addition, this document references the Conformance tests which have been completed by the NIUF. These include: Layer 3, BRI, Layer 2 BRI, PRI at the U reference point, and PRI at the U/S/T reference points. Finally, this document contains the Application Profiles for: Secure Voice Mail; Data Conferencing—Multi-Point; ISDN Telephone Workstation Integration; Engineering Workstation Interface; and the Remote Agent Application Profile.

KEY WORDS

application profile; basic rate interface; conformance test; implementation agreement; ISDN; LAPD; NIUF; primary rate interface.

NOTICE OF DISCLAIMER

ACKNOWLEDGMENTS

NIST would like to acknowledge all of the members and participants, past and present, in the North American ISDN Users' Forum for their valuable contributions to this document.

WORKSHOP AND WORKING GROUP CHAIRS

IUW Chair	Claude Stone	First Nat'l Bank of Chicago
IIW Chair	Don Auble	Ameritech Services
NIUF Secretariat	Dawn Hoffman	NIST
NIUF Asst. Secretariat	Sara Caswell	NIST
<u>IUW INDUSTRY GROUPS</u>		
Computer and Telecommunications	Rick Zipes	Mitel
Financial/Services	Martin Risbergs	American Airlines
Government Services	James Johnson	U.S. Air Force
Manufacturing	Karl Schohl	GM
Small Business	George Abbott	North Carolina State University
<u>IUW AD HOC COMMITTEES</u>		
Applications Review	Scott Beale	Aeronautical Radio, Inc.
Public Policy and Strategic Planning	David Norem	DoD
EDI	Claude Stone	First Nat'l Bank of Chicago
Broadband ISDN	Bob Doxey	Pacific Bell
<u>IUW APPLICATION FAMILIES</u>		
Network Management/ISDN Administration	N/A	
Call Management	Scott Beale	Aeronautical Radio, Inc.
CPE Compatibilities and Capabilities	Pat Krause	McDonald's Corporation
Network Interconnectivity	Rick Zipes	Mitel
Messaging and Answering	Karen Patten	AT&T Bell Labs
Issues	Karen Patten	AT&T Bell Labs
	Bill Selmeier	Dowty Network Systems, Inc.
<u>IIW EXPERT GROUPS</u>		
Applications Analysis	Bob Sherry	AT&T Bell Labs
Applications Software Interface	Cheng Chen	Teleos Communications
ISDN Conformance Testing	Matt Martini	NYNEX
Network Management	Tom Russotto	American Computer
ISDN Security	Jonathan Katz	TASC
Satellite, Radio, and Mobile	John Kennedy	Northern Telecom Canada Ltd.
Signalling	John Kantonides	AT&T Bell Labs
Supplementary Services	Chris Wallace	Bell Northern Research
<u>IIW PROFILE TEAMS</u>		
Call Management	George Gawrys	AT&T
CPE Compatibilities and Capabilities	Bob Larribeau	Fujitsu
Messaging and Answering	Glenn Ehley	Siemens Stromberg-Carlson
Network Interconnectivity	Ira Clark	DGM&S
Network Management/ISDN Admin.	Tom Russotto	American Computer
Security	William Few	DoD
<u>IIW AD HOC COMMITTEES</u>		
Versions	Gerry Hopkins	Bell Atlantic
Application Profile Development	Gerry Hopkins	Bell Atlantic
<u>EXECUTIVE STEERING COMMITTEE STANDING GROUPS</u>		
Applications Services Group	Matt Thomson	Northern Telecom
Finance Committee	James Kendrick	Aeronautical Radio, Inc.

TABLE OF CONTENTS

1 Introduction

The purpose of the Integrated Services Digital Network (ISDN) Agreements document, its organization and an overview of the North American ISDN Users' Forum (NIUF) are described in the following subsections.

1.1 Purpose of this Document

Participants in the October 1992 NIUF Plenary meeting, approved a motion to publish all agreements reached among the members as of October 1992. This document is a compilation of these NIUF agreements for an ISDN.

1.2 Evolution of this Document

New versions of this document will be issued as progress is made in developing and approving implementation agreements, conformance tests, and application profiles within the NIUF. It is the intent of the NIUF, that each new version be compatible with previous versions. Therefore, each revision will supersede preceding versions, as each new version will include all of the unchanged agreements from previous versions, as well as errata pages for previously approved agreements.

1.3 Document's Organization

The ISDN Agreements document is organized into specific sections as follows:

- Section 1
  Introduction—The purpose of this document, the document's organization, and an overview of the structure and organization of the NIUF.

- Section 2
  ISDN Versions—A specific interoperable subset of an ISDN which functions in a multi-vendor environment.

- Section 3
  Implementation Configurations—A categorization of the ISDN capabilities, based upon access and equipment class information.

- Section 4
  Implementation Agreements—The Implementation Agreements (IAs) are developed by both implementor and user representatives participating in the NIUF Expert Working Groups. The IAs provided in this section allow for expeditious development of ISDN capabilities, and promote interoperability of ISDN communications equipments.

- Section 5
  ISDN Conformance Test Specifications—Conformance Test (CT) suites for an ISDN are detailed in this section of the agreements.

- Section 6
  Application Software Interface—The Application Software Interface (ASI) section will focus on the definition of a common application interface for accessing and administering ISDN services provided by Network Adapters.

- Section 7

  Application Profiles—The Application Profiles (APs) contain the recommended set of agreements and specifications for all layers and aspects of ISDN communication which must be present to support a particular user's application or set of applications (application family).

- Section 8

  References—The References section provides a listing of documents identified but not included in this publication.

1.4 NIUF Overview

The following text introduces the NIUF purpose and organization.

1.4.1 Purpose of the Forum

The Integrated Services Digital Network (ISDN) is defined in a group of international recommendations for a worldwide communications network for the exchange of all information (voice, data, and image) among all users, independent of any manufacturer, service provider, or implementation technology.

ISDN recommendations are being developed by the International Telephone and Telegraph Consultative Committee (CCITT). In North America, the ISDN standards are being developed by Committee T1, which is accredited by the American National Standards Institute (ANSI) and sponsored by the Exchange Carriers Standards Association (ECSA).

The result is one extensive standard with a tremendous variety of options and parameters. This is necessary to meet all the possible needs and technologies for which the standards could be used. However, to ensure interoperability and terminal portability within the ISDN network and its attendant terminals and other Customer Premises Equipment (CPE), a uniform subset of these options and parameters must be selected. Each application usually only requires a subset of functionality and in order for products to work together in a multi-vendor environment, common sets of options must be selected.

To cope with this proliferation of choices and to provide practical products and services which meet users' needs, the specification process must be extended to include Application Profiles, Implementation Agreements, and Conformance tests to promote interoperability.

1.4.2 NIUF/NIST Relationship

The North American ISDN Users' Forum has created a user voice in the implementation of ISDN and ISDN applications and has helped to ensure that the emerging ISDN environment meets users' application needs. The NIUF is sponsored by the National Institute of Standards and Technology (NIST). The precise relationship of the NIUF, NIST, and other business concerns is defined by the "Cooperative Research and Development Agreement: The Consortium on ISDN Based Systems."[1]

---

[1]For more information, contact the NIUF Administrator (see sec. 1.5).

1.4.3 NIUF Organization and Procedures

The actual work of the NIUF is accomplished in two workshops; the ISDN Users' Workshop (IUW) and the ISDN Implementors' Workshop (IIW). These workshops, which consist of various working groups and special project teams, meet several times a year and develop the following products: Application Requirements, Application Analyses, Application Profiles, Implementation Agreements, Conformance Criteria, and an Applications Software Interface. The IUW produces Application Requirements which describe potential applications of ISDN and the features which may be required.

The IIW develops Application Analyses, Application Profiles, Implementation Agreements, Conformance Criteria, and an Applications Software Interface which provide the technical detail necessary to implement an Application Requirement in an interoperable manner.

The activities within the two workshops are coordinated by the NIUF Executive Steering Committee. While specifics of the NIUF organization follow, particulars relating to the procedures for the NIUF are found in the "North American ISDN Users' Forum Practices Manual."[2]

1.4.3.1 ISDN Users' Workshop (IUW)

The IUW is responsible for identifying, defining, and prioritizing user requirements, as well as working with the IIW to define and approve agreements necessary to support the implementation of user requirements. Membership in the IUW is open to any organization. Users participating in the IUW are organized into seven Industry Groups: Manufacturing Industries, Process Industries, Service Industries, Small Business, Financial Services, Government, and Computing and Telecommunications Industries. The IUW organization emphasizes the synergy present when organizations from the same industry segment work together to define applications. Activities within the IUW are coordinated by the IUW Steering Committee.

The IUW work program is based on identifying potential user applications and structuring the IIW work to satisfy the user applications. Any user can request consideration for a particular ISDN application. The request should be for an application which could be used to support business related operations. It is important that ISDN solutions to business problems be based on business considerations which include:

- cost reductions,
- productivity enhancements,
- standard application interfaces,
- and performance improvements.

For a detailed description of the "User Application" Processing within the ISDN Users' Workshop, please refer to "North American ISDN Users' Forum Practices Manual."[3]

---

[2]Ibid.

[3]Ibid.

1.4.3.2 ISDN Implementors' Workshop (IIW)

The IIW is responsible for developing Application Analyses, Application Profiles, Implementation Agreements, Conformance Criteria, and an Applications Software Interface in support of IUW defined Application Requirements. The IIW also provides technical advice and consultation to the IUW, sponsors multi-vendor demonstrations and trials, and provides formal liaisons with appropriate organizations such as the Corporation for Open Systems (COS), the Open Systems Interconnection (OSI) Implementors' Workshop (OIW), or the ANSI Accredited Standards Committee T1. Membership in the IIW is open to any organization.

The IIW Steering Committee is responsible for coordinating the activities of the IIW groups. The IIW is organized into the following groups:

- Applications Analysis Working Group (WG),
- Application Profile Teams,
- Expert WGs,
- and ISDN Conformance Test (ICOT) WG.

The Applications Analysis WG develops an analysis of the user's application requirements, which serves as a basis for development of the Application Profile by the Applications Profile Teams. The Expert WGs produce the Implementation Agreements that are generally based on ANSI standards. In addition, there is an Expert WG defining an Applications Software Interface. The ICOT WG defines conformance requirements and develops abstract test suites for Implementation Agreements and Application Profiles.

1.4.4 ISDN Versions

A version defines and specifies ISDN as it exists at a certain point in time as derived from existing national and international standards and other consensus activities. Each version should be completely compatible with earlier versions. Manufacturers and service providers would be expected to develop ISDN offerings based on a particular version.

1.5 Point of Contact

Further information about the NIUF, including information on specific groups or activities within the NIUF, can be obtained by contacting:

NIUF Secretariat
National Institute of Standards and Technology
Building 223, Room B364
Gaithersburg, Maryland 20899
(301) 975-2937

2 Future ISDN Versions

Editor's Note: This section is reserved for future agreements on the definition and specification of ISDN Versions.

3 Implementation Configurations

The ISDN architecture is intended to interconnect all user and network equipments, in a ubiquitous fashion, in order to provide a common network encompassing all possible communication scenarios. Because of this broad scope, the national standards for the ISDN could not be universally applied to all the conceivable combinations of equipment types, access arrangements and applications. The concept of implementation configurations is introduced to allow specific ISDN capabilities (procedures) to be associated with a class of equipment, an access arrangement, or an application.

The use of the equipment class/access arrangement terminology permits clarification of the circumstances under which a certain capability should be available (i.e., when a particular equipment class is in use). It also permits a mechanism for indicating that a particular capability applies only to a subset of four possible configurations.

The implementation configurations, which were defined by the NIUF Signalling Working Group (SWG), have been applied to the layer 3 circuit-switched signalling protocols only. Future work will evaluate the implementation configuration concept for applicability to all agreements emerging from the NIUF.

The following text provides the current description of implementation configurations from the SWG:

The concept of equipment classes is introduced in this document to permit certain procedures to be associated with a particular application or class of equipment, e.g., station equipment versus Private Branch Exchange (PBX). Specifically, two classes of equipment are defined on the basis of two fundamental attributes.

The first attribute relates to the possibility of an exchange of signals occurring beyond the public network's point of contact with the interface (i.e., between the equipment directly connected to the public network and ISDN terminals or telephones connected to that equipment). For example, some user equipment may support subtending Basic Access digital subscriber loops and/or analog telephone loops. For Class I equipment, the network makes no provision for such an arrangement and assumes the Class I equipment constitutes the end point of the communication. Conversely, in the case of Class II equipment, the procedures at the network take into account that communication between Class II equipment (with which it communicates directly) and other equipment (with which the network does not have direct contact) may occur. As an example, Class II equipment may support digital and/or analog subscriber loops. Use of Class II equipment also involves the possibility of having interworking occur beyond the equipment with which the network has direct contact. Therefore, it is reasonable for Class II equipment to provide the network with an interworking notification, for both outgoing and incoming calls, when either the calling or called party respectively, is a non-ISDN user. Class II equipment may also send an interworking notification, if a private network exists beyond the Class II equipment and interworking to a non-ISDN facility within that network takes place. When an interface is associated with Class I equipment, it is assumed that multiple pieces of equipment may exist and communicate with the network over the D-channel. However, in this case, all equipment is assumed to be ISDN-capable and is considered as the end point of the communication. Therefore, interworking notification should not be accepted from Class I equipment.

The second attribute relates to the manner in which a SETUP message, the message which initiates an ISDN call, should be presented to the user equipment. When Class I equipment is applied on a particular interface, the network should broadcast the SETUP message associated with each call that terminates on that interface, since interaction between the network and multiple pieces of user equipment should be supported. On the other hand, the network should not broadcast SETUP messages associated with terminating calls to an interface on which Class II equipment is being used. Here, a single piece of user equipment is assumed to be involved in all communication with the network.

To the extent possible, it is desirable to have one set of requirements for ISDN call control apply to all ISDN user configurations. However, in cases for which integrated procedures are not appropriate, the call control procedures associated with Equipment Class I will differ from those associated with Equipment Class II. Unless otherwise noted, the assumption should be that a particular procedure/capability should be provided for both classes of equipment on both basic and primary rate access. However, use of the equipment class terminology permits clarification of the circumstances under which a certain capability should be available (i.e., when a particular equipment class is in use). It also permits a mechanism for indicating that a particular capability applies only to a subset of four possible configurations which are labeled as follows.

Table 3-1. Implementation Configurations

	Class I	Class II
BRI	*IB*	*IIB*
PRI	*IP*	*IIP*

BRI: Basic Rate Interface
PRI: Primary Rate Interface

In other words, a capability that applies to Class I equipment may be provided on basic access interfaces (*IB*) and/or primary rate access interfaces (*IP*). Similarly, a capability that applies to Class II equipment may be provided on basic access interfaces (*IIB*) and/or primary rate access interfaces (*IIP*).

The notation shown in the table above is used within this implementation agreement to indicate when protocol or procedures are only expected to be supported for a particular class and/or are limited to a particular type of interface, i.e., basic or primary rate interface.

4 Implementation Agreements

The Implementation Agreements (IAs) generated by the NIUF IIW provide the agreements for implementing the American National Standard (ANS) specifications for an ISDN. These IAs were developed and approved by both industry and user representatives participating in the Expert Working Groups, as well as the NIUF Plenary. The IAs exist to expedite the development of ISDN capabilities, to promote interoperability of ISDN communications equipments, and to provide a universal, multi-vendor implementation. The following text details the IAs.[4]

4.1 ISDN Lower Layer Specifications

The ISDN lower layer specifications define the layer 1, 2, and 3 requirements of an ISDN. Network signalling, via the D-channel, is the focus of these agreements but, where appropriate, user data specifications of layers 1, 2, and 3 have been included. These IAs were developed in the Signalling Expert Working Group (SWG) of the IIW. These IAs provide a framework and a set of protocol procedures for accessing an ISDN, so that systems implemented according to these agreements can successfully interoperate. The following text details the ISDN lower layer IAs.

4.1.1 Layer 1 Basic Rate Interface (BRI)

The ISDN Basic Rate Interface (BRI) physical layer specifications are defined for their specific reference point of application. These reference points are S, T and U, providing the user and network interfaces for Terminal Equipment (TE) and Network Termination (NT) equipments. The following IAs are defined for the BRI physical layer.

4.1.1.1 U Reference Point

The American National Standard T1.601-1992, *Integrated Services Digital Network (ISDN) - Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT (Layer 1 Specification)* (Ref. [12]), is an interface standard specifying the minimal set of requirements for satisfactory transmission between the network and the NT. Its application is at the U reference point of the Basic Access Interface.

This IA adopts the ANSI T1.601-1992 specification (Ref. [12]) without exception.

NOTE: The ANSI T1.601-1992 is a revision to the previous ANSI T1.601-1988. NIUF 89-101 references T1.601-1988. This IA revises NIUF 89-101 to implement the revised ANSI T1.601-1992. Appendix J of T1.601-1992 details the changes from T1.601-1988 and hence the changes from NIUF 89-101.

4.1.1.2 S and T Reference Points

The American National Standard T1.605-1991, *Integrated Services Digital Network (ISDN) - Basic Access Interface for S and T Reference Points (Layer 1 Specification)* (Ref. [16]), is an interface standard specifying the minimal set of requirements for satisfactory transmission between the NT and the TE. Its application is at the S and T reference points of the Basic Access Interface.

This IA adopts the ANSI T1.605-1991 specification (Ref. [16]) without exception.

---

[4]The NIUF Plenary document numbers (e.g., NIUF 89-101) are included for reference purposes only, as every numbered implementation agreement is included in the present document in its entirety.

NOTE: The ANSI T1.605-1991 is a revision to the previous ANSI T1.605-1989. NIUF 89-105 references T1.605-1989. This IA revises NIUF 89-105 to implement the revised ANSI T1.605-1991. Appendix M of T1.605-1991 details the changes from T1.605-1989 and hence the changes from NIUF 89-105.

4.1.2 Layer 1 Primary Rate Interface (PRI)

The ISDN Primary Rate Interface (PRI) physical layer specifications are defined for the S, T, and U reference points. These reference points provide the user and network interfaces for TE and NT equipments. The following IA is defined for the PRI physical layer.

4.1.2.1 S, T, and U Reference Points

The IA *Primary Rate Customer Installation Metallic Interfaces, Layer 1 Specification* (NIUF 89-103R1) states: "The physical layer of the Primary Access Interface is specified by ANS T1.408-1990, *ISDN Primary Rate—Customer Installation Metallic Interfaces, Layer 1 Specification*, (Ref. [11]).

This IA applies to the Primary Rate S, T, and U reference points.

This IA adopts ANS T1.408-1990 (Ref. [11]) without exception."

NOTE: Previous revisions of this IA were based upon the ANS T1.403-1989 (Ref. [10]), (the DS1 specification) and can be found in NIST Special Publication 500-195, *North American ISDN Users' Forum Agreements on ISDN* (Ref. [53]).

4.1.3 Layer 2 BRI and PRI

The ISDN Basic Rate Interface (BRI) and Primary Rate Interface (PRI) access arrangements specify one common IA for the D-channel layer 2 data link.

The IA *Data Link Layer Signalling Specification for Application at the User-Network Interface* (NIUF 89-210) states: "The data link layer of the D-channel is specified in ANS T1.602-1989, *ISDN Data Link Layer Signalling Specification for Application at the User-Network Interface*, (Ref. [13]).

This IA adopts ANS T1.602-1989 (Ref. [13]) with the following, additional clarifications:

1) Both automatic and non-automatic Terminal Endpoint Identifier (TEI) assignment terminals shall be allowed to connect to a passive bus. Automatic TEI assignments are preferred, since it would be the responsibility of the user to ensure that different TEIs are used by each different terminal for non-automatic TEI allocation equipment.

2) It is recommended that the data link monitor function be operated on at least one link associated with each TEI."

4.1.4 Layer 3 BRI and PRI

The ISDN BRI and PRI access arrangements will utilize the layer 3 Signalling protocol as defined by ANS T1.607-1990, ANS T1.608-1991 and ANS T1.610-1990 (Refs. [17, 18, 20]). These specifications apply to two distinct connection types: circuit-switched and packet-switched. The following text details the IAs for ISDN layer 3 signalling.

4.1.4.1 Circuit-Switched Call Control Procedures

The circuit-switched layer 3 signalling protocol shall be responsible for the establishment, maintenance and tear-down of basic signalling connections and supplementary service signalling connections which utilize circuit-switched access. The following text details the circuit-switched call control procedures.

4.1.4.1.1 Basic Call Control Procedures

The IAs (NIUF 300 Series) for the ISDN Basic Call Control procedures state: the circuit-switched network layer protocol is specified in the ANS T1.607-1990, *Digital Subscriber Signalling System No. 1 (DSS1)—ISDN Layer 3 Signalling Specification for Circuit-Switched Bearer Service*, (Ref. [17]).

The IAs have adopted ANS T1.607-1990 (Ref. [17]), according to the implementation configurations, as follows:

- Class I BRI (*IB*)

The Class I BRI (*IB*) basic call control signalling IA *Layer 3 Signalling Specification for the Minimal Set of Circuit-Switched Bearer Services for the ISDN Basic Rate Interface/Class I* is included in Appendix A.

- Future Class I PRI (*IP*)

Editor's Note: This section is reserved for future agreements on Class I PRI (*IP*) basic call control signalling.

- Future Class II BRI (*IIB*)

Editor's Note: This section is reserved for future agreements on Class II BRI (*IIB*) basic call control signalling.

- Class II PRI (*IIP*)

The Class II PRI (*IIP*) basic call control signalling IA *Layer 3 Signalling Specification for the Minimal Set of Circuit-Switched Bearer Services for the ISDN Primary Rate Interface/Class II* is included in Appendix B.

4.1.4.1.2 Supplementary Services Control Procedures

The IAs (NIUF 310 Series) for the ISDN Supplementary Services Control procedures are based upon ANS T1.610-1990, *Digital Subscriber Signalling System No. 1 (DSS1)—Generic Procedures for the Control of ISDN Supplementary Services*, (Ref. [20]). The following text details the IAs.

• Class I BRI (*IB*)

The IA (NIUF 89-311) for the Class I BRI (*IB*) Supplementary Services Control procedures states: The generic procedures for the control of ISDN Supplementary Services for Class I equipment on a Basic Rate Interface (BRI) is specified in ANS T1.610-1990 (Ref. [20]).

The following changes shall apply to the ANS T1.610-1990 (Ref. [20]) specification:

1. In section 4, the Keypad protocol only applies during the establishment phase of a call;
2. In section 5.2.2.1, the option of using the dummy call reference for sending a call-associated feature request is removed.
3. In section 2.1.3, section 6, and Appendix I, the Common Information Element Category of the Functional Protocol is removed;
4. In section 7, the FACILITY and REGISTER messages are removed;
5. In section 8, the Facility information element is removed;
6. In Annex A, the Terminal Identification procedures for assignment of USID and TID at subscription time are removed;
7. In Annex B, section 2.1, the words "in the Called party number information element in one or more INFORMATION messages" should be changed to "in the Called party number information element in one INFORMATION message";
8. Remove Appendix III General Description of Component Encoding Rules.
9. The scope of this implementation agreements is applicable only to the ISDN Basic Access Rate as applied to Class I equipment.

• Future Class I PRI (*IP*)

Editor's Note: This section is reserved for future agreements on Class I PRI (*IP*) Supplementary Services Control procedures.

• Future Class II BRI (*IIB*)

Editor's Note: This section is reserved for future agreements on Class II BRI (*IIB*) Supplementary Services Control procedures.

• Future Class II PRI (*IIP*)

Editor's Note: This section is reserved for future agreements on Class II PRI (*IIP*) Supplementary Services Control procedures.

4.1.4.2 Packet-Switched Call Control Procedures

The Lower Layer Special Interest Group (LLSIG), of the OIW, has the responsibility of developing the IAs for packet-switched connections. Their work overlaps with the packet-switched services provided by an ISDN. Therefore, the SWG has the responsibility to review the LLSIG's IAs and provide to the LLSIG any additional information/clarification necessary to align these IAs with those defining the ISDN.

The packet-switched layer 3 signalling protocol shall be responsible for the establishment, maintenance and tear-down of basic signalling connections and supplementary service signalling connections which utilize packet-switched access. The following text details the packet-switched call control procedures.

The IA (NIUF 89-320) for the ISDN Basic Call Control procedures states: the packet-switched network layer protocol is specified in the CCITT Recommendation Q.931-1988 (also designated CCITT Recommendation I.451-1988), *ISDN User-Network Interface Layer 3 Specification*, (Ref. [26]).

The following agreements have been reached concerning the use of CCITT Recommendation Q.931-1988, (Ref. [26]):

1. On a BRI supporting the ISDN virtual circuit service, all of CCITT Recommendation Q.931-1988 (Ref. [26]) section 6, except for 6.1.1 and 6.2.1 (the sections covering the circuit-switched access case), shall apply. The following sections also apply; 3.2 (messages for packet-mode access connection control), 4-4.5 (section specifying general information element handling and encoding), 4.7 (information elements for packet communications).

2. On a PRI supporting the ISDN virtual circuit service all of Q.931-1988 (Ref. [26]) section 6, except for 6.1.1 and 6.2.1 (the sections covering the circuit-switched access case), 6.1.2.2, 6.2.2.2 and 6.4.2 (the sections specifying the D-channel ISDN virtual circuit service case), shall apply. The following sections also apply: 2.2 (packet-mode access connection states), 3.2 (messages for packet-mode access connection control), 4-4.5 (section specifying general information element handling and encoding), 4.7 (information elements for packet communications).

3. On a BRI or PRI supporting the Unrestricted 64 kbps circuit-mode service, CCITT Recommendation Q.931-1988 (Ref. [26]) sections 6.1.1, 6.2.1, 6.4.1 and 6.4.3 shall apply. The following sections also apply: 2.1 (circuit-mode connection states), 3.1 (messages for circuit-mode connection control), 4-4.5 (section specifying general information element handling and encoding).

4.2 Future Basic Bearer Services Specification

The ISDN basic bearer services specifications define the minimal set of bearer services provided by an ISDN. The specifications outline the set of essential bearer services, and their attributes, to be provided by an ISDN. The IAs developed for the bearer services will provide a specification outlining the required bearer services and their respective characteristics. The following text will detail the ISDN basic bearer services IAs.

4.2.1 Future Minimal Set of BRI Services

Editor's Note: This section is reserved for future agreements on the minimal set of ISDN Basic Rate Interface (BRI) bearer services (Refs. [15], [30, 31]).

4.2.2 Future Minimal Set of PRI Services

Editor's Note: This section is reserved for future agreements on the minimal set of ISDN Primary Rate Interface (PRI) bearer services (Refs. [14], [30, 31]).

4.3 Future Supplementary Services Specification

Editor's Note: This section is reserved for future agreements on the ISDN supplementary services specifications (Ref. [20]).

4.4 ISDN Terminal Adaptation Specification

The ISDN Terminal Adaptation specifications define the requirements for attaching a non-ISDN terminal to an ISDN. This attachment is performed across the R reference point, with the specification of the R reference point providing the necessary characteristics, attributes and functions such that successful interoperability between the non-ISDN and the ISDN is achieved. The IAs developed for terminal adaptation provide a specification of the R reference point requirements. The following text details the ISDN terminal adaptation IAs.

4.4.1 Circuit-Mode Data Terminal Adaptation

The Circuit-Mode Data Terminal Adaption IAs define the R reference point requirements when circuit-switched connections are provided by an ISDN. The IAs were developed in the Terminal Adaption Expert Working Group of the IIW.

The IA (NIUF 91-001) for the circuit-mode terminal adapter states: the following agreements are made with respect to ANS T1.612-1990 (Ref. [21]). ANS T1.612 is based upon the CCITT Recommendation V.120, (Ref. [27]).

- Terminal Adapters shall support the use of the Low Layer Compatibility Information Element (LLC). The calling TA will be capable of including the LLC in the SETUP MESSAGE.

  If the called TA does not receive the LLC, it shall attempt to operate in accordance with user-established parameter values.

- Since link verification is not mandatory in Unacknowledged Information Transfer Mode, Terminal Adapters supporting but not requiring link verification must be able to proceed with operation in the event that they can not verify the link.

  For Category I devices, the default operation shall be to attempt link verification, and enter the data transfer phase if link verification is unsuccessful.

  For Category II devices, the default operation shall be to attempt link verification for I-Frame mode. If Link verification fails, the device shall fall back to Unnumbered Information (UI) frame mode and attempt link verification. If that verification fails, the device shall move to the data transfer phase.

- V.120 terminal adapters should not resend the last I-frame transmitted as a poll upon expiry of T200 (although they must respond appropriately if they receive an I-frame poll).

- For each V.120 mode of operation (from among Asynchronous Mode, Synchronous Mode, and Bit Transparent Mode) supported by a particular V.120 terminal adapter, the terminal adapter shall belong to one of two categories of equipment:

  - Category I equipment which supports unacknowledged information transfer only.

  - Category II equipment supports both unacknowledged information transfer and acknowledged information transfer.

A Category I terminal adapter must support the V.120 protocol, so that it must respond appropriately to an attempt by its peer to establish multiple frame operation. Category I equipment must respond to a received Set Asynchronous Balanced Mode Extended (SABME) with a Disconnected Mode (DM) with F bit matching the value of the P bit in the received SABME (which should be "1").

The default action for Category II equipment that receives a DM in response to a transmitted SABME should be to fall back to unacknowledged information transfer. It is permissible to provide the user the ability to configure the terminal adapter to take actions other than the default in this circumstance, e.g., resending the SABME, or releasing the call.

4.4.2 Packet-Mode Data Terminal Adaptation

The packet-mode data terminal adaptation IAs define the aspects of the packet-mode services to be used by the packet-mode Data Terminating Equipment (DTE), the access requirements, and the functions of the Terminal Adapter provided across the R reference point. These IAs were developed in the LLSIG of the OSI Implementors' Workshop. Refer to the NIST OSI Implementors' Workshop *Stable Implementation Agreements for OSI Protocols* (Ref. [54]), section 7.

4.5 ISDN Management Specification

The ISDN Management specifications provide the operations and maintenance requirements for the various access interfaces and protocol levels of the ISDN. The IAs are to be developed in the Network Management Expert Working Group (NMWG) of the IIW. The following text details the ISDN Management IAs.

4.5.1 Future Layer 1 BRI

Editor's Note: This section is reserved for future agreements on layer 1 ISDN management specification, for a Basic Rate Interface (BRI) (Ref. [7]).

4.5.2 Future Layer 1 PRI

Editor's Note: This section is reserved for future agreements on layer 1 ISDN management specification, for a Primary Rate Interface (PRI) (Ref. [8]).

4.5.3 Future Layer 2 and 3, BRI and PRI

Editor's Note: This section is reserved for future agreements on layer 2 and 3 ISDN management specification, for a Basic Rate Interface (BRI) and a Primary Rate Interface (PRI) (Ref. [9]).

4.6 Future Common Channel Signalling—Signalling System #7

Editor's Note: This section is reserved for future agreements on common channel signalling system, ANSI Signalling System #7 (Refs. [1, 2, 3, 4, 5, 6, 19]).

4.7 ISDN Security Architecture

4.7.1 Introduction

The ISDN Security Expert Group (ISEG) of the North American ISDN Users' Forum (NIUF) has proposed a suite of ISDN Security Services based on the security services defined in ISO 7498-2 (Ref. [57]). The ISDN Security Services expand upon the suite of OSI Security Services to address the unique aspects of ISDN. Each of the ISDN Security Services has a service definition and service description which explain the service. The relationships of each security service to the other ISDN security services, and to their OSI counterparts, are also addressed. Finally, candidate mechanisms for achieving each service, as well as practical examples of each service and its application are discussed for each service.

4.7.1.1 Relationship of Secure ISDN Services to ISDN Services

ISDN is frequently described in terms of services provided. ISDN standards encompass three categories of services: Bearer Services, Teleservices, and Supplementary Services. Bearer Services are those normally provided by the lower three layers (1, 2, & 3) of the OSI Reference Model. Teleservices build upon the Bearer Services, and encompass all seven layers of the OSI Reference Model. Supplementary Services supply additional functionality to Teleservices and/or Bearer Services, such as advice of charge, call forwarding, etc., and therefore cannot stand alone without the other service categories. Figure 4-1 illustrates the interrelationships of ISDN Services.

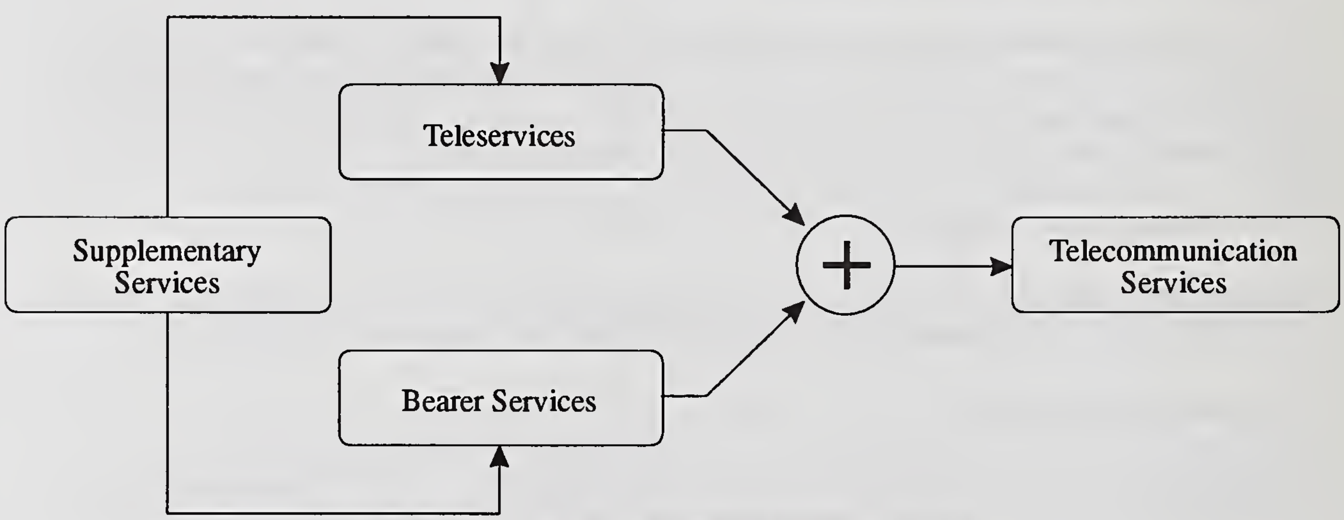


Figure 4-1. ISDN Telecommunication Services.

Secure ISDN Services: A Secure ISDN Service is a combination of Teleservices and/or Bearer Services appropriately modified by Supplementary Services, if needed, and Security Supplementary Services, as shown in figure 4-2. An ISDN Security Supplementary Service cannot stand alone without an ISDN Teleservice and/or Bearer Service. The Security Services defined by the ISEG are considered a subset of ISDN Supplementary Services. ISDN Security Supplementary Services map to one or more layers of the OSI Reference Model. A supplementary security service is normally realized by augmenting an ISDN Service's (Circuit Switched Voice (CSV), Packet Switched Data (PSD), etc.) component services (Bearer Service, Teleservice, and Supplementary Services, if required) with one or more ISDN Security Supplementary Services. For example, an

ISDN Teleservice of Teletex would become Secure Teletex with the addition of the appropriate ISDN Security Supplementary Services.

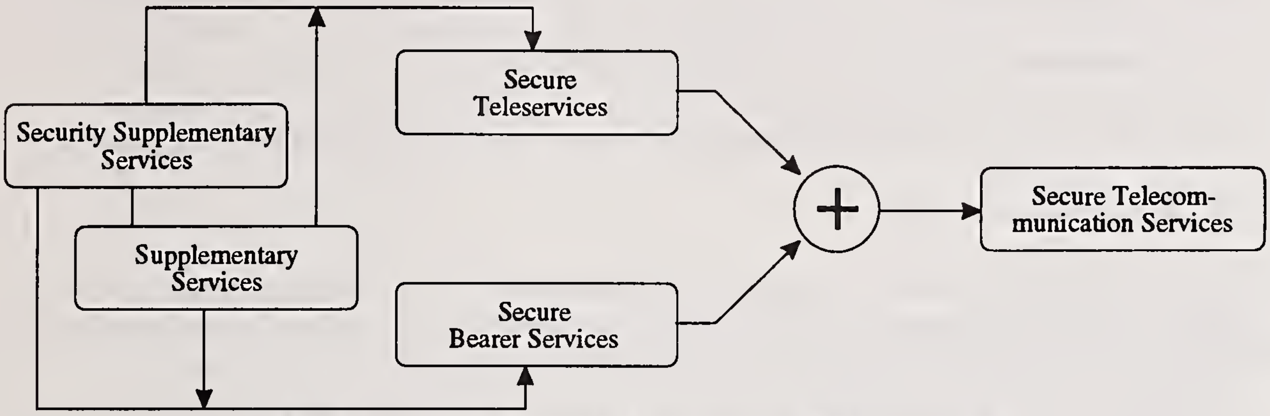


Figure 4-2. ISDN Secure Telecommunications Services.

It is intended that appropriate addenda to CCITT (Q.931 (Ref. [26]) and Q.932 (Ref. [20])) and ANSI standards be drafted to describe the message formats for requesting ISDN Security Supplementary Services. Secure ISDN Services will be defined in NIUF Application Profiles which will, *inter alia*, specify the ISDN Security Supplementary Services required for each specific Secure ISDN Service.

4.7.1.2 Scope of the ISDN Security Architecture

Security Architecture defines security services which ISDN subscriber entities, directly attached to the network, may request. These entities include the various physical and logical configurations that form the network access configuration. The security architecture provides security services for the resources and information within and directly attached to network access points. The security architecture does not address any other entities that exist behind the direct network access points. The security services embrace all communication services including voice, data, video, etc.

This document is not intended to levy minimum security requirements on any network component or implementor. It is intended, rather, to be used as a guideline for implementing security services and related mechanisms in ISDN.

4.7.1.3 Services, Mechanisms and Mappings

This document also provides guidance on candidate placement of these security services within ISDN protocol layers, as well as at appropriate ISDN access points where the security service requests may originate. Scope examples may include confidentiality requested at access point 3 and provided at Level 1 in a NT1 or at Levels 2 and 3 for the Basic Rate Interface. Another example is a provision for a non-repudiation service which may be requested at access point 5 and provided as a Layer 7 service. These candidate placements will be discussed later.

4.7.2 Service Descriptions

4.7.2.1 Authentication

4.7.2.1.1 Definition

Authentication is proof of identity exchanged between entities involved in telecommunications.

4.7.2.1.2 Service Description

ISO 7498-2 (Ref. [57]) defines two types of authentication. They are data origin authentication and (peer) entity authentication. The first proves the identity of the origin of a data item. The second proves the identity of communicating entities.

ISO 7498-2 (Ref. [57]) considers an entity to be a protocol entity, that is, an Nth layer of the 7 layer OSI model. Entities can also be users, and more generally subjects or objects. ISDN specifies two additional kinds of authentication, namely, user (subject)-to-user (object), and user (subject)-to-network (object). The intent of user-to-user authentication is to move the authentication closer to the human user than in the ISO definitions. User-to-network authentication provides for the user and the network to authenticate one another.

4.7.2.1.3 Relationship to Other Security Services

ISDN Authentication services identify a system or network entity to other entities for the purpose of requesting access. Appropriate entity authentication information assures that a stated identification is correct (authentication), and limits system or network facilities and services available to the correctly identified entity based on its identification and access control information. The specific entities of concern include communities, subscriber hosts, or local distribution systems, as well as processes, individuals, and generators of system control traffic. Both objects and subjects may be identified and authenticated. Access control governs the access of objects by subjects.

For the purposes of the security service definitions, the word "object" is used to denote any passive entity that contains or receives information, as well as an active entity which provides a service or resource. Access to an object implies access to the information it contains or its services. Similarly, the word "subject" is used to denote an active entity (i.e., an application) that acts on objects; it is a process that serves as a direct surrogate for a user, or an (internal) subject that provides services for other processes. Thus a subject takes the role of an object if its services or resources are requested from another subject.

4.7.2.1.4 Relationship to ISO and ISDN

This relationship is given in the ISDN Security Services and Functional Interface Table (ISSFIT), table 4-1.

4.7.2.1.5 Candidate Mechanisms

Candidate mechanisms for Authentication include encipherment, digital signature, and password. Bio-metric forms of Authentication could also be applied in Authentication implementations.

4.7.2.1.6 Practical Examples of Application

Practical examples include electronic messaging systems, electronic funds transfer, and document registration. In a secure E-mail system, for example, a user would authenticate himself to the network, and then would, in turn, be authenticated to the mail service. The recipient would do the same two-stage process to retrieve a message. The two-stage process may be achieved in one step if the Authentication service were provided by the ISDN.

4.7.2.2 Access Control

4.7.2.2.1 Definition

Access Control is the security service by which the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner, is provided.

4.7.2.2.2 Service Description

Access Control is a service that is concerned with prevention of unauthorized use of network and network access resources. Access Control can be used to provide protection at various levels of granularity to these resources (target). This service may require a secure exchange of access control information (ACI). ACI is information that is needed by the network and/or end system to perform basic control for access, such as granting or denying an access request. ACI is based on policy rules and access profiles associated with a particular entity, as well as authentication information provided by that entity. The basic framework used is that a user (i.e., person, process), represented by a user delegate, is requesting access to a particular resource (user delegate and resources acting as a target are roles that are assumed by various entities in a given access control service instance). Control of access can be governed by a variety of criteria, for example, factors such as time of attempted access, location of the accessor or route of access. In addition, control of access has to be timely and reactive to changes in authorization during access.

There are a number of activities that must occur to realize Access Control.

- The security policy has to be translated to rules that form the basis for access control decision.

- The ACI structure has to be established to form the template for acceptable ACI values.

- The ACI has to be disseminated to the customer premise equipment (e.g., TEs, NT2) and to the network to control subscriber access through the network interface.

- ACI and the access decision functions must be bound to the location of these elements or by some sealing process.

- There have to be provisions to be able to modify the ACI after it has been distributed to various entities.

- The capability must exist to be able to revoke the ACI. This can be done to impact current or future accesses of the initiator.

The basic entities and functions involved in Access Control are the initiator (subject), the initiator authentication information (IAI), the Access Control enforcement function (AEF), the Access

Control decision function (ADF), and the target (object/resource). This is illustrated in figure 4-3. The AEF is responsible for ensuring that any actions by the initiator on the target have been determined by the ADF to be proper. When the initiator makes a request to perform a particular action on the target, the AEF informs the ADF that a decision is required so that a determination can be made. In order to perform this decision, the ADF is provided with relevant ACI.

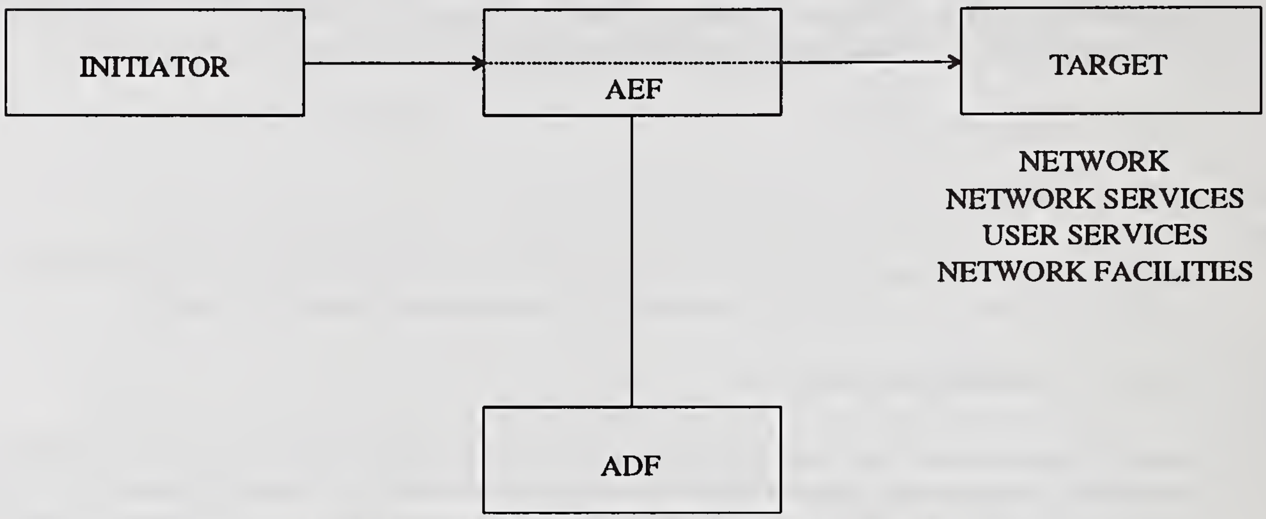


Figure 4-3. Fundamental Access Control Functions.

4.7.2.2.3 Relationship to Other Security Services

There are two kinds of interactions that can be identified: other security services that can be used to support an Access Control service, and Access Control mechanisms that can be used to support other security services. For Authentication, an authenticated identity is used as input into the access control process.

The Information Integrity service is used to preserve the integrity of inputs and outputs within and between Access Control components. Some Access Control inputs and outputs may be considered sensitive and may need to be protected by the Information Confidentiality service. The Access Control service provides protection for the other security services and their associated components by limiting access. In addition, Access Control generates a violation which is one source for the detection of Denial of Service.

4.7.2.2.4 Relationship to ISO and ISDN

Access Control has a direct application to ISDN. There are critical equipment, user and network information and network services that need to be protected from unauthorized access. Access control mechanisms will need to reside in many places in ISDN to provide the appropriate level of control.

The Access Control service will need to protect the ISDN network, network services, user services and network facilities. This is illustrated in figure 4-3. Access Control and its associated components may be provided at the various reference points (i.e., R, S, T, U) in the basic architectural model (see fig. 4-4). Any network and user services provided in the network environment needs to be protected from unauthorized use. In addition, any network facilities employed by the network needs to be protected to maintain functionality and performance of the network.

Table 4-1. ISDN Security Services and Functional Interface Table

SERVICE	ISO/OSI LAYER	ACCESS POINT	ISDN LAYER[1] B	ISDN LAYER[1] D
1) AUTHENTICATION				
a) Peer Entity	3,4,7	2,3,4,5	3[4,7][1]	2,3
b) Data Origin	3,4,7	1,2,3,4,5	3	2,3
c) User-to-User	7[2]	2,3,4,5	-	-
d) User-to-Network	-	1,2,3,4,5	3	3
2) ACCESS CONTROL				
a) ISDN (Network)	-	0[1],1,2,3,4,5	2	2,3
b) Network Services	-	2,3,4,5	3	3
c) User Services	-	2,3,4,5	3	3
d) Network Facilities	-	0[1],1,2,3,4,5	3	3
3) INFORMATION CONFIDENTIALITY				
a) Connection	1,2,3,4,6,7	0[1],1,2,3,4,5	1,2,3	1,2,3
b) Connectionless	2,3,4,6,7	1,2,3,4,5	-	1,2,3
c) Selective Field	6,7	2	-	2
d) Traffic Flow	1,3,7	0[1],1,2,4	1,2,3	1,2
4) INFORMATION INTEGRITY				[4,7][1]
a) Connection with Recovery	4,7	1,2,4	1	3
b) Connection without Recovery	3,4,7	1,2,4	1	2
c) Selective Field Connection	7	2	-	2,3
d) Connectionless	3,4,7	2,4	-	2,3
e) Selective Field Connectionless	-	2	-	
5) NON-REPUDIATION				
a) With Proof of Origin	7	3,5	[7][1]	[7][1]
b) With Proof of Delivery	7	3,5	[7][1]	[7][1]
6) SERVICE ASSURANCE				
a) Detection/Notification of Availability	-	0[1],2,3,4,5	3[7][1]	3[7][1]
b) Availability Alternatives (Routing)	-	1,2,4	3[7][1]	3[7][1]
7) NOTARIZATION	7	3,5	-	-

[1]not specified in ISDN
[2]not specified in OSI

Source: NIUF Implementors' Security Expert Group, rev. 7-91.

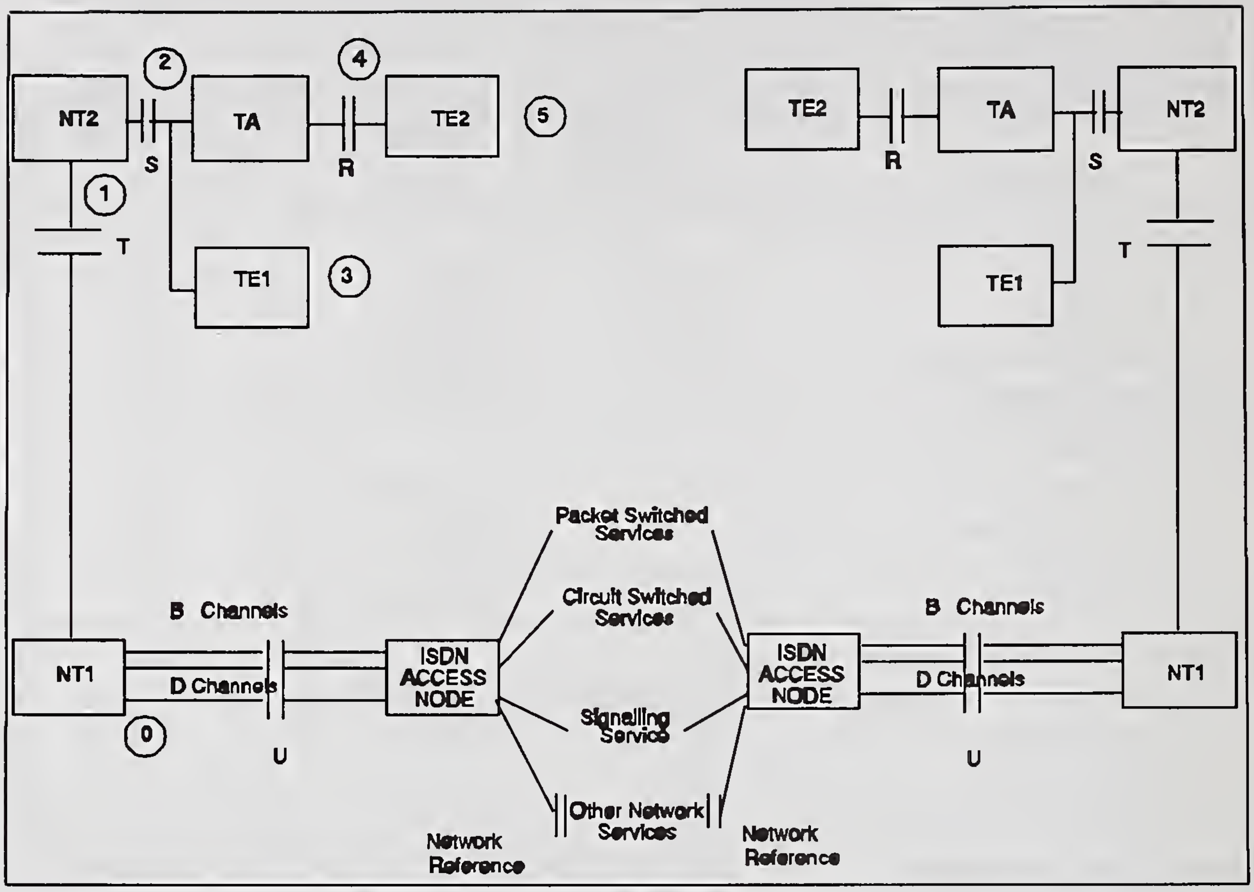


Figure 4-4. ISDN Security Services and Functional Interface.

There will be local access of resources in one domain that needs to be controlled by the service. Remote access of resources in other domains will also be required. Multiple domains may be involved, but in many instances not all will be distinct. Some of these domains may contribute ACI, some may exercise control over an access, and some may do both.

4.7.2.2.5 Candidate Mechanisms

There are many mechanisms that can be used for Access Control. They include such techniques as access control lists, capabilities and security labels.

4.7.2.2.6 Practical Examples of Applications

When a network user requests a service (e.g., e-mail, electronic messaging), a decision needs to be made to determine if the user is authorized to invoke the service. This checking, using the authenticated user identifier, occurs before the service is actually invoked. In allowing or denying access to a service, other context information (e.g., time of access) may be factored into the decision process.

4.7.2.3 Information Confidentiality

4.7.2.3.1 Definition

The security service by which one ensures that only the individual(s) for whom information is intended can gain knowledge of a telecommunication.

4.7.2.3.2 Service Description

Information Confidentiality is a service by which parties to an exchange of information ensure that only they know the contents of their telecommunications, i.e., this service ensures that no unauthorized third party is able to gain any knowledge of the contents of the telecommunication. There are four significant categories of confidentiality which are pertinent to this discussion.

4.7.2.3.2.1 Connection-oriented Confidentiality

This provides protection of all information exchanged via connection-oriented transmission media.

4.7.2.3.2.2 Connectionless Confidentiality

This provides protection of all information exchanged via connectionless transmission media.

4.7.2.3.2.3 Selective Field Confidentiality

This service provides protection for only selected portions of packetized information transmitted via connection-oriented or connectionless media.

4.7.2.3.2.4 Traffic Flow Confidentiality

This service includes confidentiality not only of the contents of a transmission, but also extends to denying the unauthorized individual any knowledge that a transmission is taking place.

This service also includes protection deriving against unauthorized individuals knowledge about telecommunications from observation of traffic flows, regardless of traffic content.

This service is directly associated with the Information Confidentiality discussed in the ISO 7498-2 Security Architecture (Ref. [57]). For application purposes, the functional descriptions found therein and above are interchangeable.

4.7.2.3.3 Relationship to Other Security Services

Information Confidentiality is logically associated with a number of other security services, especially when packaged in a potential service offering. For instance, packaging a private contract exchange service might be popular. It might contain a bundling of integrity, confidentiality, non-repudiation, and notarization to enhance and augment value to the ISDN customer.

4.7.2.3.4 Relationship to ISO and ISDN

The nature of ISDN confidentiality is perhaps more wide-ranging than its counterpart in OSI, since circuit-switched, high speed information transfer is fundamental to ISDN, such that connection-oriented confidentiality is more likely to be needed on a regular basis.

4.7.2.3.5 Candidate Mechanisms

These include, but are not limited to, encryption/encipherment, transmission medium restriction, and encoding.

4.7.2.3.6 Practical Examples of Applications

These are many and varied. Good examples include exchange of proprietary information via a physically protected transmission system, and encipherment of information prior to transmission over the public network.

4.7.2.4 Information Integrity

4.7.2.4.1 Definition

The security service which ensures that information is neither altered nor destroyed in an unauthorized manner.

4.7.2.4.2 Service Description

Information Integrity is the service by which parties to an information exchange ensure that the contents of the exchange are transmitted and delivered without unauthorized modification.

4.7.2.4.2.1 Connection-Oriented with Recovery

Information Integrity applied to information exchanged via a connection oriented transmission path with recovery of information attempted, if the exchange is interrupted.

Note: For the purpose of this document, "interrupted" includes, but is not limited to, loss of transmission path, alteration of information or loss of information.

4.7.2.4.2.2 Connection-Oriented without Recovery

Information Integrity applied to information exchanged via a connection-oriented transmission, with no attempt at information recovery in the event of interruption of the exchange.

4.7.2.4.2.3 Selective Field Connection-Oriented

Information Integrity applied only to certain fields within a unit of user information.

4.7.2.4.2.4 Connectionless-Oriented Integrity

Information Integrity applied to information exchanged via connectionless-oriented transmission.

4.7.2.4.2.5 Selective Field Connectionless-Oriented Integrity

Information Integrity applied only to certain fields within a unit of user information exchanged via connectionless-oriented transmission.

4.7.2.4.3 Relationship to Other Security Services

The Integrity service is one of the few services which could provide value to the user without combination with other services. It may also be valuable in bundled provisions.

4.7.2.4.4 Relationship to ISO and ISDN

This service is directly related to the OSI security service of data integrity, but is intended to encompass a wider range of information types.

The relationship to ISDN is that ISDN subscribers need the ability to exchange information through the network between subscriber entities with the assurance that the information is intact.

4.7.2.4.5 Candidate Mechanisms

Candidate mechanisms include cryptographic checksums, encryption algorithms and redundant transmission.

4.7.2.4.6 Practical Examples of Applications

Practical applications include Electronic Funds Transfer, message service, contract exchange, and military command, control and communication.

4.7.2.5 Non-Repudiation

4.7.2.5.1 Definition

Repudiation is the denial by one of the entities involved in an exchange of information of having participated in all or part of the exchange. Non-Repudiation provides proof of the integrity of an exchange (not the content) with a guarantee of transmission (origin) and delivery.

4.7.2.5.2 Service Description

Per ISO 7498-2 definition (Ref. [57]), there are two types of Non-Repudiation services: non-repudiation with proof of origin, and non-repudiation with proof of delivery. The former refers to the service that the recipient of information is provided with proof of the origin of the information. This will protect against any attempt by the sender to falsely deny sending the information. The latter refers to the service that the sender of the information is provided with proof of delivery of the information. This will protect against any attempt by the recipient to falsely deny receiving the information. Traditionally, Non-Repudiation service for information is the responsibility of the subscriber systems that attach to the network. ISDN backbones may, however, offer Non-Repudiation services and provide any special support for them. The request for Non-Repudiation services are a subscriber's responsibility. There is a need to define ISDN standards for these services or to adopt emerging Non-Repudiation service standards for an ISDN environment.

4.7.2.5.3 Relationship to Other Security Services

In general, Non-Repudiation service uses the Information Integrity service to support its proper operation. The Information Integrity service can be used to preserve the integrity of the information content while the message is in transit in the network. However, if Non-Repudiation is provided by a notarization mechanism, then Data Authentication service, Data Confidentiality service, as well as Data Integrity service may be needed to establish a protected connection with the notarization entity. Non-Repudiation service is most useful for applications at end-user systems. Therefore, it is very rarely that Non-Repudiation service is used to support other security services.

4.7.2.5.4 Relationship to ISO and ISDN

Non-Repudiation is considered an ISO Layer 7 security service. Non-Repudiation service also has a direct application to ISDN. Many applications at the ISDN user areas would require Non-Repudiation service to support their proper operation. Since the Non-Repudiation service is only significant to human end-users, it is logical to provide this security service at the end-systems subscriber access points 3 and 5 (or at the reference points R and S) in the basic ISDN architecture model.

4.7.2.5.5 Candidate Mechanisms

The mechanisms that can be used to provide Non-repudiation service including Digital Signature, Data Integrity, and Notarization mechanisms. The Digital Signature mechanism referred in the ISO 7498-2 (Ref. [57]) is a true signature scheme. In a true signature scheme, signed messages produced by the sender are transmitted directly to the receiver, who verifies their validity and authenticity without the need of a trusted third party. The Notarization mechanism referred in the ISO 7498-2 (Ref. [57]) is an arbitrated signature scheme. In an arbitrated signature scheme, all signed messages are transmitted from the sender to the receiver via an arbitrator who serves as a witness. The Data Integrity service is often used to protect against tampering and the integrity of the information exchange to implement the Non-Repudiation service.

4.7.2.5.6 Practical Examples of Applications

There are numerous examples where non-repudiation of services would be useful for applications at the user areas. The examples include business transactions (e.g., between a brokerage house and its clients) and military orders (e.g., between a commander and his troops,) as well as a variety of cases involving contracts or agreements between people and institutions (e.g., between a home buyer and the settlement agency). Generally speaking, non-repudiation service would be required by the communicating parties if the proof of origin or delivery of information is important to resolve the possible legal disputes afterwards about the sending/receiving of information.

4.7.2.6 Assurance As A Security Service

4.7.2.6.1 OSI Assurance

Relationship to OSI Security Addendum (see Ref. [57], Annex A—Background Information on Security in OSI, Subsection A.1.5.4—Denial of Service). Denial of Service occurs when an entity fails to perform its proper function or acts in a way that prevents other attacks. It may be general, as when an entity suppresses all messages, or there may be a specific target, as when an entity suppresses all messages directed to a particular destination, such as security audit service. The attack may involve suppressing traffic as described in this example or it may generate extra traffic. It is also possible to generate messages intended to disrupt the operation of the network, especially if the network has relay entities that make routing decisions based upon status reports received from other relay entities.

4.7.2.6.2 ISDN Assurance

The ISDN security Service of Assurance (IAS) is used to protect a user from the threat of denial of services. The IAS has two possible conditions. The first condition is when the IAS is used as a response to an entity failure, but does not result in denial of a particular service to the user. The failure can be considered a security threat to the user application even though the service may have been backed-up. The second condition is when IAS occurs because an entity is denied to the user. Here the user is deprived of all services provided by a particular entity (network, etc).

Common actions are taken whether or not services are denied to the user. When an IAS occurs, the network reports the event. When IAS-without-denial-of-service occurs, it is reported as a non-critical alarm. The alarm may be based on a threshold number of logged IAS events. When IAS-with-denial-of-service occurs, it is reported as a critical alarm.

4.7.2.6.2.1 Common IAS Actions

The common IAS actions are taken whether or not service is denied to the user. Whenever an IAS condition occurs, the Network Manager (NM) Managed Object (MO) or entity reports to the Configuration Manager (CM) the event for logging purposes only. The CM in turn reports to the Security Manager (SM) after some threshold defined number of IAS events. The SM will have access to the NM CM log to determine a response.

4.7.2.6.2.2 IAS Without Denial of Service

When this condition occurs, the NM CM reports the condition to the CM as an alarm based on a threshold defined number of logged IAS events. The IAS threshold used to report the IAS events will be less than the threshold used to report events to the SM under the common IAS actions. The IAS events will be reported to the SM as a non-critical alarm.

4.7.2.6.2.3 IAS With Denial of Service

When this condition occurs the CM will log the IAS condition as a failure with the Fault Manager (FM) and the FM will generate a trouble ticket. The NM CM also reports the condition to the FM as a failure. The IAS condition will also be reported by the CM to the SM as a critical security event.

4.7.2.6.3 Relationship to Other Security Services

Uses the security service of Audit as a mechanism to warn users when expected services are not delivered.

4.7.2.6.4 Candidate Mechanisms

Audit.

4.7.2.6.5 Practical Examples of Applications

If the network entity fails to respond with services to the user, the network should indicate status of failure. Otherwise, user should suspect attack and behave accordingly.

4.7.2.7 ISDN Notarization Service

4.7.2.7.1 Definition

Combination of other Security Services and additional functionality, i.e., integrity, non-repudiation, authenticity and time of exchange.

4.7.2.7.2 Service Description

A Notarization service for ISDN would provide third-party notarization of electronic documents to ensure their integrity and authenticity to other parties. Properly implemented, the notarization service would seal legal documents from modification but would allow anyone on a network to access and read these documents. This type of service is labeled a mechanism by the OSI Security Addendum and, in fact, the Notarization Server would be implementing the notarization mechanisms. This service is an example of a supplemental ISDN service.

4.7.2.7.3 Relationship to ISO and ISDN

The candidate mechanisms for this service have been previously placed within the ISDN structure.

4.7.2.7.4 Candidate Mechanisms

The candidate mechanisms for the service are digital signature, encipherment and integrity mechanisms, as appropriate.

4.7.2.7.5 Practical Examples of Applications

Practical examples include electronic contract exchange, electronic messaging and legal document registration.

5 ISDN Conformance Test Specifications

The NIUF's Conformance Test (CT) specifications provide test suites to be used to verify the conformance of ISDN equipments to the designated specification. They are written in abstract form so that multiple test equipment vendors may provide implementations of the test suite. The ISDN Conformance test specifications are developed in the ISDN Conformance Test (ICOT) Working Group, and its subordinate Expert Working Groups: the Abstract Conformance Test Group for layer 1 (ACT1) and the Abstract Conformance Test Group for layers 2 and 3 (ACT23). The following text details the Conformance Tests for ISDN equipments.

5.1 Layer 1 BRI

The Basic Rate Interface (BRI) Layer 1 Conformance Test specifications provide the requirements for verifying equipment conformance at layer 1 of the ISDN BRI user-network interface. The following text details the Conformance Tests for layer 1 operation of a BRI.

- Future "U" Interface

The American National Standard for Telecommunications (ANS) T1.601-1992 (Ref. [12]) specifies the minimal set of requirements to provide for satisfactory transmission between the network and the Network Transmission (NT). It describes both the physical interface and the electrical characteristics of the signals appearing at the network side of the NT, commonly called the U interface point, or U reference point. Equipment designed to operate on the North American Integrated Services Digital Network (ISDN) Basic Access U Interface must conform with this set of minimal requirements.

The CT defining this set of conformance test specifications for all NTs connected to the BRI U interface is *Integrated Services Digital Network Conformance Testing, Layer 1 Basic Rate U Interface, User Side.*

- Future "S/T" Interface

The CT defining the conformance criteria and abstract test suites to verify equipment implementation conformance to the BRI S and T interface as specified in ANS T1.605-1991 (Ref. [16]) is defined by the NIUF specification, *Integrated Services Digital Network (ISDN) Conformance Testing, Layer 1 Basic Rate S/T Interface, User Side.*

5.2 Layer 1 PRI

The CT defining the conformance criteria and abstract test suites to verify equipment implementation conformance to the Layer 1 Primary Rate Interface as specified in ANS T1.408-1990 (Ref. [11]) is defined by the NIUF specification, NIUF 400-92, *Integrated Services Digital Network (ISDN) Conformance Testing, Layer 1, Part 3 PRI, User Side.*

5.3 Layer 2 BRI

The layer 2 Conformance Test specifications, for the BRI and PRI access arrangements, provide the requirements for verifying equipment conformance at layer 2 of the ISDN BRI/PRI. The ISDN test suite development process is aligned with International Standards Organisation (ISO) 9646 (Ref. [56]), OSI Conformance Testing Methodology and Framework, Parts 1-3. The following text details the Conformance Tests for layer 2 operation of an ISDN.

The CT defining the abstract test suites to verify equipment implementation conformance to the layer 2 of an ISDN at the user-network interface is defined by the NIUF specification, NIUF 91-0012 *Layer 2 Basic Rate Interface (BRI), Link Access Procedure, D-channel (LAPD) Conformance Tests* (combination of NIUF 89-001.1 and NIUF 91-0007) (Ref. [?]). This conformance test suite is for the Link Access Procedure, D-channel (LAPD) data link protocol and is described in Tree and Tabular Combined Notation (TTCN). Its use is for ISDN terminal equipments attaching to the user side of a Basic Access interface.

The CT defines the conformance criteria to the ANS T1.602-1989 (Ref. [13]) and to the CCITT Recommendation Q.921-1988 (Ref. [25]) (Note: These specifications are the same text). The purpose of the Abstract Test Suite is to provide the most complete protocol conformance test coverage as is possible, not to be completely exhaustive. The LAPD Test Suite has many additional test cases for TEI Management procedures and system related cases which are covered in the body of the CCITT Recommendation Q.921-1988 text (Ref. [25]) but not in the CCITT Recommendation Q.921-1988 state transition tables.

5.4 Future Layer 2 PRI

Editor's Note: This section is reserved for future agreements on the layer 2 PRI conformance test abstract test suites, and conformance criteria to the ANS T1.602-1989 (Ref. [13]).

5.5 Layer 3

The CTs defining agreements on the layer 3 Conformance Test specifications, for BRI and PRI access arrangements, are contained in NIUF 413-92, *Layer 3 Network Access Layer, Part 1 BRI Circuit Switched Call Control, User Side* (Ref. [34]).

6 Application Software Interface (ASI)

This section includes the introductory material for the specification for an Application Software Interface (ASI) defined by the NIUF. The complete ASI documents are published separately.

6.1 Introduction To the ASI

6.1.1 Overview

Part 1 of the ASI provides an initial specification intended to allow implementors to begin using the ASI for implementations of applications requiring a limited subset of ISDN services within a limited set of operating systems. The specification includes the following components:

- introduction to the ASI concepts,
- description of the ASI architecture,
- description of the ASI access functionality,
- ASI command messages to support a basic subset of ISDN services,
- and ASI data structures.

Additional parts of the ASI specification will expand the above list to include:

- ASI access method for DOS, UNIX/POSIX, OS/2, Windows, etc.,
- additional ASI command messages to support additional ISDN services,
- formal specification of the ASI,
- expansion to include the full teleservices architecture,
- and conformance tests.

6.1.2 Charter

The Application Software Interface Group is one of the expert working groups within the North American ISDN Users' Forum, ISDN Implementors' Workshop (IIW).

The Application Software Interface focuses on the definition of a common application interface for accessing and administering ISDN services provided by hardware commonly referred to in the vendor community as Network Adapters (NAs) and responds to the applications requirements generated by the ISDN Users' Workshop (IUW).

The characteristics of this Application Interface shall be:

- portable across the broadest range of system architectures,
- extensible,

- abstracted beyond ISDN to facilitate interworking,

- and defined in terms of services and facilities consistent with OSI layer interface standards.

6.1.3 Goals

The primary goal of the ASI is to provide a consistent set of application software interface services and application software interface implementation agreement(s) in order that an ISDN application may operate across a broad range of ISDN vendor products and platforms.

The application software interface implementation agreements will be referenced by (and tested against) the IUW generated applications. It is anticipated that the vendor companies involved in the development of these implementation agreements will build products for the ISDN user marketplace which conform to them.

ASI Implementation Agreements are likely to become a U.S. Government Federal Information Processing Standard (FIPS).

ASI specifications are expected to serve as a contribution for further North American or International standards activities.

6.1.4 Purpose

Today there exists an ever increasing number of ISDN Network Adapters (NAs) from different manufacturers, each with the same basic subset of features, plus additional features the manufacturers hope will differentiate them from the competition. This environment is illustrated in figure 6-1.

Currently, each NA vendor presents a different software interface to the ISDN application. This produces constant frustration to the ISDN applications developer. Each interface represents the efforts on the part of the vendor to provide access to all ISDN services provided by the NA; yet each, done in isolation, differs from the others. In developing an ISDN application, therefore, the developer is faced with the task of (a) binding with an initial NA (hopefully a popular one), and (b) once his application is fielded, working to enhance his application product to interface with other NAs as well. Exemplifying this process are products in the market today which advertise "currently works with Network Adapters A, B, and C; will support Network Adapters D and E in the near future."

6.1.5 Scope

Figure 6-2 conceptualizes a solution to the application interface incompatibility problem.

The ASI is a software interface between an application and a NA within an operating environment (the operating environment includes the operating system, hardware platform, bus, etc.). Elements on the network side of the interface are referred to as the "**ASI Entity (AE).**" Elements on the application side are referred to as the "**Program Entity (PE).**"

The ASI does not guarantee interoperability between the end to end applications that may use the ASI.

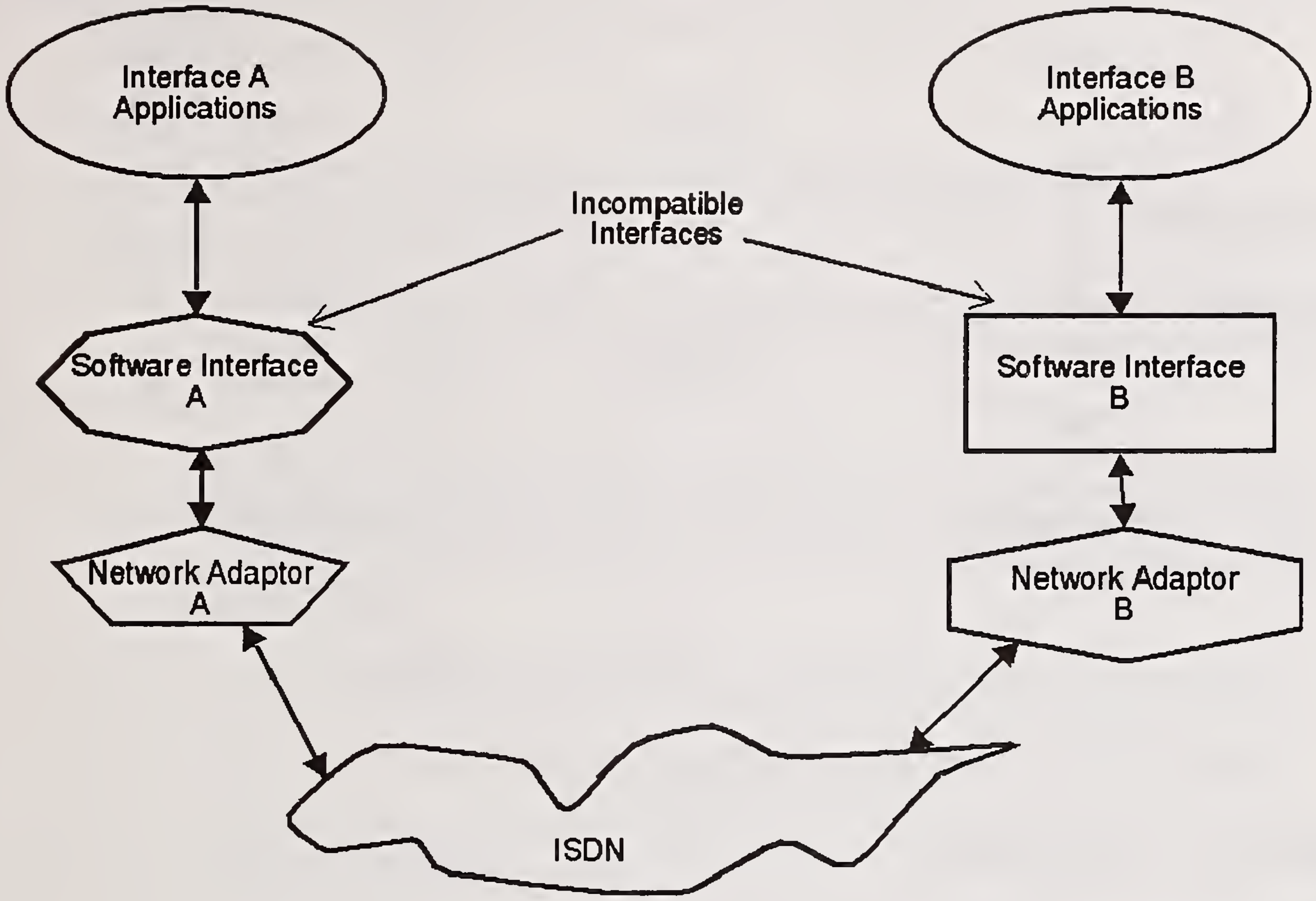


Figure 6-1. Typical Proprietary Interface Environment.

The ASI places emphasis on a common application interface as opposed to a common hardware device interface for two main reasons:

1. The most important user benefit is derived from a large selection of commercially available ISDN applications which can operate over a correspondingly large selection of NAs. The number of applications will be most influenced by the existence of a common application interface that allows the application provider to easily migrate applications to different NAs or operating system environments.

2. It is much more difficult to specify a standard hardware device interface. Vendors want to provide different NA hardware interfaces to appeal to different markets. For example, some NAs will be built for performance while others will be built for low cost. The market that a vendor desires to sell into, will determine the hardware device interface (i.e., memory mapped, polled I/O, interrupt driven, direct memory access (DMA) driven, shared memory, etc.). Vendors are accustomed to providing drivers or libraries which interface to their specific hardware implementation.

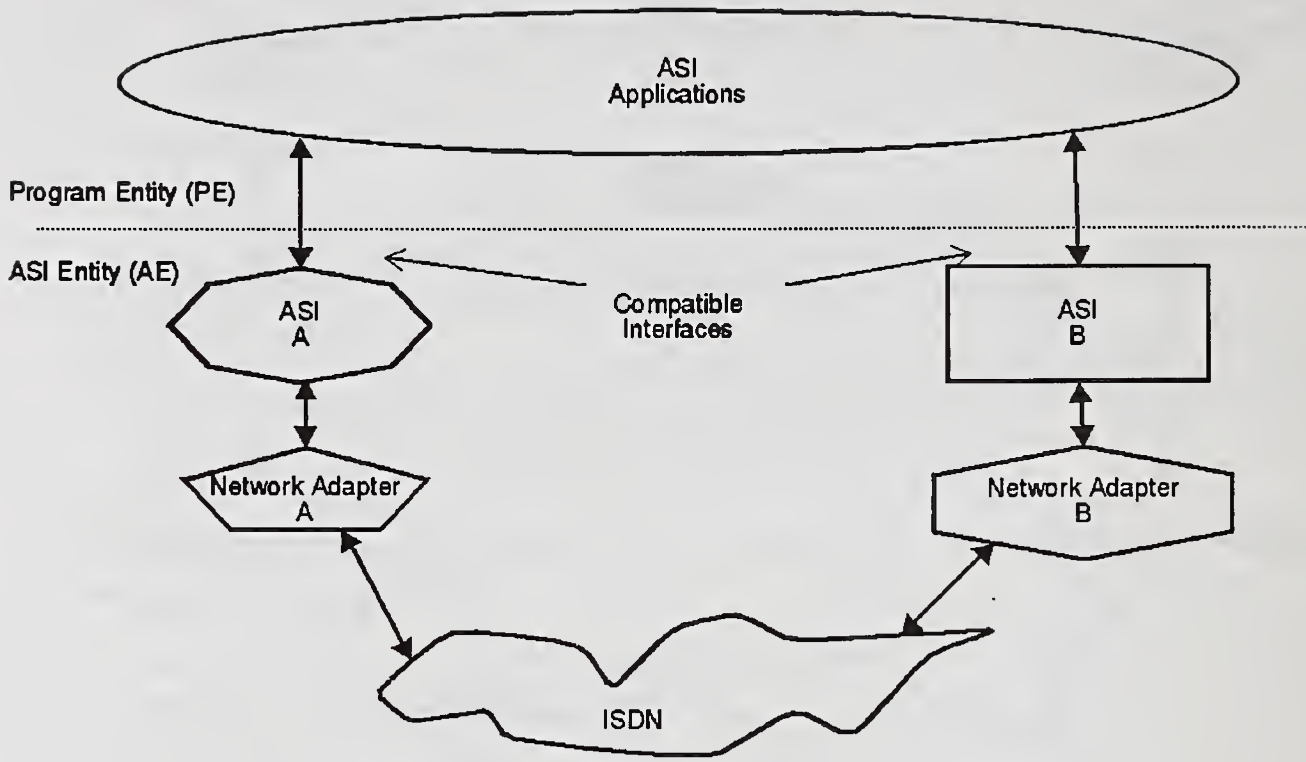


Figure 6-2. ASI Environment.

The conversion from the common ASI to the NA hardware device interface becomes the job of the adapter developer. The conversion function can, for instance, reside in a device driver which is provided by the adapter manufacturer. The application developer should have to do as little as possible to port an application written for one operating system to a different operating system (e.g., to re-compile or re-link is perceived as minimal effort). Also, within one operating system, the application developer should be able to design applications independently of the NA (e.g., the application should work the same and without modification on the variety of NAs available), assuming the NA provides equivalent services.

The conceptual objective of the ASI is to be as independent as possible of:

- Hardware Platform,
- Operating System,
- Data Protocol Type,
- Programming Language,
- and Compiler.

Although the ASI takes the approach of developing a common set of services which are applied across a broad range of environments, the access methods are environment dependent. This is true because of hardware restrictions within different operating environments, performance issues, and fundamental operating system differences.

As applicable ISDN standards evolve it is expected that the ASI will evolve to accommodate those applicable standards.

6.1.6 Assumptions

Several assumptions have gone into the development of the current ASI specification. These assumptions are described as follows:

- ISDN primary rate and basic rate access are assumed to be the network interface to the NA. This does not preclude application of this interface to NAs which interface to other ISDN access methods.

- The ASI provides a uniform software interface defined between the NA and the application. Throughout the ASI specification, the term "ASI entity" is used to refer to the ISDN service provider, and any associated hardware, network adapter card, or terminal equipment, while the term "Program Entity" is used to refer to the application which uses the ISDN service.

- This specification does not address peer-to-peer protocol or interoperability issues.

- The ASI interface is assumed to be at the OSI layer three to layer four boundary.

- ANSI Standards, NIUF Agreements, and CCITT Recommendations are the basis for this ASI specification.

- No default values for parameters are assumed by the interface. All parameter values necessary for a message must be supplied in the applicable data structures.

6.2 Technical Overview

This section presents an overview of the ASI architecture and the motivation underlying the chosen approach.

The goal of the ASI is to provide a portable, extensive, and layered software interface to ISDN hardware, call control, and services. Portability allows applications to be developed independent of any particular vendor's ISDN offering, and hence ties the success of the application to the penetration of ISDN rather than the future of a single vendor. Portability favors the application developer by making the application available for a wider audience. But widespread application availability will make it easier to use ISDN services, hastening deployment of ISDN lines, and thus ultimately benefitting the hardware (or ISDN capable computer platform) vendors as well.

ASI applications run on a computer platform employing ISDN interface hardware from different vendors without recompilation or linking. The same application is portable to a different computer platform (with the same operating system) by recompiling without changes to the source code. There may be some code changes required for a different operating system to accomodate differences in the access method.

A problem with designing application software interfaces to ISDN teleservices is the range of level of functionality such an interface could support. A high level interface would provide generic telephony interface functions, while a lower level would more closely match ISDN-specific message and event types. The ASI favors a layered approach, based on experience with the OSI model and numerous examples in distributed computing.

As such, the ASI incorporates a model with several reference points. A multi-tasking operating system will enable multiple processes to gain access to ISDN services through a server architecture which will provide a high level functional interface and event filtering to minimize ISDN-specific knowledge required of the application. This server, or the single application for a server-less or single threaded operating system, in turn communicates with ISDN call control over a lower level interface which more closely mirrors the ISDN protocol. The various reference points will be illustrated later in this section.

The current release of the ASI specification defines the core subset of the lower level reference point. It is to this reference point which vendors must supply ASI support, and, once written, early applications can be developed immediately. No vendor-specific software need operate above this reference point, although a vendor may choose to provide higher level support for added value to an ISDN product.

The ASI defines a reference point and a message protocol across that reference point. ISDN call control and hardware specific interfaces will operate below the ASI and be provided by specific vendors. Vendors may also supply an application library, in some specific programming language, to compose messages in the ASI format.

The ASI specifies a complete interface composed of an operating system *dependent* access method, an operating system *independent* message set, and an operating system *independent* message encoding method. An operating system dependent access method allows the rest of the ASI to exist independent of the OS.

Because the message set and encoding method are identical between the various implementations of the ASI for different operating systems, application portability is greatly simplified.

The ASI message set and operating system specific access methods provide an asynchronous interface to ISDN call control. The application makes requests through the ASI, and the ISDN call control beneath the ASI transmits confirmation messages and event indication messages back through the ASI as appropriate. Any blocking or synchronous interface to the ASI should be provided as a library of function calls on the application side of the ASI.

For example, an application places a call by sending an Nb-CONNECT request. After issuing the request, the application can continue execution. Call control may generate various Nb-EVENT indication messages as the call proceeds through the network. When the call completes to the called party, an Nb-CONNECT confirmation message will be sent up through the ASI. To implement a blocking call request, the application would send the Nb-CONNECT request, and await the Nb-CONNECT confirmation.

6.2.1 Application Software Interface Definition

The Application Software Interface (ASI) is a common interface for accessing ISDN services provided by ISDN network adapters (NAs). The ASI is a way for an application and an ASI entity to communicate within an operating environment (the operating environment includes the operating system, hardware platform, bus, etc.). The translation of the ASI message set to and from the instructions needed to operate any hardware interfaces is accomplished by AE vendor supplied software. The conversion function, can, for instance, reside in a device driver provided with the AE.

The application developer should be able to design applications independent of the NA with which it might be used. Within a given operating environment (e.g., a PC running DOS), applications should be able to run on any ASI-compliant AE. Finally, the application developer should have to do as little as possible (e.g., recompile/relink) in order to move from one operating system to another. The ASI allows any ISDN application written against the ASI specification to communicate with any ASI-compliant ISDN network service provider.

6.2.2 OSI Reference Model Positioning

The ASI is positioned at the Service Access Point (SAP) between layers 3 and 4 in the OSI Reference Model. Conceptually, the ASI is an asynchronous message stream between the ISDN network services provider (layers 1-3) and the user (layers 4+) of those services.

If, for example, a non-empty transport layer protocol is positioned above the ASI, then that transport protocol, and not the higher layer application, is the actual user of the ISDN bearer services provided through the ASI. Likewise, the term "ASI entity" is meant to apply to any provider of ISDN network services that meets certain qualifying assumptions. The ASI is a local interface between layer 4 and layer 3 only; it is not, itself, a layer within the OSI Reference Model, nor is it an end-to-end protocol. Such features as interoperability or end-to-end integrity must be provided by protocols above the ASI, using ISDN network services accessed through the ASI.

6.2.3 Teleservices Architecture

The environment in which the ASI is expected to operate assumes an architecture including a generic teleservices server. Such a server may offer teleservices to applications on the local machine or on the local area network without requiring the applications to implement the details of ISDN, plain old telephone service (POTS)/public switched telephone network (PSTN), or other possible teleservices media.

It would be the responsibility of a server interface definition to allow for multiple client applications to access the services provided by a single interface adapter.

The teleservices architecture has been split into several layers. Issue 1 ASI is identified as the message stream at reference point "B" in this architecture.

The definition of the Reference Points is as follows, and is depicted in figure 6-3:

- In ASI Version 1, the "A" reference point is not an exposed interface. It is defined to be the interface between the "standard" portions of Q.931 and the non-standard portions. Only the non-standard portions of ISDN need to be customized for each market.

- The "B" reference point is the interface between the ISDN signalling, management and user planes, and a server or dedicated application. Direct multi-client access is not allowed.

- The "C" reference point presents a generic teleservices interface to the server or dedicated application.

• The "D" reference point allows a server to provide a generic teleservices interface to multiple client applications. This interface also presents a simplified programming model to the application or toolkit developer.

• The "E" reference point is the programming interface provided by a high level library. This interface is the one most desired by typical applications developers.

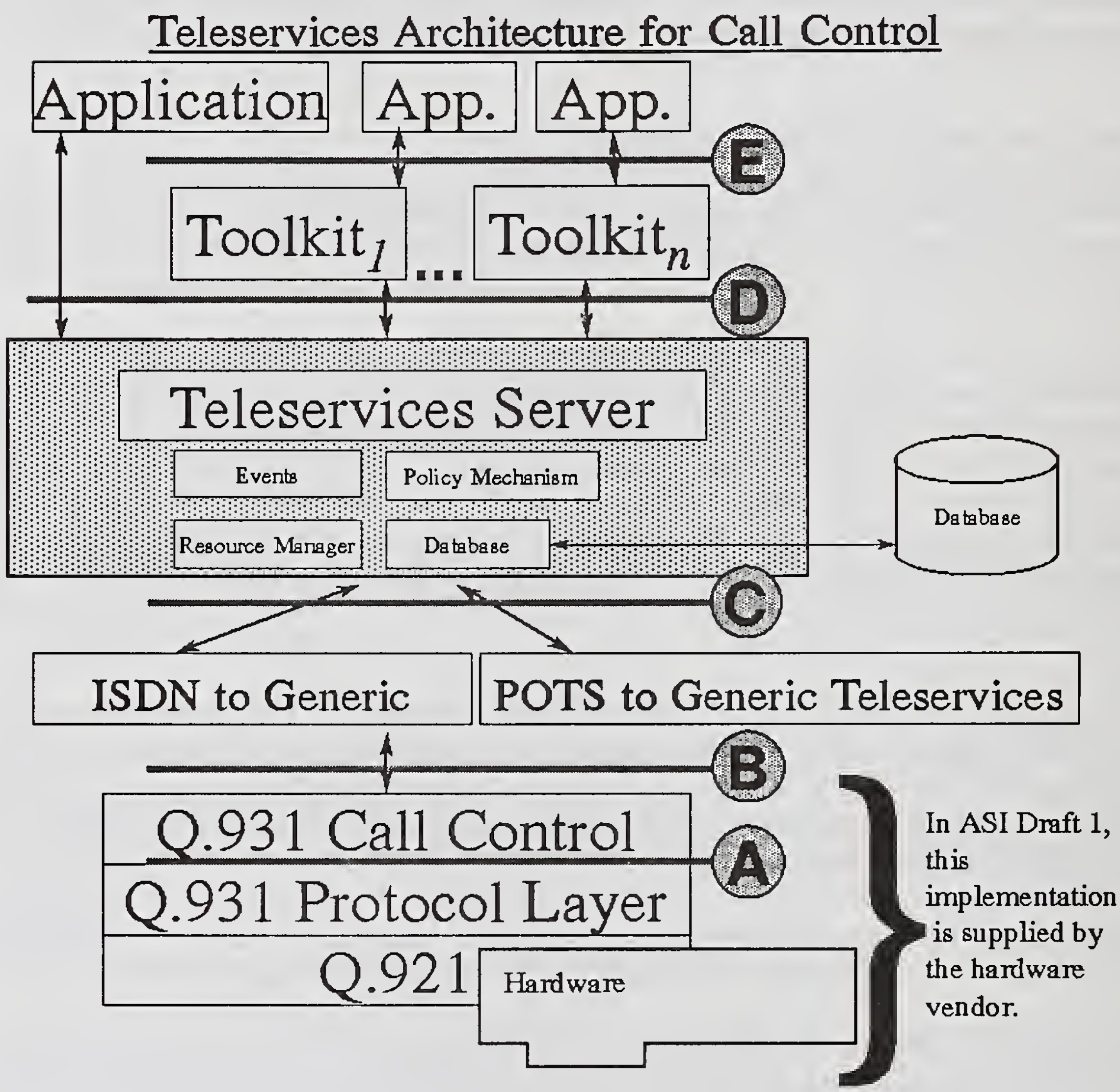


Figure 6-3. Teleservices Architecture for Call Control.

6.2.4 ASI Sessions

The Application Entity (AE) and Program Entity (PE) communicate across the ASI by reference to sessions. A session is a local virtual path between the PE and the AE which carries all requests and responses for a given instance of a service, e.g., a voice call. Once established, a session is referred to by a session ID.

Sessions are created dynamically by either the AE or the PE according to the rules defined by the ASI protocol. To allow for dynamic creation of sessions by either side, each side may create session IDs without consulting the other side. The AE's session ID is referred to as the AEI, while the PE's session ID is referred to as the PEI. Either side may refer to a session using the other's ID. An ID of all zeros indicates that the other side's ID is unknown or is not used.

Retiring and reuse of old IDs is carefully managed by the protocol.

6.2.5 ASI Components

The ASI, or any other interface in the architecture, must contain definitions for the following:

- access methods for each operating environment (DOS, Unix, etc.), for passing messages,
- a set of message types and associated parameters,
- precisely defined encodings for the above messages,
- and a formal description of the protocol semantics.

6.2.5.1 Access Methods

An access method, as defined by this document, is an operating system dependant set of procedures for passing messages between layers of software. The messages may contain control, management, or user plane information.

This architecture requires that any access method provides asynchronous message passing between software layers.

Access methods are described in the *Application Software Interface Part 1: Overview and Protocols* (Ref. [55]), section 4.

6.2.5.2 Messages

In order to meet the portability and network transparency requirements of the architecture, all messages are required to be self contained. Messages containing pointers, or other references, to external data structures are not legal.

Messages and their semantics are described in *Application Software Interface Part 1: Overview and Protocols* (Ref. [55]), section 5. Message parameters are described in *Application Software Interface Part 1: Overview and Protocols* (Ref. [55]), section 6.

6.2.5.3 Encoding

Message definition will be described using ASN.1.

Actual message encoding will be done using an ASI specific method. The method is chosen to promote ease of implementation and improve performance while providing for future expansion of the protocol.

7 Application Profiles

Since the inception of the NIUF, the goal has been to provide an ISDN that users want and need, and to do so in a way that promotes application interoperability in a multi-vendor environment. Application profiles are the final step in the functional standardization process to achieve this goal.

7.1 NIUF Application Profiles

An application profile provides an overall specification of the ISDN elements and the application elements necessary to provide a specific, interoperable application for an ISDN. A profile supports a particular application, or a set of applications, specifying the ISDN standards to use, the options to implement within each standard, the layered protocol configuration and the application's usage of the ISDN's attributes.

7.1.1 Application Profile Conformance

It is essential that the Application Profile teams identify criteria that the implementor must meet in order to claim compliance with the Application Profile. It is intended that a tester agency be established (e.g., the Corporation for Open Systems) which applies ICOT-derived conformance tests in order to verify a product's relative sufficiency of interoperability against a testbed which applies standardized testing methodologies (e.g., ISO 9646, Ref. [56]). Real multi-vendor interoperability is achieved in an interoperability testing environment which validates the Application Profile's compliance amongst participatory users and vendors.

7.1.2 Application Profile Families

The NIUF ISDN applications have been categorized into one of six "application families." The families provide a means of assimilating applications based upon a commonality of usage.

Each family has been assigned its own Application Profile team to develop the Application Profiles for the family. The following Application Profile teams have been identified:

- ISDN Call Management
- ISDN CPE Compatibility/Capability
- ISDN Network Interconnectivity
- Messaging and Answering
- Bandwidth Negotiation
- Network Management/ISDN Administration

The following sections detail the Application Profile IAs.[5]

7.2 ISDN Call Management

7.2.1 Incoming Call Management

The ISDN Call Management Profile team has completed an Application Profile, NIUF 90-003, for incoming call management which covers all of the following applications:

---

[5]The NIUF Plenary document numbers (e.g., NIUF 90-003) are included for reference purposes only, as every numbered application profile is included in the present document in its entirety.

Title	User Req't Document Number
• Database Information to Corporate Security	810005
• New Account Customer Inquiry Handling	840023
• Customer Service Call Handling	840024
• Automatic Callback for Financial Services	840025

7.2.1.1 Abstract

This application profile provides the User Descriptions, Alternative Architectures, Information Flows, and recommended Protocol Stacks for the Incoming Call Management Applications (User Application Requirements Data Form Numbers: 810005, 840023, 840024, 840025, Refs. [36, 37, 38, 39]). The Incoming Call Management Applications involve customer service agents who currently receive incoming calls, ask the caller for their member number, and input that data into a terminal connected to a host application. ISDN will be used to automate the transfer of the Caller's ID to the host. In addition, agents may transfer the call to an additional agent who should be able to continue the call without having to request the same information from the caller again. ISDN will be used to effect the call transfer and allow the second agent to bring up the right application screen without repeating questions. Finally, when all the agents are busy, the caller's number should be captured for later callback. ISDN will be used to capture the caller's number and allow callback later. ISDN can be used to connect the agent's terminal to the host.

7.2.1.2 User Description

Customer service agents currently receive incoming calls, ask the caller for their member number, and then input the member number into a terminal connected to a host application to obtain the customer information. Agents may transfer the customer to another agent to provide a different service. The second agent has to again ask for the member number and enter a transaction to receive the customer information. The second agent may access a different host application. In addition, when all agents are busy, the caller's number should be captured for later callback.

7.2.1.3 ISDN Application Breakdown

The user's proposed application and the breakdown of the application into service elements can be seen in figure 7-1.

• Call Transfer with Associated Data Service Element

Agent 1 wishes to transfer a voice call from the Customer to agent 2. The voice call is transferred to agent 2. Certain information associated with the terminal session is transferred to the host to which agent 2 is attached, so that the appropriate screen can be delivered to agent 2.

• Call Delivery with Associated Data Service Element

The customer places a voice call in order to speak to an agent. The call arrives at a Central Office (CO) or Customer Premises switch (PBX). The switch delivers the voice

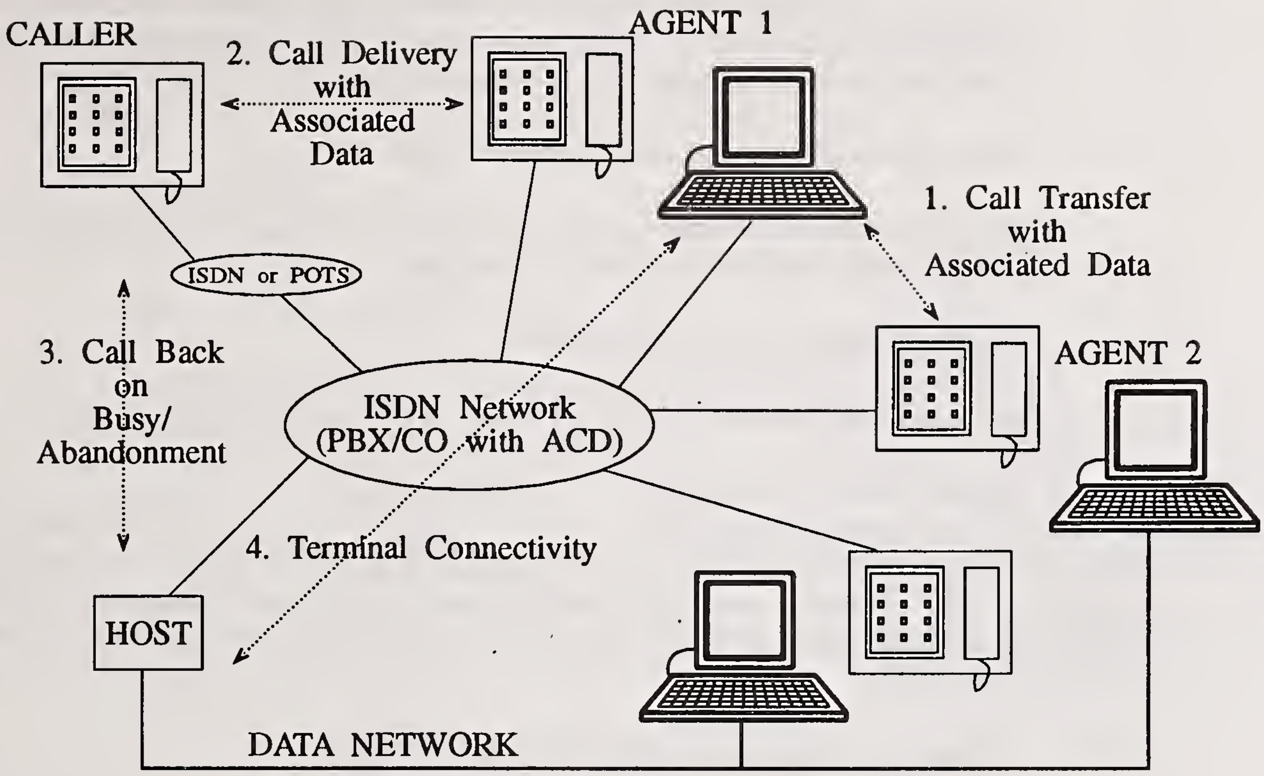


Figure 7-1. User Proposed Application Service Breakdown.

call to agent 1.[6] Certain information that is delivered to the switch with the voice call (probably the calling party's number) is delivered to a host application, so that the host application can deliver an appropriate screen to agent 1.

• Call Back on Busy/Abandonment Service Element

This service allows an available agent to place calls to customers who have received busy or abandoned the call prior to delivery to an agent.

• Terminal Connectivity Service Element

The agent's data terminal is connected to the host via an ISDN link.

7.2.1.3.1 Service Logic

Figure 7-2 shows the sequence of services put together to provide Incoming Call Management Applications. The Terminal Connectivity Service Element may be optional and a Call coming in without the associated data (Calling Line Identification (CLID)) may be available for Call Transfer with associated data.

7.2.1.4 Call Transfer with Associated Data Service Element

In this service a call is already active between agent 1 and the caller. Agent 1 could then perform any of the following:

1. Blind Transfer—Transfer the call to a second agent and disconnect before the second agent answers.

2. Transfer with Consulting—Transfer the call to a second agent, discuss the call with the second agent, then complete the transfer.

3. Consult—Agent 1 calls the second agent to discuss the call and then disconnects agent 2.

The components are shown in figure 7-3.

The sequence of events for each type is:

Blind Transfer

a. Agent 1 places the caller on hold.

b. Agent 1 places a call to agent 2 and invokes transfer.

c. Agent 1 hangs up.

d. Agent 2 is selected directly or by an intervening CO/PBX (Automatic Call Distributor (ACD) function).

---

[6]The topic of how the switch decides to deliver the call to a particular agent has not been described as part of this application, but may have some bearing on implementation.

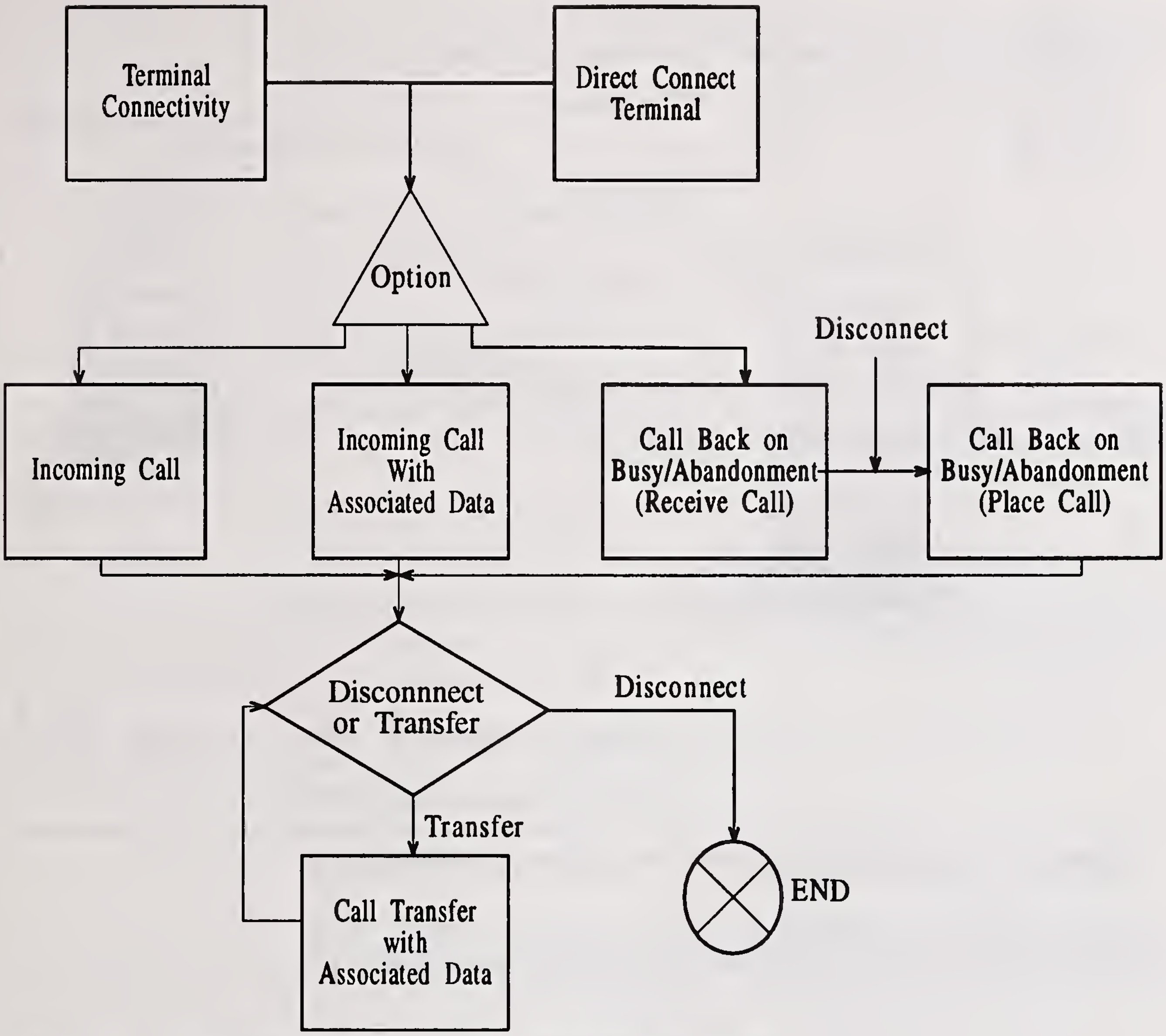


Figure 7-2. Incoming Call Management Application Logic Flow.

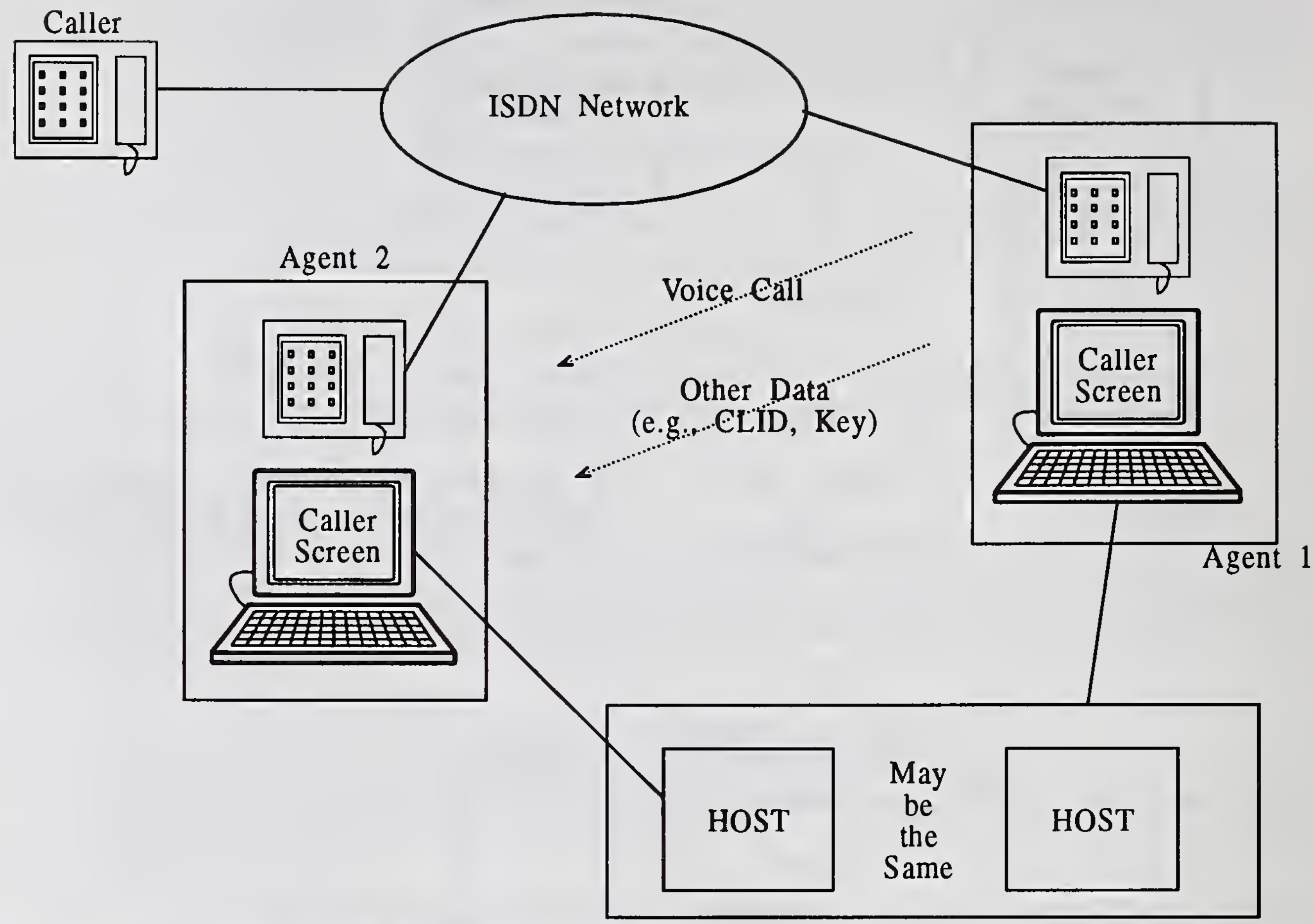


Figure 7-3. Call Transfer with Data Service Element Description.

e. Agent 2 receives the voice call, while concurrently a host[7] application brings up an appropriate screen based on some information delivered with the call to agent 2.

Transfer with Consulting

a. Agent 1 places the caller on hold.

b. Agent 1 places a call to agent 2.

c. Agent 2 is selected directly or by an intervening CO/PBX (ACD function).

d. Agent 2 receives the voice call, while concurrently a host application brings up an appropriate screen based on some information delivered with the call to agent 2.

e. Agent 1 talks with agent 2.

f. Agent 1 transfers the caller to agent 2 and disconnects.

Consulting

a. Agent 1 places the caller on hold.

b. Agent 1 places a call to agent 2.

c. Agent 2 is selected directly or by an intervening CO/PBX (ACD function).

d. Agent 2 receives the voice call, while concurrently a host application brings up an appropriate screen based on some information delivered with the call to agent 2.

e. Agent 1 talks with agent 2.

f. Agent 2 disconnects.

The information being passed along with the call will be called the Key. The Key may be any of the following:

- a database key used by the agent's application,
- the Calling Party Number,
- an Application or Screen ID,
- some other information used by the user's application,
- or a combination of the above.

---

[7]The host that the application is running on may be the same for both agents or different.

7.2.1.4.1 User Environment

Some of the users' descriptions of the service have specified a hardware and software environment in which the service should work. At a minimum, the service should work in the following environment:

- IBM 3270[†] type terminals
- An IBM-compatible host
- SNA (Systems Network Architecture) host networks.

These are minimum requirements and the actual description of the service is more general in that it will work with other terminals, hosts, and networks.

7.2.1.4.2 Alternative Architectures

Two architectures for this application have been proposed and adopted (March 1989 and June 1989 NIUF). The first architecture calls for the Call information to be delivered to the agent's station or terminal adapter (TA)[10] and then have that device transmit it to the host application (see fig. 7-4). If the agent's station is sufficiently intelligent (e.g., a personal computer), the station could run the application locally.

The second architecture calls for the Host to provide the central office or customer premises switch with the Key, and that Key is passed to agent 2's Host (see fig. 7-5). The call is delivered to the agent's station normally. The data terminal could be attached to the host directly or be attached using the **ISDN Terminal Connectivity Service Element** described in section 7.2.1.7.

7.2.1.4.3 Information Flow

The information flow diagrams show the data that must be sent between nodes necessary to provide the service described. Signalling messages that are normally present (i.e., confirmation messages, error messages, disconnect) are not shown for simplicity if they are not necessary to explain the working of the service.

The information flow for Architecture 1—Smart Terminal/TA can be seen in figure 7-6.

Agent 1 places a call (Call Setup) which is delivered to agent 2's station with the Key (carried as User-to-User information). Agent 2's station could generate an appropriate screen using the Key

---

[†]Trademark of IBM Corporation

[10]This requires intelligence not normally associated with a TA to satisfy the requirement that any 3270-like device were to be able to use this service. A separate functional entity, and Intelligence Unit (IU), will be described as providing the service of relaying Call information to the host. In effect this unit would upgrade the 3270 to an intelligent terminal with an attached voice terminal. The TA-intelligence unit will have to be able to have a separate session to the host running, so the data can be passed. Alternately, but more complex, the Intelligence Unit would have to be able to understand the screens being passed between the host and the terminal and insert information in the data stream.

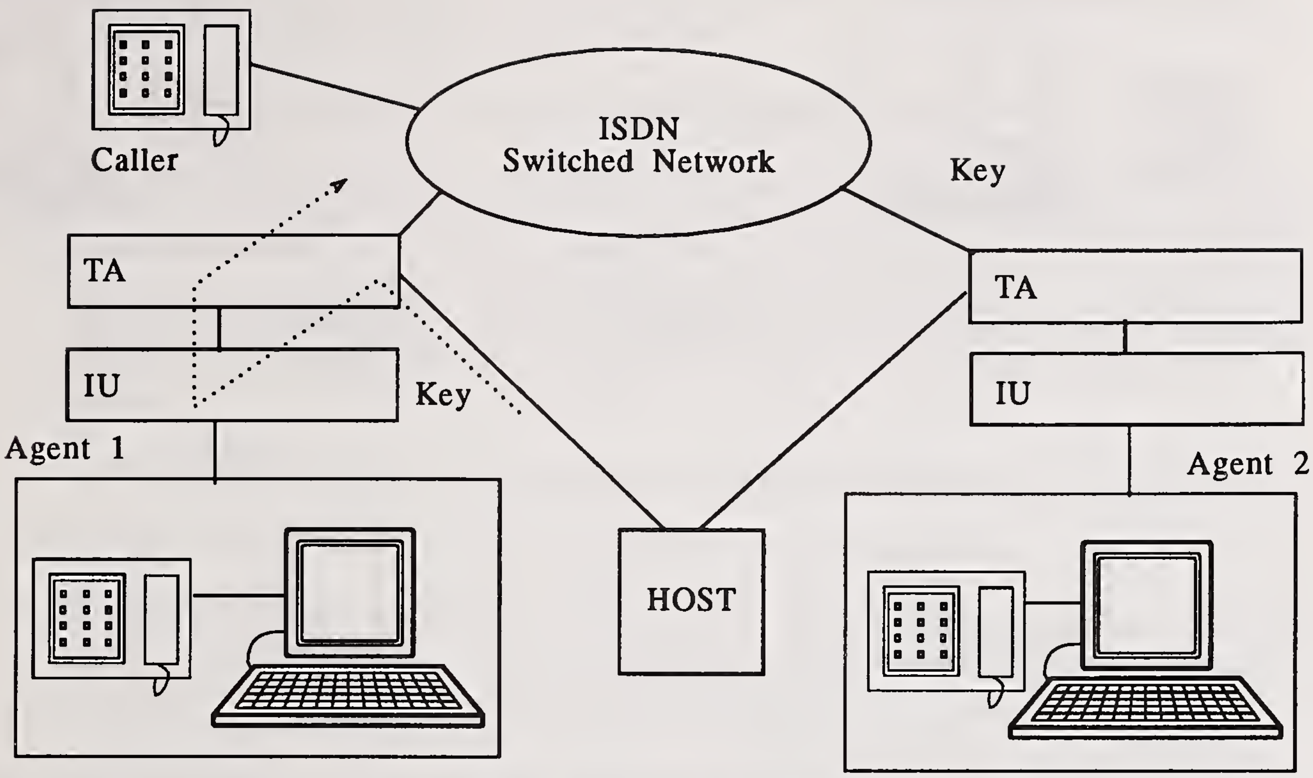


Figure 7-4. Call Transfer with Data Service Element Architecture 1—Smart Terminal/TA.

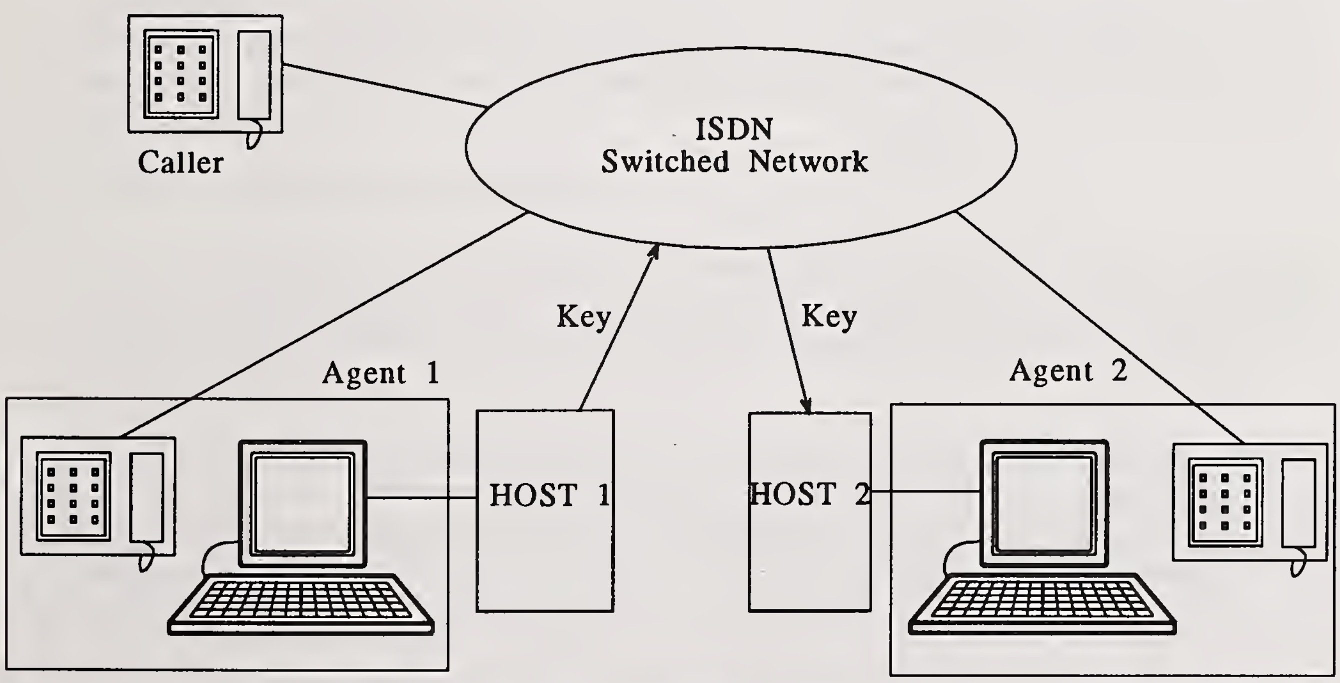


Figure 7-5. Call Transfer with Data Service Element Architecture 2—Switch Host Interface.

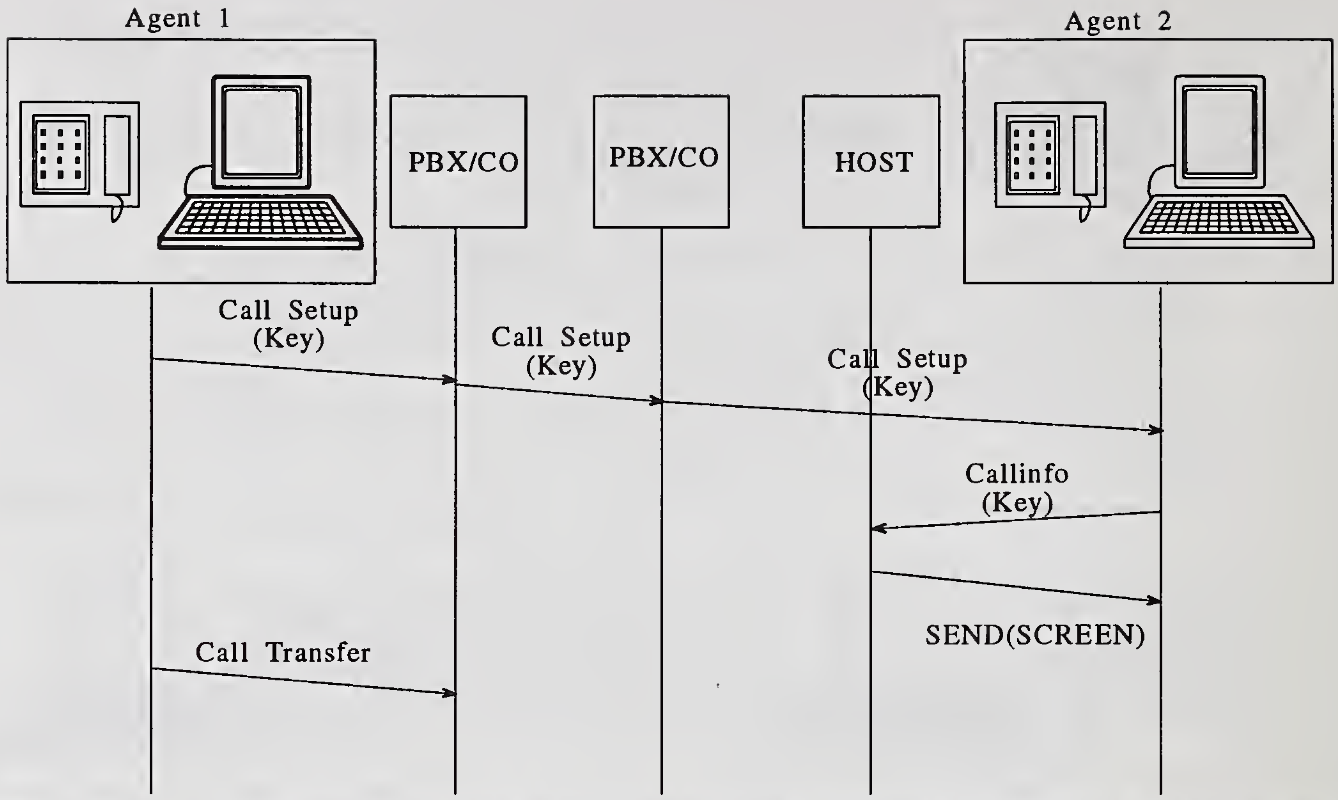


Figure 7-6. Call Transfer with Data Service Element Smart Terminal/TA—Information Flow Diagram.

or the station could then transfer the Key to the host. The host application would then select and transmit the appropriate screen to agent 2's terminal.

The information flow for Architecture 2—Switch Host interface can be seen in figure 7-7.

The call would be initiated by agent 1 selecting to transfer via the terminal. The terminal would transfer this information to the host ("Init Call"). The host would then transmit this to the PBX/CO along with the Key as User-to-User information ("Init Call (Key)"). The PBX/CO the second agent is attached to would transmit the call setup information to agent 2's station. Simultaneously the PBX/CO would send the call setup information (including the user-to-user information containing the Key) to the host computer. The host selects and transmits the appropriate screen to agent 2's terminal.

In both flows, if consulting is desired instead of completing the transfer, agent 2 would disconnect.

7.2.1.4.4 Network Signalling Requirements—Protocol Identification

The network signalling requirements for providing this service with each architecture are shown in figures 7-8 and 7-9. Not shown is how the call was originally received, since it may have come in via ISDN or POTS. The requirement for this capability is that the end points involved in the call transfer must be connected via end-to-end ISDN signalling so that user-to-user information can be exchanged.

In figures 7-8 and 7-9, any connection between two devices without a specific protocol marked may use any applicable protocol including a proprietary one.

7.2.1.4.5 Protocol Description

The messages and protocol elements described below are only those required by the service being described. Other messages and protocol elements are not discussed if they are not used by the application being described, even though they may be required for other reasons, such as routing of the call.

7.2.1.4.5.1 Call Setup User Information

The Key can be carried from the origination to destination terminal in the **SETUP** message described in NIUF 90-301 (see Appendix A) and NIUF 90-302 (see Appendix B). The **SETUP** Message described is sent to the network and by the network to the called user to initiate call establishment.

The information element used to carry the Key would be the **User-User** information element described as follows: "The purpose of the User-user information element is to convey information between ISDN users. This information is not interpreted by the network, but rather is carried transparently and delivered to the remote user(s). There are no restrictions on the content of the user information."

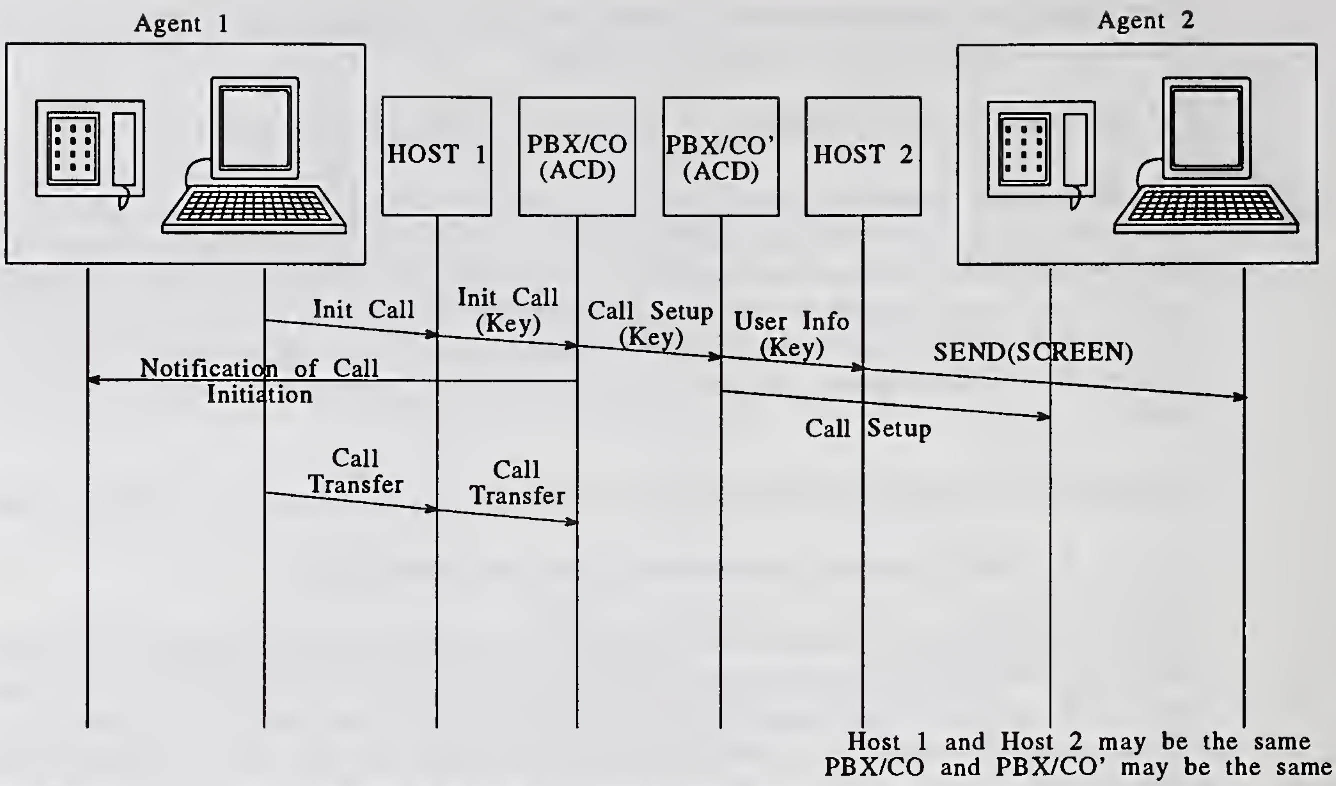


Figure 7-7. Call Transfer with Data Service Element Switch Host Interface—Information Flow Diagram.

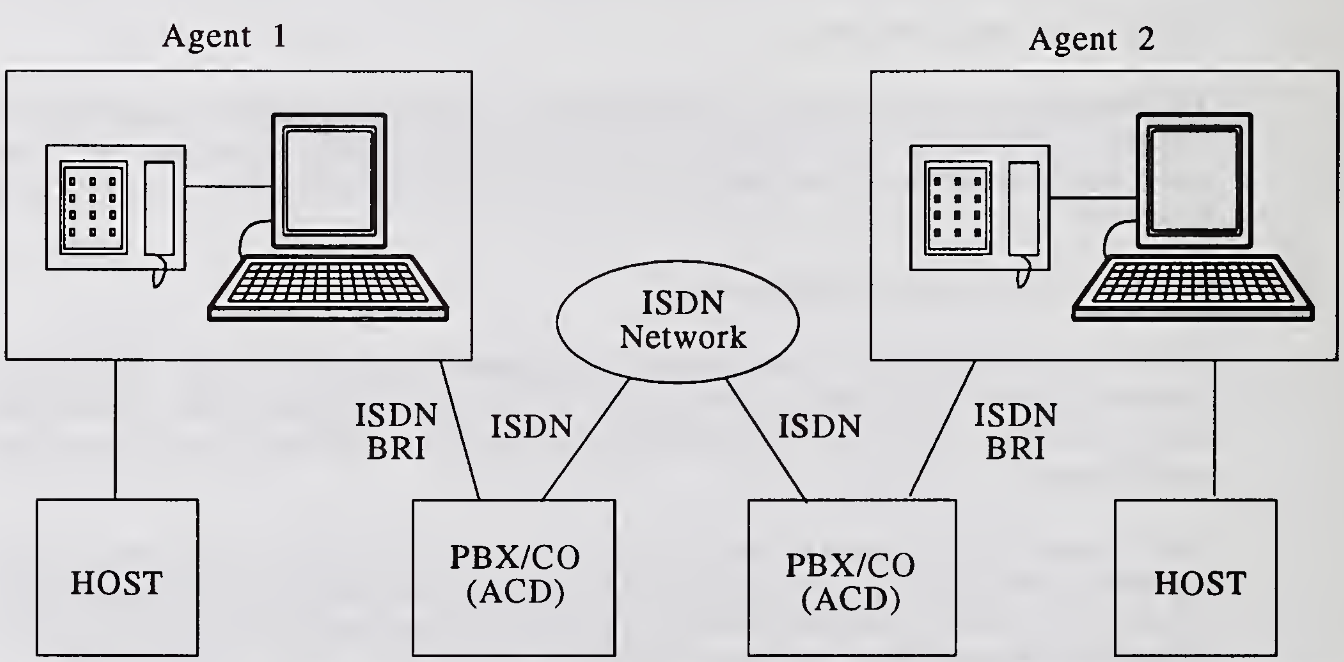


Figure 7-8. Call Transfer with Data Service Element Smart Terminal/TA—Network Signalling Requirements.

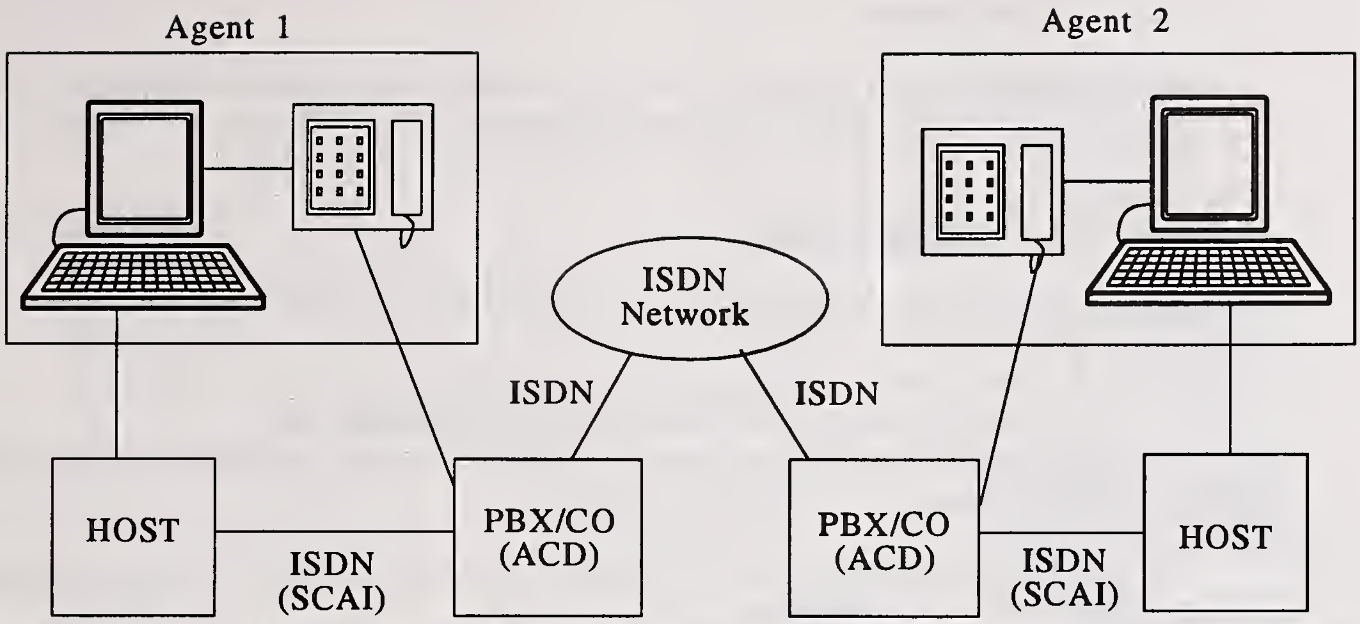


Figure 7-9. Call Transfer with Data Service Element Switch Host Interface—Network Signalling Requirements.

7.2.1.4.5.2 Call Transfer

Proposed Draft American National Standard for the Normal Call Transfer supplementary service exists at the T1 Letter Ballot 340, *ISDN Supplementary Service Normal Call Transfer*, (Ref. [22]).[11]

7.2.1.4.5.3 Host-Switch Messages

The functions that need to be provided to allow this service are the following:

- Send User-User information (Key) and initiate a call.
- Receive User-User information (Key) on an incoming call.
- Possibly initiate the call transfer operation, this could be done from the voice terminal directly.

The Host Computer messages are being described in the ANS *Switch-Computer Applications Interface (SCAI)*, T1.626-1992 (Ref. [23]).

7.2.1.5 Call Delivery with Associated Data Service Element

In this service an agent is available to receive an incoming call. When a customer's call is presented to the agent an appropriate screen is displayed on the agent's data terminal that relates to the caller or the application being provided by the agent (see fig. 7-10).

The sequence of events is as follows:

a. Caller places a call to the phone number of the "Call Delivery service user" (800 number in some user's application).

b. An agent is selected by the CO/PBX (ACD function).

c. The agent receives the voice call, while concurrently a host application brings up an appropriate screen (based upon the calling party's number).

7.2.1.5.1 User Environment

Some of the users' descriptions of the service have specified a hardware and software environment in which the service should work. At a minimum, the service should work in the following environment:

- IBM 3270 type terminals
- An IBM-compatible host
- SNA host networks

These are minimum requirements and the actual description of the service is more general in that it will work with other terminals, hosts, and networks.

---

[11]There is also ongoing work within T1S1 to define Explicit Call Transfer and Single Step Call Transfer Supplementary Services.

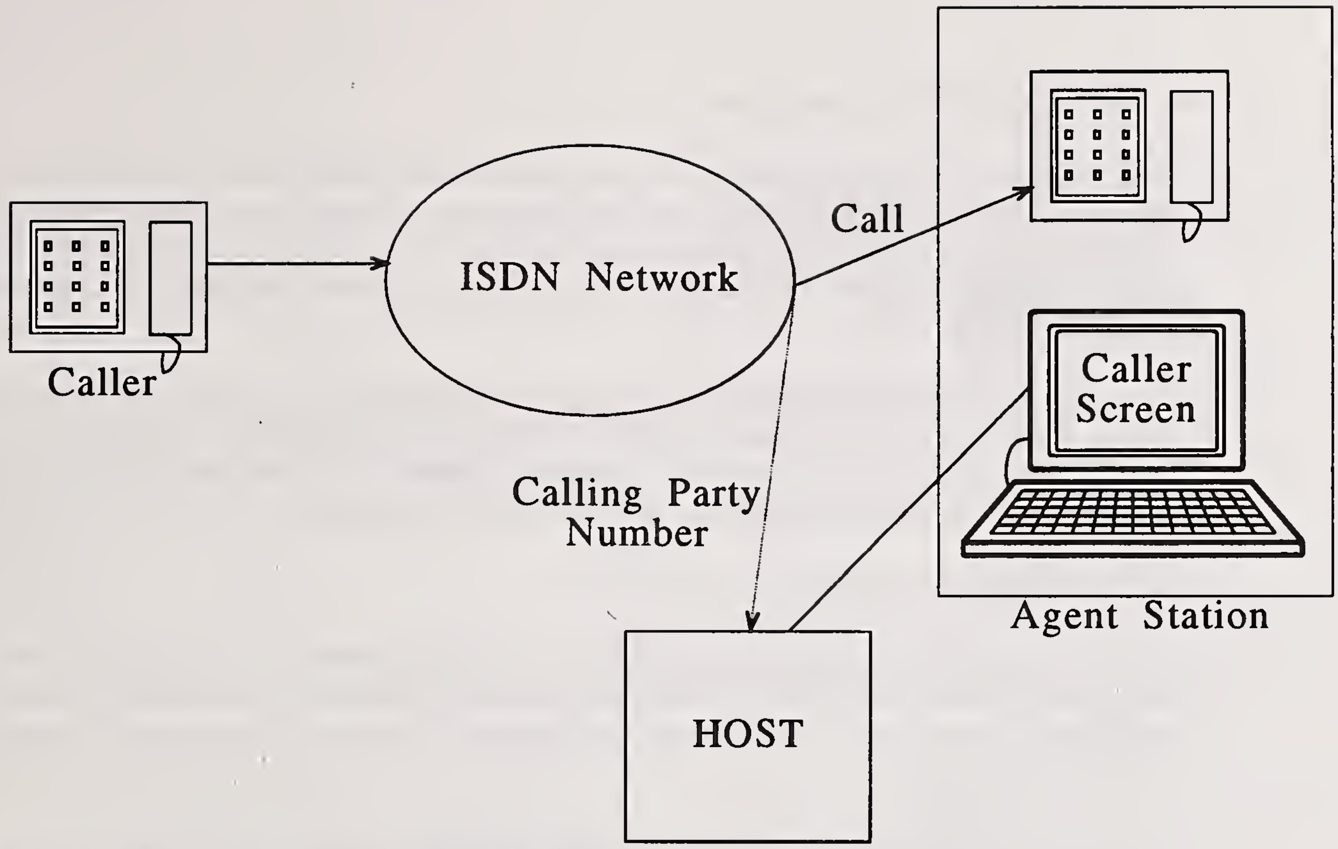


Figure 7-10. Call Delivery with Data Service Element Description.

7.2.1.5.2 Alternative Architectures

Two architectures for this application have been proposed and adopted (March 1989 and June 1989 NIUF). The first architecture calls for the Call information to be delivered to the agent's station or terminal adapter (TA)[12] and then have that device transmit it to the host application (see fig. 7-11). If the agent's station is sufficiently intelligent (e.g., a personal computer), the station could run the application locally.

The second architecture calls for the Host to provide the central office or customer premises switch with the Key, and that Key is passed to agent 2's Host (see fig. 7-12). The call is delivered to the agent's station normally. The data terminal could be attached to the host directly or be attached using the **ISDN Terminal Connectivity Service Element** described in section 7.2.1.7.

7.2.1.5.3 Information Flow

The information flow diagrams show the data that must be sent between nodes necessary to provide the service described. Signalling messages that are normally present (i.e., confirmation messages, error messages, disconnect) are not shown for simplicity, if they are not necessary to explain the working of the service.

The information flow for Architecture 1—Smart Terminal/TA can be seen in figure 7-13.

The call is delivered to the agent's station with the Calling Party Number (CPN). The station will generate an appropriate screen locally or by interacting with a host application.

The information flow for Architecture 2—Switch Host interface can be seen in figure 7-14.

The Switch transmits the call setup information to the agent's station and the host computer simultaneously. The host selects and transmits the appropriate screen.

---

[12]This requires intelligence not normally associated with a TA to satisfy the requirement that any 3270-like device were to be able to use this service. A separate functional entity, and Intelligence Unit (IU), will be described as providing the service of relaying Call information to the host. In effect this unit would upgrade the 3270 to an intelligent terminal with an attached voice terminal. The TA-intelligence unit will have to be able to have a separate session to the host running, so the data can be passed. Alternately, but more complex, the Intelligence Unit would have to be able to understand the screens being passed between the host and the terminal and insert information in the data stream.

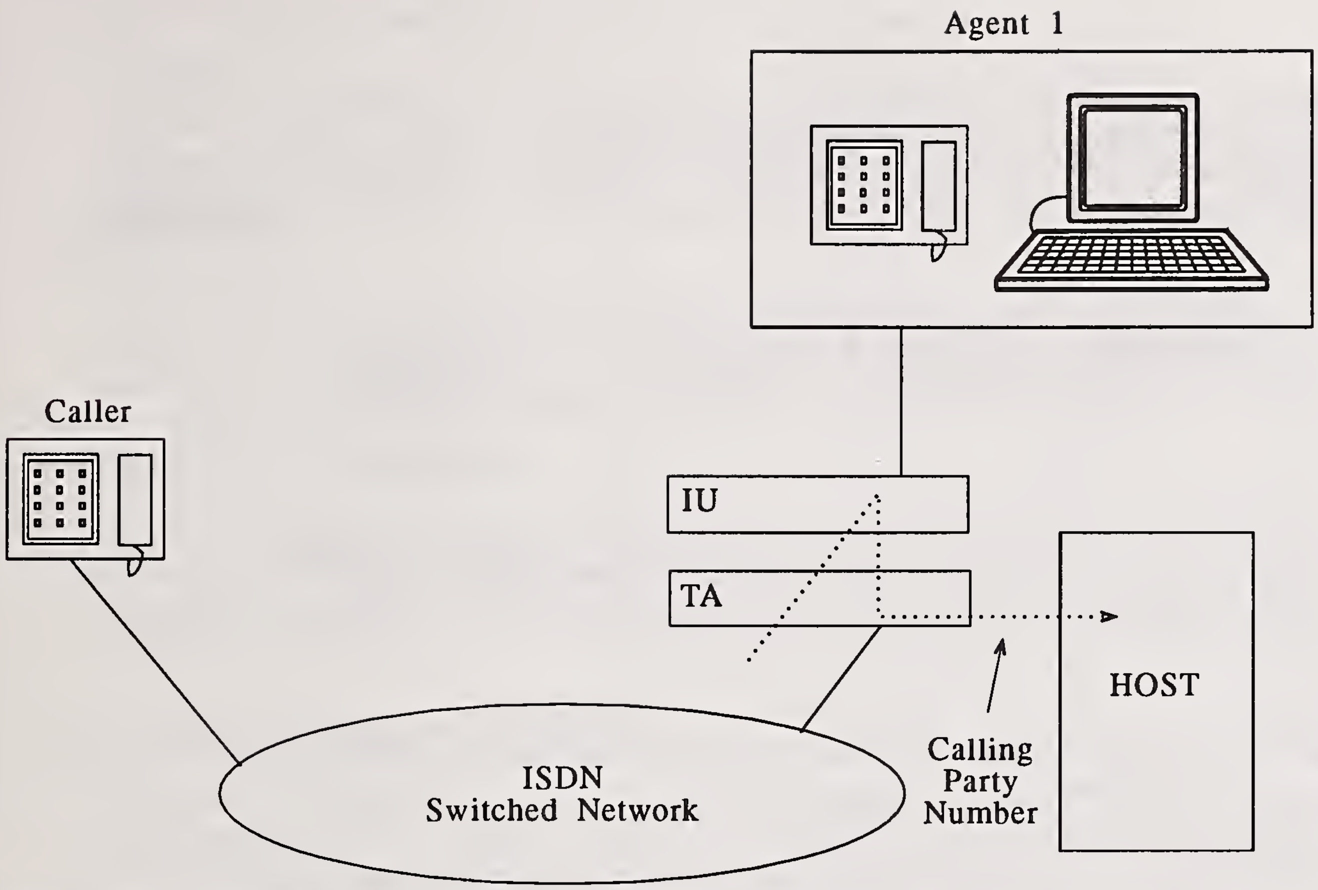


Figure 7-11. Call Delivery with Data Service Element Architecture 1—Smart Terminal/TA.

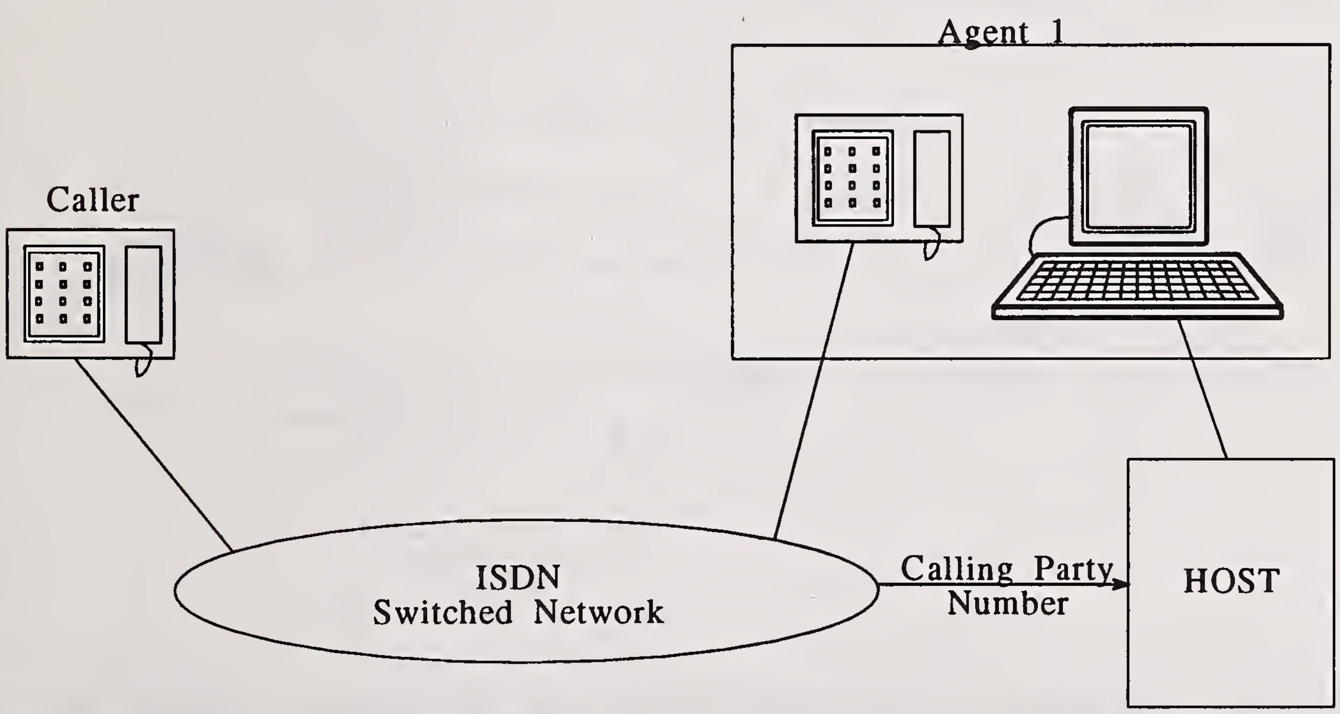


Figure 7-12. Call Delivery with Data Service Element Architecture 2—Switch Host Interface.

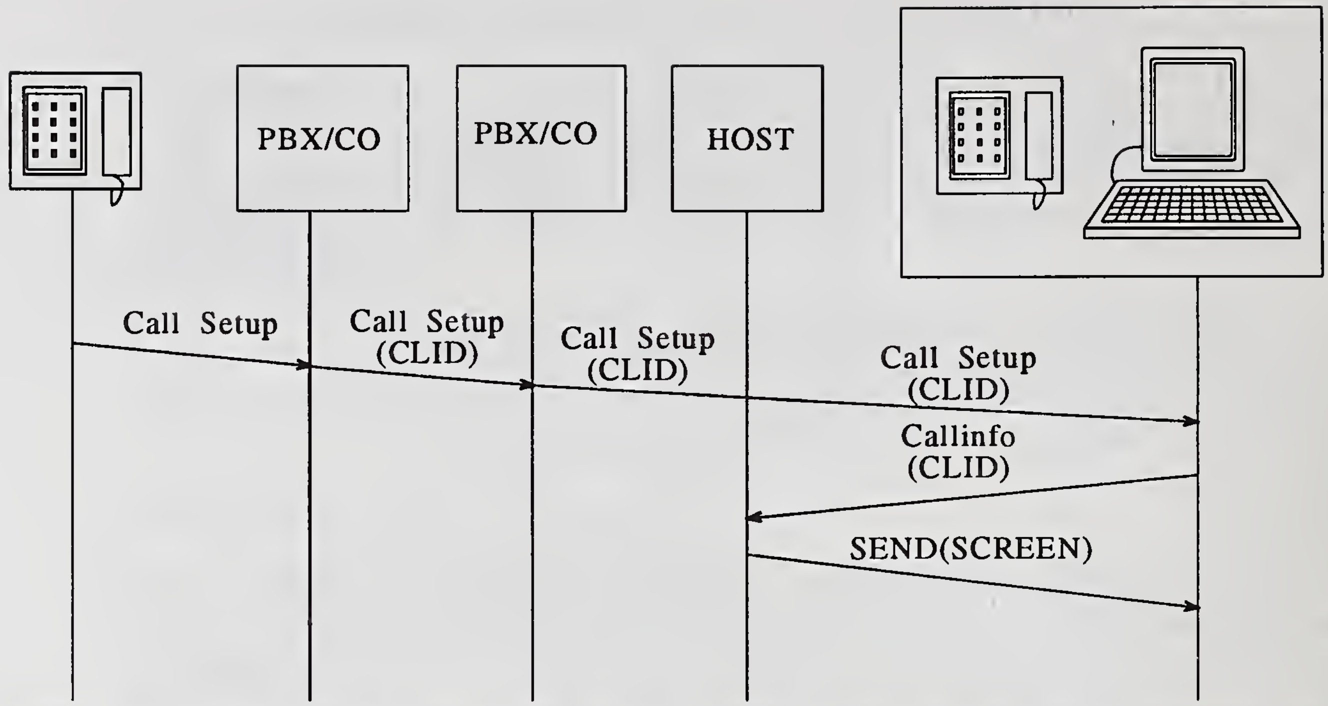


Figure 7-13. Call Delivery with Data Service Element Smart Terminal/TA—Information Flow Diagram.

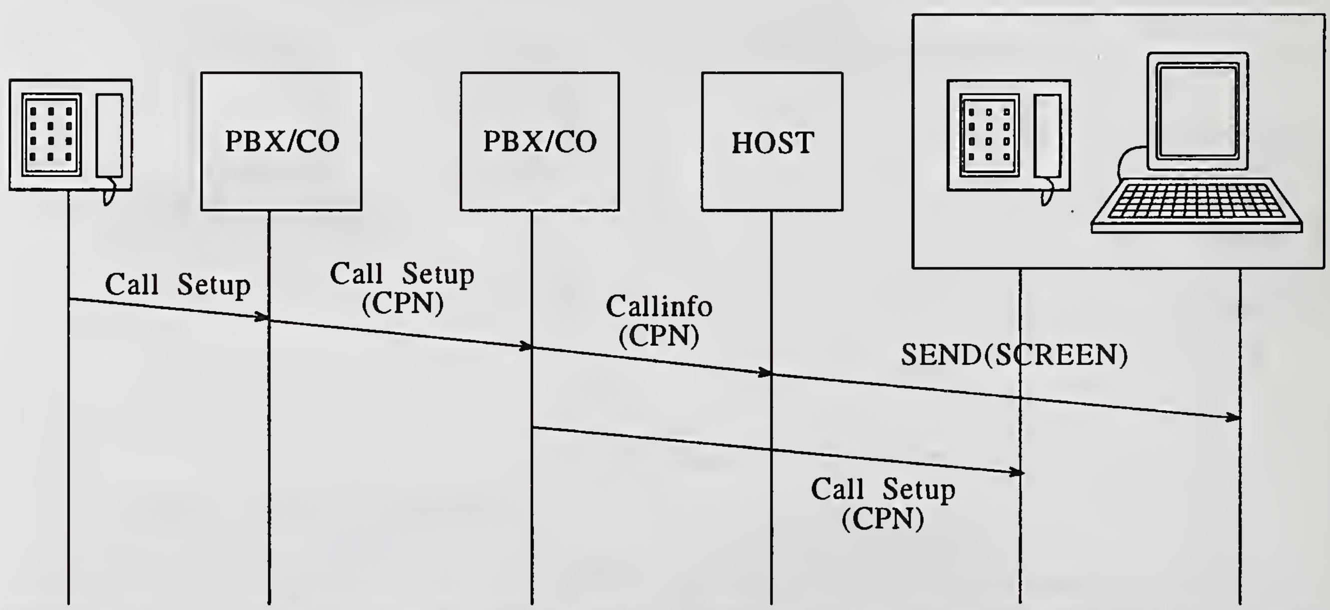


Figure 7-14. Call Delivery with Data Service Element Switch Host Interface—Information Flow Diagram.

7.2.1.5.4 Network Signalling Requirements—Protocol Identification

In order to implement this service, certain signalling capabilities are required in the user and carrier networks. Figures 7-15 and 7-16 identify what are the signalling requirements at each point in the network. As can be seen in the diagrams the requirements for signalling within the network are the same for the smart terminal and switch-host scenarios, but there are differences within the premises.

EAMF stands for Equal Access Multi-Frequency which can be used to pass the Calling Party Number. Any connection between two devices without a specific protocol marked may use any applicable protocol including a proprietary one.

7.2.1.5.5 Protocol Description

The messages and protocol elements described below are only those required by the service being described. Other messages and protocol elements are not discussed if they are not used by the application being described, even through they may be required for other reasons, such as routing of the call.

7.2.1.5.5.1 Call Setup User Information

The Calling Party Number can be carried from the origination to destination terminal in the **SETUP** message described in NIUF 90-301 (see Appendix A) and NIUF 90-302 (see Appendix B). The **SETUP** message is described as sent to the network and by the network toward the called user to initiate call establishment.

The Information needed to carry the Calling Party Number is described in a paragraph titled **Calling Party Number**. "The Purpose of the Calling party number information element is to identify the origin of the call." The information element may say that the number is not available; the application must be able to handle this situation appropriately.

7.2.1.5.5.2 Host-Switch Messages

The necessary function required by this service is the handling of the incoming Calling Party Number.

The Host Computer messages are described in the ANS *Switch-Computer Applications Interface (SCAI)*, T1.626-1992 (Ref. [23]).

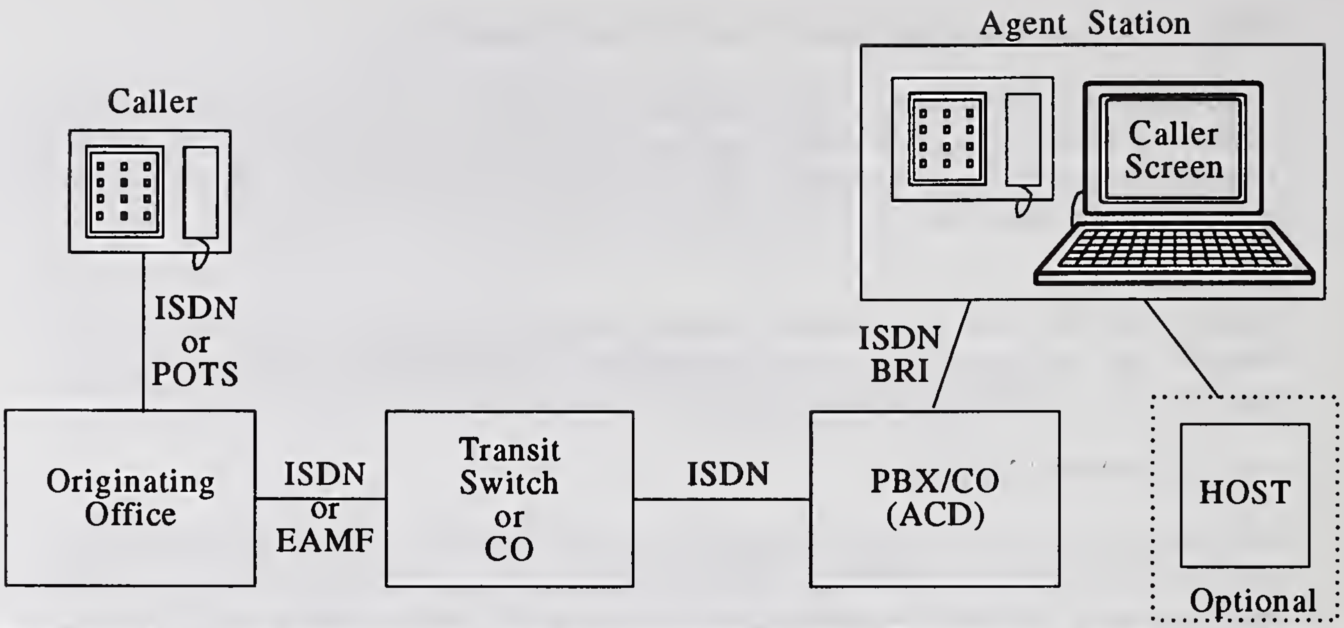


Figure 7-15. Call Delivery with Data Service Element Smart Terminal/TA—Network Signalling Requirements.

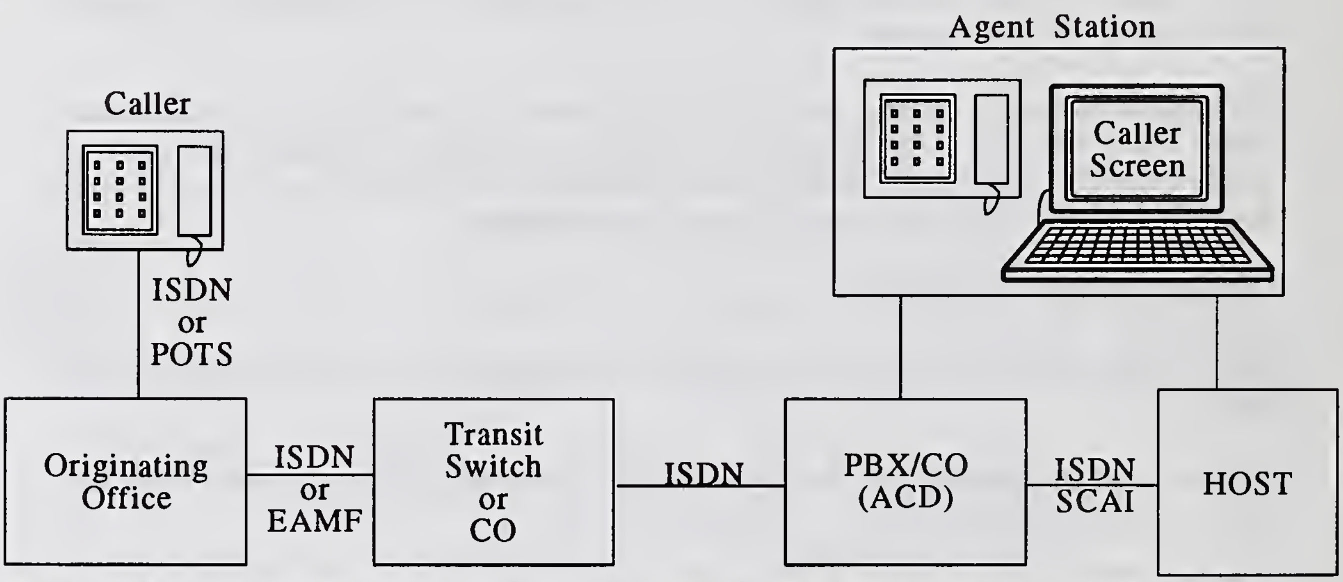


Figure 7-16. Call Delivery with Data Service Element Switch Host Interface—Network Signalling Requirements.

7.2.1.6 Call Back on Busy/Abandonment Service Element

In this service, no agents are available to receive an incoming call. The caller may do any of the following:

- receive Busy (possible reasons: all agents busy, maximum queue size),
- receive an Announcement (i.e., "All lines are busy, an agent will call you back when one becomes available") followed by disconnect,
- or be placed in a queue (possibly with an announcement "Wait for the next available agent, if you hang up, an agent will return your call") for the next available agent and then disconnect.

The caller's phone number will be recorded so that an agent can call back later (see fig. 7-17). This service cannot be invoked unless the call is delivered to the final switch.

The sequence of events is as follows:

1. Caller places a call to the phone number of the "Call Delivery service user" (800 number in one user's application).
2. The calling line identification is recorded by a host application.
3. The treatment may be busy, an announcement and disconnect, or being placed in a queue. If the caller was placed in a queue, they are subsequently disconnected.
4. Agent obtains the number from the application software and places a call.

7.2.1.6.1 User Environment

Some of the users' descriptions of the service have specified a hardware and software environment in which the service should work. At a minimum, the service should work in the following environment:

- IBM 3270 type terminals
- An IBM-compatible host
- SNA host networks

These are minimum requirements and the actual description of the service is more general in that it will work with other terminals, hosts, and networks.

7.2.1.6.2 Architecture

Two architectures for this application have been proposed and adopted (March 1989 and June 1989 NIUF). The first architecture calls for the information to be delivered to the agent's terminal and the second to a host computer. Only the second architecture is considered here because there

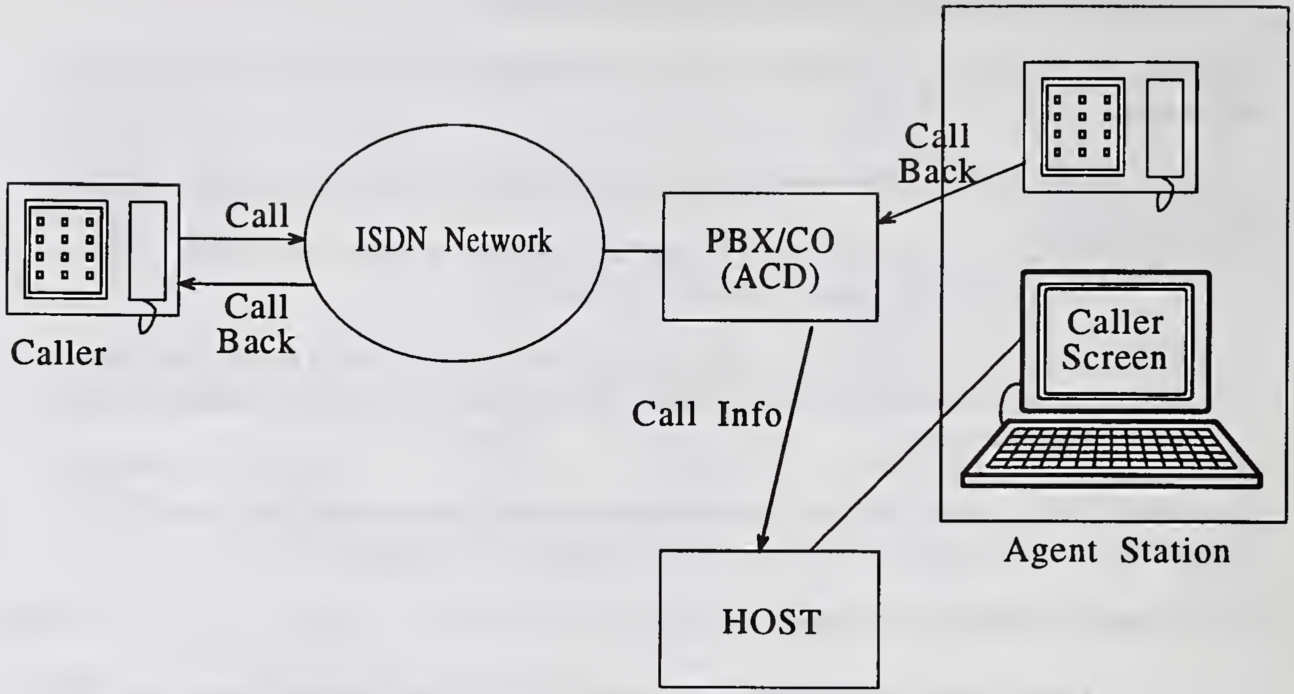


Figure 7-17. Call Back on Busy/Abandonment Service Element Description.

is no mechanism to pass information about calls that have never reached a station (i.e., Caller disconnects, PBX returns busy) to a station.

7.2.1.6.3 Information Flow

The flow diagrams show the general information flow necessary to provide the service described. Some messages that are normally present (i.e., confirmation messages, error messages, disconnect) are not shown if they are not necessary to explain the working of the service.

The flow diagram for call abandonment can be seen in figure 7-18. The call setup information, including Calling Party Number (CPN), goes across the network. The Switch transmits the call setup information (CPN) to the host computer. The caller then "Disconnects" and the host computer is informed, so it puts the number in a list for later callback. At a later time, the agent interacts with the host and selects a callback number. The agent can then either generate the call via the host or dial the number using the phone. Figure 7-19 is the flow diagram for the case where the caller receives busy or hears an announcement.

7.2.1.6.4 Network Signalling Requirements

The network signalling requirements for this service are the same as for Call Delivery using the Switch-to-Host interface (see fig. 7-16).

7.2.1.6.5 Protocol Description

The messages and protocol elements described below are only those required by the service being described. Other messages and protocol elements are not discussed if they are not used by the application being described, even through they may be required for other reasons, such as routing of the call.

7.2.1.6.5.1 Call Setup User Information

The Customer identifier can be carried from the origination to destination terminal in the **SETUP** message described in NIUF 90-301 (see Appendix A) and NIUF 90-302 (see Appendix B). The **SETUP** message is described as sent by the calling user to the network and by the network to the called user to initiate call establishment.

The Information needed to carry the Calling Party Number is found in the paragraph titled **Calling Party Number.** "The purpose of the Calling party number information element is to identify the origin of the call." The information element may say that the number is not available; the application must be able to handle this situation appropriately.

7.2.1.6.5.2 Host-Switch Messages

The necessary function required by this service is the handling of the incoming Calling Party Number.

The Host Computer messages are described in the ANS *Switch-Computer Applications Interface (SCAI)*, T1.626-1992 (Ref. [23]).

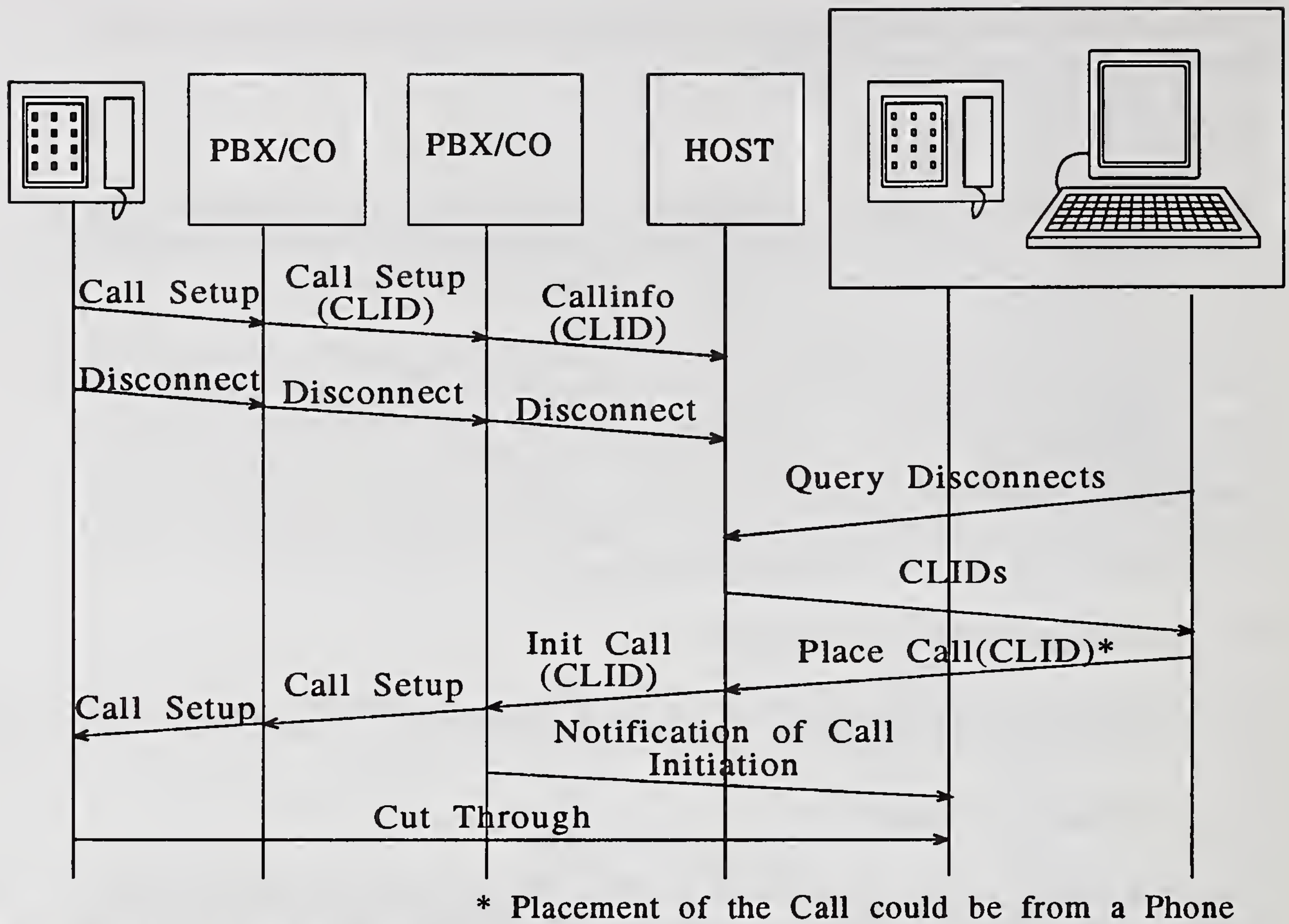


Figure 7-18. Call Back on Busy/Abandonment Service Element Information Flow Diagram—Abandonment.

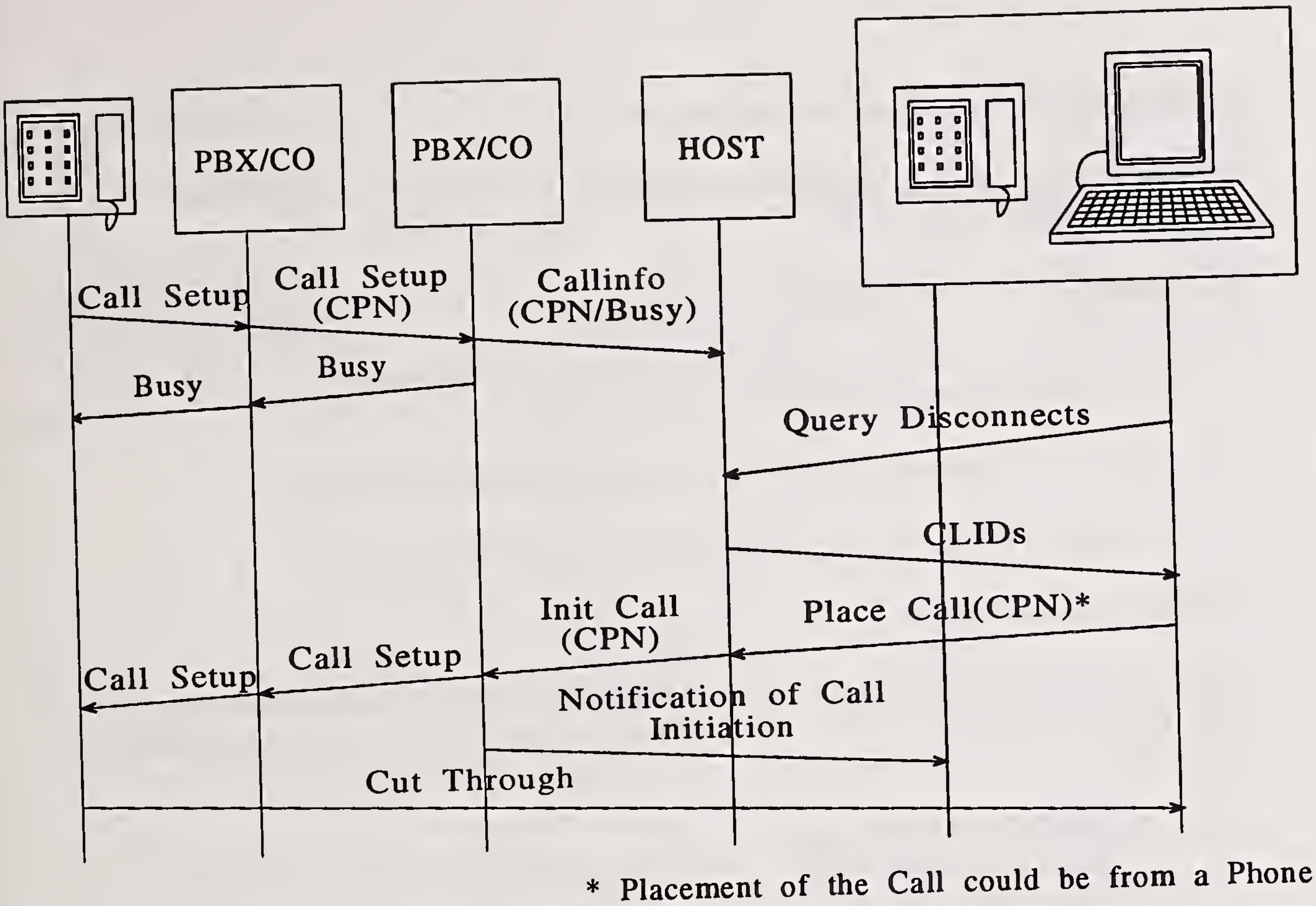


Figure 7-19. Call Back on Busy/Abandonment Service Element Information Flow Diagram—Busy.

7.2.1.7 Terminal Connectivity Service Element

This service provides connectivity between a terminal and a host using an ISDN link. This is illustrated in figure 7-20.

The sequence of events is as follows:

a. The user causes a call to be placed from the terminal to a port on the host/controller.[13]

b. Upon connection of the call the data transport protocol is initiated.

c. When the data session is complete the call is disconnected.

7.2.1.7.1 User Environment

Some of the users' descriptions of the service have specified a hardware and software environment in which the service should work. At a minimum, the service should work in the following environment:

- IBM 3270 type terminals
- An IBM-compatible host
- SNA host networks

These are minimum requirements and the actual description of the service is more general in that it will work with other terminals, hosts, and networks.

7.2.1.7.2 Information Flow

The information flow diagrams show the data that must be sent between nodes necessary to provide the service described. Signalling messages that are normally present (i.e., confirmation messages, error messages, disconnect) are shown for simplicity if they are not necessary to explain the working of the service.

The flow diagram in figure 7-21 shows the general information flow necessary to provide the described service.

---

[13]The use of some ISDN features for security (i.e., CLID) may be required, but are not part of the user application description (text or figures).

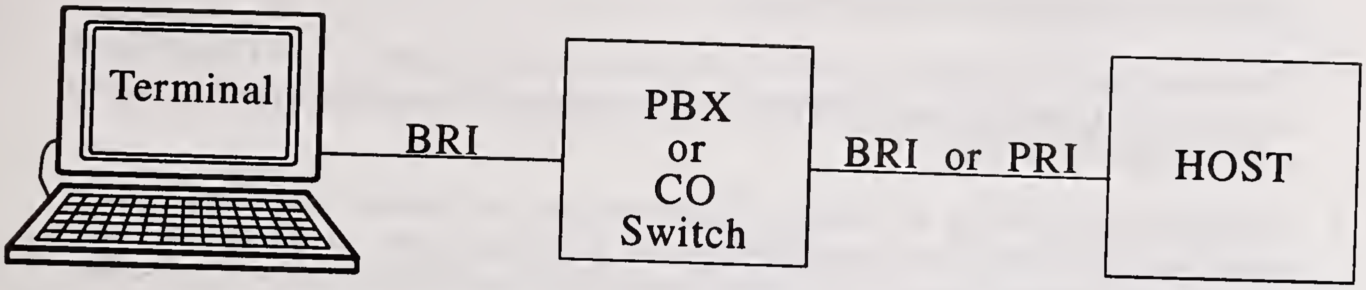


Figure 7-20. Terminal Connectivity Service Element—Description.

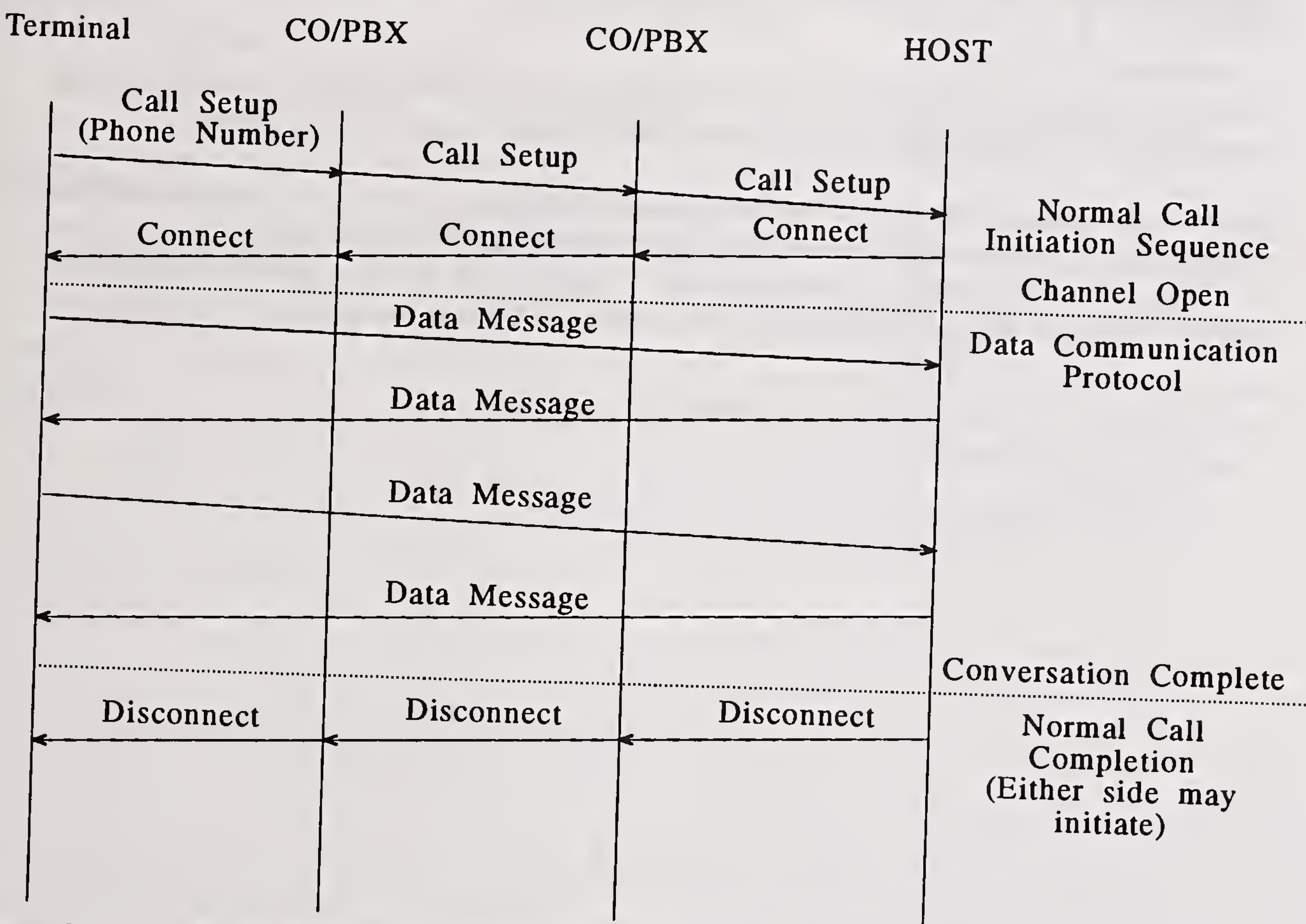


Figure 7-21. Terminal Connectivity Service Element Flow Diagram.

7.2.1.7.3 Network Protocol Requirements

The network protocol requirements for this service can be seen in figure 7-20. As shown in that figure, there must be ISDN connectivity between the terminal and the point where it is attached to the computer or controller.

The higher layer protocols for carrying the user data are not described here. The Network Interconnectivity Profile Team should provide the higher level protocol specification when completing Application Profiles for the User Application Requirements Data Forms numbered 830008, 830009, 960009 (Refs. [40, 41, 42]).

7.2.1.7.4 Protocol Description

The messages and protocol elements described below are only those required by the service being described. Other messages and protocol elements are not discussed if they are not used by the application being described, even though they may be required for other reasons, such as routing of the call.

The protocol described in NIUF 90-301 (see Appendix A) and NIUF 90-302 (see Appendix B) can be used for the setup and breakdown of the call being made to carry the data protocol.

The only information element that may have a direct bearing on the service is in the **SETUP** message described as "sent by the calling user to the network and by the network to the called user to initiate call establishment." The information element is the Bearer Capability Information Element. The user can ask for the appropriate information transfer capability and transfer mode.

7.2.1.8 Protocol Summary and Status

The following is a summary of the protocol requirements of the Incoming Call Management Application.

Table 7-1. Protocol Requirements for Incoming Call Management Application Profile

Application Service Element	Protocol Element	Document
Call Transfer With Associated Data	User-User	NIUF 90-301 & NIUF 90-302 Implementation Agreements
	Call Transfer	T1LB 340 (Ref. [22])
	Host-Switch	ANS T1.626-1992 SCAI, (Ref. [23])
Call Delivery With Associated Data	Calling Party Number	NIUF 90-301 & NIUF 90-302 Implementation Agreements
	Host-Switch	ANS T1.626-1992 SCAI, (Ref. [23])
Terminal Connectivity	Bearer Capability	NIUF 90-301 & NIUF 90-302 Implementation Agreements
	Higher Layer	Network Interconnectivity Family
Call Back	Calling Party Number	NIUF 90-301 & NIUF 90-302 Implementation Agreements
	Host-Switch	ANS T1.626-1992 SCAI, (Ref. [23])

7.2.2 Remote Agent Application Profile

7.2.2.1 User Description

7.2.2.1.1 Current Environment

The current application is one in which a caller dials a phone number (e.g., 800, 900, POTS) and that call gets routed to an Automatic Call Distributor (ACD) or a set of ACDs by the network (see fig. 7-22). The ACD selects an available agent for that type of call and delivers the call to the selected agent. The agent is normally co-located with the ACD, and the ACD can easily detect the state of the agent since the agent is directly attached to the ACD. The requirements for this application are described in the Incoming Call Management Profile (section 7.2.1), and are relevant for the Remote Agent application. The requirements defined within this profile focus on remoting the agent station.

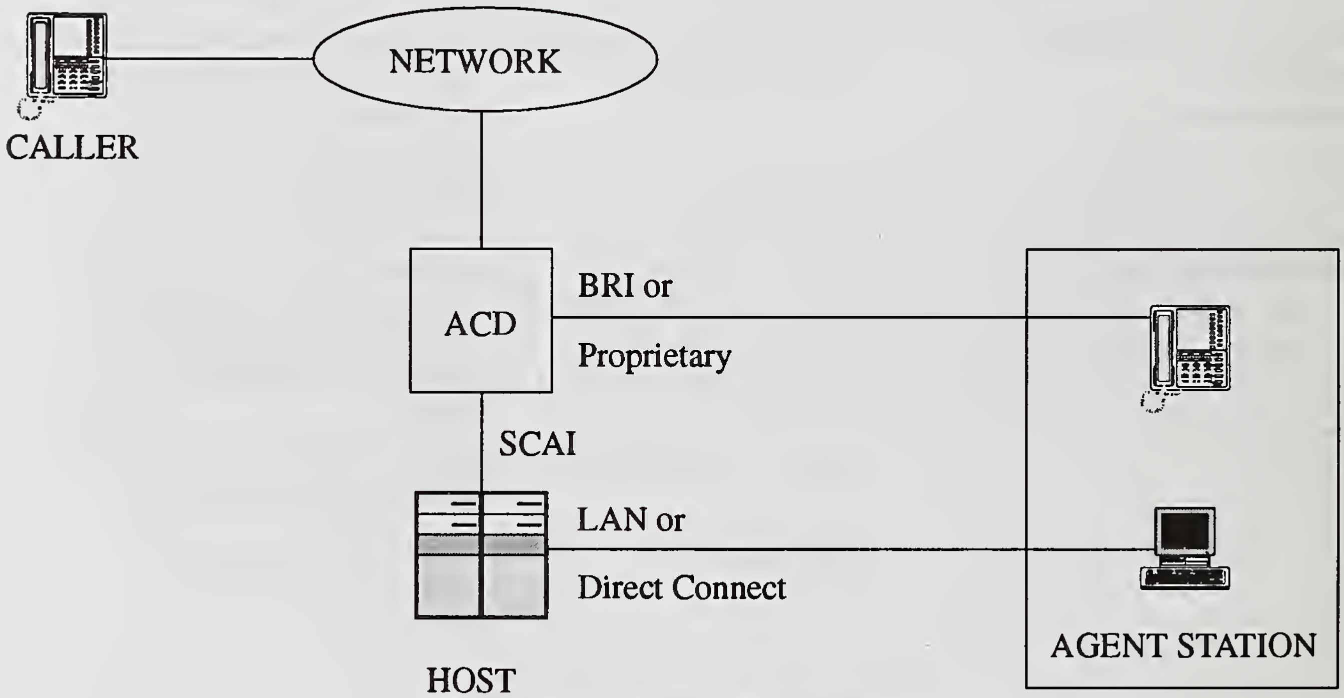


Figure 7-22. Current Architecture.

7.2.2.1.2 Remote Agent Environment

This application requires the agent to not be co-located with the premises ACD. In other words, the agent is required to provide the same level of service from a remote location. The remote location may be a residence (the agent's home), a service bureau, or a branch office (see fig. 7-23). The ISDN aspect of this application is that the remote agent will be provided connectivity via a BRI link. The agent will access the same host as the directly connected agent and be able to receive the same functionality from the telecommunications system.

7.2.2.1.3 Potential Benefits

By offering an "agent-at-home" environment the following benefits may be realized:

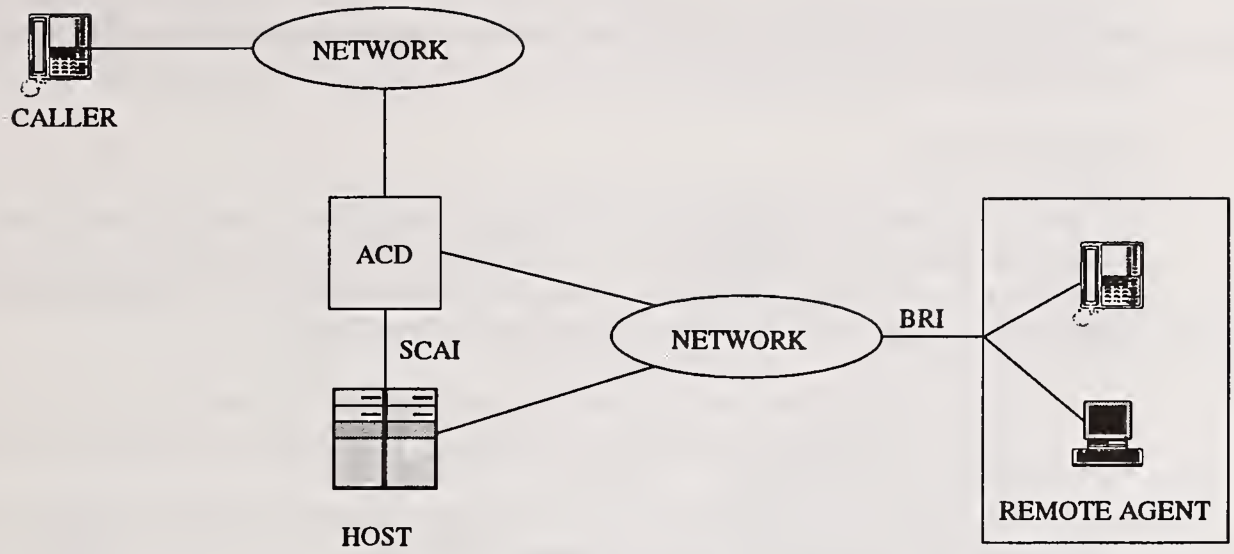


Figure 7-23. Remote Agent Architecture.

- Greater flexibility and expanding hours of coverage, through use of temporary/part-time agents working from their homes. The quality of service would improve because

  - peak calling periods could be handled efficiently
  - after hours answering service could be offered.

- Cost savings through:

  - space savings
  - employee retention will result in lower recruitment and training costs.

- Greater productivity of current workforce, because of a more congenial working environment.

- Effective utilization of a larger workforce by offering agent-at-home to

  - temporarily disabled employees
  - mobility impaired persons
  - retirees
  - contract personnel

7.2.2.1.4 Specific Requirements

The requirements in the sections to follow are in addition to those found in the Incoming Call Management Profile (section 7.2.1). This section is broken up into requirements from each possible user's perspective. In certain cases these views will overlap since multiple users may require the same service. The following is the set of users of this application: caller, agent, and agent management. In addition to the users' requirements, this section also describes the requirements for security and additions for the future.

7.2.2.1.4.1 Caller

The general requirement from the caller's perspective is that the caller gets the same service independent of the location of the agent. There may be minor additional delays, due to call setup times, but these should be slight.

7.2.2.1.4.2 Agent

The general requirement from the agent's perspective is that he/she should be able to do his/her job with the minimum of retraining. There may be differences in the types of calls they can handle, since bandwidth and terminal expense may make certain inquiries uneconomical (e.g., display of x rays, high resolution video). Specific functional needs:

- Agent Control Functions: Log in, Log Off, Make Busy, Alarm.
- Call Control Functions: Connect to Customer, Disconnect with Customer, Hold, Call Transfer, Conference.
- Displays: The agent's phone should display the same information available to the directly connected agent (e.g., customers' calling line id).
- Associated Data: The agent should receive the same associated data provided by the Incoming Call Management Application Profile (section 7.2.1), for incoming and outgoing calls. The agent should be able to query, as well as update, the database.

7.2.2.1.4.3 Agent Management

Agent Management currently has capabilities to monitor agents' activities, as well as listen to ongoing conversations.

- Real-Time Activity Monitoring: The supervisor needs to silently monitor agents and have the ability to tape agent conversations. The supervisor should be able to monitor the voice and data connection.
- Delayed monitoring from log files
- Barge in capability
- Update ACD groups with current agent lists
- Common messages from Voice Response Units independent of agent location
- Agent Management reports: The supervisor should be able to receive management reports on each agent, including how many calls an agent handled, how quickly agents responded to calls, length of conversations, agent availability, and call-abandon rate.
- Audit trail: The supervisor should be able to verify which customer accounts the agent retrieved.

7.2.2.1.4.4 Security

There are concerns on security of both the voice and data connections. The requirements are for further study.

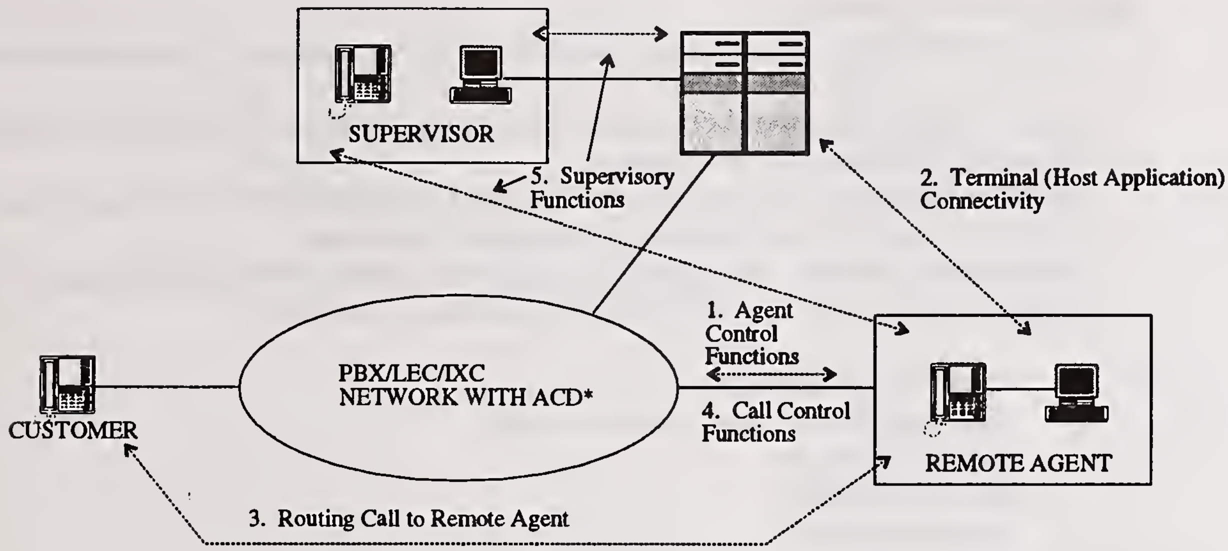
7.2.2.1.4.5 Future Requirements

The following are needs that users foresee for the near future:

- Incoming Caller ID delivered to host desirable for automatic access to customer accounts.
- Image access from the remote site should be possible.

7.2.2.2 Remote Agent Application Processes

This section breaks down the Remote Agent Application into its service elements. The relationship between these service elements can be found in figure 7-24.



*Note: The ACD and MIS functions may be provided by attached processors to the appropriate network.

Figure 7-24. Remote Agent Application Service Elements.

1. Agent Control Functions

   The functions described in this category, namely login, available, logoff, and make busy, are functions invoked by the agent independent of a specific call.

2. Terminal Connectivity

   The agent connects its data terminal to the host.

3. Routing Call to Remote Agent

   Depending on the location of the ACD (premises or public network) that the agent will be logging into, the call can be routed to the Home Agent in several different ways. These methods are discussed in detail in section 7.2.2.6.

4. Call Control Functions

   This category of functions describes functions invoked by an agent that will impact a specific call. These functions are:

   Connect to Customer: the agent invokes this function when he/she wishes to answer an incoming call.
   Hold: the agent invokes this function when he/she wishes to put the call on hold.
   Transfer: the agent invokes this function when he/she wishes to transfer the call to another end point.

Conference: the agent invokes this function when he/she wishes to conference one or more parties into the call.
Disconnect: the agent invokes this function when he/she wishes to clear the call to the end point. The connection from the ACD to the agent's telephone set remains active.

5. Agent Supervisory Functions

The functions in this category are invoked by the agent's supervisor. These functions are:

Agent Status: the supervisor invokes this function when he/she wishes to obtain the status of a specific agent or all agents.
Silent Monitoring: the supervisor invokes this function when he/she wishes to quietly listen-in on an active call between the agent and a customer.
Management Reports: the supervisor may obtain a series of management reports for a specific agent. The report may contain the following information:

- number of calls handled
- how quickly the agent responded to calls
- length of each call
- agent availability
- call-abandon rate

7.2.2.3 Service Logic

Figures 7-25 and 7-26 describe the sequence of the above service elements to provide a Remote Agent Application. Note that the Terminal Connectivity flow is optional, since not all applications may need a data connection from the agent to the premises host.

7.2.2.4 Agent Control Functions

7.2.2.4.1 Description

The agent control functions are described below:

• **Login**: invoked by agent to establish an active session between the ACD and the agent's telephone set.
• **Available**: invoked by agent to inform the ACD that the agent is ready to receive incoming calls.
• **Make busy**: invoked by agent to inform the ACD that the agent is not available to receive incoming calls, even though the agent is not on an active call.
• **Logoff**: invoked by agent to terminate the session between the ACD and the agent's telephone set.

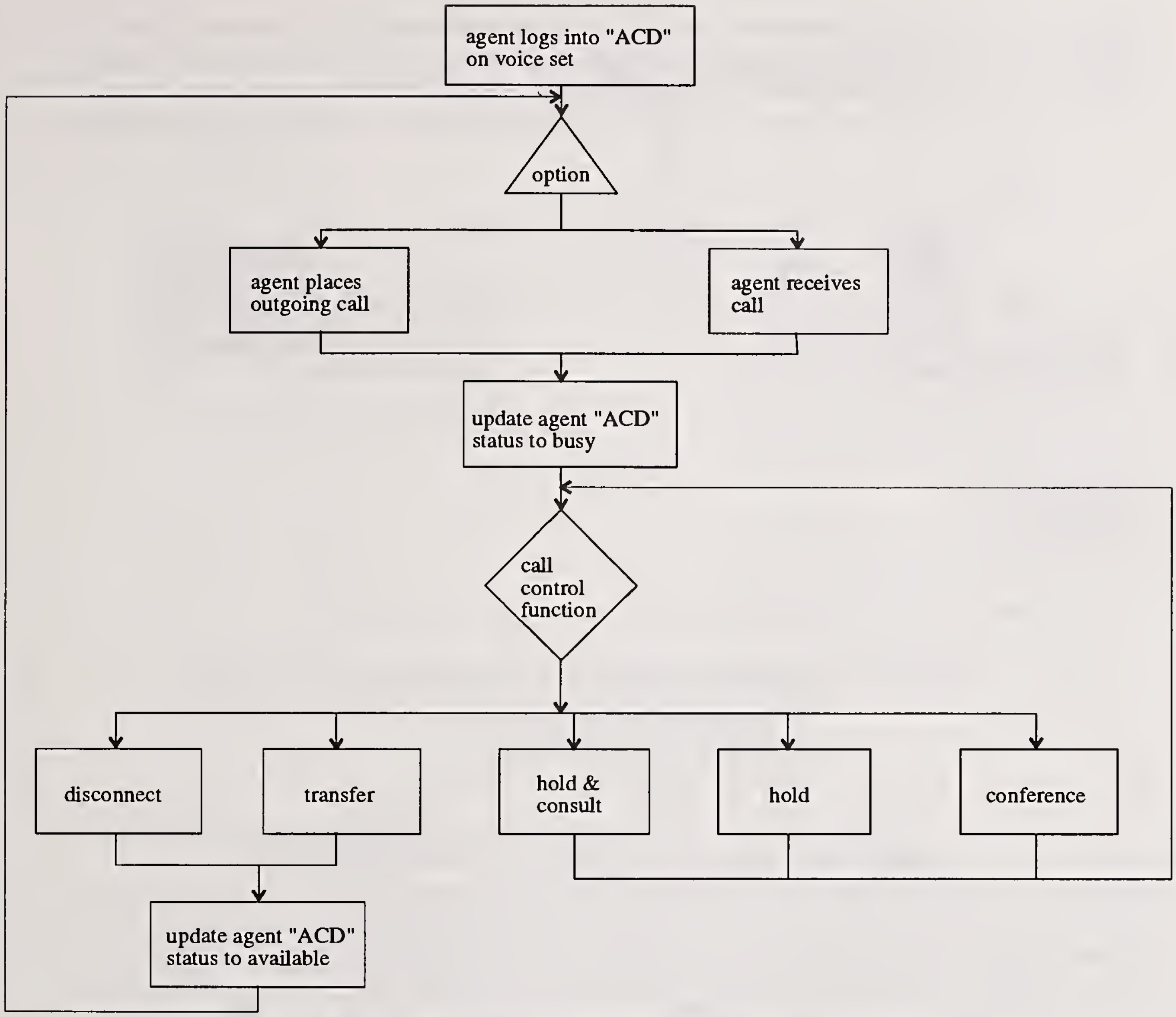


Figure 7-25. Service Logic Flow for Voice Connectivity.

7.2.2.4.2 Architectures

The information described above may be conveyed to the ACD in one of two ways:

a. voice terminal (inband): the agent's telephone set will come equipped with function keys, one for each of the agent control functions described. The agent simply depresses the required key at the appropriate time and a corresponding signal is sent to the ACD, in band.

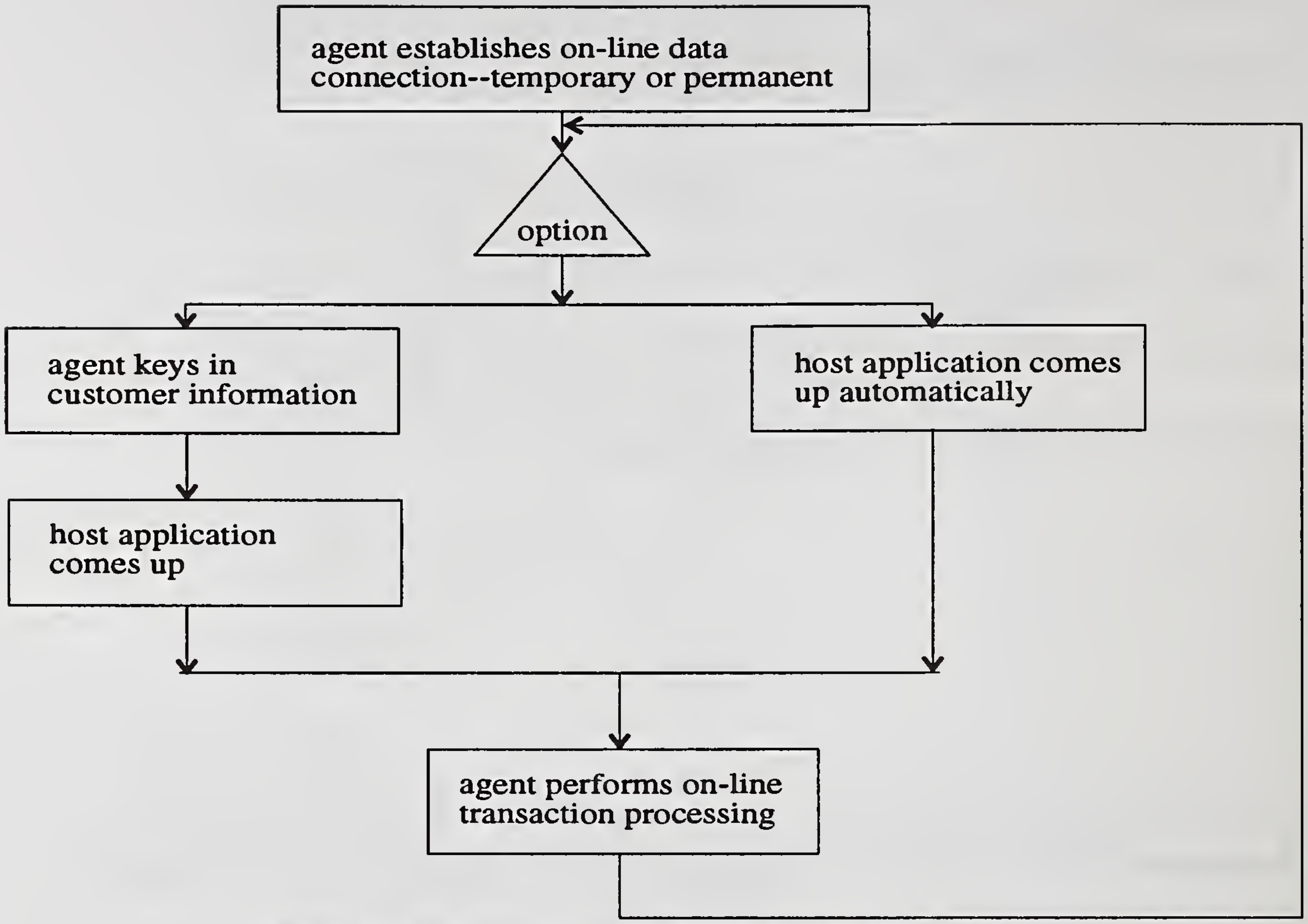


Figure 7-26. Service Logic Flow for Terminal Connectivity.

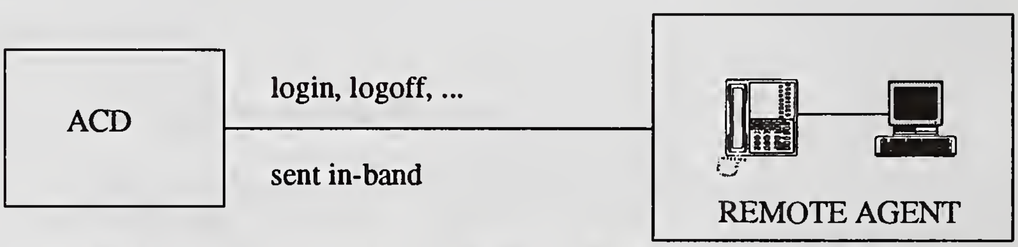


Figure 7-27. Architecture A—Agent Control Functions Sent In-Band.

b. voice terminal (out of band): the agent's ISDN telephone set will establish a D channel connection with the ACD and transmit the required information on that channel. This may be done using User-to-User Information or X.31 (Ref. [29]).

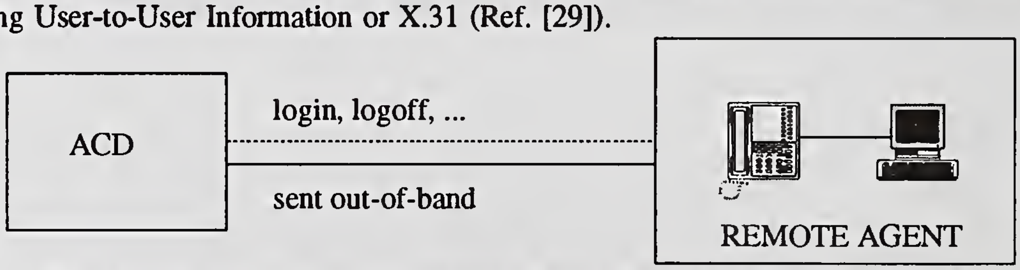


Figure 7-28. Architecture B—Agent Control Functions Sent Out-Of-Band.

c. data terminal: the agent's data terminal may have a user interface that allows the agent to signal the agent control function to the host. In this case, the host must be connected to the ACD via a Switch-Computer Application Interface (SCAI). Once the host receives the agent status from the agent's data terminal, it will notify the ACD.

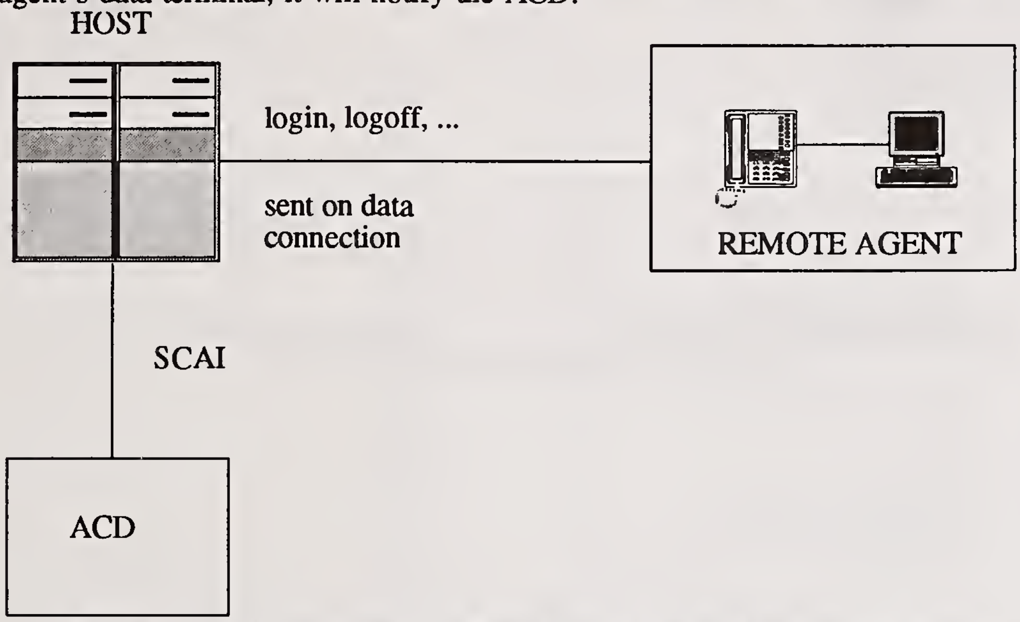


Figure 7-29. Architecture C—Agent Control Functions Sent via Data Connection.

7.2.2.4.3 Information Flow

The information flow diagrams show the data, that must be sent between nodes, necessary to provide the service described. Signalling messages that are normally present (i.e., confirmation messages, error messages, disconnect) are not shown for simplicity if they are not necessary to explain the working of the service. The information flow for Architecture A is shown in figure 7-30.

In Architecture A, the Remote Agent establishes a call to the ACD, whether the ACD is located on the premises or in the public network. Once the voice connection is established, the Remote Agent keys in its status which will be transmitted using Dual Tone Multi-Frequency (DTMF) signalling. The Remote Agent may also establish a data connection for data entry.

The information flow for Architecture B is shown in figure 7-31. In Architecture B, the Remote Agent simply keys in its status. The status will be transmitted on the already existing D channel connection between the agent's voice terminal and the ACD. Once the agent becomes available to receive a call, the ACD will send the call to the agent.

The information flow for Architecture C is shown in figure 7-32. In Architecture C, the Remote Agent enters its status on the data terminal. The data terminal sends the agent status information to the host on premises, which in turn will transmit this information to the ACD. The ACD, based on this information, will determine which agents are available to receive calls.

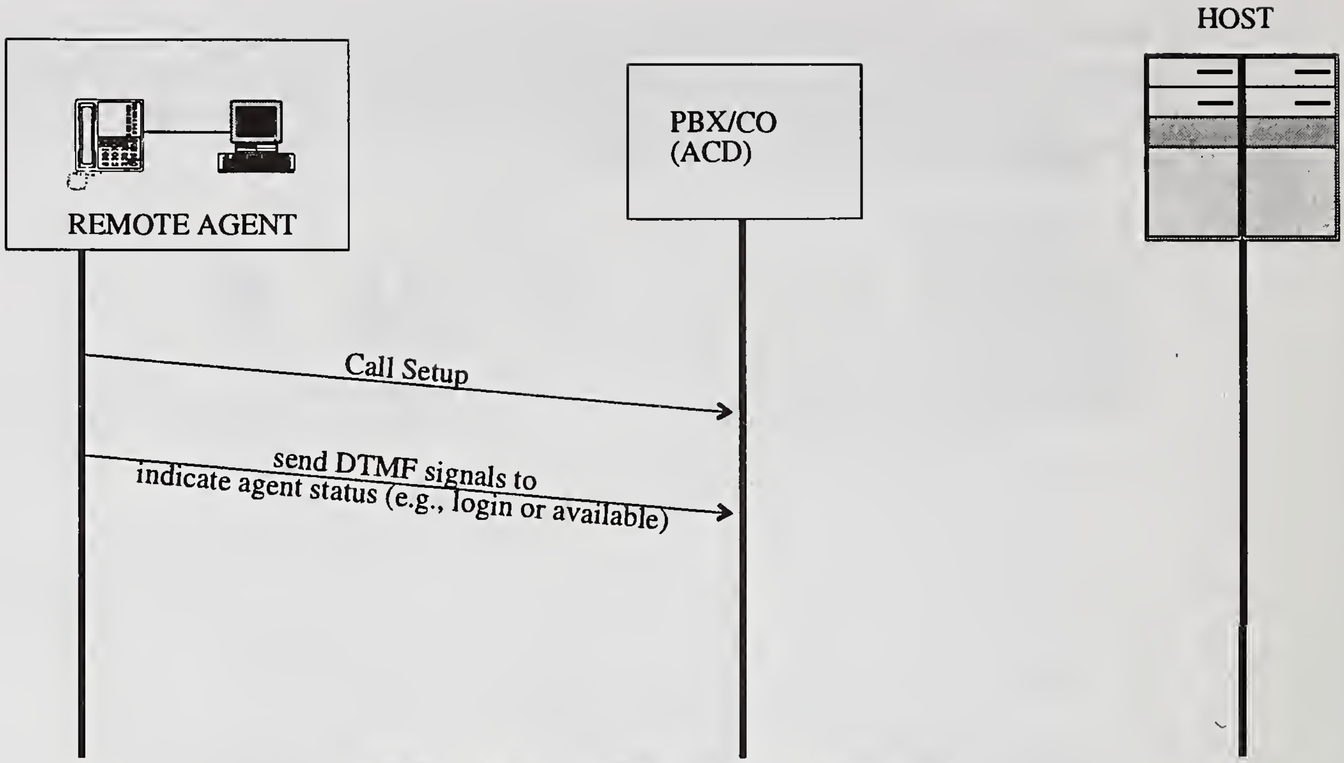


Figure 7-30. Information Flow for Architecture A.

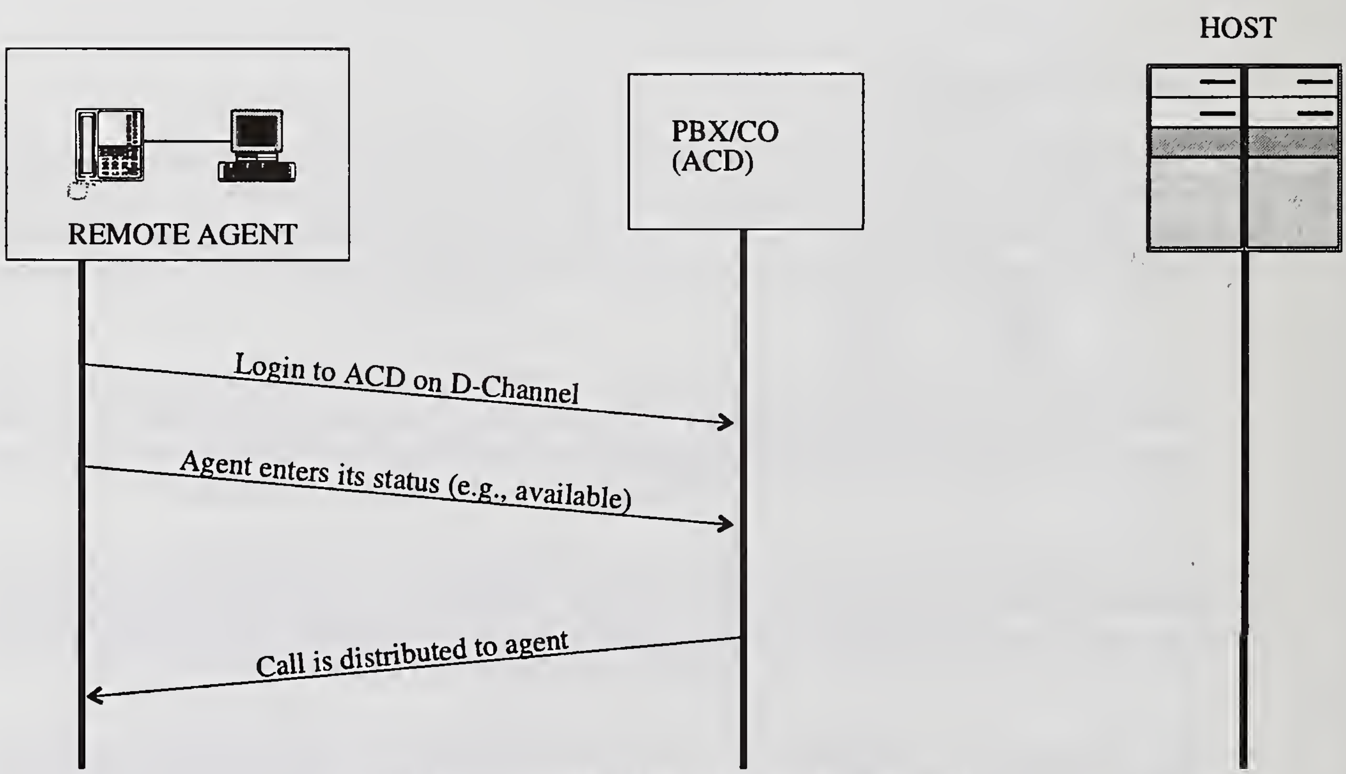


Figure 7-31. Information Flow for Architecture B.

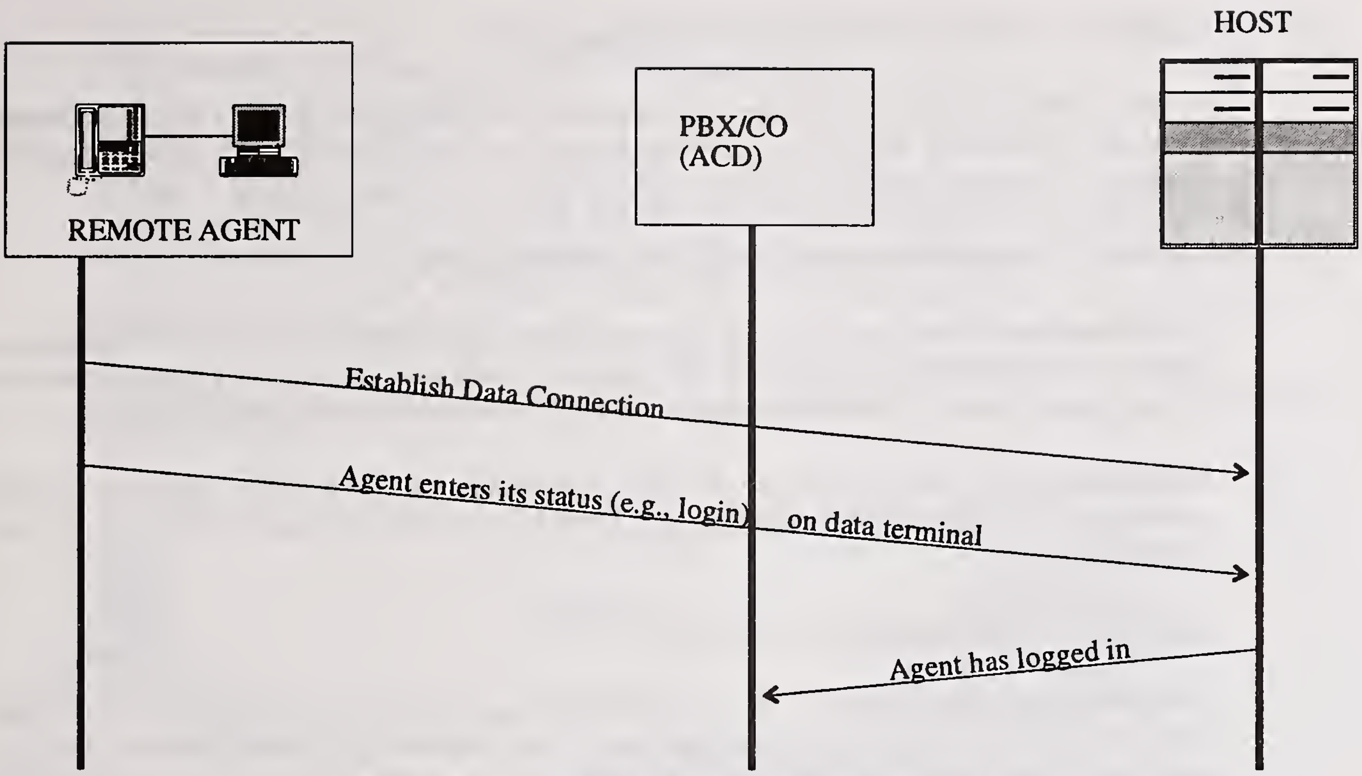


Figure 7-32. Information Flow for Architecture C.

7.2.2.4.4 Network Signalling Requirements—Protocol Identification

The network signalling requirements for providing this service with each architecture are shown below. Figure 7-33 shows the requirements for Architectures A and B. Figure 7-34 shows the requirements for Architecture C.

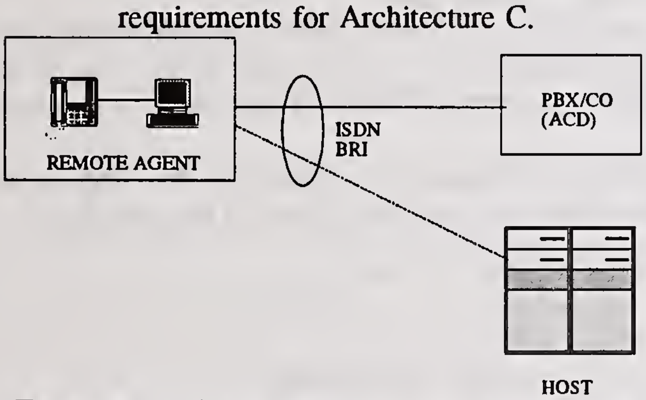


Figure 7-33. Network Signalling Requirements for Architectures A and B.

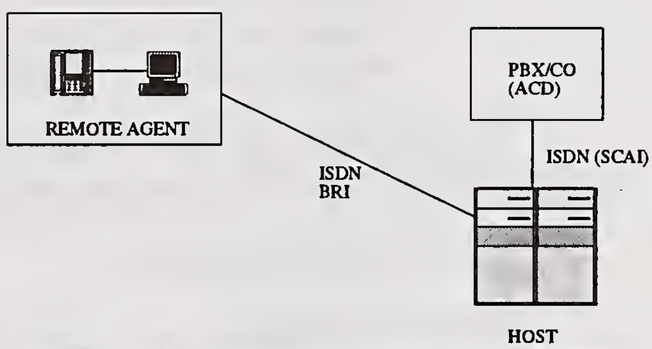


Figure 7-34. Network Signalling Requirements for Architecture C.

7.2.2.4.5 Protocol Description

The messages and protocol elements described below are only those required by the service being described. A description is provided for each architecture discussed above.

7.2.2.4.5.1 Voice Terminal (Inband)—Architecture A

In the ISDN case, the voice connection would be established using the Call Establishment procedures as defined in NIUF 90-301 (Appendix A). In the POTS environment, the voice connection would be established without messaging, so no message protocol is needed.

7.2.2.4.5.2 Voice Terminal (Out-of-Band)—Architecture B

The information element that can carry the out-of-band agent status is the User-User information element. This information is carried to the end point, in this case the ACD, without interpretation by transmitting nodes. There are no restrictions on the contents of the user information.

Alternatively, X.31 (Ref. [29]) can be used to transmit the agent status information. The information would be carried as user data. The X.31 protocol is defined in NIUF 89-320 (see section 4.1.4.2).

7.2.2.4.5.3 Data Terminal—Architecture C

The data connection to the host would be established using X.31 as defined in NIUF 89-320 (see section 4.1.4.2). Once the host receives the agent status information it would send it to the ACD using the SCAI protocol. The host computer messages are defined in the ANS *Switch-Computer Applications Interface (SCAI)*, T1.626-1992 (Ref. [23]). The functionality that is provided by SCAI is as follows:

- The ACD needs to have a monitor request established to the host that specifies that the ACD would like to receive any change that occurs in agent status. The ACD would specify which agents it would like to monitor.

- When the host receives a X.31 message from the Remote Agent regarding a change in its status, the host will send an Event Report to the ACD informing the host of the change. The Event Report needs to include the agent's id and the new status of the agent.

Note that SCAI, the Switch Computer Application Interface, is defined in the ANS SCAI Document (Ref. [23]). The added functionality needs to be defined as part of this document.

7.2.2.5 Terminal Connectivity

7.2.2.5.1 Description

This service provides connectivity between a terminal and a host. The data session may use an ISDN or POTS connection. The sequence of events is as follows:

a. The user causes a call to be placed from the terminal to a port on the host.
b. Upon connection of the call the data transport protocol is initiated.
c. When the data session is complete the call is disconnected.

7.2.2.5.2 Architectures

If the Remote Agent has ISDN access for the agent control functions, then the B or D channel may be used to establish a data session.

If the Remote Agent has POTS access, a circuit switched connection should be used. The agent, using a modem, would dial up the host and be connected.

7.2.2.5.3 Information Flow

The information flow diagrams show the data, that must be sent between nodes, necessary to provide the service described. Signalling messages that are normally present (i.e., confirmation messages, error messages, disconnect) are not shown for simplicity if they are not necessary to explain the working of the service.

The flow diagram in figure 7-35 shows the general information flow necessary to provide the described service.

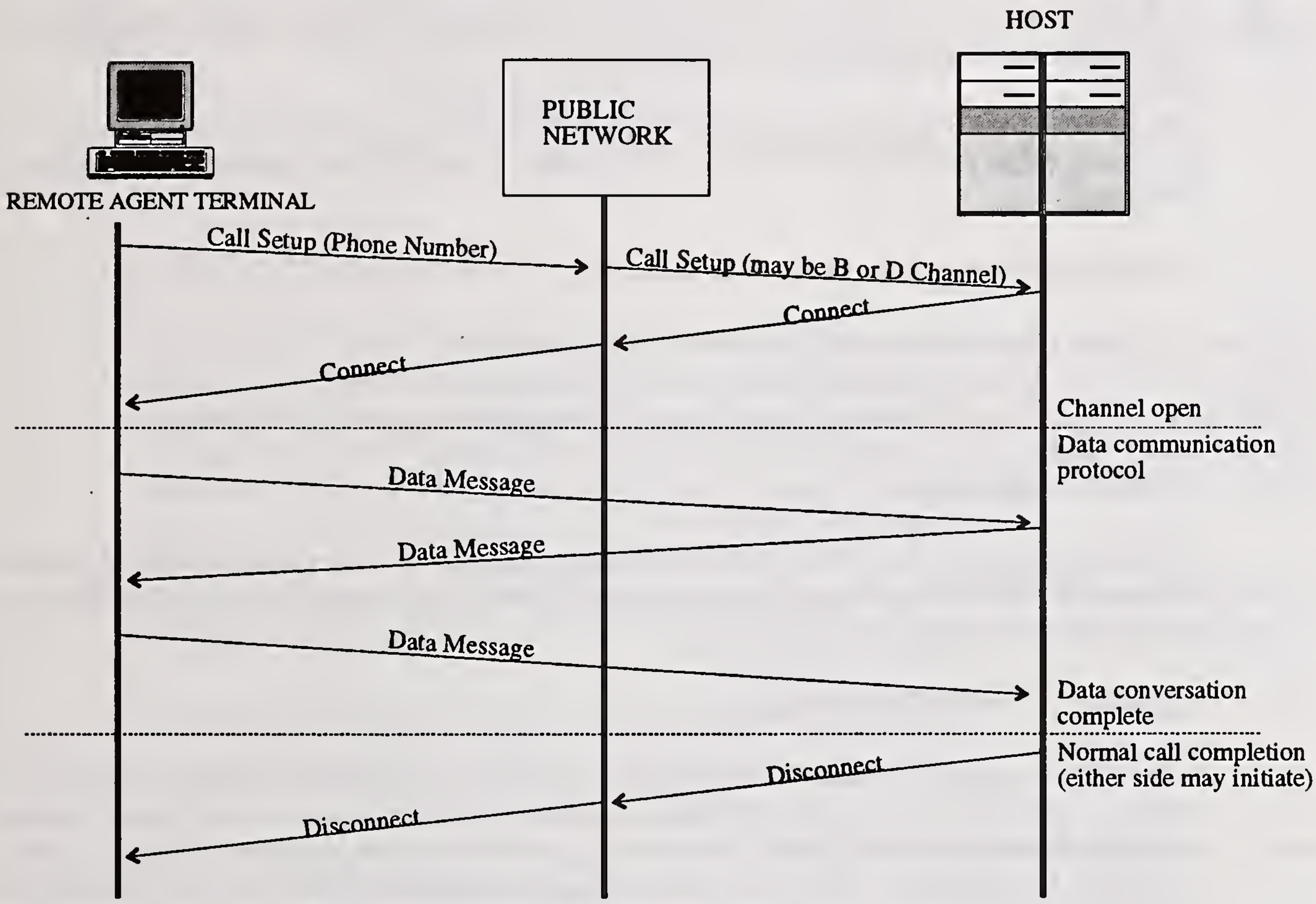


Figure 7-35. Information Flow for Terminal Connectivity.

7.2.2.5.4 Network Signalling Requirements—Protocol Identification

The network protocol requirements for this service are shown in figure 7-36.

7.2.2.5.5 Protocol Description

The protocol described in NIUF 90-301 and NIUF 90-302 (see Appendices A and B) can be used for the setup and breakdown of the call being made to carry the data protocol, in the case of ISDN access.

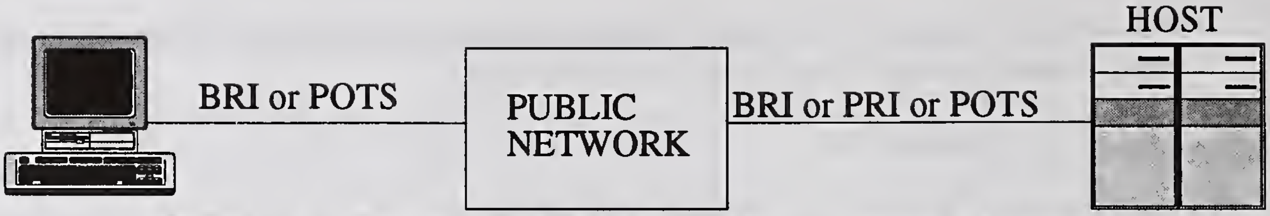


Figure 7-36. Network Signalling Requirements for Terminal Connectivity.

7.2.2.6 Routing Call to Remote Agent

7.2.2.6.1 Description

This service describes how a call may be routed to a Remote Agent, once the Remote Agent has logged into the ACD and is ready to receive calls.

The ACD that the Remote Agent logs into may be located either at the customer premises or in the central office of the public network. The location of the ACD will determine how the calls are routed.

In either case the sequence of events is as follows:

a. The incoming call must be received by the ACD.
b. The ACD will determine which agent should receive the call.
c. Once the agent is selected the ACD will connect the call to the agent.

7.2.2.6.2 Architectures

As mentioned above, the ACD may be located on the premises or in the Central Office. A Central Office ACD solution does not require a premises PBX/ACD as indicated in figure 7-38; however, a user may require integration of the two.

7.2.2.6.2.1 Premises-Based ACD

If the ACD is located on premises, the call enters the ACD or PBX as the call center environment requires. The ACD, using its call distribution algorithm, determines which of the agents that are logged in are available to take a call. This set of agents includes both agents working in the office and agents working from a remote site. Once the agent is selected, the PBX or ACD connects the call to that agent. If the Remote Agent has ISDN access, and is using only the D-channel to transmit its status to the ACD, the ACD/PBX will have to initiate a call to the Remote Agent and then connect the call to the agent.

The architecture for this scenario is shown in figure 7-37.

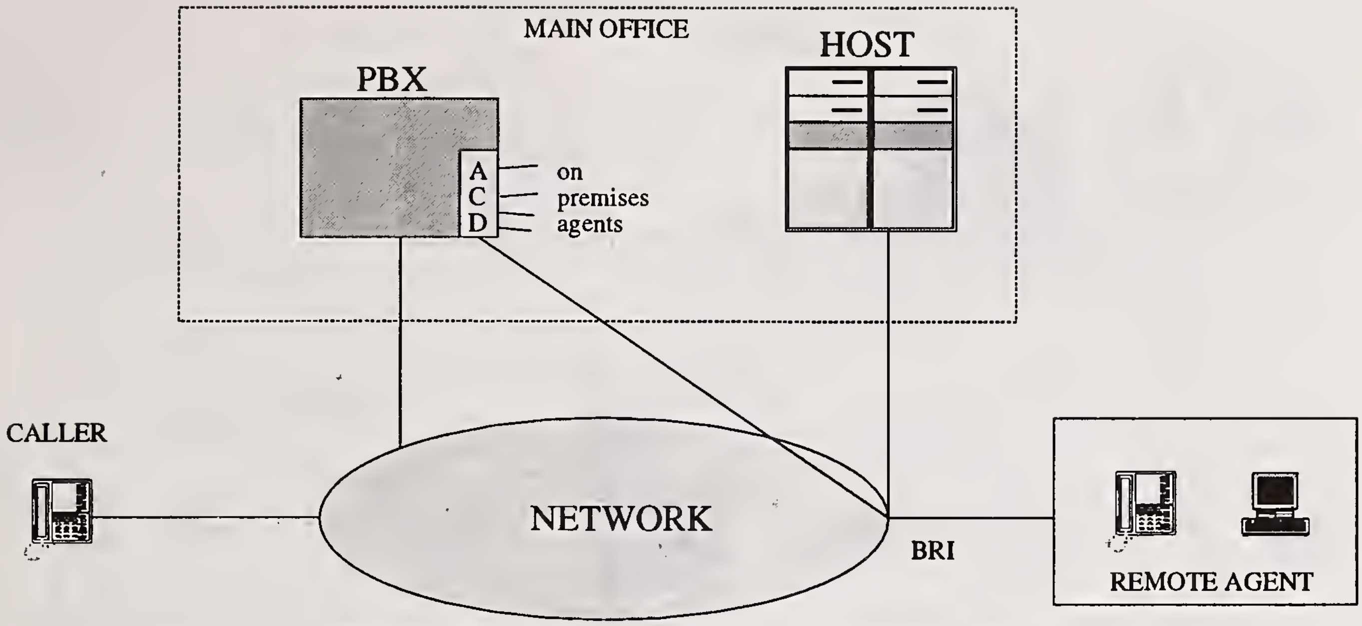


Figure 7-37. Architecture for Premises-Based ACD.

7.2.2.6.2.2 Central Office ACD

If the ACD is located in the Central Office, the calls that are to be routed to the Remote Agents will enter the Central Office instead of the premises PBX. The Central Office ACD, using its call distribution algorithms, will determine which Remote Agent is to receive this call. After selecting the agent, the Central Office will connect the call to the agent. If the Remote Agent has ISDN access and is using the D-channel to transmit its status, the Central Office will have to initiate a call to the Remote Agent before connecting the caller to the agent.

The Central Office should have a capability available that if all the Remote Agents are busy, the call can be overflowed to the premises ACD. This will allow efficient handling of all calls.

The architecture for this scenario is shown in figure 7-38.

7.2.2.6.3 Information Flow

The information flows for both the premises-based ACD and the Central Office ACD are shown in figures 7-39 and 7-40, respectively.

7.2.2.6.4 Network Signalling Requirements—Protocol Identification

The network signalling requirements are shown in figure 7-41. As shown in the figure, the caller may call over an ISDN connection or a POTS connection.

If the Remote Agent is logged into the premises ACD, the access may be either POTS or ISDN as indicated in previous sections. The connection between the Public Network and the premises ACD may be any appropriate protocol.

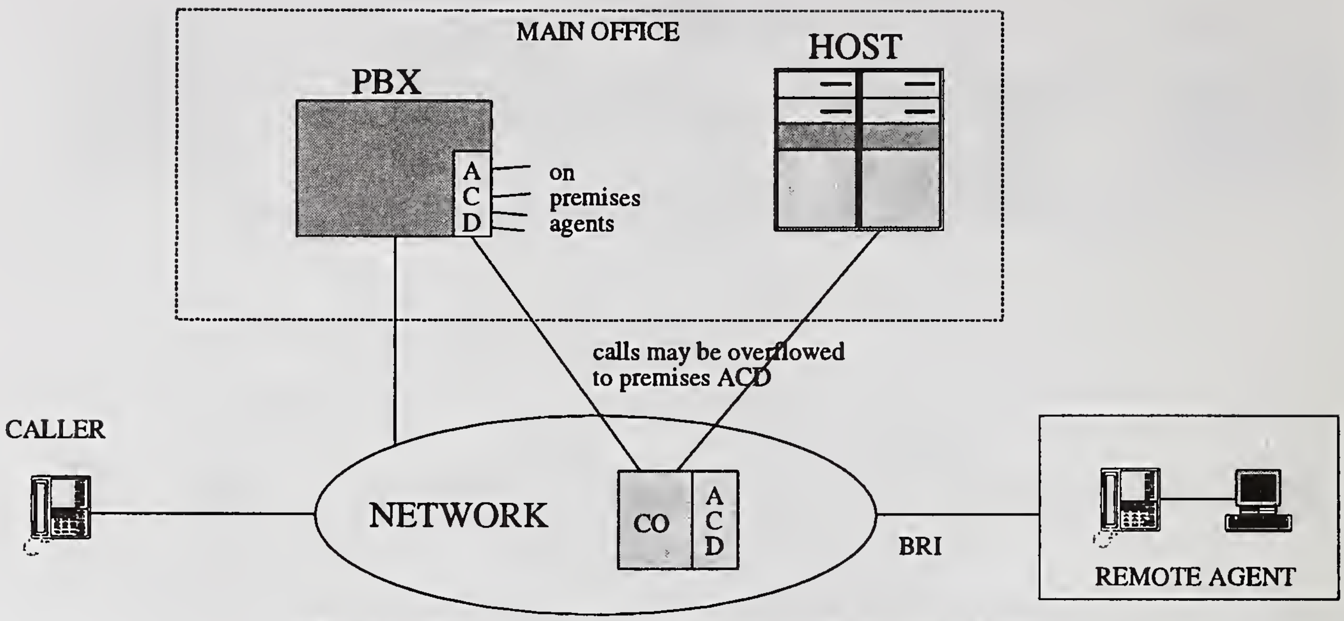


Figure 7-38. Architecture for Central Office-Based ACD.

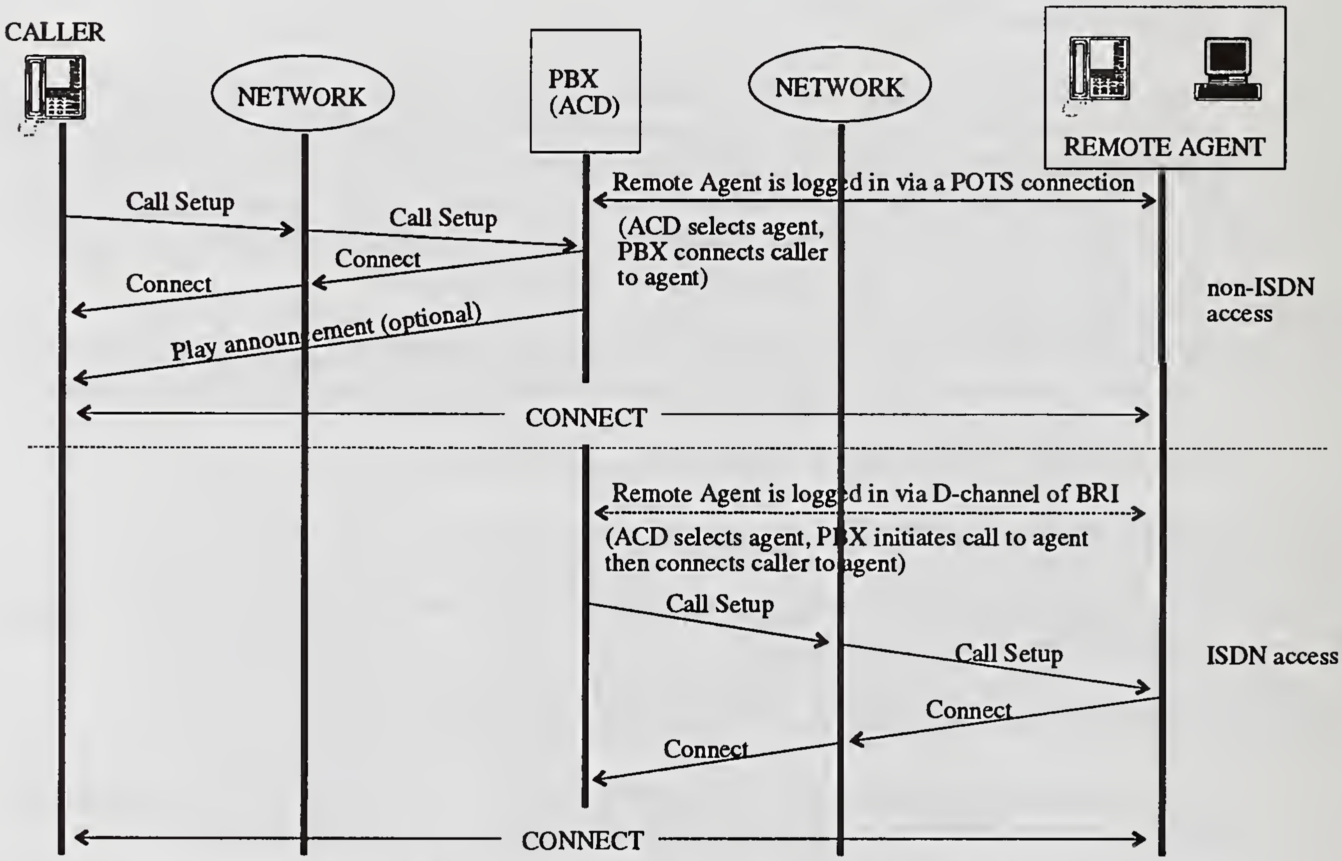


Figure 7-39. Information Flow for Premises-Based ACD.

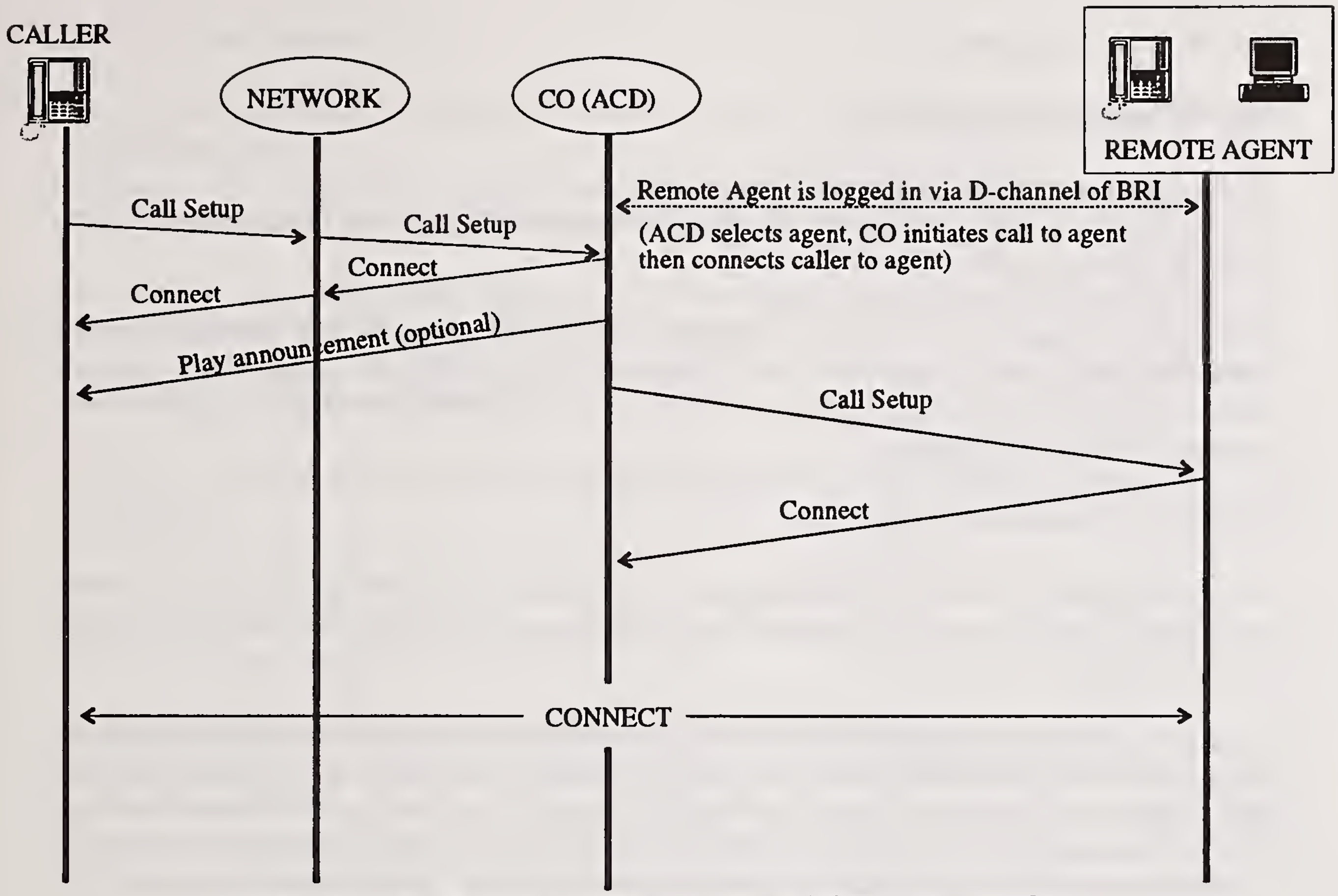


Figure 7-40. Information Flow for Central Office-Based ACD.

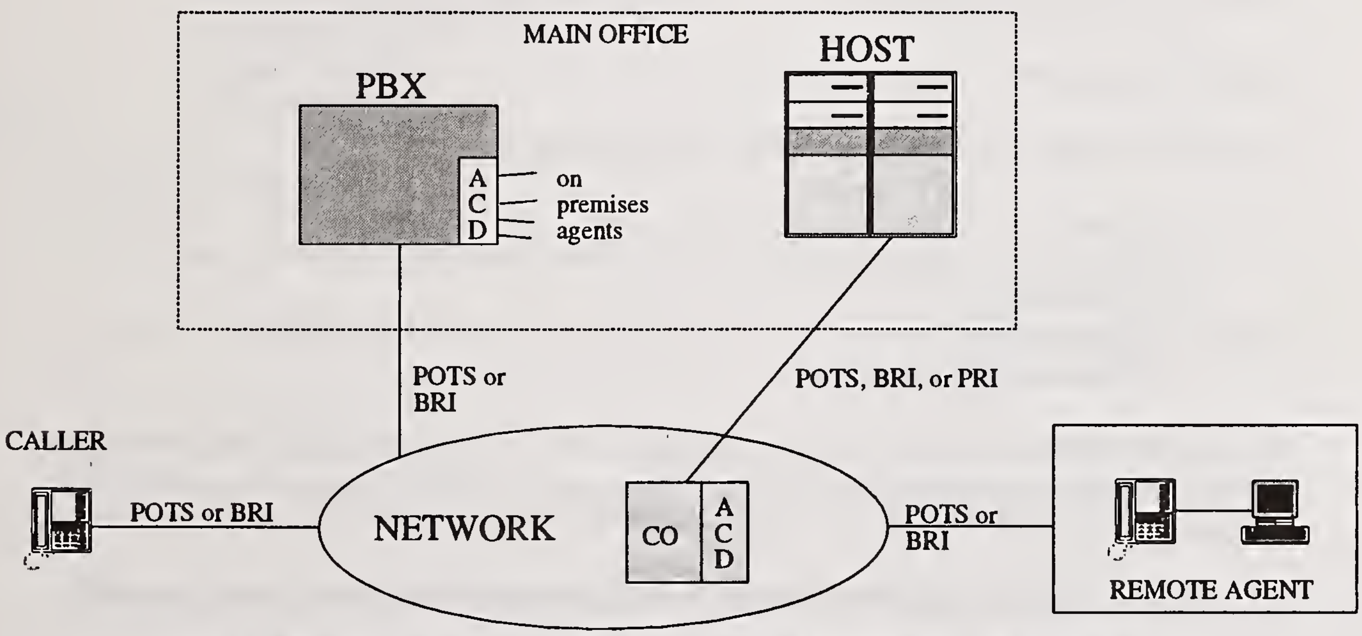


Figure 7-41. Network Signalling Requirements for Routing Call to Agent.

7.2.2.6.5 Protocol Description

7.2.2.6.5.1 Premises-Based ACD

In the case where the Remote Agent is logged into the premises ACD via a POTS connection, when a call enters the premises ACD, the ACD selects an available agent. Then the PBX simply connects the call to the agent.

If the agent is logged into the premises ACD via an ISDN connection, where the D-channel is used to transmit agent status, then the PBX must establish a call to the Remote Agent using procedures defined in NIUF 90-301 (see Appendix A). Once the connection is established, the PBX will connect the caller to the agent.

7.2.2.6.5.2 Central Office ACD

In the case where the Remote Agent is logged into the Central Office ACD, it must be decided by subscription which calls will be directed to the premises and which calls will be directed to the Central Office.

Once the call enters the Central Office, the ACD will select an available agent and initiate a call to the agent using NIUF 90-301 (Appendix A) procedures. Once the call is established the switch will connect the caller to the agent. While the ACD selects an agent, the switch may choose to play announcements to the caller. The announcements should terminate just before the caller is connected to the agent. In addition, some switches may wish to provide ringback to the caller before the agent answers the call.

7.2.2.7 Call Control Functions

7.2.2.7.1 Description

The Remote Agent must have access to the following features:

- Hold
- Transfer
- Conference
- Connect with Customer
- Disconnect with Customer

If the agent is directly connected to the premises switch, the premises switch will offer these features. Access to these features will be via in-band tones for a POTS connection and via ISDN messages for an ISDN connection.

If the agent is connected to the Central Office ACD, the Central Office will offer these features.

7.2.2.7.2 Architectures

The architectures for call control functions are the same as the architectures for the agent control functions.

7.2.2.7.3 Information Flow

The information flows for call control functions are the same as the information flows for the agent control functions.

7.2.2.7.4 Network Signalling Requirements—Protocol Identification

The network signalling requirements for call control functions are the same as the network signalling requirements for the agent control functions.

7.2.2.7.5 Protocol Description

The ISDN protocol for accessing the call control functions can be found in NIUF 90-301 (see Appendix A).

7.2.2.8 Agent Supervisory Functions

7.2.2.8.1 Description

This service allows a supervisor to monitor agents and receive management reports on the agents. Specifically, a capability called silent monitoring allows a supervisor to listen to ongoing conversations without being heard. The supervisor can begin and end this capability at any time.

The agent management reports that the supervisor receives may include the following:

- How many calls an agent handled
- How quickly agents responded to calls
- Length of each conversation
- Agent availability
- Call abandon rate

7.2.2.8.2 Architectures

For Remote Agents logged into premises-based ACDs, the architecture is shown in figure 7-42.

For Remote Agents logged into a Central Office-based ACD, the architecture is shown in figure 7-43.

7.2.2.8.3 Information Flow

The information flow diagram is shown in figure 7-44.

7.2.2.8.4 Network Signalling Requirements—Protocol Identification

There are no specific network signalling requirements for this service.

7.2.2.8.5 Protocol Description

In-band signalling is recommended to invoke the silent monitoring capability. Existing data protocols can be used between the supervisor's data terminal and the host to receive agent management reports.

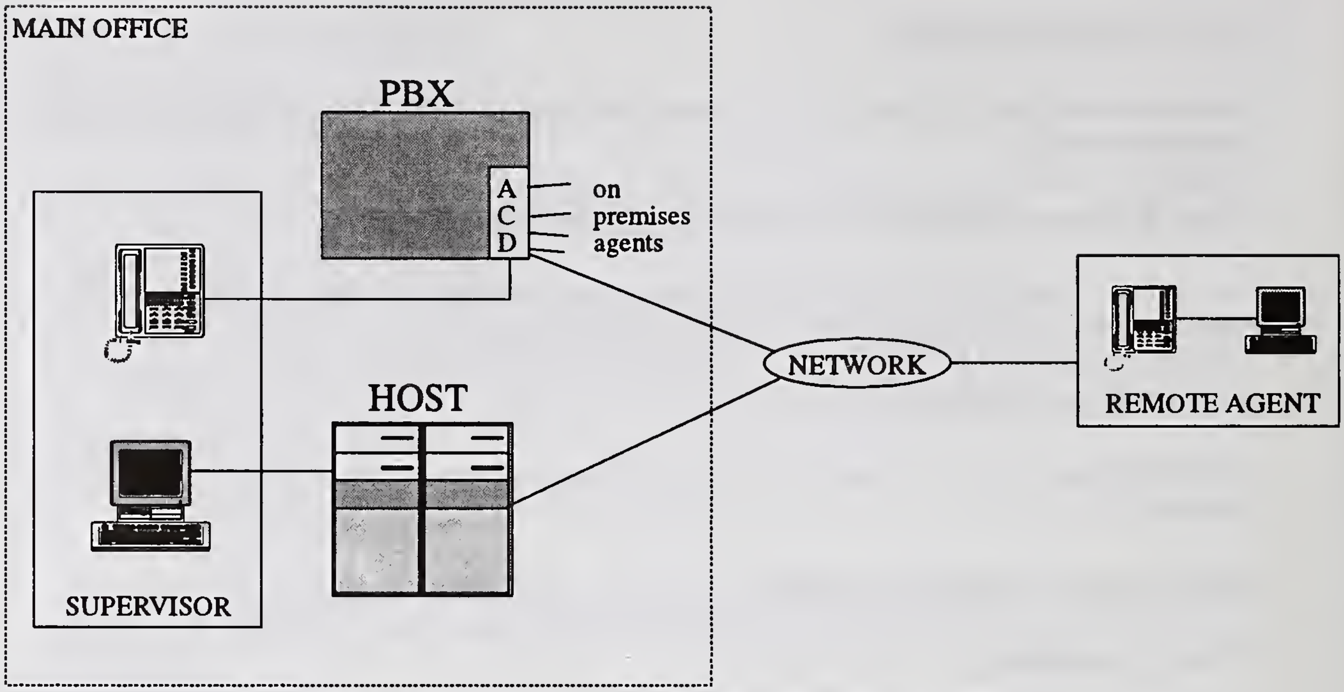


Figure 7-42. Architecture for Premises-Based ACD.

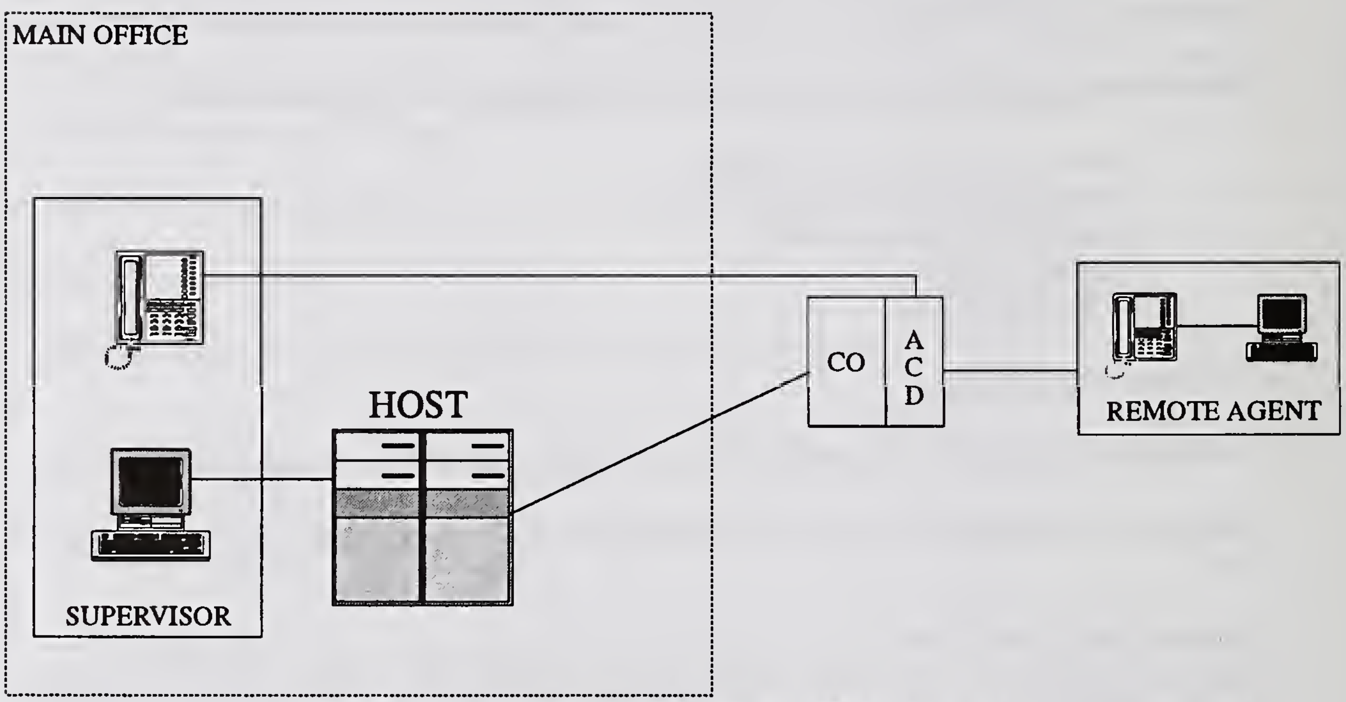


Figure 7-43. Architecture for Central Office-Based ACD.

7.2.2.9 Future Conformance Testing Agreements

This section is reserved for future work on SCAI conformance testing agreements.

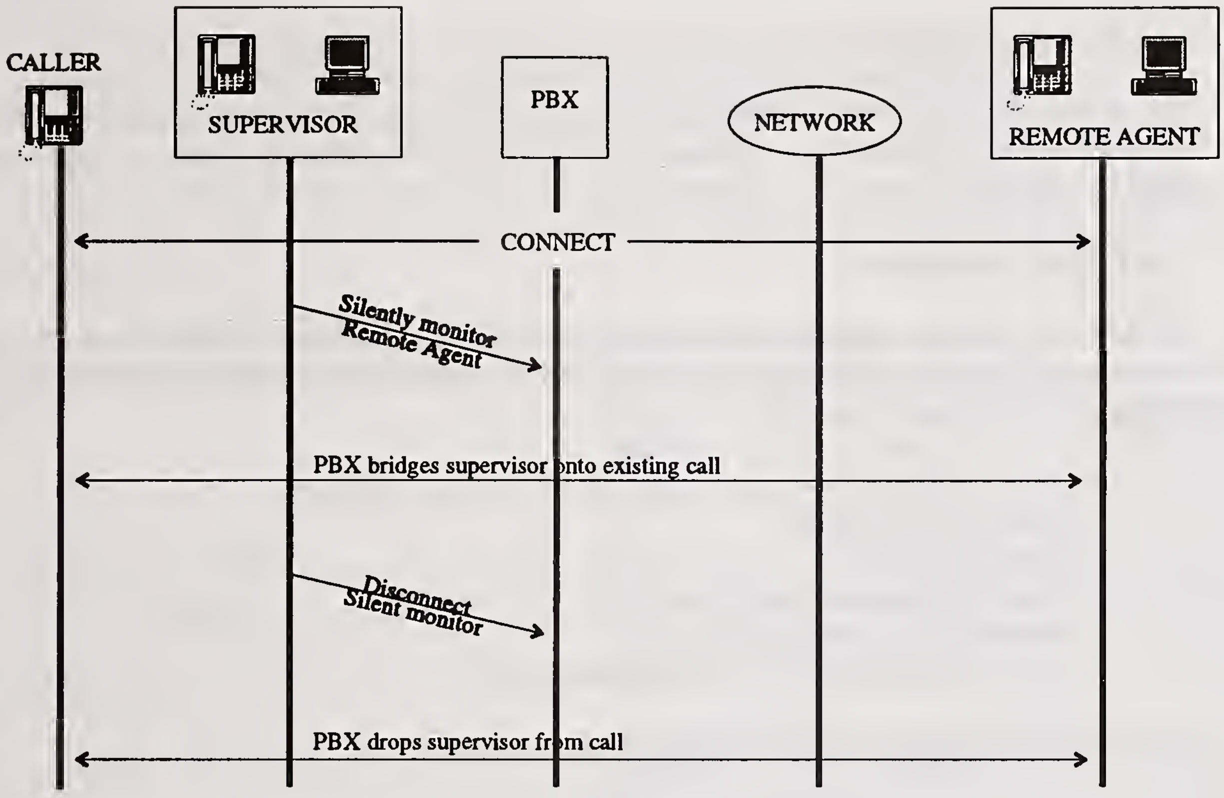


Figure 7-44. Information Flow for Agent Supervisory Functions.

7.3 ISDN CPE Compatibility/Capability

7.3.1 Building Controls

This application profile, NIUF 91-0002, provides User Descriptions, Terminal Adapter Functional Requirements and Application Architecture Analysis for the Building Controls Application 830013.0, (Ref. [43]).

7.3.1.1 User Description

The Building Controls application consists of a variety of control functions carried out with the objective of monitoring and managing a building and its facilities in a cost effective manner. Some of the representative functions are:

- Control of heating/ventilation and air conditioning equipment.
- Energy management.
- Comfort control.
- Fire monitoring and facility control in a fire situation.
- Security monitoring and control.
- Control of personnel access to restricted areas.

The application currently consists of the following components:

- Sensors that are attached to key metering equipment.
- The sensors are connected to control processors which either store information or initiate action based on the sensor readings. This connection is proprietary in nature and will not utilize ISDN services.
- Up to 31 control processors can be connected to a central processor in a multidropped, polled environment. The central processor stores, sorts and relays data received from its associated control processors. Additionally it provides an operator interface and transmits stored information to the end customer's host computer.

In the typical implementation in-house wiring is used to connect the central processor and its associated control processors. The interface used is RS-485 providing synchronous communication between 1200 and 9600 bps.

Control processors can also be connected remotely over private line facilities. The physical interface in this implementation is RS-232 providing synchronous or asynchronous communication between 1200 and 9600 bps. The asynchronous format is more common and utilizes either an 8 bit or 9 bit data format.

The link from the central processor to the customer's host utilizes an RS-232 interface which provides synchronous or asynchronous communication at 2400 bps.

This profile will focus on utilizing ISDN services for connections between 1) the control and central processors, and 2) the central processor and customer host computer.

7.3.1.2 Terminal Adapter Functional Requirements

Table 7-2 provides a summary of the basic functionality required for terminal adapters to operate in this application. This summary assumes the use of D-Channel permanent virtual circuits and B-Channel packet services between the central and control processors.

The link from the central processor to the host computer will utilize B-Channel circuit data services. The Application Architecture discussion in section 7.3.1.3 describes the ISDN data services to be used.

Table 7-2. Building Control Application Functional Requirements

Feature	Central Processor TA	Control Processor TA	Customer Host TA
RS-232 Async "R" Interface	Option	Yes	Yes
RS-232 Sync "R" Interface	Yes	Option	Yes
RS-485 Sync "R" Interface Proprietary Protocol	Option	Option	No
9 Bit Async Data	Option	Option	Option
8 Bit Async Data	Option	Yes	Yes

NOTES:

1) An answer of "Yes" means that support for this feature is required.

2) An answer of "Option" means that support for this feature appears desirable but may not be required.

3) An answer of "No" means that support for this feature is <u>not</u> required.

4) The round trip transit time for a poll and corresponding response through the network should not exceed 50 ms. This is exclusive of processing time at the Control Processor.

5) The data word formats used are 8 data bits + no parity and 8 data bits + 1 parity bit.

6) Currently the Central Processor can support up to 31 Control Processors. This number may be increased at a future date.

7.3.1.3 Application Architecture

The application architecture is based on the use of D-Channel permanent virtual circuits to each control processor. A nailed-up B-Channel packet service is used to connect the appropriate control processors to the central processor. This approach implies that the central processor will substitute X.25 for layers 1, 2 and 3 of the proprietary protocol that is currently used. The use of PVC's and nailed-up connections reasonably emulates the current multidropped environment and negates any requirement for the processor and terminal adapter to exchange commands for call setup or call clearing.

The central processor uses a file transfer facility to transmit information to the customer's host computer. Either D-Channel packet or B-Channel circuit switched data services could be used to support this requirement.

Figure 7-46 illustrates the topography of this application.

7.3.1.3.1 Layer 1 Architecture

The layer 1 architecture for this application is fully supported by T1.605 (Ref. [16]). Each control processor will function in a Point-to-Point environment; however, Point-to-Multi-point arrangements may be considered where distance limitations can be met.

7.3.1.3.2 Layer 2 Architecture

The layer 2 architecture for this application is fully supported by X.25 (Ref. [28]) LAPB procedures on the B-Channel and T1.602 (Ref. [13]) LAPD procedures on the D-Channel.

7.3.1.3.3 Layer 3 Architecture

The layer 3 architecture for this application is fully supported by T1.608-1991 (Ref. [18]).

7.3.1.3.3.1 Central Processor Terminal Adapter Architecture

Terminal adapters attached to the central processor would utilize B-Channel packet services to allow the central processor to poll up to 31 control processors. This implementation requires that the central processor utilize X.25 for layers 1, 2 and 3 of the proprietary protocol and implies that the X.25 data will be presented in a standard HDLC format.

The physical interface provided would be RS-232 and would support speeds up to 9600 bps. The requirement to support RS-485 is discussed in section 7.3.1.3.3.5 (Issues And Limitations).

The terminal adapter used for data transfer to the customer's host would utilize B-Channel circuit data services. The physical interface provided is RS-232 and it would support either asynchronous or synchronous data formats at speeds up to 9600 bps.

7.3.1.3.3.2 Control Processor Terminal Adapter Architecture

A terminal adapter attached to a control processor would utilize D-Channel PVC packet services. PVC's are required to support the following requirements:

- Round trip delay within network should not exceed 50 ms. The use of virtual circuits would not meet this requirement.

- Control processor must be able to transmit alarm information immediately to the central processor.

The terminal adapters utilizing D-Channel packet services would interface to control processors as follows:

- RS-232 interface
- Asynchronous data
- 8 bit word format
- Speeds up to 9600 bps

The following interface support is discussed in section 7.3.1.3.3.5 (Issues And Limitations):

- RS-485 interface
- Synchronous data
- 9 bit word format

7.3.1.3.3.3 Customer Host Terminal Adapter Architecture

The customer host terminal adapter would utilize B-Channel circuit data services to communicate with the central processor. D-Channel packet services could be considered, however, the terminal adapter could not currently support synchronous data.

The physical interface required is RS-232 and will support speeds up to 9600 bps. The data format can be either asynchronous or synchronous.

In the asynchronous mode the terminal adapter may have to provide a command interface to allow the establishment and clearing of calls. Alternatively an autodial mechanism may be provided which will dial a stored number when the DTE provides an appropriate signal, e.g., Data Terminal Ready.

In the synchronous mode an autodial mechanism could also be considered.

7.3.1.3.3.4 Protocol Architecture Overview

The protocol stack shown below illustrates the peer-to-peer communications in the architecture described above.

7.3.1.3.3.5 Issues And Limitations

The following issues are raised by this architecture:

1) There are currently no standards that define the interface between a synchronous DTE and X.25 packet assembler/disassembler (PAD).

2) There are currently no standards that support the use of 9-bit data from a start/stop DTE on an X.25 network. The requirement to octet align the data for transport on the network may require significant development.

3) The addition of RS-485 interfaces to terminal adapters will require significant development.

CENTRAL PROCESSOR TA		NETWORK		CONTROL PROCESSOR TA
HIGHER LAYER PROPRIETARY PROTOCOL				HIGHER LAYER PROPRIETARY PROTOCOL
LAYER 3 T1.608	←→	LAYER 3 T1.608	←→	LAYER 3 T1.608
LAYER 2 X.25 LAPB	←→	LAYER 2 T1.602 X.25 LAPB	←→	LAYER 2 T1.602
LAYER 1 T1.605	←→	LAYER 1 T1.605	←→	LAYER 1 T1.605

Figure 7-45. Building Controls Protocol Stack.

4) The requirement for a 50 ms round trip transit time for a poll and response may not be achievable in all cases.

The following limitation is imposed by this architecture:

1) The central processor will have to substitute X.25 for layers 1, 2 and 3 of the proprietary protocol.

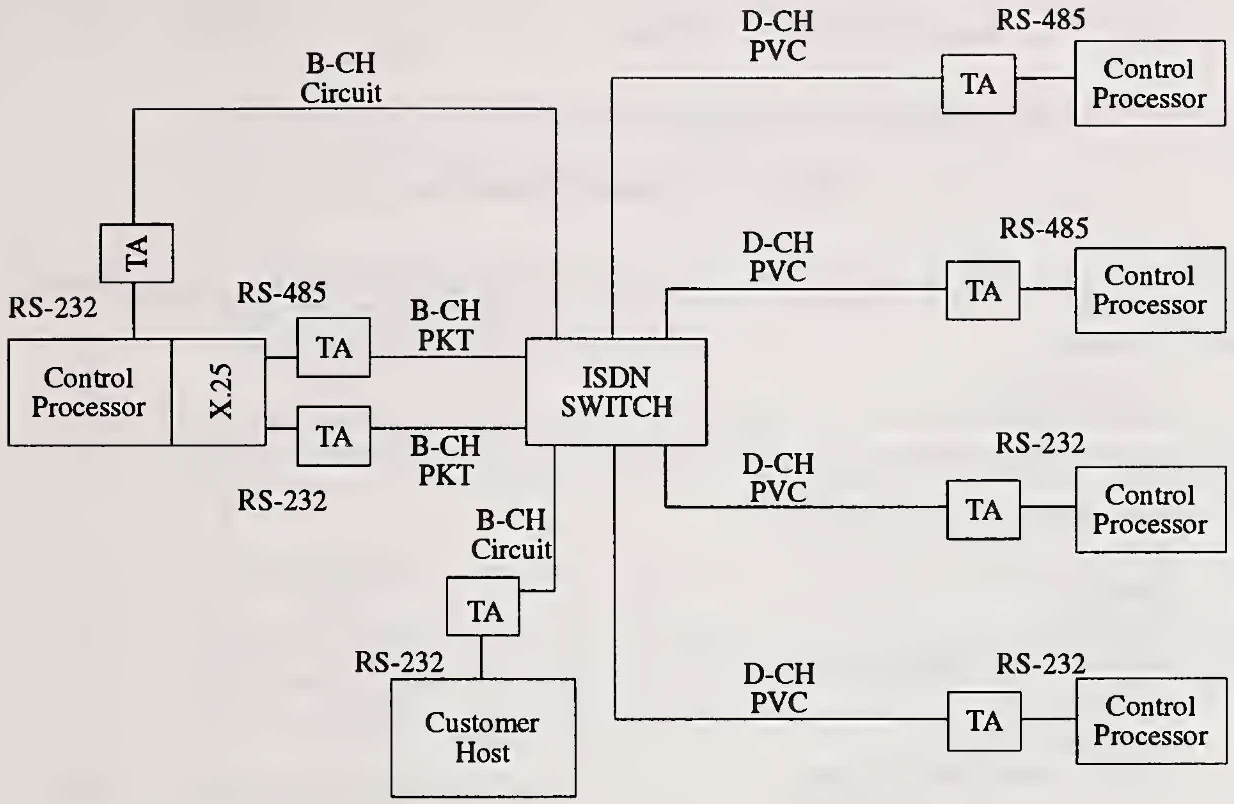


Figure 7-46. Building Controls Application Topography.

7.3.2 ISDN Telephone Workstation Integration

7.3.2.1 User Description of the Application

This section is a summarization of the information in the Application Analysis.

Table 7-3. Functional Requirements

Feature	ISDN Telephone	Workstation
Voice call handling:	Yes	Yes
Call origination	Yes	Yes
Call termination	Yes	Yes
Voice communication	Yes	No
Voice supplementary service activation:		
Hold	Yes	Yes
Transfer	Yes	Yes
Conference	Yes	Yes
Electronic key telephone service	Yes	Yes
Call pick up	Yes	Yes
Automatic call back	Yes	Yes
Calling number identification	Yes	Yes
Telephone local function control:		
Speaker phone activation	Yes	No
Speaker phone mute	Yes	No
ISDN telephone data call control:		
D Channel packet switch calling	Option	No
B Channel packet switch calling	Option	No
B Channel circuit switch calling	Option	No
Workstation data call control:		
D Channel packet switch calling	No	Yes
B Channel packet switch calling	No	Yes
B Channel circuit switch calling	No	Yes
Workstation local function control:		
Call monitoring & logging	No	Yes
Directory service	No	Yes

Notes on the Functional Requirements:

(1) An answer of "Yes" means that support for this feature is required.

(2) An answer of "Option" means that support for this feature appears desirable but may not be required.

(3) An answer of "No" means that support for this feature is <u>not</u> to be provided.

(4) It must be possible to originate or answer a call from either the ISDN Telephone or the Workstation. The user requirements specify that voice conversation takes place only on the ISDN telephone.

(5) It should be possible to activate Voice Supplementary Features from either the ISDN Telephone or the Workstation. This requirement will probably have impact on the Hold, Electronic Key Telephone Service (EKTS), Conference, and Transfer features.

(6) There was no user requirement for the Workstation to control the local telephone functions, e.g., speaker phone; however, it may be desirable for the workstation to be able to control the speaker phone in particular.

(7) It is possible that the ISDN Telephone will include an integrated terminal adapter. The assumption in this case is that the Workstation would have no control over this terminal adapter.

(8) The ISDN Telephone would have no control over the Workstation's ISDN data calling.

(9) The ISDN Telephone would not be required to provide functions best provided in the Workstation, e.g., call monitoring, call logging or directory services. However, some of these services may involve voice call handling functions, e.g., call origination.

7.3.2.2 Application Decomposition

This application will be composed of a single process. This Application Process is described in the remainder of this section.

7.3.2.2.1 Application Process Description

This Application Process handles all of the call-related activities. These include:

- Call Origination at the ISDN Telephone
- Call Origination at the ISDN Workstation
- Voice Communication at the ISDN Telephone
- Supplementary Service Control at the ISDN Telephone
- Supplementary Service Control at the ISDN Workstation
- Call Termination at the ISDN Telephone
- Call Termination at the ISDN Workstation
- Call Monitoring

7.3.2.3 Service Logic

Figure 7-47 shows the Service Logic for this application and how the above functions operate.

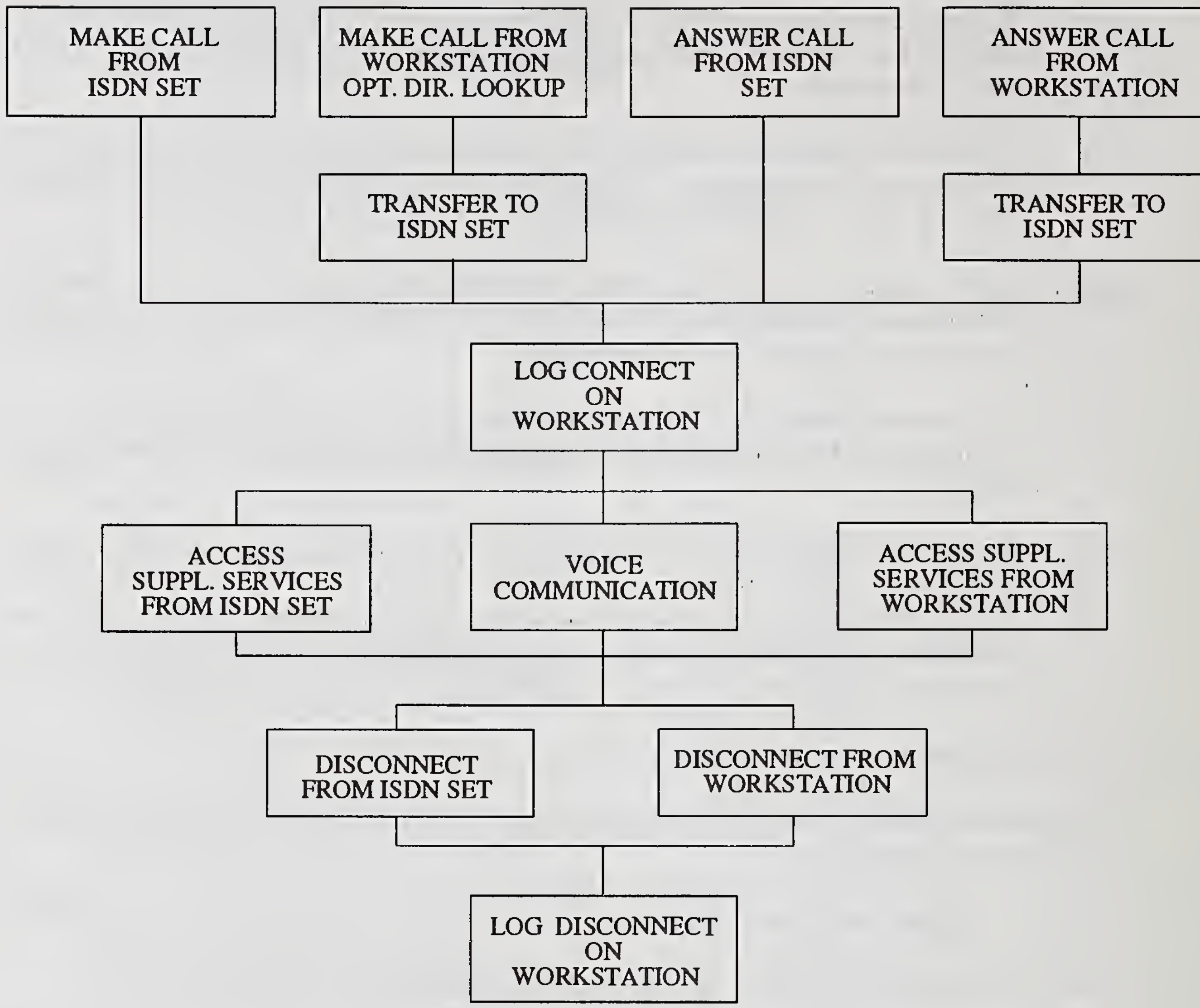


Figure 7-47. Service Logic.

7.3.2.4 Call Handling Application Process (Alternatives)

This section includes a general description of the alternative architectures that have been currently defined. In order to improve the clarity of this document the detailed implementations proposed are put in separate sections. Section 7.3.2.5 details an alternative architecture that is based on using the R interface of the ISDN Telephone to connect the ISDN Workstation to the network. Section 7.3.2.5.7 details the EKTS-based architecture. Future sections will be added based on contributions to the NIUF.

7.3.2.4.1 Application Process Description

This Application Process handles all of the call-related activities. These include:

- Call Origination at the ISDN Telephone
- Call Origination at the ISDN Workstation
- Voice Communication at the ISDN Telephone
- Supplementary Service Control at the ISDN Telephone

• Supplementary Service Control at the ISDN Workstation
• Call Termination at the ISDN Telephone
• Call Termination at the ISDN Workstation
• Call Monitoring

7.3.2.4.2 Alternative Architectures

Five potential architectures to implement this application have been identified. The primary difference is in which network element provides the control and how information is communicated between the ISDN Telephone and the workstation.

Overall Issues:

(1) Each implementation must provide a method for communicating control information between the ISDN Telephone and the Workstation.

(2) The communication method between the ISDN Telephone and the Workstation must include the ability to communicate call state information for each active call. This will be required to insure proper coordination of basic call and supplementary service call control between the ISDN Telephone and the Workstation.

7.3.2.4.2.1 ISDN Interface to the Workstation

See figure 7-48.

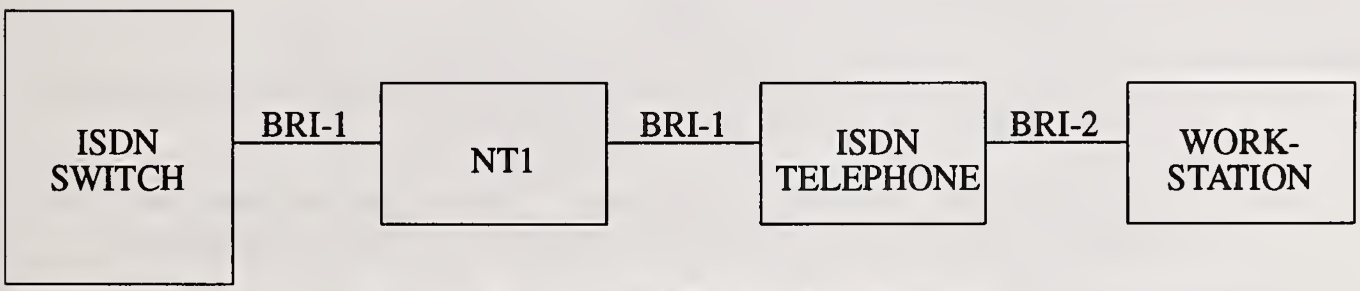


Figure 7-48. ISDN Interface to the Workstation.

Implementation Requirements:

(1) No modifications required to the switch.

(2) The ISDN Terminal may be implemented as an NT2 and must provide the physical interface and all of the signalling required to the Workstation to support the Functional Requirements.

(3) The Workstation must have an integrated ISDN TA along with software to support the Functional Requirements.

Implementation Issues:

(1) While this architecture is reasonably well defined in standards, it may not be desirable because the implementation of NT2 functionality in an ISDN telephone may have significant cost implications.

7.3.2.4.2.2 R Interface to the Workstation

See figure 7-49.

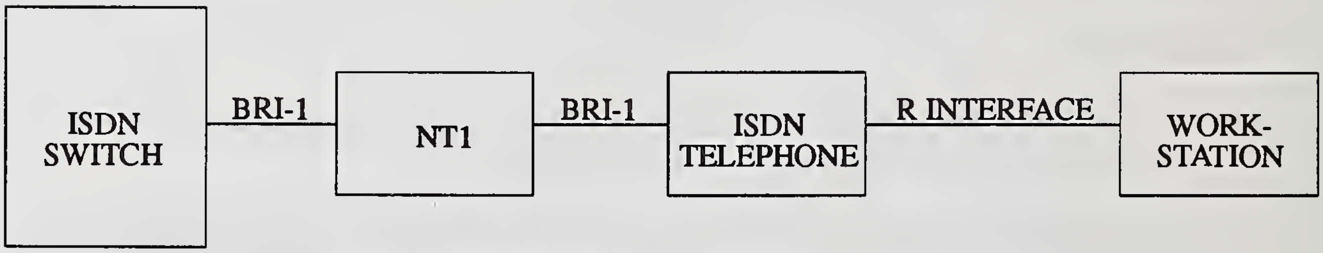


Figure 7-49. R Interface to the Workstation.

Implementation Requirements:

(1) No modifications required to the switch.

(2) The ISDN Telephone must implement a protocol to provide all of the signalling required to the Workstation to support the Functional Requirements.

(3) The Workstation must have the appropriate R Interface and implement the ISDN Telephone's protocol along with software to support the Functional Requirements.

Implementation Issues:

(1) The protocol on between the ISDN Telephone and the Workstation must be standardized for implementation.

See section 7.3.2.5 for a detailed analysis of this architecture.

7.3.2.4.2.3 ISDN Interface to the ISDN Telephone

See figure 7-50.

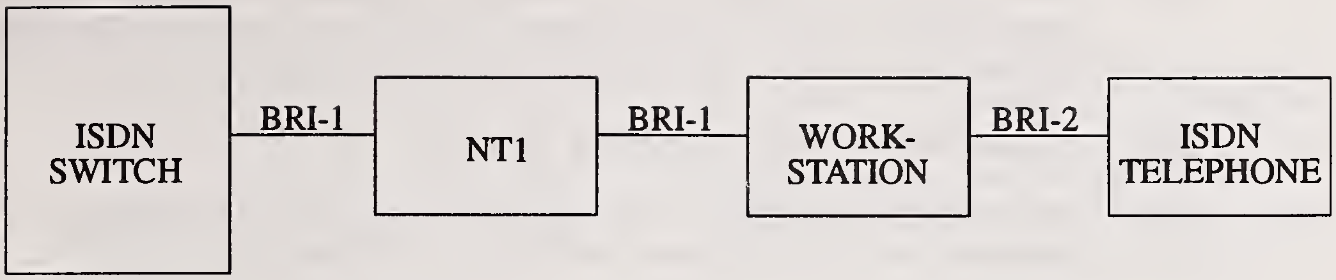


Figure 7-50. ISDN Interface to the ISDN Telephone.

Implementation Requirements:

(1) No modifications required to the switch.

(2) No modifications required to the ISDN Telephone assuming it supports the STATUS ENQUIRY and STATUS messages (note: these messages are not included in NIUF 90-301 (see Appendix A)).

(3) The Workstation may be implemented as an NT2 and must provide the physical interface and all of the signalling required to the ISDN Terminal along with appropriate software to support the Functional Requirements.

Implementation Issues:

(1) While this architecture is reasonably well defined in standards, it may not be desirable because the implementation of NT2 functionality in a Workstation may have significant cost implications.

7.3.2.4.2.4 Control in the Switch

See figure 7-51.

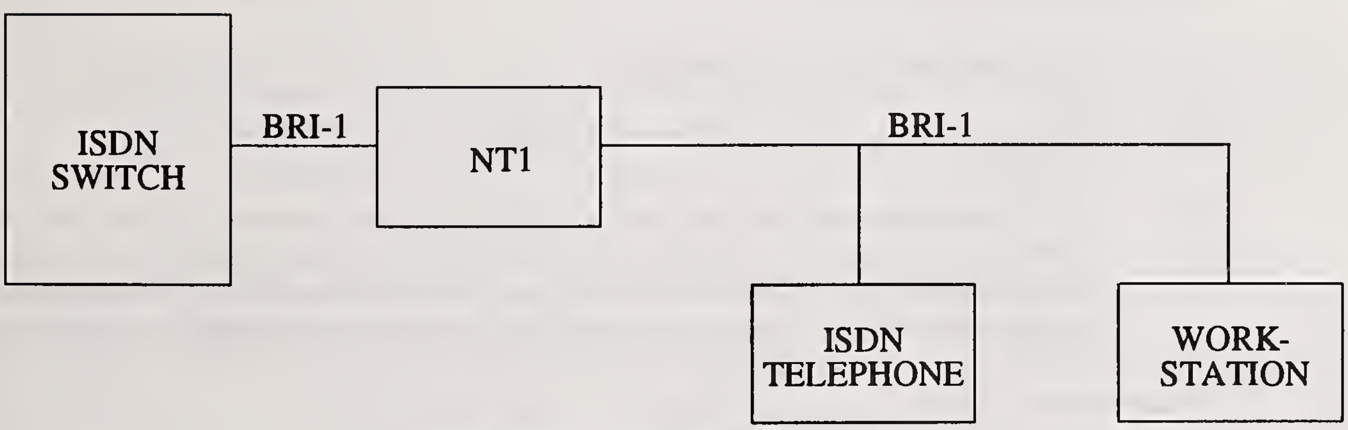


Figure 7-51. Control in the Switch.

Implementation Requirements:

(1) Modifications are required to the switch to implement a protocol to provide communication between the ISDN Telephone and the ISDN Workstation. (The Northern Telecom SAPI 17 implementation is an example of such a protocol.)

(2) No modifications required to the ISDN Telephone.

(3) The Workstation must have an integrated ISDN TA, along with software, use the signalling from the NT1 to support the Functional Requirements.

Implementation Issues:

(1) There are no standards defined that support the implementation of the control and association functions in the switch.

7.3.2.4.2.5 Electronic Key Telephone System Base

See figure 7-52.

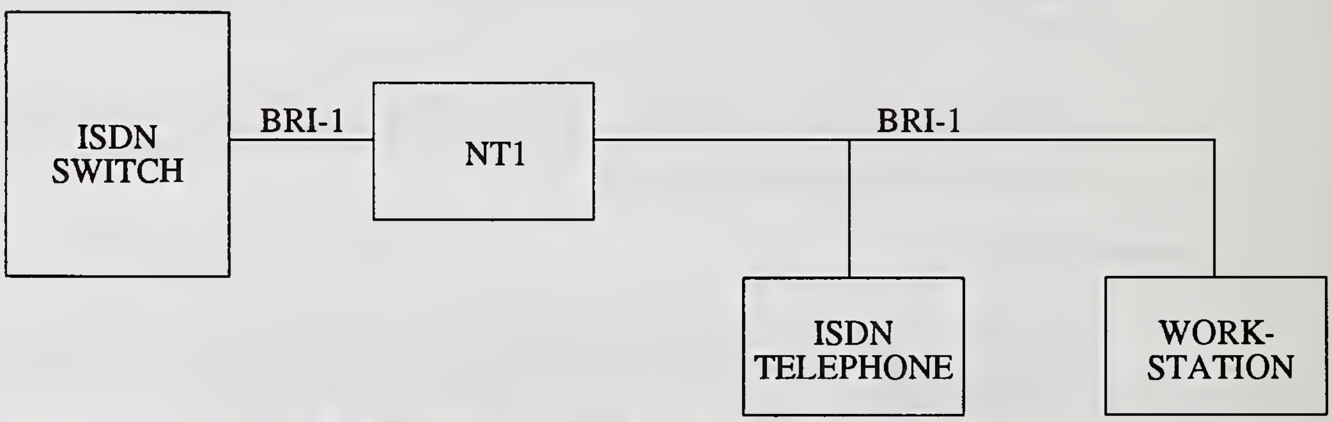


Figure 7-52. Electronic Key Telephone System Base.

Implementation Requirements:

(1) The switch must support an EKTS.

(2) The ISDN Telephone must support an EKTS.

(3) The Workstation must have an integrated ISDN TA that supports all voice and data services, including EKTS. This TA must also provide for monitoring of all D Channel Signalling traffic on the Digital Subscriber Loop (DSL). The workstation will also require software that will use this monitoring information to support the Functional Requirements.

Implementation Issues:

(1) The TA will use the Electronic Key System Simulation (EKTS) feature of the ISDN Switch to provide the ability to originate and terminate calls.

See section 7.3.2.5.7 for a detailed description of this approach.

7.3.2.4.3 Interoperation

Each of the above alternative architectures deals only with the local relationship of the Workstation, the ISDN Telephone, and the network. That is, it is independent of how calls are managed with any other terminal or terminals connected to the network. This means that any or all of the architectures described above can be connected to the network at one time and can interoperate with each other and with any other ISDN or non-ISDN terminal connected to the network in appropriate ways. This means that the user can select from the above architectures on an individual basis.

7.3.2.5 Applications Process Description—R Interface

This section details an alternative architecture that is based on using the R interface of the ISDN Telephone to connect the ISDN Workstation to the network. The advantages of this approach are that it has lower hardware cost and it does not require any changes to ISDN interfaces. A limitation of this approach is that the data transfer rate is limited to the maximum allowed by the R interface.

7.3.2.5.1 Applications Process Description

See Section 7.3.2.2.1 for the description of the Call Handling Application Process.

This Applications Process handles all of the call-related activities. These include:

- Call Origination at the ISDN Telephone
- Call Origination at the ISDN Workstation
- Voice Communication at the ISDN Telephone
- Supplementary Service Control at the ISDN Telephone
- Supplementary Service Control at the ISDN Workstation
- Call Termination at the ISDN Telephone
- Call Termination at the ISDN Workstation
- Call Monitoring

7.3.2.5.2 Architecture

This alternative architecture uses the R interface on the ISDN telephone to connect to a serial port on the workstation. It uses a standard ISDN protocol interface to the ISDN Telephone. This architecture requires the development of a standard for the R Interface to provide a method to control the operation of the ISDN Telephone from the Workstation. See figure 7-53.

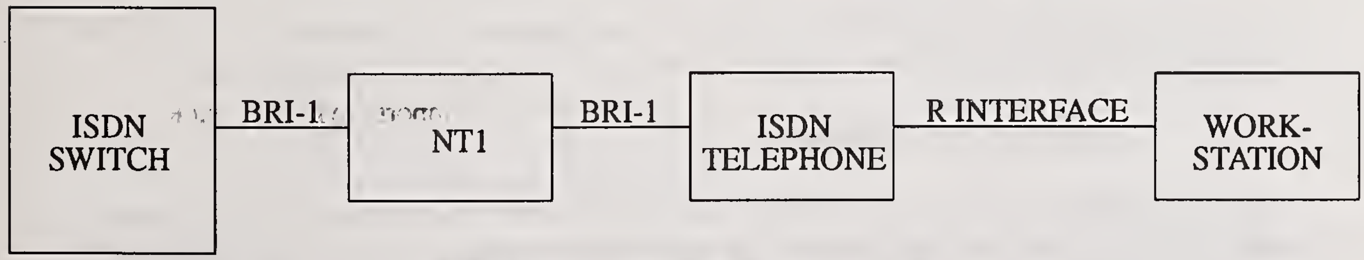


Figure 7-53. R Interface Architecture.

7.3.2.5.2.1 ISDN Interface

This section describes the requirements for the ISDN interface point. It can be implemented using current standards.

7.3.2.5.2.1.1 Layer 1 Architecture

The Layer 1 Architecture for this alternative is fully supported by NIUF 92-101R1 and NIUF 92-105R1 (see sections 4.1.1.1 and 4.1.1.2).

7.3.2.5.2.1.2 Layer 2 Architecture

The Layer 2 Architecture for this alternative is fully supported by NIUF 89-210 (see section 4.1.3).

7.3.2.5.2.1.3 Layer 3 Architecture

The Layer 3 Architecture for this alternative is fully supported by NIUF 90-301 (see Appendix A).

7.3.2.5.2.1.4 Supplementary Service Architecture

The Supplementary Service Architecture for this alternative is based on NIUF 90-311 (see section 4.1.4.1.2).

7.3.2.5.2.2 R Interface Architecture

A signalling architecture needs to be defined that will provide support for call control from the Workstation. This interface would use the physical interface provided by the ISDN Telephone and the Workstation. This architecture needs to provide the following functions:

- Call Origination (Telephone)
- Call Origination (Workstation)
- Voice Communication (Telephone)
- Supplementary Service Control (Telephone)
- Supplementary Service Control (Workstation)
- Call Termination (Telephone)
- Call Termination (Workstation)
- Notification of Call State Changes for Call Monitoring
- Circuit Switched Data Call Control (Workstation)
- Packet Switched Data Call Control (Workstation)

An example for this kind of interface is the "Hayes Standard AT Command Set for ISDN," published by Hayes Microcomputer Products, Inc.

7.3.2.5.3 Information Flow Diagrams

Either the ISDN Telephone or the Workstation could be used to originate calls or to terminate calls. The R interface protocol provides the signalling required to communicate the state of the call to the ISDN Telephone and the Workstation. The general procedures for handling calls from the ISDN Telephone do not change. The procedure for originating a call from the Workstation and conversing on the ISDN Telephone along with accessing Supplementary Services either from the

ISDN Telephone or the Workstation is given in figure 7-54. The details of the signalling protocol are not shown in order to improve clarity.

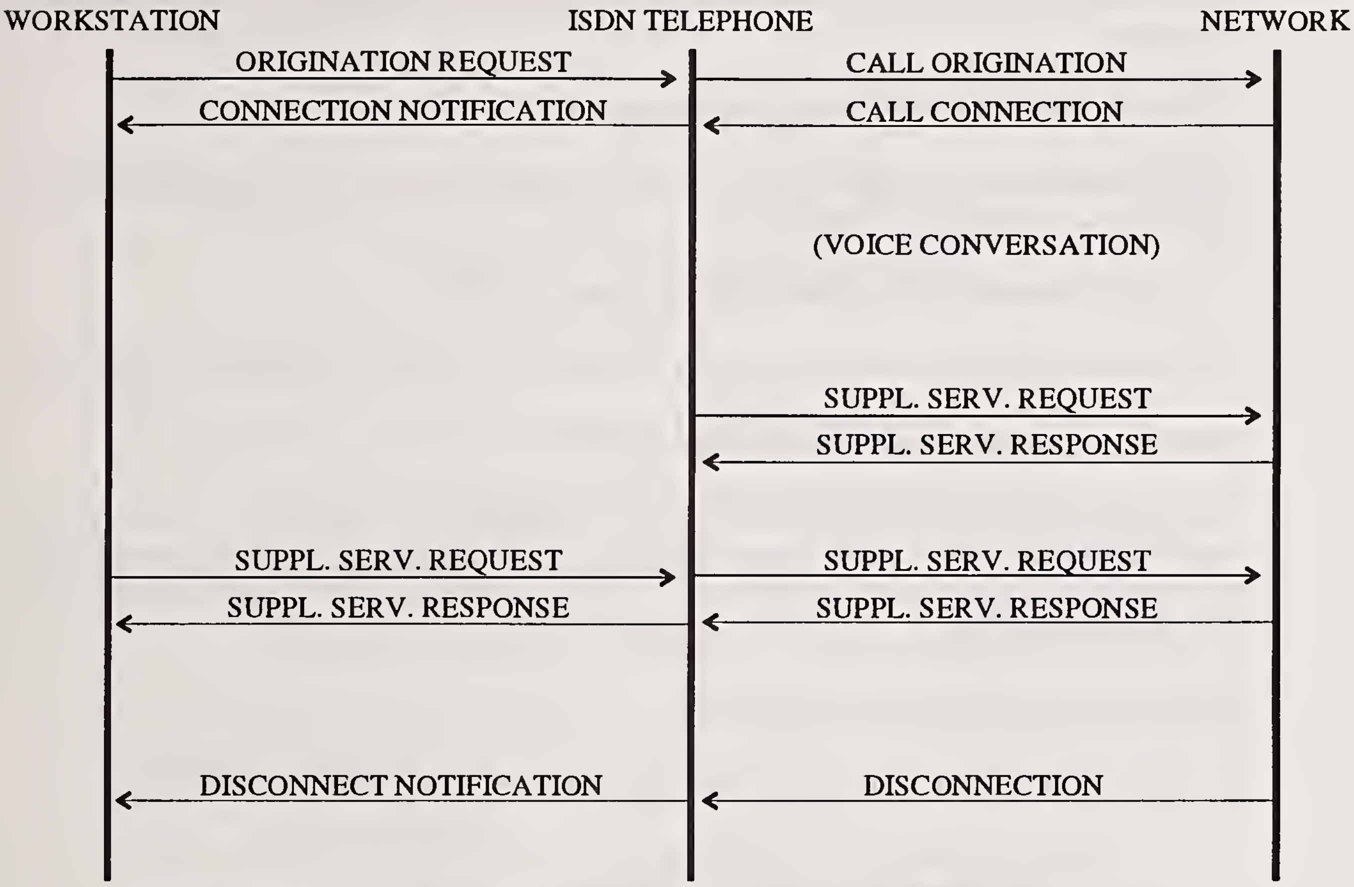


Figure 7-54. Accessing Supplementary Services—Information Flow Diagram.

7.3.2.5.4 SDLs

SDLs are not required for this Application Profile.

7.3.2.5.5 Standard Protocol Requirements

The following implementation agreements apply to this alternative architecture:

- NIUF 90-301 (see Appendix A)
- NIUF 90-311 (see section 4.1.4.1.2)
- NIUF 89-210 (see section 4.1.3)
- NIUF 92-101R1 (see section 4.1.1.1)
- NIUF 92-105R1 (see section 4.1.1.2)

This alternative architecture requires the definition of a standard for an R Interface Protocol as described in Section 7.3.2.5.2.2 above.

7.3.2.5.6 Conformance Criteria

This section contains a general description of the conformance requirements for this alternative architecture.

7.3.2.5.6.1 Protocol Conformance Requirements

An implementation of this alternative architecture should conform to the Protocol Requirements described in Section 7.3.2.5.5 above.

7.3.2.5.6.2 Functional Conformance Requirements

Meet the functional requirements described in Section 7.3.2.1, User Description of the Application.

7.3.2.5.7 Application Process Description—EKTS

This section details the EKTS-based architecture. The advantage of this approach is that it permits the Workstation to transfer data at a full 64 kbps. A disadvantage is that it requires an ISDN telephone and a separate ISDN interface in the workstation; this approach is likely to have a higher cost associated with it.

7.3.2.5.8 Application Process Description

This Application Process handles all of the call-related activities. These include:

- Call Origination at the ISDN Telephone
- Call Origination at the ISDN Workstation
- Voice Communication at the ISDN Telephone
- Supplementary Service Control at the ISDN Telephone
- Supplementary Service Control at the ISDN Workstation
- Call Termination at the ISDN Telephone
- Call Termination at the ISDN Workstation
- Call Monitoring

7.3.2.5.9 Architecture

This alternative architecture uses the EKTS feature to provide ISDN Telephone/Workstation Integration. This approach has the advantage that it can be implemented using standard ISDN Telephones, Workstations ISDN interface boards, and ISDN Networks as long as each supports the EKTS feature. The monitoring function may require specific hardware support. See figure 7-55.

7.3.2.5.9.1 ISDN Telephone Architecture

This architecture assumes that no modifications would be required of the ISDN Telephone. It assumes that any ISDN Telephone that fully supports EKTS would be compatible with this application.

7.3.2.5.9.2 Workstation Architecture

This architecture assumes that the Workstation would have a Basic Rate Interface along with application software that would support the requirements of this application.

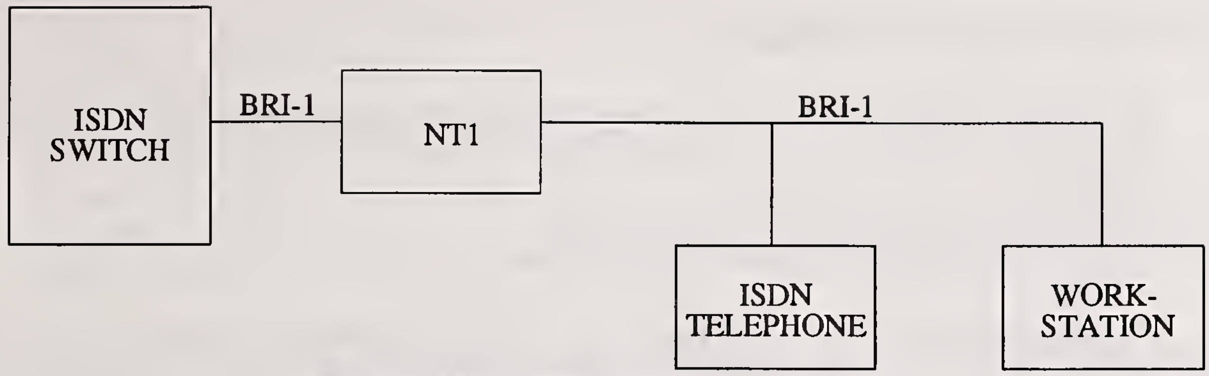


Figure 7-55. EKTS Alternative Architecture.

The Basic Rate Interface would have the following capabilities:

- Full control of voice calls including all supplementary services

- Support for EKTS as a mandatory requirement

- Ability to monitor all messages for all terminals connected to the same DSL

The Applications Software should be able to support all of the Functional Requirements of the application, including:

- Call Origination
- Call Termination
- Activation and Control of Supplementary Services
- Full Data Communications Capability
- Directory Services
- Call Monitoring and Call Logging

7.3.2.5.9.3 Protocol Architecture

This architecture uses a standard three-layer ISDN protocol architecture with the addition of supplementary services signalling in layer 3.

7.3.2.5.9.3.1 Layer 1 Architecture

The Layer 1 Architecture for this application is fully supported by NIUF 92-101R1 and NIUF 92-105R1 (see sections 4.1.1.1 and 4.1.1.2). The physical configuration options will be determined by the configuration limitations of the EKTS feature. There is a requirement to connect the ISDN Telephone and the Workstation to the same Digital Subscriber Line (DSL) to meet the monitoring requirements of this application. Consequently support for the Point-to-Multi-point configurations is a requirement for this application.

7.3.2.5.9.3.2 Layer 2 Architecture

The Layer 2 Architecture for this application is fully supported by NIUF 89-210 (see section 4.1.3). There are no special Layer 2 issues for this application.

7.3.2.5.9.3.3 Layer 3 Architecture

The Layer 3 Architecture for this application is fully supported by NIUF 90-301 (see Appendix A) for basic call control. It also uses NIUF 90-301 (Appendix A) for supplementary Services signalling.

7.3.2.5.9.4 Supplementary Service Architecture

The Supplementary Service signalling architecture for this application is based on NIUF 90-311 (see section 4.1.4.1.2). This architecture requires the support of the EKTS feature and has certain feature interaction requirements between EKTS and other supplementary services. Supplementary services where this may be an issue are described explicitly.

7.3.2.5.9.4.1 Electronic Key Telephone Service

An EKTS feature is required that supports shared call appearances between two ISDN terminals. A discussion of one implementation of EKTS can be found in Bellcore's TR-TSY-000205 "ISDN Electronic Key Telephone Service." A fundamental part of the EKTS feature is the "Call Appearance Group." A Call Appearance group is the set of ISDN Terminals that can originate or terminate calls from a given Directory Number (DN).

This application assumes that a terminal with a shared call appearance will be notified of any of the following events:

- Incoming Call Termination
- Incoming Call Connected
- Outgoing Call Initiation
- Call Put on Hold
- Call Retrieved from Hold
- Call Disconnected from all Members of the Call Appearance Group

In addition, any Terminal in the Call Appearance Group should have the capability to:

- Originate a Call
- Terminate a Call
- Connect to an Call
- Place an Active Call on Hold
- Retrieve a Held Call

These capabilities allow the integration of functions from the ISDN Telephone to the ISDN Workstation.

7.3.2.5.9.4.2 Conference Calling

It must be possible to access a Conference Call from any terminal that shares a Call Appearance that is part of the Conference. This allows the ISDN Telephone to connect to a Conference Call that has been initiated from the Workstation.

It is desirable, but not required, that a Conference Call initiated on one Terminal in a Call Appearance Group be controllable from any other terminal in the Call Appearance Group. This would allow the control of the Conference Call to move easily from the ISDN Telephone and Workstation and back again.

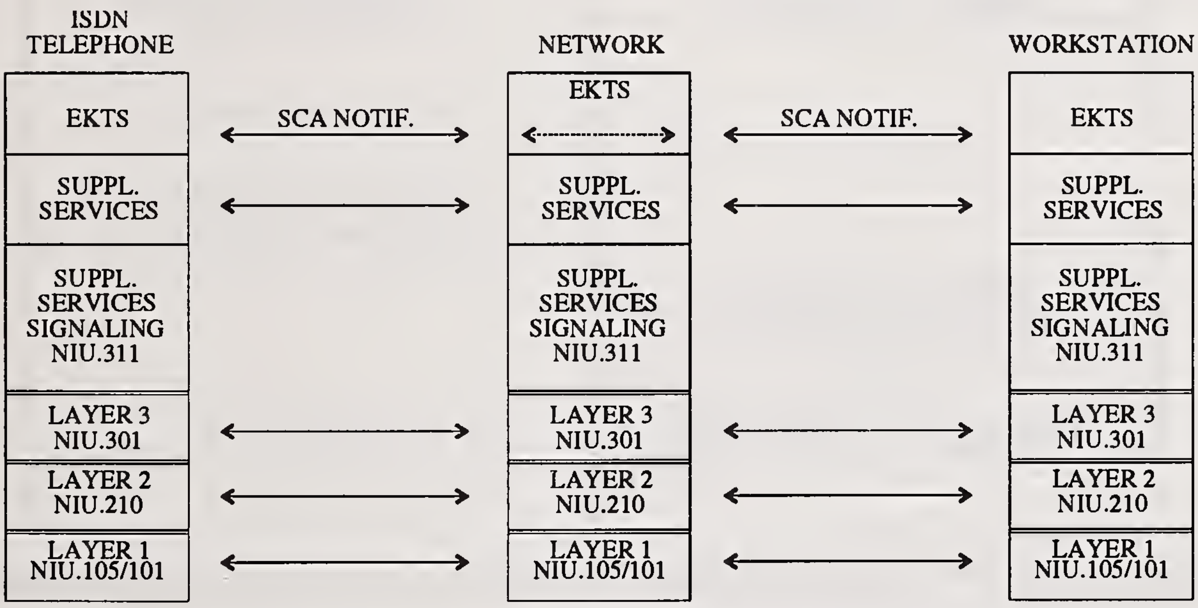
7.3.2.5.9.4.3 Other Supplementary Services

It must be possible to operate all Supplementary Services from any terminal that shares a Call Appearance. This allows the ISDN Telephone and the Workstation to operate features on a cooperative basis.

It is desirable but not required that any feature that is initiated on one Terminal in a Call Appearance Group can have the feature interaction continue from any other member of that Call Appearance Group. This would allow the activation of the feature to move easily from the ISDN Telephone and Workstation and back.

7.3.2.5.9.5 Protocol Stack

The protocol stack shown in figure 7-56 illustrates the peer-to-peer communications in the Architecture described above. It shows the relationship between the ISDN Telephone, the Workstation, and the Network.



NOTES:

1. SCA NOTIF. means Shared Call Appearance Notification. The arrows are drawn through the network to show the quasi "end-to-end" nature of the communication.

2. All other connections are between the Network and the ISDN Telephone or Workstation and not end-to-end from the ISDN Telephone to the Workstations.

Figure 7-56. Protocol Stack.

7.3.2.5.10 Information Flow Diagrams

Either the ISDN Telephone or the Workstation could be used to originate calls or to terminate calls. The EKTS protocols would provide the signalling required to communicate the state of the call to the ISDN Telephone and the Workstation. It is assumed that the Workstation would not support voice communication so the conversation would be held only from the ISDN Telephone. The general procedures for handling calls from the ISDN Telephone do not change. The procedure for originating a call from the Workstation and conversing on the ISDN Telephone is given in figure 7-57. The details of the signalling protocol are not shown in order to clarify the general flow.

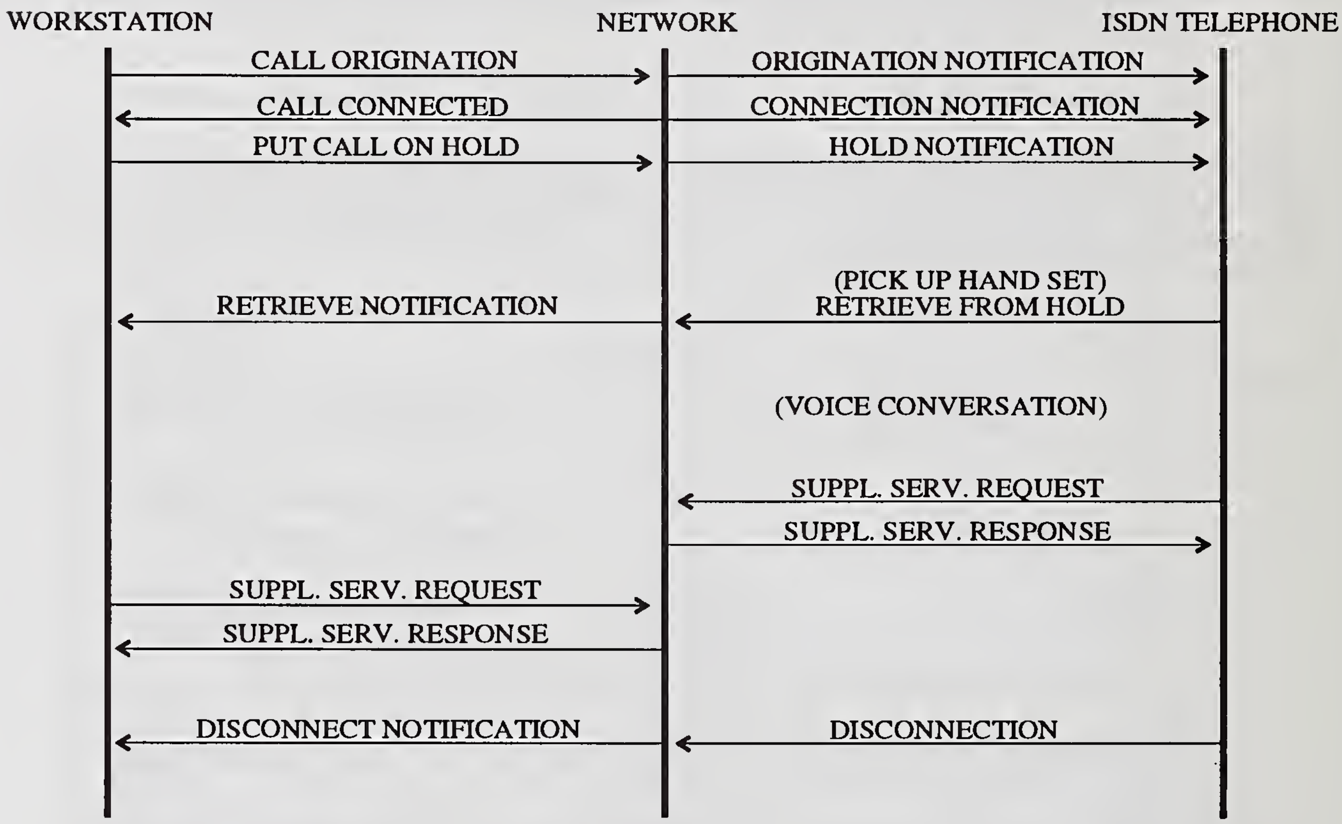


Figure 7-57. ISDN Telephone Call Originating from Workstation—Information Flow Diagram.

7.3.2.5.11 SDLs

There is no requirement for SDLs in this application profile.

7.3.2.5.12 Standard Protocol Requirements

The following implementation agreements apply to this Alternative Architecture:

- NIUF 90-301 (see Appendix A)
- NIUF 89-311 (see section 4.1.4.1.2)
- NIUF 89-210 (see section 4.1.3)
- NIUF 92-101R1 (see section 4.1.1.1)
- NIUF 92-105R1 (see section 4.1.1.2)

This alternative architecture requires the definition of a standard for an Electronic Key Telephone System feature as described in Section 7.3.2.5.9.4.1 above.

7.3.2.5.13 Conformance Criteria

This section contains a general description of the conformance requirements for this alternative architecture.

7.3.2.5.13.1 Protocol Conformance Requirements

An implementation of this alternative architecture should conform to the Protocol Requirements described in Section 7.3.2.5.12 above.

7.3.2.5.13.2 Functional Conformance Requirements

An implementation of this alternative architecture should meet the functional requirements described in Section 7.3.2.1, User Description of the Application.

7.3.3 Engineering Workstation Interface

7.3.3.1 User Description

This Application Profile (AP) addresses the requirements for an engineering workstation to provide graphic enquiry and interactive engineering and design throughout a network utilizing an ISDN communications interface. This interface would provide interoperability between workstations, local area networks, and graphic hosts of different vendors and should be able to meet both on-line and remote engineering/design requirements.

The expected benefits of utilizing the ISDN circuit mode services for this application are:

- Improve speed of deployment of workstation technology throughout the world due to the flexible connectivity capabilities of the ISDN.

- A major reduction in the cost of special wiring.

- The evolution from proprietary interfaces to standards-based interfaces for engineering and design graphics systems.

7.3.3.1.1 Definition of Terms

The following terms were used in the Application Requirements Data Form. They will be defined as follows for the purpose of the AP.

Workstation: A computer system that uses a general purpose operating system to support engineering or design applications. Examples are **workstations** provided by IBM, Sun, Hewlett Packard, and DEC. **Workstations** may be configured as stand-alone or LAN-connected resources.

Graphic Host: A centralized computer system that supports an engineering or design application. For this AP, the user interface for the **graphic host** application is provided by either a terminal emulation application on the **workstation**, or an X-Window graphics relationship between the **graphic host** and the **workstation**.

Local Area Network (LAN): A means for interconnecting computer systems. For the purposes of this AP it will be assumed that a **LAN** is based on recognized standards, such as IEEE 802.3, 802.4, or 802.5. Typically **workstations** are interconnected by **LANs** to form a distributed system.

7.3.3.1.2 General Requirements

The Application Requirements call for supporting the interconnections shown in figure 7-58.

The Application Requirements make the following specific points:

(1) 64 kbps is minimally enough bandwidth for connecting Workstations to other Workstations, LANs, or Graphic Hosts. Bandwidth greater than 64 kbps may be required for specific applications.

(2) Bandwidth greater than 64 kbps will be required to interconnect LANs with other LANs and with Graphic Hosts. This bandwidth may be provided (in the circuit mode) by either an ISDN H channel or an N x 64 channel selection capability.

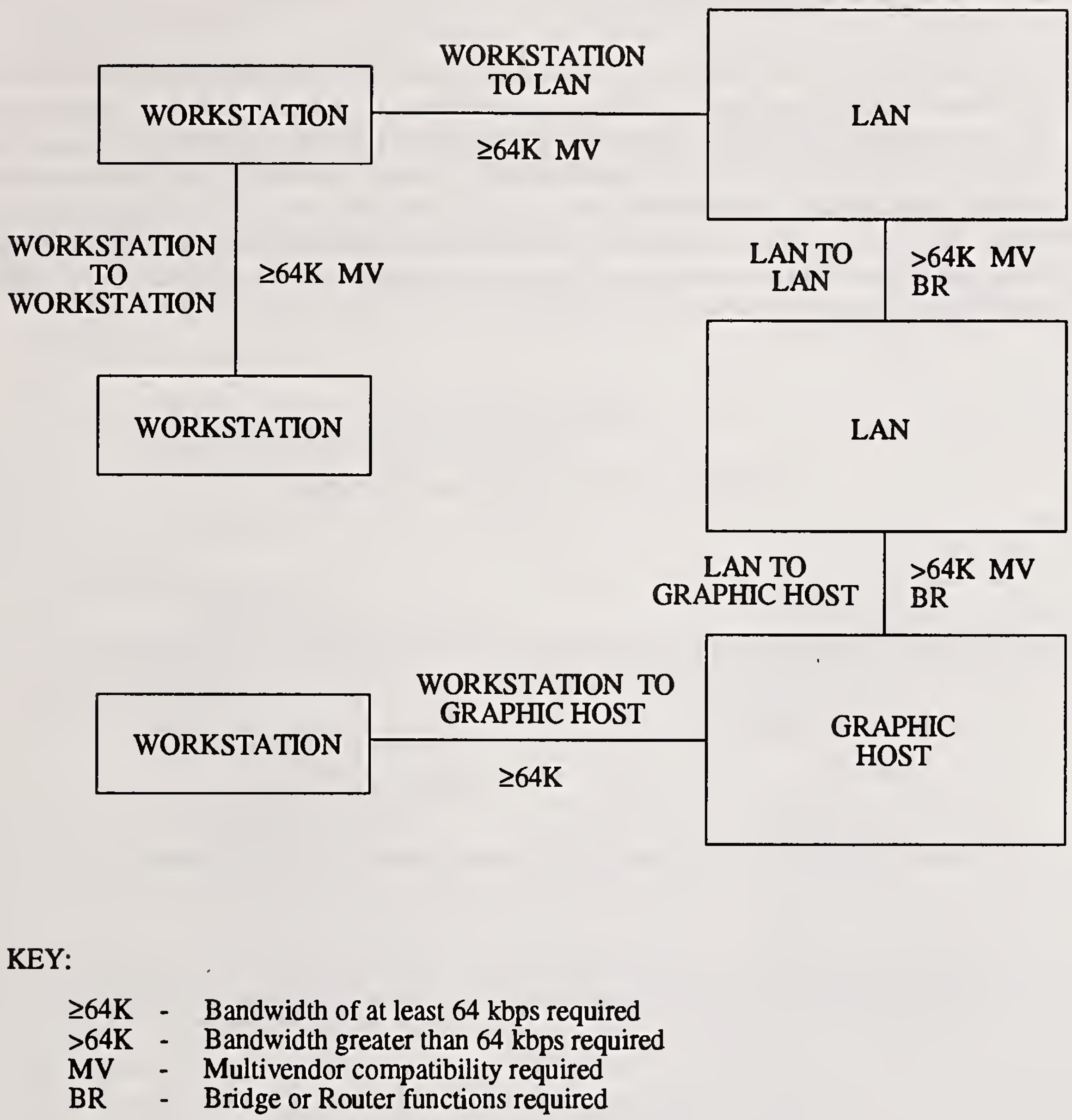


Figure 7-58. Interconnection Requirements for the Engineering Workstation Interface.

(3) Multivendor compatibility requires the graphic data formats to be compatible, or convertible so that a file created on one manufacturer's system can be modified using another manufacturer's system. The general availability of application-specific data translations is not addressed.

(4) Single vendor environment means that conversion of the graphic data format is not required.

(5) Bridge and Router functions provide the capabilities to interconnect LANs.

7.3.3.2 Application Decomposition

This AP calls for the specification of a system interconnection architecture that is adaptable to the seven layer OSI model structure. For the purposes of the AP it is convenient to divide the seven layers into two parts and define each of these parts as an Application Process. The approach taken is to take OSI layers 1 through 3 (Physical through Network) and define them to be the Network Communication Process. The remaining four upper layers (Transport through Application) together with the application itself are defined to be the System Communication Process. This permits treating issues of network connectivity and application compatibility/system connectivity separately. This is shown in figure 7-59.

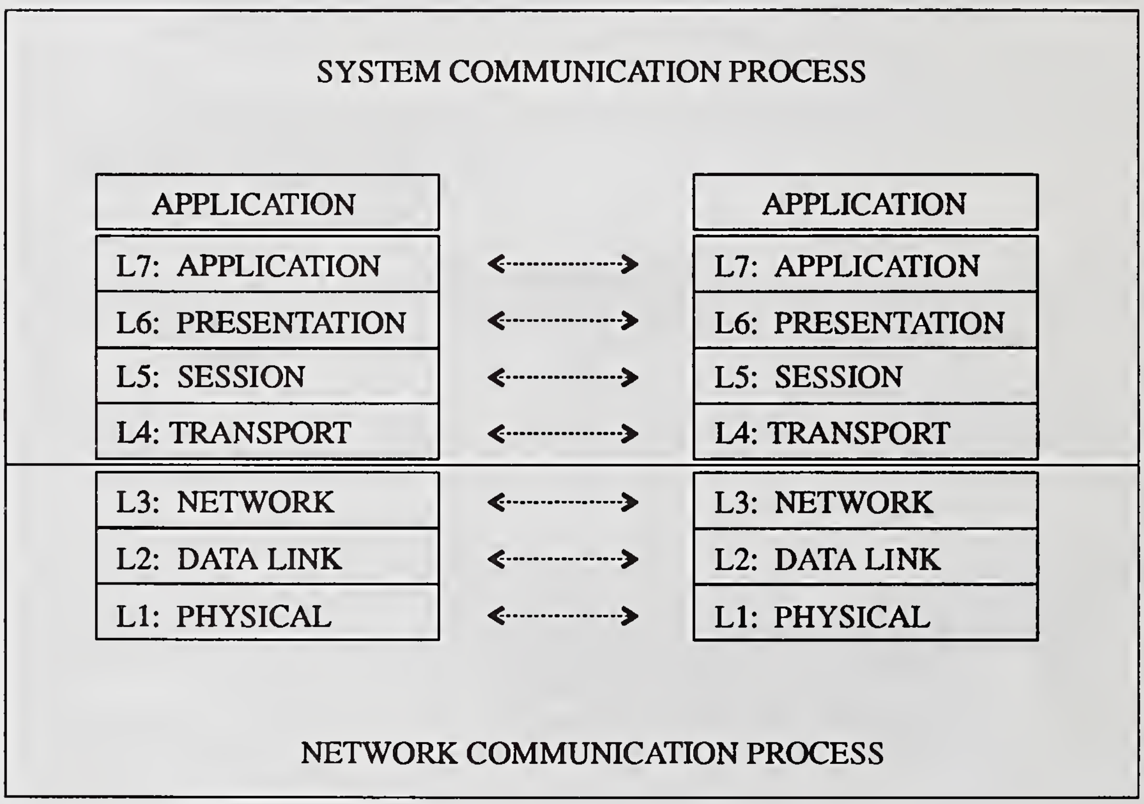


Figure 7-59. System Interconnection Architecture.

7.3.3.2.1 Network Communication Process

The Network Communication Process takes care of physical, data link, and network layer interconnection issues. These include:

- Physical Interface Connection and Conversion
- Bridging for connection of networks with the same Network Layers (Layer 2 filtering)
- Router functions for connection of networks with the same or different Network Layers (Layer 3 routing)

An architecture will be proposed that uses the ISDN Circuit Mode Services.

The ISDN connectivity issues required for managing an ISDN Circuit Mode connection for this Application Profile are all contained in the Network Communication Process. These ISDN connectivity issues include:

- User plane OSI Address mapping to control plane ISDN numbers
- Bandwidth selection based on network or systems communications processes

7.3.3.2.2 System Communication Process

The System Communication Process addresses the multivendor system compatibility issues. These include:

- End-to-End Data Transport Management
- End-to-End Session Management
- Data Translation
- Application Services

7.3.3.3 Service Logic

As described above, there are five different communications configurations required by this application:

- LAN to LAN
- Workstation to Workstation
- Workstation to LAN
- Graphic Host to LAN Connected Workstation
- Workstation to Graphic Host

In order to support all of these communications configurations, three different types of Network Communication Processes and two different types of System Communication Processes are required. The discussions on the Service Logic and the Application architecture will focus on the user plane issues and not the control plane issues. That is, the discussion focuses on the Circuit Mode communications on the B or H channels, and not on the D channel communication required to control the call, since the D channel protocol usage involves only simple call establishment and disestablishment and no deviations from standard protocols are required.

Network Communication Process:

Case 1: Identical Data Link and Network layers with a Data Link protocol that is sufficiently robust for circuit switched network connections.

Examples include communications between workstations using a wide area networking protocol stack.

Case 2: Identical Data Link and Network layers with a Data Link protocol that is not sufficiently robust for circuit switched network connections.

Examples include communications between LANs that implement identical protocol stacks.

Case 3: Different Data Link and Network layers.

Examples include communications between LANs that implement different protocol stacks.

System Communication Processes:

Case 1: Identical upper layer (4-7) protocol stacks.

Examples include communications between workstations that implement the same protocol stacks.

Case 2: Differences in any of the upper layers (4-7) of the protocol stacks.

Examples include communications between workstations that implement different protocol stacks.

Table 7-4 shows which of the communications configurations use the five cases described above.

7.3.3.3.1 Network Communication Process

Case 1: Identical Data Link and Network layers with a Data Link protocol that is sufficiently robust for circuit switched network connections.

This case will generally cover systems that are communicating with each other using robust wide area network based protocol stacks. See figure 7-60.

Case 2: Identical Data Link and Network layers with a Data Link protocol that is not sufficiently robust for circuit switched network communications.

In this case a Bridging function is required for interconnecting identical LANs. The Data Link Layer Relay function in the bridge will provide a sufficiently robust link protocol. See figure 7-61.

Case 3: Different Data Link and Network layers. This case includes a routing function that is required for communication between LANs with different protocol stacks.

The Network Layer Relay function provided by the router will provide a sufficiently robust Data Link Layer and will handle the differences in the Network layer. See figure 7-62.

7.3.3.3.2 System Communication Process

Case 1: Identical upper layer protocol stacks.

This case covers communication between workstations that use the same upper layers protocol stack (Transport through Applications). See figure 7-63.

Table 7-4. Communications Configurations

	NETWORK COMMUNICATION PROCESS			SYSTEM COMMUNICATION PROCESS	
	CASE 1	CASE 2	CASE 3	CASE 1	CASE 2
LAN TO LAN		YES	YES		
WORKSTATION TO WORKSTATION	YES			YES	YES
WORKSTATION TO LAN	YES			YES	YES
GRAPHIC HOST TO LAN CONNECTED WORKSTATION	YES			YES	YES
WORKSTATION TO GRAPHIC HOST	YES			YES	YES

LAN to LAN: Only Layers 1 through 3 issues are described. The focus is on the requirements of implementing a connection between the Network Layers of the two LAN's so Layers 4 through 7 are not discussed in this AP.

Workstation to Workstation: This configuration assumes that a robust wide area network protocol is used (Network Communication Case 1).

Workstation to LAN: This configuration assumes that a robust wide area network protocol is used (Network Communication Case 1) in the link between the workstation and the LAN Communications Server that provides the network connectivity.

Graphic Host to LAN: This configuration assumes that a robust wide area network protocol is used (Network Communication Case 1).

Workstation to Graphic Host: This configuration assumes that a robust wide area network protocol is used (Network Communication Case 1).

Case 2: Differences in any of the upper layers of the protocol stack. This case covers communication between workstations with differences in the upper layers.

Figure 7-64 should be interpreted so that conversion functions are invoked only at the layers in which they are required.

7.3.3.4 Network Communication Process Architecture

The Network Communication Process is comprised of several independent processes that are treated together. This section will discuss them by OSI Layer and then describe the protocol stacks for each communication configuration.

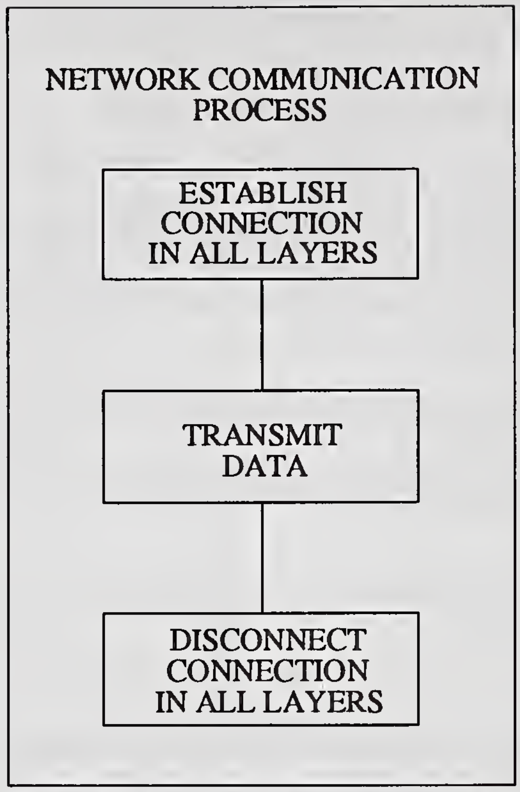


Figure 7-60. Network Communication Process Case 1.

7.3.3.4.1 Application Process Description

The Network Communication Process provides the Physical Layer through the Network Layer functions for the interconnection. It also provides any protocol conversion, bridging, or routing functions required to support the application.

7.3.3.4.2 Architecture

This section describes the protocol architecture required to support the application. It first describes each of the Layers and then shows how these layers can be combined with conversion, bridging, or routing functions to support the specific communications called for in the application. Again, this architecture discussion is addressing the user plane protocols and not the control plane protocols.

7.3.3.4.2.1 Layer 1: Physical Layer

This layer addresses the conversion of the physical interface to the appropriate ISDN interface. Table 7-5 lists the possible physical interfaces. Any one of the options in the left column could be converted to either of the options in the right hand column.

7.3.3.4.2.2 Layer 2: Data Link Layer

The Data Link Layer that will be used on the ISDN link depends on which one of the Network Communication Process Cases applies. Case 3 is discussed in Layer 3 discussion below.

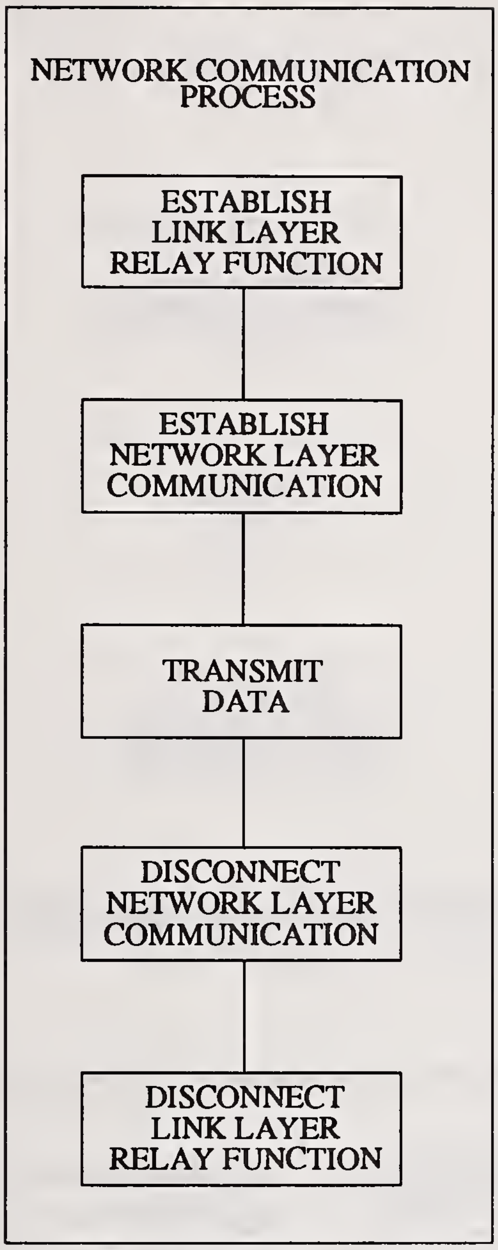


Figure 7-61. Network Communication Process Case 2.

Case 1: Identical Data Link and Network layers with a Data Link protocol that is sufficiently robust for circuit switched data network communications.

The Data Link Layer of the wide area protocol stack will be used.

Case 2: Identical Network layers with a Data Link protocol that is <u>not</u> sufficiently robust for circuit switched data network communications.

A Data Link Layer relay protocol will be used by the bridges for Layer 2 communications.

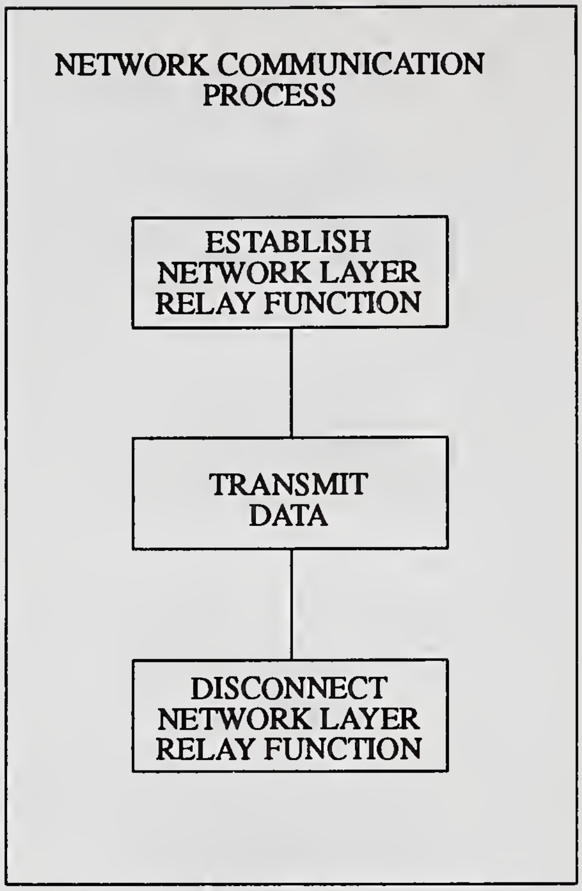


Figure 7-62. Network Communication Process Case 3.

Table 7-5. Physical Interface/ISDN Interface Conversions

R INTERFACE PHYSICAL LAYER	ISDN PHYSICAL LAYER
V.35	BRI
X.21	PRI
IEEE 802.3	
IEEE 802.4	
IEEE 802.5	
COMPUTER BUS	

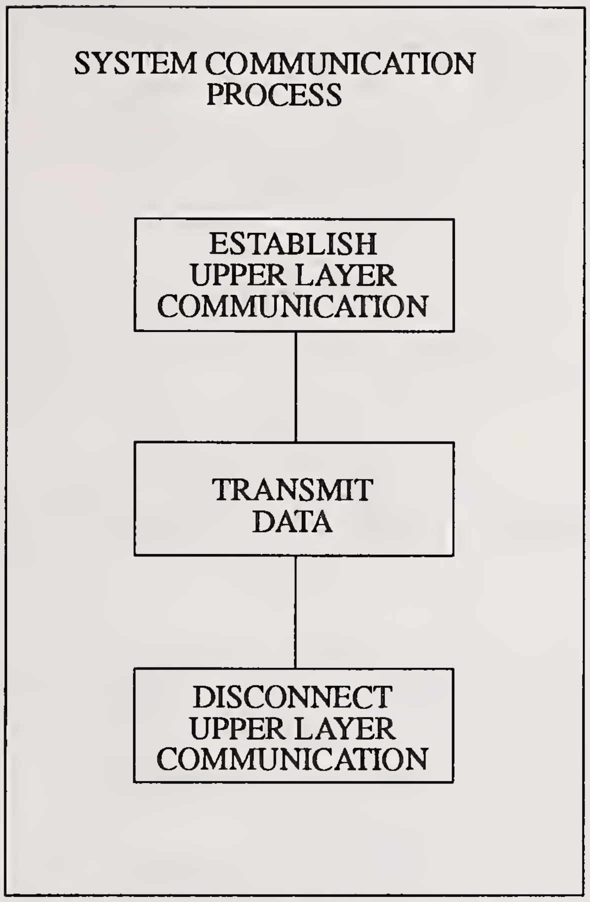


Figure 7-63. System Communication Process Case 1.

7.3.3.4.2.3 Layer 3: Network Protocol

The Network Layer protocol that will be used on the ISDN link depends on which one of the Network Communication Process Cases applies:

Case 1: Identical Data Link and Network layers with a Data Link protocol that is sufficiently robust for circuit switched data network communications.

The Network Layer of the wide area protocol stack will be used.

Case 2: Identical Data Link and Network Layers with a Data Link protocol that is not sufficiently robust for circuit switched data network communications.

The common Network Layer Protocol of the interconnected networks will be carried transparently.

Case 3: Different Network Layers.

A Network Layer relay protocol, which handles the ISDN addressing and routing issues appropriately, will be provided in the routers.

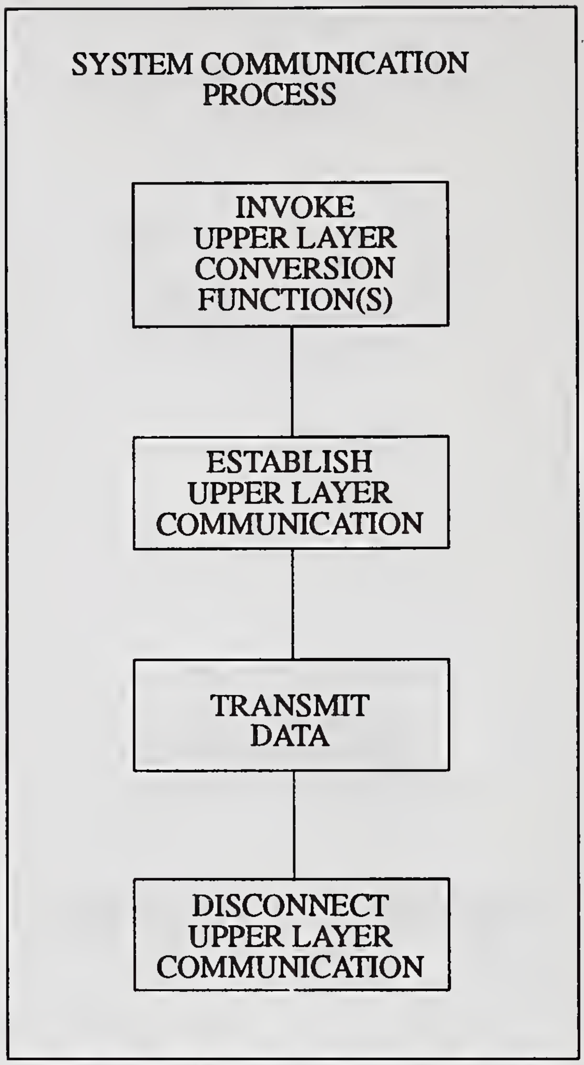
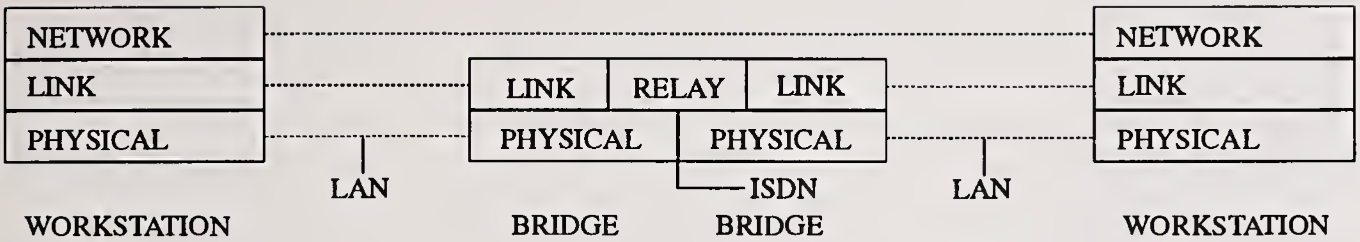


Figure 7-64. System Communication Process Case 2.

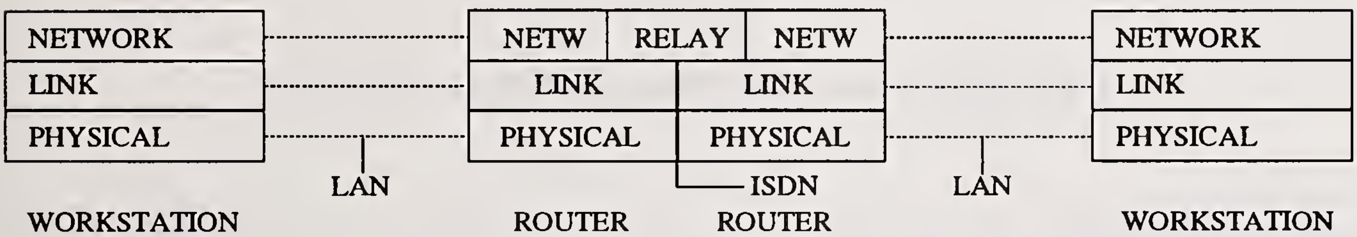
7.3.3.4.2.4 Protocol Stacks

This section includes a protocol stack diagram for each of the six Network communications configurations described in table 7-4.



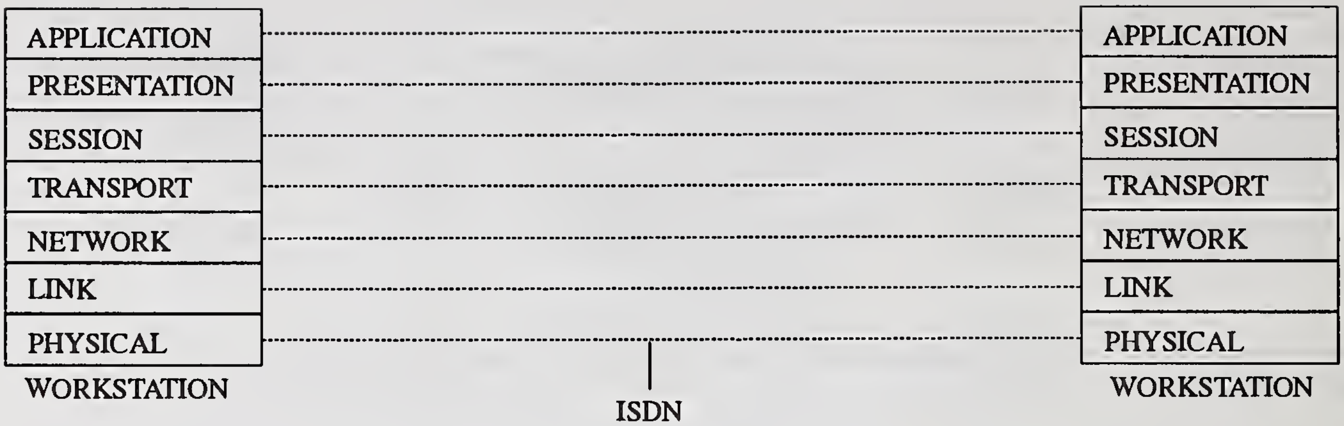
In this configuration the ISDN is used to provide the communications link between Bridges that are connected to each of the LANs.

Figure 7-65. LAN to LAN: Same Protocol Stacks.



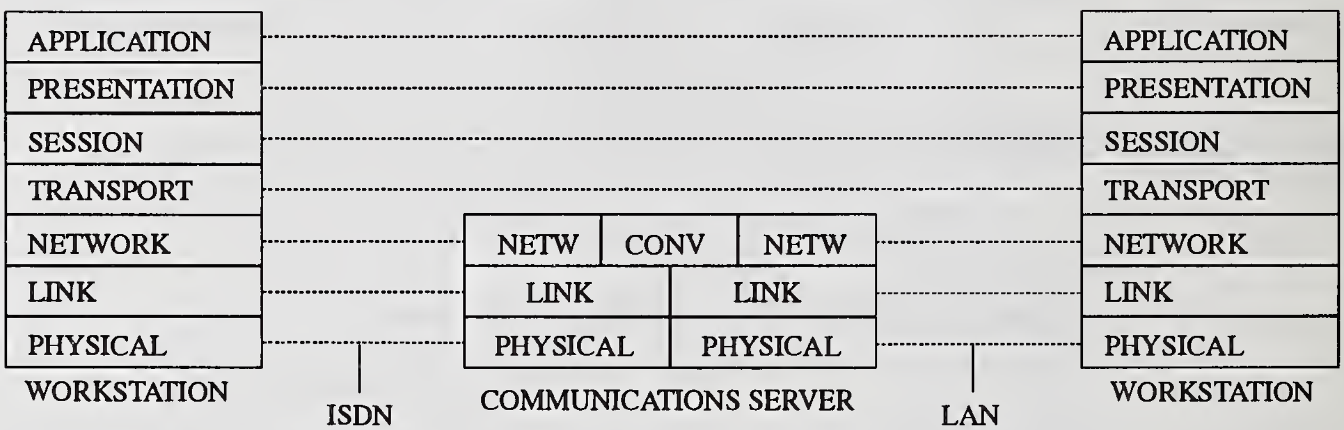
In this configuration the ISDN is used to provide the communications link between Routers that are connected to each of the LANs.

Figure 7-66. LAN to LAN: Different Protocol Stacks.



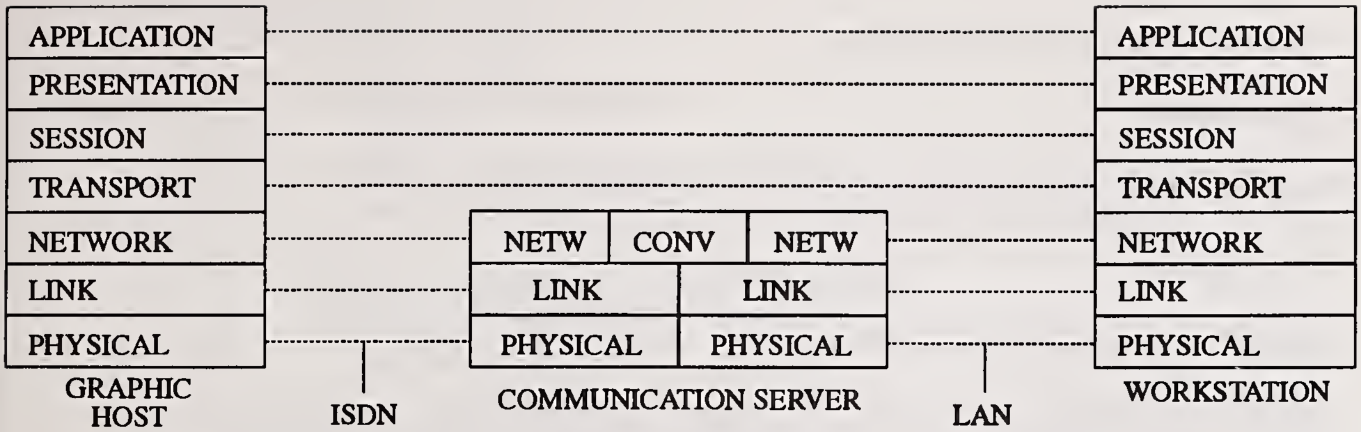
In this configuration the ISDN is used to provide the communications link between the two workstations. The workstations would communicate using a common protocol stack.

Figure 7-67. Workstation to Workstation Communications.



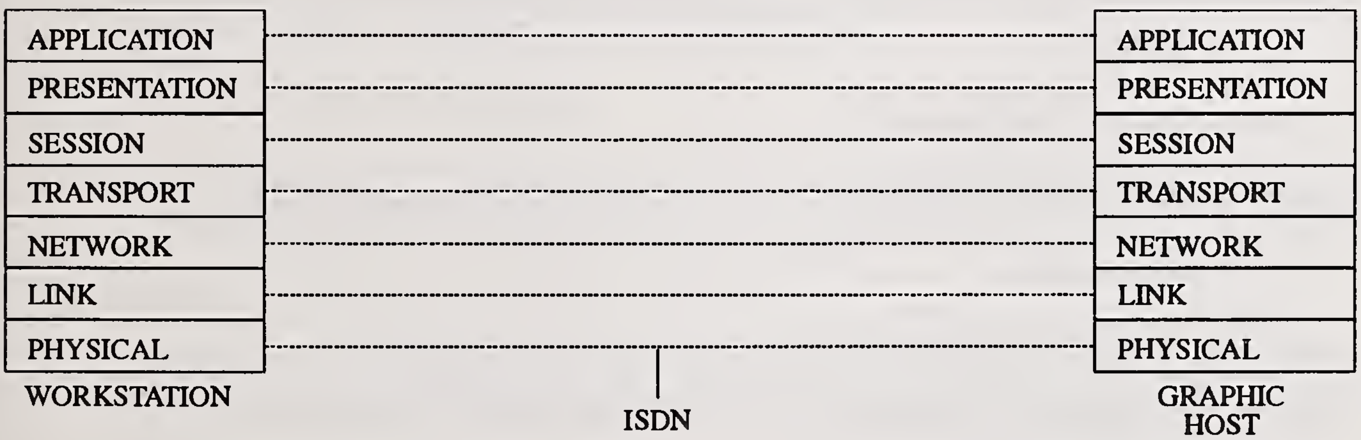
In this configuration the ISDN is used to provide the communications link between the workstation and a Communications Server, Bridge, or Router that provides remote access to the LAN.

Figure 7-68. Workstation to LAN.



In this configuration the ISDN is used to provide the communications link between the graphic host and a Communication Server that provides remote access to the LAN.

Figure 7-69. Graphic Host to LAN-Connected Workstation.



In this configuration the ISDN is used to provide the communications link between the workstation and the Graphic Host.

Figure 7-70. Workstation to Graphic Host.

7.3.3.4.3 Information Flow Diagrams

None required.

7.3.3.4.4 SDLs

None required.

7.3.3.4.5 Standard Protocol Requirements

The following ISDN protocols apply to D Channel signalling for this Application Profile. The protocols for the B Channel communications need to meet the general requirements described above.

7.3.3.4.5.1 Layer 1 Requirements

BRI Layer 1 Implementation Agreement: NIUF 92-105R1 (see section 4.1.1.2) for S/T Interface
NIUF 92-101R1 (see section 4.1.1.1) for U Interface

Options: None

PRI Layer 1 Implementation Agreement: NIUF 91-103R1 (see section 4.1.2.1)

Options: None

7.3.3.4.5.2 Layer 2 Requirements

Layer 2 Implementation Agreement: NIUF 89-210 (see section 4.1.3)

Options: None

7.3.3.4.5.3 Layer 3 Requirements

BRI Layer 3 Implementation Agreement: NIUF 90-301 (see Appendix A)

PRI Layer 3 Implementation Agreement: SSWG 303 (see Ref. [52])

Options: (Options are the same for PRI and BRI)

Optional Information Element:

Setup Message:
- High Layer Compatibility required to determine if same or different communications functions

Information Element Contents:

Bearer Capability Information Element:
- Information Transfer Capability
  - Unrestricted Digital Information
  - Restricted Digital Information

- Transfer Mode
  Circuit Mode
- Information Transfer Rate
  64 Kbps
  Note: Support for 384 kbps, 1472 kbps, and N x 64 kbps information transfer rates are also required for this application on the PRI interface.

High Layer Compatibility Information Element:
- High Layer Characteristic Identification
  OSI Application

Circuit Switched Call Control Procedures:

None

7.3.3.4.6 Conformance Criteria

7.3.3.4.6.1 Layer 1 Conformance

BRI conformance tests to support this layer 1 profile have not been written. This data will be supplied at a later date. See section 5 for the status of conformance tests.

Layer 1 PRI shall be conformant with the parts of NIUF 400-92 (Ref. [33]) that support the required functions of NIUF 91-103R1 (see section 4.1.2.1).

7.3.3.4.6.2 Layer 2 Requirements

Layer 2 shall be conformant with the parts of NIUF 91-0012 (Ref. [32]) that support the required functions of NIUF 89-210 (see section 4.1.3) and the options listed in section 7.3.3.4.5.2 above.

7.3.3.4.6.3 Layer 3 Requirements

Layer 3 BRI shall be conformant with the parts of NIUF 413-92 (Ref. [34]) that support the required functions of NIUF 90-301 (see Appendix A) and the options listed in section 7.3.3.4.5.3 above.

Layer 3 PRI shall be conformant with SSWG 303 (Ref. [52]) and the options listed in Section 7.3.3.4.5.3 above.

7.3.3.5 System Communication Process Architecture

The System Communication Process is made of several independent processes that are grouped together to simplify the higher layer view of the AP. These processes are treated as the upper four layers of the OSI stack.

7.3.3.5.1 Application Process Description

The System Communication Process takes care of all of the end-to-end communications issues that are modeled by using the upper four layers of the OSI protocol stack (Transport Layer through Applications Layer) including any required conversion and translation functions.

7.3.3.5.2 Architecture

The upper layer architecture is not treated in detail. The potential requirement for a conversion or translation function at each layer is noted.

Security is an issue that should be considered carefully in the upper layer architecture. Security is basically an upper layer, end-to-end consideration; however, ISDN services like Calling Line ID delivery should be considered as a way to enhance security. For example, the Calling Line ID could be used as a first level of security screening when it is known that the calling party may call from only one of a fixed number of locations.

7.3.3.5.2.1 Layer 4: Transport Layer

Translated as required.

7.3.3.5.2.2 Layer 5: Session Layer

Translated as required.

7.3.3.5.2.3 Layer 6: Presentation Layer

Format conversion as required.

7.3.3.5.2.4 Layer 7: Application Layer

Translated as required.

7.3.3.5.3 Information Flow Diagrams

None required.

7.3.3.5.4 SDLs

None required.

7.3.3.5.5 Standard Protocol Requirements

As required to support the end-to-end higher layer communication.

7.3.3.5.6 Conformance Criteria

As required to support the end-to-end higher layer communication.

7.4 ISDN Network Interconnectivity
7.4.1 Data Conferencing (Point-to-Point)

This proposed Application Profile (pAP) for application 810004 (Ref. [35]) Data Conferencing (Point-to-Point) is distinguished from that of International Standardized Profile (ISP) application profiles for ISDN/OSI functional standards.

The Attachments are either tutorial in nature or provide information as to extensions for pAP 810004. When a pAP is progressed through the IIW Expert Working Groups, it will then achieve a status of approved Application Profile (aAP). As contained herein, pAP 810004 is a first-order approach to identifying particular profiles that need to be expanded in the sense of Implementors' Conformance Statements (ICS), PICS, and Requirements Lists (RLs) that encompass both the application environment and the ISDN/OSI environment.

7.4.1.1 Scope

The pAP 810004 delineates a set of profiles that identify the service/protocol specifications needed in order to comply with the ISDN functional standards (de jure) for aAP 810004.

pAP 810004 is point-to-point data conferencing. Multi-way (multi-peer) data conferencing is outside the scope of pAP 810004. pAP 810004 is limited to circuit-switched profiles. pAP 810004 logical or physical realizations are outside this scope, unless they are implicit in the cited reference model or standards for pAP 810004.

De facto aspects (NetBIOS) of pAP 810004 have been mandated by the IUW of the NIUF. Circuit switched facilities are also stipulated by the IUW. OSI profiles are cited if they have been defined by other SPOs*.

7.4.1.2 Field Of Application

pAP 810004 in its future state (aAP 810004), coupled with NIUF implementation agreements, will govern compliant product implementations (physical realizations) of point-to-point data conferencing over public or private wide-area ISDNs.

Customer premise environments have either Basic Rate Access (BRA) or Primary Rate Access (PRA) network termination and may involve LANs, PBXs or Private Switched Networks (PSN).

7.4.1.3 References

ISO DISP AFTnn-1: 1989 (E); Source: Standards Promotion and Application Group (SPAG).

COS Profile Selection (1989-1990) Final Draft Version 2.0, May 25, 1989.

ISPBX Networking by ECMA, TR/NTW, 2nd Draft, agreed, April 1988.

ISO XX: 1989 (E), *Information Processing Systems - XX - Common Upper Layer Requirements.*

NetBIOS Interface to ISO Transport Services and Name Service Protocol Specification 89-00-0001-TNS (MAP/TOP)

*Standards Promotion Organizations such as NIST, ETSI, INTAP, COS, MAP/TOP, et al.

ISO TR/10000, *Information Processing Systems - International Standardized Profiles, ISO/IEC JTC1/SGFS*

Part 1 - Taxonomy Framework N109, 1989-02-15

Part 2 - Taxonomy of Profiles N126, 1989-04-13

CCITT I.Series Blue Book

ISO 9646 *OSI Conformance Testing Methodology and Framework*

7.4.1.4 Definitions

Table 7-6. Definitions

Definitions	pAP - oriented
1. ICS*	Implementation Conformance Statement is a statement by the vendor (as constrained by the applicable profiles and PICS) regarding the implemented product's compliance with the base standard(s), profiles, PICS and the requisite conformance options.
2. ISPICS*	International Standardized Profiles Implementation Conformance Statement which aligns ISP features, functions or options in the sense of static conformance requirements. This alignment includes base standards, the profiles, and implementation choices.
3. pAP/ICS	is equivalent to a pAP/RL (which is provided for each profile in a pAP) but shows the general options of the profile (as a whole) coupled with a list of protocols selected and combined in the Profile as reflected in the PICS
4. PICS	protocol implementation conformance statement
5. Profile*	a profile makes explicit the relationships between a set of standards used together. A pAP/ICS is the equivalent of a PICS. The pAP/ICS emphasizes function, service options and features. The PICS concentrates on the protocol parameters, ranges, or characteristics.
6. Requirements List (RL)	it is the purpose of an RL to specify the NIUF pAP/RL Profile's constraints on what may appear in the "Support" and "non-support" (values, etc.) columns in the relevant pAP and PICS pro forma.

*adapted from DTR/10000-1

7.4.1.5 pAP 810004 Requirements List

Table 7-7. General Level Plus Scenario Level

Field of Application	(RL) 810004	
A.A	PUBLIC	Services
A.B	PRIVATE	Services
A.C	HYBRID	Services

User/Provider Feature Set	(RL) 810004
X.U	Peer User(s) Types
X.R	Server Types
X.D	Domain Types

Table 7-8. General Level plus Scenario Level plus Functional Level

Field of Application	(RL) 810004
A.A1	User's CPE - Public Service
A.A5	Peer User CPE - Public Service
A.B1	User's CPE - Private Service
A.B6	Peer User's CPE - Private Service
A.C1	User's CPE - HYBRID Service
A.C7	Peer User's CPE - HYBRID Service

User/provider Feature Set	(RL) 810004
X.1F	no peer user
X.2F	one (1) peer user
X.5F	server coincident with user
X.6F	servers are symmetric
X.4F	one domain (multi-in-sessions)
X.8F	symmetric peer domains (multi-in-sessions)

Table 7-9. All 810004 "leafs"

Field of Application	(RL) 810004 leafs	branch
A.A11	TE1	PUBLIC
A.A12	TE2	PUBLIC
A.A13	NT2 (S/T)	PUBLIC
A.A14	PSN (S/T)	PUBLIC
A.A57	NT1 (T)	PUBLIC
A.A58	peer user LLF	PUBLIC
A.A59	peer user HLF	PUBLIC
A.B11	TE1	PRIVATE
A.B12	TE2	PRIVATE
A.B13	NT2 (S/T)	PRIVATE
A.B14	PSN (S/T)	PRIVATE
A.B67	NT1 (T)	PRIVATE
A.B68	peer user LLF	PRIVATE
A.B69	peer user HLF	PRIVATE
A.C11	TE1	HYBRID
A.C12	TE2	HYBRID
A.C13	NT2 (S/T)	HYBRID
A.C14	PSN (S/T)	HYBRID
A.C77	NT1 (T)	HYBRID
A.C78	peer user LLF	HYBRID
A.C79	peer user HLF	HYBRID

Table 7-10. Requirements List

User/provider Feature Set	(RL) 810004 leafs
X.15d	file transfer, NetBIOS (no peer)
X.25d	file transfer, NetBIOS (pt-to-pt)
X.55d	file transfer, NetBIOS (coincident)
X.65d	file transfer, NetBIOS (symmetric)

7.4.1.6 pAP 810004 Conformance Requirements

See section 7.4.1.5 for details.

Table 7-11. Conformance Requirements

RL pAP 810004 features	pAProfiles Supported on CPE	pAProfiles Supported on ISDN	Conformance Option
A.A1	X, M, Q	I, M	m
A.A5	X, M, Q	I, M	m
A.B1	X, M, Q	I, M	o
A.B6	X, M, Q	I, M	o
A.C1 (ffs)	Q, V	I, M	o
A.C7 (ffs)	Q, V	I, M	o
X.2	X, M, Q	I, M	m
X.6	X, M, Q	I, M	m
X.8 (ffs)	X, M, Q	I, M	o
X.25d	X, M, Q	I, M	m
X.65d (ffs)	X, M, Q	I, M	o

M profiles are different at CPE than ISDN environments
m = mandatory conformance
o = optional conformance
ffs = for further study

7.4.1.7 pAP 810004 Configurator

Note: the following section contains all of the information from the 810004 application requirements and application analysis documents.

Figure 7-71, figures 7-73 and 7-74, and table 7-16 used in this section depict the basis for a pAP 810004 Configurator. The notion of a configurator enables functional (e.g., service overview—table 7-16) and logical (figs. 7-71, 7-73 and 7-74) models to abstract the pAP 810004 application and connectivity details.

Table 7-12. Requirements Stipulated by the IUW as Augmented by the IIW/AAG

NIUF/810004	must	want
interworking	public	private (PSN)
de facto industry LAN protocols	NETbios	PC/LAN
LAN-type access to databases		X
LAN-type ACCESS to data server		X
bearer service (ckt. switched)	64 kb/s	128 kb/s
bearer service	demand	BRA or PRA
file transfer & sharing	X	
image (graphics) flow		X
PCs and servers (IBM compat.)	X	
host		with TA
multi-peer		X
multi-sessions		X
voice		future
security	No	No
performance (128 kb/s synch'd)	ckt. switched	ffs
access arrangements	departmental	nationwide
application-independent	X	
PBX/CO-LAN/VPN/CCS #7/PSN		X
LAN media-independent		X
Addressing and/or signalling	I.Series	PSN

NOTE: ffs = for further study

Adapting the ISDN Reference Configuration, the pAP 810004 configurator is depicted in figure 7-71. This figure implies an end-to-end set of interworking (general-level) profiles based on the preceding values for the "must" requirements. This set of profiles is in table 7-13.

Table 7-13. General-Level pAP 810004 Profiles

Source	Wide-Area	Destination
a) M (MAP/TOP NETBIOS)	I.Series	M (NETbios)
b) V (file xfr, file sharing)	I.Series	V (file xfr. ...)
c) Q = M = I = LLF	I.Series	Q (...)
d) X = (.U, .R, .D)	I.Series	X ...
e) A = PUBLIC	I.Series	A ...

NOTES:

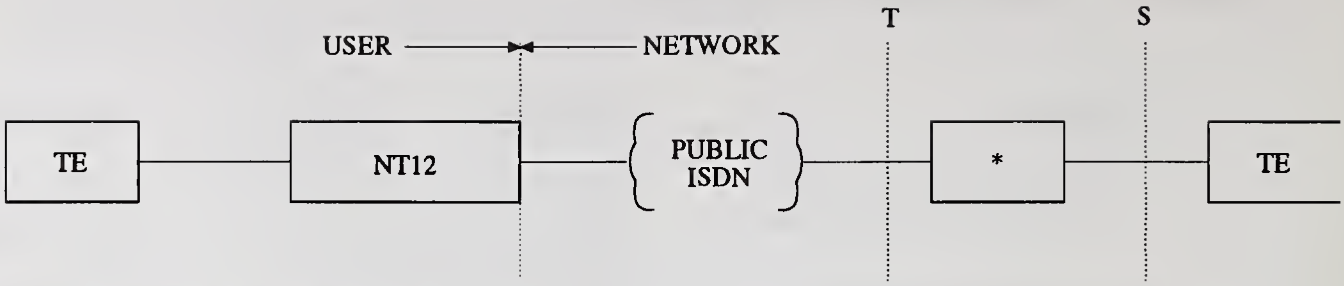
a) adopts the MAP/TOP NetBIOS Interface document and the Name Service Protocol functions.

b) enables high level functions (HLF) that denote file transfer and file sharing as utilized by application-independent means (e.g., elec. publishing, document sharing, screen sharing, etc.).

c) determines circuit switched bearer service of 1 or 2 transparent B channels on-demand.

d) addresses the user CPE as to access arrangements for types of users, types of servers, types of domains, etc.

e) isolates the field of application aligned with bearer, supplementary or teleservice functions.



Where network facilities are circuit switched

* - NT2 or NULL

Where TE may be a host (via TA&R reference point)

Where NT12 may be:
A) PSN of one or more ISxyz: Where xyz may be
B) Sub-network configuration of one or more of
I) ISLAN
II) ISPBX
III) Centrex/CO-LAN
IV) LAN G/W or IWU

Figure 7-71. pAP 810004 Reference Model.

Figure 7-73 further refines or simplifies figure 7-71 to the extent that the "basic" pAP 810004 products need only deal with symmetric CPE environments and interoperability, namely:

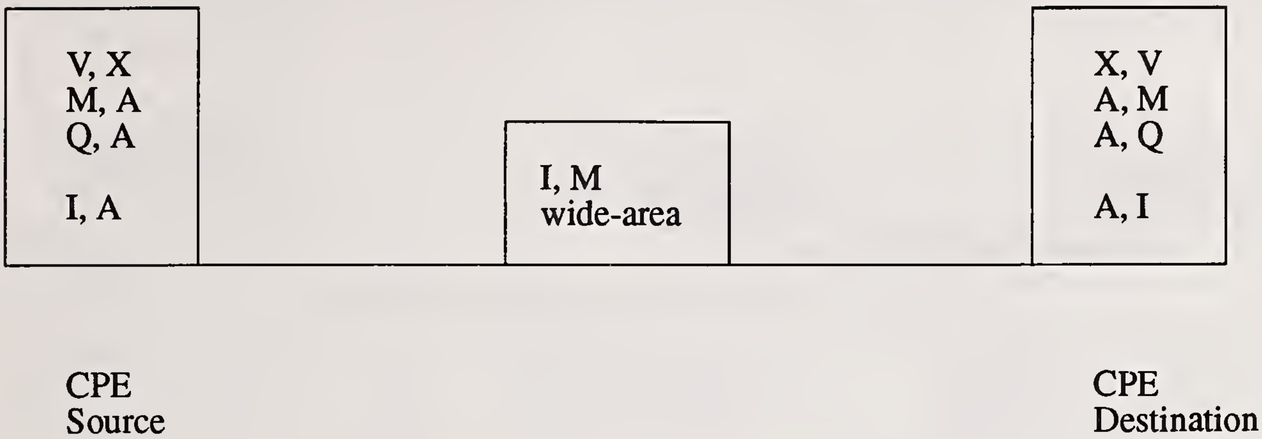


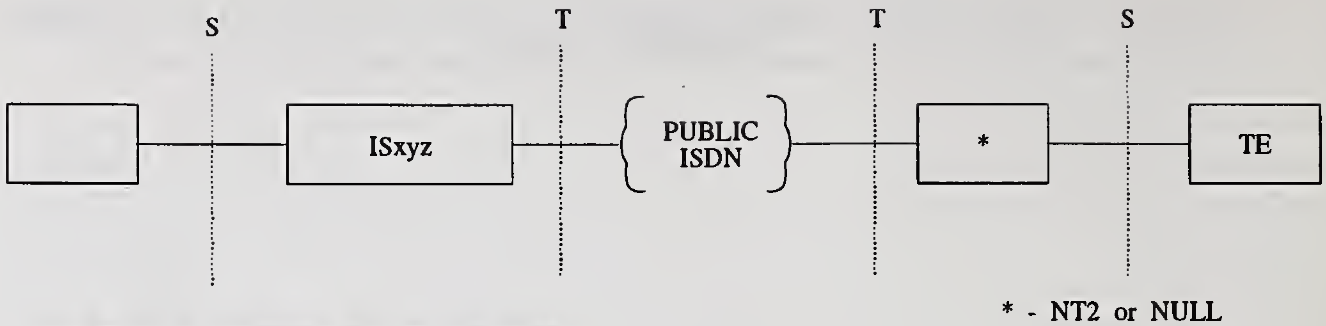
Figure 7-72. pAP Profile Stacks.

This aligns the prior figure 7-71 discussion with the above stacks as follows:

b), d) = V, X	c), e) = Q, A
a), e) = M, A	e), (w/a) = I, A

See notes a-e after General-level Profile in this section.

This alignment reveals that wide-area (w/a) ISDN connectivity is based upon I.Series and SPO [M] profiles that are to evolve via NIST (NIUF), ETSI (EWOS), INTAP (AOW), etc., for provider services.



Where ISxyz is represented as NT12 in Figure 1.

NOTE: "Basic" means one sub-network type in CPE (Customer Premise Environment)

Figure 7-73. pAP 810004 Basic Configuration.

Figure 7-74 is the "extended" pAP 810004 configurator which is outside the scope of this pAP 810004 (point-to-point) "basic" configurator.

The purpose of including the pAP 810004 extended configurator is to encourage vendors to adopt general-purpose architectural criteria when setting out to meet pAP 810004 requirements.

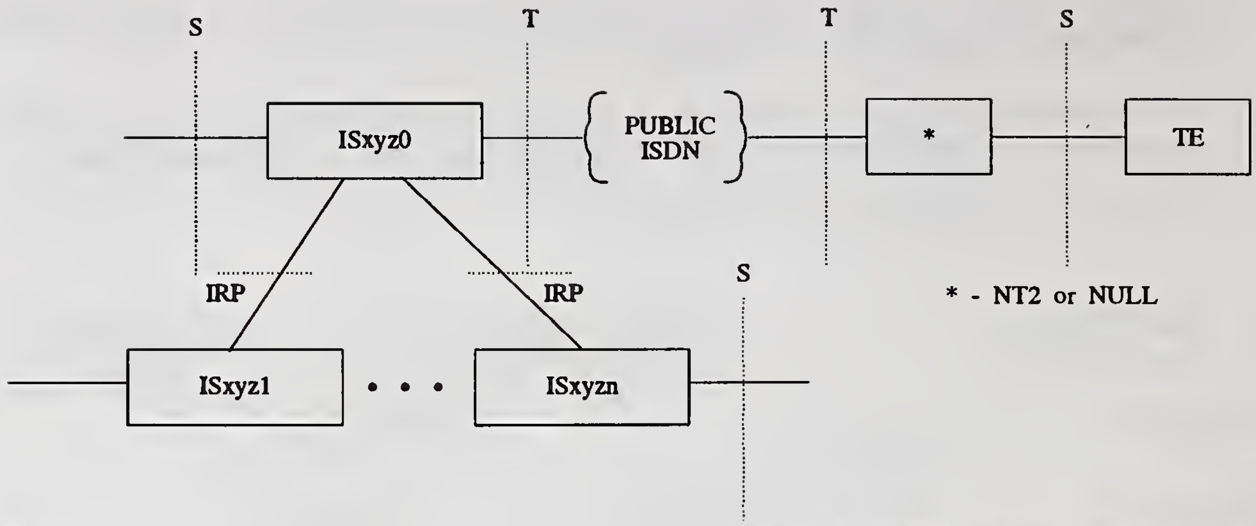
Table 7-14. Extended pAP 810004 Configurator*

ISDN customer premise end point		Private Switched (NT12) network (ISDN)	ISDN carrier network
on-demand			on-demand
open	(B)	null	dial-up (P)
on-demand		on-demand	on-demand
open	(B)	(p) open availability	dial-up (P)
(p,P) shared-facility	(E)	+ exclusive-use (P)	dial-up
CUG	(E)	exclusive-use (P)	dial-up
(P) off-net	(E)	gateway (p/P)	dial-up
open	(B)	null	CO-LAN
CUG	(B)	null	PVN
dedicated end point			dedicated (leased)
leased	(B)	(p) permanent	pure ckt. switched
leased	(E)		ckt. switched/ISDN signalling control
dedicated end point		dedicated (leased)	dedicated (leased)
leased	(B)	(p) pure ckt. switched	pure ckt. switched
leased	(E)	(P) ckt. switched/ISDN signalling control	ckt. switched/ISDN signalling control
pre-established-channels (E)			permanent (P)
channel assoc. signalling		null	ckt. switched/ISDN signalling
pre-established-channels (E)		permanent (p)	
shared facility		channel assoc. signalling	ckt. switched/ISDN signalling
CUG		channel assoc. signalling	ckt. switched/ISDN signalling
off-net		channel assoc. signalling + gateway (p/P)	ckt. switched/ISDN signalling
		permanent (p)	permanent (P)
shared facility		intra-PSN	invisible
CUG		intra-PSN	invisible
off-net (ffs)		intra-PSN	invisible

P = public
p = private
intra-PSN = PVN

B = basic configurator
E = extended configurator

*deduced from ECMA ISPBX TR/XX



Where

0, 1, ..., n	Are Circuit-Switched NT2
0, 1, ..., n	Are Circuit-Switched Sub-networks
0, 1, ..., n	Are Dedicated (NT2) Channels e.g., PRI or PVN or PSN

NOTE: IRP-ISDN Reference Point (T, K* or N*)

Where
N* = ISDN To Another ISDN
K* = Dedicated Network to ISDN
AND * = IWF Inside/Outside Reference Configuration

Figure 7-74. pAP 810004 Extended Configuration.

Table 7-16 is the overall framework for the pAP 810004 configurator. It is also an overview of a service model. The properties of this framework are addressed in the Attachments.

The key aspects of the table 7-16 framework include:

• the notion that the carrier backbone network is augmented by a private network backbone in the sense of ISDN ISP profiles

• such augmentation is facilitated by profiles for Basic low layer functions (BLLF) that are aligned end-to-end across private and/or public sub-networks. Similarly, Additional LLFs are so aligned (ALLF). High-level functions may also be augmentations to both the (basic and additional) carrier and private backbones

• these Basic and Additional functions are provider-oriented in the sense of supporting the user's application environment. This notion of augmentation, when extended into the user's application environment, leads to further value-added application(s) augmentation as the following examples depict:

Table 7-15. pAP Configurator Descriptors (E) (examples only)

User/Provider Feature Set Aspects	user		provider	
	VLLF	VHLF	VLLF	VHLF
service	B		B, A	B, A
application	S	N	S	N
features	-		-	
interfaces	S		S	

user/provider related descriptors
where V = value-added
S = supported
N = non-supported
- = profile RLs

backbone-related descriptors
B = basic LLF or HLF
A = additional LLF or HLF

• the substance of the above notions, augmentations and alignments, are administered via requirements list(s) at each plateau (carrier, private, CPE). The RLs are the fundamental application of the pAP taxonomy which is detailed in the Attachments. Viewed as a tree with trunk, branches and leaves, it enables each pAP/RL to denote work items or work-to-be-done in the sense of implementation agreements.

Table 7-16. pAP 810004 Service Overview

	pAP-810004		
Customer Premise Environment	User/Provider Feature Set	810004 RL	Field of Application
	AHLF ALLF	PSN RL	BHLF BLLF
Wide-Area Network	AHLF ALLF	ISDN RL	BHLF BLLF

RL - Requirements List
HLF - High Layer Function(s)
LLF - Low Layer Function(s)
PSN - Private Switched Network
B = Basic
A = Additional

NOTE: PSN and ISDN HLF and LLF May differ

7.4.1.8 Attachment 1—Proposed Application Profile (pAP) Overview

The following pAP concerns are separate:

I. ISP Profiles per part 1, section 6 of TR/10000

- A. Standards
- B. Registration Mechanisms
- C. Conformance

II. IIW Profiles per the NIUF

- A. Environment (Application)
  1. Application Requirements (IUW)
  2. Application Analysis (IIW)
- B. User/Provider Interaction
- C. Application Requirements List
- D. SPO Profile Selection
- E. I.Series Services
- F. NIUF Conformance

The following pro forma outline of a pAP is based on the notion that a service-oriented model should convey a sufficient set of properties of a pAP which are aligned with standardized functions and options (in the sense of profiles) to enable implementors to succeed in having their pAP-derived products interoperate.

pAP products may be realized via application, product, service, or combinations thereof:

<u>pAP pro forma</u>

1. Scope
   1.1 Functional Model (Service-oriented)
   1.2 Objective Criteria
   1.3 Field of Application

2. Services
   2.1 Service Elements/Class
   2.2 Features/Functional Units
   2.3 Facilities/Interworking

3. Profiles
   3.1 Identify
   3.2 Requirements List - pAP
   3.3 Implementors' Conformance Statement (ICS) pAP

4. Conformance Requirements

The root structural identifier for a proposed Application Profile (pAP) is designated as

pAP xxxxxx

This identifier assumes the Application Environment definitions per the IUW treatment of xxxxxx which is the numeric IUW identifier for each ISDN-oriented application.

7.4.1.9 Attachment 2—pAP Taxonomy Overview

The pAP identifier structure is extended for user/provider interplay and for user/network, or user-user signalling: The general form of the schema is

$$\gamma.\Delta\chi\chi\chi$$

where

γ = the major structural identifier for the general-level
Δ = the minor structural identifier for sub-levels of organization of the general-level
$\chi\chi\chi$ = the particular sub-levels as defined by Δ

if Δ = S it signifies the scenario-level of interaction within a particular general-level identifier

if Δ = s F it signifies the functional-level of interaction within the scenario-level identifier(s)

if Δ = s f P It signifies the protocol-level of interaction within the functional-level identifier which is within the scenario-level (s f)

finally, where Δ is <u>Physical-level</u>

.D	signalling channel
.B	basic rate access
.E	primary rate mux channel
.H	wide-band rate access

the schema shifts so that the physical-level identifier always occupies first position in the schema following the decimal point;

thus γ.xxxx is
.D s f p
.B s f p
.E s f p
.H s f p

The latter identifiers are the most subordinate in the pAP Taxonomy and are the "leaf" of the pAP Taxonomy "tree" of profiles. These leaf profiles may enable such details and options like attachment speeds and connectors to be registered by the pAP identifier. This specificity is for further study.

pAP Schema Overview

The pAP Application Environment resides within the Customer Premises Environment unless Enhanced Service Providers are part of the service interworking.

The root identifier [pAP xxxxxx] and related definition of the Application Context (signals from the environment) is linked to general-level profile identifiers such as:

X	user/provider feature set
R	requirement list
A	field of application
M	Standards Promotion Organizations (SPO) profile selection
I	ISDN I.Series base standards

NOTE: M profiles may encompass I profiles

When the general-level designator <M> is used in the sense of the I profiles, it extends the schema and profile descriptor's beyond the Application Environment designators <X>, <R>, and <A> to the standardized ISP realm of profiles.

When $\gamma.\Delta$ is M.Δ it depicts SPO general-level profiles

and if Δ is it is	general-level
2	I.200 Series
3	I.300 Series
4	I.400 Series
5	I.500 Series
6	I.600 Series

The pAP Application resides on customer premise sub-networks/equipment/environment. Such CPE may be as small as one sub-network or as large as an extensive private switched network. The structural profile identifiers for the CPE/PSN backbone are

Q	Low Layer Compatibility Functions
V	High Layer Compatibility Functions

7.4.1.10 Attachment 3—pAP 810004 Tutorial

Organization

The service framework depicted in table 7-16 is structured in a top-down manner. This structure incorporates two independent stacks of profile factors, the field-of-application stack and the user/provider feature-set stack, which are separated by RL identifiers.

NOTE: The profile factors "stacks" should not necessarily be interpreted as protocol stacks.

The structure depicted in table 7-16 is an integrated layered-view of the properties of the pAP 810004 taxonomy (based on Attachment 4), the pAP 810004 application and the pAP 810004 configurator (basic and extended—pages 7-93 through 7-102).

The middle column of table 7-16 depicts pAP 810004, PSN and ISDN requirement lists (RL) which are descriptors that are dependent on the two types of profile stacks mentioned in the first paragraph. This means that particular realizations of pAP 810004 will encompass RL selected profile factors, services, features and conformance requirements. These RLs are directly related to pAP 810004 profile attributes in contrast to generic properties of the taxonomy, configurator, application, service, conformance, or features.

NOTE: Attachment 1 is also an attempt to separate pAP 810004 intrinsic matters, e.g., services, from pAP 810004 extrinsic realization matters, e.g., profile ICSs.

Reference Model

Returning to table 7-16, the structure discussed in Organization above displays the following dependencies whereby the application (pAP 810004), premises (CPE, PSN and provider support), and intervening networks (ISDN WAN) are unified in terms of services, application, function, features, reference configurations and everything short of particular de facto logic and implementation details.

The table 7-16 depiction suggests the pAP 810004 top-most-level is the umbrella for all the subsidiary levels and profile stacks. It may also imply that this umbrella dictates the contextual requirements and context/scope for the underlying levels/sub-networks/networks.

The level below pAP 810004 is labeled "Customer Premise Environment" and this level has two sub-levels. The major sub-level directly addresses pAP 810004 user/provider feature sets and services that are distinguished from underlying PSN provider functions, services, support and interworking. The PSN sub-level is an intervening sub-networking infrastructure which visibly (to the user sub-level) connects the various premise interfaces to the user/application service elements or functional groupings per the reference configurations.

The orientation of table 7-16 with A = additional—at the left profile stack—and B = basic—at the right hand profile stack—means that the BLLF and BHLF may be designated for either the ISDN WAN and/or PSN intervening networks whereas the ALLF and AHLF are considered user-premise extensions. In other words, "Basic" is a property of intervening provider facilities, and Basic facilities may only be overlaid by "Additional" user provisioned resources, albeit networked, which are not visible to intervening provider resources.

Table 7-17 is an attempt to consolidate the foregoing pAP 810004 "tutorial" notions by recasting table 7-16 in order to depict a more traditional end-to-end topology for the pAP 810004 application umbrella. Table 7-16 was designed to stress the types of profile factors needed to adequately describe pAP 810004 in generic terms, independent of source or destination realizations.

Table 7-17 stresses user/provider feature sets in the form of high-level (HLF) or low-level (LLF) functions stacked according to basic (B), additional (A) and value-added (V) service interworking across the ISDN WAN (the basic capability), the ISDN PSN (the additional capability), and the ISDN user functions (the value-added capability).

Using table 7-17 and beginning at p. 7-90 (section 7.4.1.5. pAP 81004 RL [General-plus scenario-level]), it should be discernable what might be the particular properties of a point-to-point pAP 810004 profile, including configurator and conformance parameters.

Table 7-17. pAP 810004 Distributed Networked Resources Example

		pAP 810004			
CPE	VHLF	teleservice ESP (IWF outside ISDN)			VHLF
CPE	VLLF	teleservice database retrieval			VLLF
CPE / PSN	AHLF	NETbios file transfer			AHLF
CPE / PSN	ALLF	permanent intra-PSN (CUG) B-Channels			ALLF
WAN	BHLF	closed user group	BHLF	supplementary service	BHLF
WAN	BLLF	circuit-switched	BLLF	B-Channels	BLLF
	Source CPE		ISDN WAN		Destination CPE

7.4.1.11 Attachment 4—Application Profile (pAP) Taxonomy

NOTE: See Attachment 2 for definitions and summary details.

When the general-level is distinguished using the schema and scenario-level, it enables trees to be structured which have their roots in the general-level identifiers, for example:

when		is		
	γ.Δ		A.S	it is the scenario-level of the field of application
and when		is		it signifies that this profile is based on PUBLIC services
	A.S		A.A	
and when		is		it signifies that this profile is keyed to PRIVATE services
	A.S		A.B	although public wide-area or transit networks may underlie the PRIVATE networks
and when		is		it signifies that the profile is a HYBRID of public/private
	A.S		A.C	services, e.g., a virtual private network (VPN) using public services

By extending the field of application tree <A> to the functional-level, it enables several branches which isolate the particular areas of the pAP 810004 Service Overview (depicted in table 7-16) as follows:

when		is		it is	
	γ.Δx		A.Ax		the functional-level of the field of application for PUBLIC services
and when		is		it is	
	A.Ax		A.A1		the user's CPE profile that is being addressed
	A.Ax		A.A2		the provider's Low Layer service profile that is being addressed
	A.Ax		A.A3		the provider's High Layer service(s) profile
	A.Ax		A.A4		the provider's value-added (teleservices) that are distinguished
	A.Ax		A.A5		the profile for the peer user using PUBLIC services
	A.Ax		A.A6		the profile for multi-peer users using PUBLIC Services

NOTE: peer (recipient) user's of PUBLIC services are virtually the same as the originating user's profile.

when		is		it is	
	γ.Δx		A.Bx		the functional-level of the field of application for PRIVATE services
and when		is		it is	
	A.Bx		A.B1		the profile for the user's (originator) CPE
	A.Bx		A.B2		the profile for the user's (originator) PSN Low Layer Functions
	A.Bx		A.B3		the profile for the user's (originator) PSN High Layer Functions
	A.Bx		A.B4		the profile for the user's (originator) PSN value-added (teleservice)
	A.Bx		A.B5		the profile for the user's (originator) PSN value-added provider, i.e., ESP
	A.Bx		A.B6		the profile for the peer user (recipient) CPE
	A.Bx		A.B7		(same as A.B2) for the peer user PSN LLFs
	A.Bx		A.B8		(same as A.B3) for the peer user PSN HLFs

	A.Bx	A.B9	(same as A.B4) for the peer user PSN VAFs
	A.BX	A.B0	(same as A.B5) for the peer user PSN ESP

NOTE: A.B6 thru A.B9 & A.B0 apply to the recipient peer user

when	is	it is	
	γ.Δx	A.Cx	the functional-level of the field of application for HYBRID services.

and when	is	it is	
	A.Cx	A.C1	the profile for the user's (originator) CPE using HYBRID services
	A.Cx	A.C2	the profile signifies a user's (originator) PSN's use of HYBRID services
	A.Cx	A.C3	the profile for the user's VPN using PUBLIC service(s)
	A.Cx	A.C4	the profile for the user's VPN using PRIVATE service(s)
	A.Cx	A.C5	the profile for user's CENTREX/CO-LAN using PUBLIC services
	A.Cx	A.C6	the profile A.C5 but using PRIVATE services
	A.Cx	A.C7	the profile for the peer (recipient) user's CPE using HYBRID services
	A.Cx	A.C8	peer (recipient) user's PSN use of HYBRID services
	A.Cx	A.C9	peer (recipient) user's VPN using PRIVATE services
	A.Cx	A.C0	peer (recipient) user's CENTREX/CO-LAN using PRIVATE services

NOTE: peer (recipient) user's of PUBLIC services are virtually the same as the originating user's profile

when	is	it is	
	γ.Δxx	A.s f P	the protocol-level of the field of application

and when		it is	
		A.A f P	the protocol-level of the field of application for PUBLIC services

likewise		are	
		A.B f P	the protocol-levels of the field of application for PRIVATE
		A.C f P	and HYBRID and services respectively

when	is	it signifies the profile	
	A.s f P	A.s f 1	for TE1
	A.s f P	A.s f 2	for TE2
	A.s f P	A.s f 3	for NT2 (S/T)
	A.s f P	A.s f 4	for PSN (S/T)
	A.s f P	A.s f 5	for PSN (N_x)
	A.s f P	A.s f 7	for NT1 (T)
	A.s f P	A.s f 8	for peer user LLF
	A.s f P	A.s f 9	for peer user HLF
	A.s f P	A.s f a	for peer provider LLF
	A.s f P	A.s f b	for peer provider HLF
	A.s f P	A.s f c	for peer provider value-added (teleservice)

NOTE (1): when the above profiles have an f=1; it signifies the user's (originator) CPE use of visible PUBLIC services for the intervening ISDN WAN

NOTE (2): both "a" and "b" and "c" may associate with the N_x reference point to another ISDN

NOTE (3): for the above profiles, when s = A or B and f = 2, 3, or 4 respectively for the above profiles p = 7, 8, and 9

NOTE (4): A.s f 6 and A.s f d are reserved for future use

when	is		it signifies the profiles for:
	A.s f P	A.s f k	peer provider LLF and IWF is inside ISDN
	A.s f P	A.s f l	peer provider HLF and IWF is inside ISDN
	A.s f P	A.s f m	peer provider value-added (teleservice) and IWF is inside ISDN
	A.s f P	A.s f n	peer provider LLF and IWF is outside ISDN
	A.s f P	A.s f o	peer provider HLF and IWF is outside ISDN
	A.s f P	A.s f p	peer provider value-added (teleservice) and IWF is outside

When the functional-level (f=2) then P=k at the protocol-level and N_x=IWF is (inside) ISDN

When the functional-level (f=3) then P=l at the protocol-level and N_x=IWF is (inside) ISDN

When the functional-level (f=4) then P=m at the protocol-level and N_x=IWF is (inside) ISDN

When the functional-level is f=2, 3, or 4 and P=n, o, or p respectively, then N_x=IWF is (outside) ISDN in each case

when	is		it signifies the protocol-level functions for
	γ.Δxx	A.A f P	PUBLIC Services
		A.B f P	PRIVATE Services
		A.C f P	HYBRID Services

and when		it designates the following protocol-function categories
	P=H	Connection Handling
	P=Z	Routing
	P=R	Resources Handling
	P=S	Supervision
	P=M	Operation and Main
	P=I	Interworking
	P=C	Charging
	P=P	L-2/-3 data unit handling (packet mode)

For the general-level user/provider feature set the specific structural identifiers for the scenario-level follow:

when	is		it is
	γ.Δ	X.S	the scenario-level of the user/provider feature set

and when	is		
	X.S	X.U	the variable U signifies the number of conferencing users (peer-to-peer)

so when				it signifies
	U=1			no peer user
	U=2			one peer user, i.e., point-to-point
	U=3			multi-peer users
and when		is		
	X.S		X.R	the variable R signifies the number of independent server domains
so when				it signifies the
	R=5			server is coincident with the user CPE
	R=6			servers are symmetric with peer users (point-to-point) or multi-peer users
	R=7			server(s) is asymmetric with peer users including being in a separate CPE from peer users or multi-peer users
and when		is		
	X.S		X.D	the variable D signifies the type of CPE domains that contain users and/or servers
so when				it signifies
	D=4			one domain which encompasses U=1 and R=5 but may have multiple users in-session with their respective servers
	D=8			symmetry of peer-to-peer domains and encompasses U=2 or 3 and R=6 but may signify multi-in-sessions between peer domains
	D=9			multi-peer domains which are symmetric as to users and servers U=3 and R=6 but may signify multi-in-sessions between multi-peer domains
	D=0			multi-peer domains which are asymmetric as to users and associated servers U=3 and R=7 but may also signify multi-in-sessions between multi-peer users and asymmetric server domains
when		is		it is
	$\gamma.\Delta x$		X.s F	the functional-level of the user/provider feature set
when		then		
				<u>Functional Components</u>
	F=i			Hold Invocation (disconnect & reservation)
	F=f			Retrieve (reestablish)
	F=n			Notify (inform, no response)
	F=e			Inquire
	F=t			Transfer
	F=j			Join (multiparty)
	F=a			Adjourn
	F=r			Reroute (to alternate address)
	F=m			Monitor (watch for Event)
	F=x			Restart
	F=s			Split (from a multipart connection)

7.4.1.11.1 Other Profile Taxonomy Matters

The capabilities of the user/provider feature set encompasses the Application/Service/User Program set, the Application Layer (7) Systems servicing the former set(s), the Upper Layer Architecture as regards directory services, Security and Network Management, and all Application Platforms whether software or hardware which form the infrastructure to support the former set(s).

The pAP Taxonomy reserves a number of structural identifiers for several types of service-independent/scenario profiles for user-type CPE/PSN environments, as follows:

Identifier	User Processing Environment
X.V	Application Programs
X.W	Communications Processes
X.Q	Application Platforms

The user/provider feature set may also address the classical OSI Reference Model application-layer.

when		is extended to	
	X.s F		the OSI Functional-level
and		is a	Provider Feature Set
	F=1		Directory
	F=2		Security
	F=3		Management
	F=4		(reserved)
	F=5		File Transfer
	F=6		Virtual Terminal
	F=7		Message Handling
	F=8		Transaction Processing
	F=9		Remote Database Access
	F=0		Job Transfer & Manipulation

This enables the functional-level designator to distinguish the particular protocol-level by the following extension

when		is extended to the Protocol-level	
	X.s f P		
and when		is	
	X.s 5		file transfer
then		is	Protocol-identifier
	X.s 5 a		FTAM (file transfer access and management)
	X.s 5 b		FTP (file transfer protocol)
	X.s 5 c		NFS (network file system)
	X.s 5 d		NetBIOS
	X.s 5 e		(reserved)

when		is		it is
	γ.Δ		2.S	the scenario-level for the CCITT I.200 series which identifies types of services

where		is the	
	2	type of ISDN service described in the CCITT I.200 series	
if			
Δ = Z,Y,X,...		types of CCITT I.200 bearer services, e.g., circuit-mode	
if			
Δ = a,b,...,z		types of CCITT I.200 supplementary services of basic functional components	
if			
Δ = A,B,C,...		types of CCITT I.200 signalling channel management services	
if			
Δ = ...		types of CCITT I.200 management services	

NOTE: .... = any unused alpha designator

when		is	then	
	$\gamma.\Delta$		2.S	CCITT I.200 services may be registered at the scenario-level

thus		is	category
	2.X		circuit-mode
	2.Y		packet-mode
	2.Z		signalling-mode
or		is	Supplementary Service function (SS)
	2.a		Number Identification
	2.b		Call Offering
	2.c		Call Completion
	2.d		Multiparty
	2.e		Community of Interest
	2.f		Charging
	2.g		Additional Information Transfer
when		signifies	Supplementary Service
	2.a		Number Identification
then		is	
	2.a 1		Direct Dialing In (DDI)
	2.a 2		Multiple Subscriber No. (MSN)
	2.a 3		Calling Line ID Presentation(CLIP)
	2.a 4		Calling Line ID Restriction (CLIR)
	2.a 5		Connected Line ID Presentation (COLP)
	2.a 6		Connected Line ID Restriction (COLR)
	2.a 7		Malicious Call Identification (MCI)
	2.a 8		Sub-addressing (SUB)
when		signifies	Supplementary Service
	2.b		Call Offering
then		is	
	2.b 1		Call Transfer (CT)
	2.b 2		Call Forwarding Busy (CFB)
	2.b 3		Call Forwarding No Reply (CFNR)
	2.b 4		Call Forwarding Unconditional (CFU)
	2.b 5		Call Deflection (CD)
	2.b 6		Line Hunting

when		signifies	Supplementary Service
	2.c		Call Completion
then		is	
	2.c 1		Call Waiting (CW)
	2.c 2		Call Hold (HOLD)
	2.c 3		Completion of calls to busy subscribers (CCBS)
when		signifies	Supplementary Service
	2.d		Multiparty SS
then		is	
	2.d 1		Conference Calling (CONF)
	2.d 2		Three Party Service (3PTY)
when		signifies	Supplementary Service
	2.e		Community of Interest SS
then		is	
	2.e 1		Closed User Group (CUG)
	2.e 2		Support for Private Numbering Plan (SPNP)
when		signifies	Supplementary Service
	2.f		Charging SS
then		is	
	2.f 1		Credit Card Calling (CRED)
	2.f 2		Advice of Charge (AOC)
	2.f 3		Reverse Charging (REV)
when		signifies	Supplementary Service
	2.g		Additional Information Transfer
then		is	
	2.g 1		User-to-User Signalling (UUS)
when			it is
	Δ = A,B,C...		types of CCITT I.200 signalling channel management services
then		signifies	category[14]
	2.A		Telephony (E)
	2.B		Telephony (A)
	2.C		Teletex (A)
	2.D		Telefax 4 (A)
	2.E		Mixed Mode (A)
	2.F		Videotex (A)
when		is	it is
	γ.Δ		3.S the scenario-level of the CCITT I.300 Series
and when		is	
	S		ISDN reference points

[14]from I.230:
(E) an essential access arrangement or bearer service category
(A) an additional access arrangement or bearer service category

then		is		
	S=K			existing telephony n/w or dedicated
	S=M			specialized service provider
	S=N			another ISDN
	S=P			specialized n/w resource
when		is	it is	
	$\gamma.\Delta$	4.S		the scenario-level of the I.400 Series

NOTE: previously, in these Appendices, the schema was extended to identify profiles encompassing channel types, B, D, E, and H by shifting the schema at the physical-level, e.g., B s f where "s" is also the scenario-level shifted right one character.

when		is	or	
	$\gamma.\Delta$	4.S		4.Bs, 4.Ds, 4.Es, 4.Hs
then		may be		
	S(or s)		ISDN Reference Points	
such as				
	S=R			
	S=S			
	S=T			
	S=U			
	S=V			
when		is	or	
	$\gamma.\Delta x$	4.s		4.Bs, ..., 4.Hs
then			signifies	
	S(or s)			scenario-level based upon types of service
when		is	<u>scenario-types</u>[15]	
	4.B1		Dedicated (pre-established) systems connections	
	4.B3		Permanent Public network connections	
	4.B5		On-demand Public network connections	
when		is	at	
	$\gamma.\Delta xxx$	$\gamma.\Delta sF$		the functional-level
then		signifies		
	F		an extension of the various types of scenario-level facilities with designations for category of connections	
and when		it is	<u>connection category</u>[16]	
	F=l		link	
	F=t		transmission system	
	F=p		purely circuit switched	
	F=c		circuit switched/ISDN signalling	
	F=k		circuit switched/packet	

[15] adapted from ECMA ISPBX TR/NTW

[16] Ibid.

when	is	
	γ.Δs F	extended to the functional-level
and	is the	<u>connection categories</u>[17]
	F	*Dedicated*
	4.B 1 l	physical link
	4.B 1 t	transmission systems
		Permanent
	4.B 3 p	purely circuit switched
	4.B 3 c	circuit switched/ISDN signalling
	4.B 3 k	circuit switched/packet switched signalling
		On-Demand
	4.B 5 p	purely circuit switched
	4.B 5 c	circuit switched/ISDN signalling
	4.B 5 k	circuit switched/packet switched signalling
when	is	
	4.Δ s f P	extended to the protocol-level[18]
then		<u>Dedicated Connections</u> (s=l=physical link)
	4.B 1 l 1	link establishment
	4.B 1 l 2	synchronization
	4.B 1 l 3	thruput delay
	4.B 1 l 4	signalling transparency
	4.B 1 l 5	failure performance
and		
then	is	<u>Dedicated Connections</u> (s=t=transmission system)
	4.B 1 t 1	link establishment
	4.B 1 t 2	synchronization
	4.B 1 t 3	thruput delay
	4.B 1 t 4	signalling transparency
	4.B 1 t 5	failure performance

and so forth for

<u>Permanent</u>	and	<u>On-Demand</u>
4.B 3 p		4.B 5 p
4.B 3 c		4.B 5 c
4.B 3 k		4.B 5 k

---

[17]Ibid.

[18]Ibid.

NOTE: If H channels instead of B channels, then the 4.Hxxx schema is needed.

when		is	it is
	γ.Δ	5.S	the scenario-level for the CCITT I.500 series
and when		it signifies	
	5.1		Layer 1 interworking (I.511)
	5.3		Parameter Exchange (I.515)
	5.5		ISDN-ISDN interworking
	5.7		ISDN-Private Nets interworking
when		is	
	5.s F		extended to the functional-level
and		signifies	interworking functional requirements
	5.5		
then		is	
	5.5 c		common channel signalling
	5.5 x		X.75
and when		is	
	5.s f P		extended to the protocol-level
then		is	
	5.5 c k		signalling at K reference point
	5.5 c n		signalling at N reference point

7.4.1.12 Attachment 5—ISDN RL Structure

Table 7-18. Circuit-mode bearer services, from I.335

#	xfr mode	xfr rate	xfr capab.	Estab. of conn.
1.1	ckt	64	unres}	demand
1.2	ckt	64	unres} (3)	reserved
1.3	ckt	64	unres}	permanent
5.1	ckt	2x64	unres	demand
5.2	ckt	2x64	unres	reserved
5.3	ckt	2x64	unres	permanent

(3) - during an interim period some networks may only offer restricted digital information transfer capability (i.e., an all-zero octet is not allowed)

Table 7-19. Unrestricted digital connection types, from I.335

#	xfr mode	xfr rate	xfr capab.	struc	Estab. of conn.
A.1	ckt	64	unres	8 kHz	switched
A.2	ckt	64	unres	8 kHz	semi-permanent
A.3	ckt	64	unres	8 kHz	permanent
A.10	ckt	2x64	unres	8 kHz}	switched
A.11	ckt	2x64	unres	8 kHz}(2)	semi-permanent
A.12	ckt	2x64	unres	8 kHz}	permanent

(2) - RDTD "Restricted differential time delay"

<u>I.510 Definition Relied Upon For a pAP</u>

from: I.510 section 4.2 Definitions Related to the General ISDN Interworking Configuration

"Interworking

Within the scope of the I.500 series of recommendations, the term interworking is used to express interactions between networks, between end systems, or between parts thereof, with the aim of providing a functional entity capable of supporting an end-to-end communication. The interactions required to provide a functional entity rely on functions and on the means to select these functions. These functions which include the conversion of physical and electrical states and the mapping of protocols, are referred to as interworking functions (IWFs). An IWF may be implemented in the ISDN, in the other network(s), at the user's premises, through a third-party service provider, or in some combination of these."

<u>ISO/IEC ISP Taxonomy</u>[19]

The following extracts[20] are a small portion of the referenced identifier structure.

The ISDN subnetwork identifier structure for ISPs is

4	Integrated Services Digital Network
4 1	Circuit Switched bearer service at S or T
4 1 1	B Channel
4 1 1 1	Semi-permanent access
4 1 1 2	Demand Access

The LAN subnetwork identifier structure for ISPs is

5	Local Area Networks
5 1	CSMA/CD
5 2	Token Bus
5 3	Token Ring
5 4	FDDI

[19]extract from DTR/10000-1

[20]adapted from ECMA ISPBX TR/NTW

7.4.1.13 Attachment 6—Open Distributed Processing

Both ISO and ECMA are defining a reference model (RM) for Open Distributed Processing (ODP). This tutorial relies heavily on the notions, techniques, and examples of ECMA's SE-ODP document TR/.. dated June, 1989.

ODP RM Overview

The NIUF has registered over one hundred applications which are progressing towards application profiles in order to address implementation conformance statements (ICSs). Few, if any, of these applications are limited to CCITT OSE layer 7 applications, e.g., X.400, X.500, FTAM, etc. Most of them emphasize ISDN bearer and supplementary services with value-added user-derived applications that could benefit from ISDN teleservices.

Figure 7-75 is an illustration which depicts layer "7½" in relation to the OSI RM. This label is used in order to clearly separate the field of applicability of the OSI and ODP RMs. The upper plane depicts ODP objects interacting between end points A and B. This upper plane of layer "7½" could be termed the service user level. The lower plane of layer "7½" is depicted as the SE-ODP plane, i.e., the support environment plane for the ODP plane. This plane may be viewed as the service provider level. The SE-ODP end points A' and B' may be coincident with the ODP A and B end points.

- modules + interfaces + encapsulation
- autonomy + separation
- dependability + scaling
- portability
- heterogeneity + federation

SOURCE: ECMA SE-ODP TR/.. final draft July 1989

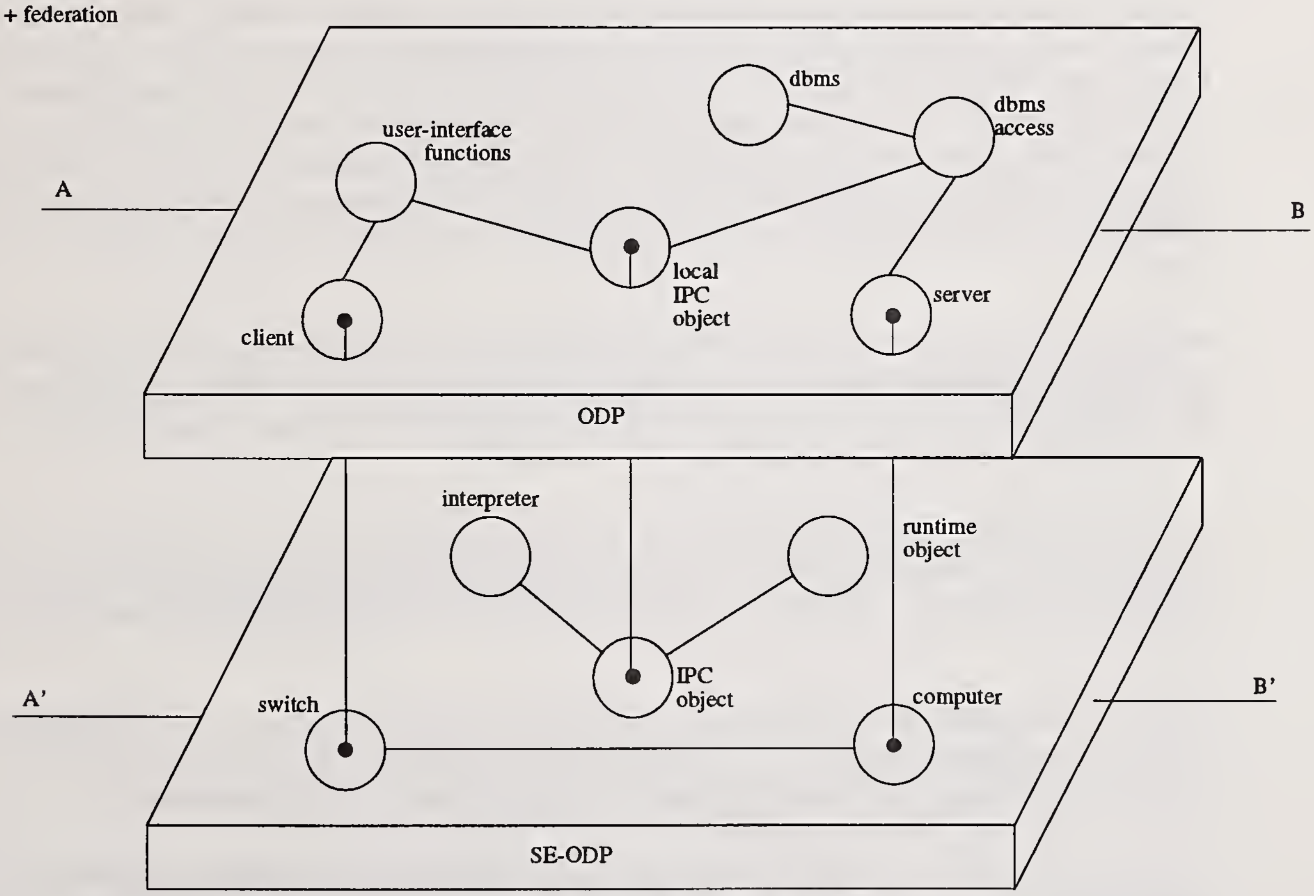


Figure 7-75. Overview of ODP and SE-ODP Planes.

The circles in each plane represent communicating objects. These objects can be anything, as long as certain object modeling rules are followed. The lines between the communicating objects represent interactions, connections, or associations. When this coupling is placed in layer "7½," OSI layer 7 connections and associations are distinguished from layer "7½" connections and associations. The latter imply relationships between ODP application end points (A, B, A' or B') which are distinctly separate from the OSI end points for open interconnections. In ODP practice, A and B end points can reach through the customer premise equipment to the user's man-machine interface.

Some of the object modeling rules concern the notion of a trading application. The upper level of figure 7-75 depicts client/server objects which are importing or exporting interface descriptions in order to establish connections to other communicating objects. In a real implementation, the client/server objects would interact according to remote procedure call (RPC) protocols.

The lower plane of figure 7-75 similarly depicts the producer/consumer objects which also function under importer or exporter ODP rules. The vertical lines which link the upper plane objects with the lower plane objects depict service primitives passing parameters between planes via service access points (SAPs).

The basic advantages of the ODP/SE-ODP layer "7½" are listed at the top of figure 7-75. The reader is referred to the ECMA reference for the detailed description of such advantages but suffice it to say that the principal advantages involve separation of concerns and information hiding.

Object Diagramming Techniques

Figure 7-76 depicts a series of relationships between various types of objects. Figure 7-76a shows ODP objects 1 and 2 with the connection X. Figure 7-76b introduces the notion of an interface object which may interpose the SE-ODP plane hidden interactions via connection X between the same objects 1 and 2 of figure 7-76a. Figure 7-76c simply drops (i.e., hides) object 2 and figure 7-76d does the same for object 1. In figure 7-76e, rather than interposing the SE-ODP interface object, an ODP object 3 is inserted. Figures 7-76a to 7-76e are logically equivalent since each of them maintains connection X—and only this connection. Every diagram of figures 7-76b through 7-76f may be considered transformations of figure 7-76a.

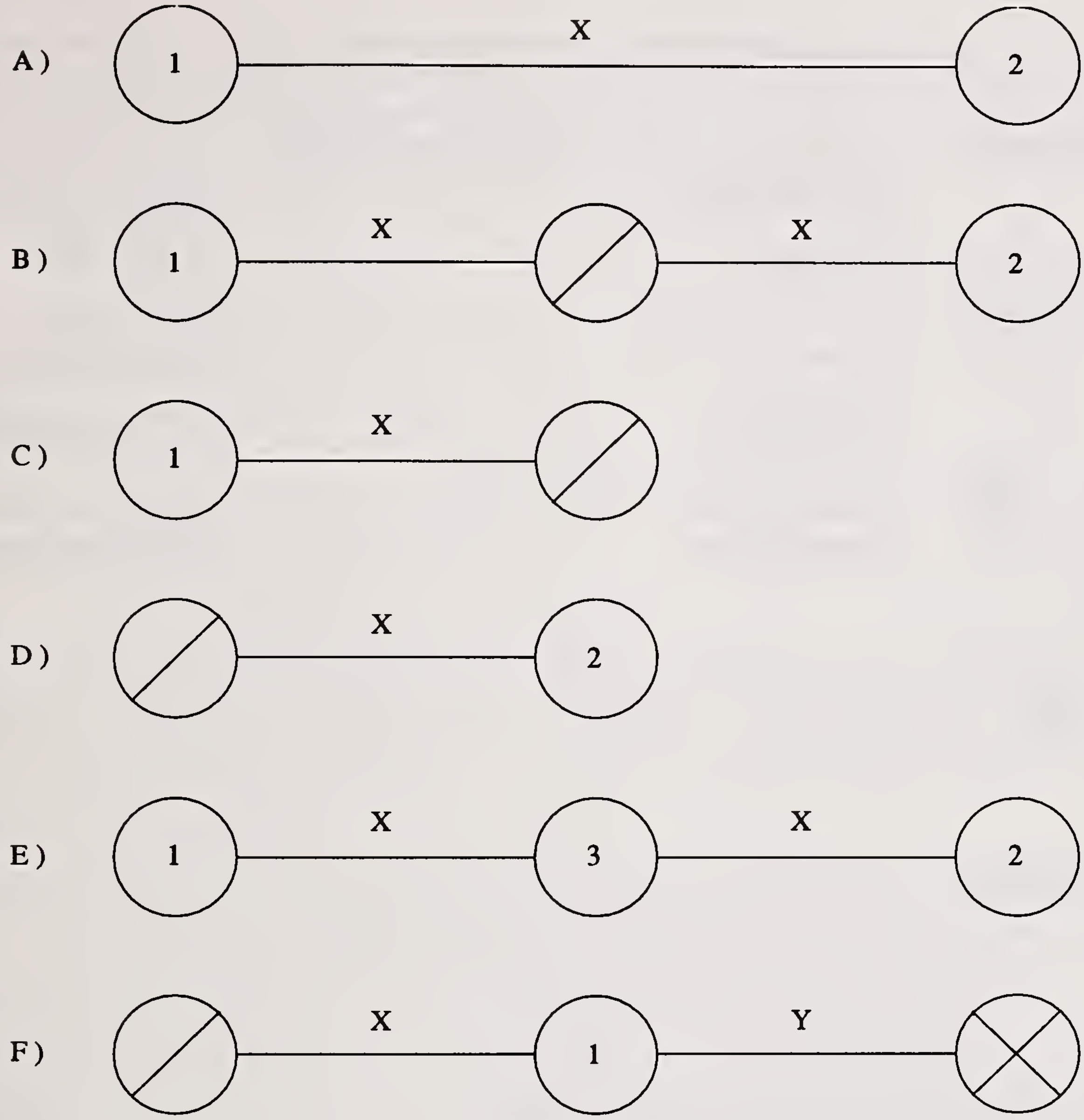
In figure 7-76f, figure 7-76c is shown with a refinement of a new connection Y to an object which is of type "native" component. The native component is an object outside the ODP/SE-ODP RMs. It enables the de facto world of systems to be expressed in object notation. In the case of figure 7-76f, the connection Y is invisible to the ODP interface object.

So far in this tutorial (with reference to fig. 7-75), the ODP plane has been the chief focus. Everything to do with this ODP plane illustration is classed by ECMA as the "computation viewpoint" whereas the SE-ODP plane is captured by ECMA's "engineering viewpoint." Such structural viewpoints align as shown in table 7-20.

However, with respect to NIUF application profiles the viewpoints in table 7-20 are not obvious. Figure 7-77 depicts an orientation of the fundamental ODP-RM viewpoints. This orientation concerns a reference model for Information Technology (IT) which is demonstrated by ODP-RM viewpoints.

At the top of figure 7-77, the Information (I) and Computation (C) viewpoints are aligned in terms of modeling the information and algorithmic structures of the distributed information system (of IT genre), respectively. The Enterprise (E') viewpoint is independent of the I and C viewpoints, and it models what the distributed information IT system is specified to do.

The Engineering (E) viewpoint is dependent upon both the I and C structures because it determines how the distributed information IT system will be realized in the sense of SE-ODP modeling.



NOTE: A) through E) are logically equivalent

LEGEND:

○ = ODP object where X and Y = connections between ODP objects

⊗ = "Native" component

⊘ = ODP interface

SOURCE: ECMA SE-ODP TR/... June, 1989 (as amended)

Figure 7-76. ODP Object Diagrams.

Table 7-20. Structural Viewpoints

Computation Viewpoint		Engineering Viewpoint	
•	(layer "7½" upper)	•	(layer "7½" lower)
•	ODP plane	•	SE-ODP plane
•	service user	•	service provider
•	client/server	•	producer/consumer
•	computational (algorithmic)	•	engineering (qualitative)
•	processes change information flow	•	supports the distributed nature of the processing

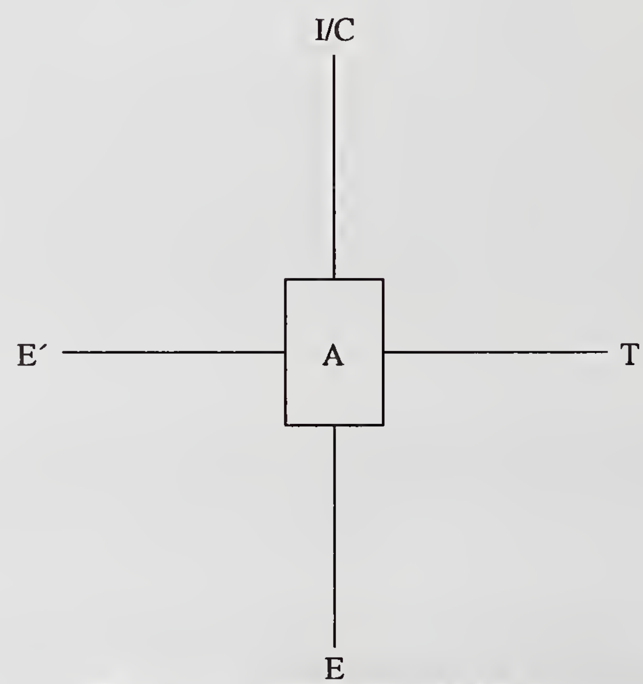
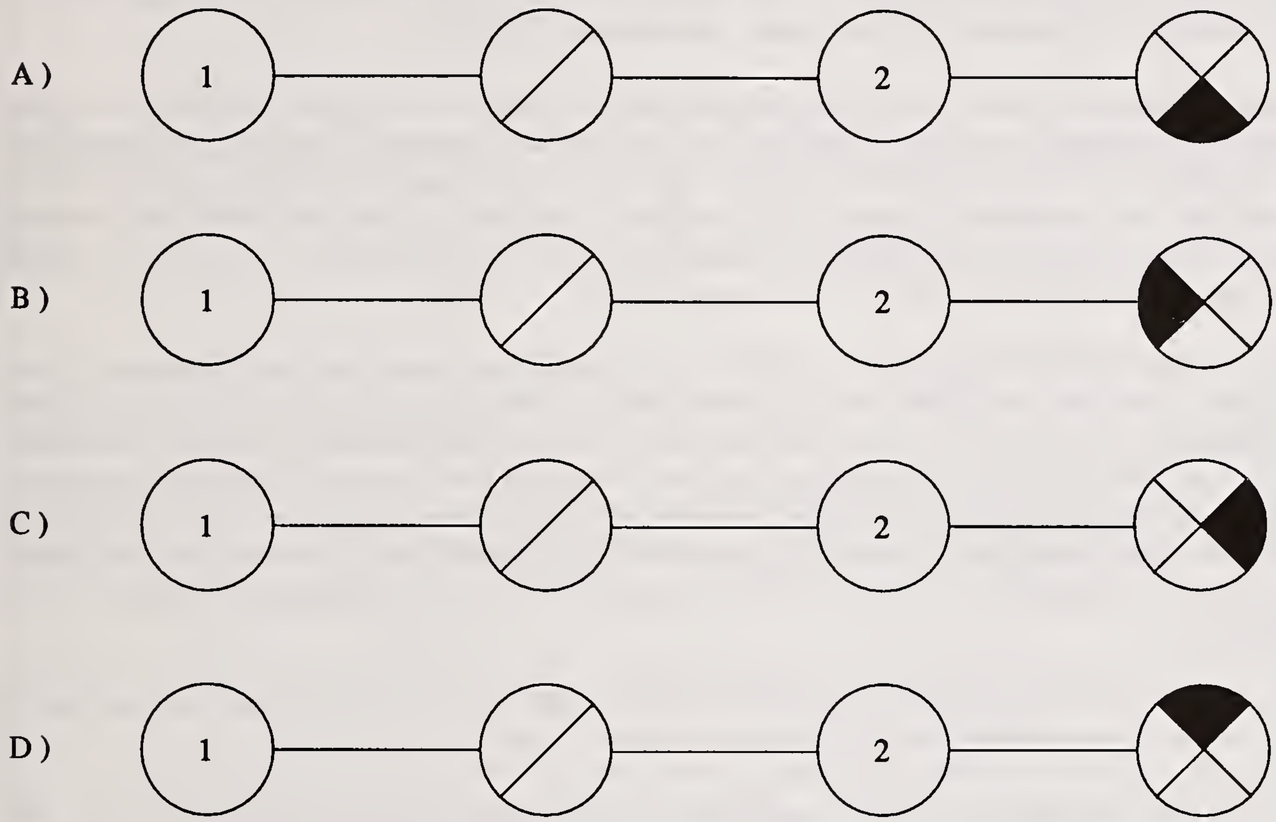


Figure 7-77. Orientation of ODP-RM Viewpoints.

The Technology (T) viewpoint is dependent upon the E' modeling because it associates the nature of the realized (E') components in terms of their specification as to where they will be realized, e.g., perhaps in hardware, software or firmware. The center of figure 7-77 portrays an A which represents aspects of viewpoints. In fact, aspects that are treated in an SE-ODP modeling sense pertain to all the viewpoints aligned in figure 7-77. Performance, quality, compatibility are just a few aspects that might pertain to all ODP/SE-ODP RM viewpoints.

Object Notation for NIUF pAP Profiles

Figure 7-78 introduces further object-oriented notations which are not in conformance with the ECMA notation, but are used to facilitate a functional viewpoint with respect to the ECMA object modeling. In this case, viewpoint is used with respect to the nature of the SE-ODP objects, and not the IT/ODP-RM viewpoints. Figure 7-78a depicts a native component which is an "IPC" for the SE-ODP run-time modeling. The IPC is the realization of any joint action between objects in the sense of inter-process- or inter-program-communications, but only such joint action that is to be made visible with respect to SE-ODP run-time modeling. The IPC object is particularly aligned with the Engineering viewpoint.



LEGEND:

= Native object

= Type of native object (isolated but visible)

NOTE: A) through D) are SE-ODP realizations:

A) = IPC
B) = Endpoint
C) = Stable Resource
D) = Interpreter

Figure 7-78. SE-ODP Object Diagram (Technology Viewpoint).

Figure 7-78b is a notation for a native component that is an end point to a modeling of end-to-end interplay. Unfortunately, using these terms might lead the reader to believe that these ODP models imply that something in the way of input, process, or output is actually occurring, but this is far from the case. All of the ODP-RM techniques should be considered akin to an abstract machine which reflects the potential of an intelligent tinker toy. The attributes of the abstract tinker toy concern architectural properties very much akin to an architect that spends hundreds of thousands of dollars to make a miniature scale model of an intended building complex. This end point component aligns with the Enterprise viewpoint of the ODP/RM and is not an included subject of the ECMA SE-ODP.

Figure 7-78c represents a native object that concerns stable media for the replicated projected or derivative modeled object. Basically, it is stable storage of where the object will reside within the Technology viewpoint. This placement could model a native object related to a global satellite system as one extreme, or at the other extreme, an object that is a subroutine in a mathematical software algorithm.

Figure 7-78d depicts a native object that ECMA calls an interpreter within the SE-ODP run-time model. However, the basic purpose of the interpreter is to confine, limit, or bound the scope of the computation viewpoint object's field of applicability. This happens to be a structural IT matter and may be either associated with the Information or Computation viewpoints of ODP-RM.

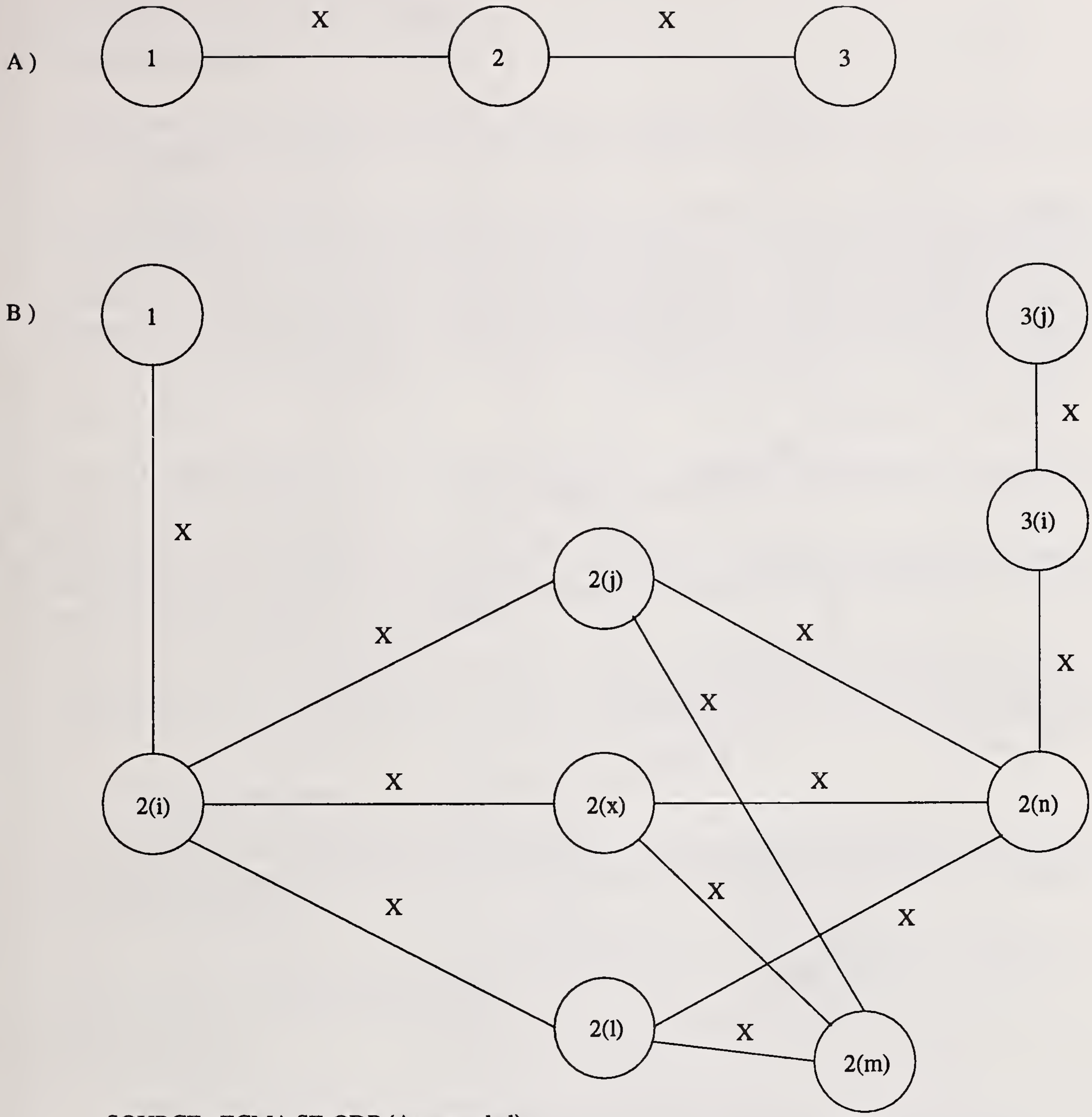
The object notation for 7-78a and 7-78d reveals that they conform to the IT figure orientation as to polar alignment. This alignment implies that they are also complementary modeling functions which means that any variability of 7-78d of the ODP viewpoints will directly affect the SE-ODP viewpoint of 7-78a. Likewise, the ODP viewpoint of figure 7-78b is aligned at the polar opposite of figure 7-78c SE-ODP viewpoint. This implies that any change in the specificity of the ODP viewpoint of 7-78b causes a direct impact upon the modeling of the SE-ODP viewpoint of 7-78c.

Returning to the IT orientation, since the vertical and horizontal axis viewpoints are independent of one another, they can only be unified via the aspects which permeate all of the viewpoints. Another reconciliation of this IT figure is to align the control functions of the object modeling along the vertical axis, and the input, process and output modeling functions along the horizontal axis. This means that the horizontal E'/T viewpoints of ODP modeling may be hidden or transparent to the SE-ODP C/E viewpoints without sacrificing the respective properties of either axis. This control axis property of the pAP 810004 is best conveyed by the schema of section 7.4.1.11 as applied to the various modeling configurators of this same profile.

Figure 7-79 is an ODP diagram from the ECMA SE-ODP TR/... which merely depicts the insertion of objects 6b that are a decomposition of the objects in figure 7-79a.

Figure 7-80 is an SE-ODP object diagram which takes a different view of the objects in figure 7-79. This figure hides the horizontal ODP connectivity implied by figure 7-79. Figure 7-80 implies that the ODP objects are now hidden by the interface adapter objects in the SE-ODP diagram, and that each native object matches with the previous ODP objects of figure 7-79. However, the focus of the model has now changed to encompass Technology viewpoint type objects which are posited (in real systems) outside the scope of both the ODP and the SE-ODP RMs.

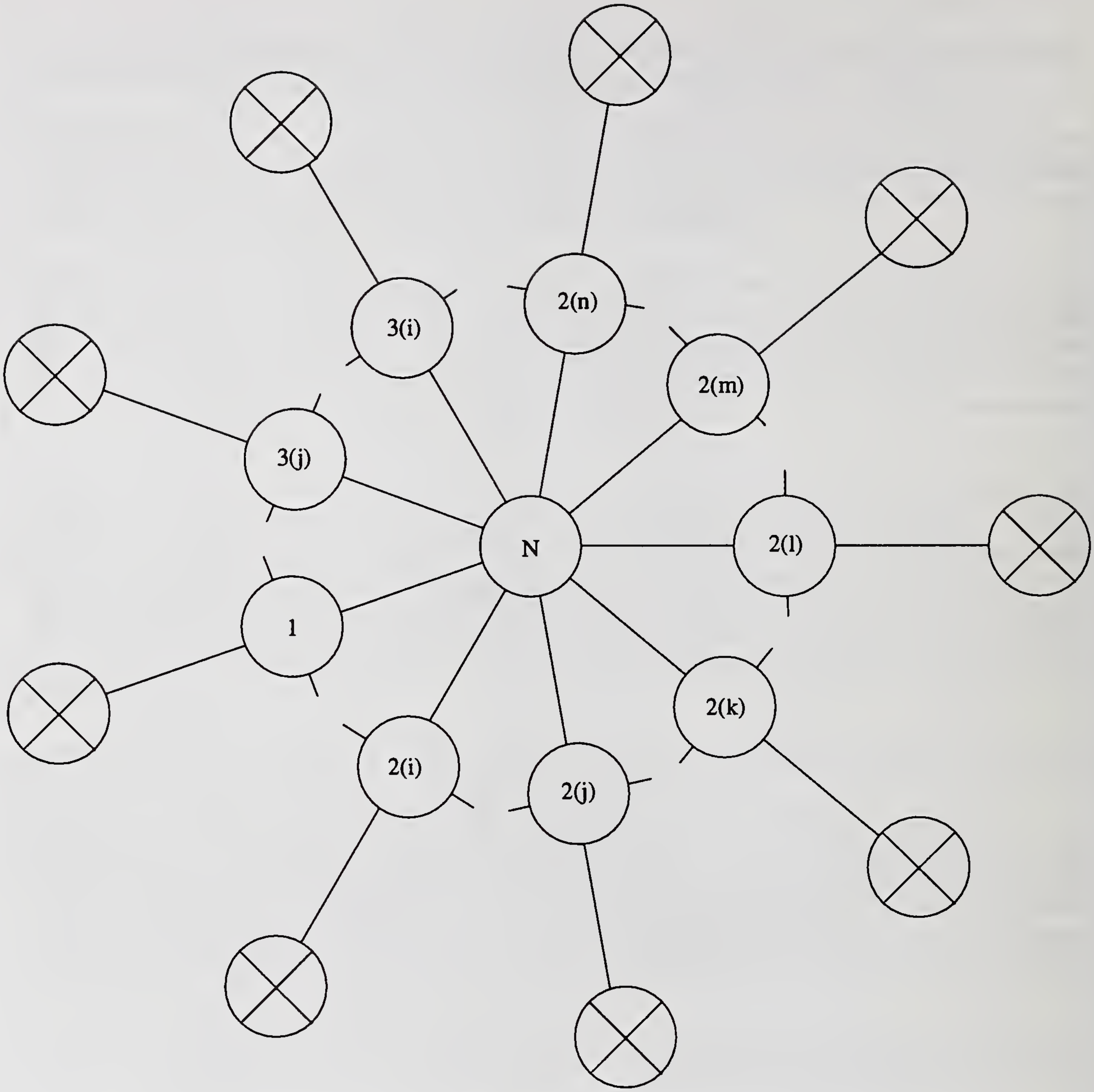
This tutorial is very basic and does not purport to convey but a few particulars of the ECMA SE-ODP TR/...



SOURCE: ECMA SE-ODP (As amended)

NOTE: Distributed application B) is a decomposition of A)

Figure 7-79. SE-ODP Object Diagram (Engineering Viewpoint).



NOTE: N = Nucleus of SE-ODP runtime basic distribution transparencies

SOURCE: ECMA SE-ODP

LEGEND:

= Native component

= ODP transferred to an SE-ODP interface adapter

Figure 7-80. ODP Object Diagram (Computation Viewpoint).

7.4.2 Data Conferencing (Multi-Point)

7.4.2.1 Introduction

This proposed Application Profile (pAP) for 810004 Data Conferencing (Multi-point) is distinguished from that of ISP application profiles for ISDN/OSI functional standards.

The Attachments are either tutorial in nature or provide information as to extensions for pAP 810004. When pAP is progressed through the IIW Expert Working Groups, it will then achieve a status of approved Application Profile (aAP). The Attachments may orient pAP 810004 functional standardization concerns. As contained herein, pAP 810004 is a first-order approach to identifying particular profiles that need to be expanded in the sense of Implementors' Conformance Statements (ICS), PICS, and Requirements List (RL) that encompass both the application environment and the ISDN/OSI environment.

7.4.2.2 Scope

The pAP 810004 delineates a set of profiles that identify the service/protocol specifications needed in order to comply with the ISDN functional standards (de jure) for aAP 810004.

pAP 810004.2 is multi-point data conferencing. pAP 810004 is limited to circuit-switched profiles. pAP 810004 logical or physical realizations are outside this scope, unless they are implicit in the cited reference model or standards for pAP 810004.

De facto aspects (NetBIOS) of pAP 810004 have been mandated by the IUW of the NIUF. Circuit switched facilities are also stipulated by the IUW. OSI profiles are cited if they have been defined by other SPOs.

7.4.2.3 Field of Application

pAP 810004 in its future state (aAP 810004), coupled with NIUF implementation agreements, will govern compliant product implementations (physical realizations) of multi-point data conferencing over public or private wide-area ISDNs.

Customer premise environments have either BRA or PRA network termination and may involve LANs, PBXs or Private Switched Networks (PSN).

7.4.2.4 Standards

"Guide to the Use of Standards," SPAG (Revision 2.0).

SE-ODP by ECMA, TR/.., final draft, June 1989 (Normative Reference).

Also refer to the sources listed in section 7.4.1.3.

7.4.2.5 Definitions

Refer to the definitions in section 7.4.1.4, table 7-6.

7.4.2.6 pAP 810004.2 Profile

Sections 7.4.1.8 to 7.4.1.13 should be referenced for complete details of the taxonomy used in this section.

The Requirements Lists in tables 7-7 and 7-9 are the same for pAP 810004.2. Other requirements lists are in tables 7-21 and 7-22.

Table 7-21. General Level plus Scenario Level plus Functional Level

Field of Application	(RL) 810004.2
A.A1	User's CPE—Public Service
A.A6	Multi-Peer User CPE—Public Service
A.B1	User's CPE—Private Service
A.B6	Multi-Peer User's CPE—Private Service
A.C1	User's CPE—HYBRID Service
A.C7	Multi-Peer User's CPE—HYBRID Service

User/Provider Feature Set	(RL) 810004.2
X.1F	no peer user
X.3F	multi-peer user
X.5F	server coincident with user
X.6F	servers are symmetric
X.4F	one domain (multi-in-sessions)
X.8F	symmetric peer domains (multi-in-sessions)
X.9F	symmetric multi-peer domains
X.0F	asymmetric multi-peer domains

Table 7-22. pAP 810004.2 Requirements List

User/provider Feature Set	(RL) 810004.2 leafs
X.05d	file transfer, NetBIOS (multi-peer)
X.15d	file transfer, NetBIOS (no peer)
X.25d	file transfer, NetBIOS (point-to-point)
X.35d	file transfer, NetBIOS (multi-peer)
X.55d	file transfer, NetBIOS (coincident)
X.65d	file transfer, NetBIOS (symmetric)
X.85d	file transfer, NetBIOS (multi-peer)
X.95d	file transfer, NetBIOS (multi-peer)

7.4.2.7 pAP Conformance Requirements

Reference sections 7.4.2.6 and 7.4.1.11 for details.

Refer to table 7-11 for pAP 810004 point-to-point basic version conformance requirements. Refer to table 7-23 for pAP 810004.2 multi-point version conformance requirements.

Table 7-23. pAP 810004.2 Multi-Point Basic Version Conformance Requirements

RL pAP 810004.2 features	pAP Profiles Supported on CPE	pAP Profiles Supported on ISDN	Conformance Option
A.A1x	X, M, Q	I, M	m
A.A6x	X, M, Q	I, M	m
A.B1x	X, M, Q	I, M	m
A.B6x	X, M, Q	I, M	m
A.C1x (ffs)	Q, V	I, M	o
A.C7x (ffs)	Q, V	I, M	o
X.3xy	X, M, Q	I, M	m
X.6xy	X, M, Q	I, M	m
X.7xy (ffs)	X, M, Q	I, M	o
X.8xy	X, M, Q	I, M	o
X.9xy	X, M, Q	I, M	o
X.0xy (ffs)	X, M, Q	I, M	o
X.35d	X, M, Q	I, M	m
X.65d	X, M, Q	I, M	m
X.75d (ffs)	X, M, Q	I, M	o
X.85d	X, M, Q	I, M	o
X.95d	X, M, Q	I, M	o
X.05d (ffs)	X, M, Q	I, M	o
2.ax (ffs)	X, M, Q	I, M	m
2.dx	X, M, Q	I, M	m
2.bx	X, M, Q	I, M	o
2.f (ffs)	X, M, Q	I, M	o
2.g (ffs)	X, M, Q	I, M	o

Note: See the legend of table 7-11.

7.4.2.8 pAP 810004 Configurator

Note: The following section contains all of the information from the 810004 application requirements and application analysis documents.

The figures 7-71 through 7-74, table 7-16, and figures 7-81 through 7-90 used in this section depict the basis for a pAP 810004 Configurator. The notion of a configurator enables functional (e.g., service overview—table 7-16) and logical (figures 7-71, 7-73 and 7-81) models to abstract the pAP 810004 application and connectivity details at a level that does not specify or constrain implementations.

A configurator extracts the types of connections that are achievable based upon the requirements of the particular application profile and the capabilities admitted by the particular normative reference models. In the case of pAP 810004 the configurator is only interested in types of circuit switched connections such as on-demand, dedicated or pre-established facilities that enable public and/or private data conferencing.

The pAP 810004 extended configurator (table 7-14) depicts the various attributes that may be selected by vendors for robust implementations of pAP 810004.

7.4.2.8.1 IUW Application Profile Requirements

The pAP 810004 configurations and configurator capabilities are not intended to specify or constrain point-to-point or multi-point data conferencing ISDN implementations.

The requirements in table 7-12 were stipulated by the IUW as augmented by the IIW/AAG.

7.4.2.8.2 Basic Multi-Point Reference Model

By adapting the standard ISDN Reference Model configuration, the pAP 810004 reference model is derived as depicted in figure 7-71 for point-to-point data conferencing. The pAP 810004 configuration for point-to-point data conferencing is depicted in figure 7-73 by simplifying the notation of figure 7-71.

The prior figures imply an end-to-end set of interworking (general-level) profiles based on the preceding IUW requirements for the "must" category as described in table 7-13.

Figure 7-81 depicts the pAP 810004.2 Multi-point Reference Model (RM) in two styles, namely the ISDN RM style and the ECMA/ODP style. The latter style is used to depict the pAP 810004.2 data conferencing infrastructure. Section 7.4.1.13 contains a tutorial on the ECMA SE-ODP TR/.... The former style presents a symmetric multi-point reference model as an extended figure 7-71.

7.4.2.8.3 Basic Multi-Point Configurator

Figure 7-73 further refines or simplifies figure 7-71 to the extent that the basic pAP 810004 profile options need only deal with symmetric CPE environments and associated servers and multi-point sessions as summarized in figure 7-72.

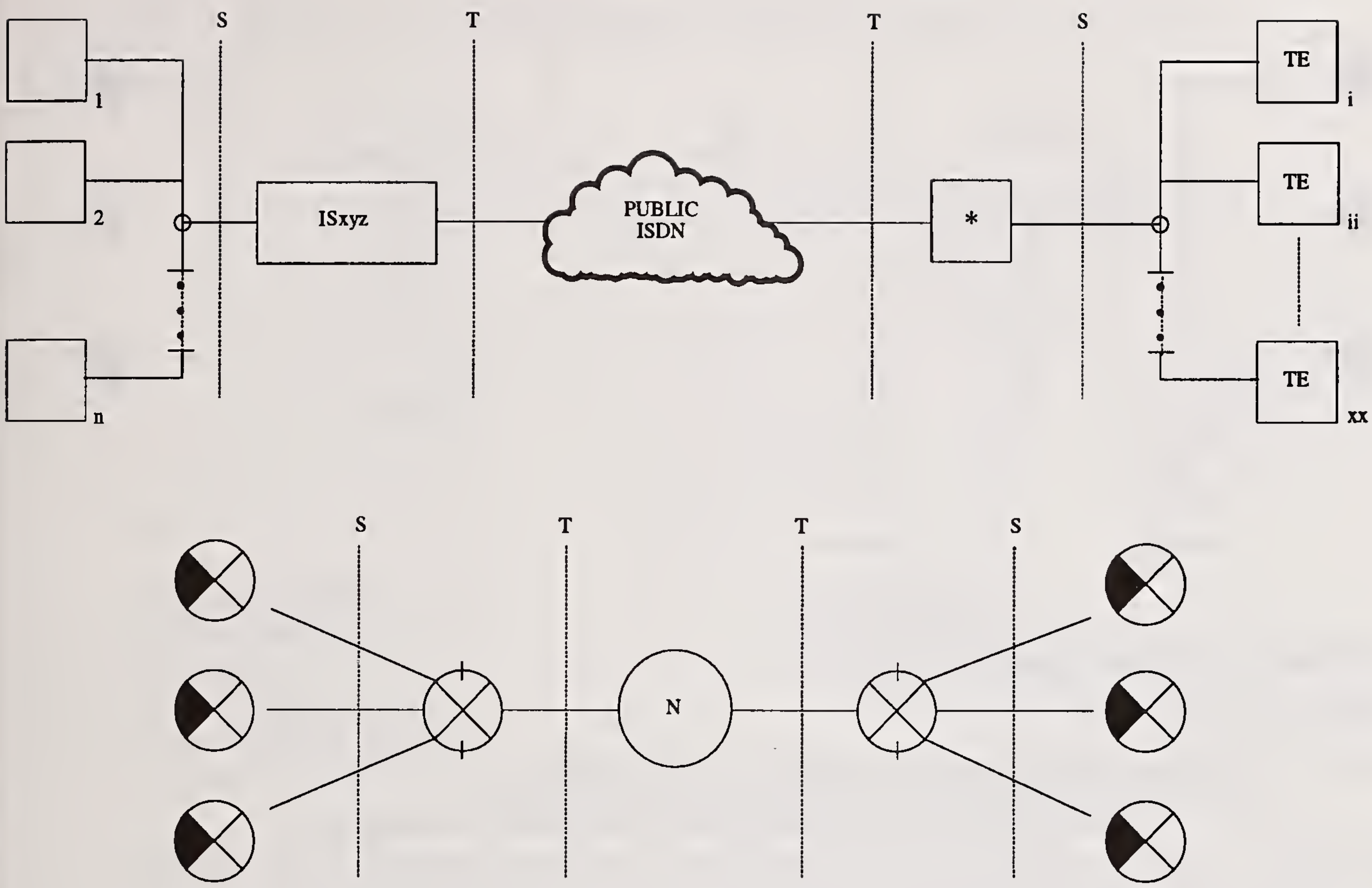
The use of the term basic typically means one type of subnetwork reference model is encompassed by the customer premise environments. The stacks of profiles in figure 7-72 align the prior discussion for figures 7-71, 7-73 and 7-81. Figure 7-82 is an ODP object notation of figure 7-72. The center interface object "hides" the wide-area interactions (see section 7.4.1.13 for more object-oriented explanations).

The profile stacks reveal that wide-area (w/a) ISDN connectivity (the center box of figure 7-72) is based upon I.Series and SPO [M] profiles that are to evolve via NIST (NIUF), ETSI (EWOS), INTAP (AOW), etc., for the underlying implementation agreements (see section 7.4.1.9 for the distinction regarding [M] profiles).

7.4.2.8.4 Extended Multi-Point Configurator

The use of the term extended typically means that multiple types of subnetwork reference models are encompassed by the customer premise environments.

Figures 7-74 and 7-83 are the extended pAP 810004 point-to-point and multi-point basic configurations, respectively. The purpose of including the pAP 810004 extended configurators in Table 7-14 is to encourage vendors to adopt general-purpose architectural criteria when setting out to meet pAP 810004 requirements.



NOTE (1): See the legend of figure 7-71.

NOTE (2): A multi-point ISDN RM expressed in ECMA ODP/SE-ODP RM (as amended) components (native objects and native interface adapters).

Figure 7-81. pAP 810004.2 Multi-Point Basic Configuration.

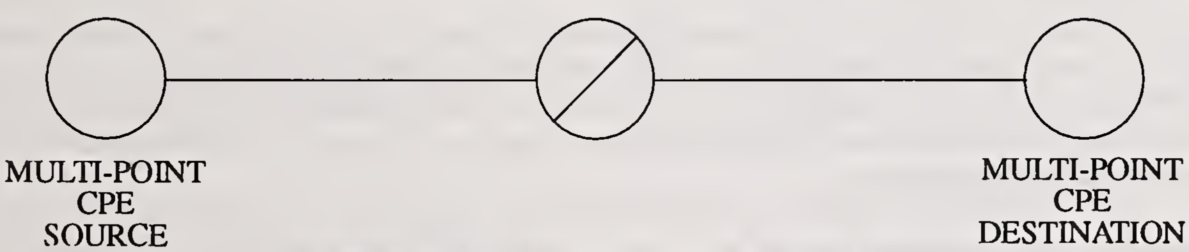
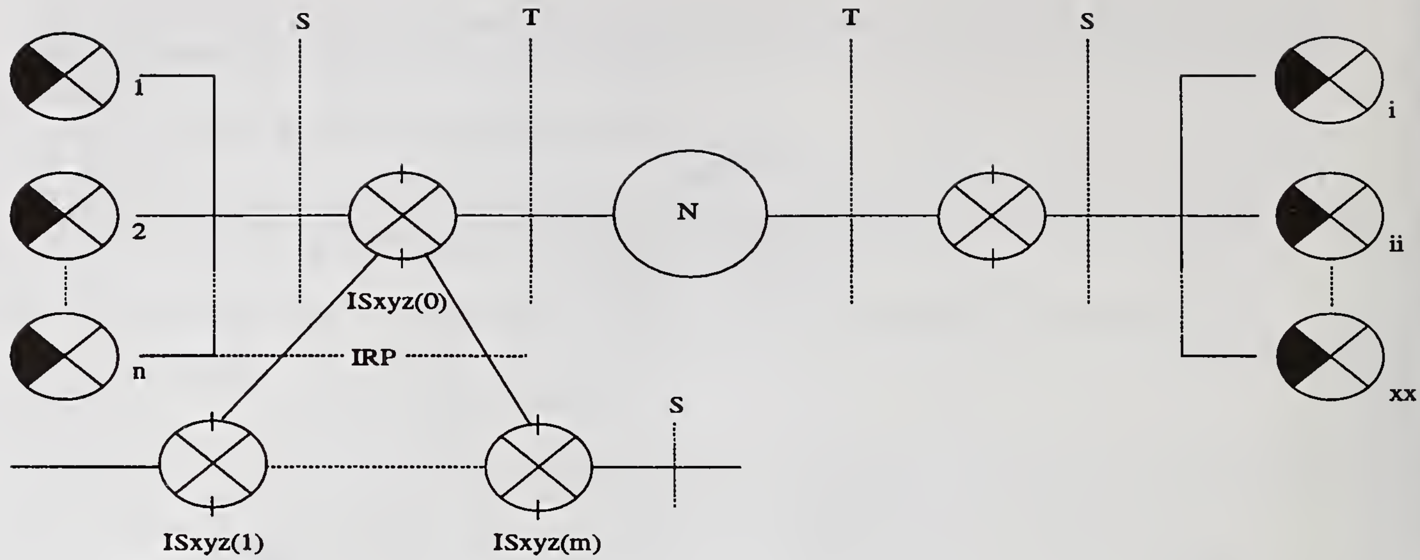


Figure 7-82. pAP 810004.2 Profile Stacks.

7.4.2.8.5 Multi-Point/Point-to-Point Multi-Part Profile

Table 7-16 is the overall profile framework for both the point-to-point and multi-point pAP 810004 configurator. It is also an overview of a generic service model. The properties of this framework are also addressed in sections 7.4.1.8 through 7.4.1.13.

The key aspects of the table 7-16 framework include the notion that the carrier backbone network is augmented by a private network backbone in the sense of ISDN NIUF or ISP profiles. Such augmentation



NOTE: IRP = ISDN reference point (T, K*, or N*)

NOTE (1): See figure 7-74 s.

NOTE (2): A multi-point ISDN RM expressed in ECMA ODP/SE-ODP RM (as amended) components (native objects and native interface adapters)

Figure 7-83. pAP 810004.2 Basic Multi-Point Configuration.

is facilitated by profiles for Basic low layer functions (BLLF) that are aligned end-to-end across private and/or public sub-networks. Similarly, Additional LLFs (ALLF) are so aligned. High-level functions may also be augmentations to both the (basic and additional) carrier and private backbones. These Basic and Additional functions are provider-oriented in the sense of supporting the user's application environment. This notion of augmentation, when extended into the user's application environment, leads to further value-added application(s) augmentation, as the examples in table 7-24 depict.

The substance of the above notions, augmentations and alignments, are administered via requirements list(s) (RL) at each plateau (carrier, private, CPE) pursuant to Table 7-16. The RLs are the fundamental application of the pAP taxonomy which is detailed in the Appendices. Viewed as a tree with trunk, branches and leaves, it enables each pAP/RL to denote work items or work-to-be-done in the sense of implementation agreements.

Pursuant to the explanation concerning the table 7-16 pAP 810004 Service Overview framework, figures 7-84 through 7-87 will elaborate the data conferencing interactions for the basic-mode and value-added profiles. The basic-mode multi-point profile concerns the Multiparty Supplementary Service (SS) for ISDN conference calling (CONF). The value-added multi-point profile features concern the CONF plus the interworking with multi-peer users who subscribe to, or are equipped with, the Three Party (3 PTY) supplementary service.

7.4.2.8.6 Data Conferencing Application Model

Figure 7-84 depicts an overview diagram using object diagram notations and practices adopted and customized from the ECMA SE-ODP RM. Section 7.4.1.13 provides a basic tutorial in order to assess the merits of figures 7-84 through 7-87; however, nothing herein purports to replace or conflict with the ECMA TR/...document.

Table 7-24. pAP 810004 Extended Configurator Descriptors (examples only)

User/Provider Feature Set Aspects	user		provider	
	VLLF	VHLF	VLLF	VHLF
service	B	E	B, A	B, A
application	S	N	S	N
features	-		-	
interfaces	S		S	

Legend:

user/provider related
V = value-added
S = supported
N = non-support
E = extended configurator
- = profile RLs

backbone-related
B = basic LLF or HLF
A = additional LLF or HLF

Basically, figure 7-84 shows a group object for both the conferencing clients and servers. This means that three or more clients (the term "conferees" is used in I.250) are participating in a multi-point data conference using one or more conference servers (the term "controllers" is used in I.250).

At the bottom of figure 7-84, the connection between the client group and the server group has the following types of interactions:

Client	Server
X.U multi-peer users	X.R servers either coincident, symmetric, or asymmetric with the clients
X.D clients are utilizing a multiparty SS	2.d server interactions with clients are based on multiparty SS

The interface adapter objects hide the underlying wide-area and private switched network services/profiles that are depicted in figures 7-81 and 7-83.

The upper portion of figure 7-84 displays an overview of the data conferencing trading application. Trading concepts are adopted from ECMA's SE-ODP RM. Figure 7-84 indicates that the server object will export an interface description in order to establish a particular type of trading association which will be imported by the clients desiring to engage in a multi-point data conference.

The merits of the association in terms of the type of interactions that are modeled in figure 7-84 are summarized below. Further details are provided in figures 7-85 through 7-90, sections 7.4.1.11 and 7.4.1.13, as well as in the I.254 series Blue Book standard. The foregoing paragraphs have discussed the X.U, X.R and X.U properties of the user/provider feature set. The 2.x interactions are described in section 7.4.1.11 and are summarized in table 7-26.

Table 7-25. Functional Procedures*

F=a	Adjourn
F=e	Inquire
F=f	Retrieve (reestablish)
F=i	Hold Invocation (disconnect & reservation)
F=j	Join (multiparty)
F=m	Monitor (watch for Event)
F=n	Notify (inform, no response)
F=r	Reroute (to alternate address)
F=s	Split (from a multipart connection)
F=t	Transfer
F=x	Restart

*adapted from I.310 Annex A.

X.sF refers to the functional-level (F) of the schema which is described in sections 7.4.1.9 and 7.4.1.11. F pertains to the particular procedures that are imported/exported in determining the modeled multi-point data conferencing parameters for multi-in-sessions between clients, servers and certain resources (X.R) that are attached to clients and servers in order to support their data conferencing needs (see section 7.4.2.6).

Part of section 7.4.1.11 is reproduced in table 7-25 with a few of the procedures.

F=i pertains to adding or dropping clients from the conference. F=j means that parties to a data conference may be in non-active states and are not active or engaged in the multi-point conference until this procedure takes effect. Likewise F=s causes a party to the data conference to be removed from interaction with other clients but remain connected to the data conference server, i.e., controller or administrator. F=n could mean that a party can participate in the data conference as an observer, but this party is isolated from being able to engage in the threads of the data conference as a contributing party.

PAP 810004.2 must be viewed as an intricate model that guides vendors in independently devising realizations of this profile that would be able to interwork or interoperate in a distributed processing environment. The I.Series should be referenced in order to determine the detailed services, functions, capabilities and procedures that should guide vendors when implementing pAP 810004-based products. Vendors would first represent some aspect of pAP 810004.2 in the form of a functional description or specification for a compliant product or service offering.

In table 7-26, the pAP 810004.2 designators from figure 7-84 round out the other types of interactions between clients, clients and servers, or clients, servers and resources that are linked to the particular data conference.

7.4.2.8.7 Data Conferencing Value-Added Model

Finally, at the top of figure 7-84 are objects that pertain to interactions that may be viewed as a superstructure to guide types of realizations of this profile. Conferencing Administration interactions are outlined as part of figure 7-85 and the facilitator is a future conferencing notion that may be necessary for data conferences that have large numbers of participants over wide-area networks and data conferencing for extended periods of time. A brief abstract of this notion is included when describing figures 7-85 and 7-86.

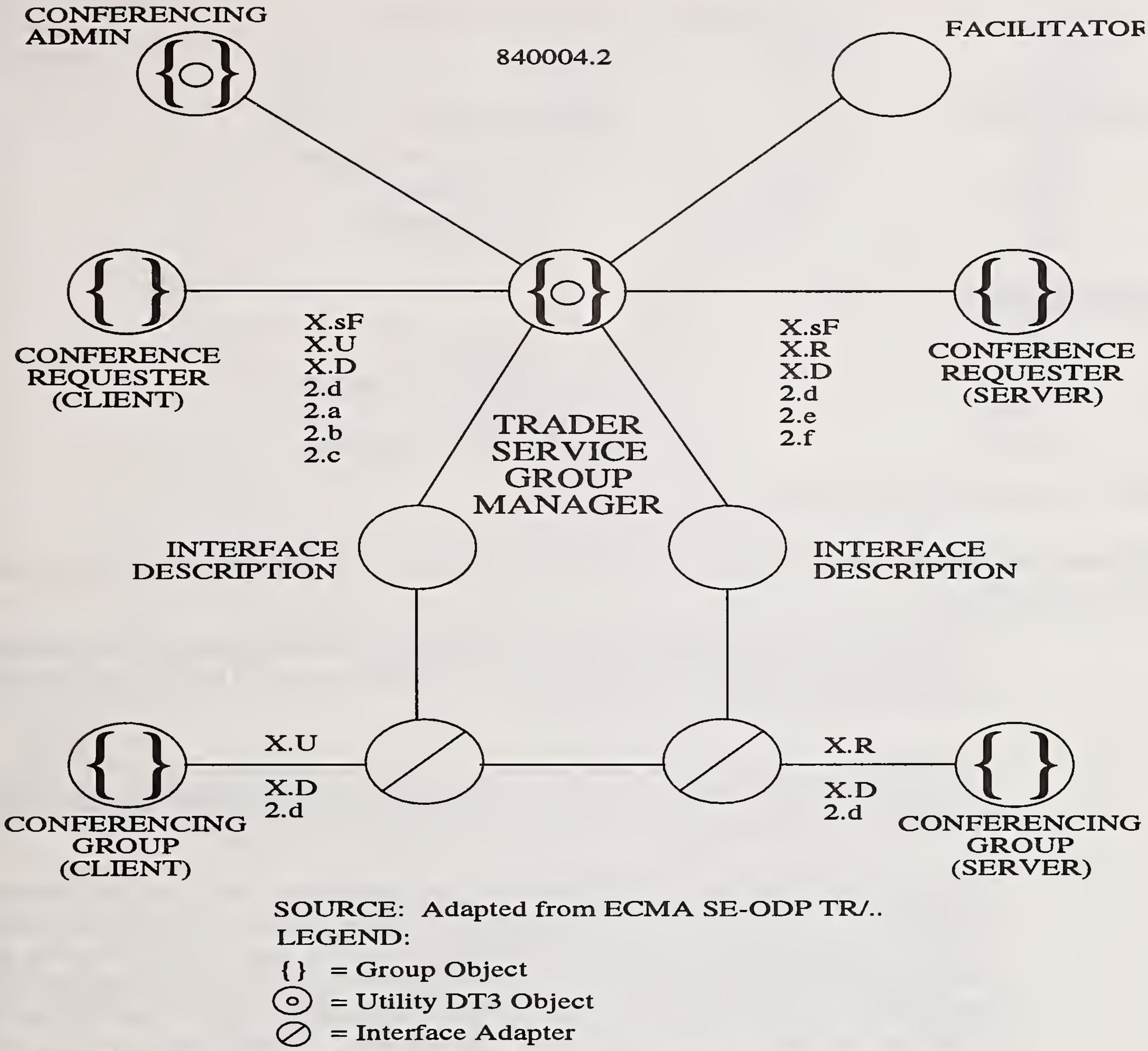


Figure 7-84. pAP 810004.2 Multi-Point Data Conferencing (Trading Application Overview).

Figure 7-85 is a refinement of figure 7-84. All of the notions concerning export/import, associations, and types of interactions carry over from the multi-point data conferencing environment conveyed via figure 7-84. The refinements introduced in figure 7-85 are discussed in the following paragraphs:

A. Administrator vs. Facilitator

B. Clients interworked across wide-area networking topologies of diverse public and private ISDNs

C. Separation of concerns regarding Trader Service Group Manager versus Conferencing Administration

A. The notion of a Facilitator is distinguished from that of the Administrator. The Administrator is substantially the capability aligned with the conference controller that is described in the X.254

Table 7-26. Client and Server Interactions

Client Interactions	Supplementary Service
2.ax	Number Identification
2.bx	Call Offering
2.cx	Call Completion
2.dx	Multiparty
Server Interactions*	
2.dx	Multiparty
2.ex	Community of Interest
2.fx (ffs)	Charging
2.gx (ffs)	User-to-user signalling

NOTE: See section 7.4.1.11 for the breakdown of x.

*The server negotiates or allows the foregoing client interactions either by client subscriptions, default provisions, or bi-lateral agreements.

series Multiparty Supplementary Services in the Blue Books. The Facilitator is a value-added high level function (VHLF) which is acknowledged as a potential extension of the user/provider feature set layer of figure 7-74.

The Facilitator functions as a master-client who is not particularly concerned, from an Administrator's control standpoint, with the data conferencing configurator interactions as modeled in figures 7-81, 7-74 and 7-83.

The Facilitator is concerned with the human-factors and application-context of the particular multi-point data conference. The Facilitator manages the clients in the sense of Closed User Groups (CUGs) applied to the roles played by particular clients in a large, multi-dimensional data conference; for example, one dimension is an editor-CUG for those clients with editing privileges. Such privileges may gain access to other clients' contributions and drafts of documents which are the outcome of a multi-point standards creation data conference. A second dimension could control a Q.series CUG for those clients enrolled in a standard's data conference registered as experts on Q.series protocols. Another dimension could be for the role of clients as part of a T.series CUG, and so forth. The Facilitator is a future requirement pertaining to a hypothetical set of IUW expectations for advanced intelligent multi-point data conferencing.

B. Data Conference Interworking concerns the basic function of the Trader Service Group Manager (TSGM) which was not described as part of figure 7-84. The TSGM is an object that hides all of the intricacies involving associations, connections, and interactions involving more complex interactions with ISDN-to-ISDN networks or ISDN-to-non-ISDN networks. The features in table 7-27 are to be considered in future versions of pAP 810004.2.

Likewise, the interworking reference points in table 7-28 determine the types of connections that are invoked by the TSGM.

C. The TSGM object is more concerned with the low layers of the wide-area and/or private backbone networks. The types of interactions address (i) specific facilities, (ii) interworking aspects and (iii) the selection for interworking when no IWF is required, i.e., one-stage vs. two-stage selection. The

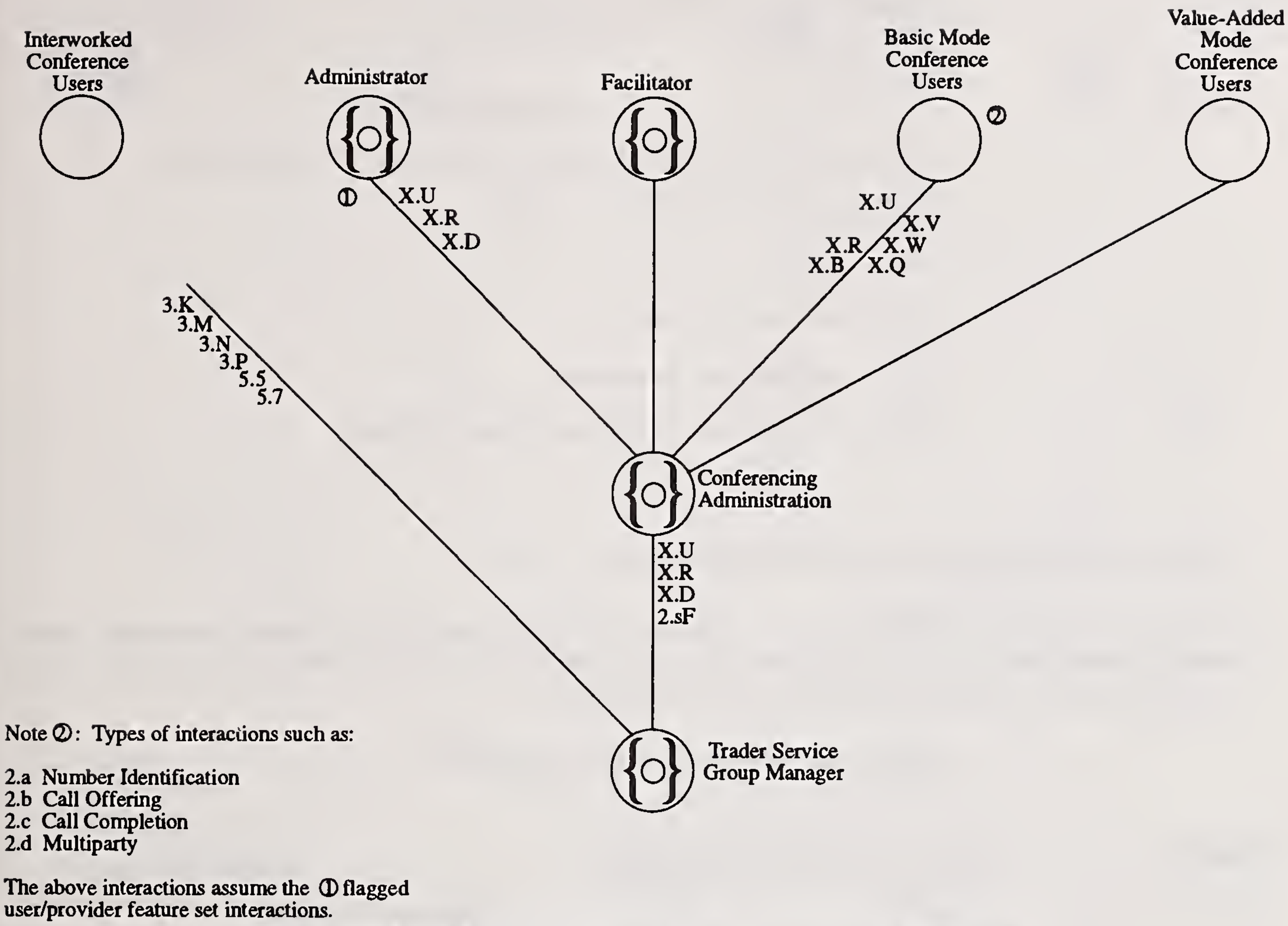


Figure 7-85. pAP 810004.2 Multi-Point Conferencing Overview.

Table 7-27. Future Features of pAP 810004.2

IWF	Interworking Aspect	I.500 Series
1	Layer 1 Internetworking	I.511
1	Parameter Exchange	I.515
1	ISDN-to-ISDN Interworking	I.520
2	ISDN-to-PSTN	I.530
3	ISDN-to-PSPDN	I.550
4	ISDN-to-CSPDN	I.540
n	ISDN-to-Private Internetwork	I.310/I.510

TSGM also selects values for terminal compatibility, terminal parameter exchange, low layer compatibility information element, or layer 1 internetwork termination. Terminal adaption, parameter exchange and low layer compatibility procedures are typically transparent to the Conferencing Administration Group Manager described pursuant to figure 7-85.

Table 7-28. Interworking Reference Points

Ref. Pt.	Interworking
K	Existing telephony network, dedicated network, or transit network.
M	Specialized service provider, e.g., ESP.
N	Another ISDN.
P	Specialized network resource.
Q	Layer 1 internetwork termination.
S/T	Interworking between ISDN and Private Networks.

7.4.2.8.8 Data Conferencing Support Environment

Figure 7-86 introduces a different object diagram notation in order to map diverse interactions into a particular procedural grouping which binds to objects called native adapters in the ECMA SE-ODP. Figure 7-86 introduces four types of conference native components.

Table 7-29. Conference Native Components

Paragraph	Native Conference Component	Purpose
(D)	Setup	Resource Location
(E)	Configurator	Interprocess Communication (IPC)
(F)	Initialization, Mediation, and Release	Interpreter
(G)	Operation	End Point Location

D. The resource native component achieves the binding with particular mechanisms, e.g., memory requirements for the multi-point data conference setup. Since this binding may be static or dynamic, the static property infers that all resources for a particular data conference must be located and confirmed prior to run time. Native objects may be associated with application components and, in such circumstances, all interactions are considered local to whatever mechanism or device a vendor chooses to design.

E. The IPC object is a native object in the SE-ODP run-time communications model. All of the external interactions that occur between separate locations or domains for multi-point data conferencing must bind to the IPC object. Given a pAP 810004.2 configurator, all interactions that are not considered of local inter-module scope can be considered external interactions requiring IPC mechanisms either for this profile or for its realization.

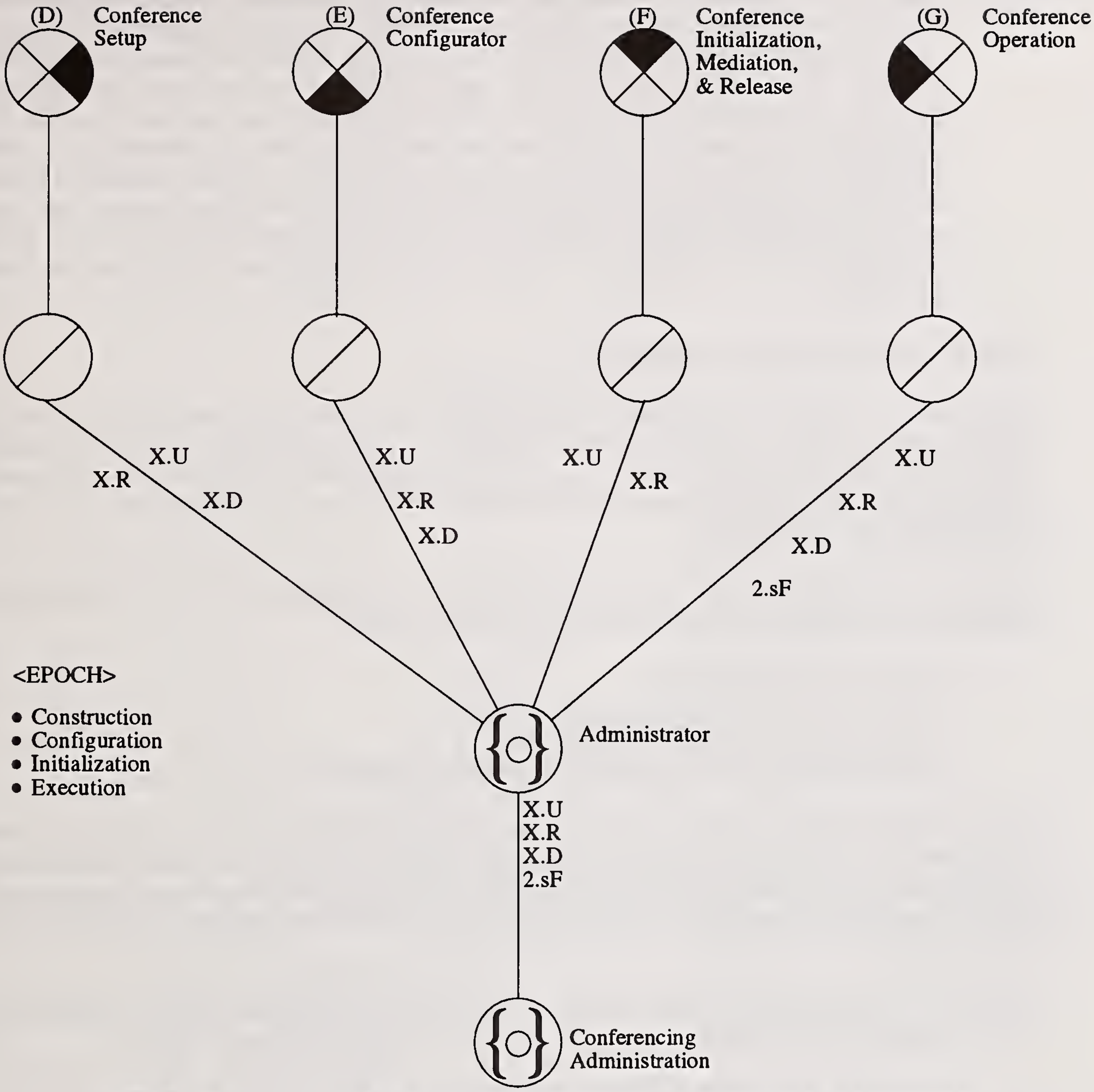


Figure 7-86. pAP 810004.2 Multi-Point Conferencing Administration Administrator.

F. The interpreter native object is part of ECMA's SE-ODP processing model. Effectively, all of the interactions that transpire (as designated by this profile) that concern binding of processing components will be invoked by the interpreter object via primitives. The resultant binding of such processing components are called capsules, which will be described in figures 7-89 and 7-90 in conjunction with the basic-mode and value-added client services appropriate for this profile. Basically, all processes involving data conference initialization, mediation, and release that bind to a particular application component subsequently determine the behavior of the total service mechanism that realizes such processing, e.g., the execution of all client requests to join a data conference is encompassed by the interpreter object.

G. Although the native adapters in paragraphs E and F may be considered independent of particular clients and server mechanisms, the end point native object (in conjunction with the resource native object) furnishes the interface mechanisms that achieve the conference operation as governed by the multi-party supplementary services (I.254). The notion that certain sequences of activities or events are repetitive, reproducible, or cyclic—in a SE-ODP run-time environment—is called an epoch by ECMA. Figure 7-86 cites four generic categories of epochs that substantially all application profiles would demonstrate by virtue of their particular bindings to the SE-ODP infrastructure. The realization of compliant mechanisms, as a result of bindings of application components with interpreter and IPC components, could achieve compliant interactions between all end points and resource components (similarly bound) which then interface with these processing and communications support mechanisms. The resultant behavior of such a derived distributed application could manifest in the form of epochs based upon suitable vendor realization techniques.

7.4.2.8.9 Data Conferencing Administration

Pursuant to I.141, when ISDNs perform services as defined by the I.200 series, there has to be means to charge for such services, as well as uniform mechanisms to derive such charges for billing purposes. Similarly, this data conferencing service, as an outcome of a realization of the pAP 810004.2 agreements, should provide for applicable charging procedures that are specific to data conferencing services, e.g., multi-party Supplementary Services (SS).

Figure 7-87 acknowledges types of charging mechanisms that conform to I.141 for multi-party SS characteristics, capabilities and underlying transport services, namely:

- I.254 Service Requirements
- I.254 Service Charging Requirements
- I.500 Internetwork Service Requirements
- I.500 Internetwork Charging Reconciliation and Settlements

Figure 7-87 also identifies an object named Interpreted Conferencing Policy (ICP). The primary purpose of this object is to support the multi-point access requirements for the data conferencing facilitator type service profiles (see section 7.4.2.8.7) that are realized by particular mechanisms, or epochs, in deriving a simulated data conference, i.e., a live data conference would be the outcome of vendor/provider implementations.

Pursuant to Q.932 (basis for Ref. [20]), the procedures in table 7-30 are required for epoch instantiation of data conferencing service profiles.

Table 7-30. pAP 810004.2 Service Profiles/Epochs

EPOCH	PROCEDURES
Construction	SP-A
Configuration	SP-B
Initialization	SP-C
Execution	SP-Q

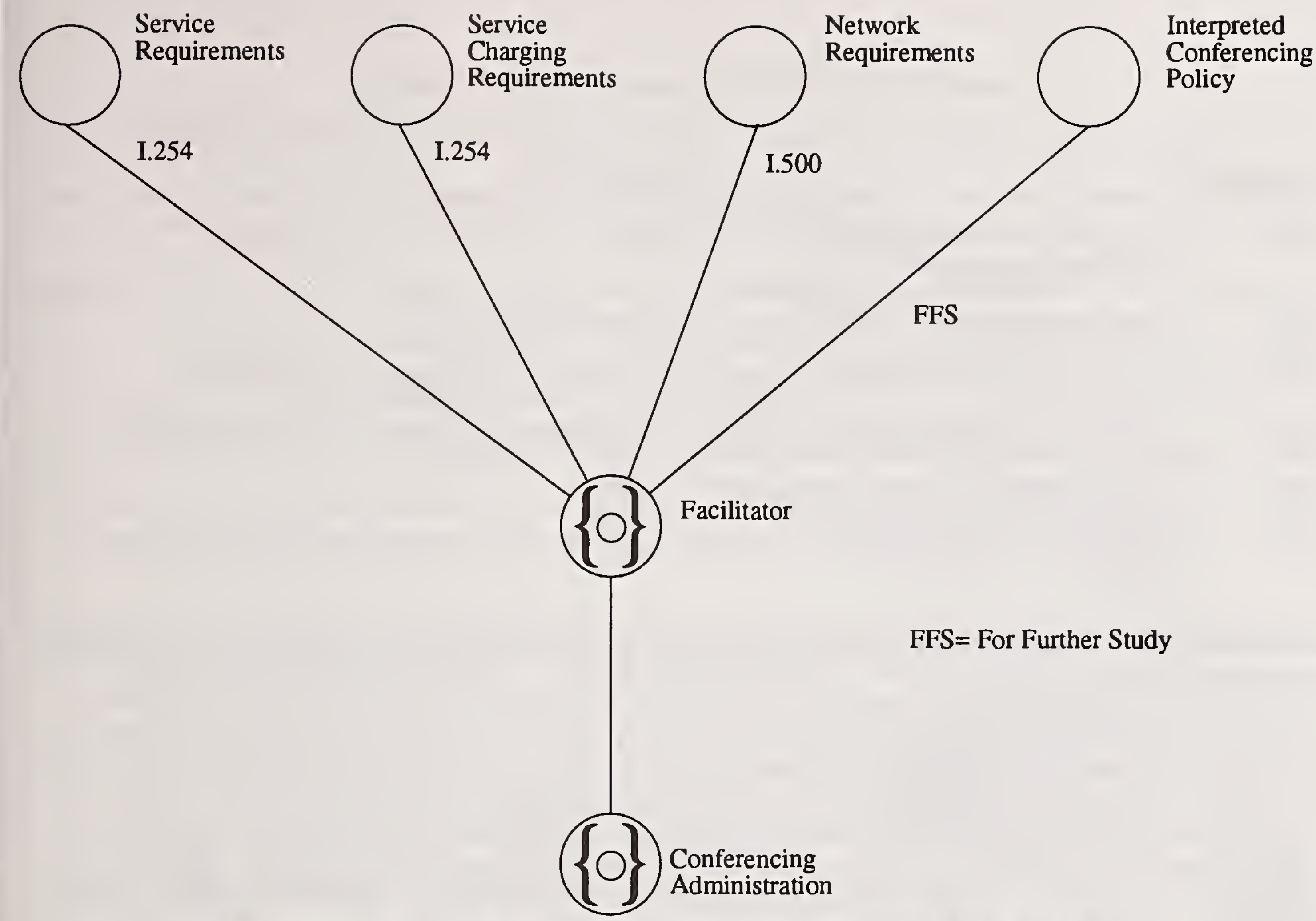


Figure 7-87. pAP 810004.2 Multi-Point Conferencing Administration Facilitator.

The list of service profiles in table 7-30 are considered the minimal set in order to conduct a multi-point data conference. Each Service Profile (SP) makes use of the following Q.932 (Ref. [20]) identifiers.

- SPID Service Profile Identifier
- USID User Service Identifier
- TID Terminal Identifier
- EID Endpoint Identifier

However, these SPs/Epochs are applicable to the user-to-network interface whereby the network is able to retain these identifiers in order to resolve the grouping of users, terminals, and end points under a particular multi-point service offering, e.g., CONF or 3PTY connections. Figure 7-74 and section 7.4.1.10 will help in order to structure the minimal set of pAP 810004.2 service profiles as exemplified in table 7-31.

7.4.2.8.10 pAP 810004.2 Operations Overview

Figure 7-88 portrays an ODP/SE-ODP field of application for multi-point data conferencing operation. The objects with a "c" in the center are the ODP objects called capsules. The remaining objects are various native objects from the SE-ODP run-time environment which supports the trading between the ODP capsules and the SE-ODP native objects.

The capsules are mechanisms that enable all of the processes that are related to Distribution Transparency 3 (DT3) objects of any type (i.e., utility, user, trading, or application objects) to be confined in one object for purposes of associations and interactions with other non-capsule objects. In the case of figure 7-88, all

Table 7-31. pAP 810004.2 Service Profile (SP) Structure

Capability	Description
VHLF	ICPs plus data conferencing SPs/Q.931 (Codeset 6) for PVN and Q.931 (Codeset 7) for dynamic facilitator SFCs*.
VLLF	Data conferencing SPs/Q.931 (Codeset 7) for static facilitator SFCs.
AHLF	Q.932 per BHLF/NetBIOS/Q.932 multiparty SS and Q.931 (Codeset 6) for NetBIOS.
ALLF	Q.931 for BLLF/NetBIOS/PVN Multiparty SS permanent multi-point I.231.1 bearer service.
BHLF	Q.932 multiparty SS with network service profiles.
BLLF	Q.931 messages for circuit-mode connection control. I.231.1 circuit-mode multi-point bearer service.

*SFC stands for a supplemental functional component which is illustrated in the Q.932 (section 7.4.1.9) functional reference model.

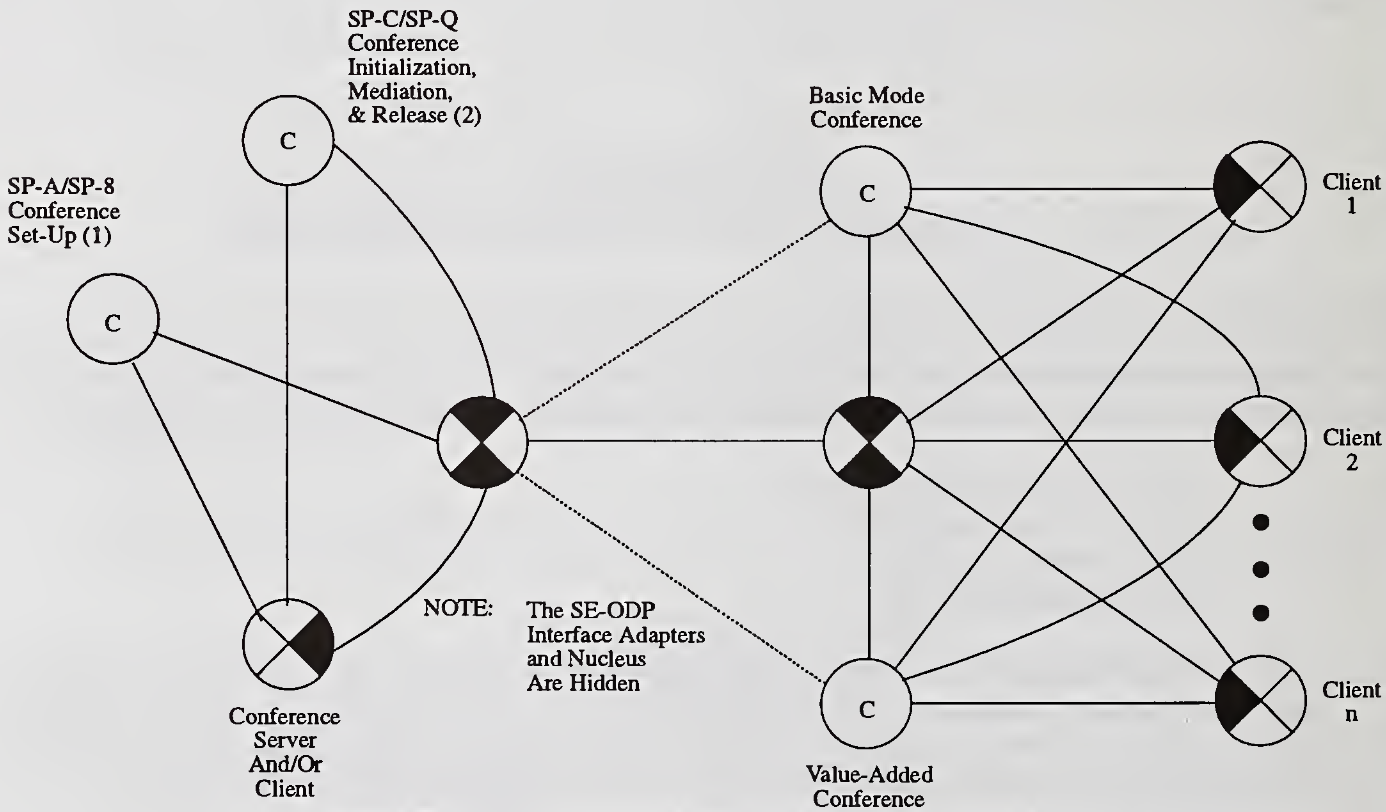


Figure 7-88. pAP 810004.2 Data Conferencing Operation.

such processes have been confined to four capsules for this top-layer view of the pAP 810004.2 operations scenario. Two of the four capsules confine all processes concerning the conference server native component. The other two capsules confine all processes related to the client native components. The hourglass objects in the center of figure 7-88 depict a notation for a combined SE-ODP interpreter and IPC runtime object, i.e., the native component for the processing and communication run-time objects; a logical assumption is that the server is at a location separate from the clients.

The Conference Server capsule(s) confines all processes related to the Epochs/SPs in table 7-32.

Table 7-32. Conference Server Capsules

Capsule	**Epoch**	**to**	**p810004.2 Service Profile**
1	Construction		SP-A
1	Configuration		SP-B
2	Initialization		SP-C
2	Execution		SP-Q

The construction epoch concerns confinement that may be achieved when programs are constructed and linked together perhaps with respect to a local operating system. The configuration epoch could address the binding processes when data conferencing resources have been named, identified, and located, perhaps accessing a wide-area distributed data conference. The initialization epoch are those processes that may bind as a result of the first capsule's confinement and instantiation, whereby joint actions between either the processing or the communications (support) native objects are either statically or dynamically initialized prior to the operation's active state. The execution epoch is all the processes that may be confined due to a particular multi-point data conference which has become active and wherein trading is taking place between all visible objects as prescribed by the other epochs, confinements, and service profiles.

The capsules labeled Basic-mode and Value-added conference(s) also consort with the same epochs and service profiles as the Conference Server capsules, but these capsules do not lend themselves to classification by epoch. The dashed lines in figure 7-88 illustrate a special type of binding which transcends the confinement to interactions with SE-ODP support-type native components. This special kind of binding/confinement is depicted in figures 7-89 and 7-90. These figures emphasize a service-oriented confinement in contrast to the epoch/SP context of figure 7-88. However, the multi-part Service Profiles SP-A, -B, -C, and -Q have subsidiary specifications which marry both the service- and operations-oriented interactions.

7.4.2.8.11 pAP 810004.2 Basic-Mode Data Conferencing

Figure 7-89 is a different operations viewpoint from that of figure 7-88 as reviewed in the foregoing section. Figure 7-89 introduces particular functions for capsules that are confined to the Conference Server, and another set of capsules—using a group capsule notation—that cite the capsules which confine the supplementary services that interwork with the I.254 CONF supplementary service. The following tables relate properties of the Basic-Mode Service Profiles that are applicable to this profile's guidelines.

All wide-area ISDN circuits are point-to-point. Primary rate access is only available in a point-to-point configuration. Bearer capability and low layer compatibility information elements only provide for point-to-point configurations at the user-network interface.

Using ISDN CPE reference configurations, multiple access points, point-to-multi-point connections, and broadcast channels should enable the equivalent of a multi-point connection or configuration as required by this profile. The passive bus or extended passive bus at the S reference point provides the equivalent of a multi-point connection. The NT1 star arrangement, with separate point-to-point links to terminal equipment, functions as a point-to-multi-point configuration.

The service connectivity required to effect a multi-point data conferencing profile is available via the I.231 series as listed in table 7-33. The unidirectional multi-point service may meet the needs of a particular data conference, but its adoption is an implementation issue. For the bidirectional multi-point service, it must be symmetric for 1 x 64 or 2 x 64 B-channels per I.231. In the future, the H-channels will enable a bidirectional asymmetric data conferencing profile, e.g., 384K from server resources and 64K between the clients.

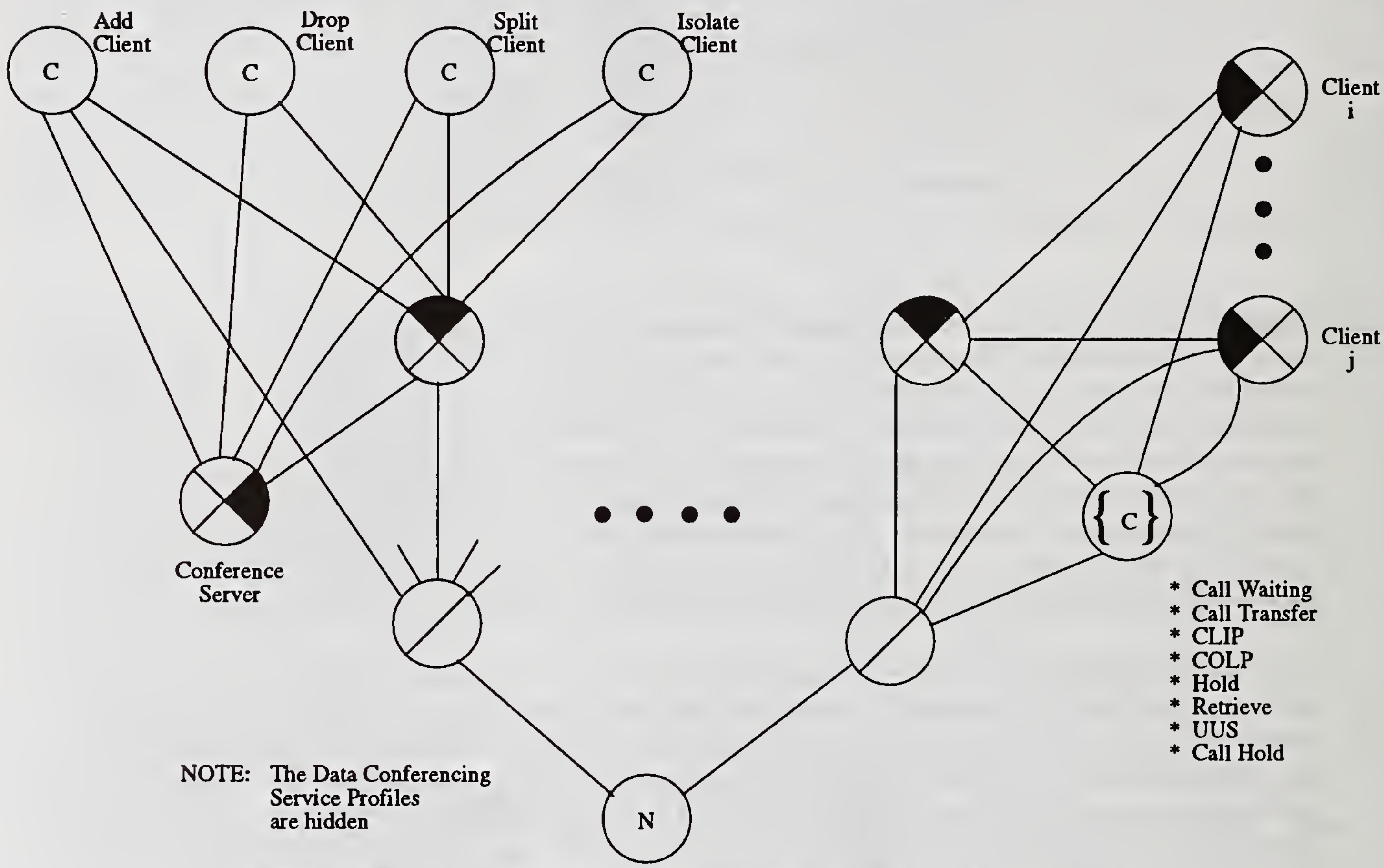


Figure 7-89. pAP 810004.2 Data Conferencing Basic-Mode Procedures.

This profile requires the I.254 supplementary service for multi-party conferencing. I.254 assumes that the facilities to achieve a multi-point connection are provided outside the scope of I.254, e.g., data bridging equipment. Likewise, this profile makes no assumptions as to the physical realization or implementation issues for bridging multi-point data conferencing participants.

Based on the I.254 requirement, this profile defines the feature sets for a basic-mode multi-point (I.254 = CONF) data conferencing service, and presents the conformance options from the viewpoint of the Conference Server. Additionally, the I.254 = CONF + 3PTY multi-point data conferencing service is defined. These options are reflected in table 7-34 for the Server Capability.

This profile also defines a value-added multi-point data conferencing operation which is accommodated when other I.250 supplementary services are engaged between clients, clients and server, or parties that are entering, leaving or on hold from the data conference.

Table 7-33. pAP 810004.2 Bearer Service Categories

Channels	Bearer*	Service	Circuit-mode	8kHz-Structured
1 x 64	I.231.1/7	demand	bidirectional	multi-point
1 x 64	I.231.1/8	reserved	bidirectional	multi-point
1 x 64	I.231.1/9	permanent	bidirectional	multi-point
1 x 64	I.231.1/10	demand	unidirectional	multi-point
1 x 64	I.231.1/11	reserved	unidirectional	multi-point
1 x 64	I.231.1/12	permanent	unidirectional	multi-point
2 x 64	I.231.5/1	demand	bidirectional	point-to-point
2 x 64	I.231.5/2	reserved	bidirectional	point-to-point
2 x 64	I.231.5/3	permanent	bidirectional	point-to-point

* extracted from the CCITT Blue Books

1 x 64 = 64 Kbps unrestricted digital information transfer capability.

NOTE: For an interim period, some networks may only support restricted digital information transfer capability. Interworking between 64 Kbps UDI and the restricted type will be provided in the network.

Subsequent paragraphs describe the basic-mode/value-added supplementary services as viewed from object-oriented operation scenarios pursuant to figures 7-89 and 7-90.

7.4.2.8.11.1 Equipment

Data Conference Equipment for bridging, routing or switching of calls does not have to be specified in order to conform to this multi-point profile. If data conferencing equipment is specified, it does not have to be integral to either the CPE, PSN, or wide-area switching equipment. For the purpose of pAP 810004.2, it is assumed that the bridging equipment to activate multi-party connections on one or more data conferences is transparent to clients or server capabilities and shall automatically interconnect in a compatible manner. Data bridging may occur at layer 1 or above.

7.4.2.8.11.2 Number of Data Conferences

The number of clients that must be furnished in each Service Profile must be three or more although the Conference Server may be a client who has subscribed to the CONF server and is not active as a client but is active as a server (X.R) site.

There is no limit in pAP 810004.2 as to the number of clients, servers or clients/servers that may participate in a CONF, however, practical limits via standards, equipment, interworking, etc. will prevail.

7.4.2.8.11.3 Data CONF Types

The "add on" or progressive conference is the only type that the ISDN Blue Book procedures describe. Other types of data CONF such as "meet me" or "pre-determined" CONF are for further study and await ISDN standardization.

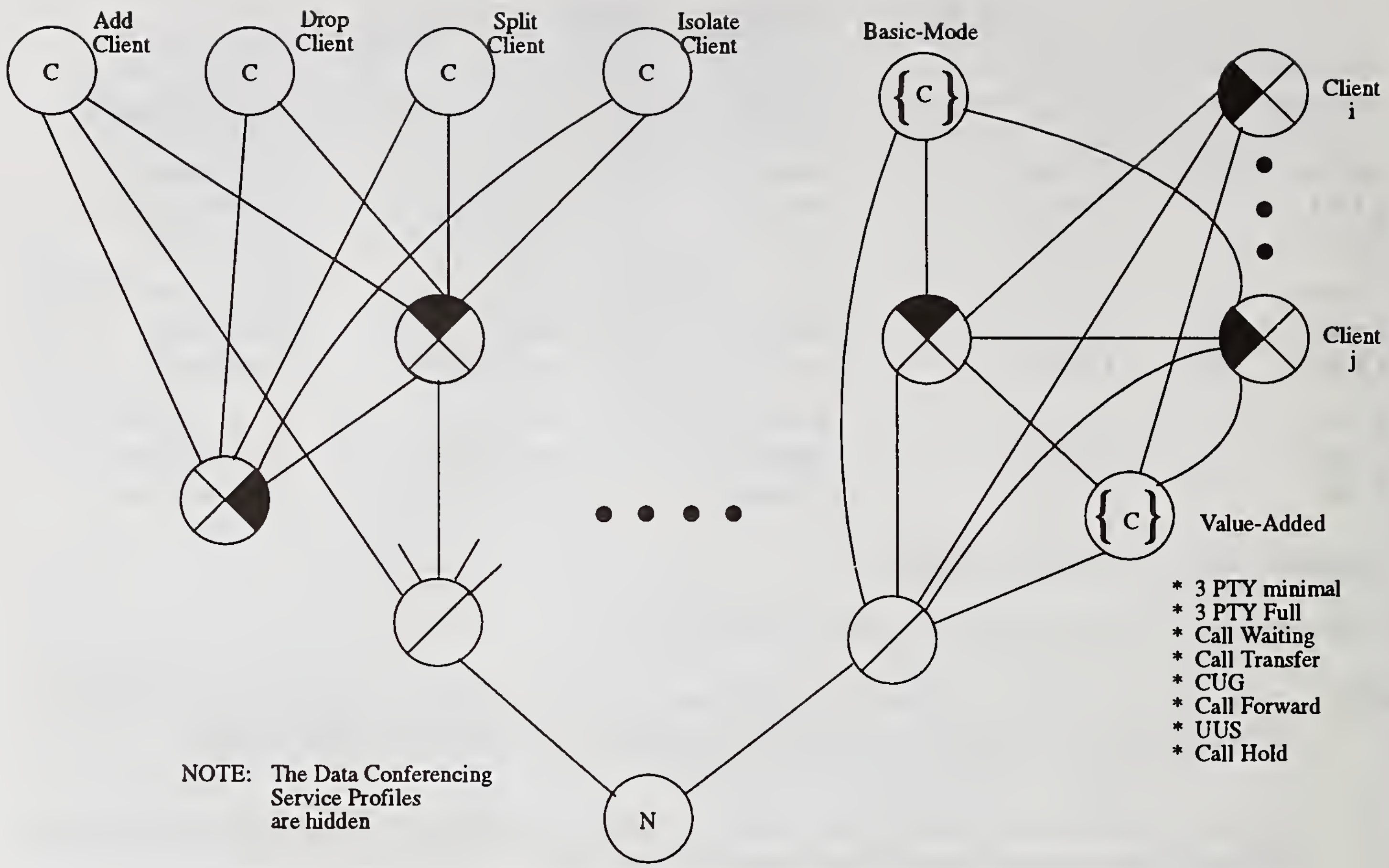


Figure 7-90. pAP 810004.2 Data Conferencing Value-Added Procedures.

7.4.2.8.11.4 Multiple Data Conferences

Clients or Servers may participate in more than one data conference. Switching from one data CONF to another via I.254 specifications or other I.250 supplementary services are prescribed by the Blue Books.

7.4.2.8.11.5 Multi-Point Conferencing Arrangements

The multi-point type nature of point-to-multi-point facilities in table 7-36 are assumed to conform to the terminology of CCITT X.1 and X.2 for descriptive purposes only.

In every demand multi-point arrangement, the nodes will function on a per call basis pursuant to the pAP 810004.2 Service Profiles. The permanent multi-point facilities are provided for an agreed contractual or subscription period. The multi-point reserved arrangements are for further study for this profile.

The permanent centralized multi-point arrangement is the only mandatory requirement for this profile. A broadcast connection type has not been defined in the Blue Books to date. Demand facilities—per public ISDN—would have to assume there are charging mechanisms for more than two access points with CONF services on a per-call basis.

The permanent centralized multi-point connection will transmit data to three or more remote end points simultaneously on a 64 kbps UDI bearer service. Unless the multi-point communications are statistically multiplexed, the remote end points on the multi-point connection can only transmit to the centralized end point one at a time. Also, data delivered from the remote end points is not delivered to the other remote

Table 7-34. Basic-Mode/Value-Added Server Capability (pAP 810004.2)

Data Conferencing Calling Supplementary	Circuit Mode			3PTY Notes
	64 UDI	64 restricted	2 x 64 UDI	
Add new client				
- server (hold)	m	m	o	3 PTY minimum
- new call (c/s)	m	m	o	3 PTY minimum
- existing call (c/s)	m	m	o	
• call ID	m	m	o	3 PTY minimum
• + client ID	o	o	o	
Drop new client				
- server				
• no client ID	m	m	o	
• client ID	o	o	o	
• 2 pty call origination	o	o	o	
Split client				
- call ID	o	o	o	
- client ID	o	o	o	
Isolate client	o	o	o	
Reattach client	o	o	o	

Legend:

c/s = client/server
m = mandatory for this profile
o = optional for this profile

end points.

Decentralized multi-point connections may transmit and receive from all end points on the multi-point arrangement. Broadcast arrangements for data conferencing are a future study item for this profile.

7.4.2.8.11.6 pAP 810004.2 Data Conferencing Basic-Mode Procedures

Using the object notation of figure 7-89, the capsules confined to the Conference Server depict the capability which either the Administrator or the Facilitator function will choose depending upon the particular "appearances" of the client activities, or the needs of controlling or administering the data conferencing application.

Figure 7-89 is a processing model, and by use of the nucleus and interface adapter objects, hides the SE-ODP run-time communication IPC objects. The group capsule symbol is used with the client native components in order to confine all of the I.250 Supplementary services to this basic-mode processing model.

Table 7-35. Basic-Mode/Value-Added Client Capability (pAP 810004.2)

CONF[1] Supplementary Services	Circuit Mode			Conference Calling or 3 PTY (Notes)
	64 UDI	64 restricted	2 x 64 UDI	
DDI	o	o	o	
MSN	o	o	o	Will receive the number of the conference server.
CLIP/R	o	o	o	
COLR/P	o	o	o	Conference server with a COLP subscription should receive the COLP.
Call Transfer	o	o	o	Conference server, client, or any party in the data conference.
Call Forwarding Unconditional	o	o	o	Forwarded-to user will be added.
Line Hunting	o	o	o	
Call Waiting	o	o	o	Any conference client or server will receive an indication and the server may add the caller to the conference.
Call Hold	o	o	o	Any conference client or server may place the data conference/party on hold and then later retrieve the data conference/party, plus the conference server may be a server or client on more than one data conference and may switch between data conferences.

[1]see I.250 Series
o = optional pAP 810004.2 Capability

7.4.2.8.12 pAP 810004.2 Multi-Point Data Conferencing Value-Added Procedures

Figure 7-90 is another ODP processing model. It is fundamentally the same model as figure 7-89, with the addition of a group capsule notation for enabling the conferencing supplementary service to interwork with the 3 PTY supplementary service. The specifications for 3 PTY and CONF supplementary service are according to I.254.

The value-added model also incorporates user-to-user signalling (I.257) and community of interest (CUG) supplementary services (I.255).

Table 7-36. pAP 810004.2 Multi-Point Facilities

Type	1x64 UDI	Service	Type	Profile Option
Broadcast	unidirectional	I.231.1/10	demand	ffs
	unidirectional	I.231.1/11	reserved	ffs
	unidirectional	I.231.1/12	permanent	o
	bidirectional	I.231.1/7	demand	ffs
	bidirectional	I.231.1/9	permanent	o
Centralized Multi-point (i.e., polled)	bidirectional	I.231.1/7	demand	o
	bidirectional	I.231.1/8	reserved	ffs
	bidirectional	I.231.1/9	permanent	m
Decentralized Multi-point (i.e., random access)	bidirectional	I.231.1/7	demand	o
	bidirectional	I.231.1/8	reserved	ffs
	bidirectional	I.231.1/9	permanent	o

ffs = for further study
o = optional
m = mandatory

7.5 Messaging and Answering

7.5.1 Voice Messaging Systems

This application profile provides the descriptions necessary to meet the requirements of three NIUF user applications: "Transparent Networking of Voice Messaging Systems" (860016.0) (Ref. [44]); "Interface to Voice Messaging Systems" (860018.0) (Ref. [45]); and "Interface to Centralized Voice Messaging System" (810034.0) (Ref. [46]).

7.5.1.1 User Description

Voice Messaging Systems (VMS) are becoming a fundamental component of corporate telecommunications networks. ISDN services and products must be capable of interfacing with these units while providing as good or better service than is available today. North American ISDN Users' Forum "users" have submitted ISDN applications requiring an ISDN application that provides the capability for integrating VMS with ISDN service.

VMS allows automatic telephone coverage without the need for individual station equipment (i.e., answering machines) or full-time monitoring by other personnel (i.e., secretaries). VMS can also provide the functionality for voice mail where callers may leave voice messages for others without directly calling the others. A third function of VMS is call prompting which provides callers with additional information before selecting various options processed by the VMS. Call Prompting goes beyond the scope of this document.

Calls to VMS subscribers' telephones are redirected by the ISDN switch (Telco central offices or PBXs) to the VMS with sufficient information for the VMS to efficiently handle the call. Calls can be redirected several ways—the VMS subscriber can "call forward all calls" to the VMS (CFU—Call Forward Unconditional); calls with no answer can be call forwarded (CFNR—Call Forward No Reply); and calls to a busy telephone can be call forwarded (CFB—Call Forward Busy). In the case of voice mail, the VMS subscriber directly calls the VMS to leave messages rather than being call forwarded by the ISDN switch. Calling parties select options provided by call prompting (i.e., redirecting to another telephone by the ISDN switch, redirected to another VMS subscriber's mailbox by the VMS).

The VMS must be able to receive and store the message in the appropriate VMS subscriber's mailbox and in turn alert the VMS subscriber that a message is waiting by activating some type of message waiting indicator (MWI) (i.e., lamp, display, interrupted dial tone). Future functions may allow the VMS to include the calling ID or name, an urgent indication, etc., in the message waiting notification. The VMS should be capable of serving both ISDN and non-ISDN subscribers.

Figure 7-91 shows an overview of the user physical environment for voice messaging and answering applications. It includes one or more ISDN switches networked together, one or more VMSs networked together, non-VMS calling parties (analog, digital and ISDN) and VMS subscribers (analog, digital and ISDN). The BRI and PRI ISDN interfaces should support this VMS Application Profile.

This application profile provides the descriptions necessary to meet the requirements of three NIUF user applications: "Transparent Networking of Voice Messaging Systems" (860016.0); "Interface to Voice Messaging Systems" (860018.0); and "Interface to Centralized Voice Messaging System" (810034.0). The profile also refers to "Secure Voice Mail" (050015.0) (Ref. [47]), "Secure E-Mail" (050014.0) (Ref. [48]) and "Secure Facsimile Transmission through ISDN" (050016.0) (Ref. [49]) although the security aspects are not included in this profile.

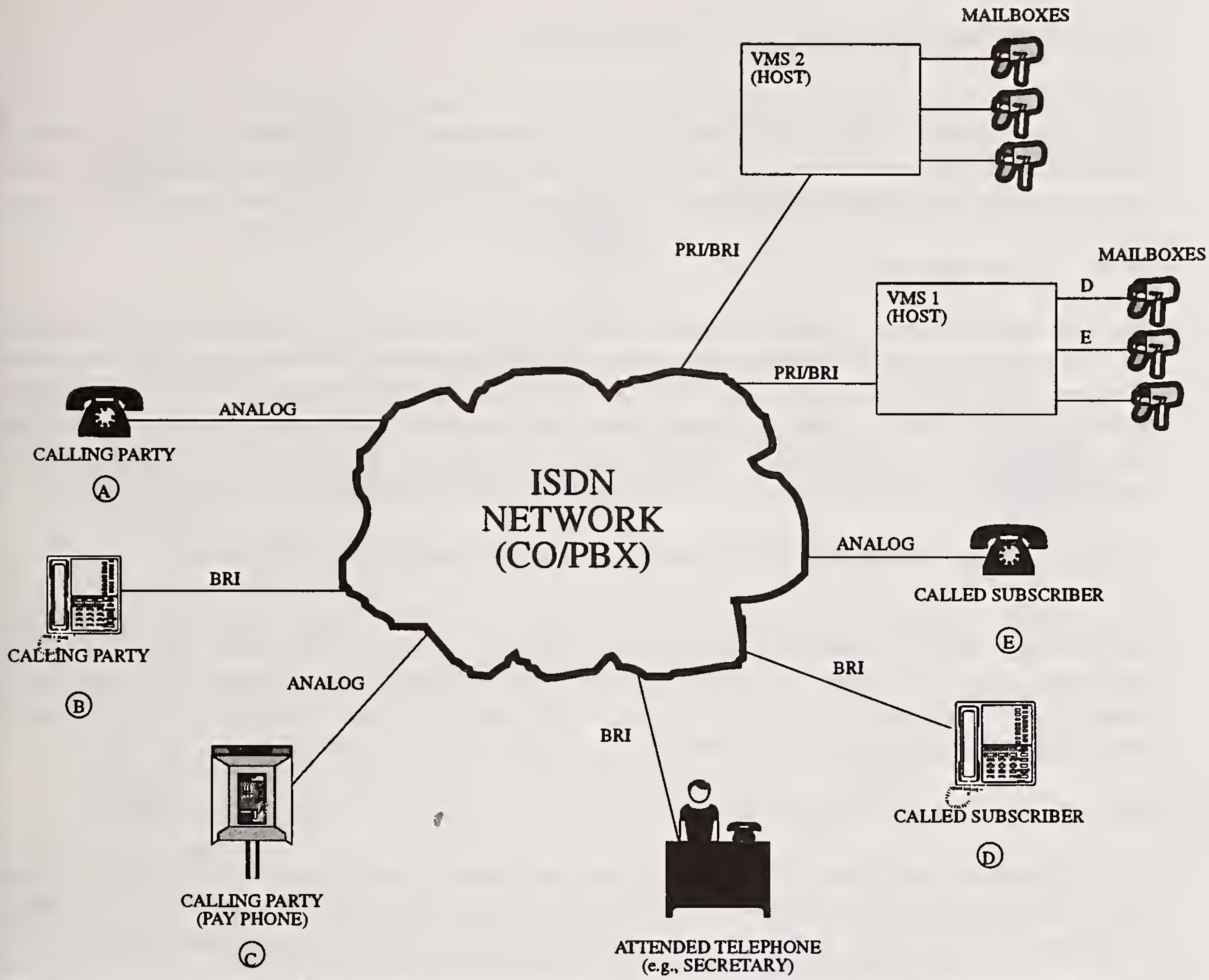


Figure 7-91. Overview of Physical Environment for Voice Messaging and Answering Applications.

7.5.1.2 ISDN Application Breakdown

The above user description is divided into three distinct cases based on different interactions between the ISDN switch and the VMS user. The three cases, Call Answering, Call Answering with Call Transfer to an Attendant, and Direct Access to Voice Mail are depicted in figure 7-92. The following describes the different interactions required between the ISDN switch, the VMS, the calling party and the called party.

7.5.1.2.1 Call Answering

The VMS function allows automatic telephone coverage without the need for individual station equipment (i.e., answering machines) or for full-time monitoring by other personnel. Calls to the VMS subscriber's telephone are redirected by the ISDN switch to the VMS with sufficient information for the VMS to handle the calls. The calls may be redirected several ways: call forward all calls to the VMS; call forward calls encountering a busy status; call forward no response calls. Calls may also be call transferred to a VMS subscriber mailbox by a third party such as a secretary or call attendant who received the initial call.

7.5.1.2.2 Call Answering With Call Transfer To An Attendant Or Pager Notification

This is similar to the above description when the initial call is call forwarded to the VMS. The VMS has the additional feature allowing the calling party the ability to transfer out of the VMS back to an attendant/secretary's telephone. The VMS may also allow the calling party the ability to page the desired person. These capabilities are used for urgent or emergency calls when a message is not sufficient or timely. The calling party may also transfer out of the VMS to make other calls.

7.5.1.2.3 Direct Access To Voice Mail

A VMS subscriber may call the VMS directly to leave messages for one or more VMS subscribers or other VMS subscribers if networked together with the initial subscriber's VMS. The voice mail functionalities are analogous to E-mail and include the ability to edit, broadcast, save, delete and retrieve messages, etc.

7.5.1.3 Service Logic

Voice Messaging and Answering Applications involve combinations of three different processes: VMS Subscriber Access, VMS Subscriber Notification and VMS Subscriber Message Retrieval. Section 7.5.1.4, Messaging and Answering Application Processes, describes each of these processes in more detail. In a single VMS system, the calling party accesses the VMS subscriber's mailbox and leaves a message. The subscriber is notified that a message is waiting and then retrieves the message. The VMS subscriber's notification is then canceled. This flow is shown in figure 7-93. The flow is basically the same in a multiple VMS environment, except that after the calling party leaves a message, the first VMS sends the message to the VMS subscriber's mailbox on the second VMS through message networking. The multiple VMS messaging and answering applications flow is shown in figure 7-94.

7.5.1.4 Messaging And Answering Application Process

The following describes the three basic Messaging and Answering application processes in more detail: Subscriber Access, Subscriber Notification, and Subscriber Message Retrieval.

7.5.1.4.1 Subscriber Access

Subscriber access is the first stage in Messaging and Answering application process.

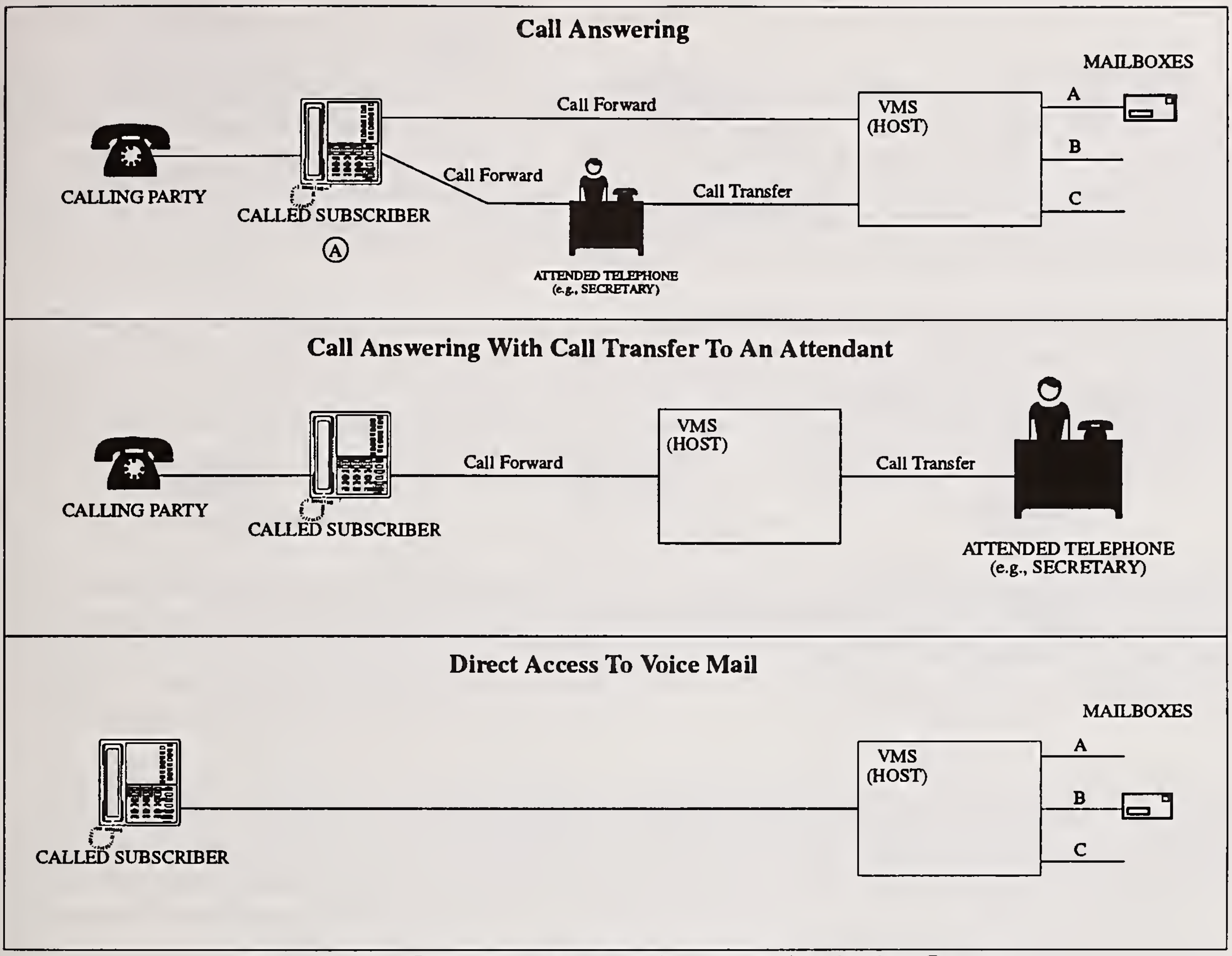


Figure 7-92. ISDN Messaging and Answering Application Cases.

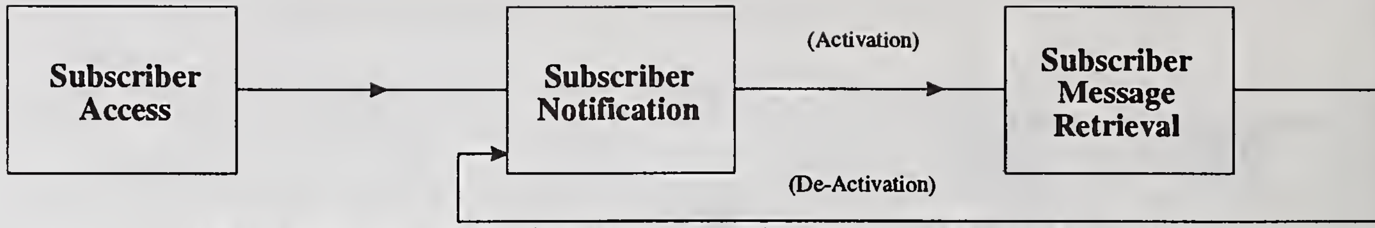


Figure 7-93. Single VMS Messaging and Answering Application Processes.

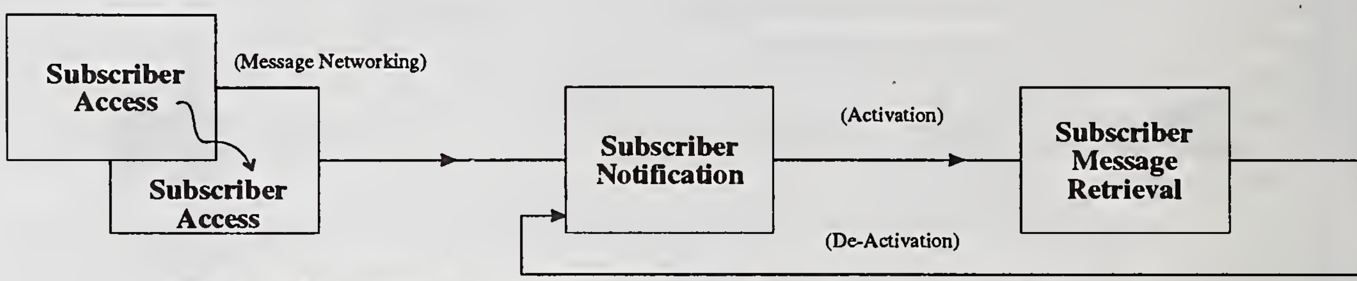


Figure 7-94. Multiple VMS Messaging and Answering Application Processes.

7.5.1.4.2 Application Process Description

Subscriber access includes the steps to connect the calling party to the VMS so that a message may be recorded and deposited in the called party's VMS subscriber mailbox. It allows the calling party to transfer out of the VMS when desired. This occurs when the calling party desires to speak to an attendant or secretary. When this happens, the calling party has left the Messaging and Answering applications process. Sometimes a secretary or attendant may transfer a calling party to the VMS to leave a recorded message for the called party. In this case, the process treats the call exactly as if the calling party called directly.

The Message Networking subprocess is optional and used only when multiple VMSs need to communicate with each other using the ISDN network. This situation occurs in campus environments with multiple VMSs and one ISDN switch or in inter-location environments with multiple VMSs and multiple ISDN switches. The networking communication occurs when one VMS needs to deliver messages to another VMS. The objective is that multiple VMSs should appear as one large VMS to the VMS subscribers.

7.5.1.4.2.1 Subscriber Access Process Alternative Architectures

A calling party may be forwarded or transferred to the VMS using one of several different service elements including Call Forwarding Busy (CFB), Call Forwarding Variable (CFV), or Call Forwarding No Answer. The particular service element used to establish connectivity is not critical to the Subscriber Access stage. What is critical is that the calling party is connected to the VMS with an opportunity to leave a voice message in the VMS subscriber's mailbox.

Figures 7-95, 7-98, 7-101, 7-104, and 7-106 show the specific physical environment for each of the three cases described in section 7.5.1.2. The various steps in each case are simplified to show typical interactions between the calling party and the VMS. In the real world this interaction might be more complicated. For example, a VMS subscriber might be the calling party wishing to leave another subscriber a message and retrieving a message on the single call.

In 7-95, 7-98, 7-101, and 7-104, Subscriber Access is defined so that all the VMS subscribers are connected to a single ISDN switch or PBX. In the real world, however, Messaging and Answering applications will also occur in multiple ISDN switched networks.

The Message Networking physical environment necessary to have one VMS communicate with a second VMS is shown in figure 7-106. This environment will require multiple VMSs (possibly from different manufacturers) to forward voice mail over ISDN networks in a standard and uniform way.

7.5.1.4.2.2 Information Flow Diagrams

Information Flow Diagrams show the specific service elements necessary to complete the Messaging and Answering application process. For example, the Information Flow Diagram for Call Answering—No Answer is shown in figure 7-96. The Diagram for Call Forwarding—Busy or Variable is shown in figure 7-97. The remaining Diagrams for Subscriber Access are shown in figures 7-99, 7-100, 7-102, 7-103, 7-105 and 7-107.

7.5.1.4.2.3 Protocol Requirements and Application Service Element Description

The supplementary services, messages and protocol elements described below are only those required by this profile. Other messages and protocol elements are not discussed if they are not used by the application being described, even though they may be required for other reasons, such as routing of the call. See figures 7-95, 7-98, 7-101, 7-104, and 7-106. Please note that the required ANSI and NIUF documents will be supplied as they become available. NIUF.xxx implies that the Messaging and Answering Profile team is requesting the Supplementary Services Working Group to create that particular document.

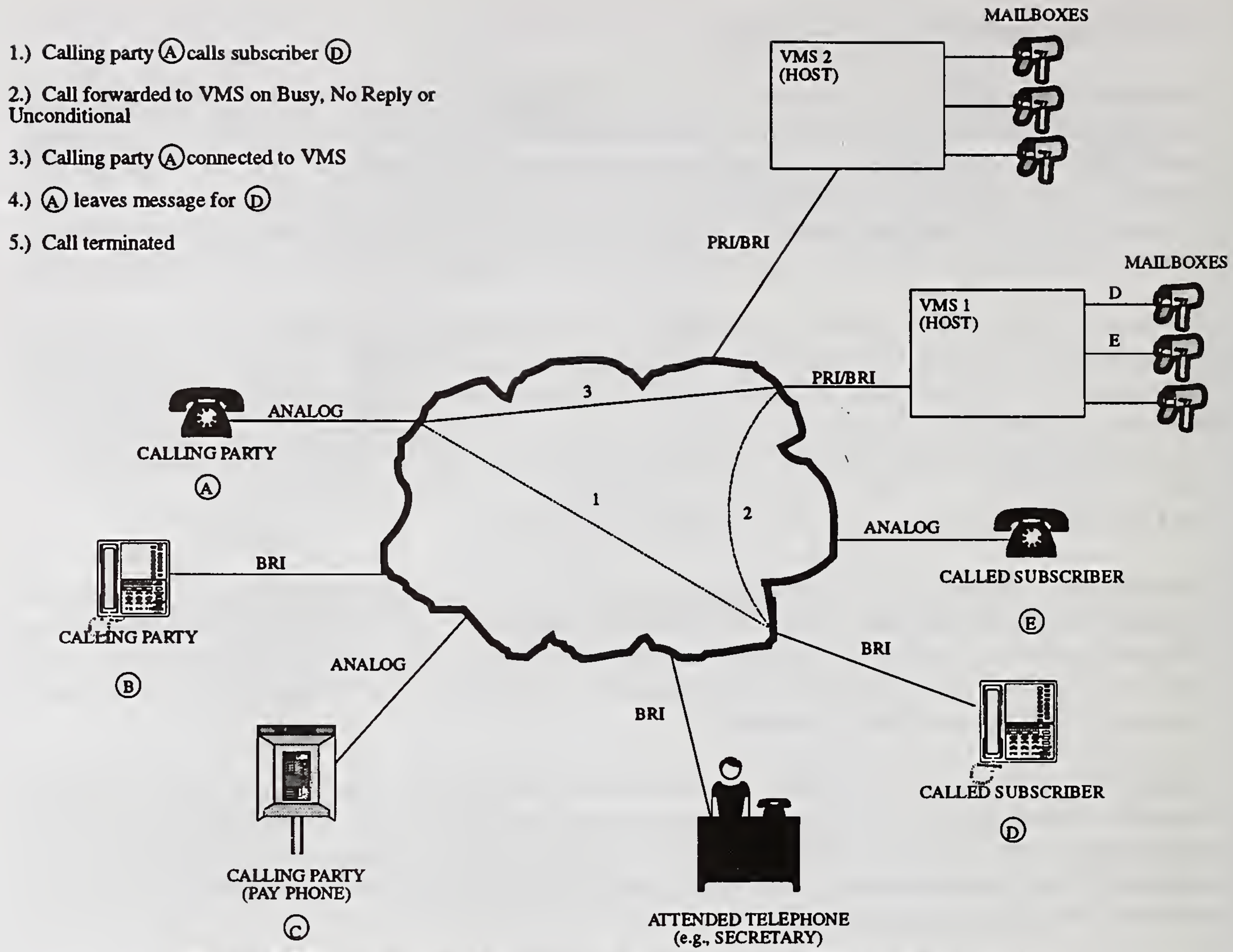
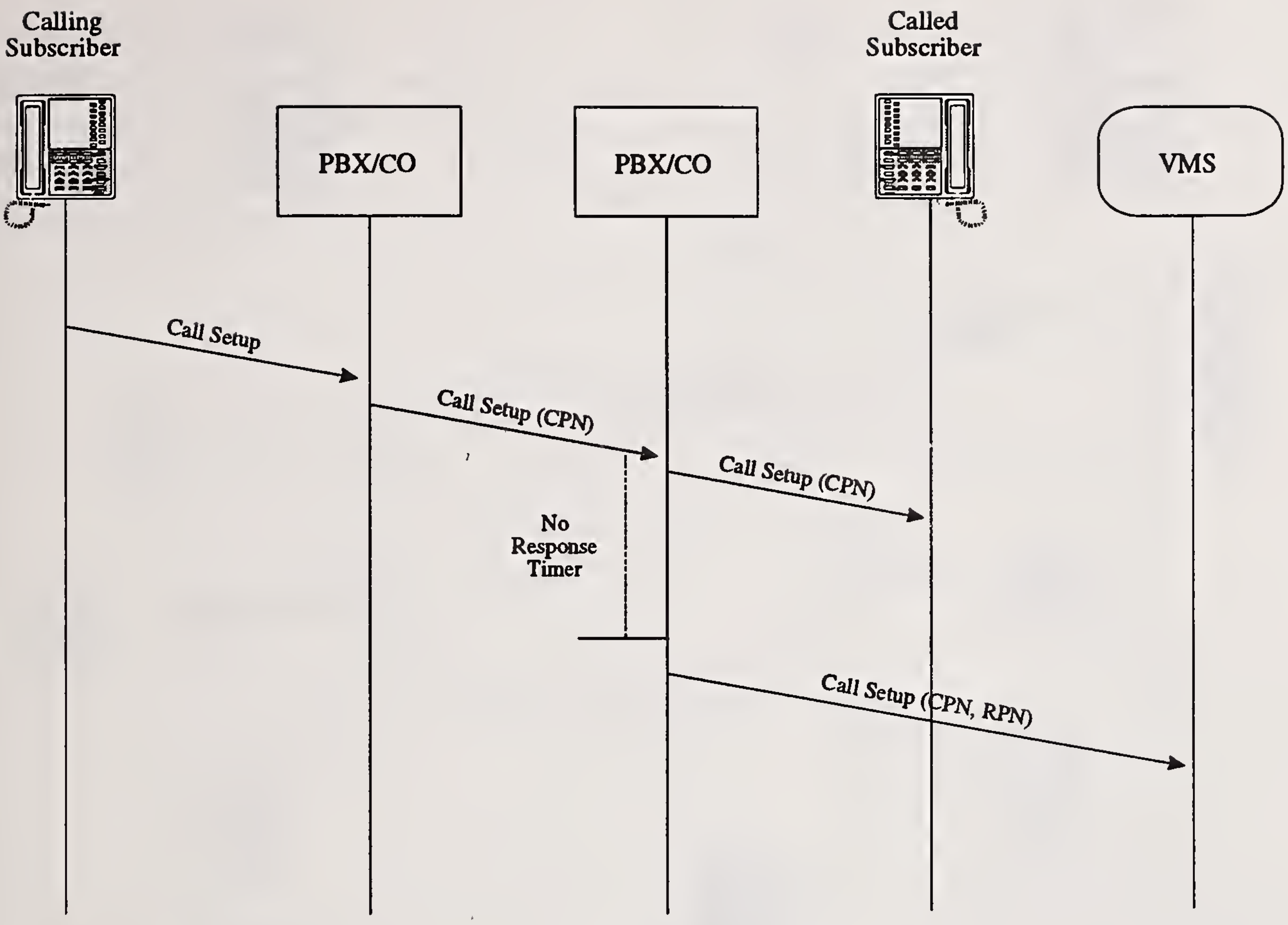
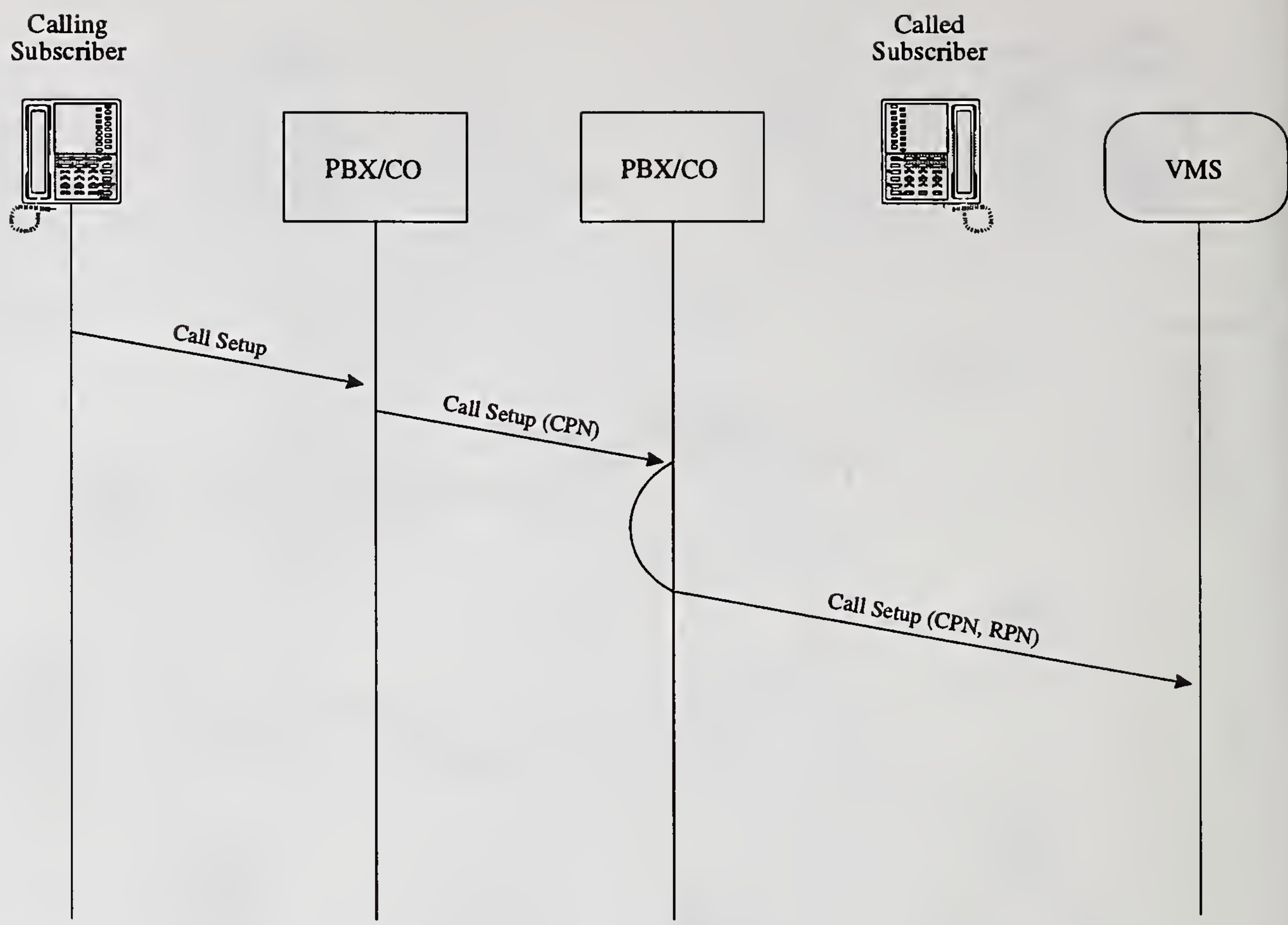


Figure 7-95. Subscriber Access—Call Answering (Call Forwarded to VMS).



CPN = Calling Party Number
RPN = Redirected Party Number

Figure 7-96. Subscriber Access—Call Answering (Call Forwarded to VMS on No Reply)—Information Flow Diagram.



CPN = Calling Party Number
RPN = Redirected Party Number

Figure 7-97. Subscriber Access—Call Answering (Call Forwarded to VMS on Busy/Unconditional)—Information Flow Diagram.

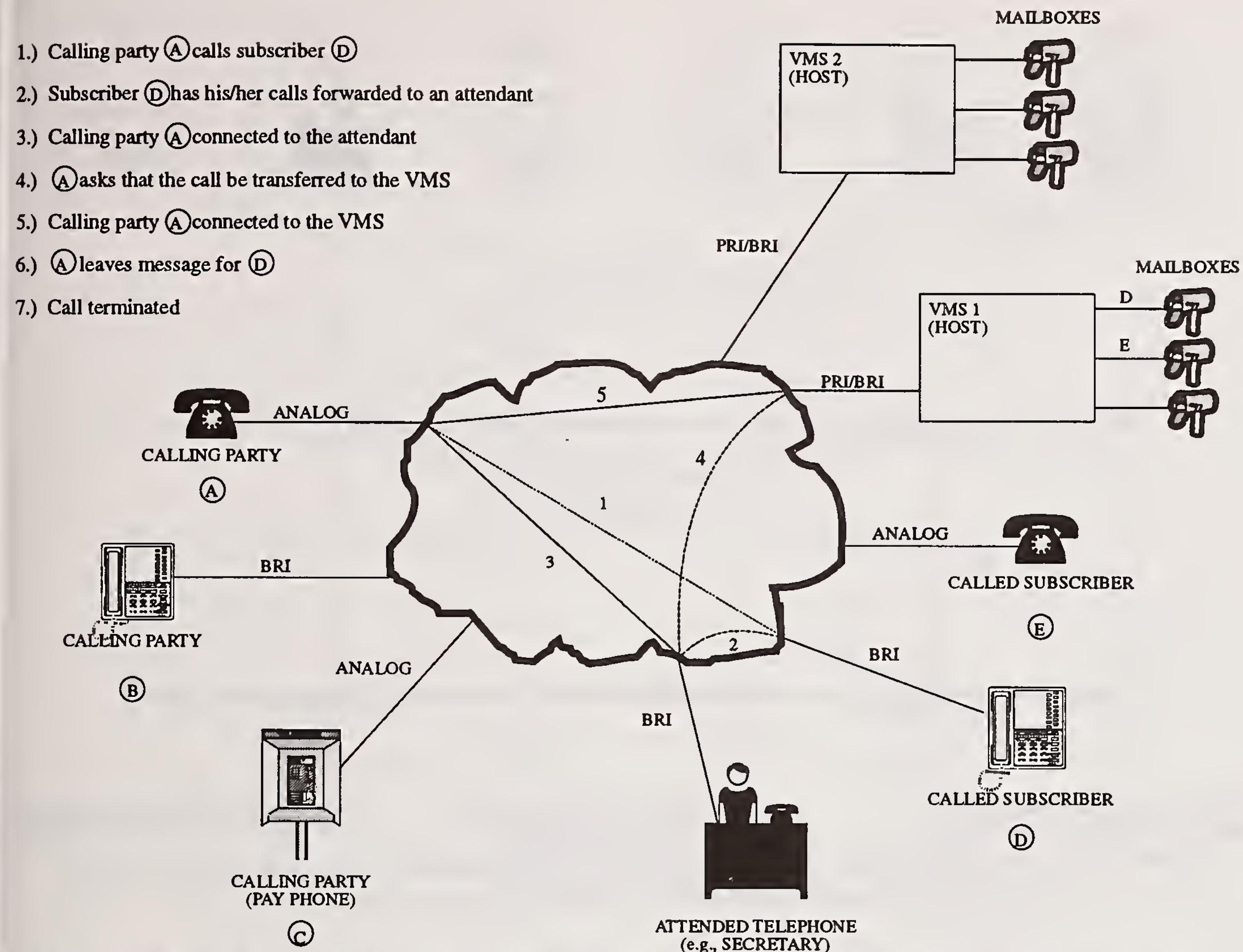
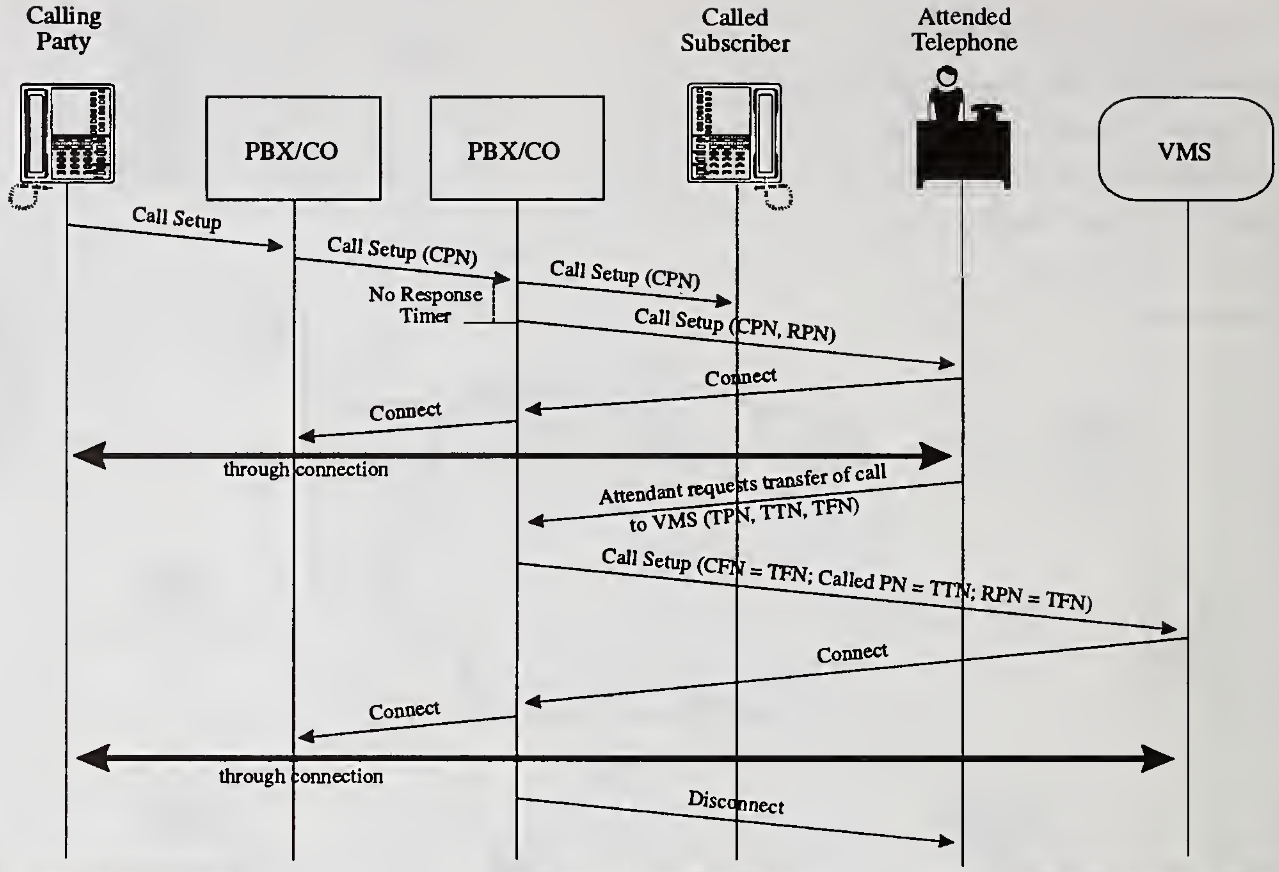
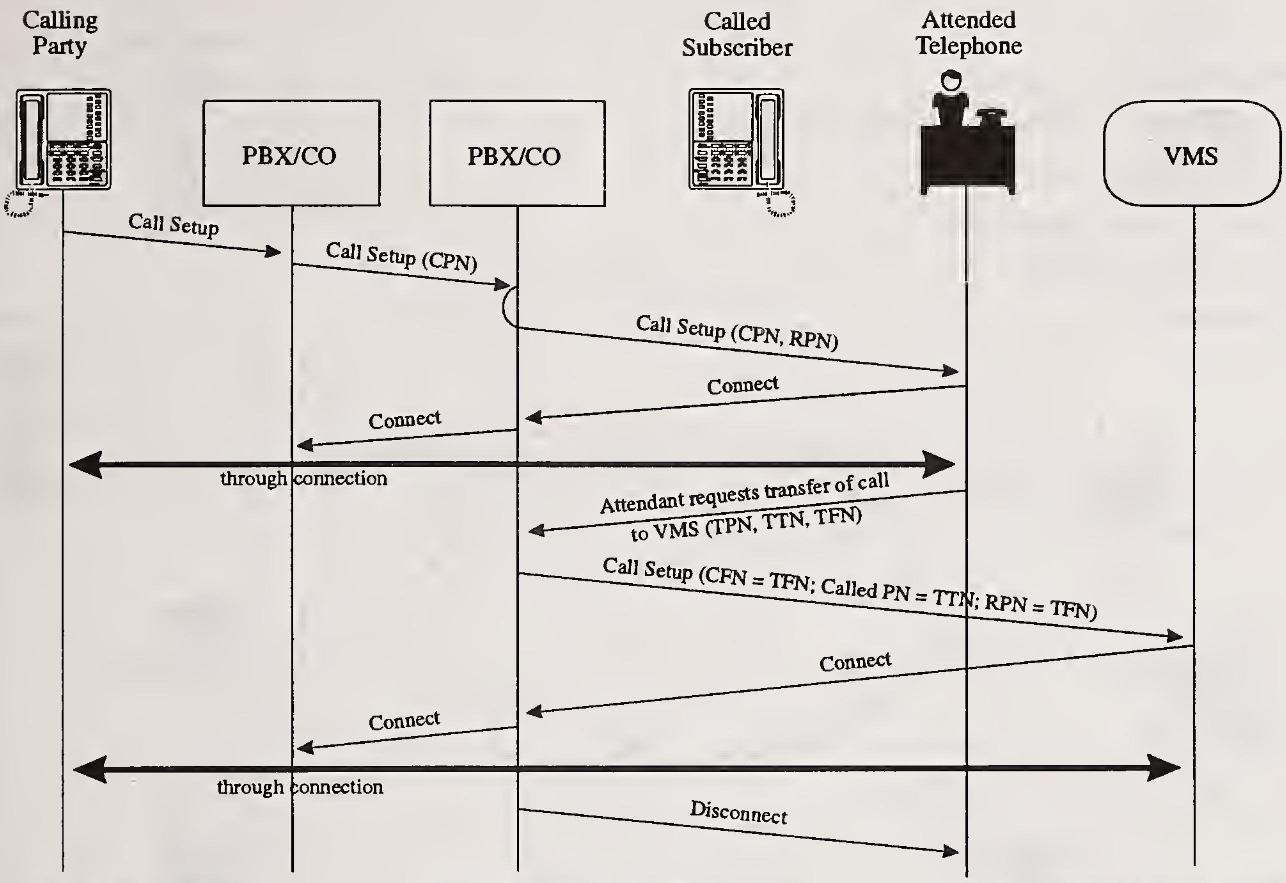


Figure 7-98. Subscriber Access—Call Answering (Call Forwarded to Attendant Who Transfers the Call to VMS).



CPN = Calling Party Number **TPN = Transferred Party Number** **TFN = Transferred From Number**
RPN = Redirecting Party Number **TTN = Transferred to Number**

Figure 7-99. Subscriber Access—Call Answering (Call Forwarded on No Reply to Attendant Who Transfers the Call to the VMS)—Information Flow Diagram.



CPN = Calling Party Number
RPN = Redirecting Party Number
TPN = Transferred Party Number
TTN = Transferred to Number
TFN = Transferred From Number

Figure 7-100. Subscriber Access—Call Answering (Call Forwarded on Busy/Unconditional to an Attendant Who Transfers the Call to the VMS)—Information Flow Diagram.

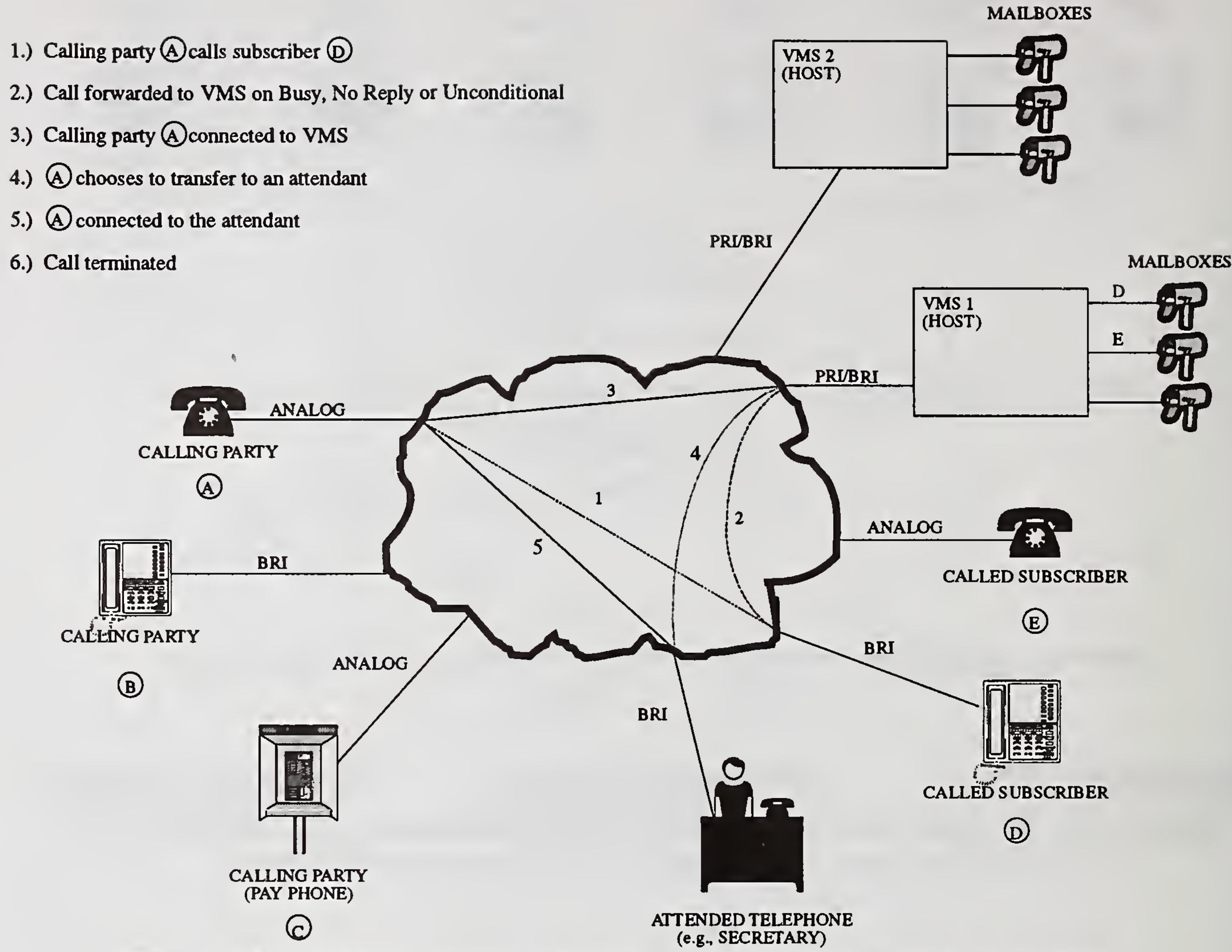
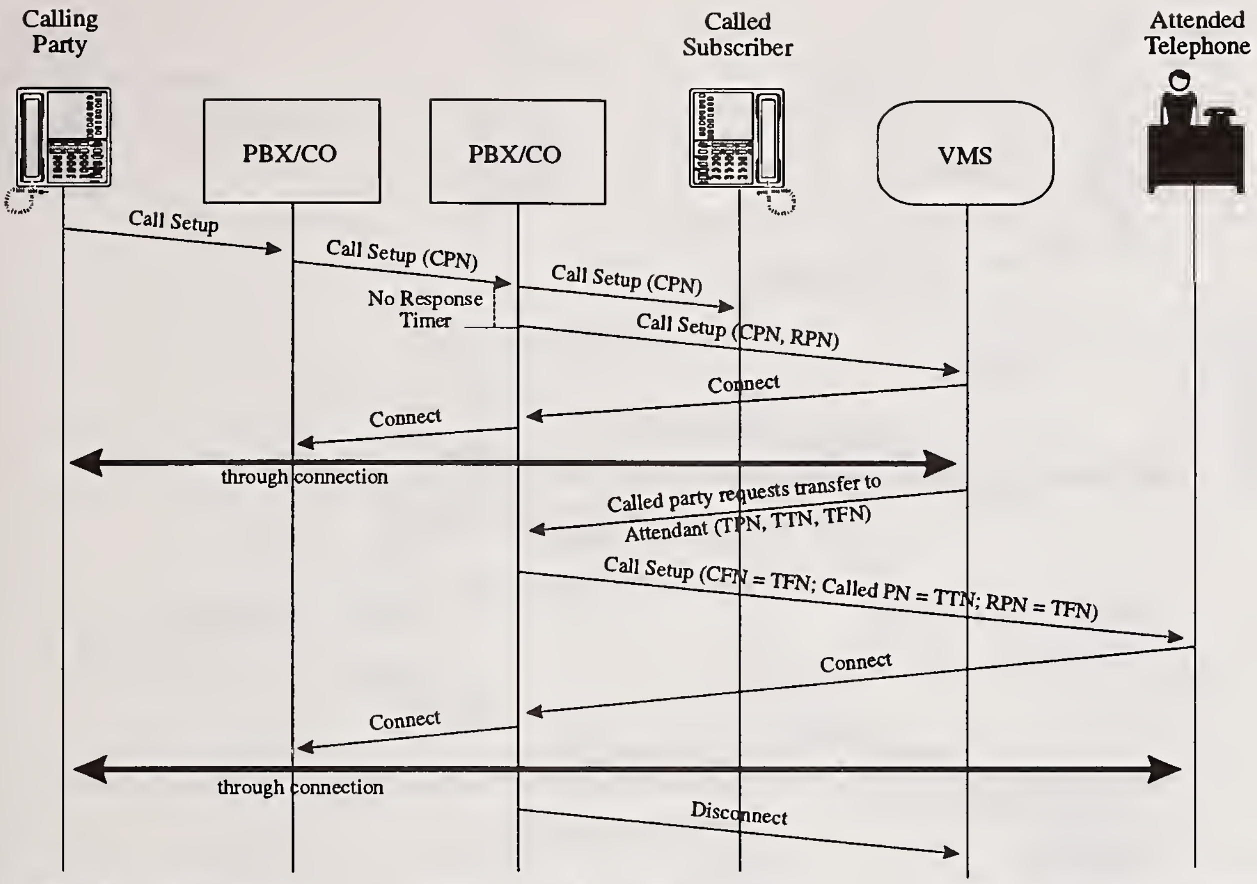
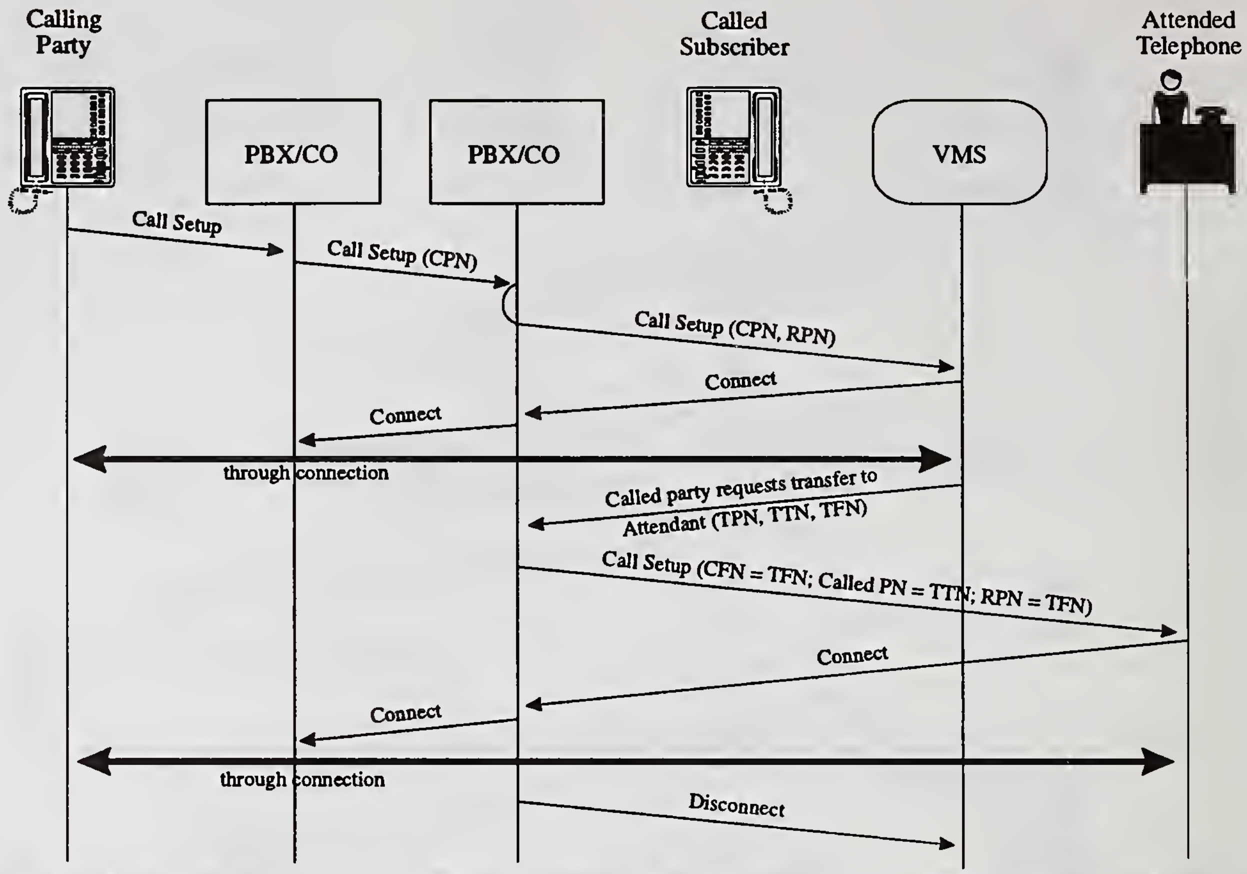


Figure 7-101. Subscriber Access—Call Answering with Call Transfer to an Attendant.



CPN = Calling Party Number
RPN = Redirecting Party Number
TPN = Transferred Party Number
TTN = Transferred to Number
TFN = Transferred From Number

Figure 7-102. Subscriber Access—Call Answering (Call Forwarded to VMS on No Reply) With Call Transfer to an Attendant—Information Flow Diagram.



CPN = Calling Party Number
RPN = Redirecting Party Number
TPN = Transferred Party Number
TTN = Transferred to Number
TFN = Transferred From Number

Figure 7-103. Subscriber Access—Call Answering (Call Forwarded to VMS on Busy/Unconditional) With Call Transfer to an Attendant—Information Flow Diagram.

1.) Subscriber D calls VMS

2.) D leaves voice message for E

3.) Call terminated

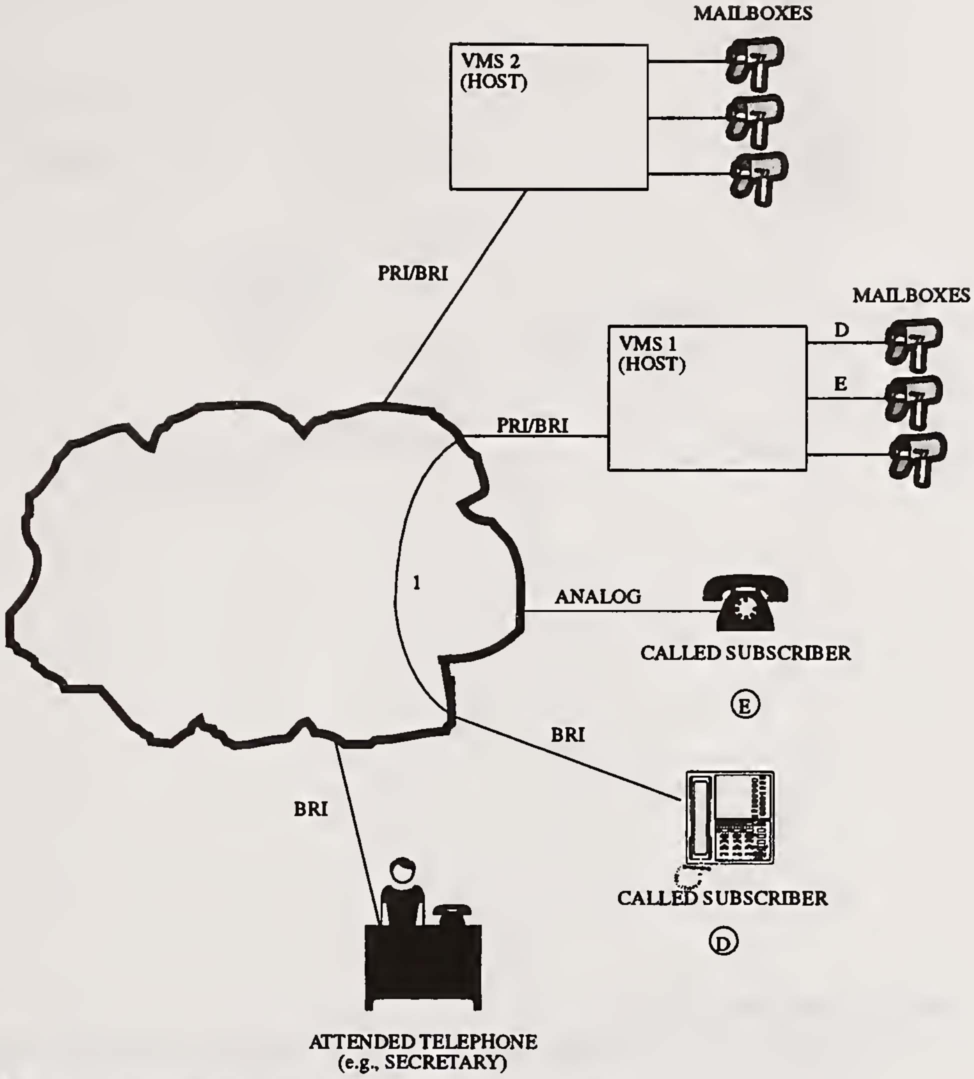
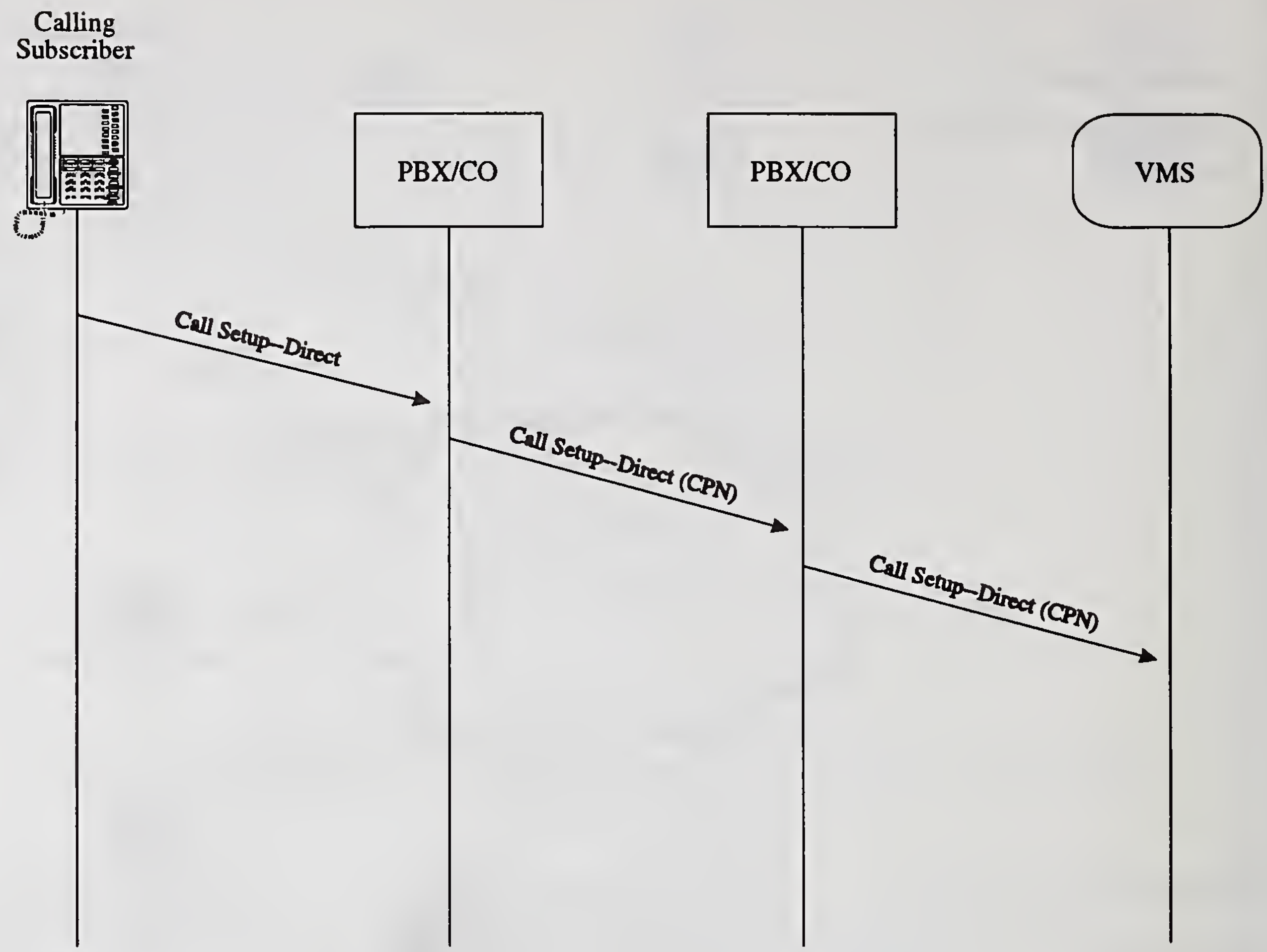


Figure 7-104. Subscriber Access—Direct Call to Voice Mail.



CPN = Calling Party Number

Figure 7-105. Subscriber Access—Direct Call to Voice Mail—Information Flow Diagram.

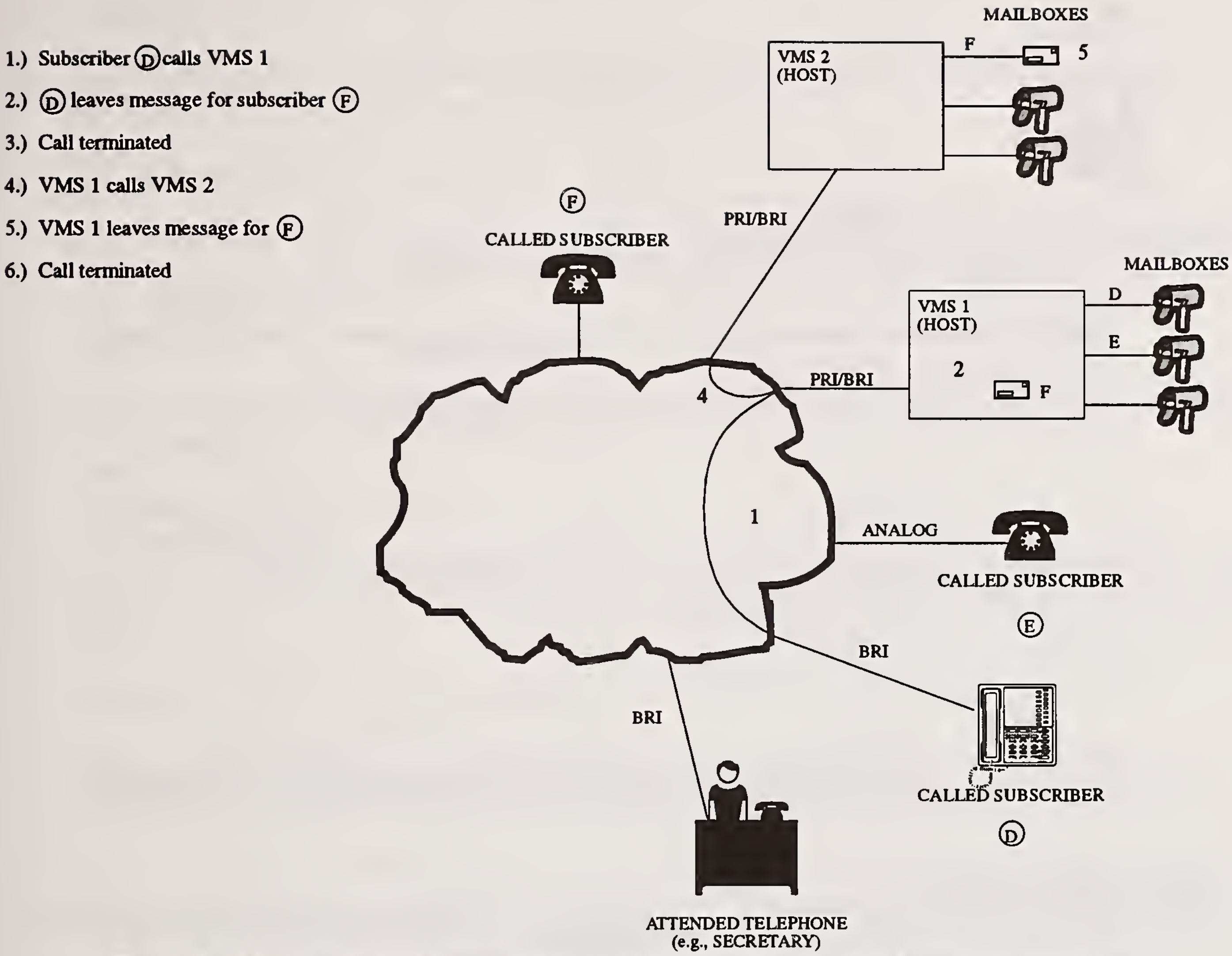
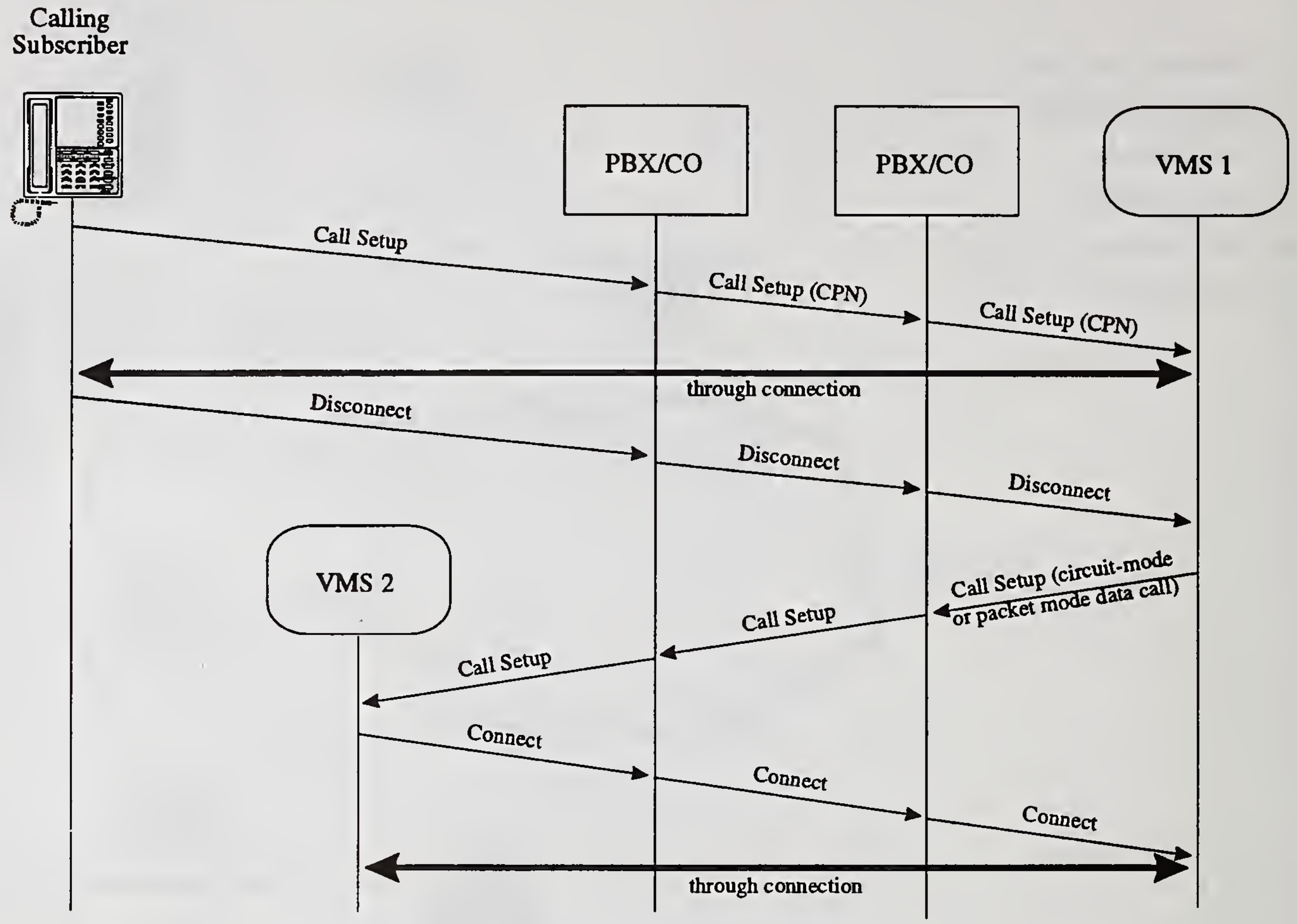


Figure 7-106. Subscriber Access—Direct Call to Voice Mail with Message Networking.



CPN = Calling Party Number

Figure 7-107. Subscriber Access—Direct Call to Voice Mail with Message Networking—Information Flow Diagram.

Call Setup

The call setup process is described in NIUF 90-301 (Appendix A) and NIUF 90-302 (Appendix B). This process is used to establish the initial call.

Call Forwarding With Associated Data

The Call Forwarding supplementary service is defined in T1.xxx and NIUF.xxx. This service supplies the VMS with the subscriber's DN which will be used to deposit the message in the proper mailbox.

Call Setup (direct)

The call setup process is described in NIUF 90-301 and NIUF 90-302. This process is used to set up a call directly to the VMS.

Call Delivery With Associated Data

The call (i.e., voice message) is delivered to the VMS using NIUF 90-301 or NIUF 90-302. These protocols supply the VMS with the subscriber's DN which will be used to deposit the message in the proper mailbox.

Connectivity to Called Subscriber's Mailbox

Current protocols exist to supply connectivity between the switch and the VMS; however, when connecting the VMS and the Switch via ISDN, the NIUF 90-301 and NIUF 90-302 documents are required.

Call Transfer With Associated Data

The Call Transfer supplementary service is defined in T1.xxx and NIUF.xxx. These services supply the VMS with the subscriber's DN which will be used to deposit the message in the proper mailbox.

Call Termination

NIUF 90-301 and NIUF 90-302 describe the necessary terminating procedures required to release the connection between the VMS and the Switch.

Call Termination Outside VMS/Switch

NIUF 90-301 and NIUF 90-302 describe the necessary terminating procedures required to release the connection between the calling party and the Switch.

VMS Interoperability

The VMS Interoperability requirements are defined in T1.xxx and NIUF.xxx. VMS Interoperability is critical in defining how VMSs communicate with one another.

7.5.1.4.2.4 Conformance Tests

All of the conformance tests to support this profile have not been written. This data will be supplied at a later date. See section 5 for the status of conformance tests.

7.5.1.4.3 Subscriber Notification

The VMS Subscriber Notification is the second stage in the Message and Answering application process.

7.5.1.4.3.1 Application Process Description

The VMS has the capability to control the message waiting indicator (MWI) provided to the VMS subscriber via the ISDN switch. The MWI informs the VMS subscriber the status of recorded messages in the subscriber's mailbox. For an ISDN subscriber, the MWI may be a lamp, display or audible indication (e.g., interrupted dial-tone). For non-ISDN subscribers, the MWI should be in the form of an audible indication or visual indication supplied by the switch.

The MWI should be able to notify VMS subscribers when they have messages waiting and when there are no messages waiting. The terms activated and deactivated indicate which notification is being provided.

7.5.1.4.3.2 Subscriber Notification Process Alternative Architectures

VMS subscriber notification process is invoked whenever the VMS causes the ISDN network to activate or deactivate the VMS subscriber's message waiting indicator. Typically, the MWI is activated when a message is waiting and deactivated when no messages remain. However, the VMS may activate or deactivate the MWI at other times, such as during an error recovery process or if redundant MWI activation or deactivation messages are sent.

In typical existing implementations, all of the VMS's subscribers are connected to a single ISDN switch or PBX. The Messaging and Answering application physical environment, for subscriber notification when the VMS subscribers and the VMS are connected to a single ISDN switch, is shown in figure 7-108. However, when a number of users in many locations subscribe to a single, centrally located VMS, then multiple ISDN switches are involved. The VMS first notifies the ISDN switch to which it is directly connected to tell the next switch (or the third, etc.) connected to the VMS subscriber to activate the VMS subscriber's MWI. This environment is shown in figure 7-110. The same steps occur in both environments when the VMS notifies the ISDN switch(s) to deactivate the subscriber's MWI. These environments are shown in figures 7-112 and 7-114.

7.5.1.4.3.3 Information Flow Diagrams

The Information Flow Diagrams for VMS subscriber notification are shown in figures 7-109, 7-111, 7-113 and 7-115.

7.5.1.4.3.4 Protocol Requirements and Application Service Element Description

The supplementary service, Message Waiting Indicator Control and Notification, will be the primary requirement specification to implement the following sub-sections. See figures 7-108 through 7-114. Please note that the required T1.622-1992, *Message Waiting Indicator Control and Notification Supplementary Services and Associated Switching and Signalling Specification* (Ref. [24]), and NIUF.xxx will be supplied as they become available. NIUF.xxx implies that the Messaging and Answering Profile team is requesting the Supplementary Services Working Group to create the Message Waiting Indicator Control and Notification document.

Message Waiting Indicator Control Activation (VMS to Switch)

The requirements for MWI Control activation between the VMS and the Switch are in T1.622-1992 (Ref. [24]) and NIUF.XXX.

1.) VMS 1 notifies ISDN switch to activate (D)'s Message Waiting Indicator

2.) ISDN switch activates (D)'s MWI

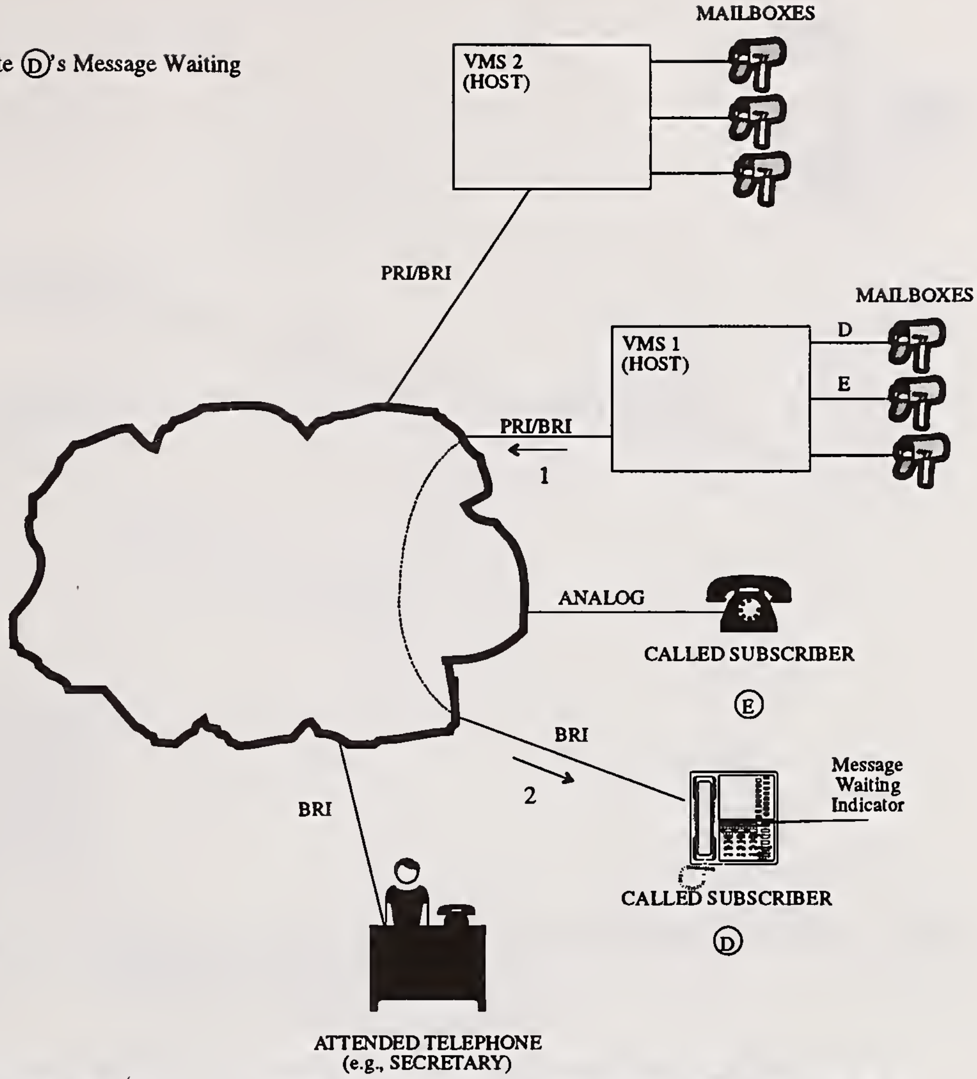


Figure 7-108. Subscriber Notification (MWI Activation)—VMS and Subscriber Off a Single ISDN Switch.

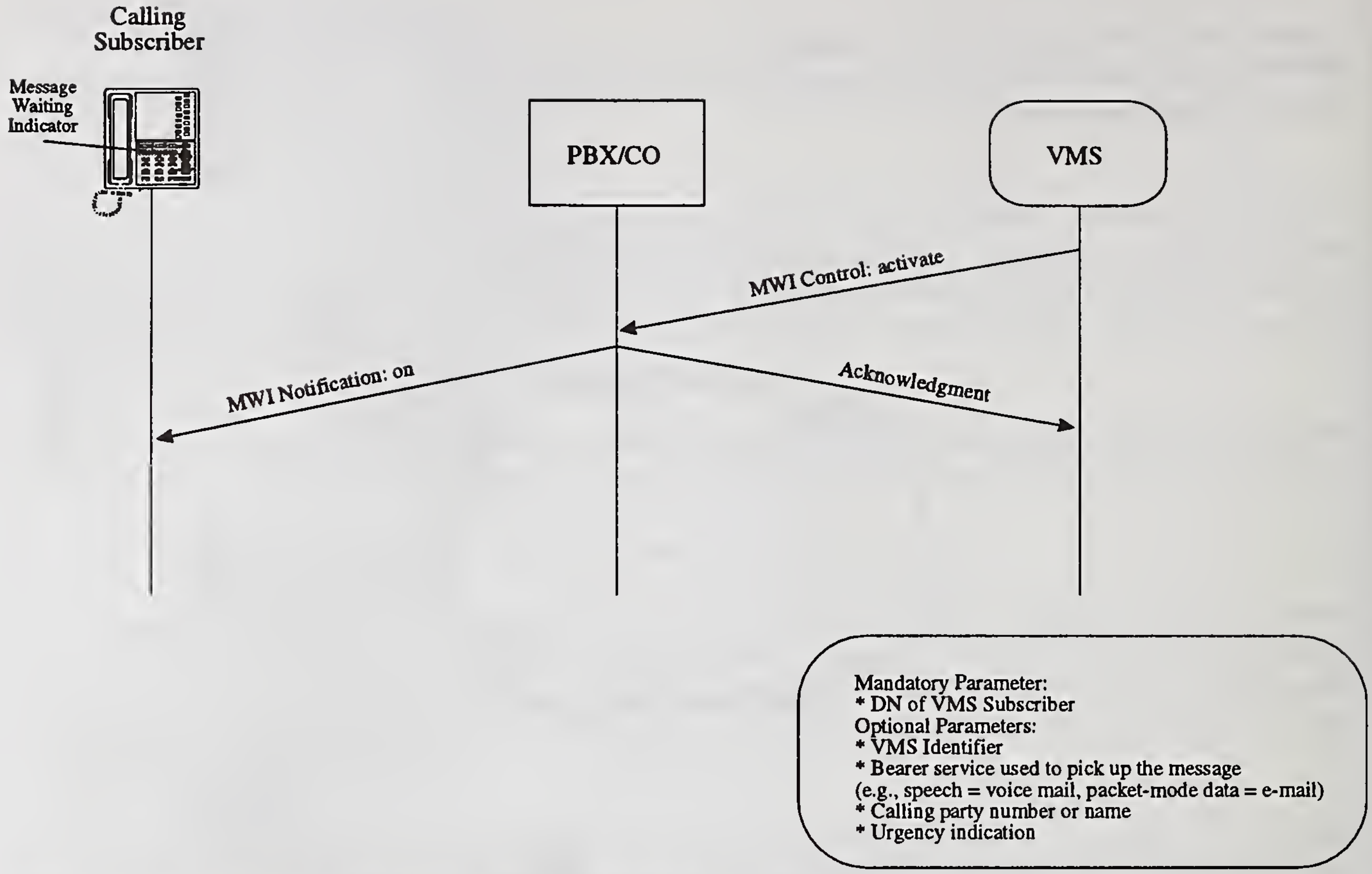


Figure 7-109. Subscriber Notification (MWI Activation—VMS and Subscriber Off a Single ISDN Switch) Information Flow Diagram.

1.) VMS 1 notifies ISDN switch to activate Ⓑ's Message Waiting Indicator

2.) Switch 1 notifies Switch 2 to activate Ⓑ's MWI

3.) Switch 2 activates Ⓑ's MWI

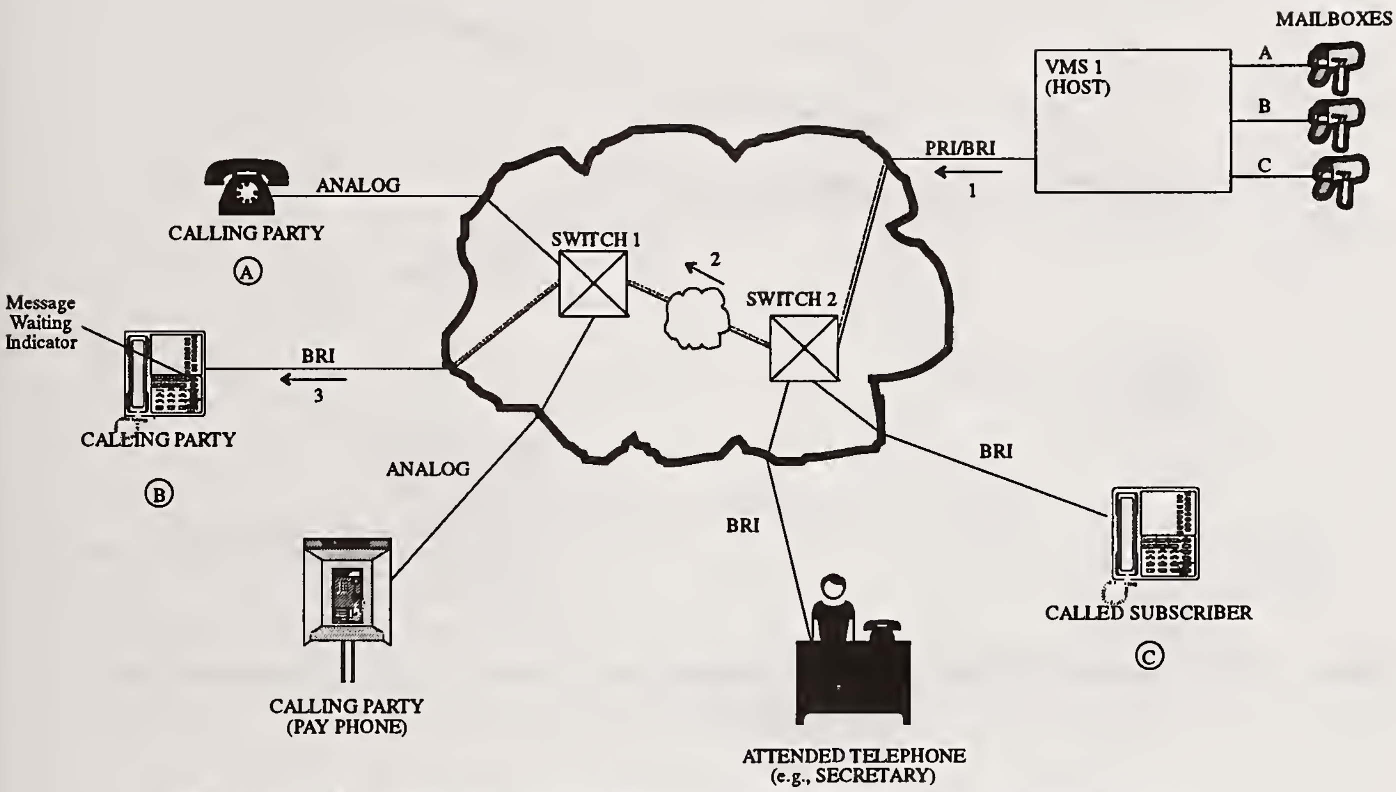


Figure 7-110. Subscriber Notification (MWI Activation) with Centralized VMS.

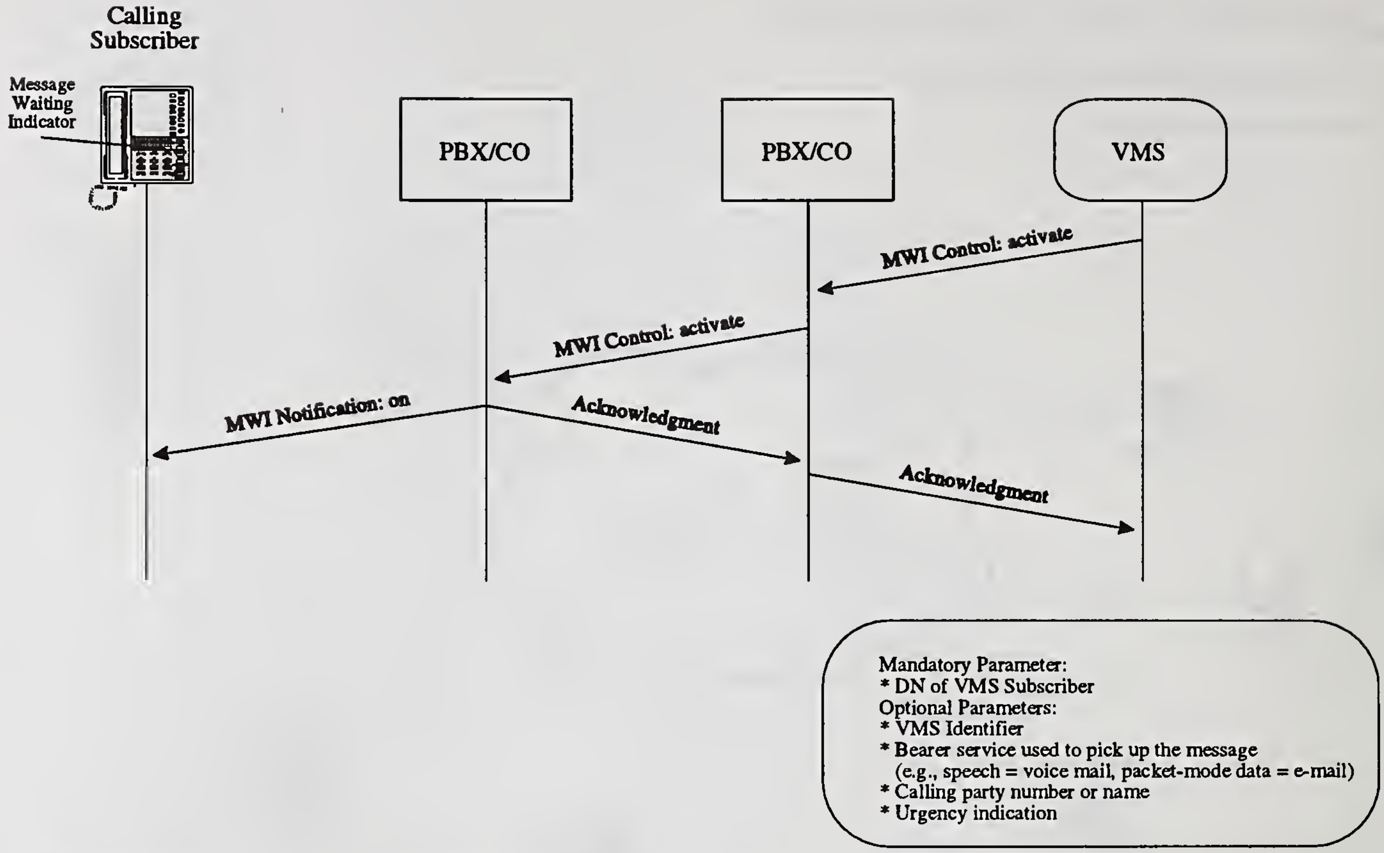


Figure 7-111. Subscriber Notification (MWI Activation) with Centralized VMS—Information Flow Diagram.

1.) VMS 1 notifies ISDN switch to de-activate Ⓓ's Message Waiting Indicator

2.) ISDN switch de-activates Ⓓ's MWI

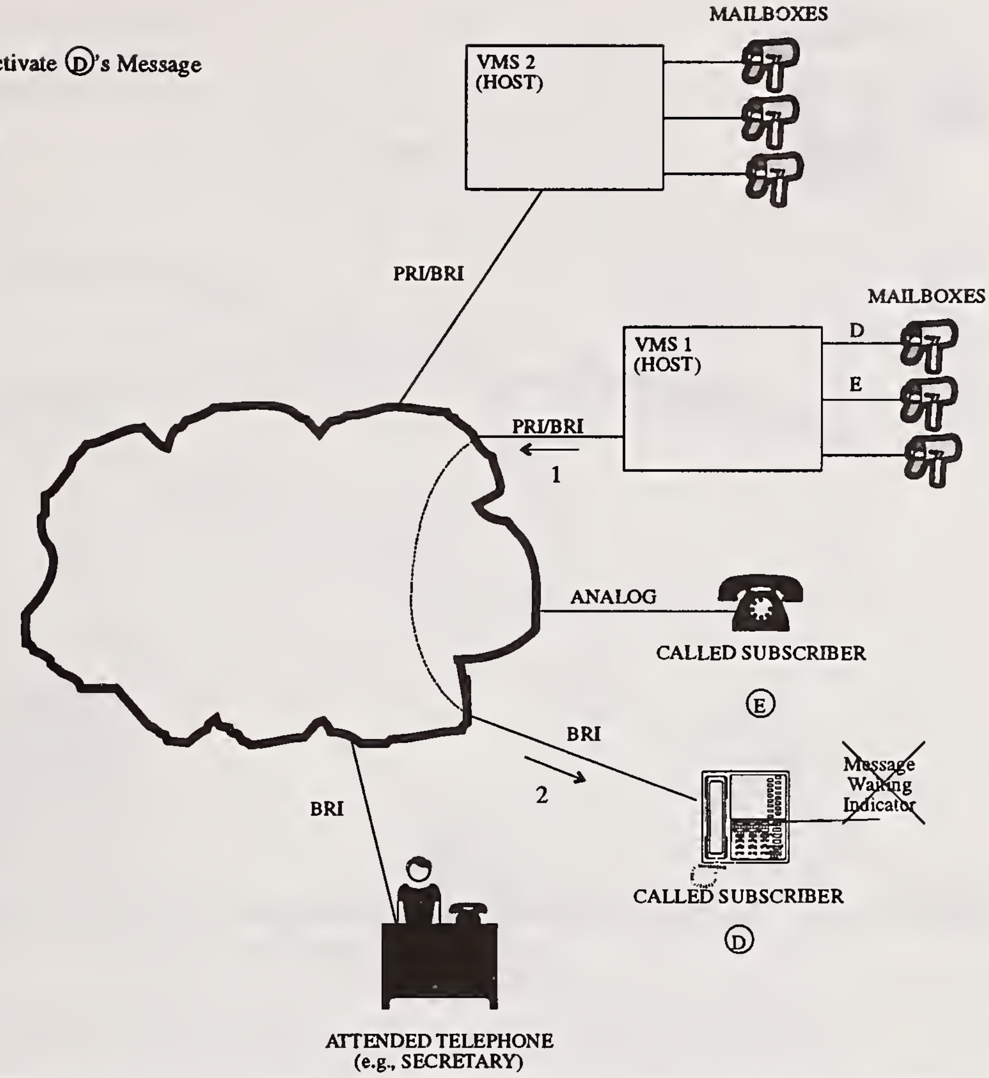


Figure 7-112. Subscriber Notification (MWI Deactivation)—VMS/Subscriber Off a Single ISDN Switch.

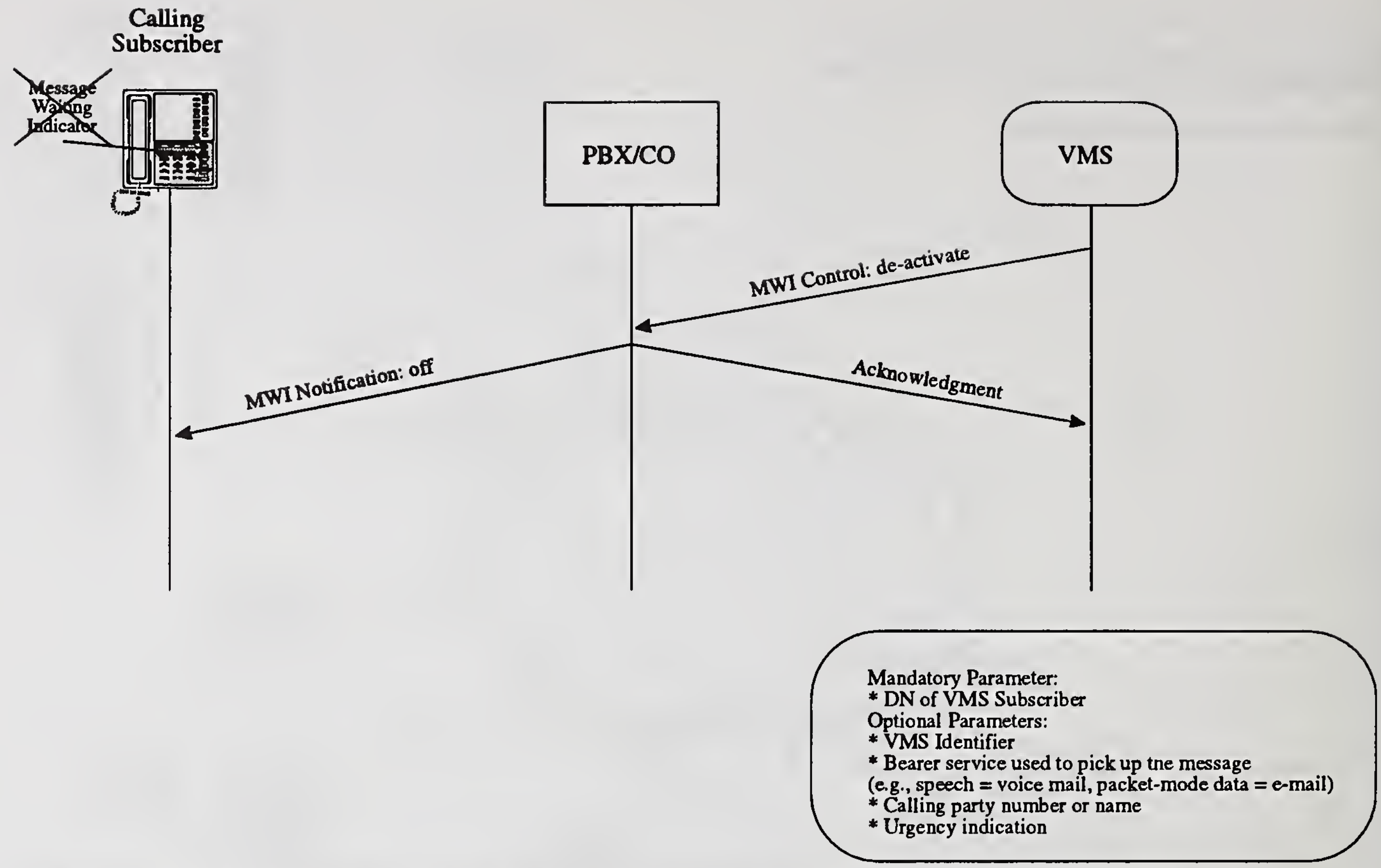


Figure 7-113. Subscriber Notification (MWI Deactivation)—VMS and Subscriber Off a Single ISDN Switch—Information Flow Diagram.

1.) VMS 1 notifies ISDN Switch 1 to de-activate Ⓑ's Message Waiting Indicator

2.) Switch 1 notifies Switch 2 to de-activate Ⓑ's MWI

3.) Switch 2 de-activates Ⓑ's MWI

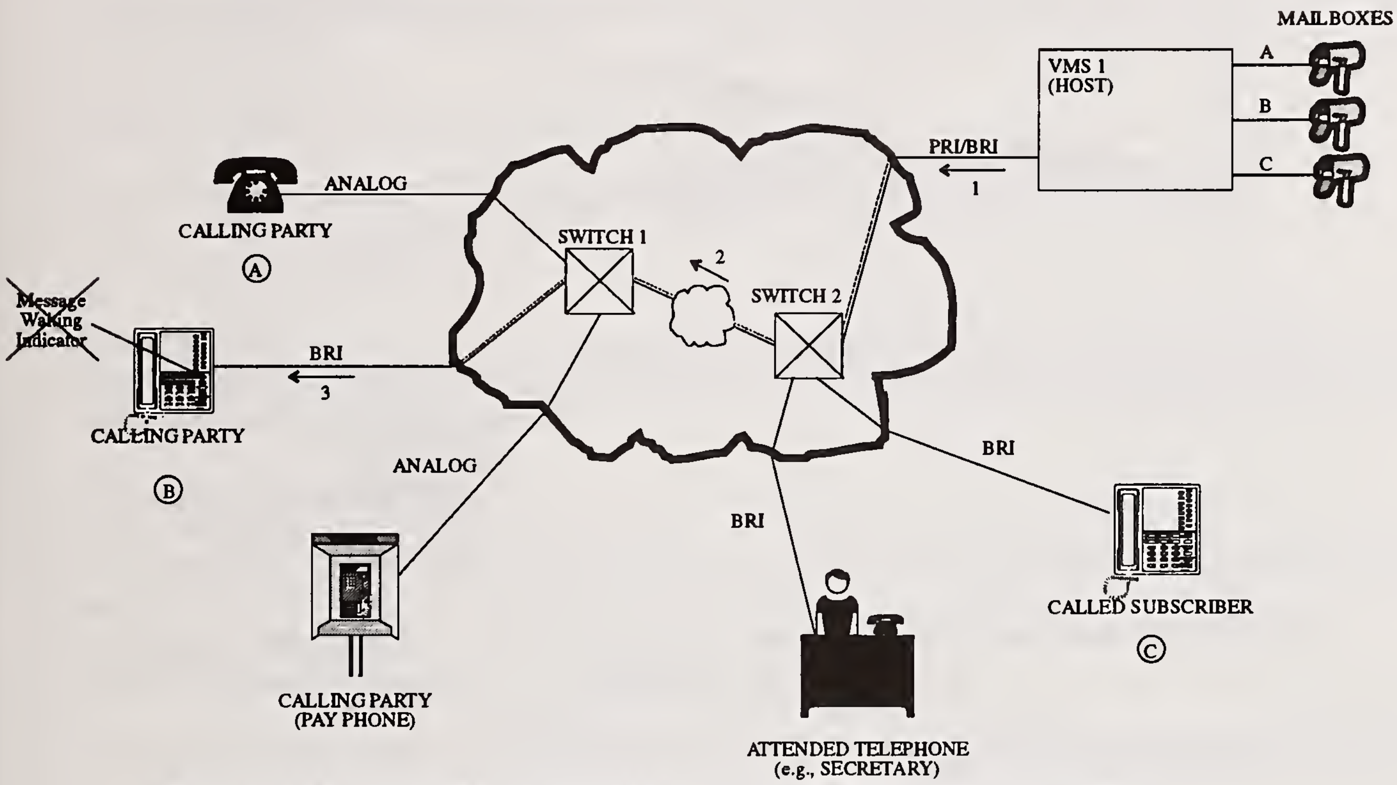


Figure 7-114. Subscriber Notification (MWI Deactivation) With Centralized VMS.

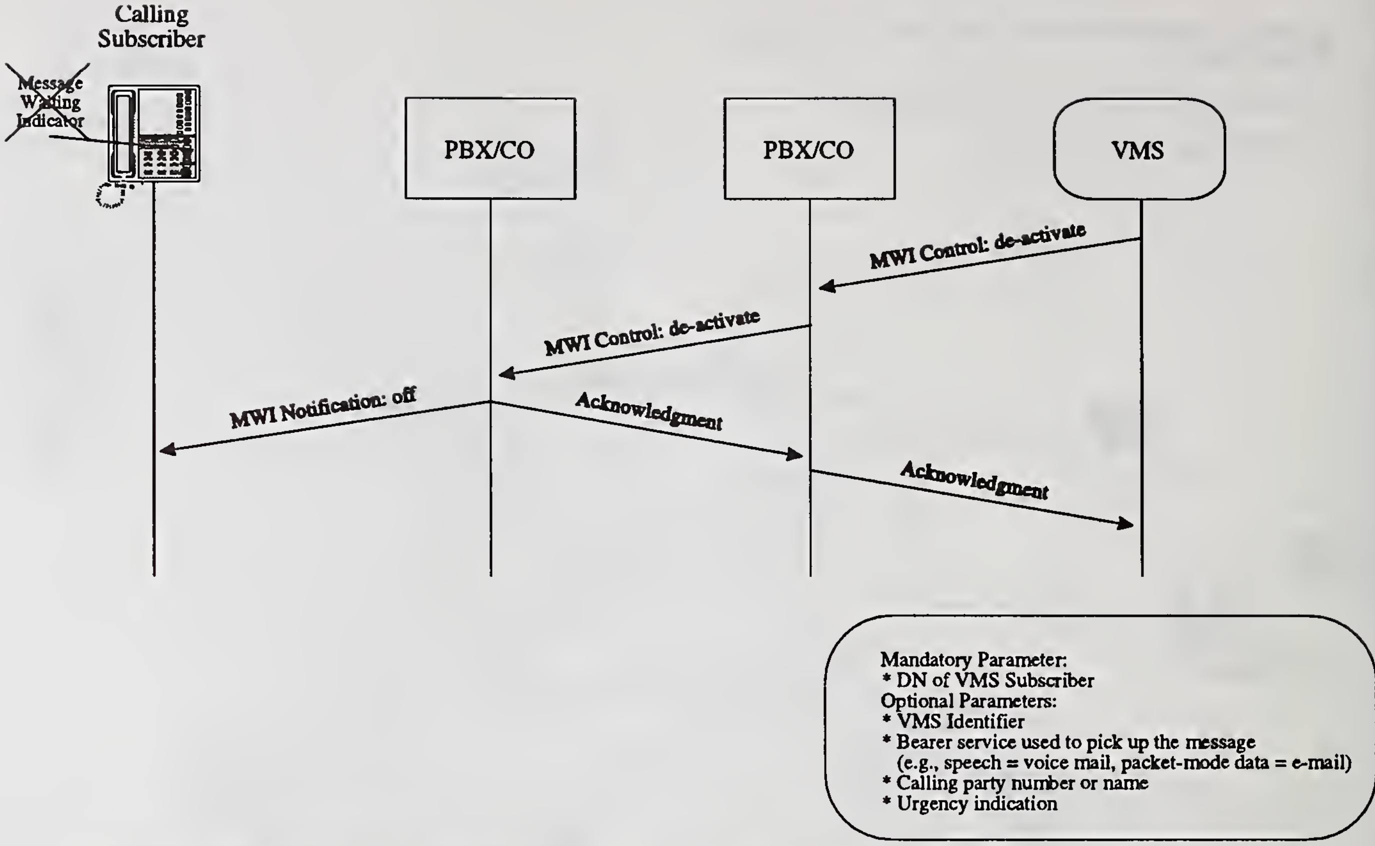


Figure 7-115. Subscriber Notification (MWI Deactivation) With Centralized VMS—Information Flow Diagram.

MWI Activation (Switch to Terminal Equipment)

The requirements for MWI activation are in T1.622-1992 (Ref. [24]) and NIUF.XXX.

MWI Control Deactivation (VMS to Switch)

The requirements for MWI Control deactivation between the VMS and the Switch are in T1.622-1992 (Ref. [24]) and NIUF.XXX.

MWI Deactivation (Switch to Terminal Equipment)

The requirements for MWI deactivation are in T1.622-1992 (Ref. [24]) and NIUF.XXX.

Network Signalling Requirements

The requirements for MWI Network signalling are in T1.622-1992 (Ref. [24]) and NIUF.XXX. These requirements are necessary for controlling the MWI for a centralized VMS. The TCAP messages are sent within the network to control the MWI.

7.5.1.4.3.5 Conformance Tests

The conformance tests to support this profile have not been written. This data will be supplied at a later date.

7.5.1.4.4 Subscriber Retrieval

The VMS Subscriber Retrieval process is the third stage in the Message and Answering application process.

7.5.1.4.4.1 Application Process Description

When the VMS subscribers message waiting indicators show waiting messages, the VMS subscribers access the VMS directly to retrieve and process their voice messages. Once the retrieval stage is completed, the VMS must notify the ISDN switch to deactivate the MWI.

7.5.1.4.4.2 Called Subscriber Retrieval Alternative Architectures

A VMS subscriber may be connected to the VMS by several different service elements, such as Direct Call Set up, Call Forwarding, Call Transfer, etc. The particular service element used to establish connectivity is not critical to the VMS subscriber retrieval stage. It is important that the VMS subscribers be connected to the VMS with an opportunity to retrieve the messages from their mailboxes.

The Message and Answering physical environments for when the VMS subscribers and VMS are connected to the same ISDN switch are shown in figure 7-116.

7.5.1.4.4.3 Information Flow Diagrams

The Information Flow from VMS subscriber access into a VMS is shown in figure 7-117.

1.) Subscriber D calls VMS

2.) D retrieves message(s)

3). Call terminated

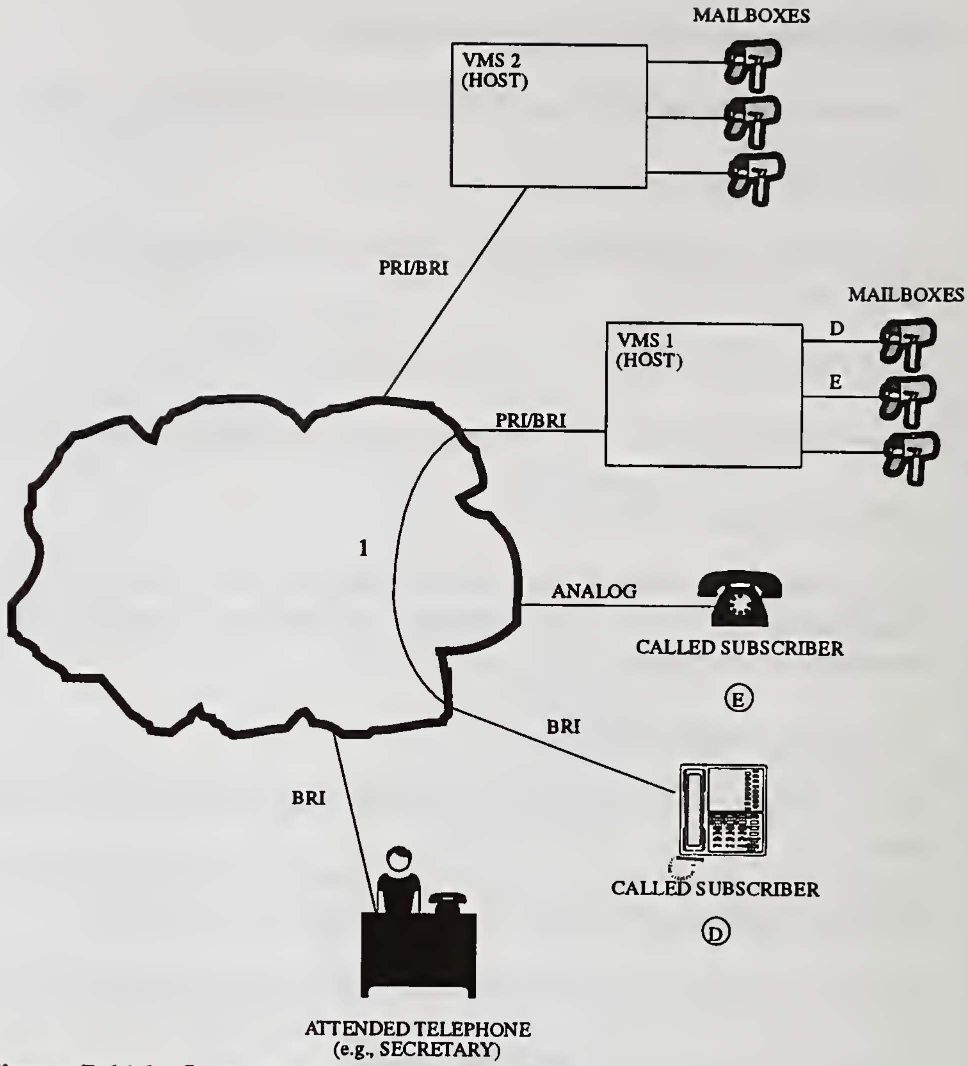
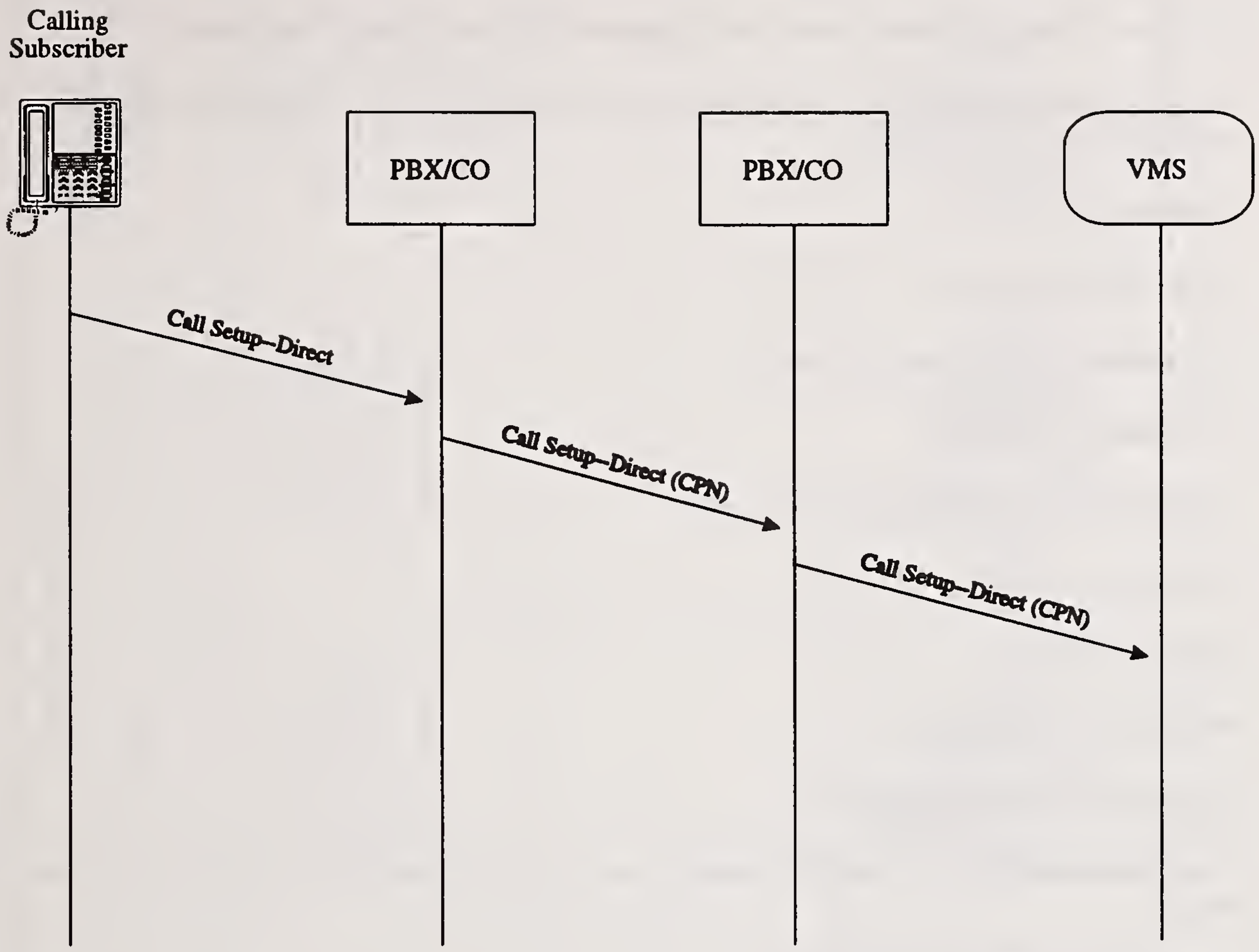


Figure 7-116. Subscriber Message Retrieval.



CPN = Calling Party Number

Figure 7-117. Subscriber Message Retrieval—Information Flow Diagram.

7.5.1.4.4.4 Protocol Requirements and Application Service Element Description

The protocol requirements and application service elements necessary for subscriber retrieval are a subset of those in section 7.5.1.4.2.3.

Call Setup (Direct)

See section 7.5.1.4.2.3.

Call Delivery With Associated Data

See section 7.5.1.4.2.3.

Connectivity to Called Subscriber's Mailbox

See section 7.5.1.4.2.3.

Call Termination

See section 7.5.1.4.2.3.

7.5.1.4.4.5 Conformance Tests

The conformance tests to support this profile have not been written. This data will be supplied at a later date.

7.5.1.4.5 Summary of MA processes

See Table 7-37.

Table 7-37. Voice Messaging and Answering Application Service Elements

PROCESSES / CASES	Subscriber Access		Subscriber Notification		Subscriber Message Retrieval
	Caller	Message Networking	Activation	De-Activation	
Call Answering	• Call Setup • Call Forward with Assoc. Data • Connectivity to Called Subscriber's Mailbox • Call Termination	NA	• MWI Control Activation • MWI Activation • Network Signalling Requirements	• MWI Control Deactivation • MWI Deactivation • Network Signalling Requirements	• Call Setup • Call Delivery with Associated Data • Connectivity to Called Subscriber's Mailbox • Call Termination
Call Answering With Call Transfer	• Call Setup • Call Forward with Assoc. Data • Connectivity to Called Subscriber's Mailbox (• Call Termination outside VMS/Switch)	NA	NA	NA	NA
Direct Access to VoiceMail	• Call Setup (direct) • Call Delivery with Assoc. Data • Connectivity to Called Subscriber's Mailbox • Call Termination	• Call Setup (direct) • Call Delivery with Assoc. Data • Connectivity to Called Subscriber's Mailbox • Call Termination • VMS Interoperability	• MWI Control Activation • MWI Activation • Network Signalling Requirements	• MWI Control Deactivation • MWI Deactivation • Network Signalling Requirements	•Call Setup •Call Delivery with Associated Data • Call Termination

7.6 Future Bandwidth Negotiation

Editor's Note: This section is reserved for future agreements on Bandwidth Negotiation.

7.7 Network Management/ISDN Administration

Editor's Note: This section is reserved for future agreements on Network Management/ISDN Administration.

7.7.1 ISDN Station Event Recording (ISER)

7.7.1.1 Basic Description

ISDN (and non-ISDN) users require detailed records of station events in a universal format independent of the switching element.

The expected benefits of this application are:

- Standard format for ISDN station event data
- Standard protocol for data transfer
- User-selectable interface
- Flexibility with regard to the data transferred
- Improved ability to process the data

This application (Ref. [51]) involves standardizing the information content and format of information provided to the user as well as providing a standard interface from which the user obtains the data. This interface is defined as "A" in figure 7-118.

The user has the ability to retrieve the data in a uniform manner. The retrieval method preserves the integrity and completeness of the data.

This application involves primarily the accounting management functional area of OSI network management.

The intention of this application is to be able to provide data for an event from its originating station to its terminating station including all intermediate switching nodes as required by the ISER user.

7.7.1.2 Functional Requirements

The ISDN Station Event Recording Module (ISERM) is a managed object for formatting, recording, and retrieving user data from the ISDN environment. The ISERM includes the following attributes:

- Standard Interface Protocol
- ISER Configuration Profile
- Standard ISER Data Delivery Format
    - Minimum Data Set for Event Recorded Information

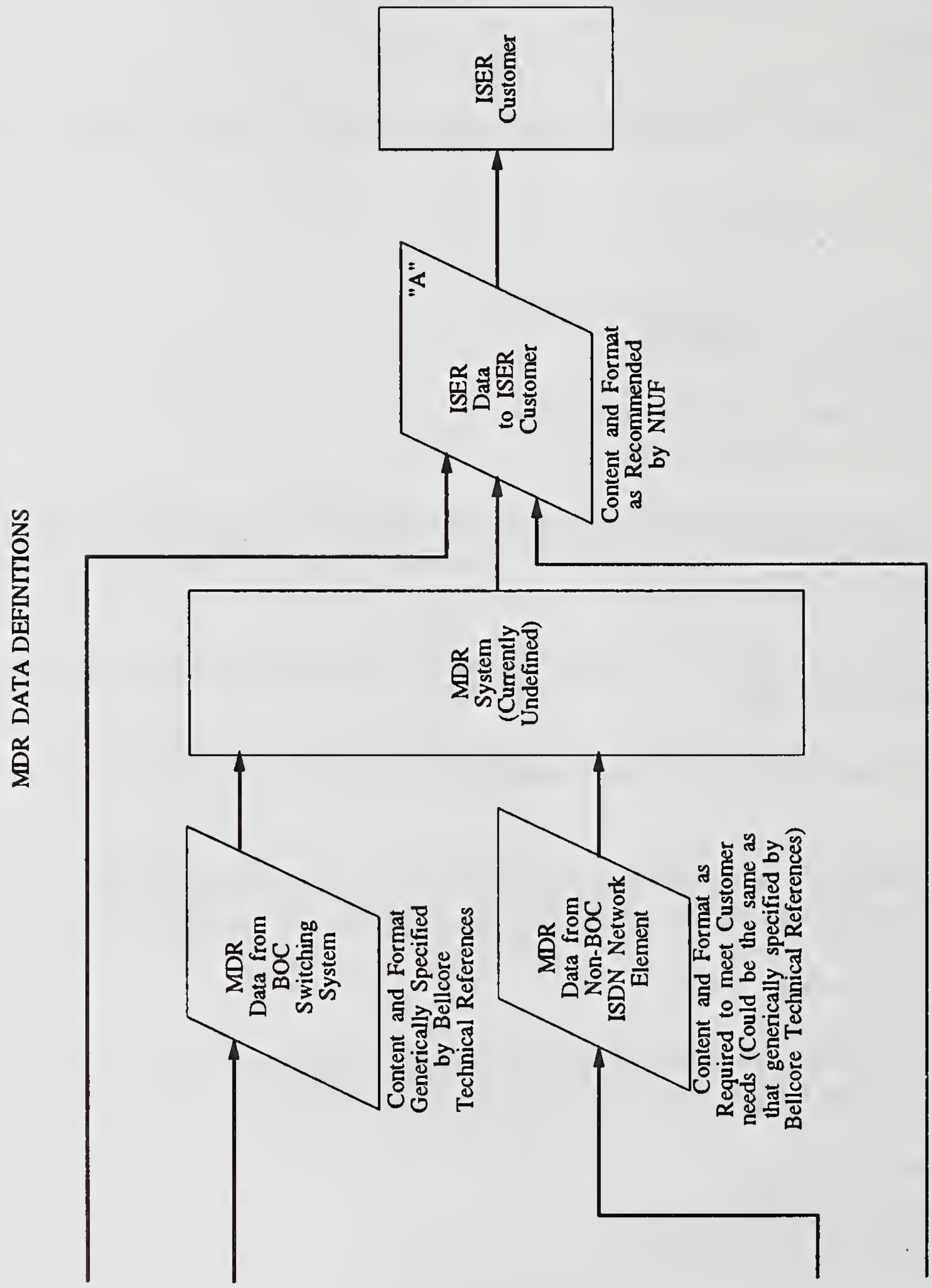


Figure 7-118. ISER Functional Schematic.

7.7.1.2.1 Standard Interface Protocol

A standard interface is provided to allow the user device (OSI agent) to establish a connection to the ISDN environment for ISER activities. Any such interface has the capability to establish a 2-way communications link (full duplex) between the user device and the ISDN environment using managed objects.

This connection uses a standard protocol which facilitates the orderly and efficient transfer of ISER data from the ISDN environment to the user's device(s). This protocol provides the following minimum capabilities:

- The ability to request the ISERM to perform the transfer of ISER data from the ISDN environment to user's devices.

- The ability to access an ISER Standard Configuration profile for the purpose of reviewing and changing its current information.

- The ability to establish and maintain a secure user environment for the purpose of restricting control and access to the ISERM.

In order to support this application, the protocol suites shown in figures 7-119 and 7-120 are to be considered as suggested implementation alternatives.

ISER implementation should not preclude future TP (Distributed Transaction Processing) protocol support for this application. See figures 7-121 and 7-122 for suggested implementation alternatives once TP has been made to accepted standard.

7.7.1.2.2 ISER Configuration Profile

A configuration profile will exist in the ISDN environment for each user for the purpose of controlling and downloading ISER data to the user's external device(s). This configuration profile is the minimum subset of the management data base for the managed object, ISERM, and its processes required to interact with the external device(s).

At a minimum, this profile allows:

7.7.1.2.2.1 Event record selection based on:

- Event classes
  - Station-to-station
  - Message network access
  - Private facility access

- Event types
  - All attempts
  - All completions
  - Answered only

- Event category
  - Originating
  - Terminating

Application	ISO 8571 $\boxed{\text{FTAM}}$ $\boxed{\text{ACSE}}$
Presentation	ISO 8822-25 Kernel
Session	ISO 8326, 8327 Kernel
Transport	ISO 8602, 8072, 8073
Network	X.25 PLP
Data Link	LAPB
Physical	V.35/RS232-C/RS-449

Figure 7-119. FTAM NON-ISDN Protocol Usage for Universal ISER Application.

Application	ISO 8571 $\boxed{\text{FTAM}}$ $\boxed{\text{ACSE}}$
Presentation	ISO 8822-25 Kernel
Session	ISO 8326, 8327 Kernel
Transport	ISO 8602, 8072, 8073
Network	T1.607, T1.608, T1.610/ NIU 301, NIU 302, NIU 320
Data Link	T1.602/NIU 210
Physical	T1.601, T1.605/NIU 101, NIU 105

Figure 7-120. FTAM ISDN Protocol Usage for Universal ISER Application.

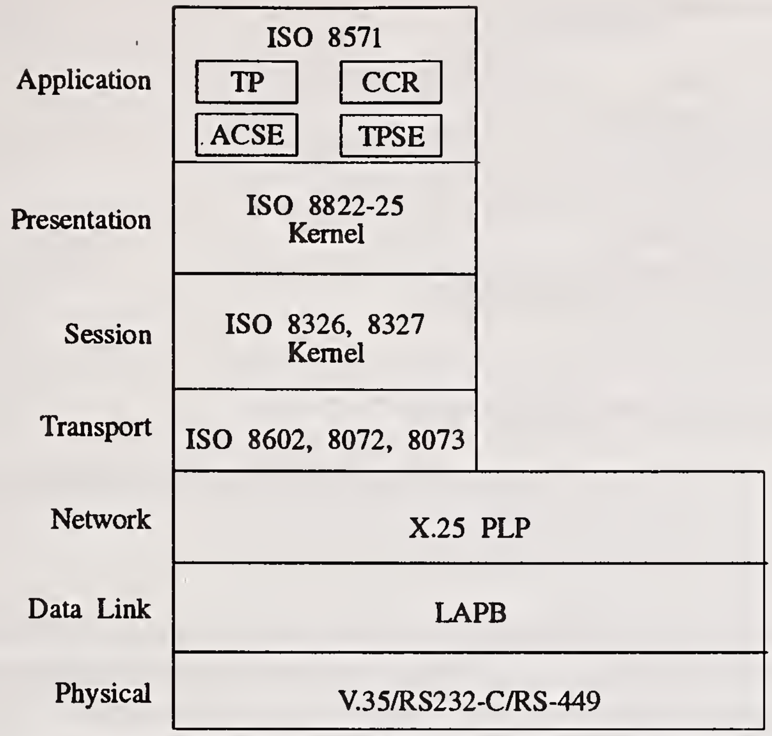


Figure 7-121. TP Non-ISDN Protocol Usage for Universal ISER Application.

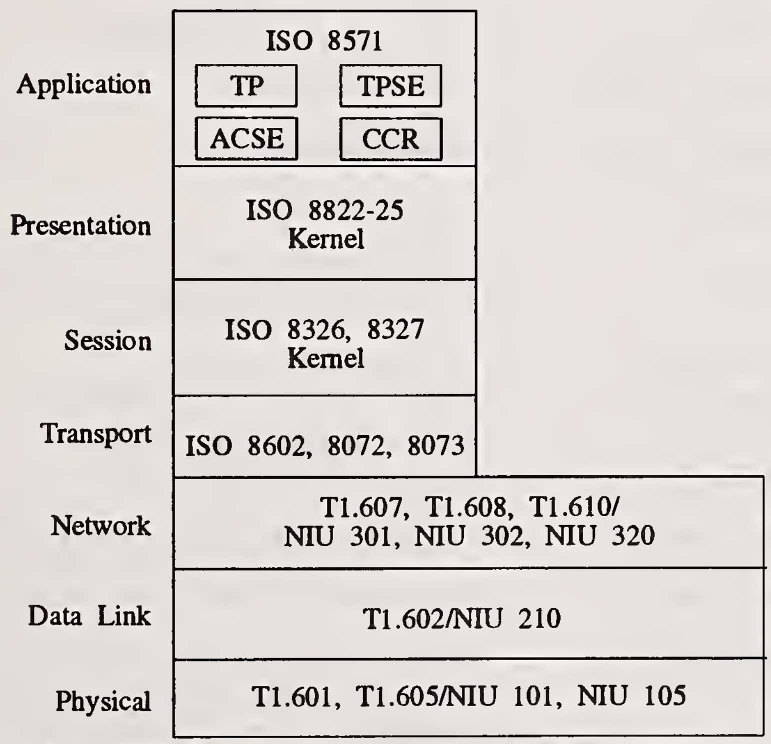


Figure 7-122. TP ISDN Protocol Usage for Universal ISER Application.

7.7.1.2.2.2 Access control based on:

- Set of actions
  - Interface protocol
  - Interface speed

- Set of constraints
  - Authorized users
  - Numbers of simultaneous users
  - Restricted actions

7.7.1.2.2.3 User identification based on:

- Unique identification assigned to each ISER user (User Identifier in ISER record)

7.7.1.2.3 Standard ISER Data Delivery Format

A standard delivery format is established that allows the user to receive ISER data in a form that is consistent in format and content. An implementation agreement should be established for the specific contents of each data segment and the grouping of those segments into standard ISER records.

The following is the required minimum set of event data that should be included, as applicable, for an event.

Item	Description
Network Element Identifier	Switch Identification
User Identifier	User Identification
Group Identifier	Customer Identifier
Record Type	Identifies the Event Record Content and Format, e.g., Originating, Terminating, etc.
Service Identification Event Type Event Category Event Class	Type of Service Provided: Circuit-Switched Voice (CSV), Circuit-Switched Data (CSD), Packet-Switched Data (PSD)
Originating Number	Telephone Number plus Routing Digits (DNIC, etc.)
Route Information	ARS (Automatic Route Selection) Pattern Group
Originating Type	Station, Attendant, Trunk (Virtual and Physical), Offnet Line, Offnet Trunk, Foreign Exchange, other Onnet/Offnet, Shared Directory Number
Originating Trunk Group/Member	Private Trunk Group and Member Number
Call Complete Code	Answered, Unanswered, Busy, Abandoned, Attendant Extended
Facility Restriction Level	Privilege Class Level
Terminating Number	Telephone Number (DNIC, etc.)

Item	Description
SPID	Station Profile Identification
Terminating Type	Station, Attendant, Trunk, (Virtual and Physical), Offnet Line, Offnet Trunk, Foreign Exchange, other Onnet/Offnet, Shared Directory Number
Terminating Trunk Group/Member	Private Trunk Group and Member Number
Event Start Time (Time of Day)	Julian Date, Hours, Minutes, Seconds, and Tenths Answer Time if Answered, End of Dial Time if Unanswered
Call Duration	Usage Time in Seconds and Tenths
Digits Dialed	Digits actually Dialed by User
Digits Outpulsed	Digits actually Transmitted over the Network
Authorization Code	Used to Define Privilege Level
Account Code	Used to assign Charges to a particular Account
Volume of Packet Data Both In/Out	Number of octets Transferred
Network User Identification (NUI)	Identify Users for Billing Purposes
Billing Number	To cause Charging and Acceptance for Packet Calls, if Subscribed

7.8 Security

7.8.1 Secure Voice Mail

Communications between various users have begun to require increasing amounts of security services such as authentication, access control, confidentiality, integrity, non-repudiation, denial of service, and notarization. With the advent of Centralized Voice Messaging application profiles, users have determined that there is a need for these services to be applied to provide secure voicemail capability using ISDN technology with the centralized secure voicemail server.

Government secure voice mail communications require such mechanisms as encrypted channels, protected network routes, and other security features. Without this capability, secure voice communications involving classified operations must be conducted by direct conversations between participants using terminals which provide confidentiality, integrity, and other security services. Often, participants must be recalled to secure facilities to receive secure telecommunications. At other times, secure meetings must be convened to exchange information among several participants. Arranging meetings often involves travel cost and additional time expenditures that introduces inefficiencies into the process and so adversely affect productivity and effectiveness.

When comparing a Centralized Secure Voice Messaging System (CSVMS) with separate smaller systems, a CSVMS will save circuit costs, improve functionality, and lower initial purchase costs.

7.8.1.1 Scope

This profile describes the implementation agreement of the NIUF for a standard approach to providing secure ISDN voicemail using a CSVMS. Applying this approach will ensure a minimum level of interoperability between different vendor implementations for a secure voicemail system.

Nothing in this profile shall be construed as to require functionality inherently incompatible with the requirements set forth in the series of application profiles developed by the NIUF Messaging and Answering Expert Group. Those profiles, rather, shall form the functional basis for operation of Centralized Voice Messaging Systems. As users require increasing levels of assurance in the stringency of mechanisms used by a CSVMS, it should be recognized that there may be some inherent loss of flexibility in the capability of the CSMVS in exchange for a greater degree of confidence in the strength of a given security service mechanism. An example of this would be restrictions on forwarding aspects of voice messages in exchange for increased confidence in the ability of the system to provide information confidentiality, authentication, non-repudiation, and possibly notarization.

7.8.1.2 Normative References

NIUF 860016.0—Transparent Networking of Voice Messaging (Ref. [44])
NIUF 860018.0—Interface to Voice Message Systems (Ref. [45])
NIUF 810034.0—Centralized Voice Mail (Ref. [46])
NIUF 950023.0—Secure ISDN Terminal (Ref. [50])

ISO STANDARDS:

- ISO/IEC (CCITT X.509 Recommendation) Information Technology—Open Systems Interconnection—The Directory—Part 8: Authentication Framework.

- ISO 8649/50: 1988/DAD 1 Service Definition for the Association Control Service Element, Addendum 1: Peer-Entity Authentication During Association Establishment.

- ISO 7498-2 (Ref. [57]).

- ISO Layer Standards:

  - Layer 1: I.430, I.431, I.460-463, ISO 8877
  - Layer 2: I.462
  - Layer 3: I.462, T.70
  - Layer 4: ISO 8073 Connection Oriented
  - Layer 5: Need Security Profile
  - Layer 6: Need Security Profile
  - Layer 7: Need Security Profile

7.8.1.3 Definitions

7.8.1.3.1 ISDN Security Services

7.8.1.3.1.1 General

The common ISDN security services of Authentication, Access Control, Non-Repudiation, Integrity, and Confidentiality are defined in the base standard ISO 7498-2 (Ref. [57]).

7.8.1.3.1.2 Assurance

The ISDN Security Service of Assurance is defined as a technique to use in making sure an ISDN event has taken place in an intended manner.

7.8.1.3.1.3 Notarization

The ISDN security service of Notarization is defined as a technique to use in providing ISDN transmission type Notary services to protect user environments from the threat of denial of service. By using the security service of Notarization, the need for paper Notary filing is eliminated.

7.8.1.3.2 ISDN Mechanisms

7.8.1.3.2.1 General

The common ISDN security mechanisms of Encipherment, Digital Signature, Access Control, Data Integrity, Authentication Exchange, Traffic Padding, Notarization, and Auditing are defined in the base standard ISO 7498-2 (Ref. [57]).

7.8.1.3.2.2 Calling Line Identification

The security mechanism of Calling Line Identification (CLID) is provided by the ISDN switch in forwarding to the distant end the ISDN number of the User (Calling Party) initiating the transmission. It is a form of Authentication.

7.8.1.3.2.3 CLID Restriction

The security mechanism of CLID Restriction is defined as the process of taking both the CLID authentication event and the user request event to use a secured resource and comparing these two events with the pre-programmed authorizations to use the secured ISDN resource. The CLID Restriction security mechanism is not activated in an implementation until the user requests use of a secured resource. The security mechanism of CLID Restriction is a form of Access Control. A system administrator activates this mechanism by authorizing a user access to ISDN resources after the user's CLID is provided. An example of a related access control mechanism with current telephony is when a system administrator activates restrictions for a telephone to making only local, area only, or non-international calls. A calling card authorization limit can also be considered an example of access control restriction since the limit value would be entered by a system administrator and enforced by matching an authenticated user's number with the credit limit before permitting the call. In this last case, the access control is activated when the user requests to use more resources than he is authorized.

7.8.1.3.2.4 Personal Identification Number

The security mechanism of Personal Identification Number (PIN) is defined as the process of a user providing a unique individual identifier to the ISDN secured resource. The PIN is a form of Authentication. A PIN is provided by the user as an alphanumeric sequence through ISDN to the secured ISDN resource. It can be issued by a user at call setup, e.g., voice detectable digits, or by entering digits using the ISDN key pad.

7.8.1.3.2.5 Time Stamp

The security mechanism of Time Stamp is defined as the process of the ISDN switch providing the time of day to the secured ISDN resource at call setup. Time Stamp is used in Auditing. It is the recognized time of day that an event took place.

7.8.1.3.2.6 Voice Print

The security mechanism of Voice Print is defined as the process of a user verbalizing a defined phrase that can be recognized by the ISDN secured resource. Voice Print can be used as either a form of authentication or, when recorded, a form of Notarization. It is used to verify a user's identification in the same manner as a Digital Signature.

7.8.1.3.3 Security Threats

The ISDN security threats of Masquerading, Information Modification, Denial of Service, Leakage of Information, Repudiation, and Replay are defined in the base standard ISO 7498-2 (Ref. [57]).

7.8.1.4 Functional Requirements

Network services which provide secure voicemail capabilities require network implementation, standardization procedures, secure voicemail storage, and telephone company commitment to security.

7.8.1.4.1 Network Features

The public and private networks should be developed to provide the following network features:

- Encrypted links
- Secure network management—i.e., network integrity
- Protected signalling channels
- End-user route detection and control
- Secure voicemail handling features
  - Key management and distribution
  - Directory services
  - Security labeling

7.8.1.4.2 Security Services

7.8.1.4.2.1 Threats to Secure Voice Mail Environment (SVME) Functions

Table 7-39 defines the security services required to protect against various security threats to the SVME.

Table 7-39. Mapping of Security Threats/Security Services

	SECURITY SERVICES						
THREAT	Author-ization	Acc. Ctrl.	Non-Rep.	Info. Integrity	Info. Confid.	Assur-ance	Notif.
Masquerade	X						
Information Modification		X		X		X	X
Denial of Service		X		X[2]			
Leakage of Information		X	[3]		X	X	[3]
Repudiate			X[1]				X
Replay				X	X		

[1]Non-Repudiation service employs both authentication and integrity security mechanisms to protect against repudiation in peer entity operations. The service uses only authentication mechanisms to protect against repudiation in data origin operations.

[2]Data integrity security service protects against denial of service caused by malicious code being introduced into the system.

[3]Non-Repudiation and Notarization services can be used to protect against the n+1 loss of information, but not the nth loss since this service is not employed until after a loss has occurred.

7.8.1.4.2.2 Mapping of SVME Security Services To Mechanisms

Table 7-40 defines the security mechanisms to use in providing security services to protect against the defined threats.

7.8.1.4.2.3 Mapping of OSI Base Standard Mechanisms to ISDN Mechanisms

Table 7-41 maps the various ISDN mechanisms to the OSI base standard. This table is intended to eliminate confusion on what ISDN mechanisms relate to OSI defined mechanism and their related security services. Table 7-41 maps the ISDN mechanisms to OSI base standard mechanisms defined in ISO 7498-2 (Ref. [57]).

Table 7-40. Mapping SVME Security Services To Security Mechanisms

ISDN SECURITY SERVICES	OSI SECURITY MECHANISMS							
	Encipher	Dig. Sig.	Acc. Ctrl.	Data Intg.	Auth. Ex.	Trff Pad.	Notar-ization	Audit
Authentication	X	X			X			1
Access Control			X		X			1
Non-Repudiation		X		X			X	
Data Integrity	X			X				1
Confidentiality	X					X		1
Assurance			X	X			X	1
Notarization	X	X		X	X		X	1

[1]The security mechanisms of auditing can be used to provide added security to any security service.

Table 7-41. Map of ISDN Security Mechanisms to ISO Security Mechanism

ISDN MECH. NO.	ISDN SECURITY MECHANISM	OSI SECURITY MECHANISM
1.0	COMMUNICATIONS	
1.1	Caller ID by CLID	AUTHENTICATION
1.2	CLID Restriction	ACCESS CONTROL
1.3	PIN = By Voice	AUTHENTICATION
1.4	PIN = By User	AUTHENTICATION
1.5	Digital Signature	DIGITAL SIG.
1.6	Mailbox No. by User	AUTHENTICATION
1.7	B CH Encryption	Encryption
1.8	Data Integrity	Data Integrity
1.9	Traffic Padding	Confidentiality
2.0	CSVMS ACTIVITY:	
2.1	Encrypted Info Str.	Encryption
2.2	Audit Trail	
2.2.1	Time Stamp	Audit
2.2.2	CLID Record	Notarization
2.2.3	Destination No.	Audit
2.2.4	PIN/Password	Audit
2.2.5	Dig. Signature	Notarization
2.2.6	Voice Print Str.	Notarization

7.8.1.4.3 Assumptions

a. There must be at least one ISDN path between all switches which will support the CSVM functions.

b. A Secure Voice Mail System (SVMS) will support voice mail services from subscribers at remote sites as though they were served by the same switch as that to which the CSVMS is connected.

c. Verification of user's authorization to use CSVMS (user is the subscriber whose phone service is being forwarded).

d. CSVMS will support non-secure Voice Mail (VM) as well as secure VM users. The CSVMS function is not DOD government Type I, but will support Type I applications.

e. The user whose call is being forwarded to the centralized SVMS should not incur additional charges because of this forwarding.

f. The ISDN must support call forwarding.

g. Support originating station number.

h. Support destination station number.

i. Reason for forwarding to voice mail server.

j. Provide prompts to the calling subscriber (audible and/or display) according to the display capability of the subscriber.

k. Provide message waiting status to the called subscriber.

l. Transfer of call back to another number at caller's request.

m. Inquiry of message status by ISDN voice/data terminal.

n. Work with both BRI and PRI interfaces.

7.8.1.4.4 Information Flow Diagrams

There are two primary methods of forwarding VM to the CSVMS:

1. The local switch (SWX #1) provides CSVMS services when station A calls station C, whose phone service is forwarded to the CSVMS, and station C places a call to the CSVMS and transfers the call to that new connection.

2. The distant end switch (SWX #2) provides CSVMS services when station C directed calls from station A are sent through the network to switch #2. The second method is most likely to be a corporate private network.

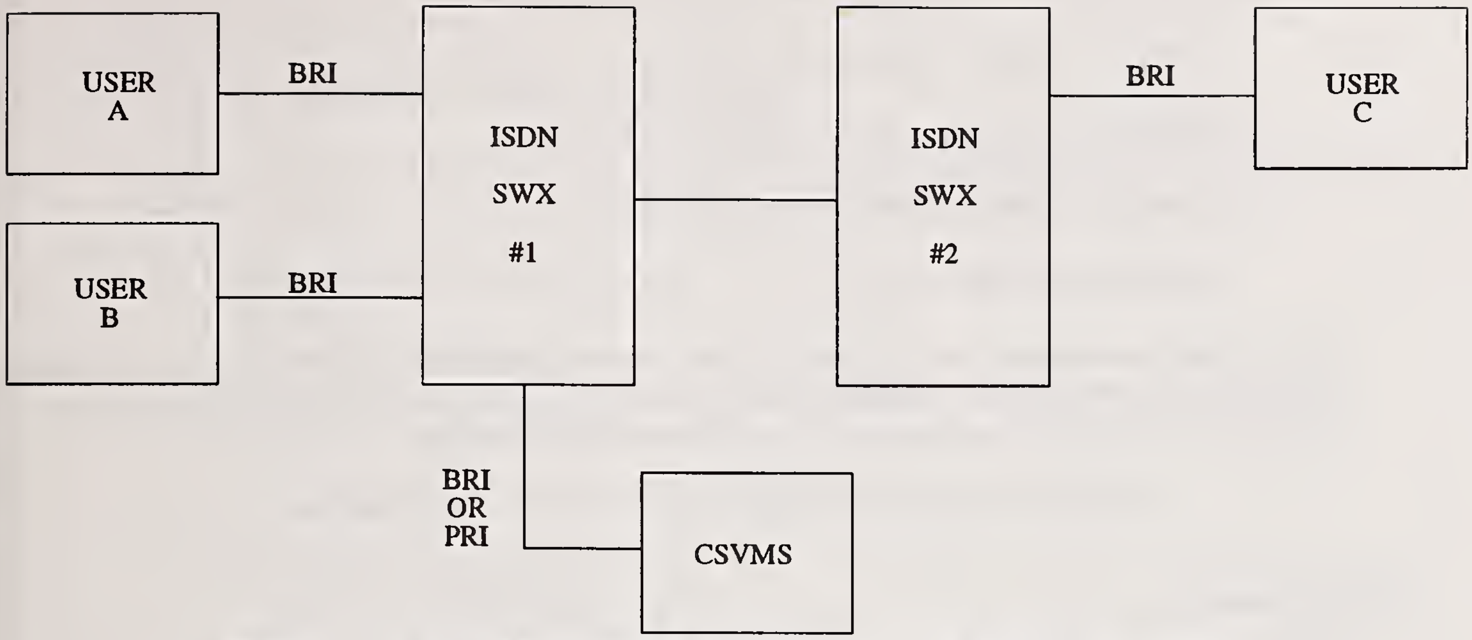


Figure 7-123. Functional Diagram of Secure Voice Mail With Local CSVMS.

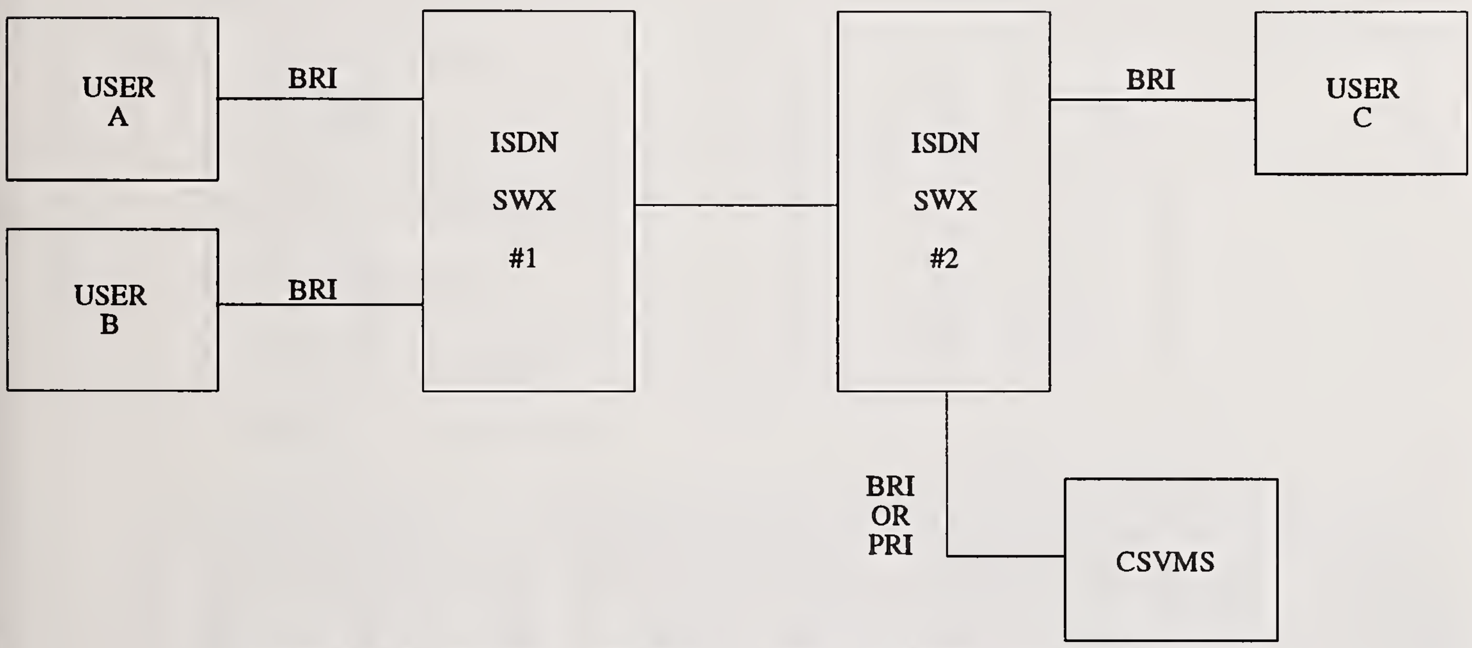


Figure 7-124. Functional Diagram of Secure Voice Mail With End CSVMS.

7.8.1.4.4.1 SVME

The security environment consists of a set of services and mechanisms designed to respond to defined vulnerabilities, threats, and risks established by organizational policy. The purpose of defining a security environment as part of the profile is to provide a level of security for the SVM ISDN application. In implementations, it will lead to development of standard modules by ISDN implementors that are interoperable between implementations.

7.8.1.4.4.2 Functional Groups

The following functional groups are defined for the SVM Environment:

fSVME(0) = User A—ISDN SWX—CSVMS

fSVME(0A) = User A—ISDN SWX—CSVMS—User B

fSVME(1) = User B—ISDN SWX—CSVMS

fSVME(2) = CSVMS—User B

As part of the development process, table 7-42 was constructed to relate the ISDN security mechanisms to the defined ISDN functions. General security classes are defined for low (SL) and high (SH) end security, i.e., SL provides the least security and SH provides the greatest.

Table 7-42. ISDN Security Mechanisms to ISDN SVM Functions

ISDN Mechanism Number	SVME FUNCTIONS							
	fSVME(0)		fSVME(0A)		fSVME(1)		fSVME(2)	
	SL	SH	SL	SH	SL	SH	SL	SH
1.0								
1.1	O	O	O	O	O	O	N	N
1.2	O	M	O	O	O	M	N	N
1.3	N	N	N	M	O	O	N	N
1.4	N	N	N	M	M	M	N	N
1.5	N	O	N	N	N	O	N	N
1.6	M	M	M	M	O	M	M	M
1.7	N	M	N	M	N	M	N	N
1.8	O	M	O	M	O	M	O	O
1.9	N	O	O	M	N	O	N	O
2.0								
2.1	O	M	N	N	O	M	N	N
2.2								
2.2.1	M	M	N	N	N	M	O	M
2.2.2	O	O	O	O	O	O	N	N
2.2.3	M	M	N	N	O	M	M	M
2.2.4	N	N	N	N	N	N	N	N
2.2.5	N	O	N	N	N	N	N	N
2.2.6	N	N	N	N	N	N	N	N

LEGEND:

Security Class—Lowest = SL
Security Class—Highest = SH
N = Not Required; O = Optional; M = Mandatory

7.8.1.4.5 Security Classes

7.8.1.4.5.1 Description of SVME Security Classes

The following Security classes provide initial security in a defined class SO and increasing levels of security for classes S1 and S2. Optional security classes are designated with letter suffixes.

SO = {Authentication and Non-Repudiation}

SOA = SO + {Data Integrity}

SOB = SO + {Access Control}

S1 = SO + {Data Integrity}

S1A = S1 + {Notarization}

S1B = S1 + {Access Control}

S1C = S1 + {Confidentiality}

S2 = S1 + {Access Control}

S2A = S2 + {Notarization}

S2B = S2 + {Confidentiality}

S3 = S2 + {Confidentiality}

S3A = S3 + {Notarization}

S3B = S3 + {Assurance}

In choosing the SO class, it is acknowledged that the null set of security includes the simple case of only weak Authentication as applied to the originator's number that is provided without any security. This is in contrast to the chosen minimum level of security of requiring both Authentication and some kind of Non-Repudiation service. This security class may be as simple as providing Authentication with the originator's number in addition to providing Non-Repudiation by recording some aspect of the event.

Table 7-43 defines the possible uses of security classes to the functional groups.

7.8.1.5 Technology Implications of Application

7.8.1.5.1 Hardware/Software Architecture

The hardware is a network distributed community of subscribers using existing analog, digital, and ISDN telephones/stations. The network can be either Public or Private (using PBXs with ISDN capabilities). The hardware architecture includes a centralized SVMS of sufficient capability to support the network subscriber requirements. Compatibility will be provided for CSVMS in accordance with NIUF 950023.0 (Ref. [50]).

Table 7-43. Mapping of SVM Security Classes to Functional Groups

SECURITY CLASS	FUNCTIONAL GROUP			
	fSVME(0)	fSVME(0A)	fSVME(1)	fSVME(2)
S0	X	X	X	X
S0A	X	X	X	X
S0B	X	X	X	-
S1	X	X	X	X
S1A	X	X	X	X
S1B	X	X	X	X
S1C	X	X	X	X
S2	X	X	X	-
S2A	X	X	X	-
S2B	X	X	X	-
S3	X	X	X	-
S3A	X	X	X	-
S3B	X	X	X	-

7.8.1.5.2 Protocol

The protocol throughout the network must be ISDN and provides the ISDN messaging support necessary to the application. NIUF 90-301 and NIUF 90-302 (Appendices A and B) relate to Q.931 (Ref. [26]) supporting protocols and NIUF 311 (see section 4.1.4.1.2) relates to Q.932 (Ref. [21]) protocols.

7.8.1.5.3 Speed

The handshaking for encryption link-up should take place in less than 250 ms to ensure transparency of secure link-up.

7.8.1.5.4 Security For CSVMS

Secure voice mail storage should be protected at the highest level of classification of the system.

7.8.1.5.5 Performance

The performance requirement is the number of simultaneous users that might be attempting to access the voice mail server which includes the calls currently forwarded to the voice mail server and the subscribers with mail accessing their mailboxes.

7.8.1.5.6 Access Universe

The bounds of the network represent the access universe.

7.8.1.6 Alternatives

The centralized SVMS concept applies equally to public and private (ISDN PBX) networks.

7.8.1.6.1 Circuit

This application applies only to circuit switched calls.

7.8.1.6.2 Packet

Encryption link-up via D channel is acceptable as an alternative.

7.8.1.6.3 Placement of Control or Intelligence

The control and intelligence is distributed throughout the network in the various switches and in the centralized SVMS.

7.8.1.7 Network Management Requirements

Network Management is required to determine on a network basis the access requirements for access to the centralized SVMS.

7.8.1.8 Diagrams of Alternatives

7.8.1.8.1 Secure Voice Mail System

See figure 7-125.

7.8.1.9 Conformance Criteria

To be determined.

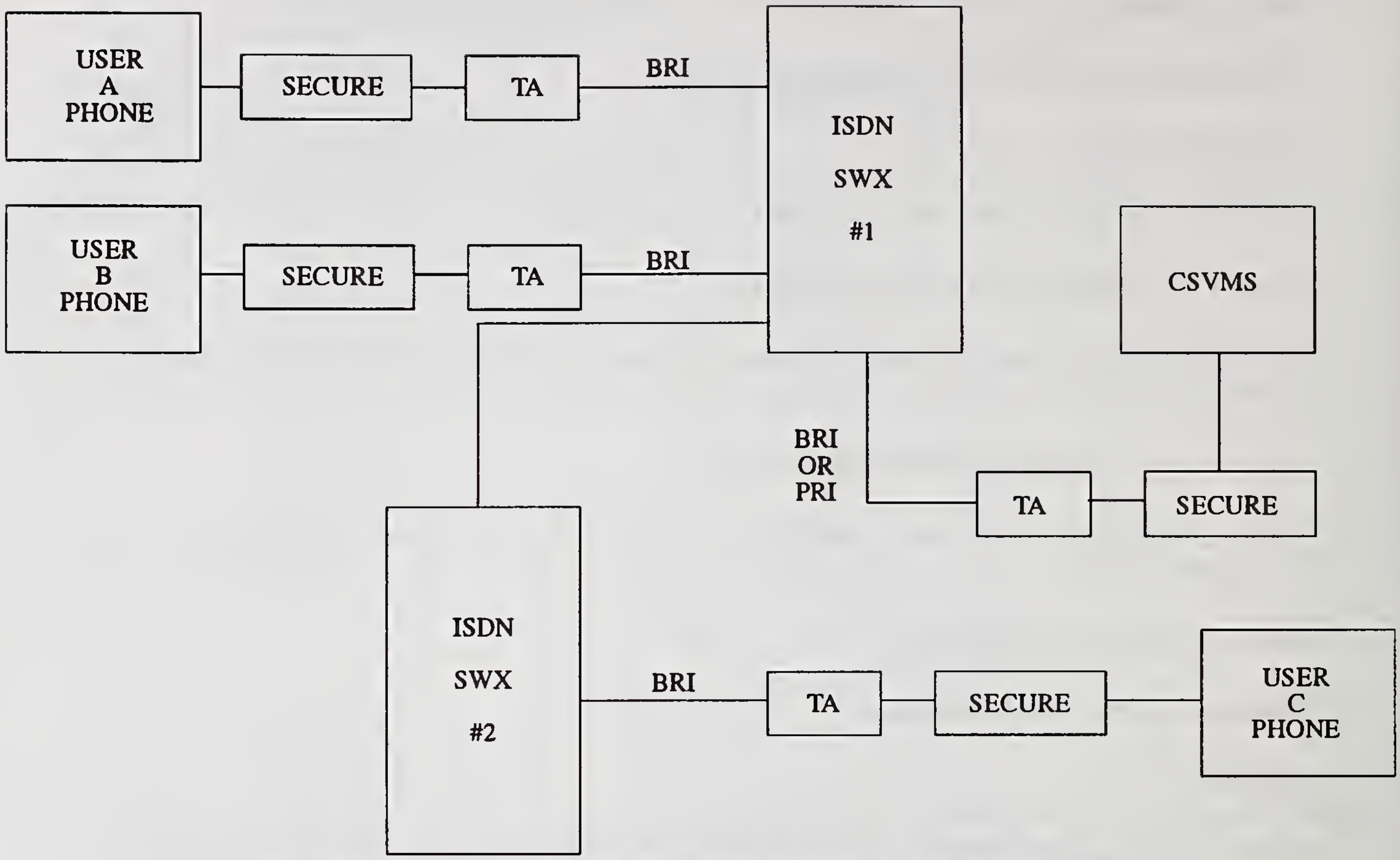


Figure 7-125. Hardware Configuration of Secure Voice Mail System.

8 References

8.1 ANS documents

[1] ANS T1.111-1992, *Telecommunications—Signalling System Number 7 (SS7)—Message Transfer Part (MTP).*

[2] ANS T1.112-1992, *Telecommunications—Signalling System Number 7 (SS7)—Signalling Connection Control Part (SCCP).*

[3] ANS T1.113-1992, *Telecommunications—Signalling System Number 7 (SS7)—ISDN User Part (ISUP).*

[4] ANS T1.114-1992, *Telecommunications—Signalling System Number 7 (SS7)—Transactions Capability Application Part (TCAP).*

[5] ANS T1.115-1990, *Telecommunications—Signalling System Number 7 (SS7)—Monitoring and Measurements.*

[6] ANS T1.116-1990, *Telecommunications—Signalling System Number 7 (SS7)—Operations, Maintenance, Administration and Provisioning (OMAP).*

[7] ANS T1.216-1991, *ISDN Management—Basic Rate Physical Layer.*

[8] ANS T1.217-1991, *ISDN Management—Primary Rate Physical Layer.*

[9] ANS T1.218-1991, *ISDN Management—Data Link and Network Layers.*

[10] ANS T1.403-1989, *Telecommunications—Carrier to Customer Installation—DS1 Metallic Interface.*

[11] ANS T1.408-1990, *Telecommunications—Integrated Services Digital Network (ISDN)—Primary Rate—Customer Installation Metallic Interfaces (Layer 1 Specification).*

[12] ANS T1.601-1992, *Telecommunications—Integrated Services Digital Network (ISDN)—Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT (Layer 1 Specification).*

[13] ANS T1.602-1989, *Telecommunications—Integrated Services Digital Network (ISDN)—Data-Link Layer Signalling Specification for Application at the User-Network Interface.*

[14] ANS T1.603-1990, *Telecommunications—Integrated Services Digital Network (ISDN)—Minimal Set of Bearer Services for the Primary Rate Interface.*

[15] ANS T1.604-1990, *Telecommunications—Integrated Services Digital Network (ISDN)—Minimal Set of Bearer Services for the Basic Rate Interface.*

[16] ANS T1.605-1991, *Telecommunications—Integrated Services Digital Network (ISDN)—Basic Access Interface for S and T Reference Points (Layer 1 Specification).*

[17] ANS T1.607-1990, *Telecommunications—Integrated Services Digital Network (ISDN)—Digital Subscriber Signalling System Number 1 (DSS1)—Layer 3 Signalling Specification for Circuit-Switched Bearer Service.*

[18] ANS T1.608-1991, *Telecommunications—Integrated Services Digital Network (ISDN)—Digital Subscriber Signalling System Number 1 (DSS1)—Signalling Specification for X.25 Packet-Switched Bearer Service.*

[19] ANS T1.609-1990, *Telecommunications—Integrated Services Digital Network (ISDN)—Interworking between the ISDN User-Network Interface Protocol and the Signalling System Number 7 (SS7) ISDN User Part.*

[20] ANS T1.610-1990, *Telecommunications—Integrated Services Digital Network (ISDN)—Digital Subscriber Signalling System Number 1 (DSS1)—Generic Procedures for the Control of ISDN Supplementary Services.*

[21] ANS T1.612-1990, *Telecommunications—Integrated Services Digital Network (ISDN)—Terminal Adaptation Using Statistical Multiplexing.*

[22] T1 Letter Ballot 340, *ISDN Supplementary Service Normal Call Transfer.*

[23] ANS T1.626-1992, *Switch-Computer Applications Interface (SCAI).*

[24] ANS T1.622-1992, *Message Waiting Indicator Control and Notification Supplementary Services and Associated Switching and Signalling Specification.*

8.2 CCITT Documents

[25] CCITT Recommendation Q.921-1988 (also designated CCITT Recommendation I.441-1988), *ISDN User-Network Data Link Layer Specification.*

[26] CCITT Recommendation Q.931-1988 (also designated CCITT Recommendation I.451-1988), *ISDN Primary Rate User-Network Interface—Layer 3 Specification.*

[27] CCITT Recommendation V.120-1988, *Support by an ISDN of Data Terminal Equipment with V-series Type Interfaces with Provision for Statistical Multiplexing.*

[28] CCITT Recommendation X.25-1984, *Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit.*

[29] CCITT Recommendation X.31-1988, *Support of Packet Mode Terminal Equipment by an ISDN.*

[30] CCITT Recommendation I.231-1988, *Circuit-Mode Bearer Service Categories.*

[31] CCITT Recommendation I.232-1988, *Packet-Mode Bearer Services Categories.*

8.3 NIUF Documents[21]

[32] NIUF 91-0012, *Integrated Services Digital Network (ISDN) Conformance Testing, Layer 2 Basic Rate Interface, Link Access Procedure, D-channel (LAPD), User Side*, 1991.

[33] NIUF 400-92 (NIUF/IIW/ICOT/91-53), *Integrated Services Digital Network (ISDN) Conformance Testing Specification: Primary Rate Interface Layer 1 U S/T*, 1992.

[34] NIUF 413-92, *Integrated Services Digital Network (ISDN) Conformance Testing, Layer 3 Network Access Layer, Part 1 Basic Rate Interface Circuit Switched Call Control, User Side, 1992.*

[35] NIUF User Application Requirements Data Form 810004, "Data Conferencing (Point-to-Point)."

[36] NIUF User Application Requirements Data Form 810005, "Database Information to Corporate Security."

[37] NIUF User Application Requirements Data Form 840023, "New Account Customer Inquiry Handling."

[38] NIUF User Application Requirements Data Form 840024, "Customer Service Call Handling (Incoming Call Management)."

[39] NIUF User Application Requirements Data Form 840025, "Automatic Callback for Financial Services."

[40] NIUF User Application Requirements Data Form 830008, "Asynchronous to SNA/SDLC."

[41] NIUF User Application Requirements Data Form 830009, "Synchronous Terminal to Controller."

[42] NIUF User Application Requirements Data Form 960009, "Asynchronous Access to Host Computer."

[43] NIUF User Application Requirements Data Form 830013, "Building Controls."

[44] NIUF User Application Requirements Data Form 860016, "Transparent Networking of Voice Messaging Systems."

[45] NIUF User Application Requirements Data Form 860018, "Interface to Voice Messaging Systems."

[46] NIUF User Application Requirements Data Form 810034, "Interface to Centralized Voice Messaging System."

[47] NIUF User Application Requirements Data Form 050015, "Secure Voice Mail."

[48] NIUF User Application Requirements Data Form 050014, "Secure E-Mail."

---

[21]These documents are available by contacting the NIUF Administrator, NIST, Building 223, Room B364, Gaithersburg, MD 20899.

[49] NIUF User Application Requirements Data Form 050016, "Secure Facsimile Transmission through ISDN."

[50] NIUF User Application Requirements Data Form 950023, "Secure ISDN Terminal."

[51] NIUF User Application Requirements Data Form 960029, "ISDN Station Event Recording (ISER)."

[52] NIUF/SSWG/91-040 (SSWG.303), "Class I/PRI Implementation Agreement."

8.4 Other Documents

[53] NIST Special Publication 500-195, *North American ISDN Users' Forum Agreements on Integrated Services Digital Network*, September 1991.

[54] NIST Special Publication 500-183, *Stable Implementation Agreements for Open Systems Interconnection Protocols*, Version 5, Edition 1, December 1991.

[55] NIST Special Publication, *Application Software Interface Part 1: Overview and Protocols*, September 1991.

[56] ISO 9646, *Information Processing Systems, OSI Conformance Testing Methodology and Framework*. Parts 1-5, 1989.

[57] ISO 7498-2, *Open Systems Interconnection Basic Reference Model.* Part 2, Security Architecture, 1988(E).

APPENDIX A.

NIUF 90-301
Implementation Agreement
of the North American ISDN Users' Forum

Layer 3 Signalling Specification for the
Minimal Set of Circuit-Switched Bearer Services for
the ISDN Basic Rate Interface/Class I.

Baseline Text
American National Standard T1.607-1990:
Integrated Services Digital Network (ISDN) —
Layer 3 Signalling Specification for
Circuit-Switched Bearer Service for
Digital Subscriber Signalling System Number 1 (DSS1).

Base Standards
CCITT Recommendation Q.931 (1988):
ISDN User-Network Interface Layer 3 —
Specification For Basic Call Control.
ANSI T1.607-1990
ANSI T1.604*:
Integrated Services Digital Network (ISDN) —
Minimal Set of Bearer Services for
the Basic Rate Interface.

A.1 Abstract

This Implementation Agreement specifies procedures for establishing, maintaining, and clearing connections at the Integrated Services Digital Network (ISDN) user-network interfaces and are mandatory for the support of the minimal set of circuit-switched bearer services specified by ANSI T1.604-1990* *Integrated Services Digital Network (ISDN)—Minimal Set of Bearer Services for the Basic Rate Interface*, (Ref. [15]). Procedures for circuit-mode digital, circuit-mode speech and circuit-mode voiceband data bearer services are as specified in the baseline text ANS T1.607-1990, *Integrated Services Digital Network (ISDN)—Digital Subscriber Signalling System Number 1 (DSS1)—Layer 3 Signalling Specification for Circuit-Switched Bearer Service*, (Ref. [17]) as further resolved by this agreement. The packet-mode data service is included in this document as a bearer service. Procedures for the packet-mode bearer service will be detailed in another document.

---

*Subject to further discussion.

A.2 Introduction

The original implementation agreement (NIUF 90-301) was reached by marking up the text of ANS T1.607-1990, (Ref. [17]) to reflect the clarifications of text and selection of options. This appendix translates the implementation agreement markup into a listing of these clarifications and selections, (i.e., this appendix lists the differences (the "delta") between the implementation agreement marked up ANS T1.607-1990, and the original text of ANS T1.607-1990).

A.3 NIUF 90-301 Delta List**

The IA has adopted the ANS T1.607-1990*** (Ref. [17]) standard with the following clarifications of the text, and selection of options:

ANS T1.607-1990 SECTION/TABLE NUMBER/NAME	IMPLEMENTATION AGREEMENTS - CLARIFICATION OF TEXT AND SELECTION OF OPTIONS
Section 1 General	Delete "1. General" heading.
Section 1.1 Scope and Purpose	Replace this section with Attachment A of this document.
Section 2.2 States associated with the global reference call	Delete this section including subsections.
Section 3 Message functional definition and content Item (b), Subitem (2)	Delete last sentence from the Note: "Annex D contains a description of the information element usage for symmetric NT2-NT2 interfaces."
Section 3.1 Messages for circuit-mode connection control Table 1 — Messages for circuit-mode connection control	Change "NOTIFY 3.1.7" to "*NOTIFY".
Section 3.1 Messages for circuit-mode connection control Table 1 — Messages for circuit-mode connection control	Add the following footnote below table 1: "* See section 5.8.4 for treatment of this message."

**Note that this Delta List was developed in "good faith" by NIST as a simple equivalent representation of the actual agreements. It has been reviewed and approved by the editors of the Signalling Working Group as per recommendation of the Executive Steering Committee.

***This documents can be purchased from: American National Standards Institute, 11 West 42nd Street, New York, NY 10036.

Section 3.1.1 ALERTING Table 2 — ALERTING message content	Change the "Call Reference/Length" cell from "2-*" to "2-3".
Section 3.1.1 ALERTING Table 2 — ALERTING message content	Change the "Channel Identification/Direction" cell from "both (Note 1)" to "u -> n".
Section 3.1.1 ALERTING Table 2 — ALERTING message content	Change the "Channel Identification/Length" cell from "2-*" to "2-3".
Section 3.1.1 ALERTING Table 2 — ALERTING message content	Change the "Progress Indicator/Direction" cell from "both" to "n -> u".
Section 3.1.1 ALERTING Table 2 — ALERTING message content	Change the "Progress Indicator/Length" cell from "2-4" to "2,4".
Section 3.1.1 ALERTING Table 2 — ALERTING message content	Delete "Display" row.
Section 3.1.1 ALERTING Table 2 — ALERTING message content	Delete Notes 1, 4, 5.
Section 3.1.1 ALERTING Table 2 — ALERTING message content	Delete the last sentence from Note 3.
Section 3.1.1 ALERTING Table 2 — ALERTING message content	Change Note "6 Included if the network optionally provides additional information describing tones." to "6 The network will always provide this IE."
Section 3.1.2 CALL PROCEEDING Table 3 — CALL PROCEEDING message content	Change the "Channel Identification/Length" cell from "2-*" to "2-3".
Section 3.1.2 CALL PROCEEDING Table 3 — CALL PROCEEDING message content	Delete reference to "Note 2" in the "Progress indicator/Type" cell.
Section 3.1.2 CALL PROCEEDING Table 3 — CALL PROCEEDING message content	Change the "Progress Indicator/Length" cell from "2-4" to "2, 4".
Section 3.1.2 CALL PROCEEDING Table 3 — CALL PROCEEDING message content	Delete "Display" row.

Section 3.1.2 CALL PROCEEDING Table 3 — CALL PROCEEDING message content	Delete Notes 2, 3, 4.
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Change the "Call Reference/Length" cell from "2-*" to "2-3".
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Change the "Channel Identification/Direction" cell from "both (Note 1)" to "u -> n (Note 1)".
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Change the "Channel Identification/Length" cell from "2-*" to "3".
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Change the "Progress indicator/Direction" cell from "both" to "n -> u".
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Change the "Progress Indicator/Length" cell from "2-4" to "2, 4".
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Delete the following rows: • "Display"; • "Connected number"; • "Connected subaddress"; • "Low Layer compatibility".
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Change Note 1 from "Included in the network-to-user direction for support of the procedures in Annex D." to "The coding of this IE should be always 'Exclusive B'."
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Delete the following from Note 3: "or in connection with the provision of in-band tones and patterns."
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Delete Notes 4, 5, 7, 8, 9.
Section 3.1.4 CONNECT ACKNOWLEDGE Table 5 — CONNECT ACKNOWLEDGE message content	Change the "Call Reference/Length" cell from "2-*" to "2-3".

Section 3.1.4 CONNECT ACKNOWLEDGE Table 5 — CONNECT ACKNOWLEDGE message content	Delete "Display" row.
Section 3.1.4 CONNECT ACKNOWLEDGE Table 5 — CONNECT ACKNOWLEDGE message content	Delete Notes 1, 2.
Section 3.1.4 CONNECT ACKNOWLEDGE Table 5 — CONNECT ACKNOWLEDGE message content	Change Note 3 from "Included if the network optionally provides additional information describing tones." to "Included if the network is required to turn Alerting off."
Section 3.1.5 DISCONNECT Table 6 — DISCONNECT message content	Change the "Call Reference/Length" cell from "2-*" to "2-3".
Section 3.1.5 DISCONNECT Table 6 — DISCONNECT message content	Change the "Cause/Length" cell from "4-32" to "4-10".
Section 3.1.5 DISCONNECT Table 6 — DISCONNECT message content	Delete the following rows: • "Display"; • "Connected Number"; • "Connected subaddress".
Section 3.1.5 DISCONNECT Table 6 — DISCONNECT message content	Delete Notes 1, 2, 4, 5.
Section 3.1.5 DISCONNECT Table 6 — DISCONNECT message content	Change Note 3 to: "Included if the network must turn tones on or off, or turn ALERTING off."
Section 3.1.6 INFORMATION Table 7 — INFORMATION message content	Change the "Call Reference/Length" cell from "2-*" to "2-3".
Section 3.1.6 INFORMATION Table 7 — INFORMATION message content	Delete "Display" row.
Section 3.1.6 INFORMATION Table 7 — INFORMATION message content	Change the "Keypad Facility/Length" cell from "2-34" to "3-34".
Section 3.1.6 INFORMATION Table 7 — INFORMATION message content	Delete Notes 2, 3.

Section 3.1.6 INFORMATION Table 7 — INFORMATION message content	Add the following to the end of Note 4 ("The Keypad facility information element..."): "When INFO is sent u -> n, this IE must be present."
Section 3.1.6 INFORMATION Table 7 — INFORMATION message content	Change Note 5 from "Included if the network optionally provides additional information describing tones." to "Included if the network is required to turn tones off."
Section 3.1.7 NOTIFY	Delete this section.
Section 3.1.8 PROGRESS Table 9 — PROGRESS message content	Change "Direction" in table header from "both" to "n -> u".
Section 3.1.8 PROGRESS Table 9 — PROGRESS message content	Change the "Direction" cell in the following rows from "both" to "n -> u": • "Protocol discriminator"; • "Call reference"; • "Message type"; • "Cause"; • "Progress Indicator".
Section 3.1.8 PROGRESS Table 9 — PROGRESS message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.8 PROGRESS Table 9 — PROGRESS message content	Change the "Cause/Length" cell from "2-32" to "2,4-10".
Section 3.1.8 PROGRESS Table 9 — PROGRESS message content	Delete "Display" row.
Section 3.1.8 PROGRESS Table 9 — PROGRESS message content	Delete Notes 2, 3.
Section 3.1.8 PROGRESS Table 9 — PROGRESS message content	Change Note 4 from "Included if the network optionally provides additional information describing tones." to "Included when tones or some announcement are provided in-band."
Section 3.1.9 RELEASE Table 10 — RELEASE message content	Change the "Call reference/Length" cell from "2-*" to "2-3".

Section 3.1.9 RELEASE Table 10 — RELEASE message content	Change the "Cause/Length" cell from "2-32" to "2,4-10".
Section 3.1.9 RELEASE Table 10 — RELEASE message content	Delete the following rows: • "Display"; • "Connected number"; • "Connected subaddress".
Section 3.1.9 RELEASE Table 10 — RELEASE message content	Delete Notes 3, 4, 6, 7.
Section 3.1.9 RELEASE Table 10 — RELEASE message content	Change Note 5 from "Included if the network optionally provides additional information describing tones." to "Included if the network must turn tones or Alerting off."
Section 3.1.10 RELEASE COMPLETE Table 11 — RELEASE COMPLETE message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.10 RELEASE COMPLETE Table 11 — RELEASE COMPLETE message content	Change the "Cause/Length" cell from "2-32" to "2, 4-10".
Section 3.1.10 RELEASE COMPLETE Table 11 — RELEASE COMPLETE message content	Delete the following rows: • "Display"; • "Connected number" • "Connected subaddress".
Section 3.1.10 RELEASE COMPLETE Table 11 — RELEASE COMPLETE message content	Delete Notes 3, 4, 6, 7.
Section 3.1.10 RELEASE COMPLETE Table 11 — RELEASE COMPLETE message content	Change Note 5 from "Included if the network optionally provides additional information describing tones." to "Included if the network is required to turn tones on or off."
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Call Reference/Length" cell from "2-*" to "2-3".
Section 3.1.11 SETUP Table 12 — SETUP message content	Delete the following rows: • "Repeat Indicator"; • "Network-Specific Facilities"; • "Display".

Section 3.1.11 SETUP Table 12 — SETUP message content	Delete from the "Bearer Capability/Type" cell the reference to Note 2.
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Bearer Capability/Length" cell from "4-13" to "4-8".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Channel Identification/Length" cell from "2-*" to "2-3".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Progress Indicator/Direction" cell from "both" to "n -> u".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Progress Indicator/Length" cell from "2-4" to "2,4".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Calling party number/Length" cell from "2-*" to "2-19".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Called party address/Length" cell from "2-*" to "2-18".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Transit Network Selection/Length" cell from "2-*" to "2-7".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Higher Layer Compatibility/Length" cell from "2-4" to "2-5".
Section 3.1.11 SETUP Table 12 — SETUP message content	Delete Notes 1, 2, 5, 6, 7.
Section 3.1.11 SETUP Table 12 — SETUP message content	Add to the end of Note 8: "The digits in this IE are 0 to 9, *, and #."
Section 3.1.11 SETUP Table 12 — SETUP message content	Change Note 9 from "Included if the network optionally provides additional information describing tones." to "The network will always provide this IE."
Section 3.1.11 SETUP Table 12 — SETUP message content	Add to the end of Note 13: "The network should transport this IE transparently. This IE is optional on the user side."

Section 3.1.11 SETUP Table 12 — SETUP message content	Add to the end of Note 15: "The network should transport this IE transparently. This IE is optional on the user side. The total length is 2 to 16 octets."
Section 3.1.11 SETUP Table 12 — SETUP message content	Add to the end of Note 16: "The network should transport this IE transparently. This IE is optional on the user side."
Section 3.1.11 SETUP Table 12 — SETUP message content	Add to the end of Note 17: "The network will treat this IE on sending and receiving as described in the User-User supplementary service Implementation Agreement."
Section 3.1.11 SETUP Table 12 — SETUP message content	Delete "and 7kHz audio" from Note 20.
Section 3.1.12 SETUP ACKNOWLEDGE Table 13 — SETUP ACKNOWLEDGE message content	Change the "Call Reference/Length" cell from "2-*" to "2-3".
Section 3.1.12 SETUP ACKNOWLEDGE Table 13 — SETUP ACKNOWLEDGE message content	Change the "Channel Identification/Type" cell from "M" to "M*".
Section 3.1.12 SETUP ACKNOWLEDGE Table 13 — SETUP ACKNOWLEDGE message content	Add the following footnote before Note 1: "* The coding of the channel ID should always be 'Exclusive B'."
Section 3.1.12 SETUP ACKNOWLEDGE Table 13 — SETUP ACKNOWLEDGE message content	Change the "Channel Identification/Length" cell from "3-*" to "3".
Section 3.1.12 SETUP ACKNOWLEDGE Table 13 — SETUP ACKNOWLEDGE message content	Change the "Progress Indicator/Length" cell from "2-4" to "2,4".
Section 3.1.12 SETUP ACKNOWLEDGE Table 13 — SETUP ACKNOWLEDGE message content	Delete "Display" row.
Section 3.1.12 SETUP ACKNOWLEDGE Table 13 — SETUP ACKNOWLEDGE message content	Change Note 1 to: "The only valid value for progress indicator is 8 (refer to section 4.5.21 octet 4). Included in connection with the provision of in-band information/patterns."

Section 3.1.12 SETUP ACKNOWLEDGE Table 13 — SETUP ACKNOWLEDGE message content	Delete Notes 2, 3.
Section 3.1.12 SETUP ACKNOWLEDGE Table 13 — SETUP ACKNOWLEDGE message content	Change Note 4 from "Included if the network optionally provides additional information describing tones (e.g., activate dial tone)." to "Included if the network is required to turn on dial tone."
Section 3.1.13 STATUS	Change the first sentence from "This message is sent by the user or the network in response to a STATUS ENQUIRY message or at any time during a call to report certain error conditions as listed in 5.8." to "This message is sent by the user in response to a STATUS ENQUIRY message sent by the network, or by either the user or the network to report certain error conditions as listed in 5.8."
Section 3.1.13 STATUS Table 14 — STATUS message content	Change the "Call Reference/Length" cell "2-*" to "2-3".
Section 3.1.13 STATUS Table 14 — STATUS message content	Change the "Cause/Length" cell from "4-32" to "4-10".
Section 3.1.13 STATUS Table 14 — STATUS message content	Delete "Display" row.
Section 3.1.13 STATUS Table 14 — STATUS message content	Delete Notes 1, 2.
Section 3.1.14 STATUS ENQUIRY	Change "This message is sent by the user or the network at any time to solicit a STATUS message from the peer layer 3 entity." to "This message is sent by the network during the active state to solicit a STATUS message from the peer layer 3 entity."
Section 3.1.14 STATUS ENQUIRY Table 15 — STATUS ENQUIRY message content	Change "Direction" in the table header from "both" to "n -> u".
Section 3.1.14 STATUS ENQUIRY Table 15 — STATUS ENQUIRY message content	Change the "Direction" cell in the following rows from "both" to "n -> u": • "Protocol discriminator"; • "Call reference"; • "Message type".

Section 3.1.14 STATUS ENQUIRY Table 15 — STATUS ENQUIRY message content	Change "Call Reference/Length" cell from "2-*" to "2-3".
Section 3.1.14 STATUS ENQUIRY Table 15 — STATUS ENQUIRY message content	Delete "Display" row.
Section 3.1.14 STATUS ENQUIRY Table 15 — STATUS ENQUIRY message content	Delete Notes 1, 2.
Section 3.2 Messages used with the global call reference	Delete this section including subsections.
Section 4.2 Protocol Discriminator	Add the following paragraph after the second paragraph. "The only value supported for call control messages is described below, in Figure 2."
Section 4.2 Protocol Discriminator Figure 2 — Protocol Discriminator	Change "ANSI T1.607" to "Q.931".
Section 4.2 Protocol Discriminator Table 19 — Protocol Discriminator	Change "ANSI T1.607" to "Q.931" in the row labeled "0000 1000".
Section 4.3 Call Reference	Change the first sentence of the third paragraph from "... for a basic user-network interface, and a call reference value of two octets for a primary rate interface." to "and a maximum of 2. The network will send one octet call reference value (CRV) unless all 127 available codepoints are occupied."
Section 4.3 Call Reference	Delete the fourth paragraph "As a network option ... one or two octets."
Section 4.3 Call Reference	Add "The Dummy Call Reference and the Global Call Reference are not supported for BRI/Class I circuit-switched calls." after figure 5.
Section 4.3 Call Reference	Delete the last sentence from the eighth paragraph "The call reference ... (e.g., Restart procedures)."
Section 4.3 Call Reference	Delete Note 2 ("The numerical value ... defined in 3.2.").
Section 4.4 Message Type Table 20 — Message types	Add an asterisk (*) to the beginning of the "NOTIFY" row.

Section 4.4 Message Type Table 20 — Message Types	Add as a footnote "* See section 5.8.4 for treatment of this message type."
Section 4.5.1 Coding Rules	Delete the last 3 sentences of the fourth paragraph "Two types of ... octet elements."
Section 4.5.1 Coding Rules Figure 7 — Formats of information elements	Delete Figure 7 (b). Single octet information element format (type 2).
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Delete "Repeat Indicator" row.
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Delete reference to Note 6 in row "Bearer capability".
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Change the "Bearer capability/max length" cell from "13" to "8".
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Change the "Cause/max length" cell from "32" to "10".
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Change the "Cause/max. no. of occurrences" cell from "3" to "2".
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Change the "Channel identification/max length" cell from "(Note 4)" to "3".
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Delete the following rows: • "Network-specific facilities"; • "Notification indicator"; • "Display"; • "Connected number"; • "Connected subaddress".
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Change the "Calling Party Number/max length" cell from "(Note 4)" to "19".
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Change the "Called Party Number/max length" cell "(Note 4)" to "18".

Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Delete reference to Note 2 in the "Transit Network selection" row.
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Change the "Transit Network selection/max length" cell from "(Note 4)" to "7".
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Delete "4" from the "Transit Network Selection/max. no. of occurrences" cell.
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Delete the following rows: • "Restart indicator" and • "Escape for extension".
Section 4.5.1 Coding Rules Table 21 — Information element identifier coding	Delete Notes 3, 4, and 6.
Section 4.5.1 Coding Rules Figure 8 — Information element format using escape for extension	Delete this figure.
Section 4.5.2 Extensions of codesets	Change "T1.608" to "NIUF 89-320" in the first bullet in the fourth paragraph.
Section 4.5.2 Extensions of codesets	Change the ninth paragraph to: "Codeset 7 information elements shall be handled according to the procedures for unrecognized information elements (see 5.8.7.1) by the first exchange."
Section 4.5.2 Extensions of codesets	Delete the tenth paragraph ("Codeset 6 ... bilateral agreements.").
Section 4.5.3 Locking shift procedure New codeset identification coding	Change "T1.608" to "NIUF 89-320" in row "codeset 5".
Section 4.5.4 Non-locking shift procedures	Delete "(a) process the non-locking ... below." from the second paragraph.
Section 4.5.4 Non-locking shift procedures Temporary codeset identification coding	Change "T1.607" to "NIUF 90-301" in row "codeset 0".
Section 4.5.4 Non-locking shift procedures Temporary codeset identification coding	Change "T1.608" to "NIUF 89-320" in row "codeset 5".

Section 4.5.5 Bearer capability	In the second paragraph change "13 octets" to "8 octets".
Section 4.5.5 Bearer capability Figure 11 — Bearer capability information element	Change octet 4, bit 8 from "0/1" to "1".
Section 4.5.5 Bearer capability Figure 11 — Bearer capability information element	Delete octets • 4a*; • 4b*; • 5b* Note 2; • 5b* Note 3; • 5c*; • 5d*.
Section 4.5.5 Bearer capability Figure 11 — Bearer capability information element	Change octet 5a*, bit 8 from "0/1" to "1".
Section 4.5.5 Bearer capability Figure 11 — Bearer capability information element	Delete Notes 1, 2, and 3.
Section 4.5.5 Bearer capability Figure 11 — Bearer capability information element	Delete "or V.120" from the end of Note 4.
Section 4.5.5 Bearer capability	Add the following after Figure 11: "Octets 6 and 7 are included for information only and shall not be used for circuit-switched calls. The coding and application for these octets are included in another document."
Section 4.5.5 Bearer capability Information transfer capability (octet 3) coding	Delete row "10001 7 kHz audio".
Section 4.5.5 Bearer capability Information transfer rate (octets 4 and 4b) coding	Change the title to "Information transfer rate (octet 4)".
Section 4.5.5 Bearer capability Information transfer rate (octet 4) coding	Delete the following rows: • "10011 384 kbit/s"; • "10100 1472 kbit/s (see Note 2)"; • "10101 1536 kbit/s".
Section 4.5.5 Bearer capability Information transfer rate (octet 4) coding	Change Note 1 to: "The bearer capability is bidirectional symmetric at the information transfer rate specified in octet 4."

Section 4.5.5 Bearer capability Information transfer rate (octet 4) coding	Delete Note 2.
Section 4.5.5 Bearer capability	Delete the codings of octets 4a (structure, configuration, establishment) and 4b (symmetry).
Section 4.5.5 Bearer capability User information layer 1 protocol (octet 5) coding	Delete "and optionally octets 5b, 5c, and 5d as defined below." from row "00001".
Section 4.5.5 Bearer capability User information layer 1 protocol (octet 5) coding	Delete "and G.725 7 kHz audio" from row "00101".
Section 4.5.5 Bearer capability User information layer 1 protocol (octet 5) coding	Delete rows "00111" and "01000".
Section 4.5.5 Bearer capability User information layer 1 protocol (octet 5) coding	Delete Note 2.
Section 4.5.5 Bearer capability Synchronous/asynchronous (octet 5a) coding	Delete row "1 asynchronous".
Section 4.5.5 Bearer capability Synchronous/asynchronous (octet 5a) coding	Delete the second and third sentences from the Note.
Section 4.5.5 Bearer capability Negotiation (octet 5a) coding	Delete row "1 In-band negotiation possible".
Section 4.5.5 Bearer capability User rate (octet 5a) coding	Delete all code points except "01111 56 kbit/s CCITT Recommendation V.6."
Section 4.5.5 Bearer capability	Delete all text relating to octet 5b (i.e., sections labeled "Octet 5b for CCITT Recommendation V.100 or X.30 rate adaption" and "Octet 5b for CCITT Recommendation V.120 rate adaption").
Section 4.5.5 Bearer capability	Delete all tables and text referring to octets 5c (number of data bits excluding parity bit, parity information) and 5d (duplex mode, modem type).
Section 4.5.6 Call state Global interface state value (octet 3) coding	Delete this coding.

Section 4.5.7 Called party number	Change the second paragraph to: "The maximum length of this information element is 18 octets."
Section 4.5.7 Called party number Type of number (octet 3) coding	Delete the following rows: • "011 network specific number (see Note 4)" and • "111 reserved for extension".
Section 4.5.7 Called party number	Delete Note 4.
Section 4.5.7 Called party number Numbering plan identification (octet 3) coding	Delete the following rows: • "0011 Data numbering plan (CCITT Recommendation X.121)"; • "0100 Telex numbering plan (CCITT Recommendation F.69)"; • "1111 Reserved for extension".
Section 4.5.7 Called party number	Add Attachment B of this document after the following: "*Number digits (octets 4, etc.)* This field is coded with ASCII characters, according to the formats specified in the appropriate numbering and dialing plan."
Section 4.5.9 Calling party number	Change the second paragraph from: "The maximum length of this information element is network dependent." to "The maximum length of this information element is 19 octets."
Section 4.5.9 Calling party number Type of number (octet 3) coding	Delete the following rows: • "011 network specific number (see Note 4)" and • "111 reserved for extension".
Section 4.5.9 Calling party number Type of number (octet 3) coding	Delete Note 4.
Section 4.5.9 Calling party number Numbering plan identification (octet 3) coding	Delete the following rows: • "0100 Telex numbering plan (CCITT Recommendation F.69)" and • "1111 Reserved for extension".
Section 4.5.9 Calling party number	Add Attachment C of this document after the following: "*Number digits (octets 4, etc.)* This field is coded with ASCII characters, according to the formats specified in the appropriate numbering or dialing plan."

Section 4.5.10 Calling party subaddress	Add a new paragraph at the end of the section: "In the network to user direction (n —> u), the coding and delivery of this IE depends on the definition of the Calling Line ID service."
Section 4.5.11 Cause	Change the second sentence of the first paragraph from "The maximum length of this information element is 32 octets." to "The maximum length of this information element is 10 octets."
Section 4.5.11 Cause Figure 17 — Cause information element	Change octet 3, bit 8 from "0/1" to "1".
Section 4.5.11 Cause Figure 17 — Cause information element	Delete octet 3a*.
Section 4.5.11 Cause Figure 17 — Cause information element	Delete the Note.
Section 4.5.11 Cause Recommendation (octet 3a) coding	Delete this coding and its associated Notes 1 and 2.
Section 4.5.11 Cause	Add the following sentence to the end of the paragraph under "Diagnostics (octet 5)": "If more than one IE is identified in a diagnostic, they should be ordered as IE's normally appear in a message."
Section 4.5.11 Cause Cause table	Change the "diagnostics" cell of the first three code points to "Not used".
Section 4.5.11 Cause Cause table	Change the "Normal call clearing/diagnostics" cell from "(see Note 12)" to "Not used".
Section 4.5.11 Cause Cause table	Add to the "User busy/diagnostics" cell: "(see Note 10)"
Section 4.5.11 Cause Cause table	Change the "call rejected/diagnostics" cell from "(see Note 12, user supplied diagnostic) (see Note 4)" to "Not used".
Section 4.5.11 Cause Cause table	Delete row "Number changed".

Section 4.5.11 Cause Cause table	Add "(see Note 10)" to the "Network out of order/diagnostics" cell.
Section 4.5.11 Cause Cause table	Add "(see Note 10)" to the "Requested circuit or channel not available/diagnostics" cell.
Section 4.5.11 Cause Cause table	Delete row "Quality of service unavailable".
Section 4.5.11 Cause Cause table	Change the "Requested facility not subscribed/ diagnostics" cell from "Facility identification (see Note 1)" to "Not used".
Section 4.5.11 Cause Cause table	Change the "Bearer capability not authorized/ diagnostics" cell from "(see Note 3)" to "Not used".
Section 4.5.11 Cause Cause table	Delete row "Bearer capability not presently available".
Section 4.5.11 Cause Cause table	Delete row "Service or option not available, unspecified".
Section 4.5.11 Cause Cause table	Change the "Bearer capability not implemented/ diagnostics" cell from "(see Note 3)" to "Not used".
Section 4.5.11 Cause Cause table	Delete row "Channel type not implemented".
Section 4.5.11 Cause Cause table	Change the "requested facility no implemented/ diagnostics" cell from "Facility identification (see Note 1)" to "Not used".
Section 4.5.11 Cause Cause table	Delete rows "Only restricted digital information bearer capability is available" and "Service or option not implemented, unspecified".
Section 4.5.11 Cause Cause table	Delete row "Identified channel does not exist".
Section 4.5.11 Cause Cause table	Change the "incompatible destination/diagnostics" cell from "Incompatible parameter (see Note 2)" to "Not used".

Section 4.5.11 Cause Cause table	Delete row "Invalid message, unspecified".
Section 4.5.11 Cause Cause table	Change the "Recovery on timer expiry/diagnostics" cell from "Timer number (see Note 9)" to "Not used".
Section 4.5.11 Cause Cause table	Delete Notes 2, 3, 4, 5, 7, 9, 11, 12.
Section 4.5.11 Cause Figure 18 — Coding of the diagnostic field for causes 57, 58 and 65	Delete Figure 18 and text for octets 5, 5a, and 5b.
Section 4.5.12 Channel identification Figure 19 — Channel identification information element	Delete the octets 3.1, 3.2, and 3.3.
Section 4.5.12 Channel identification Figure 19 — Channel identification information element	Delete Notes 1, 2, 3, 4.
Section 4.5.12 Channel identification Interface identifier present (octet 3) coding	Delete row "1 Interface explicitly ... with octet 3.1."
Section 4.5.12 Channel identification Interface identifier present (octet 3) coding	Delete the Note and the reference to it in row "0 Interface implicitly identified".
Section 4.5.12 Channel identification Interface type (octet 3) coding	Delete row "1 other interface: ... (see Note)".
Section 4.5.12 Channel identification Interface type (octet 3) coding	Delete the Note.
Section 4.5.12 Channel identification Information channel selection (octet 3) coding	Add the following after Note 3: "4 The combination of 'Any Channel' (bits 1,2), and 'Exclusive' (bit 4) is invalid."
Section 4.5.12 Channel identification	Delete the text, codings, and figures relating to octets 3.1, 3.2, and 3.3.

Section 4.5.13 Connected Number	Delete this section.
Section 4.5.14 Connected subaddress	Delete this section.
Section 4.5.15 Display	Delete this section.
Section 4.5.16 High layer compatibility	Change the second paragraph from "The maximum length of this information element is four octets." to "The maximum length of this information element is five octets."
Section 4.5.18 Low layer compatibility	Delete the second paragraph.
Section 4.5.18 Low layer compatibility Negotiation indicator (octet 3a) coding	Delete row "1 Out-band negotiation possible".
Section 4.5.18 Low layer compatibility Negotiation indicator (octet 3a) coding	Delete Note 1.
Section 4.5.18 Low Layer compatibility User information layer 3 protocol (octet 7) coding	Change "ANSI T1.607" to "NIUF 90-301" in row "00010".
Section 4.5.19 Network-specific facilities	Delete this section.
Section 4.5.20 Notification Indicator	Delete this section.
Section 4.5.21 Progress indicator Progress description (octet 4) coding	Delete row "000 0100 4 call has returned to the ISDN."
Section 4.5.21 Progress indicator Progress description (octet 4) coding	Add the following after Note 2: "3 In the SETUP message, n -> u, one of two values may be used: 1 or 3."
Section 4.5.22 Repeat indicator	Delete this section.
Section 4.5.23 Restart indicator	Delete this section.

Section 4.5.24 Signal Figure 32 — Signal information element	Add below the figure: "Note In the n -> u direction, and in the absence of supplementary services, the public network will offer signalling pattern 0 only."
Section 4.5.24 Signal Signal value (octet 3) coding	Delete the following rows: • "intercept tone on"; • "answer tone on"; • "off hook warning tone on"; • "ALERTING on — pattern 5"; • "ALERTING on — pattern 6"; • "ALERTING on — pattern 7".
Section 4.5.25 Transit network selection	Change the second sentence of the first paragraph to: "The transit network selection information element should not be repeated in a message (See Annex C)."
Section 4.5.25 Transit network selection	Change the second paragraph to: "The default maximum length of this information element is 7 octets."
Section 4.5.25 Transit network selection Type of network identification (octet 3) coding	Delete row "011 international network identification".
Section 4.5.25 Transit network selection Network identification plan (octet 3) coding	Delete row "0011 Data network identification code (CCITT Recommendation X.121)".
Section 4.5.26 User-user	Add the following sentence to the end of the Note (after the second paragraph): "This IE is included based on user-user supplementary service description and user application."
Section 4.5.26 User-user Protocol discriminator (octet 3) coding	Change "ANSI T1.607" to "NIUF 90-301" in row "0000 1000".
Section 4.6.1 Operator system access type of access (octet 3) coding	Delete row "10 private/principal".
Section 5 Circuit-switched call control procedures	Delete the fourth paragraph ("As a general principle, ...").
Section 5 Circuit-switched call control procedures	Delete the last sentence of second Note ("Display information ... network to user.").
Section 5.1 Call establishment at the originating interface	Change "ANSI T1.602" to "NIUF 89-210" in the last sentence of the first paragraph.

Section 5.1.3 Overlap sending	Add the following at the end of section 5.1.3: "However, as an option, the network can determine that a potentially complete code has been received following the receipt of address information, and the network could use critical interdigit timing (instead of T302) to determine whether additional digits are following. This timing could be 3-5 seconds. If implemented, when this timer expires, a complete address is assumed and the procedures in Sec. 5.1.5.2 shall be followed. In an INFORMATION message is received and the critical interdigit timing is running, it shall be stopped."
Section 5.1.4 Invalid call information	Delete the following line from the last paragraph: "22 'number changed'."
Section 5.1.4 Invalid call information	Add the following two paragraphs to the end of section 5.1.4: "The network should reject the call request if the SETUP message contains the keypad information element, and any of the following information elements: transit network selection, called party number, or operator system access. In this case, the network should send the calling user equipment a RELEASE COMPLETE message containing cause 28, 'invalid number format (location: public network serving the local user).'." "If the network receives a called party number information element containing more address digits than expected, as determined by the 'type of number and numbering plan identification' field, the network should discard the superfluous digits and route the call. Similarly, if the transit network selection information element contains more address digits than expected, as determined by the 'type of network identification' and 'network identification plan' fields, the network should discard the superfluous digits and route the call. If the network receives a keypad information element containing more address digits than required for completion of digit analysis, the network should discard the superfluous digits (according to the network dialing plan) and route the call. If any of these events occur, the local public network should send the calling user equipment a STATUS message containing National-specific cause 11, 'More digits received than allowed: call is proceeding (location: public network serving the local user' and the call state information element coded as call state 1, 'call initiated.' Private networks may support this procedure, optionally."

Section 5.1.5.1
Call proceeding, en-bloc sending

Delete causes "58 'bearer capability not presently available';" and "63 'service or option not available, unspecified';" from the second paragraph.

Section 5.1.5.1
Call proceeding, en-block sending

Add to the second paragraph after "57 ... authorized": "34 'no circuit or channel available';".

Section 5.1.5.2
Call proceeding, overlap sending

Delete "58 ...available" and "63 ... unspecified" from the first paragraph.

Section 5.1.5.2
Call proceeding, overlap sending

Add after "57 ... not authorized": "34 'no circuit or channel available';" in the first paragraph.

Section 5.1.5.2
Call proceeding, overlap sending

Add the following at the end of section 5.1.5.2:

"*Other Misdialing Treatments*

The Network should be capable of recognizing several types of misdialing. If network-provided tones and announcements do not apply, the network should initiate call clearing in response to a misdialing error. If en-bloc sending has been used, the network should send a RELEASE COMPLETE message to the calling user equipment. If overlap sending has been used, the network should send a DISCONNECT message to the calling user equipment. The initial clearing message should contain the appropriate cause information, as indicated below, and the signal information 'reorder tone on.' If tones and announcements apply, see section 5.3.4.1.

— Vacant code: National-specific cause 4, 'vacant code.'

— Prefix 0 dialed in error: National-specific cause 8, 'prefix 0 dialed in error.'

— Prefix 1 dialed in error: National-specific cause 9 'prefix 1 dialed in error.'

— Prefix 1 not dialed: National-specific cause 10, 'prefix 1 not dialed.'"

Section 5.1.6
Notification of interworking at the originating interface

Change (a) in the first paragraph to: "In an appropriate call control message when a state change is required (i.e., CONNECT); or,".

Section 5.1.6
Notification of interworking at the originating interface

Delete from the second paragraph the progress description value "4 'call has returned to the ISDN'. Call is now end-to-end and ISDN."

Section 5.1.7 Call confirmation indication	Change the last sentence of the first paragraph to: "When the user receives the ALERTING message, the user shall enter the Call Delivered state."
Section 5.2 Call establishment at the destination interface	Change "ANSI standard T1.602" to "NIUF 89-210" in the first sentence of the first paragraph.
Section 5.2 Call establishment at the destination interface	Delete the third paragraph ("The SETUP message offered ... of the data link layer.").
Section 5.2.1 Incoming call	Delete "Display," from the second paragraph "(e.g., Display, Low layer compatibility)."
Section 5.2.1 Incoming call	Add the following to the end of second paragraph. "In general, a call terminating from a non-ISDN line or from a Public Switched Telephone Network (PSTN) trunk should be offered to the called user equipment with the 3.1 kHz audio bearer capability."
Section 5.2.1 Incoming call	Change "(e.g., for DDI)" to "(e.g., 7 digits)" in the second sentence of the third paragraph.
Section 5.2.1 Incoming call	Delete the third sentence from the third paragraph.
Section 5.2.2 Compatibility checking	Delete the third paragraph.
Section 5.2.3.1 SETUP message delivered by point-to-point data link	Delete this section.
Section 5.2.3.2 SETUP message delivered by broadcast data link	Combine the first and second sentences of the first paragraph to: "When the SETUP message is delivered by a broadcast data link, the network sends a SETUP message with the Channel identification information element indicating a specific channel with no alternative acceptable."
Section 5.2.5.1 Response to en-block SETUP	Delete "(see Note)" from the first sentence of the first paragraph.
Section 5.2.5.1 Response to en-block SETUP	Delete the Note after the first paragraph.
Section 5.2.5.1 Response to en-block SETUP	Delete the third paragraph ("When the SETUP message was delivered via a point-to-point data link ...").
Section 5.2.5.3 Called user clearing during incoming call establishment	Delete the first paragraph.

Section 5.2.5.3
Called user clearing during incoming call establishment

Change the second sentence of the second paragraph to: "If timer T303 expires (i.e., if no valid message such as CALL PROCEEDING, ALERTING, or CONNECT has been received), the network shall take action as follows:

a. If all clearing messages received from the called user equipment contain cause 88, 'incompatible destination,' the call should be cleared at the calling ISDN interface with cause 18, 'no user responding (location: public network serving the remote user)' and signal 'ring-back/audible ringing tone on.'

b. If one or more call clearing messages with cause 17, 'user busy,' have been received from the called user equipment, the call should be cleared at the calling ISDN interface with cause 17, 'user busy (location: user).' The signal information should be coded as 'busy tone on' unless an audible ringing tone was indicated because timer T delay (if implemented) previously expired (see sec. 5.2.1). If audible ringing is being provided, the signal information should be coded as 'ring-back/audible ringing tone on.'

c. If no call clearing messages with cause 17 have been received from the called user equipment and at least one call clearing message with a cause other than 88 has been received, the call should be cleared at the calling ISDN interface with cause 21, 'call rejected (location: user),' and signal 'ring-back/audible ringing tone on.'."

Section 5.2.5.3
Called user clearing during incoming call establishment

Delete the last sentence from the second paragraph: "When multiple RELEASE COMPLETE ... sent to the originating user (see 5.3)."

Section 5.2.5.3.1
DISCONNECT received prior to expiry of T312

Change the second sentence in the second paragraph from "If an ALERTING message has been received, ... any other cause sent by a called user." to "If an ALERTING message has been received, the cause sent to the calling user shall be 21 'call rejected' (location: user)."

Section 5.2.5.3.1 DISCONNECT received prior to expiry of T312	Change the third sentence in the second paragraph from "In only CALL PROCEEDING ... sent by a called user." to "If only CALL PROCEEDING messages have been received from called users, the cause sent to the calling user shall be as in 5.2.5.3."
Section 5.2.5.3.2 DISCONNECT received after expiry of timer T312	Change the second sentence in the third paragraph from "If an ALERTING message has been received, ... any other cause sent by a called user." to "If an ALERTING message has been received, the cause sent to the calling user shall be 21 'call rejected' (location: user)."
Section 5.2.5.3.2 DISCONNECT received after to expiry of T312	Change the third sentence in the third paragraph from "If only CALL PROCEEDING ... by a called user" to "If only CALL PROCEEDING messages have been received, the cause sent to the calling user shall be as in 5.2.5.3."
Section 5.2.5.4 Call failure	Delete all occurrences of "(b) ..." (paragraphs 1, 3, 4) from this section.
Section 5.2.6 Notification of interworking at the terminating interface	Delete this section.
Section 5.2.7 Call accept	Add to the end of the second paragraph: "If the CONNECT message is the first response to the SETUP message, it shall contain the channel ID information element."
Section 5.2.8 Active indication	Delete the last paragraph of section 5.2.8 ("A user which has ... has been completed").

Section 5.3.2
Exception conditions

Add the following before the Note that appears at the end of this section.

" — In the case of a SETUP message sent to the user via the broadcast data link, if a called user terminal sends a first response to the SETUP message after timer T303 has expired (the first expiration of T303 is the SETUP message should not be retransmitted, and the second expiration of T303 if the SETUP message should be retransmitted — note that the SETUP message is retransmitted only when no response is received prior to the first expiry of T303, e.g., the SETUP message should not be retransmitted when a call clearing message(s) is received prior to the first expiry of T303), but before timer T312 expires, the network should clear the call to that user by sending a RELEASE message. This message should contain cause 102, 'recovery on timer expiry' (location: public network serving the local user).

— In the case of call offering via the broadcast data link, if either timer T310 or T301 expires at the called user interface, the network should initiate call clearing by sending a RELEASE message to all called user equipment responding to the SETUP message sent by the network. The RELEASE message(s) should contain cause 102, 'recovery on timer expiry' (location: public network serving the local user).

— If a call attempt is unsuccessful and a speech, 3.1 kHz audio call will not be immediately cleared because inband tones or announcements are being provided, the network should send the calling user a PROGRESS message containing progress message containing progress indicator 8, 'inband information or appropriate pattern now available.'."

Section 5.3.3
Clearing initiated by the user

Delete the last Note in this section.

Section 5.3.4.1 Clearing when tones or announcements provided	Add the following at the end of section 5.3.4.1: "To return an inband tone for an unsuccessful speech, 3.1 kHz audio the network should send a PROGRESS message and start a tone timer (value to be specified by network provider) in anticipation of the user initiating the clearing process. The PROGRESS message should contain the cause value indicated in the detailed procedures of Section 5.3, along with progress indicator 8, 'inband information or appropriate pattern now available.' If the tone timer expires, the network should initiate call clearing by sending the calling user a DISCONNECT message containing cause 102, 'recovery on timer expiry.' The network should then continue clearing the connection to the calling user equipment according to the procedures for sending a DISCONNECT message. The procedures described above also apply for returning an inband announcement for an unsuccessful speech, 3.1 kHz audio call, with the exception that the tone timer is not used. Inband announcements should not be timed; however, it is desirable that the network Delete an inband announcement after one or two message cycles, depending on the number specified by the network provider. In removing the inband announcement, the network should follow the above procedures for expiration of the tone timer."
Section 5.3.4.3 Completion of clearing	Delete the last Note at the end of section 5.3.4.3.
Section 5.5 Restart procedure	Delete this section including all subsections.
Section 5.8 Handling of error conditions	Change "T1.607" to "Q.931" in the first sentence of the first paragraph.
Section 5.8.1 Protocol discrimination error	Change "T1.607" to "Q.931" in the first sentence in the first paragraph.
Section 5.8.3.1 Invalid call reference format	Change the second paragraph to: "If the Call reference information element octet 1, bits 1 through 4 indicates a length greater than the maximum length supported by the receiving equipment (see 4.3), or the Null call reference, or the global call reference is used to identify a call, then the message shall be ignored."
Section 5.8.3.2 Call reference procedural errors	Delete item "(f) When any message ... shall be returned."

Section 5.8.4 Message type or message sequence errors	Add as a new paragraph "A NOTIFY message may also be ignored by the recipient." after the first paragraph (i.e., after the list of cause values).
Section 5.8.4 Message type or message sequence errors	Change the fourth sentence in the second paragraph to: "Whenever the network receives an unexpected RELEASE message, the network shall: disconnect and release the B-channel; clear the network connection and the call to the remote user with cause as specified in 5.2.5.3, or cause in the RELEASE message sent by the user. If no cause is included, cause 31 'normal, unspecified' or other causes as specified in 5.8.6.1; return a RELEASE COMPLETE message to the user; release the call reference; stop all timers; and enter the Null state."
Section 5.8.4 Message type or message sequence errors	Change the second sentence of the third paragraph to: "Whenever the network receives an unexpected RELEASE COMPLETE message, the network shall: disconnect and release the B-channel; clear the network connection and the call to the remote user with the cause indicated by the user or, if not included, cause 111 'protocol error, unspecified' or other causes as specified in 5.8.6.1; release the call reference; stop all timers; and enter the Null state."
Section 5.8.6.1 Mandatory information element missing	Change the beginning of the first sentence in the third paragraph to: "When a DISCONNECT message (first clearing message) is received with ...."
Section 5.8.6.1 Mandatory information element missing	Add the following as a new paragraph after the third paragraph: "As an option the network shall follow the following procedure. The DISCONNECT message sent to the network should contain cause information. If the network receives an initial clearing message without a cause information element, it should accept the message, disconnect the associated channel, and initiate procedures to clear the network connection and the call to the remote user. If the call is active or if the originating user cleared the call while in the setup phase, the network should send cause 16, 'normal clearing (location: user)' to the remote user. It should send cause 21, 'call rejected (location: user)' if the terminating user cleared the call while in the setup phase. The network should respond to the user initiating call clearing by sending a RELEASE message containing cause 96, 'mandatory information element is missing (location: public network serving the local user; diagnostic: cause information element identifier).'."

Section 5.8.6.2 Mandatory information element content error	Change the third paragraph to: "When a DISCONNECT message is received with invalid content of the Cause information element, the action taken shall be the same as if a DISCONNECT message with the cause missing was received with the exception that the RELEASE message sent on the local interface contains cause 100 'invalid information element contents'."
Section 5.8.7.1 Unrecognized information elements	Add the following to the Note after the first paragraph: "or not implemented by the receiver in a specific message."
Section 5.8.8 Data-link reset	Change "ANSI T1.607" to "NIUF 90-301" in the first sentence of the first paragraph.
Section 5.8.9 Data-link failure	Change "ANSI T1.607" to "NIUF 90-301" in the first sentence of the first paragraph.
Section 5.8.9 Data-link failure	Change both occurrences of "ANSI T1.607" in the first paragraph bullet b) to "NIUF 90-301".
Section 5.8.9 Data-link failure	Change the first Note after the first paragraph to: "If the transfer mode of the call is circuit-mode, the NIUF 90-301 entity may clear the calls."
Section 5.8.10 Status enquiry procedure	Delete the first paragraph.
Section 5.8.11 Receiving a STATUS message	Delete "As an option:" from the second sentence of the third paragraph ("The determination ...").
Section 5.8.11 Receiving a STATUS message	Change "a)" in the third paragraph to: "If a STATUS message indicating any call state except the Null state is received in the Null state, then the receiving entity shall send a RELEASE COMPLETE message with a cause 101 'message not compatible with call state' or cause 81 'Invalid Call reference value' and remain in the Null state. Otherwise, no action shall be taken on receipt of STATUS unless it is in response to STATUS ENQUIRY."
Section 5.8.11 Receiving a STATUS message	Delete "b) If a ..." and "c) If a STATUS message, indicating the Null ... into the Null state." after the third paragraph.
Section 5.8.11 Receiving a STATUS message	Delete the last three paragraphs and the last Note in this section.
Section 5.9 User notification procedure	Delete this section.

Section 6
Packet communication procedures

Change sentence to "See NIUF 89-320".

Section 9.1
Timers in the network side
Table 22 — Timers in the network side

Change the "T302/Default time out value" cell from "10-15 s" to "16-24 s".

Section 9.1
Timers in the network side
Table 22 — Timers in the network side

Change the "T302/cause for start" cell from "SETUP ACKNOWLEDGE sent. Receipt of INFORMATION restarts T302." to "SETUP ACKNOWLEDGE sent. Receipt of INFORMATION not containing complete address information restarts T302."

Section 9.1
Timers in the network side
Table 22 — Timers in the network side

Change the "T302/NORMAL STOP" cell to: "With sending complete indication, or potentially complete address information received, as an option, the network can determine that a potentially complete code has been received following the receipt of address information, and the network could use critical interdigit timing (instead of T302) to determine whether additional digits are following. This timing could be 3-5 seconds. If implemented, when this timer expires, a complete address is assumed and the procedures in section 5.1.5.2 shall be followed. In an INFORMATION message is received and the critical interdigit timing is running, it shall be stopped."

Section 9.1
Timers in the network side
Table 22 — Timers in the network side

Add the following row entry for Timer "Tpot_comp" after row "T302":

TIMER NUMBER	DEFAULT TIME OUT VALUE	STATE OF CALL	CAUSES FOR START	NORMAL STOP	AT THE FIRST EXPIRY	AT THE SECOND EXPIRY	CROSS REFERENCE
Tpot_comp	3-5 s	Overlap Sending	Potentially complete address information received	INFORMATION received	Route call	Timer not restarted	*

"* optional—as an option, the network can determine that a potentially complete code has been received following the receipt of address information, and the network could use critical interdigit timing (instead of T302) to determine whether additional digits are following. This timing could be 3-5 seconds. If implemented, when this timer expires, a complete address is assumed and the procedures in Section 5.1.5.2 shall be followed. In an INFORMATION message is received and the critical interdigit timing is running, it shall be stopped."

Section 9.1 Timers in the network side Table 22 — Timers in the network side	Change the "T303/DEFAULT TIME OUT VALUE" cell from "4s" to "2.5s".
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Change the "T303/NORMAL STOP" cell to "ALERT, CONNECT, or CALL PROCEEDING received."
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Change the "T303/AT THE FIRST EXPIRY" cell to "Retransmit SETUP; re-start T303."
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Delete "Note 7" from the "T308/AT SECOND EXPIRY" cell.
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Change "10s" to "5s" in the "T310/DEFAULT TIME OUT VALUE" cell.
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Delete "Note 6" from the "T310/DEFAULT TIME OUT VALUE" cell.
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Delete the following rows: "T316", "T317", "T321".
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Delete the following Notes: 3, 6, 7 at the end of Table 22.
Section 9.2 Timers in the user side Table 23 — Timers in the user side	Change the "T301/CROSS REFERENCE" cell to "Note 3".
Section 9.2 Timers in the user side Table 23 — Timers in the user side	Change the "T303/NORMAL STOP" cell to "SETUP ACKNOWLEDGE, CALL PROCEEDING or RELEASE COMPLETE received".
Section 9.2 Timers in the user side Table 23 — Timers in the user side	Delete "(annex D)" from the "T303/AT THE FIRST EXPIRY" cell.
Section 9.2 Timers in the user side Table 23 — Timers in the user side	Change the "T303/CROSS REFERENCE" cell to "optional".
Section 9.2 Timers in the user side Table 23 — Timers in the user side	Delete "Note 5" from the "T308/AT THE SECOND EXPIRY" cell.

Section 9.2 Timers in the user side Table 23 — Timers in the user side	Delete rows "T310", "T316", "T317", "T321".
Section 9.2 Timers in the user side Table 23 — Timers in the user side	Delete Notes 2 and 5 that appear at the end of table 7.
Annex A	Delete this section. NOTE: This section has not been addressed.
Annex B, Section B.3.1 Compatibility checking with addressing information	Change the second sentence under "a)" to: "In the case of a mismatch, the user shall either ignore or reject the call."
Annex B, Section B.3.2 Network to user compatibility	Change the last sentence in this section to: "If a mismatch is detected, then the user shall either ignore or reject the offered call using cause 88 'incompatible destination'."
Annex B, Section B.3.4 User action figures Figure B.1 — Bearer capability compatibility checking Figure B.2 — Low layer and high layer compatibility checking; compatibility assured Figure B.3 — Low layer and high layer compatibility checking; compatibility not assured	Delete the "point-to-point data link" columns.
Annex B, Section B.3.4 User action figures Figure B.1 — Bearer capability compatibility checking Figure B.2 — Low layer and high layer compatibility checking; compatibility assured	Change the "Incompatible/Broadcast data link" cell from "Reject" to "Ignore or Reject".
Annex B, Section B.3.4 User action figures Figure B.2 — Low layer and high layer compatibility checking; compatibility assured Figure B.3 — Low layer and high layer compatibility checking; compatibility not assured	Delete "Note 3" from the "Incompatible/broadcast data link" column.
Annex B, Section B.3.4 User action figures Figure B.1 — Bearer capability compatibility checking Figure B.2 — Low layer and high layer compatibility checking; compatibility assured Figure B.3 — Low layer and high layer compatibility checking; compatibility not assured	Delete the reference to "Note 1" from the last column.

Annex B, Section B.3.4 User action figures Figure B.3 — Low layer and high layer compatibility checking; compatibility not assured	Change "Accept or Reject" to "Accept, Ignore, or Reject" in the Broadcast Data Link column.
Annex B, Section B.3.4 User action figures Figure B.3 — Low layer and high layer compatibility checking; compatibility not assured	Delete Note 1 below figure B.3.
Annex B, Section B.3.4 User action figures Figure B.3 — Low layer and high layer compatibility checking; compatibility not assured	Change "will reject the call if incompatible" to "may reject the call if incompatible" in Note 2 below figure B.3.
Annex B, Section B.3.4 User action figures Figure B.3 — Low layer and high layer compatibility checking; compatibility not assured	Delete Note 3 ("Attempt low layer compatibility negotiation (see Annex M).") below Figure B.3.
Annex C, Section C.1 Introduction	Delete "optional" from the first paragraph.
Annex C, Section C.2 Selection not supported	Delete this section.
Annex C, Section C.3 Selection supported	Change the first sentence of the first paragraph to: "The user identifies the selected transit network in the SETUP message."
Annex C, Section C.3 Selection supported	Delete the second and third paragraphs.
Annex C, Section C.3 Selection supported	Delete the first sentence of the fourth paragraph.
Annex C, Section C.3 Selection supported	Delete the last sentence in the sixth paragraph.
Annex C, Section C.3 Selection supported	Delete the seventh, eighth, and ninth paragraphs.
Annex D Extension for symmetric call operation	Delete this section.
Annex E Network-specific facility selection	Delete this section.
Annex F D-channel backup procedure	Delete this section.

Annex G, Section G.1 Introduction	Add the following at the end of the first paragraph: "Section 4.5.11 identifies the causes supported in NIUF 90-301."
Annex G Cause Definitions	Delete the following sections: • Section G.2.16 Cause 22 "number changed" • Section G.3.2 Cause 38 "network out of order" • Section G.3.7 Cause 45 "preemption" • Section G.3.8 Cause 46 "precedence call blocked" • Section G.3.9 Cause 47 "resource unavailable, unspecified" • Section G.4.1 Cause 49 "quality of service unavailable" • Section G.4.4 Cause 58 "bearer capability no presently available" • Section G.4.5 Cause 63 "service or option not available, unspecified" • Section G.5.2 Cause 66 "channel type not implemented" • Section G.5.4 Cause 70 "only restricted digital information bearer capability is available" • Section G.5.5 Cause 79 "service or option not implemented, unspecified" • Section G.6.2 Cause 82 "identified channel does not exist" • Section G.6.4 Cause 91 "invalid transit network selection" • Section G.6.5 Cause 95 "invalid message, unspecified"
Annex H Examples of Information elements coding	Change the status of this section from "informative" to "normative".
Annex H, Section H.1 Introduction	Replace the first and second paragraphs with the following: "These are the only recognized codings of the following Information Elements for circuit-mode services: — Bearer capability information element — Channel identification information element".
Annex H Examples of information elements coding	Delete the following figures and sections: • Figure "H.3 Coding for 7 kHz Audio" • Figure "H.6 Coding for synchronous 1472 kbit/s"; • sections H.3.2 (Figures H.9, H.10, H.11); • H.3.3 (Figures H.12 through H.17); • H.4 (Figures H.18 through H.21);
Annex H, Section H.3.1 Basic Interface, circuit mode, B-channel	Add Attachment D of this document.

Annex I Use of Progress Indicators	Change the status of this Annex from "Informative" to "Normative".
Annex I Use of progress indicators	Delete the fifth paragraph ("*Progress Indicator 4 ...*").
Annex I Use of Progress Indicators	Delete "or primary" from the left side (between TE and ISDN) of Figure I.1.
Annex I Use of Progress Indicators	Delete "Basic or" from the right side (between ISDN and NT2) of Figure I.1
Annex J Examples of Cause Values and location for busy condition	Change "American National Standard T1.607" to "NIUF 90-301" in the first sentence of the first paragraph.
Annex L low layer information coding principles	Change the first sentence of the first paragraph to: "This annex is part of NIUF 90-301."
Annex M Low layer compatibility Negotiation	Delete this annex.
Annex N Procedures for establishment of bearer connection prior to call acceptance	Delete this annex.
Annex O Optional procedures for bearer service change	Delete this annex.
Annex P, Section P.1 Introduction	Delete "optional" from the first sentence.
Annex P, Section P.1 Introduction	Delete "or attendant system" from the end of the first sentence in the first paragraph.
Annex P, Section P.1 Introduction	Change the last sentence of the first paragraph to: "These procedures apply to the speech and 3.1 kHz audio bearer services."
Annex P, Section P.1 Introduction	Delete "or attendant system" from the first sentence in the second paragraph.
Annex P, Section P.2 Operator system access requested in keypad facility information element	Delete "or attendant system" from the first sentence of the first paragraph.
Annex P, Section P.2 Operator system access requested in keypad facility information element	Delete "or attendant system" from the last sentence of the first paragraph.

Annex P, Section P.3 Use of the operator system access information element	Delete "or attendant system" from the first sentence of the first paragraph.
Annex P, Section P.3 Use of the operator system access information element	Delete "c) Private/principal ... SETUP message." from the second paragraph.
Annex P, Section P.3 Use of the operator system access information element	Delete "or attendant system" from the third paragraph.
Annex P, Section P.3 Use of the operator system access information element	Delete the sixth paragraph.
Annex Q Responding address requirements of the OSI network layer service	Delete this annex.
Annex R Application of the Signal Information Element to Tones and Alerting Patterns	Change the status of this Annex from "informative" to "normative".
Annex R Application of the Signal Information Element to Tones and Alerting Patterns Table 21 — Tones	Delete the following rows: 2, 6, 8.
Annex S Comparison of CCITT Recommendation Q.931 to ANSI T1.607	Delete this annex.

Attachment A
(of Appendix A)

1. General

1.1 Scope and Purpose

This Implementation Agreement specifies a minimal subset of procedures and codepoints from the American National Standards T1.607-1990 (Ref. [17]) for the establishment, maintenance, and clearing of ISDN connections at the user-to-network interface. This signalling standard is used to support the circuit-switched bearer services specified in ANSI standards T1.603*.

Terminals are not required to support all services. Switches will support all of the mandatory protocols and codepoints in this implementation agreement. This does not preclude the support of additional services and procedures. However, equipment must be able to interoperate with equipment supporting only this minimal subset.

1.1.1 Definitions

The ANS T1.607-1990 (Ref. [17]) assumes that procedures apply generically to ISDN access interfaces, i.e., the document does not distinguish between basic and primary rates access interfaces. In addition, there are no references to specific applications in that document. The concept of equipment classes is introduced in this document to permit certain procedures to be associated with a particular application or class of equipment, e.g., station equipment versus PBX. Specifically, two classes of equipment are defined on the basis of two fundamental attributes.

The first attribute relates to the possibility of an exchange of signals occurring beyond the public network's point of contact with the interface (i.e., between the equipment directly connected to the public network and ISDN terminals or telephones connected to that equipment). For example, some user equipment may support subtending Basic Access digital subscriber loops and/or analog telephone loops. For Class I equipment, the network makes no provision for such an arrangement and assumes the Class I equipment constitutes the end point of the communication. Conversely, in the case of Class II equipment, the procedures at the network take into account that communication between Class II equipment (with which it communicates directly) and other equipment (with which the network does not have direct contact) may occur. As an example, Class II equipment may support digital and/or analog subscriber loops. Use of Class II equipment also involves the possibility of having interworking occur beyond the equipment with which the network has direct contact. Therefore, it is reasonable for Class II equipment to provide the network with an interworking notification, for both outgoing and incoming calls, when either the calling or called party respectively, is a non-ISDN user. Class II equipment may also send an interworking notification if a private network exists beyond the Class II equipment and interworking to a non-ISDN facility within that network takes place. When an interface is associated with Class I equipment, it is assumed the multiple pieces of equipment may exist and communicate with the network over the D-channel. However, in this case, all equipment is assumed to be ISDN-capable and is considered as the end point of the communication. Therefore, interworking notification should not be accepted from Class I equipment.

The second attribute relates to the manner in which a SETUP message should be presented to the user equipment. When Class I equipment is applied on a particular interfaces, the network should broadcast the SETUP message associated with each call that terminates on that interface, since interaction between the network and multiple pieces of user equipment should be supported. On the other hand, the network should not broadcast SETUP messages

*Subject to further discussion.

associated with terminating calls to an interface on which Class II equipment is being used. Here, a single piece of user equipment is assumed to be involved in all communication with the network.

To the extent possible, it is desirable to have one set of requirements for ISDN call control apply to all ISDN user configurations. However, in cases for which integrated procedures are not appropriate, the call control procedures associated with Equipment Class I will differ from those associated with Equipment Class II. Unless otherwise noted, the assumption should be that a particular procedure/capability should be provided for both classes of equipment on both basic and primary rate access. However, use of the equipment class terminology permits clarification of the circumstances under which a certain capability should be available (i.e., when a particular equipment class is in use). It also permits a mechanism for indicating that a particular capability applies only to a subset of four possible configurations which are labeled as follows.

	Class I	Class II
BRI	*IB*	*IIB*
PRI	*IP*	*IIP*

In other words, a capability that applies to Class I equipment may be provided on basic access interfaces (IB) and/or primary rate access interfaces (IP). Similarly, a capability that applies to Class II equipment may be provided on basic access interfaces (IIB) and/or primary rate access interfaces (IIP).

The notation shown in the table above is used within this implementation agreement to indicate when protocol or procedures are only expected to be supported for a particular equipment class and/or are limited to a particular type of interface, i.e., basic or primary rate interface.

Attachment B
(of Appendix A)

The various parts of the called party number information element should be coded as follows:

— Type of number and numbering plan (octet 3)

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	Unknown
0 0 1 0 0 0 1	International number in ISDN numbering plan (Rec. E.164)
0 1 0 0 0 0 1	National number in ISDN numbering plan (Rec. E.164)
1 0 0 0 0 0 1	Local (directory) number in ISDN numbering plan (Rec. E.164)
1 1 0 1 0 0 1	Abbreviated Number in Private Numbering plan

All other values are reserved

— Digits (octet 4, etc.)

Bits 7 6 5 4 3 2 1	Meaning
0 1 1 0 0 0 0	0
0 1 1 0 0 0 1	1
0 1 1 0 0 1 0	2
0 1 1 0 0 1 1	3
0 1 1 0 1 0 0	4
0 1 1 0 1 0 1	5
0 1 1 0 1 1 0	6
0 1 1 0 1 1 1	7
0 1 1 1 0 0 0	8
0 1 1 1 0 0 1	9

All other values are reserved

Digits should be represented by IA5 characters whose encoding is shown above.

In the network to user direction (n -> u), this IE will be always signaled in the SETUP message, and public network interfaces will use only one codepoint: local number in ISDN. For private networks, this IE can contain the following codepoints: abbreviated type of number, and private numbering plan, and extra digits such A, B, C, and D (as per IA5).

Attachment C
(of Appendix A)

The various parts of the calling party number information element should be coded as described below. The numbering plans are as described in CCITT Recommendations E.164 or X.121.

— Type of number and numbering plan (octet 3) follows:

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	Unknown
0 0 1 0 0 0 1	International number in ISDN numbering plan (Rec. E.164)
0 0 1 0 0 1 1	International number in data numbering plan (Rec. X.121)
0 1 0 0 0 0 1	National number in ISDN numbering plan (Rec. E.164)
1 0 0 0 0 0 1	Local (directory) number in ISDN numbering plan (Rec. E.164)
1 1 0 1 0 0 1	Abbreviated Number in Private Numbering plan

All other values are reserved

— Origin of number and presentation status (octet 3a) follows:

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	Presentation allowed of user-provided number, number not screened
0 0 0 0 0 0 1	Presentation allowed of user-provided number, number passed network screening
0 0 0 0 0 1 0	Presentation allowed of user-provided number, number failed network screening
0 0 0 0 0 1 1	Presentation allowed of network-provided number
0 1 0 0 0 0 0	Presentation prohibited of user-provided number, number not screened
0 1 0 0 0 0 1	Presentation prohibited of user-provided number, number passed network screening
0 1 0 0 0 1 0	Presentation prohibited of user-provided number, number failed network screening
0 1 0 0 0 1 1	Presentation prohibited of network-provided number
1 0 0 0 0 1 1	Number not available

All other values are reserved

Notes

1—When octet 3a is omitted, the default value of Number Presentation parameter for the signaled DN value should be used, if it is available. If a value for this parameter is unavailable (i.e., the signaled DN value either fails screening or is not screened by the SPCS), the presentation parameter value of the default DN should be used.

2—Octet 3a, bits 7 and 6 are for the Presentation Indicator; bits 2 and 1 are for the Screening Indicator.

— Digits (octet 4, etc.)

Digits should be represented by IA5 characters whose encoding is shown below:

Bits 7 6 5 4 3 2 1	Meaning
0 1 1 0 0 0 0	0
0 1 1 0 0 0 1	1
0 1 1 0 0 1 0	2
0 1 1 0 0 1 1	3
0 1 1 0 1 0 0	4
0 1 1 0 1 0 1	5
0 1 1 0 1 1 0	6
0 1 1 0 1 1 1	7
0 1 1 1 0 0 0	8
0 1 1 1 0 0 1	9

All other values are reserved

Codings At Originating Party Interface

The calling party number information element should only be accepted when in the SETUP message. When the type of number and numbering plan indicator indicates "local number in the ISDN (E.164) numbering plan," the calling party number information element should contain a 7-digit local number. When the type of number and numbering plan indicator indicates "national number in the ISDN (E.164) numbering plan" the calling party number information element should contain a 10-digit national number.

In the network to user direction (n -> u), the coding and delivery of this IE depends on the definition of the Calling Line ID service. For private networks, this IE can contain the following codepoints: abbreviated type of number, and private numbering plan, and extra digits such as A, B, C, and D (as per IA5).

- add the following figures to section H.3.1

8	7	6	5	4	3	2	1	octet
Channel identification								
0	0	0	1	1	0	0	0	1
Information element identifier								
0	0	0	0	0	0	0	1	2
Length of the channel identification contents								
1	0	0	0	1	0	0	1	3
	int id	int type		Pref/ Excl	D ch. id.	Ch. sel.		

Figure H.7-1. Channel B1 exclusive.

8	7	6	5	4	3	2	1	octet
Channel identification								
0	0	0	1	1	0	0	0	1
Information element identifier								
0	0	0	0	0	0	0	1	2
Length of the channel identification contents								
1	0	0	0	0	0	1	0	3
	int id	int type		Pref/ Excl	D ch. id.	Ch. sel.		

Figure H.7-2. Channel B2 preferred.

8	7	6	5	4	3	2	1	octet
Channel identification								
0	0	0	1	1	0	0	0	1
Information element identifier								
0	0	0	0	0	0	0	1	2
Length of the channel identification contents								
1	0	0	0	1	0	1	0	3
	int id	int type		Pref/ Excl	D ch. id.	Ch. sel.		

Figure H.7-3. Channel B2 exclusive.

8	7	6	5	4	3	2	1	octet
Channel identification								
0	0	0	1	1	0	0	0	1
Information element identifier								
0	0	0	0	0	0	0	1	2
Length of the channel identification contents								
1	0	0	0	0	0	1	1	3
	int id	int type		Pref/ Excl	D ch. id.	Ch. sel.		

Figure H.7-4. Any B-channel.

8	7	6	5	4	3	2	1	octet
Channel identification								
0	0	0	1	1	0	0	0	1
Information element identifier								
0	0	0	0	0	0	0	1	2
Length of the channel identification contents								
1	0	0	0	0	0	0	0	3
	int id	int type		Pref/ Excl	D ch. id.	Ch. sel.		

Figure H.7-5. No B-channel Indicated.

APPENDIX B.

NIUF 90-302
Implementation Agreement
of the North American ISDN Users' Forum

Layer 3 Signalling Specification for the
Minimal Set of Circuit-Switched Bearer Services for
the ISDN Class II Primary Rate Interfaces.

<u>Baseline Text</u>
American National Standard T1.607-1990:
Integrated Services Digital Network (ISDN) —
Layer 3 Signalling Specification for
Circuit-Switched Bearer Service for
Digital Subscriber Signalling System Number 1 (DSS1).

<u>Base Standards</u>
CCITT Recommendation Q.931 (1988):
ISDN User-Network Interface Layer 3
Specification For Basic Call Control.
ANSI T1.607-1990
ANSI T1.603-1990*:
Integrated Services Digital Network (ISDN) —
Minimal Set of Bearer Services for
the Primary Rate Interface.

B.1 Abstract

This Implementation Agreement specifies procedures for establishing, maintaining, and clearing connections at the Integrated Services Digital Network (ISDN) user-network interfaces identified as Class II PRI, and are mandatory for the support of the minimal set of circuit-switched bearer services specified by ANSI T1.603-1990* *Integrated Services Digital Network (ISDN)—Minimal Set of Bearer Services for the Primary Rate Interface*, (Ref. [14]). Procedures for circuit-mode digital, circuit-mode speech and circuit-mode voiceband data bearer services are as specified in the baseline text ANS T1.607-1990, *Integrated Services Digital Network (ISDN)—Digital Subscriber Signalling System Number 1 (DSS1)—Layer 3 Signalling Specification for Circuit-Switched Bearer Service*, (Ref. [17]), as further resolved by this agreement. The packet-mode data service is included in this document as a bearer service. Procedures for the packet-mode bearer service will be detailed in another document.

*Subject to further discussion

B.2 Introduction

The original implementation agreement (NIUF 90-302) was reached by marking up the text of ANS T1.607-1990, (Ref. [17]) to reflect the clarifications of text and selection of options. This appendix translates the implementation agreement markup into a listing of these clarifications and selections, (i.e., this appendix lists the differences (the "delta") between the implementation agreement marked up ANS T1.607-1990, and the original text of ANS T1.607-1990).

B.3 NIUF 90-302 Delta List**

The IA has adopted the ANS T1.607-1990*** (Ref. [17]) standard with the following clarifications of the text, and selection of options:

ANS T1.607-1990 SECTION/TABLE NUMBER/NAME	IMPLEMENTATION AGREEMENTS - CLARIFICATION OF TEXT AND SELECTION OF OPTIONS
Section 1.1 Scope and Purpose	Replace this section with Attachment A of this document.
Section 2.1.1.3 Overlap Sending (U2)	Delete this section.
Section 2.1.2.3 Overlap Sending (N2)	Delete this section.
Section 2.1.2.14 Call Abort (N22)	Delete this section.
Section 3.1 Table 1 — Messages for circuit-mode connection control	Delete the following message and reference: "INFORMATION 3.1.6".
Section 3.1 Table 1 — Messages for circuit-mode connection control	Delete the following message and reference: "SETUP ACKNOWLEDGE 3.1.12".
Section 3.1 Table 1 — Messages for circuit-mode connection control	Change "NOTIFY 3.1.7" to "NOTIFY*".

**Note that this Delta List was developed in "good faith" by NIST as a simple equivalent representation of the actual agreements. It has been reviewed and approved by the editors of the Signalling Working Group as per recommendation of the Executive Steering Committee.

***These documents can be purchased from: American National Standards Institute, 11 West 42nd Street, New York, NY 10036.

Section 3.1 Messages for circuit-mode connection control	Add the following footnote below Table 1 "* See section 5.8.4 for treatment of this message."
Section 3.1.1 ALERTING Table 2 — ALERTING message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.1 ALERTING Table 2 — ALERTING message content	Change the "Channel identification/Length" cell from "2-*" to "2, 5-6".
Section 3.1.1 ALERTING Table 2 - ALERTING message content	Delete the following rows: • "Display"; • "Signal".
Section 3.1.1 ALERTING Table 2 — ALERTING message content	Delete Notes 4, 5, 6.
Section 3.1.2 CALL PROCEEDING Table 3 — CALL PROCEEDING message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.2 CALL PROCEEDING Table 3 — CALL PROCEEDING message content	Change the "Channel identification/Type" cell from "O(Note 1)" to "M".
Section 3.1.2 CALL PROCEEDING Table 3 — CALL PROCEEDING message content	Change the "Channel identification/Length" cell from "2-*" to "2, 5-6".
Section 3.1.2 CALL PROCEEDING Table 3 — CALL PROCEEDING message content	Delete rows • "Progress indicator"; • "Display".
Section 3.1.2 CALL PROCEEDING Table 3 — CALL PROCEEDING message content	Delete Notes 1, 2, 3, 4.
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Change the "Channel identification/Length" cell from "2-*" to "2, 5-6".

Section 3.1.3 CONNECT Table 4 — CONNECT message content	Delete the following rows: • "Display"; • "Signal"; • "Connected number"; • "Connected subaddress"; • "Low layer compatibility".
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Change Note 3 to: "Included in the event of interworking."
Section 3.1.3 CONNECT Table 4 — CONNECT message content	Delete Notes 4, 5, 6, 7, 8, 9.
Section 3.1.4 CONNECT ACKNOWLEDGE Table 5 — CONNECT ACKNOWLEDGE message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.4 CONNECT ACKNOWLEDGE Table 5 — CONNECT ACKNOWLEDGE message content	Delete the following rows: • "Display"; • "Signal".
Section 3.1.4 CONNECT ACKNOWLEDGE Table 5 — CONNECT ACKNOWLEDGE message content	Delete Notes 1, 2, 3.
Section 3.1.5 DISCONNECT Table 6 — DISCONNECT message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.5 DISCONNECT Table 6 — DISCONNECT message content	Change the "Cause/Length" from "4-32" to "4-10".
Section 3.1.5 DISCONNECT Table 6 — DISCONNECT message content	Delete the following rows: • "Display"; • "Signal"' • "Connected Number"; • "Connected subaddress".
Section 3.1.5 DISCONNECT Table 6 — DISCONNECT message content	Delete Notes 1, 2, 3, 4, and 5.
Section 3.1.6 INFORMATION	Delete this section.

Section 3.1.7 NOTIFY	Delete this section.
Section 3.1.8 PROGRESS Table 9 — PROGRESS message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.8 PROGRESS Table 9 — PROGRESS message content	Change the "Cause/Length" cell from "2-32" to "2, 4-10".
Section 3.1.8 PROGRESS Table 9 — PROGRESS message content	Delete the following rows: • "Display"; • "Signal".
Section 3.1.8 PROGRESS Table 9 — PROGRESS message content	Delete Notes 2, 3, 4.
Section 3.1.9 RELEASE Table 10 — RELEASE message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.9 RELEASE Table 10 — RELEASE message content	Change the "Cause/Length" cell from "2-32" to "2, 4-10".
Section 3.1.9 RELEASE Table 10 — RELEASE message content	Delete the following rows: • "Display"; • "Signal"; • "Connected number"; • "Connected subaddress".
Section 3.1.9 RELEASE Table 10 — RELEASE message content	Delete Notes 3, 4, 5, 6, 7.
Section 3.1.10 RELEASE COMPLETE Table 11 — RELEASE COMPLETE message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.10 RELEASE COMPLETE Table 11 — RELEASE COMPLETE message content	Change the "Cause/Length" cell from "2-32" to "2, 4-10".

Section 3.1.10 RELEASE COMPLETE Table 11 — RELEASE COMPLETE message content	Delete the following rows: • "Display"; • "Signal"; • "Connected number"; • "Connected subaddress".
Section 3.1.10 RELEASE COMPLETE Table 11 — RELEASE COMPLETE message content	Delete Notes 3, 4, 5, 6, 7.
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.11 SETUP Table 12 — SETUP message content	Delete the following rows: • "Repeat indicator"; • "Display"; • "Keypad facility"; • "Signal".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Bearer capability/Type" cell from "M(Note 2)" to "M".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Bearer capability/Length" cell from "4-13" to "4-8".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Channel identification/Type" cell from "O(Note 3)" to "M".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Channel identification/Length" cell from "2-*" to "5-6".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Network specific facilities/Length" cell from "2-*" to "2-32".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Calling party number/Length" cell from "2-*" to "2-19".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Called party address/Length" cell from "2-*" to "2-18".

Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "Transit network selection/Length" cell from "2-*" to "2-7".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the "High layer capability/Length" cell from "2-4" to "2-5".
Section 3.1.11 SETUP Table 12 — SETUP message content	Delete Notes 1, 2, 3, 6, 7, 8, 9.
Section 3.1.11 SETUP Table 12 — SETUP message content	Change Note 4 to: "Included in the event of interworking."
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the first sentence of Note 12 to: "The called party number information element is included by the user ....".
Section 3.1.11 SETUP Table 12 — SETUP message content	Change the first sentence of Note 20 to: "This information applies to speech and 3.1 kHz audio bearer services."
Section 3.1.11 SETUP Table 12 — SETUP message content	Add the following to the end of Note 13: "The network should transport this IE transparently. This IE is optional on the user side."
Section 3.1.11 SETUP Table 12 — SETUP message content	Add the following to the end of Note 15: "The network should transport this IE transparently. This IE is optional on the user side. The total length is 2 to 16 octets."
Section 3.1.11 SETUP Table 12 — SETUP message content	Add the following to the end of Note 16: "The network should transport this IE transparently. This IE is optional on the user side."
Section 3.1.11 SETUP Table 12 — SETUP message content	Add the following to the end of Note 17: "The network will treat this IE on sending and receiving as described in the User-User supplementary service Implementation Agreement."
Section 3.1.12 SETUP ACKNOWLEDGE	Delete this section.
Section 3.1.13 STATUS Table 14 — STATUS message content	Change the "Call reference/Length" cell from "2-*" to "2-3".

Section 3.1.13 STATUS Table 14 — STATUS message content	Change the "Cause/Length" cell from "4-32" to "4-10".
Section 3.1.13 STATUS Table 14 — STATUS message content	Delete row "Display".
Section 3.1.13 STATUS Table 14 — STATUS message content	Delete Notes 1, 2.
Section 3.1.14 STATUS ENQUIRY	Change the first sentence to: "This message is sent by the user or the network during the active state to solicit a STATUS message from the peer layer 3 entity."
Section 3.1.14 STATUS ENQUIRY Table 15 — STATUS ENQUIRY message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.1.14 STATUS ENQUIRY Table 15 — STATUS ENQUIRY message content	Delete row "Display".
Section 3.1.14 STATUS ENQUIRY Table 15 — STATUS ENQUIRY message content	Delete Notes 1, 2.
Section 3.2.1 RESTART Table 17 — RESTART message content	Change the "Call reference/Length" cell from "2-*" to "2-3".
Section 3.2.1 RESTART Table 17 — RESTART message content	Change the "Channel identification/Length" cell from "2-*" to "2, 5-6".
Section 3.2.1 RESTART Table 17 — RESTART message content	Delete row "Display".
Section 3.2.1 RESTART Table 17 — RESTART message content	Delete Notes 3, 4.
Section 3.2.2 RESTART ACKNOWLEDGE Table 18 — RESTART ACKNOWLEDGE message content	Change the "Call reference/Length" cell from "2-*" to "2-3".

Section 3.2.2 RESTART ACKNOWLEDGE Table 18 — RESTART ACKNOWLEDGE message content	Change the "Channel identification/Length" cell from "2-*" to "2, 5-6".
Section 3.2.2 RESTART ACKNOWLEDGE Table 18 — RESTART ACKNOWLEDGE message content	Delete row "Display".
Section 3.2.2 RESTART ACKNOWLEDGE Table 18 — RESTART ACKNOWLEDGE message content	Delete Notes 3, 4.
Section 4.2 Protocol discriminator	Add the following sentence after the first sentence in the second paragraph: "The only value supported for call control messages is described below in Figure 2."
Section 4.2 Protocol discriminator Figure 2 — Protocol Discriminator	Change "ANSI T1.607" to "Q.931".
Section 4.2 Protocol discriminator Table 19 — Protocol Discriminator	Change "ANSI T1.607" to "Q.931" in row "0000 1000".
Section 4.3 Call reference	Change the third paragraph ("At a minimum ...") to: "At a minimum, all networks and users must be able to support a call reference value of one and two octets for a primary rate interface."
Section 4.3 Call reference	Delete the first sentence of the fourth paragraph "As a network ... also be supported."
Section 4.3 Call reference Figure 4 — Dummy call reference	Change "Figure 4. Dummy call reference" to "Figure 4. Dummy call reference *".
Section 4.3 Call reference	Add the following footnote after Figure 4: "*The dummy call reference is not supported for primary rate Class II circuit-switched calls."
Section 4.3 Call reference	Delete Note 1 ("The call reference ... ") at the end of the section.
Section 4.4 Message type Table 20 — Message types	Delete the following rows: • "SETUP ACKNOWLEDGE"; • "INFORMATION".

Section 4.4 Message type Table 20 — Message types	Add the following to the end of row "NOTIFY": "(see sec. 5.8.4 for treatment of this message type)."
Section 4.5.1 Coding rules	Delete the second, third, and fourth sentences from the fourth paragraph.
Section 4.5.1 Coding rules Figure 7 — Formats of information elements	Delete figure (b) Single octet information element format (type 2).
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Delete the following rows: • "Repeat indicator"; • "Notification indicator"; • "Display"; • "Keypad facility"; • "Signal"; • "Connected number"; • "Connected subaddress"; • "Escape for extension".
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Delete reference to "(Note 6)" from "Bearer capability" row.
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Change the "Bearer capability/Max length" cell from "13" to "8".
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Change the "Cause/Max length" cell from "32" to "10".
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Change the "Cause/Max no of occurrences" cell from "3" to "2".
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Change the "Channel identification/Max length" cell from "(Note 4)" to "6".
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Change the "Network-specific facilities/Max length" cell from "(Note 4)" to "32".
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Change the "Network-specific facilities/Max no. of occurrences" cell from "4" to "2".

Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Change the "Calling party number/Max length" cell from "(Note 4)" to "19".
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Change the "Called party number/Max length" cell from "(Note 4)" to "18".
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Delete reference to "(Note 2)" from "Transit network selection" row.
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Change the "Transit network selection/Max length" cell from "(Note 4)" to "7".
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Delete "4" from the "Transit network selection/Max no. of occurrences" cell.
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Change the "High layer compatibility/Max length" cell from "4" to "5".
Section 4.5.1 Coding rules Table 21 — Information element identifier coding	Delete Notes 3, 4, 6.
Section 4.5.1 Coding rules Figure 8 — Information element format using escape for extension	Delete this figure.
Section 4.5.2 Extensions of codesets	Change "T1.608" to "NIUF 89-320" in the first bullet in the fourth paragraph.

Section 4.5.2 Extensions of codesets	Replace the tenth paragraph ("Codeset 6 ...") with the following: "Codeset 6 is reserved for information elements specific to the local network (either public or private). These information elements can appear in a call establishment (i.e., SETUP, ALERTING, or CONNECT) or first clearing message. As such, they do not have significance across a national or international boundary. For these two cases, codeset 6 information elements shall be handled according to the procedures for unrecognized information elements (see sec. 5.8.7.1) beyond the local network boundary. Inside a private local network recognized codeset 6 information elements shall be consumed, manipulated, or passed transparently according to the rule for that information element. Across the boundary between local networks (e.g., a public and a private network), recognized codeset 6 information elements shall be consumed and manipulated according to the rule for that information element. Inside a private local network, unrecognized codeset 6 information elements may be passed transparently. Across the boundary between a private local network and a public local network, unrecognized codeset 6 information elements shall be either treated as per section 5.8.7.1 or passed transparently if a bilateral agreement exists."
Section 4.5.3 Locking shift procedure New codeset identification table	Change "T1.608" to "NIUF 89-320" for codeset 5.
Section 4.5.4 Non-locking shift procedures	Delete "a) process the nonblocking ... as described below" from the second paragraph.
Section 4.5.4 Non-locking shift procedures Temporary codeset identification table	Change "T1.607" to "NIUF 90-302" for codeset 0.
Section 4.5.4 Non-locking shift procedures Temporary codeset identification table	Change "T1.608" to "NIUF 89-320" for codeset 5.
Section 4.5.5 Bearer Capability	Change "13 octets" to "8 octets" in the second sentence ("The maximum length ...") of the second paragraph.
Section 4.5.5 Bearer Capability Figure 11 — Bearer capability information element	Change octet 4, bit 8 from "0/1" to "1".

Section 4.5.5 Bearer Capability Figure 11 — Bearer capability information element	Delete the following octets: • 4a; • 4b; • 5b (Note 2); • 5b (Note 3); • 5c; • 5d.
Section 4.5.5 Bearer Capability Figure 11 — Bearer capability information element	Change octet 5a, bit 8 from "0/1" to "1".
Section 4.5.5 Bearer Capability Figure 11 — Bearer capability information element	Delete Notes 1, 2, 3.
Section 4.5.5 Bearer Capability Figure 11 — Bearer capability information element	Add the following after Note 4: "5 Octets 6 and 7 are included for information only. The coding and application of these octets are included in another document."
Section 4.5.5 Bearer Capability Information transfer capability (octet 3) coding	Delete row "10001 7 kHz audio".
Section 4.5.5 Bearer Capability Information transfer rate (octets 4 and 4b) coding	Change the title to "Information transfer rate (octet 4)".
Section 4.5.5 Bearer Capability Information transfer rate (octets 4 and 4b) coding	Delete the following rows: "10011 384 kbit/s", "10100 1472 kbit/s (Note 2)", "10101 1526 kbit/s".
Section 4.5.5 Bearer Capability Information transfer rate (octets 4 and 4b) coding	Change Note 1 to: "The bearer capability is bidirectional symmetric at the information transfer rate specified in octet 4."
Section 4.5.5 Bearer Capability Information transfer rate (octets 4 and 4b) coding	Delete Note 2.
Section 4.5.5 Bearer Capability	Delete all codings and text referring to octet 4a (structure, configuration, establishment) and octet 4b (symmetry).
Section 4.5.5 Bearer Capability User information layer 1 protocol (octet 5) coding	Delete "and optionally octets 5b, 5c, and 5d as defined below." from row "00001".

Section 4.5.5 Bearer Capability User information layer 1 protocol (octet 5) coding	Delete "and G.725 7 kHz audio" from row "00101".
Section 4.5.5 Bearer Capability User information layer 1 protocol (octet 5) coding	Delete rows "00111" and "01000".
Section 4.5.5 Bearer Capability User information layer 1 protocol (octet 5) coding	Delete Note 2.
Section 4.5.5 Bearer Capability Synchronous/asynchronous (octet 5a) coding	Delete row "1 asynchronous".
Section 4.5.5 Bearer Capability Synchronous/asynchronous (octet 5a) coding	Delete the second and third sentences from the Note.
Section 4.5.5 Bearer Capability Negotiation (octet 5a) coding	Delete row "1 In-band negotiation possible".
Section 4.5.5 Bearer Capability User rate (octet 5a) coding	Delete all rows except row "01111 56 kbit/s CCITT Recommendation V.6".
Section 4.5.5 Bearer Capability	Delete all text relating to octet 5b (i.e., sections labeled "Octet 5b for CCITT Recommendation V.100 or X.30 rate adaption" and "Octet 5b for CCITT Recommendation V.120 rate adaption").
Section 4.5.5 Bearer Capability	Delete all codings and text referring to octets 5c (number of data bits excluding parity bit, parity information) and 5d (duplex mode, modem type).
Section 4.5.6 Call state Call state value (octet 3) coding	Delete row "000010 U2 — overlap sending".
Section 4.5.6 Call state Call state value (octet 3) coding	Add the following column to the right of the coding: <u>Symmetric States*</u> S0 — Null S1 — Call Initiated S3 — Outgoing Call Proceeding S4 — Call Delivered S6 — Call Present S7 — Call Received S8 — Connect Request S9 — Incoming Call Proceeding

	S10 — Active S11 — Disconnect Request S12 — Disconnect Indication S19 — Release Request
Section 4.5.6 Call state Call state value (octet 3) coding	Add the following after the coding: "*Note—For Symmetric states see Annex D."
Section 4.5.6 Call state Call state value (octet 3) coding	Delete "N22 — Call abort" from the "010110/ Network State" cell.
Section 4.5.7 Called party number	Change the second paragraph to: "The maximum length of this information element is 18 octets."
Section 4.5.7 Called party number Type of number (octet 3) coding	Delete the following rows: • "011 network specific number"; • "111 reserved for extension".
Section 4.5.7 Called party number Type of number (octet 3) coding	Change the end of Note 2 to: "this information element cannot be used in combination with Operator System Access or Transit Network Selection information elements."
Section 4.5.7 Called party number Type of number (octet 3) coding	Delete Note 4.
Section 4.5.7 Called party number Numbering Plan Identification (octet 3) coding	Delete the following rows: • "0011 data numbering plan"; • "0100 telex numbering plan"; • "1111 reserved for extension".
Section 4.5.7 Called party number Numbering plan identification (octet 3) coding	Change "c)" under the Note to: "this information element cannot be used in combination with Operator System Access or Transit Network Selection information elements."
Section 4.5.7 Called party number	Add Attachment B of this document after the following: "*Number digits (octets 4, etc.)* This field is coded with ASCII characters, according to the formats specified in the appropriate numbering/dialing plan."
Section 4.5.9 Calling party number	Change the second paragraph from "The maximum length of this information element is network dependent." to "The maximum length of this information element is 19 octets."

Section 4.5.9 Calling party number Type of number (octet 3) coding	Delete the following rows: • "011 network specific number"; • "111 reserved for extension".
Section 4.5.9 Calling party number Type of number (octet 3) coding	Delete Note 4.
Section 4.5.9 Calling party number Numbering Plan Identification (octet 3) coding	Delete the following rows: • "0100 telex numbering plan"; • "1111 reserved for extension".
Section 4.5.9 Calling party number	Add Attachment C of this document after the following: "*Number digits (octets 4, etc.)* This field is coded with ASCII characters, according to the formats specified in the appropriate numbering/dialing plan."
Section 4.5.11 Cause	Change the second sentence of the first paragraph to: "The maximum length of this information element is 10 octets."
Section 4.5.11 Cause Figure 17 — Cause information element	Change octet 3, bit 8 from "0/1" to "1".
Section 4.5.11 Cause Figure 17 — Cause information element	Delete octet 3a.
Section 4.5.11 Cause Figure 17 — Cause information element	Delete the Note under the figure.
Section 4.5.11 Cause Recommendation (octet 3a) coding	Delete this coding and Notes 1 and 2.
Section 4.5.11 Cause	Add the following sentence to the end of the paragraph following "*Diagnostics (octet 5)*": "If more than one IE is identified in a diagnostic, they should be ordered as IEs normally appear in a message."
Section 4.5.11 Cause Cause table	Change the "unallocated (unassigned) number/ diagnostics" cell to "Not used".
Section 4.5.11 Cause Cause table	Change the "no route to specified transit network/ diagnostics" cell to "Not used".

Section 4.5.11 Cause Cause table	Change the "no route to destination/diagnostics" cell to "Not used".
Section 4.5.11 Cause Cause table	Change "normal call clearing/diagnostics" cell to "Not used".
Section 4.5.11 Cause Cause table	Change the "user busy/diagnostics" cell to "(see Note 10)".
Section 4.5.11 Cause Cause table	Change the "call rejected/diagnostics" cell to "Not used".
Section 4.5.11 Cause Cause table	Delete the "number changed/diagnostics" cell.
Section 4.5.11 Cause Cause table	Delete the following rows: • "non-selected user clearing"; • "network out of order"; • "resource unavailable, unspecified"; • "quality of service unavailable"; • "only restricted digital information bearer capability is available"; • "service or option not implemented, unspecified"; • "invalid transit network selection"; • "invalid message, unspecified".
Section 4.5.11 Cause Cause table	Change the "No circuit/channel available/diagnostics" cell to "(see Note 10)".
Section 4.5.11 Cause Cause table	Delete reference to "(see Note 6)" in the "access information discarded/diagnostics" cell.
Section 4.5.11 Cause Cause table	Add "(see Note 10)" to the "requested circuit or channel not available/diagnostics" cell.
Section 4.5.11 Cause Cause table	Delete the corresponding cell in the "diagnostics" column for the following rows: • "requested facility not subscribed"; • "bearer capability not authorized"; • "bearer capability not presently available"; • "channel type not implemented"; • "requested facility not implemented".

Section 4.5.11 Cause Cause table	Change the "bearer capability not implemented/ diagnostics" cell to "Not used".
Section 4.5.11 Cause Cause table	Change the "identified channel does not exist/ diagnostics" cell to "Not used".
Section 4.5.11 Cause Cause table	Delete the "incompatible destination/diagnostics" cell.
Section 4.5.11 Cause Cause table	Delete the reference to "(see Note 6)" in the "mandatory information element is missing/ diagnostics" cell.
Section 4.5.11 Cause Cause table	Change the "information element non-existent or not implemented/diagnostics" cell to "Information element identifier(s) (see Note 8)".
Section 4.5.11 Cause Cause table	Change the "invalid information element contents/ diagnostics" cell to "Information element identifier(s)".
Section 4.5.11 Cause Cause table	Change the "recovery on timer expiry/diagnostics" cell to "Not used".
Section 4.5.11 Cause Cause table	Delete the following Notes: 2, 3, 4, 5, 6, 7, 9, 11, 12.
Section 4.5.11 Cause Figure 18 — Coding of the diagnostic field for causes 57, 58 and 65.	Delete this figure and Notes 1 and 2 appearing below it.
Section 4.5.11 Cause	Delete all text referring to octets 5 (attribute number), 5a (rejected attribute), and 5b (available attribute).
Section 4.5.12 Channel identification	Change the last sentence in the first paragraph to: "The default maximum length for this information element is 6 octets."
Section 4.5.12 Channel identification	Delete the second paragraph.

Section 4.5.12 Channel identification Figure 19 — Channel identification information element	Change octet 3.1, bit 8 from "0/1" to "1".
Section 4.5.12 Channel identification Figure 19 — Channel identification information element	Delete the reference to "Note 2" of octet 3.2.
Section 4.5.12 Channel identification Figure 19 — Channel identification information element	Delete the references to "(Note 2)" and "Note 4" in octet 3.3.
Section 4.5.12 Channel identification Figure 19 — Channel identification information element	Delete the last sentence of Note 1.
Section 4.5.12 Channel identification Figure 19 — Channel identification information element	Delete Notes 2 and 4.
Section 4.5.12 Channel identification Figure 19 — Channel identification information element	Add the following to the end of Note 3: "For completeness, a pointer to slot map is shown. It is not supported for this IA."
Section 4.5.12 Channel identification Interface identifier present (octet 3) coding	Change row the last row ("1") to: "1 Interface explicitly identified in octet 3.1."
Section 4.5.12 Channel identification Interface type (octet 3) coding	Delete the following row: "0 basic interface".
Section 4.5.12 Channel identification Information channel selection (octet 3) coding	Delete the column "basic interface".
Section 4.5.12 Channel identification Information channel selection (octet 3) coding	Delete the last two rows ("10" and "11").
Section 4.5.12 Channel identification Information channel selection (octet 3) coding	Delete Note 3.

Section 4.5.12 Channel identification Interface identifier (octet 3.1) coding	Delete the second sentence ("At subscription time ...").
Section 4.5.12 Channel identification Coding standard (octet 3.2) coding	Delete row " 1 0 National Standard ..."
Section 4.5.12 Channel identification Number/map (octet 3.2) coding	Delete the last row.
Section 4.5.12 Channel identification Channel type/map element type (octet 3.2) coding	Delete the last three rows.
Section 4.5.12 Channel identification Channel type/map element type (octet 3.2) coding	Delete the Note.
Section 4.5.12 Channel identification	Delete all text and Figure 20 referring to "Slot map (octet 3.3)".
Section 4.5.12 Channel identification	Add the following at the end of the section: "Note—In the network to user direction (n -> u), the terminating PRI will allow channel negotiation. The network will support offering calls with preferred B-channel and the user responds specifying the channel to be used for the call."
Section 4.5.13 Connected number	Delete this section.
Section 4.5.14 Connected subaddress	Delete this section.
Section 4.5.15 Display	Delete this section.
Section 4.5.16 High layer compatibility	Change the second paragraph to: "The maximum length of this information element is five octets."
Section 4.5.17 Keypad facility	Delete this section.
Section 4.5.18 Low layer compatibility	Delete the second paragraph.
Section 4.5.18 Low layer compatibility Negotiation indicator (octet 3a) coding	Delete the last row.

Section 4.5.18 Low layer compatibility Negotiation indicator (octet 3a) coding	Delete Note 1.
Section 4.5.18 Low layer compatibility User information layer 3 protocol (octet 7) coding	Change "ANSI T1.607" to "NIUF 90-302" in the first row.
Section 4.5.19 Network-specific facilities	Change the second sentence of the first paragraph to: "No more than two Network-specific facilities information elements may be included in a single message."
Section 4.5.19 Network-specific facilities	Change the second paragraph to: "The maximum length of this information element is 32 octets."
Section 4.5.19 Network-specific facilities	Add Attachment D of this document to the end of this section.
Section 4.5.20 Notification indicator	Delete this section.
Section 4.5.21 Progress indicator Progress description (octet 4) coding	Delete row "000 0100 4 call has returned to the ISDN."
Section 4.5.21 Progress indicator	Add the following Note after Notes 1 and 2 following the "*Progress description (octet 4)*" coding: "3 In the SETUP message, in the user to network direction (u -> n) on PRI, one of two values may be used in the progress description field: 'call is not end-to-end ISDN' (1), or 'calling equipment is non-ISDN' (3). In the SETUP message, in the network to user direction (n -> u) on PRI, one of two values may be used in the progress description field: 'call is not end-to-end ISDN' (1), or 'calling equipment is non-ISDN' (3)."
Section 4.5.22 Repeat Indicator	Delete this section.
Section 4.5.24 Signal	Delete this section.
Section 4.5.25 Transit network selection	Change the first paragraph to: "The purpose of the Transit network selection information element is to identify one requested transit network (See Annex C)."

Section 4.5.25 Transit network selection	Change the second paragraph to: "The default maximum length of this information element is 7 octets."
Section 4.5.25 Transit network selection Type of network identification (octet 3) coding	Delete the last row ("011 ...").
Section 4.5.25 Transit network selection Network identification plan (octet 3) coding	Delete the last row ("0011 ...").
Section 4.5.26 User-user	Add the following to the end of the first paragraph: "This IE is to be included based on the User-to-user supplementary service description and user application."
Section 4.5.26 User-user Protocol discriminator (octet 3) coding	Change "ANSI T1.607" to "NIUF 90-302" in the last row of the coding.
Section 5 Circuit-switched call control procedures	Change the third paragraph ("All messages ...") to: "All messages in this standard contain the functional type of information elements. Functional information elements are characterized as requiring a degree of intelligent processing by the Customer Premise Equipment (CPE) in either their generation or analysis."
Section 5 Circuit-switched call control procedures	Delete the fifth paragraph ("As a general ..."), the second Note of the section, and the seventh paragraphs ("In addition ...").
Section 5.1 Call establishment at the originating interface	Change "ANSI T1.602" to "NIUF 89-210" in the last sentence.
Section 5.1.1 Call request	Change the last sentence of the first paragraph to: "The Bearer capability information element is mandatory in the SETUP message."
Section 5.1.1 Call request	Change the third paragraph to: "Furthermore, the SETUP message shall also contain all of the call information (i.e., address and facility requests) necessary for call establishment."
Section 5.1.1 Call request	Delete the following from the fourth paragraph: "b) the Keypad information ... other call information," and the Note ("All networks are ...").
Section 5.1.1 Call request	Delete the last paragraph ("For overlap ...").

Section 5.1.2 B-channel selection — originating	Delete the following from the first paragraph: "c) any channel ... alternative c) is assumed."
Section 5.1.2 B-channel selection — originating	Delete the last sentence from the third paragraph: "In case c), the ... with the D-channel."
Section 5.1.2 B-channel selection — originating	Change the end of the first sentence in the fourth paragraph from "(i.e., a SETUP ACKNOWLEDGE or CALL PROCEEDING message)." to "(i.e., a CALL PROCEEDING message)."
Section 5.1.2 B-channel selection — originating	Change the fifth paragraph to: "The user need not attach until receiving a: a) CALL PROCEEDING, b) ALERTING message with the progress indicator 8 'in-band information or appropriate pattern is now available' or c) a PROGRESS message with the progress indicator 1 'call is not end-to-end ISDN; further call progress information may be available in-band'. Prior to this time, the network cannot assume that the user has attached ... (if it has not already done so)."
Section 5.1.2 B-channel selection — originating	Change the first sentence of the last paragraph to: "In case a), if the specified channel is not available, and in case b) if not channel is available, a RELEASE COMPLETE message with a cause value of 44 'requested circuit/channel not available' or 34 'no circuit/channel available', respectively, is sent by the network as described in 5.3."
Section 5.1.3 Overlap sending	Delete this section.
Section 5.1.4 Invalid call information	Change the first sentence in the first paragraph to: "If, following the receipt of the SETUP message, the network determines ... cause such as the following:".
Section 5.1.4 Invalid call information	Add the following to the end of the first paragraph after "28 ...": "82 'identified channel does not exist'."
Section 5.1.5.1 Call proceeding, en-bloc sending	Add the following to the second paragraph after "58 ...": "34 'no circuit/channel available'."
Section 5.1.5.2 Call proceeding, overlap sending	Delete this section.
Section 5.1.6 Notification of interworking at the originating interface	Change "a) ..." in the first paragraph to: "a) in an appropriate call control message when a state change is required (CONNECT); or,".

Section 5.1.6 Notification of interworking at the originating interface	Add to the end of "1 ..." in the second paragraph "(i.e., in a PROGRESS message); or,".
Section 5.1.6 Notification of interworking at the originating interface	Change "2 ..." in the second paragraph to: "2 'destination address is non-ISDN' (i.e., in a CONNECT message);".
Section 5.1.6 Notification of interworking at the originating interface	Delete "4 ... end-to-end ISDN" from the second paragraph.
Section 5.1.6 Notification of interworking at the originating interface	Delete "or more" from the second part of the first sentence in the fourth paragraph.
Section 5.1.7 Call confirmation indication	Change the last sentence in the first paragraph to: "When the user receives the ALERTING message, the user shall enter the Call Delivered state."
Section 5.2 Call establishment at the destination interface	Delete the last sentence of the third paragraph ("No use ...").
Section 5.2.1 Incoming call	Delete the last two sentences of the first paragraph.
Section 5.2.1 Incoming call	Change the last part of the second paragraph from "(e.g., Display, Low layer compatibility)." to "(e.g., Low layer compatibility.)".
Section 5.2.1 Incoming call	Add the following to the end of the second paragraph: "In general, a call terminating from a non-ISDN line or from a Public Switched Telephone Network (PSTN) trunk should be offered to the called user equipment with the 3.1 kHz audio bearer capability."
Section 5.2.1 Incoming call	Delete the first and second sentences of the third paragraph. Delete "However, if ... the interface" from the third sentence. The third paragraph will now read: "A point-to-point data link shall be used to carry the SETUP message. After sending the SETUP message, the network starts timer T303."
Section 5.2.1 Incoming call	Delete the fifth paragraph and the Note following this paragraph.
Section 5.2.1 Incoming call	Change the second part of the last sentence in the seventh paragraph from "timers T303 and T312 are restarted." to "timer 303 is restarted."

Section 5.2.2 Compatibility checking	Delete the second paragraph ("When the SETUP message ...").
Section 5.2.3.1 SETUP message delivered by point-to-point data link	Delete the following from the first paragraph under "a) ...": "3) any channel is acceptable."
Section 5.2.3.1 SETUP message delivered by point-to-point data link	Delete the paragraph under "b) ...." that reads "In case 3), ..."
Section 5.2.3.1 SETUP message delivered by point-to-point data link	Change the first sentence in the third paragraph under "b)" to: "If in case 1) the B-channel indicated in the first response message is not the channel offered by the network, or in case 2) the B-channel indicated in the first response message is unacceptable to the network, it will clear the call by sending a RELEASE message with cause 6 'channel unacceptable' (see 5.3.2 d)."
Section 5.2.3.1 SETUP message delivered by point-to-point data link	Change the first part of "e) ..." to: "e) In case 1) if the indicated B-channel is not available, or in case 2) if no B-channel is available ...."
Section 5.2.3.2 SETUP message delivered by broadcast data link	Delete this section.
Section 5.2.5.1 Response to en-bloc SETUP	Change the first sentence of the Note to: "A Progress indicator information element may be included in a CONNECT message (e.g., when an analogue terminal is connected to an NT2 functional grouping)."
Section 5.2.5.1 Response to en-bloc SETUP	Delete the second paragraph ("When the SETUP message was delivered via a broadcast ...").
Section 5.2.5.2 Receipt of CALL PROCEEDING and ALERTING	Delete the first paragraph ("When the SETUP message is delivered on a broadcast ...").
Section 5.2.5.2 Receipt of CALL PROCEEDING and ALERTING	Change the second paragraph to: "Upon receipt of the first CALL PROCEEDING message from a user, the network shall: stop timer T303; start time T310; and enter the incoming Call Proceeding state."
Section 5.2.5.2 Receipt of CALL PROCEEDING and ALERTING	Delete the fourth paragraph ("When the SETUP message was delivered via a broadcast ...").

Section 5.2.5.2 Receipt of CALL PROCEEDING and ALERTING	Change the fifth paragraph to: "Upon receipt of the ALERTING message from a user, the network shall: stop timers T303 or T310 (if running) and TDEL (if running); start optional timer T301 (unless another internal alerting supervision timer function exists; w.g. incorporated in call control); enter the Call Received state; and send a corresponding ALERTING message to the calling user."
Section 5.2.5.2 Receipt of CALL PROCEEDING and ALERTING	Delete the sixth paragraph ("When a SETUP message has been delivered on a broadcast link ...").
Section 5.2.5.3 Called user clearing during Incoming call establishment	Change the first part of the first paragraph to: "If the RELEASE COMPLETE or DISCONNECT message is received ...."
Section 5.2.5.3 Called user clearing during Incoming call establishment	Delete the second and third paragraphs.
Section 5.2.5.3.1 DISCONNECT received prior to expiry of T312	Delete this section.
Section 5.2.5.3.2 DISCONNECT received after expiry of timer T312	Delete this section.
Section 5.2.5.4 Call failure	Delete the following from the first paragraph: "a) If the SETUP message ... Call Abort state;"
Section 5.2.5.4 Call failure	Change "b)" in the first paragraph to: "b) The network shall also initiate clearing procedures toward the called user in accordance with 5.3.4, using cause 102 'recovery on timer expiry'."
Section 5.2.5.4 Call failure	Delete the second paragraph ("If the network receives ...").
Section 5.2.5.4 Call failure	Delete the following from the third paragraph: "a) If the SETUP ... shall be sent."
Section 5.2.5.4 Call failure	Change "b)" in the third paragraph to: "b) The called user shall be cleared in accordance with 5.3.4, using cause 102 'recovery on timer expiry'."
Section 5.2.5.4 Call failure	Change the beginning of the first sentence in the fourth paragraph to: "If the network supports timer T301 and has received a ALERTING message, ..."
Section 5.2.5.4 Call failure	Delete from the fourth paragraph: "a) If the SETUP message was ... shall be sent."

Section 5.2.5.4 Call failure	Change "b)" in the fourth paragraph to: "b) The called user shall be cleared in accordance with 5.3.4, using cause 102 'recovery on timer expiry'."
Section 5.2.6 Notification of interworking at the terminating interface	Change the first item in the list in the second paragraph from: "— in an appropriate ..." to: "— in an appropriate call control message when a state change is required (CONNECT); or,".
Section 5.2.6 Notification of interworking at the termination interface	Delete the third item from the list in the third paragraph: "4 Call has ...'".
Section 5.2.7 Call accept	Add the following to the end of the last paragraph: "If the CONNECT message is the first response to the SETUP message, it shall contain the channel identification information element."
Section 5.2.8 Active indication	Delete the fourth paragraph ("A user that has received the SETUP via the broadcast data link ...").
Section 5.2.9 Non-selected user clearing	Delete this section.
Section 5.3.2 Exception conditions	Change in the first paragraph "a)" to: "a) In response to a SETUP message, the user or network can reject a call (e.g., because of the unavailability of a suitable B-channel) by: responding with a RELEASE COMPLETE message provided no other response has previously been sent releasing; the call reference and entering the Null state."
Section 5.3.2 Exception conditions	Delete from the first paragraph: "b) In the case ... user clearing".
Section 5.3.2 Exception conditions	Delete from the first paragraph e)1) and e)2) and the Note at the end of the section.
Section 5.4 In-band tones and announcements	Change the title of this section to "In-band audible ringing tone and announcements".

Section 5.4 In-band tones and announcements	Change the first paragraph to: "It is assumed that the originating Class II device will provide a busy tone and a reorder tone to the calling user for speech and 3.1 kHz calls. The network will not provide in-band busy or reorder tone. When in-band audible ringing tone/announcements not associated with a call state change are to be provided by the network before reaching the Active state, a PROGRESS message is returned simultaneously with the application of the in-band audible ringing tone/announcement. The PROGRESS message contains the progress indicator 8 'in-band information or appropriate pattern is now available'."
Section 5.4 in-band tones and announcements	Change the second paragraph to: "When an audible ringing tone has to be provided together with a ... is sent simultaneously with the application of the inband audible ringing tone."
Section 5.4 in-band tones and announcements	Delete Note 1.
Section 5.4 in-band tones and announcements	Change Note 2 to: "When the PROGRESS message is used, the user may initiate call clearing as a result of the applied in-band audible ringing tone/ announcement, according to procedures specified in 5.3.3."
Section 5.5 Restart procedure	Delete from the second paragraph "b) the interface is a ... exists; or,".
Section 5.5.2 Receipt of RESTART	Change in Note 2 the reference to "ANSI T1.602" to "NIUF 89-210".
Section 5.5.2 Receipt of RESTART	Change in Note 2 "b)" to: "b) that correspond to the specified channel or interface."
Section 5.7 Call collisions	Delete the Note at the end of the section.
Section 5.8.2 Message too short	Change this paragraph to: "When a message is received that is too short (less than 4 octets) to contain a complete message type information element, that message shall be ignored."
Section 5.8.4 Message type or message sequence errors	Add the following after the first paragraph: "The NOTIFY message may be ignored by the recipient."
Section 5.8.7.2 Non-mandatory information element content error	Delete the last sentence of the second paragraph ("However, in some ...").

Section 5.8.8 Data link reset	Delete from the first paragraph: "a) For calls in the Overlap ... procedures of 5.3".
Section 5.8.9 Data link failure	Delete from the first paragraph the first sentence of "a) ..." ("The calls in the ... internally.").
Section 5.8.9 Data link failure	Delete the second sentence of the Note following the first paragraph ("Note—If the transfer mode ....").
Section 5.9 User notification procedure	Delete this section.
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Delete row "T302".
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Delete the second sentence in the "T310/NORMAL STOP" cell ("If DISCONNECT ...").
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Delete rows "T312" and "T321".
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Delete Notes 4 and 5.
Section 9.1 Timers in the network side Table 22 — Timers in the network side	Add the following to the end of Note 6: "(see Annex D)".
Section 9.2 Timers in the user side Table 23 — Timers in the user side	Delete the following rows: • "T301"; • "T304".
Section 9.2 Timers in the user side Table 23 — Timers in the user side	Delete "SETUP ACKNOWLEDGE" from the "T303/ NORMAL STOP" cell.
Section 9.2 Timers in the user side Table 23 — Timers in the user side	Delete the reference to "Note 4" in the "T310/TIMER NUMBER" cell.
Section 9.2 Timers in the user side Table 23 — Timers in the user side (Part 2)	Delete Notes 3 and 4.
Annex A — SDL diagrams	Delete this section. NOTE: This section has not been addressed.

Section B.3.1 Compatibility checking with addressing information	Delete Note 2 ("If an incoming call, ... or subaddress.").
Section B.3.4 User action figures Figure B.1 — Bearer capability compatibility checking Figure B.2 — Low layer and high layer compatibility checking; compatibility assured	Delete the reference to "(Note 1)" from the cell in the first row of the second column.
Section B.3.4 User action figures Figure B.1 — Bearer capability compatibility checking Figure B.2 — Low layer and high layer compatibility checking; compatibility assured	Delete the "broadcast data link" column.
Section B.3.4 User action figures Figure B.3 — Low layer and high layer compatibility checking; compatibility not assured	Delete the reference for "(Note 1)" in the cells in the first row of the second and third columns.
Section B.3.4 User action figures	Delete Notes 1 and 3 (ed. note: Note 3 is still referenced in the figures).
Annex C, Section C.1 Introduction	Delete "optional" from the first paragraph.
Annex C, Section C.2 Selection Not Supported	Delete this section.
Annex C, Section C.3 Selection Supported	Change the first paragraph to: "The user identifies the selected transit network in the SETUP message. One Transit network selection information element is used to convey a single network identification."
Annex C, Section C.3 Selection Supported	Delete the second ("The user may ..."), third ("As the call ..."), and fourth ("No more than ...") paragraphs.
Annex C, Section C.3 Selection Supported	Delete the last sentence of the sixth paragraph ("The diagnostic ...").
Annex C, Section C.3 Selection Supported	Delete the seventh ("A network may ...") and eighth ("If the transit ...") paragraphs.
Annex D Extensions for Symmetric Call Operation	Delete Annex D and replace with Attachment E of this document.

Annex E, Section E.3 Routing Not Supported	Add the following paragraph before at the end of this section: "When the requested facility can not be provided an indication shall be returned in the first clearing message with cause 29 'facility rejected'."
Annex E, Section E.4 Routing Supported	Change the first sentence in the fourth paragraph to: "No more than two Network-specific facilities information elements may be used in a SETUP message."
Annex E, Section E.4 Routing Supported	Delete the last sentence of the fifth paragraph ("The diagnostic ...").
Annex F D-channel Backup Procedure	Delete this Annex.
Annex G, Section G.1 Introduction	Add the following to the end of the first paragraph: "Section 4.5.11 identifies the causes supported in NIUF 90-302."
Annex G, Section G.3.8 Cause 46 "precedence call blocked"	Change "precedence circuits" to "preemptable circuits".
Annex H, Section H.1 Introduction	Change the first paragraph to: "These are the only recognized codings of the following information elements."
Annex H, Section H.1 Introduction	Delete the last two bullet items from the second paragraph.
Annex H Examples of Information Elements Coding	Delete the following figures and sections: • Figure "H.3 Coding for 7kHz Audio"; • Figure "H.6 Coding for synchronous 1472 kbit/s"; • Section H.3 Channel identification information element; • Section H.4 Called and Calling party subaddress information element.
Annex I Use of Progress indicators	Delete the fifth paragraph ("*Progress indicator 4 ...*").
Annex I Use of Progress indicators	Delete "or basic" from the left side of Figure I.1 (between the TE and ISDN).
Annex I Use of Progress indicators	Delete "or basic" from the right side of Figure I.1 (between ISDN and NT2).
Annex M Low Layer Compatibility Negotiation	Delete this Annex.

Annex N Procedures for Establishment of Bearer Connection Prior to Call Acceptance	Delete this Annex and replace with Attachment F of this document.
Annex O Optional Procedures for Bearer Service Change	Delete this Annex.
Annex P, Section P.1 Introduction	Delete "optional" from the first sentence in the first paragraph.
Annex P, Section P.1 Introduction	Change the last sentence of the first paragraph to: "These procedures apply to the speech, and 3.1 kHz and audio bearer services."
Annex P, Section P.1 Introduction	Change the second paragraph to: "The user may indicate a request for access to an operator or attendant system using the Operator system access information element."
Annex P, Section P.2 Operator system access requested in Keypad facility information	Delete this section.
Section P.4 invalid request	Delete this section.
Annex Q Responding address requirements of the OSI network layer service	Delete this Annex.

Attachment A
(of Appendix B)

1. General

1.1 Scope and Purpose

This Implementation Agreement specifies a minimal subset of procedures and codepoints from the American National Standards T1.607-1990 (Ref. [17]) for the establishment, maintenance, and clearing of ISDN connections at the user-to-network interface. This signalling standard is used to support the circuit-switched bearer services specified in ANS T1.604-1990*.

Terminals are not required to support all services. Switches will support all of the mandatory protocols and codepoints in this implementation agreement. This does not preclude the support of additional services and procedures. However, equipment must be able to interoperate with equipment supporting only this minimal subset.

1.1.1 Definitions

The ANS T1.607-1990 (Ref. [17]) assumes that procedures apply generically to ISDN access interfaces, i.e., the document does not distinguish between basic and primary rates access interfaces. In addition, there are no references to specific applications in that document. The concept of equipment classes is introduced in this document to permit certain procedures to be associated with a particular application or class of equipment, e.g., station equipment versus PBX. Specifically, two classes of equipment are defined on the basis of two fundamental attributes.

The first attribute relates to the possibility of an exchange of signals occurring beyond the public network's point of contact with the interface (i.e., between the equipment directly connected to the public network and ISDN terminals or telephones connected to that equipment). For example, some user equipment may support subtending Basic Access digital subscriber loops and/or analog telephone loops. For Class I equipment, the network makes no provision for such an arrangement and assumes the Class I equipment constitutes the end point of the communication. Conversely, in the case of Class II equipment, the procedures at the network take into account that communication between Class II equipment (with which it communicates directly) and other equipment (with which the network does not have direct contact) may occur. As an example, Class II equipment may support digital and/or analog subscriber loops. Use of Class II equipment also involves the possibility of having interworking occur beyond the equipment with which the network has direct contact. Therefore, it is reasonable for Class II equipment to provide the network with an interworking notification, for both outgoing and incoming calls, when either the calling or called party respectively, is a non-ISDN user. Class II equipment may also send an interworking notification if a private network exists beyond the Class II equipment and interworking to a non-ISDN facility within that network takes place. When an interface is associated with Class I equipment, it is assumed the multiple pieces of equipment may exist and communicate with the network over the D-channel. However, in this case, all equipment is assumed to be ISDN-capable and is considered as the end point of the communication. Therefore, interworking notification should not be accepted from Class I equipment.

The second attribute relates to the manner in which a SETUP message should be presented to the user equipment. When Class I equipment is applied on a particular interfaces, the network should broadcast the SETUP message associated with each call that terminates on that interface, since interaction between the network and multiple pieces of user equipment should be supported. On the other hand, the network should not broadcast SETUP messages associated with terminating calls to an interface on which Class II equipment is being used. Here, a single piece of user equipment is assumed to be involved in all communication with the network.

---

*Subject to further discussion.

To the extent possible, it is desirable to have one set of requirements for ISDN call control apply to all ISDN user configurations. However, in cases for which integrated procedures are not appropriate, the call control procedures associated with Equipment Class I will differ from those associated with Equipment Class II. Unless otherwise noted, the assumption should be that a particular procedure/capability should be provided for both classes of equipment on both basic and primary rate access. However, use of the equipment class terminology permits clarification of the circumstances under which a certain capability should be available (i.e., when a particular equipment class is in use). It also permits a mechanism for indicating that a particular capability applies only to a subset of four possible configurations which are labeled as follows.

	Class I	Class II
BRI	*IB*	*IIB*
PRI	*IP*	*IIP*

In other words, a capability that applies to Class I equipment may be provided on basic access interfaces (IB) and/or primary rate access interfaces (IP). Similarly, a capability that applies to Class II equipment may be provided on basic access interfaces (IIB) and/or primary rate access interfaces (IIP).

The notation shown in the table above is used within this implementation agreement to indicate when protocol or procedures are only expected to be supported for a particular equipment class and/or are limited to a particular type of interface, i.e., basic or primary rate interface.

Attachment B
(of Appendix B)

The various parts of the called party number information element should be coded as follows:

— Type of number and numbering plan (octet 3)

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	Unknown
0 0 1 0 0 0 1	International number in ISDN numbering plan (Rec. E.164)
0 1 0 0 0 0 1	National number in ISDN numbering plan (Rec. E.164)
1 0 0 0 0 0 1	Local (directory) number in ISDN numbering plan (Rec. E.164)

All other values are reserved

— Digits (octet 4, etc.)

Bits 7 6 5 4 3 2 1	Meaning
0 1 1 0 0 0 0	0
0 1 1 0 0 0 1	1
0 1 1 0 0 1 0	2
0 1 1 0 0 1 1	3
0 1 1 0 1 0 0	4
0 1 1 0 1 0 1	5
0 1 1 0 1 1 0	6
0 1 1 0 1 1 1	7
0 1 1 1 0 0 0	8
0 1 1 1 0 0 1	9

All other values are reserved

Digits should be represented by IA5 characters whose encoding is shown above.

In the network to user direction (n -> u), this IE will be always signaled in the SETUP message, and public network interfaces will use only one codepoint: local number in ISDN. For private networks, this IE can contain the following codepoints: abbreviated type of number, and private numbering plan, and extra digits such A, B, C, and D (as per IA5).

Attachment C
(of Appendix B)

The various parts of the calling party number information element should be coded as described below.

— Type of number and numbering plan (octet 3) follows:

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	Unknown
0 0 1 0 0 0 1	International number in ISDN numbering plan (Rec. E.164)
0 0 1 0 0 1 1	International number in data numbering plan (Rec. X.121)
0 1 0 0 0 0 1	National number in ISDN numbering plan (Rec. E.164)
1 0 0 0 0 0 1	Local (directory) number in ISDN numbering plan (Rec. E.164)
1 1 0 1 0 0 1	Abbreviated Number in Private Numbering plan
	All other values are reserved

— Origin of number and presentation status (octet 3a) follows:

Bits 7 6 5 4 3 2 1	Meaning
0 0 0 0 0 0 0	Presentation allowed of user-provided number, number not screened
0 0 0 0 0 0 1	Presentation allowed of user-provided number, number passed network screening
0 0 0 0 0 1 0	Presentation allowed of user-provided number, number failed network screening
0 0 0 0 0 1 1	Presentation allowed of network-provided number
0 1 0 0 0 0 0	Presentation prohibited of user-provided number, number not screened
0 1 0 0 0 0 1	Presentation prohibited of user-provided number, number passed network screening
0 1 0 0 0 1 0	Presentation prohibited of user-provided number, number failed network screening
0 1 0 0 0 1 1	Presentation prohibited of network-provided number
1 0 0 0 0 1 1	Number not available
	All other values are reserved

Note 1 — When octet 3a is omitted, the default value of the Number Presentation parameter for the signaled DN value should be used, if it is available. If a value for this parameter is unavailable (i.e., the signaled DN value either fails screening or is not screened by the SPCS), the presentation parameter value of the default DN should be used.

Note 2 — Octet 3a, bits 7 & 6, are for the Presentation indicator; bits 2 & 1 are for the screening indicator.

— Digits (octet 4, etc.)

Digits should be represented by IA5 characters whose encoding is shown below:

Bits 7 6 5 4 3 2 1	Meaning
0 1 1 0 0 0 0	0
0 1 1 0 0 0 1	1
0 1 1 0 0 1 0	2
0 1 1 0 0 1 1	3
0 1 1 0 1 0 0	4
0 1 1 0 1 0 1	5
0 1 1 0 1 1 0	6
0 1 1 0 1 1 1	7
0 1 1 1 0 0 0	8
0 1 1 1 0 0 1	9

All other values reserved

Codings At Originating Party Interface

The calling party number information element should only be accepted when in the SETUP message. When the type of number and numbering plan indicator indicates "local number in the ISDN (E.164) numbering plan," the calling party number information element should contain a 7-digit local number. When the type of number and numbering plan indicator indicates "national number in the ISDN (E.164) numbering plan" the calling party number information element should contain a 10-digit national number.

In the network-to-user direction (n -> u). the coding and delivery of this IE depends on the definition of the Calling Line ID service. For private networks, this IE can contain the following codepoints: abbreviated type of number, and private numbering plan, and extra digits such as A, B, C, and D. (as per IE5)

Attachment D
(of Appendix B)

Network — Specific facilities Information Element Examples

One recommended use for the Network Specific Facilities information element is to indicate which type of network facilities are being invoked at the specified network. In this arrangement, many different facility types are allowed to share a single Primary Rate Interface. Examples of the different DS-1 facility types allowed are:

Private Lines
Inwats Circuits
Outwats Circuits
Foreign Exchange (FX)
Tie Trunks

Attachment E
(of Appendix B)

(editor's note: the sections contained in the parentheses are unchanged from the original Annex D)

*Annex D — Extensions for symmetric **(peer-to-peer)** call operation*

This annex is part of NIUF 90-302.

Symmetric call operation, or peer-to-peer call operation, shall be applied to the switches within a private network where all switches, such as PBXs and central office switches serving business group users are considered as peers. For example, PBX-to-PBX, PBX-to-Centrex, Centrex-to-Centrex.

D.1 Additional message handling

(In symmetric applications, the SETUP message will contain a Channel Identification information element indicating a particular B-channel to be used for the call. A point-to-point data link shall be used to carry the SETUP message.)

The following procedures shall be followed for symmetrical operation. The call control states followed should be the symmetric states defined in section D.6.

D.1.1 Call Request

The initiator of the call shall follow the network side procedures described in section 5.2.1.

D.1.2 B-channel Selection — symmetric interface

(Only B-channels controlled by the same D-channel will be the subject of the selection procedure. The selection procedure is as follows:

a) The SETUP message will indicate one of the following:

   1) channel is indicated, no acceptable alternative, or

   2) channel is indicated, any alternative is acceptable.

b) In cases 1) and 2), if the indicated channel is acceptable and available, the recipient of the SETUP message reserves it for the call. In case 2), if the recipient of the SETUP message cannot grant the indicated channel, it reserves any other available B-channel associated with the D-channel.)

c) The recipient of the SETUP message indicates the selected B-channel in a CALL PROCEEDING, message transferred across the interface and enters the Incoming Call Proceeding state. If an ALERTING or a CONNECT message is received in response to a SETUP message, the call should continue to be processed, if the channel indicated is acceptable to the initiator of the call, in accordance with sections D.1.5.1 and D.1.8, respectively. Although these are acceptable responses, a CALL PROCEEDING message is the recommended response to a SETUP message.

d)

e) In case 1) if the indicated B-channel is not available, or in case 2) if no B-channel is available, a RELEASE COMPLETE message with a cause value of No. 44 "requested circuit/channel not available" or No. 34 "no circuit/channel available" respectively is returned to the initiator of the call. The sender of this message remains in the Null state.

f) If the channel indicated in the CALL PROCEEDING, message is unacceptable to the initiator of the call, it clears the call in accordance with section 5.3. If an ALERTING or a CONNECT message is received in response to a SETUP message and the channel indicated is unacceptable to the initiator of the call, it clears the call in accordance with section 5.3. Although these are acceptable responses, a CALL PROCEEDING message is the recommended response to a SETUP message.

D.1.3 Invalid Call Information

The recipient of a SETUP message shall follow the network side procedures described in section 5.1.4.

D.1.4 Compatibility Checking

The recipient of a SETUP message shall follow the user side procedures described in section 5.2.2.

D.1.5 Call Confirmation

Upon receipt of a SETUP message, the equipment enters the Call Present state. Valid responses to the SETUP message are a CALL PROCEEDING, or a RELEASE COMPLETE message. If an ALERTING or a CONNECT message is received in response to a SETUP message, the call should continue to be processed, if the channel indicated is acceptable to the initiator of the call, in accordance with sections D.1.5.1. and D.1.8, respectively. Although these are acceptable responses, a CALL PROCEEDING message is the recommended response to a SETUP message.

If the indicated channel is acceptable to the initiator of the call, the initiator shall attach to the indicated B-channel according to the procedures in Annex N.

D.1.5.1 Receipt of CALL PROCEEDING and ALERTING

The Initiator of a call shall follow the network side procedures in section 5.2.5.2.

D.1.5.2 Clearing during incoming call establishment

The initiator of a call shall follow the network side procedures in section 5.2.5.3.

D.1.5.3 Call Failure

The initiator of a call shall follow the network side procedures in section 5.2.5.4.

D.1.6 Clearing by the called user employing user-provided tones/announcements

When tones or announcements are provided in conjunction with call clearing, the party providing the in-band treatment shall send a PROGRESS message.

D.1.7 Call Accept

The recipient of the call shall follow the user side procedures in section 5.2.7.

D.1.8 Active indication

Upon receipt of a CONNECT message, the initiator of the call shall respond with a CONNECT ACKNOWLEDGE message and enter the Active State (see sec. 5.2.8 network side procedures).

D.1.9 Call Clearing

D.1.9.1 Normal Call Clearing

Then sender of the DISCONNECT message shall follow the user side procedures in section 5.3.3. The recipient of the DISCONNECT message shall follow the network side procedures in section 5.3.3.

D.2 Timers for call establishment

The timers described in section 9 table 7 shall be implemented along with the corresponding procedures for action's taken upon expiration of these timers. The default of T310 should be extended to 20 seconds. In addition, timer T309 shall be mandatory.

D.3 Call collisions

In symmetric arrangements, call collisions can occur when both sides simultaneously transfer a SETUP message indicating the same channel. In the absence of administrative procedures for assignment of channels to each side of the interface, the following procedure is employed.

First, one side of the interface will be designated the **"controlling function"** and the other side of the interface will be designated the **"responding function."** This can be accomplished by administering the Layer 2 Command/ Response bit. The controlling function is assigned **"command"** and has control of all the channels on the interface. The responding function is assigned **"response."** Second, for the three possible scenarios where the same channel is indicated by combinations of preferred and exclusive from the responding function and controlling function, the following procedure is used:

a) **"controlling function"** preferred, **"responding function"** preferred:

The **"controlling function"** preferred channel is awarded and an alternate channel is indicated in the first response to the **"responding function"** SETUP message.

b) **"controlling function"** exclusive, **"responding function"** exclusive:

The **"controlling function"** exclusive channel is awarded and the **"responding function"** SETUP message is cleared with a RELEASE COMPLETE message with cause No. 34 "no circuit/channel available".

c) **"controlling function"** preferred, **"responding function"** exclusive; or **"controlling function"** exclusive, **"responding function"** preferred:

The side of the interface with an exclusive indicator in a SETUP message is awarded the channel and an alternate channel is indicated in the first response to the side using a preferred indicator in the SETUP message.

Channel identification is allowed in both directions for ALERTING and CONNECT.

D.4 Restart Procedures

See section 5.5.

D.5 Handling of Error Codes

See section 5.8.

D.6 Call control states for symmetric call operation

The state below are used in association with call references other than the global call reference, and apply to symmetric interfaces. The Outgoing side is the side of the symmetric interface that transmits the SETUP message, while the incoming side is the recipient of the SETUP message.

D.6.1 Null State (S0)

No call exists.

D.6.2 Call Initiated (S1)

This state exists for an outgoing call when the Outgoing Side has sent a request for call establishment to the Incoming Side but has not yet received a response.

D.6.3 Outgoing Call Proceeding (S3)

This state exists for an outgoing call when the Outgoing Side has received acknowledgment that the Incoming Side has received all call information necessary to effect call establishment.

D.6.4 Call Delivered (S4)

This state exists for an outgoing call when the Outgoing Side has received from the Incoming Side an indication that the called user is being alerted.

D.6.5 Call Present (S6)

This state exists for an incoming call when the Incoming Side has not yet responded to the request from the Outgoing Side for call establishment.

D.6.6 Call Received (S7)

This state exists for an incoming call when the Incoming Side has indicated to the Outgoing Side that the called user is being alerted.

D.6.7 Connect Request (S8)

This state exists for an incoming call when the Incoming Side has indicated to the Outgoing Side that the called user has answered the call.

D.6.8 Incoming Call Proceeding (S9)

This state exists for an incoming call when the Incoming Site has sent to the Outgoing Side acknowledgment that it has received all call information necessary to effect call establishment.

D.6.9 Active (S10)

This state exists for an incoming call when the Incoming Side has received from the Outgoing Side an acknowledgment of the indication that the called user has answered the call. This state exists for an outgoing call when the Outgoing Side has received from the Incoming Side an indication that the called user has answered the call.

D.6.10 Disconnect Request (S11)

This state exists when a Side has sent to the other Side a request to disconnect the user information connection and is waiting for a response.

D.6.11 Disconnect Indication (S12)

This state exists when a Side has received from the other Side a request to disconnect the user information connection and has not yet responded.

D.6.12 Release Request (S19)

This state exists when a Side has sent to the other Side a request to release the call and has not yet received a response.

Attachment F
(of Appendix B)

Annex N — Procedures for Establishment of Bearer Connection Prior to Call Acceptance

This annex is part of NIUF 90-302.

N.1 General

For some applications, it is desirable to allow the completion of the transmission path associated with a bearer service prior to receiving call acceptance. In particular, the completion of the backward direction for non-peer communication or both directions for peer-to-peer communication (see Annex D for peer-to-peer call operation) of the transmission path prior to receipt of a CONNECT message from the called user may be desirable to:

1) allow the called user to provide internally-generated tones and announcements that are sent in-band to the calling user prior to answer by the called user; or,

2) avoid speech clipping on connections involving an NT2 where delays may occur in relaying the answer indication within the called user equipment.

The procedures described in this annex are applicable to the speech and 3.1 kHz audio bearer services, for non-peer communication of both directions for peer-to-peer communication (see Annex D for peer-to-peer call operation).

N.2 Procedures

Completion of the transmission path prior to receipt of a call acceptance indication shall be provided in three ways:

1) For peer-to-peer communications on receipt of a CALL PROCEEDING message or an ALERTING message indicating completion of successful channel negotiation.

2) For non-peer communication on receipt of an ALERTING message; and

3) For non-peer communications on receipt of a PROGRESS message.

When criteria (1) is used to determine that a transmission path should be established, the sender of the SETUP message shall connect, both directions of the transmission path upon receipt of either a CALL PROCEEDING message or an ALERTING message containing an acceptable B-channel indication.

When criteria (2) is used to establish the transmission path, the network shall connect, the backward direction of the transmission path upon receipt of an ALERTING message assuming channel negotiation procedures have been successful.

When criteria (3) is used to establish the transmission path, the network shall connect, the backward direction of the transmission path upon receipt of a PROGRESS message containing progress indicator 1 "call is not end-to-end ISDN; further call progress information may be available in-band," assuming that the user has already returned a CALL PROCEEDING message and channel negotiation procedures have been successful.

If an ALERTING message follows a PROGRESS message containing progress indicator 1, it should be treated as an unexpected message.

The network may choose to further restrict when message(s) will result in establishment of the transmission path. These restrictions may be imposed on a per interface basis to provide an administrative means for limiting potential misuse of the early connection capabilities.

Acronyms

3PTY	Three Party Service
ACD	Automatic Call Distributor
ACT1	Abstract Conformance Test Group for Layer 1
ACT23	Abstract Conformance Test Group for Layers 2 and 3
AE	ASI Entity
ALLF	Additional Lower Layer Functions
ANS	American National Standard
ANSI	American National Standards Institute
AOC	Advice of Charge
AOW	Asian Oceanic Workshop
AP	Application Profile
ARS	Automatic Route Selection
ACSE	Association Control Service Element
ASI	Application Software Interface
BLLF	Basic Lower Layer Functions
BOC	Bell Operating Company
BRA	Basic Rate Access
BRI	Basic Rate Interface
CCBS	Completion of Calls to Busy Subscribers
CCITT	International Telephone and Telegraph Consultative Committee
CCR	Concurrency, Commitment, and Recovery
CD	Call Deflection
CFB	Call Forward Busy
CFNR	Call Forward No Reply
CFU	Call Forwarding Unconditional
CLID	Calling Line Identification
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CO	Central Office
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
CONF	Conference calling
COS	Corporation for Open Systems
CPE	Customer Premises Equipment
CPN	Calling Party Number
CRED	Credit Card Calling
CSD	Circuit-Switched Data
CSV	Circuit-Switched Voice
CSVMS	Centralized Secure Voice Messaging System
CT	Conformance Test
CT	Call Transfer
CUG	Closed User Group
CW	Call Waiting
DCE	Data Circuit-Terminating Equipment
DN	Directory Number
DSS1	Digital Subscriber Signalling System Number 1
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-Frequency
DTP	Distributed Transaction Processing

EAMF	Equal Access Multi-Frequency
ECMA	European Computer Manufacturers Association
EDI	Electronic Data Interchange
EKTS	Electronic Key Telephone Service
ESCA	Exchange Carriers Standards Association
ETSI	European Telecommunications Standards Institute
EWOS	European Workshop for Open Systems
FIPS	Federal Information Processing Standard
FTAM	File Transfer and Management
FTP	File Transfer Protocol
HLDC	High-Level Data Link Control
HLF	High Level Function
HOLD	Call Hold
IA	Implementation Agreements
IAS	ISDN Assurance Service
ICOT	ISDN Conformance Test
ICS	Implementation Conformance Statement
IIW	ISDN Implementors Workshop
INTAP	Interoperability Technical Association Processing
ISDN	Integrated Services Digital Network
ISER(M)	ISDN Station Event Recording (Module)
ISP	International Standardized Profile
ISPICS	International Standardized Profiles Implementation Conformance Statement
IUW	ISDN Users' Workshop
IWF	Interworking Functions
LAN	Local Area Network
LAPD	Link Access Procedure, D-Channel
LLSIG	Lower Layer Special Interest Group
MA	Messaging and Answering
MCI	Malicious Call Identification
MSN	Multiple Subscriber Number
MWI	Message Waiting Indicator
NA	Network Adapter
NFS	Network File System
NIST	National Institute of Standards and Technology
NIUF	North American ISDN Users' Forum
NMWG	Network Management Expert Working Group
NT	Network Termination
NUI	Network User Identification
OIW	OSI Implementors Workshop
OSI	Open Systems Interconnection
pAP	proposed Application Profile
PBX	Private Branch Exchange
PIN	Personal Identification Number
PNP	Private Numbering Plan
PRA	Primary Rate Access
PRI	Primary Rate Interface
PSD	Packet-Switched Data
PSN	Private Switched Network
REV	Reverse Charging
RL	Requirments List

RPN	Redirecting Party Number
SAP	Service Acces Point
SCAI	Switch-Computer Applications Interface
SNA	Systems Network Architecture
SPID	Station Profile Identification
SPO	Standards Promotion Organization
SS	Supplementary Service
SS7	Signalling System Number 7
SUB	Sub-addressing
SVME	Secure Voice Mail Environment
SVMS	Secure Voice Mail System
SWG	Signalling Working Group
TA	Terminal Adapter
TE	Terminal Equipment
TEI	Terminal Endpoint Identifier
TFN	Transferred From Number
TP	Transaction Processing (Distributed)
TPN	Transferred Party Number
TPSE	Transaction Processing Service Element
TTCN	Tree and Tabular Combined Notation
TTN	Transferred To Number
UUS	User-to-User Signalling
VM	Voice Mail
VMS	Voice Messaging Systems
VPN	Virtual Private Network
WAN	Wide Area Network
WG	Working Group

*U.S. GOVERNMENT PRINTING OFFICE: 1994-300-568/03000

ANNOUNCEMENT OF NEW PUBLICATIONS ON INTEGRATED SERVICES DIGITAL NETWORK

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 823-.

Name ____

Company ____

Address ____

City ________________ State ____________ Zip Code __________

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bi-monthly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW., Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program in support of the efforts of private-sector standardizing organizations.

Consumer Information Series—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards and Technology
Gaithersburg, MD 20899