NIS-A211-1

Digital Switching Systems

ISDN Primary Rate User-Network Interface Specification

NA011 Standard 08.01 August 1998

NORTEL
NORTHERN TELECOM

Notice

This specification is provided as a guide for network planners and suppliers of systems and equipment designed to meet the requirements of Northern Telecom’s DMS-100 NA011 Primary Rate Interface specification. Northern Telecom reserves the right to revise the contents of this specification for any reason, including, but not limited to, conformity with standards promulgated by any public standards agency, advances in technology, or to reflect changes in requirements of communication networks, systems, or applications.

Northern Telecom makes no representation with respect to and does not warrant the technical information contained in this specification including, without limitation, any warranty as to fitness for a particular purpose or merchantability or against infringement of patents, copyrights, trademarks, or other intellectual property rights.

The provision of any capabilities described in this document is dependent on certain business decisions, resolution of which may result in changes to, withdrawal of, or addition to, any or all of the capabilities herein.

Receipt and use of the technical information contained in this specification by recipient shall constitute agreement by recipient that it waives any claims it might have against Northern Telecom as a consequence thereof and that in no event shall Northern Telecom be liable for any special, indirect, incidental, or consequential damages of any nature whatsoever.

Digital Switching Systems

ISDN Primary Rate User-Network Interface Specification

Publication number: NIS-A211-1
Product release: NA011
Document release: Standard release 08.01
Issue date: August 1998

Printed in the United States and Canada.

Publication History

January 1993

BCS35 Standard NIS A211-1 Release 5

January 1994

BCS36 Preliminary NIS A211-1 Release 6

- New ISDN PRI functionality has been added as described below:

Cause Screening
A screening facility has been added to map locally significant causes received by the terminating interface to more generalized ones.

Inband Treatment Subscription
A capability has been added to provide inband treatment for calls originating on a PRI interface.

March 1994

BCS36 Standard NIS A211-1 Release 6

- A number of minor technical changes have been made in this release.

May 1997

NA007 Standard NIS A211-1 Release 7

- New ISDN PRI functionality has been added as described below.

Release Link Trunk (RLT)
RLT is a feature available on an optionality basis which optimizes the usage of NTNA PRI trunks.

CPN Screening
The actions on receipt of a call setup request from a PRI user is dependent on the values of the Screening Indicator (SI) in the *Calling party number* information element (CPN).

- A number of additional minor technical changes have been made in this release.

August 1998

NA011 Standard NIS A211-1 Release 8

A number of minor technical changes have been made in this release.

Table of Contents

Chapter 2-3: Layer 1 electrical specification 2-9

Chapter 2-4: Layer 1 frame formats 2-15

Chapter 2-5: Layer 1 clear channel capability 2-21

Chapter 2-6: Layer 1 maintenance 2-23

Chapter 2-7: Layer 1 connector arrangements 2-29

3- Section 3: Layer 2 specification for primary rate interfaces 3-1

Chapter 3-1:
Introduction to Layer 2 3-5

Chapter 3-2:
Layer 2 frame structure 3-9

Chapter 3-3:

Layer 2 elements of procedures 3-15

Chapter 3-4:
Layer 2 elements for layer-to-layer communication 3-29

Chapter 3-5:
Definition of peer-to-peer procedures for Layer 2 3-35

Chapter 4-3:
Layer 3 message functional definitions 4-11

Chapter 4-4:
Layer 3 message formats 4-37

Chapter 4-5:
Layer 3 call control procedures 4-113

Chapter 5-3: Called number delivery 5-19

Chapter 5-4: Network redirection and reason 5-21

Chapter 5-5: Network name 5-37

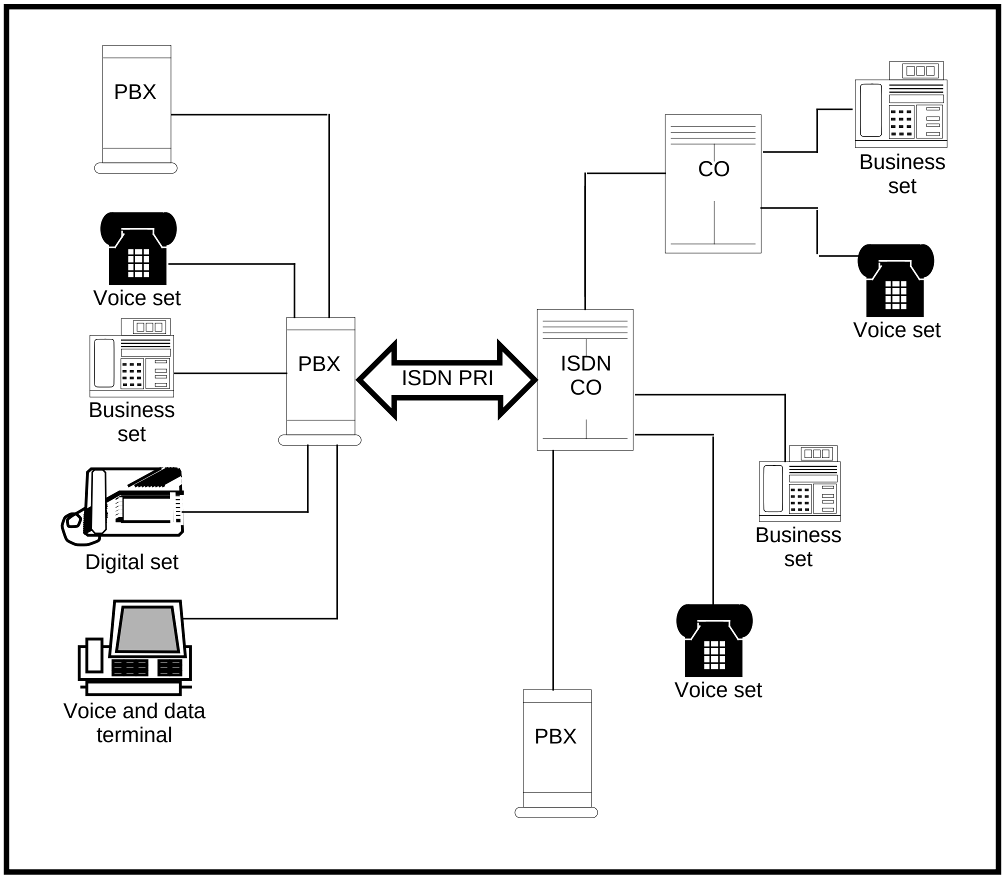
Chapter 5-6: Network ring again 5-59

Chapter 5-7: Network automatic call distribution 5-73

About this specification

This document contains the specification for the Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) user-network interface between the Northern Telecom ISDN DMS-100 switch and user equipment. The interface described in this document is based on the CCITT ISDN I and Q Series Recommendations, ISDN Standards established by ANSI/ECSA-T1, and the National ISDN-1 basic call and supplementary services requirements as specified in Bellcore Special Report SR-NWT-001937.

Figure 1
ISDN PRI service



Scope

This specification describes the distribution of services across a network, highlighting the connectivity between a central office (CO) and a user (for example, a private branch exchange). This provides the basis for the definition of ISDN call control for PBX to CO applications and, hence, the signaling protocol requirements for PRI.

In the definition of PRI services, full consideration has been given to the requirements to provide end-to-end service for all users (for example, the need to connect a station user on a PBX to another station user on a CO or Centrex switch).

Structure of document

This specification contains five sections:

- Section 1: Introduction
- Section 2: Layer 1 specification for primary rate interfaces
- Section 3: Layer 2 specification for primary rate interfaces
- Section 4: Layer 3 call control signaling
- Section 5: Supplementary services

Section 1 of this specification contains a brief description of the ISDN primary rate user-network interface on DMS-100, including PRI structure, network configurations and basic connection service.

Service compatibility

The ISDN Primary Rate service and signaling protocol described in this document is aligned as closely as possible to the requirements of National ISDN-1 as specified in SR-NWT-001937, and to the emerging North American (ANSI/ECSA-T1) and International (CCITT) standards.

Since several of the PRI supplementary and maintenance services are defined prior to the emerging standards, extensions to standardized protocol elements have been used when necessary to provide these services.

Section 1: Introduction

Chapter 1-1: Overview of PRI 1-3

Chapter 1-1: Overview of PRI

This chapter provides an overview of the primary rate interface (PRI) in the telecommunications network, and describes how PRI interworks with other network facilities.

1.1 PRI structure

The basic PRI structure consists of 23 B-channels and a D-channel, for a total transmission rate of 1544 kbit/s, which is equivalent to a DS-1. Each 64 kbit/s B-channel carries user information such as voice calls or circuit switched data. The D-channel is a 64 kbit/s channel that is used to carry the control or signaling information.

B-channels can be combined using the multirate service to achieve user information rates of 128 to 1536 kbit/s. In addition, H0 channels (384 kbit/s) and H11 channels (1536 kbit/s) are supported.

A D-channel may also support the signaling requirements of B-channels on other DS-1 interfaces in addition to the B-channels located on the same DS-1 as the D-channel. This configuration is called non-facility associated signaling. DMS-100 supports a maximum PRI structure that consists of 479 B-channels plus one D-channel. The one D-channel provides the signaling for all the B-channels. For increased reliability in larger PRI configurations, a backup D-channel can be assigned on a DS-1 different from the one for the primary D-channel. The backup D-channel becomes active if the DS-1 containing the primary D-channel fails, resulting in no loss of service.

1.2 Network configurations

When PRI is used to connect a private branch exchange (PBX) to a central office (CO), the following configurations are supported

- access to public network services (see Figure 1-1 on page 1-4)
- logical private network connection to central exchange (Centrex) users (see Figure 1-2 on page 1-4)

When PRI is used as a logical private network connection, the PBX and Centrex are considered as peer switches and play a similar role in the provision of private network services (see Section 5 of this specification).

Figure 1-1
PRI provides access to the public switched telephone network

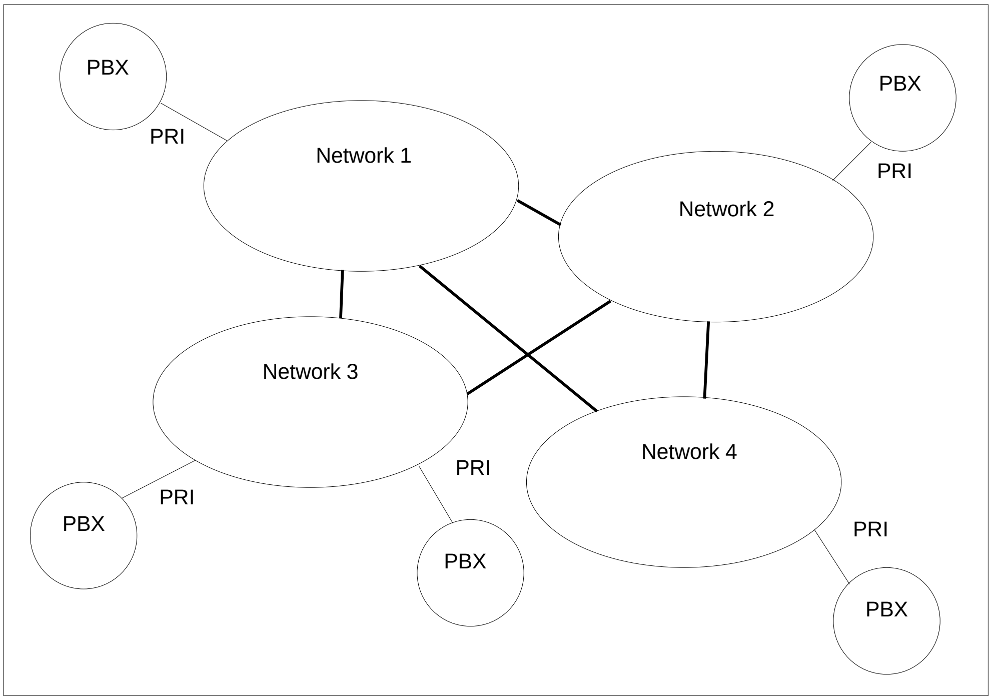
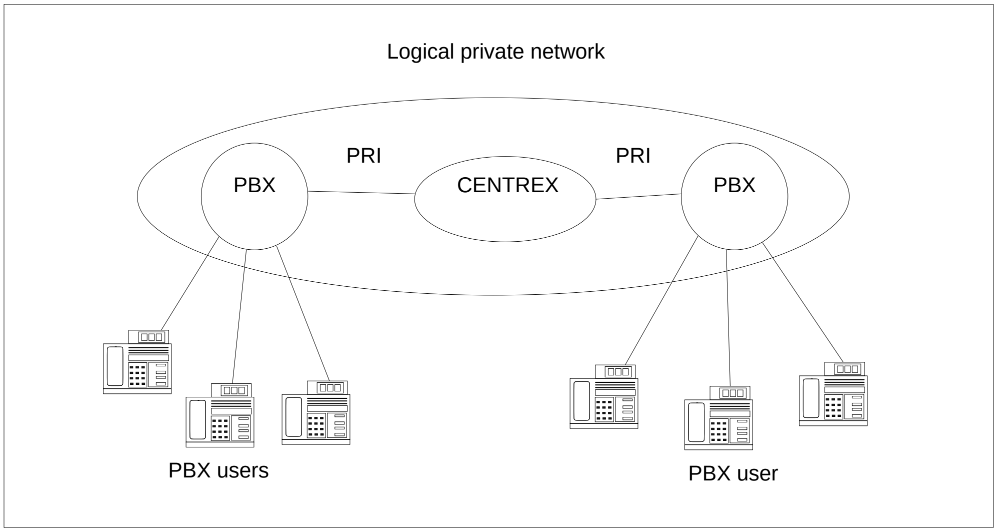


Figure 1-2
PRI distributes services in a private network



1.3 Connection types

The basic connection service provides two types of connections

- switched
- permanent

1.3.1 Switched connections

Switched connections are set up under control of the user, using D-channel PRI Layer 3 signaling. The user provides the appropriate call establishment information in a connection request, which includes a destination address, the bearer service and the B-channel for each call.

1.3.2 Permanent connections

Permanent connections are nailed-up or provisioned connections between a B-channel on a PRI and a trunk or a line interface (including a B-channel on another PRI). The capability of the permanent connection to carry the different bearer services is dependent on the information transfer capability of the end-to-end connections.

A permanent B-channel shares the same characteristics as a switched B-channel, except they are provisioned by service order. That is, D-channel call control signaling does not apply to permanent connections.

To establish a permanent connection, the address associated with the connection may not uniquely identify the endpoints of the connection and further qualification is needed (for example, local switch loop numbers and B-channel number in ISDN PRI).

The addresses associated with permanent connections should have a single appearance.

A permanent connection between a PBX and a public network service does not constrain the PBX from associating any PBX user access interface with the permanent connection.

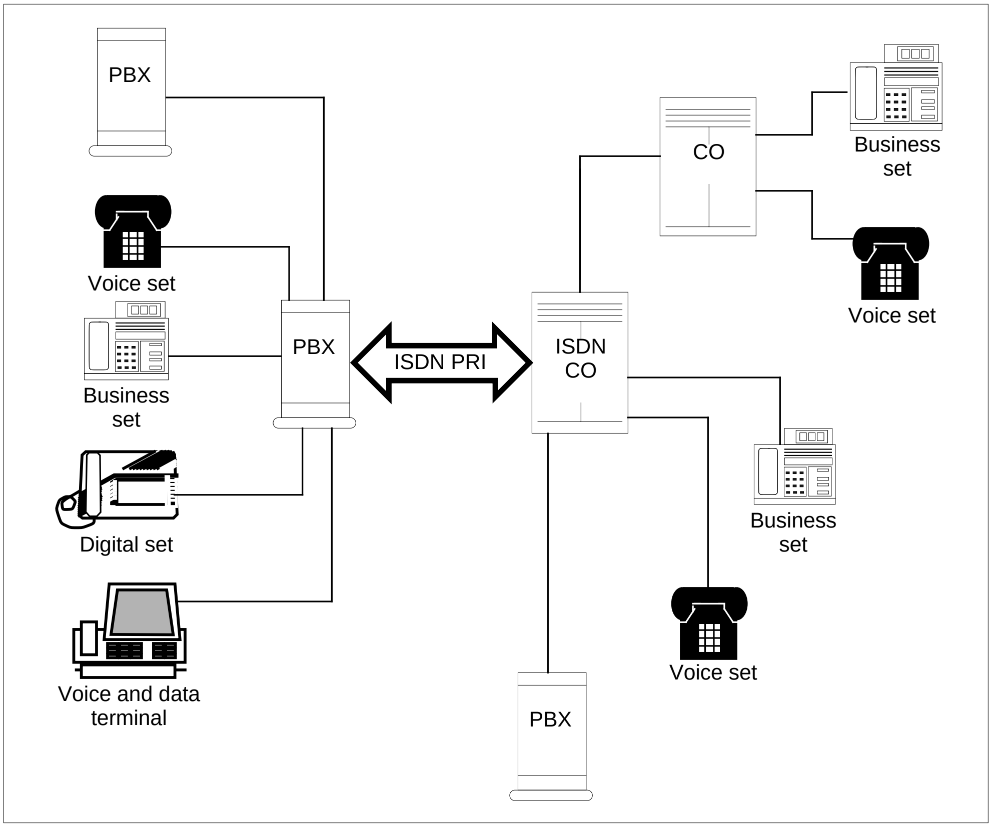
1.4 Bearer services

In an ISDN, each end-to-end connection has associated with it a specific bearer service. The bearer service must be specified to allow the network to reserve the appropriate circuits. Bearer services can be generally divided into voice and data categories. These are described further in the following sections.

1.4.1 Voice terminal connectivity

Figure 1-3 on page 1-6 shows the end-to-end connection of voice terminals in a typical ISDN network.

Figure 1-3
Voice terminal connectivity



For voice connections, the following bearer services are supported

- speech
- 3.1 kHz audio

The default bearer service that is used in the case of interworking with the public network is the 3.1 kHz audio bearer service.

The speech bearer service has the following characteristics

- information transfer rate of 64 kbit/s
- information transfer capability of speech
- user information Layer 1 protocol of μ-law speech

The 3.1 kHz audio bearer service has the following characteristics

- information transfer rate of 64 kbit/s
- information transfer capability of 3.1 kHz audio

- user information Layer 1 protocol of μ-law speech

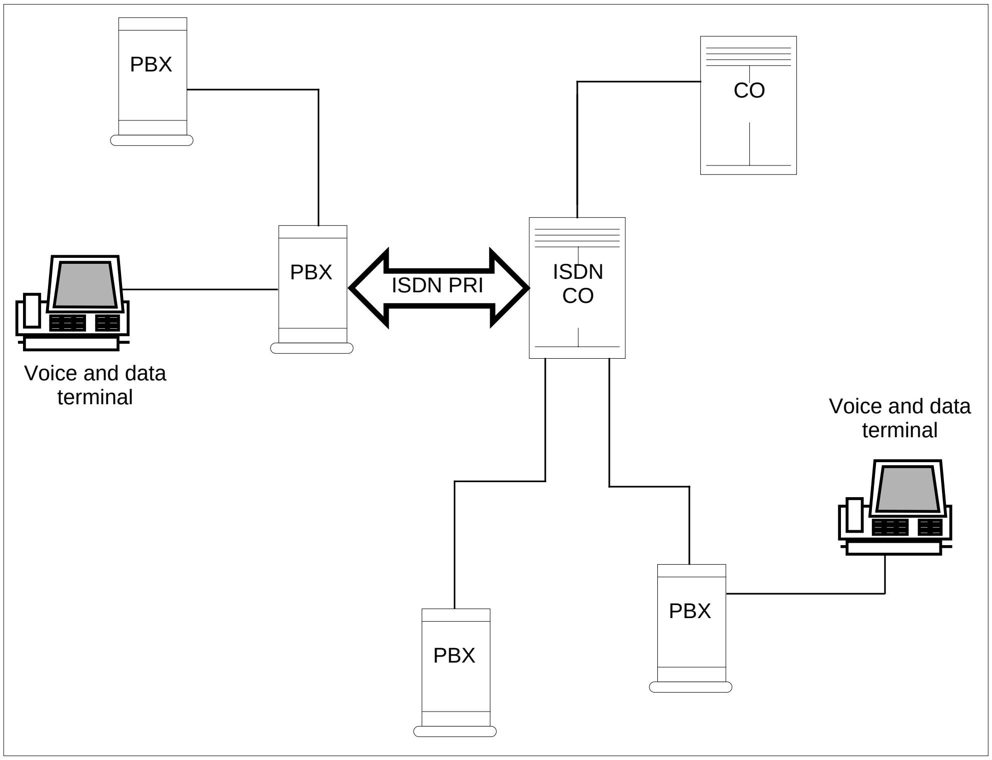
Layer 1 μ-law coding is in accordance with CCITT Recommendation G.711.

> ***Note:*** The 3.1 kHz audio bearer service can be used to support voice band (analog) data.

1.4.2 Digital data terminal connectivity

Figure 1-4 shows the end-to-end connection of digital data terminals in a typical ISDN network.

Figure 1-4
Data terminal connectivity



For digital data connections, the following bearer services are supported

- unrestricted digital information
- restricted digital information

The unrestricted digital information bearer service has the following characteristics

- information transfer rate of 64 kbit/s, multirate, 384 kbit/s or 1536 kbit/s

  Multirate, 384 kbit/s and 1536 kbit/s information transfer rates allows higher bandwidth digital data by combining multiple 64 kbit/s channels. Multirate allows the combining of 2 to 24 B-channels, which supports data rates from 128 to 1536 kbit/s.
- information transfer capability of "unrestricted digital information"

  This allows the digital data to be routed over facilities that support the B8ZS transmission scheme. This transmission scheme does not require zero code suppression and it allows 64 kbit/s clear data to be transmitted.

  When unrestricted digital information is specified, the user information Layer 1 protocol and user rate may be omitted.
- user information Layer 1 protocol of "CCITT rate adaption"

  This parameter specifies that the 56 kbit/s data rate adaption scheme used is a CCITT standard (CCITT Recommendations I.463 or V.110) which sets every 8th bit to "1".

  The advantage of setting the 8th bit to "1" is that it meets the current ZCS ones density requirements, and allows transmission of the user's data over transmission facilities using in-band A/B bit signaling (which robs bit 8).
- user rate of 56 kbit/s

  The user rate specifies the data transfer rate to be used.

An information transfer capability of "restricted digital information" allows digital data to be routed over T1 facilities with a restricted data transfer capability. The restriction is that some transmission facilities require a certain "ones density" (that is, no more than 15 consecutive zeros) or they may lose synchronization. To avoid losing synchronization they use the Zero Code Suppression (ZCS) coding method which inserts a "1" into the bit stream, as required, which would corrupt the user's digital data at rates over 56 kbit/s.

When restricted digital information is specified, the user information Layer 1 protocol and user rate are omitted.

1.4.3 Packet handler access

DMS-100 supports permanent B-channel connections to a remote packet handler, such as the DPN-100 packet switch. Both X.25 and X.75 services are supported on these connections.

1.4.4 Frame relay access

DMS-100 supports switched B-channel access to Frame Relay service, with the following attributes

- maximum data rate of 56 kbit/s
- unique network address for each Frame Relay port
- each Frame Relay port supports subscribed permanent virtual circuits

Further information on Frame Relay access on PRI can be found in the Northern Telecom document NIS S215-1, Issue 2.0, “DataSPAN Frame Relay UNI Specification.

1.5 Numbering plans and dialing plans

There is a clear distinction between dialing plans and numbering plans. The following definitions will be used throughout this specification:

1.5.1 Numbering plans

A numbering plan defines the network address of a user and is used for routing within the network. Numbering plans are internationally standardized (for instance, CCITT Recommendation E.164).

To support both public and private network calls, two numbering plans are used to address end-users of the basic connection service. Each numbering plan is identified by a Numbering Plan Identification (NPI).

- NPI of “ISDN/telephony numbering plan E.164/E.163”

  Public network users will be allocated numbers from the CCITT Recommendation E.164 ISDN numbering plan. E.163, the pre-ISDN telephony numbering plan, is a subset of E.164.

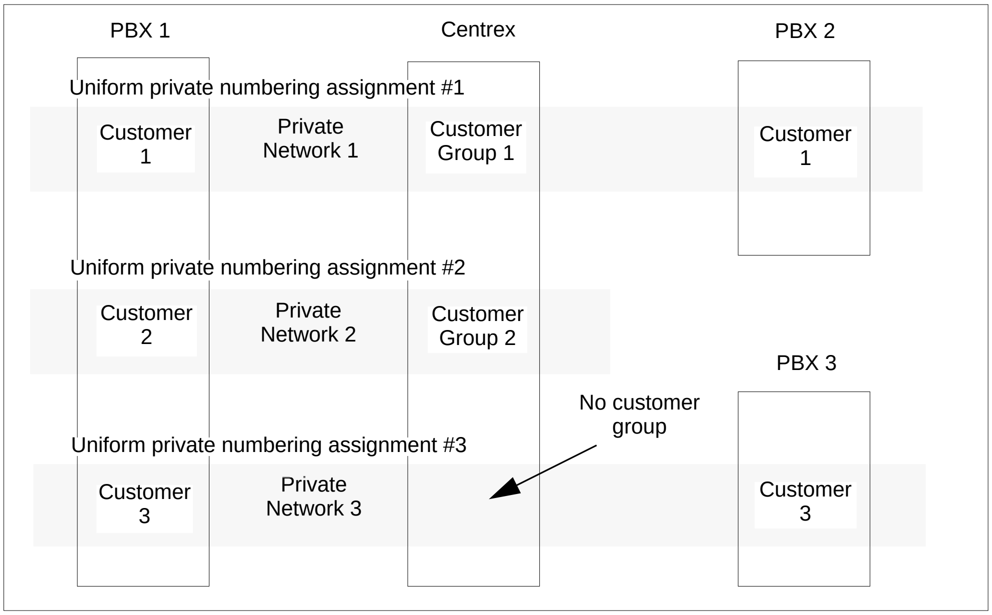
  Note: A PBX as a user of the PSTN may have one or more E.164 numbers associated with it, that is, one or more Listed Directory Numbers (LDNs) and PBX stations with Direct Inward Dialing (DID) numbers.

- NPI of “Private numbering plan”

  PBX users and Centrex users may be allocated numbers conforming to a private numbering plan. These numbers may be arranged in a uniform numbering plan between PBX and Centrex users as provided by the Meridian Switched Network (MSN) numbering plan.

A PBX may support multiple customers and multiple private networks, as shown by the example in Figure 1-5.

Figure 1-5
Multiple private networks on PBX and Centrex



Note: Until appropriate standards have been agreed, many customers sharing a PBX will typically have their own PRI services.

1.5.2 Dialing plans

A dialing plan defines the digits that a terminal user should dial to establish a connection or to access a service. Dialing plans may include prefix digits and special numbers. Private dialing plans, which may be used by PBX and Centrex users, are not subject to standardization.

In ISDN signaling, dialing plan digits are carried within information elements. These digits request the functions implied by the digits dialed, and are not necessarily part of the numbering plan. In most cases, users will access the basic connection service by using a dialing plan which contains additional information or special numbers (for example 0, 411, 9+..., etc.) that are not part of the numbering plan.

1.5.3 Conversion of a dialing plan to a numbering plan

It is necessary to convert the dialing plan in use by the user to a network numbering plan, either private or public, to allow the call to be routed by the network.

Figure 1-6 on page 1-11 shows an example of how a user's dialed digits can be converted to a network numbering plan.

Figure 1-6
Conversion of a dialing plan into a numbering plan

On a typical terminal connected to a PBX, the user dials the digits

10573

The PBX recognizes the customer as a member of Group 1. The Group 1 translation table indicates that the initial **1** in the number should be replaced with the following digits

919-992

Thus, the complete numbering plan number that is used to route the call is

919-992-0573

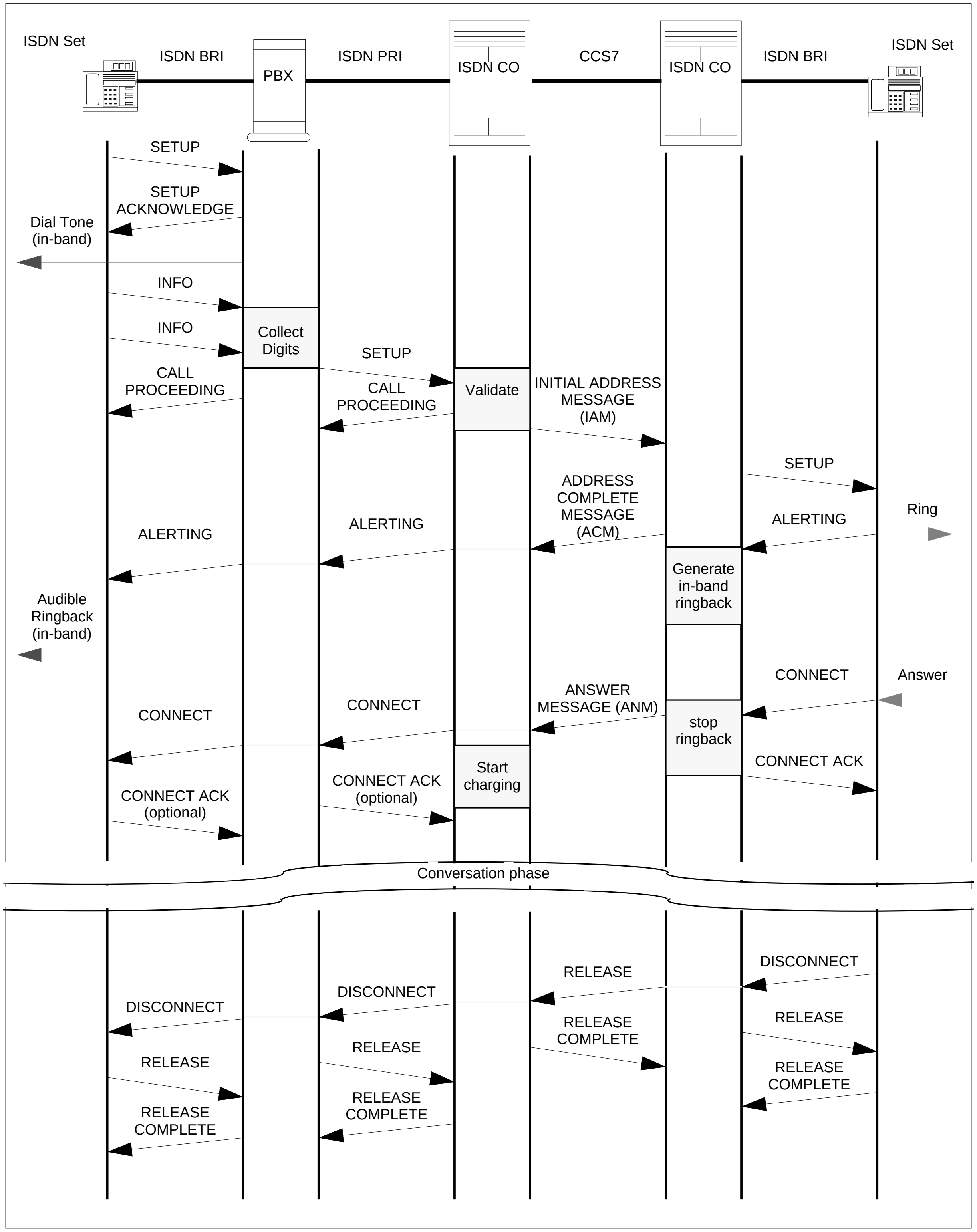
1.6 Basic connection service

The objective of the basic connection service is to connect voice or data terminals in cooperation with existing public and private networks. The following basic functions are supported to accomplish this goal

- selection of connection facilities
- progress reporting and cut-through
- conversion between dialing plans and numbering plans
- channel allocation
- interworking with other trunk types, such as analog trunks, digital trunks with A/B-bit signaling and CCS7 trunks

See Figure 1-7 on page 1-12 for normal message flows associated with the basic connection service, including interworking with ISDN BRI terminals and CCS7 network signaling.

Figure 1-7
Basic connection service: normal call setup and release message flow



1.6.1 Selection of connection facilities

By default, when the called party number has an NPI of “E.164”, public switched network facilities are selected to route the call and support the connection. Similarly, when the called party number has an NPI of “Private” (for a private network), reserved private facilities may be selected. For example, PBX tie trunks or reserved CO tie trunks within the public network.

1.6.2 Progress reporting and cut-through

The philosophy of the basic connection service is to move, as far as possible, to the target ISDN solution with only out-of-band D-channel and CCS7 signaling. The user interface to terminals is to be driven as close as possible to the user. For example, ISDN terminals will receive the out-of-band signals and generate the appropriate displays, audible tones and announcements, etc. For other terminals, the user interface would be generated from the local switch. This objective allows for customization consistency of the user interface. For example, since the local switch creates the custom user interface, if a call is made to a foreign country, the local switch would receive the out-of-band messages and translate them to locally generated tones, English announcements and English displays (assuming that English is the user’s desired language).

Some exceptions to the rule above have been made to permit interworking with non-ISDN network trunks (for example, DS-1 with A/B-bit signaling) and to overcome engineering problems. These special cases are:

- When a call is set up between an ISDN network and a non-ISDN network, call progress signaling reverts to “far-end” in-band signaling (for example, busy tone, audible ringing, and announcements). A progress report is always sent back to the originating party indicating that interworking with non-ISDN facilities has occurred.
- In order to provide consistent operation to non-ISDN terminals, the local switch translates ISDN messages and progress reports to the appropriate protocol on the terminal access interface. For example, it will translate an ISDN *DISCONNECT* message to a busy tone. The general rule in an ISDN network is that, as a call progresses through the ISDN, the circuit is cut through in both directions at the originating and intermediate switches. Cut-through at the terminating switch to the terminating access interface occurs when the called terminal indicates it is connected to (accepts) the call. This introduces a short clipping delay as there is a race condition between the connected indication arriving and being acted upon in the D-channel and the user talking on the B-channel.

  However, a major clipping problem is introduced if near-end audible “ringback” is generated on receipt of the D-channel *ALERTING* message. The circuit cannot be cut-through to the far-end if the near-end supplies a ringback generator. The *CONNECT* message has to be forwarded across the ISDN network, to switch out the ringback generator, before cut-through is achieved. For this reason, audible ringback, when needed, will always be generated in-band from the far end.

To allow the generation of tones and announcements from the terminating switch, the intermediate switches cut through the B-channel on successful B-channel selection.

1.6.3 Conversion of a dialing plan into a network numbering plan

PBX users and Centrex or CO users that have simple terminals supply routing and destination information to the basic connection service by supplying digit strings in conformance to the network dialing plan. The dialed digits must be converted into information elements in a *SETUP* message for routing and conveyance through the ISDN network. This conversion is done by the originating switch (PBX or CO) supporting the non-ISDN user access interface. Some conversion from an ISDN BRI interface at the originating switch may also be required (for example, converting dialing plan to numbering plan).

The following fields are provisioned in the PBX to allow the user to define how the dialing plan is converted into ISDN information:

- Network Specific Facilities (NSF): is used to select between reserved private network or PSTN facilities for routing the call. It is also used to select specific Tie Trunk, FX, and WATS facilities.
- Number, address, directory number: a string of digits conforming to a standardized numbering plan (for example, E.164) or a private numbering plan.
- Numbering plan identification (NPI): private or E.164 numbering plan.
- Type of number: “subscriber number”, “national number”, “international number”, or “unknown”.
- Transit Network Selection (TNS): specifies which carrier to use for routing, when required.

The following rules are used by the network for calls received from PRI users to determine numbering plan and routing information. The PRI user should encode the *SETUP* message for outgoing calls according to these requirements for desired services. Customer-specific dialing plans to access private facilities must be arranged with the network by subscription.

Digit strings are encoded in the number digits field of the *Called party number* information element. It is assumed that 6 and 9 are digits which select private and public numbering plans, respectively. In practice, the actual digits used are assigned by the customer through service orders/changes. Details of the encoding of the referenced information elements can be found in Section 4.

Detailed information on the use of NSF can be found in Section 5 of this specification in the description of Integrated Services Access.

- Binary Facility Coding Value (BFCV)

  The BFCV is in the *Network specific facilities* information element (NSF).

  - First digit is “6”: BFCV of “Private” (optional if the NPI is “Private”)
  - First digit is “9”: no NSF is included for public calls
  - Specific trunk access code digit(s): BFCV of “Private”, “Tie Trunk”, “FX” or “OUTWATS”, as appropriate, and the NSF service identifier is set to a specific facility or trunk group within the given BFCV (for example, OUTWATS band).

- Numbering Plan Identification (NPI)

  The NPI is in the *Called party number* information element.

  - First digit is “6”: NPI is “Private” or “E.164”, depending on subsequent number analysis
  - First digit is “9”: NPI is “E.164”

- Type of Number (TON)

  The TON is in the *Called party number* information element.

  When the NPI is “Private”, the TON is “Subscriber”. When the NPI is “E.164”, the TON is set as follows:

  - less than 10 digits: TON is “Subscriber”
  - exactly 10 digits: TON is “National”
  - more than 10 digits: TON is “International”
  - Special Number Services (for example, 0, 411, 911, etc.): TON is “Subscriber”

- Carrier Identification Code

  For equal access public calls (NPI of “E.164”), the PRI user can explicitly specify a carrier. The carrier identification code can appear in the *Called party number* information element as part of the digit string (for example, 9+10XXX, where XXX is the carrier identification code) or in the *Transit network selection* information element.

1.6.4 Channel allocation

Where there is a choice of channels to be allocated, the equipment routing the call (for example, the terminal or switch) allocates the outgoing channel. That is, the PBX usually allocates channels on the PRI for calls originating from the PBX, and the CO allocates channels on calls terminating to the PBX.

In the event of “glare” (channel contention) one end of the channel or trunk must be preconfigured as the “master”. The master is set to win all contentions.

To minimize the possibility of glare, both ends should allocate channels in a complementary fashion. For example, the “master” should allocate channels in ascending order and the “slave” in descending order. In this specification, the CO is always the “master”.

1.7 Supplementary services

In addition to the basic connection service, PRI supports a number of supplementary services. These consist of both services visible to end users and those that are only accessible by operations personnel responsible for management of the PRI.

User services supported in this specification are

- calling number delivery
- called number delivery
- network redirection and reason
- network ring again
- network automatic call distribution
- equal access
- special number services
- integrated services access
- network message service
- release link trunk

Administration services supported in this specification are

- backup D-channel
- private network hop-off
- private network overflow
- integrated trunk access

Detailed descriptions of the supplementary services are in Section 5 of this specification.

Section 2:
Layer 1 specification for primary rate interfaces

Chapter 2-5:
Layer 1 clear channel capability 2-21

Chapter 2-6:
Layer 1 maintenance 2-23

Chapter 2-7:
Layer 1 connector arrangements 2-29

Chapter 2-1:
Layer 1 introduction

This section defines the physical layer of the ISDN primary rate interface (PRI) between a central office (CO) and a private branch exchange (PBX). The physical layer consists primarily of a standard DS-1 interface; however there are some configuration differences caused by regulatory conditions attached to the CPE functionality, that is, the need for Network Circuit Terminating Equipment (NCTE). There are a number of DS-1 options which have to be specified for this application.

This specification is based on ANSI T1.408, which describes the PRI layer 1 characteristics. Various annotations and additions are included herein which reflect Northern Telecom's implementation of the applicable standards.

This section includes

- a general description of the interface and configuration
- an electrical definition including formats for the data link (DL)
- a physical definition of connectors

1.1 Technical conformance

All products which fully conform to this specification implement DS-1 with the following schemes:

- bipolar coding with 8-zero suppression (B8ZS)
- zero code suppression (ZCS), with bit insertion

  Note: Although the ISDN PRI standard requires the support of 64 kbit/s unrestricted/clear information transfer for a DS-0 channel (which requires B8ZS), the current ZCS scheme is also supported since many existing DS-1 transmission facilities do not yet support B8ZS. Provision of ZCS avoids the need for the telephone company to have to replace the ZCS equipment. It also avoids restricting PRI to a clear channel service.

Bit-robbed signaling (for example, A/B bits) are supported on a per DS-0 channel basis, allowing ISDN PRI DS-0 channels (that is, B- and D-channels) to be intermixed on the same DS-1 facility as conventional trunks.

Additionally, a DS-0 nominated as the ISDN PRI D-channel must be able to transmit data at 56 kbit/s (by setting bit 8 to “1”) or at 64 kbit/s clear.

> ***Note:*** A D-channel with a transmission rate of 56 kbit/s (by setting bit 8 to “1”) is needed for ISDN PRI configurations where the deployed transmission facilities require the use of ZCS coding.

1.2 Standards compatibility

The network interface is based on

- ANSI T1.403, Carrier to customer installation — DS-1 metallic interface specification, 1989
- ANSI T1.408, ISDN primary rate — customer installation metallic interfaces Layer 1 specification, 1990
- FCC Part 68 Subpart D
- EIA PN 1378 Section 4.13 Page 204, Synchronization
- “Digital Synchronous Network Plan”, Bell Labs Technical Reference PUB60110.
- “High Capacity Digital Service Channel Interface Specification”, Bell Labs Technical Reference PUB62411

The interface does not support the following features (for further information, see the following chapters)

- extended super frame data link message-oriented code words
- extended super frame data link bit-oriented code words other than remote alarm indication (RAI)
- line and payload loopbacks

Chapter 2-2: Layer 1 general information

2.1 Architecture

This specification defines the physical DS-1 interface including the DS-0 channels used by the ISDN B-channels, D-channels and conventional bit-robbing trunks to transmit information. Figure 2-1 shows the ISDN PRI functional architecture.

Figure 2-1
ISDN PRI architecture

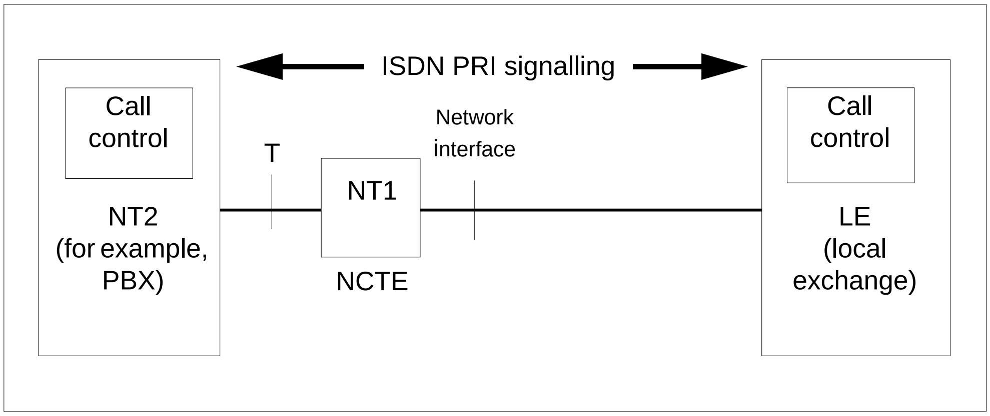
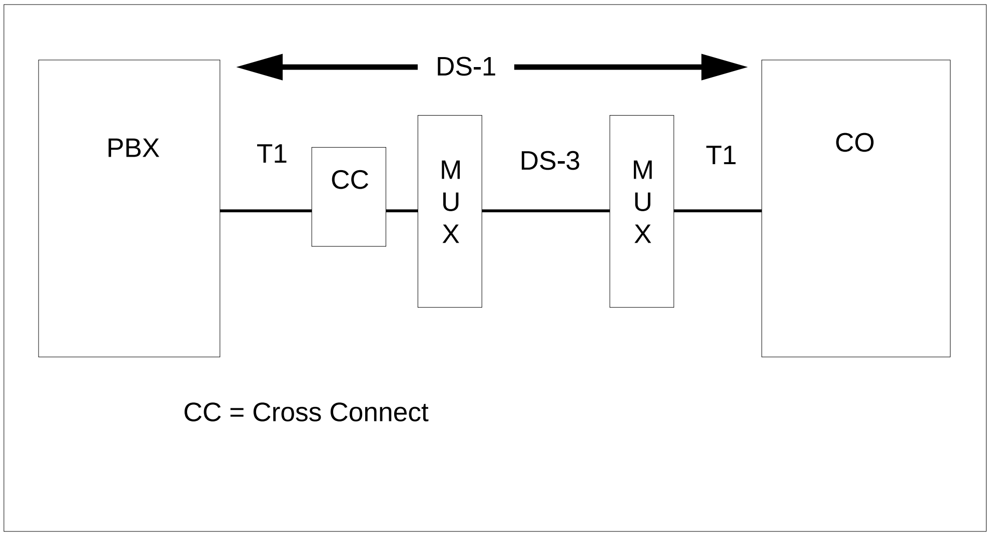


Figure 2-1 shows a network view of the physical architecture.

Figure 2-2
Network view of ISDN PRI functionality



2.2 Services offered by the physical layer

The physical layer DS-1 facility provides the following services to the higher layers. These services are dependent on the DS-1 facility options being used.

- DS-1 with B8ZS and extended superframe (ESF)

  This DS-1 option set conforms to the ISDN PRI standard as defined in ANSI T1.408, ISDN primary rate—customer installation metallic interfaces Layer 1 specification. The DS-0 channels may be used for ISDN PRI (B-channels or D-channels) or for conventional bit robbing signaling trunks with A/B/C/D bit signaling or A/B signaling. The DS-0 channels used for ISDN PRI have the capability to support an information transfer rate of 64 kbit/s unrestricted. An end-to-end 64 kbit/s connection requires the access and network connections to support the 64 kbit/s capability.

  Note: The use of the ESF format also provides a special data link which may be used for link management (for example, alarm indication, loopback set up, performance reporting).

- DS-1 with ZCS and standard framing (SF)

  This DS-1 option set permits DS-0 channels to be used for ISDN PRI (D-channels or B-channels) with an information transfer rate of up to 56 kbit/s (by setting bit 8 of each byte to “1”), and for conventional trunking with A/B bit signaling.

Note: In general, the ISDN PRI DS-0 channels may be used for a restricted 64 kbit/s information transfer service provided that “1”s density requirements of current ZCS are met to prevent “1”s insertion, and out-of-band signaling is used.

2.3 Layer 1 signaling

This section defines the characteristics of the metallic interface between a carrier and customer installation (CI), referred to as the network interface (NI), at the DS-1 level. It establishes requirements at the NI necessary for compatible operation between the Carrier and the CI.

The signals at the network interface, described in the following chapters, are of two types:

- normal operating signals
- maintenance signals

Signals that appear as a result of the environment (for example, voltages and currents induced by lightning hits) are not covered.

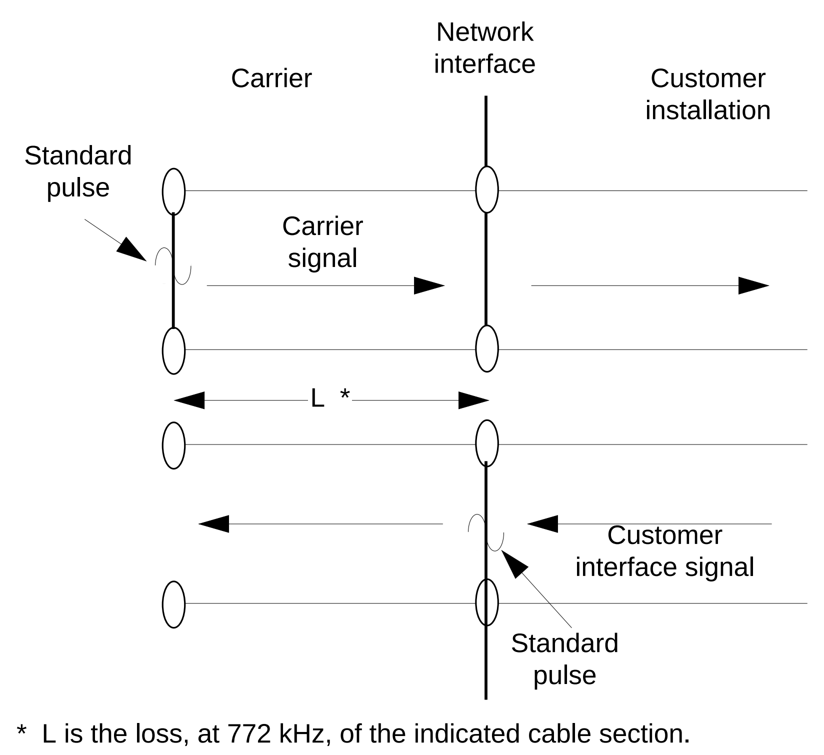
The specification covers the 4-wire DS-1 interface based on the various digital facilities currently in use. Physical arrangements, electrical parameters, signal formats and maintenance protocols are described.

Chapter 2-3:
Layer 1 electrical specification

3.1 Introduction

The Layer 1 electrical specification describes the DS-1 signals delivered to the carrier and to the customer installation (CI) at the network interface (NI). The NI is shown in Figure 2-3. The signal delivered to the NI by the carrier is identified as the carrier signal, and the signal delivered to the NI by the CI is identified as the CI signal. The NI, as defined in this document, is not symmetrical. That is, at the NI, some of the electrical requirements of the carrier signal differ from those of the CI signal.

Figure 2-3
Network interface



* L is the loss, at 772 kHz, of the indicated cable section.
0.0 < L < 16.5 dB

3.2 Impedance matching

Exchange cables generally used by the carriers in the loop plant are non-loaded, staggered-twist paired cables. The characteristic impedance of these cable pairs and the impedance of their associated terminations at 772 kHz is nominally 100 ohms[1].

3.3 Signal specifications

The following signal specifications describe characteristics for all signals at the NI. Differences between the carrier and the CI signals are identified in sections 3.4 and 3.5.

3.3.1 Transmission rate

The transmission rate of the DS-1 signal is 1.544 Mbit/s ± 50 bit/s. Older equipment has rate variations of ±200 bit/s.

3.3.2 Line codes

The line code for the DS-1 signal is bipolar, except where intentional bipolar violations are introduced by B8ZS.

3.3.3 Test load

A termination of 100 ohms ± 5% resistive is used at the network interface for the evaluation of signal characteristics.

3.3.4 Standard pulse characteristics

3.3.4.1 Pulse shape

An isolated pulse, both positive and inverted negative, has an amplitude between 2.4 V and 3.6 V and fits the normalized template shown in Figure 2-4 when scaled by a constant factor. Table 1-1 and Table 1-2 define the corner points of the pulse template.

3.3.4.2 Power levels

For an all “1”s transmitted pattern, the power in the 3 kHz band centered at 772 kHz is in the range of 12.0 to 19.0 dBm and the power in the 3 kHz band centered around 1544 kHz is at least 25 dB less.

3.3.4.3 Pulse imbalance

In any window of 17 consecutive bits, the maximum variation in pulse amplitudes is less than 200 mV, and the maximum variation in pulse width (half amplitude) is less than 20 nsec.

---

[1] There may be a small number of low capacitance-type cables in the carrier’s plant. The characteristic impedance of these cables ranges from 120 to 145 ohms at 772 kHz. These cables are non-standard for this interface and, if used, must be tested on an individual basis to ensure that impedance discontinuities do not result in interface reflection losses great enough to affect the stated performance objectives.

Figure 2-4
Isolated pulse template

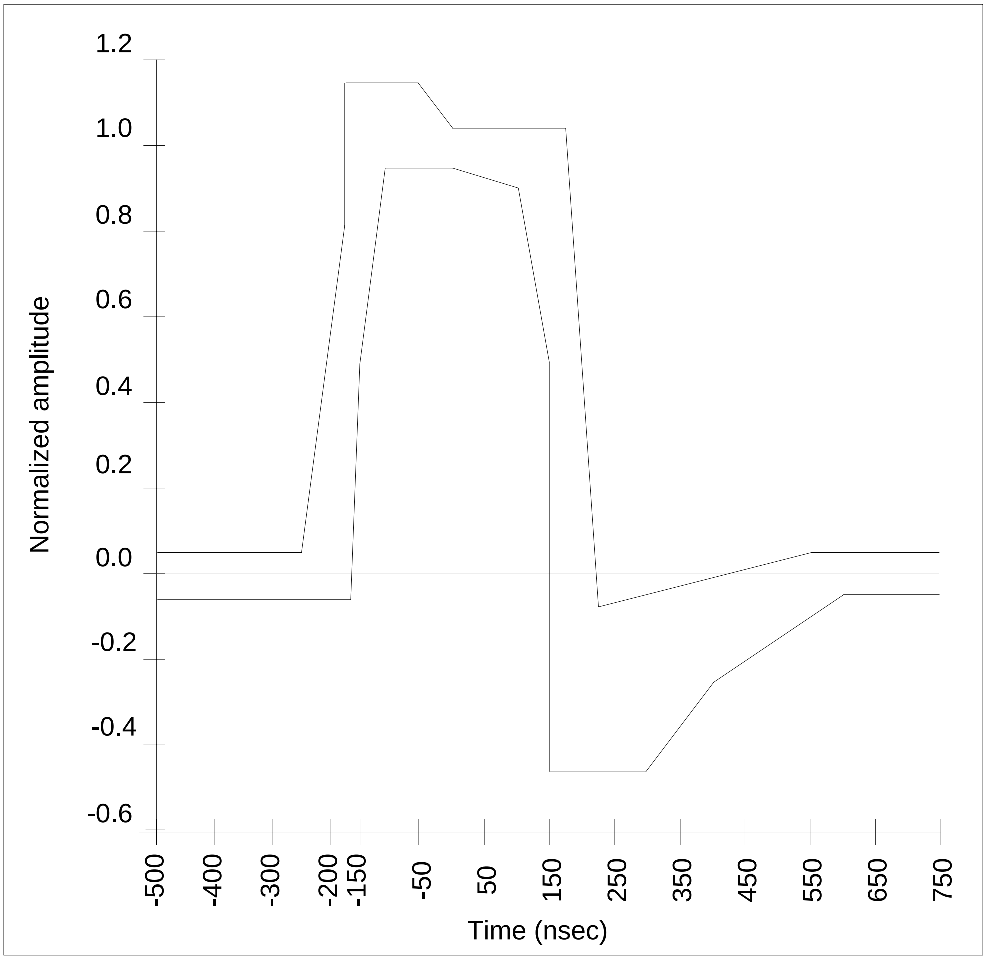


Table 1-1
Pulse template corner points: maximum curve

Time	**nanoseconds**	-500	-250	-175	-175	-75	0	175	228	500	750
	time slots	-0.77	-0.39	-0.27	-0.27	-0.12	0	0.27	0.35	0.77	1.16
Normalized amplitude		0.05	0.05	0.80	1.15	1.15	1.05	1.05	-0.07	0.05	0.05

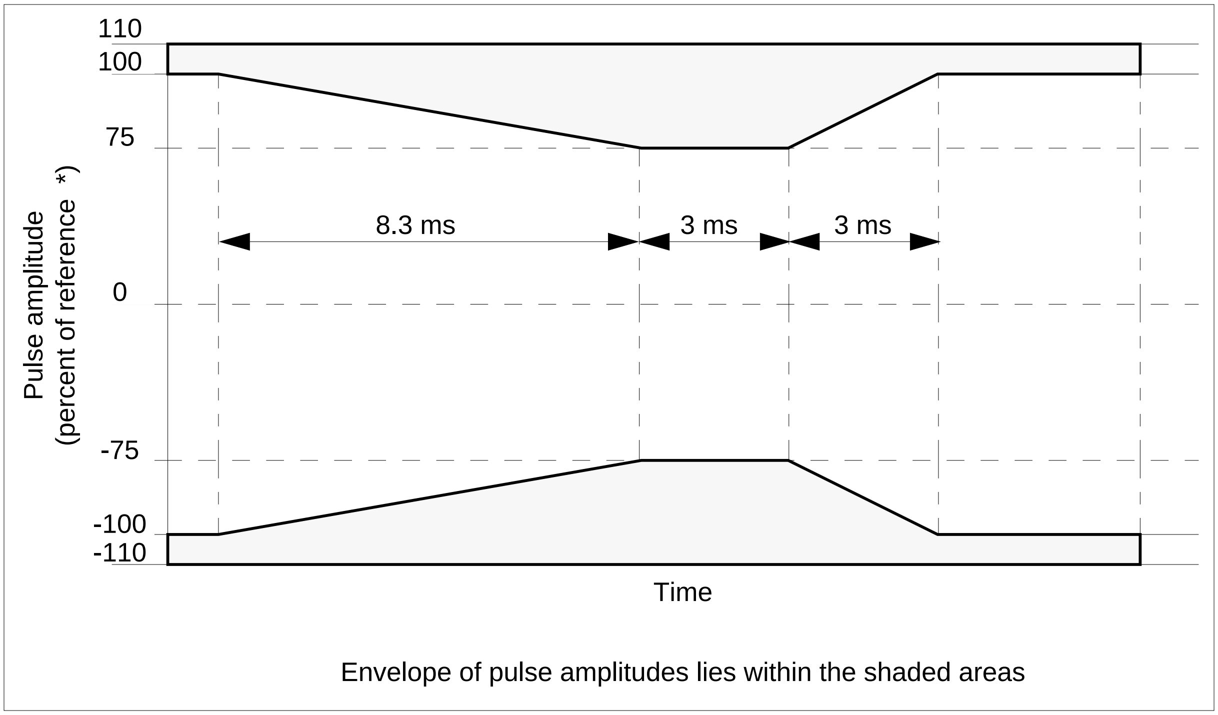
Table 1-2
Pulse template corner points: minimum curve

Time	**nanoseconds**	-500	-150	-100	0	100	150	300	390	600	750
	time slots	-0.77	-0.23	-0.15	0	0.15	0.23	0.46	0.66	0.93	1.16
Normalized amplitude		-0.05	0.50 -0.05	0.95	0.95	0.90	0.50 -0.45	-0.45	-0.26	-0.05	-0.05

3.3.5 60 Hz variations in pulse amplitude

Pulse amplitude may vary at a 60 Hz rate as a result of the presence of 60 Hz longitudinal currents in the powering loops of T1 repeaters. In such cases, the envelope of pulse amplitudes is limited as shown in Figure 2-5. Any pulse amplitude in the range of 2.4 V to 3.45 V may be used as the 100 per cent point in the figure.

Figure 2-5
Pulse amplitude envelope



Envelope of pulse amplitudes lies within the shaded areas

3.4 Signal from the carrier (carrier signal)

The carrier signal at the network interface meets the signal specifications identified in section 3.3, except that

- the pulse characteristics are those of a standard pulse (see section 3.3.4) transmitted through a cable pair with a loss in the range of 0.0 to 16.5 dB at 772 kHz between 100 ohm terminations
- the lower limit on the standard pulse amplitude is 2.25 V rather than 2.4 V

The variable length and characteristics of installed cable pairs make it impractical to define a pulse template for the carrier signal at the NI. However, the standard pulse template may be used with the appropriate mathematical procedures to construct representative hypothetical signals (see Figure 2-4). These signal constructions should be based on the approximate electrical characteristics of 100 ohm cables as shown in Appendix A of T1.403 “Carrier to Customer Installation — DS-1 Metallic Interface Specification”, 1989.

3.5 Signal from the customer installation (CI signal)

The CI should not apply voltages to the NI other than those described in this specification.

The CI signal at the NI should meet all the specifications defined in section 3.3.

3.6 Pulse density

The CI signal at the NI must contain at least one pulse in each eight-bit time slot.

3.7 Jitter and wander

The following specification provides a quantitative measurement for jitter and wander.

Jitter is defined as the short-term variations of the significant instants of a DS-1 signal from their ideal positions in time. Wander is the long-term variation of the same instants. The boundary between long-term and short-term is a frequency of 10 Hz. The magnitudes of jitter and wander are specified in terms of unit intervals (UIs). One UI is equal to 648 nsec (one pulse period).

3.7.1 Jitter

Timing jitter is specified in two frequency bands: Band 1 and Band 2. The characteristics of the weighting functions which define these bands are provided in Figure 2-6.

3.7.1.1 Carrier signal

At the NI, the jitter of the carrier signal does not exceed the following limits:

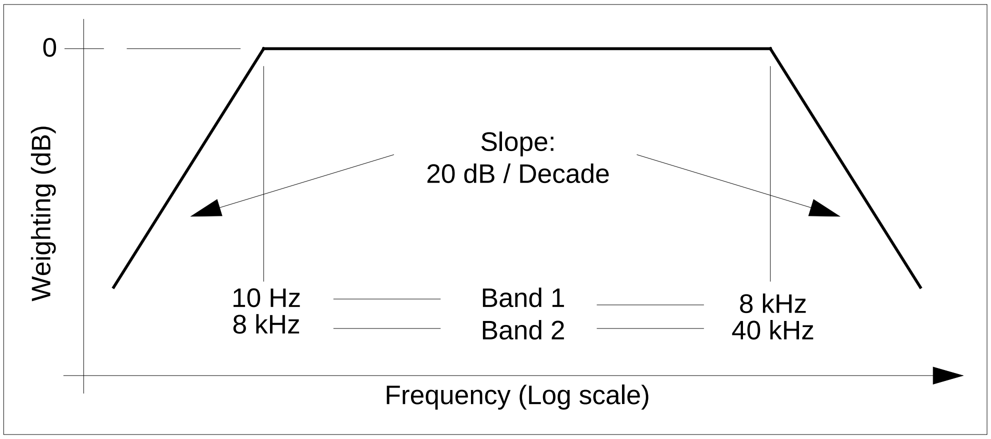
- Band 1: 5.0 UI, peak-to-peak
- Band 2: 0.1 UI, peak-to-peak

3.7.1.2 CI signal

At the NI, the jitter of the CI signal must not exceed the following limits:

- Band 1: 0.5 UI, peak-to-peak
- Band 2: 0.05 UI, peak-to-peak

Figure 2-6
Frequency weighting function for jitter



3.7.2 Wander

Wander is specified in frequency band 3. The characteristics of the weighting function which define this band are shown in Figure 2-7.

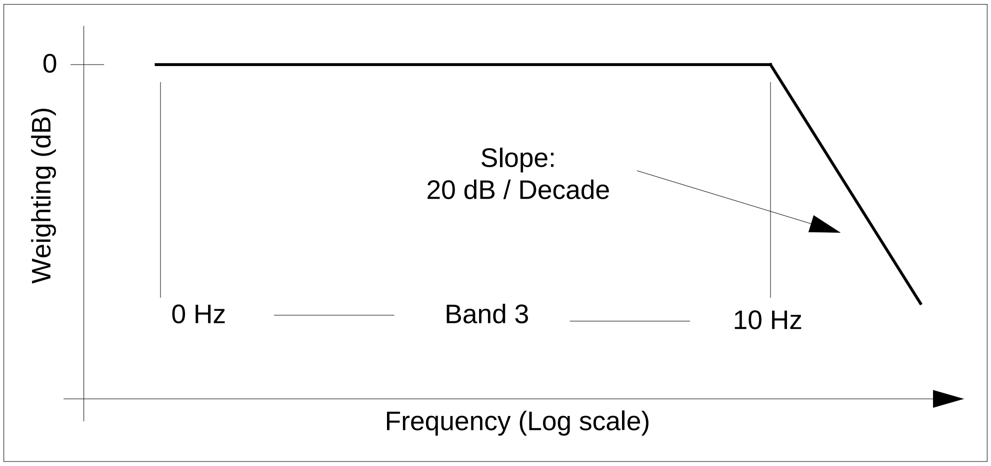
3.7.2.1 Carrier signal

At the NI, the wander of the carrier signal does not exceed 28 UI, peak-to-peak.

3.7.2.2 CI Signal

At the NI, the wander of the CI signal also must not exceed 28 UI, peak-to-peak.

Figure 2-7
Frequency weighting function for wander



3.8 Powering arrangements

Direct-current power is not delivered to the NI.

Chapter 2-4: Layer 1 frame formats

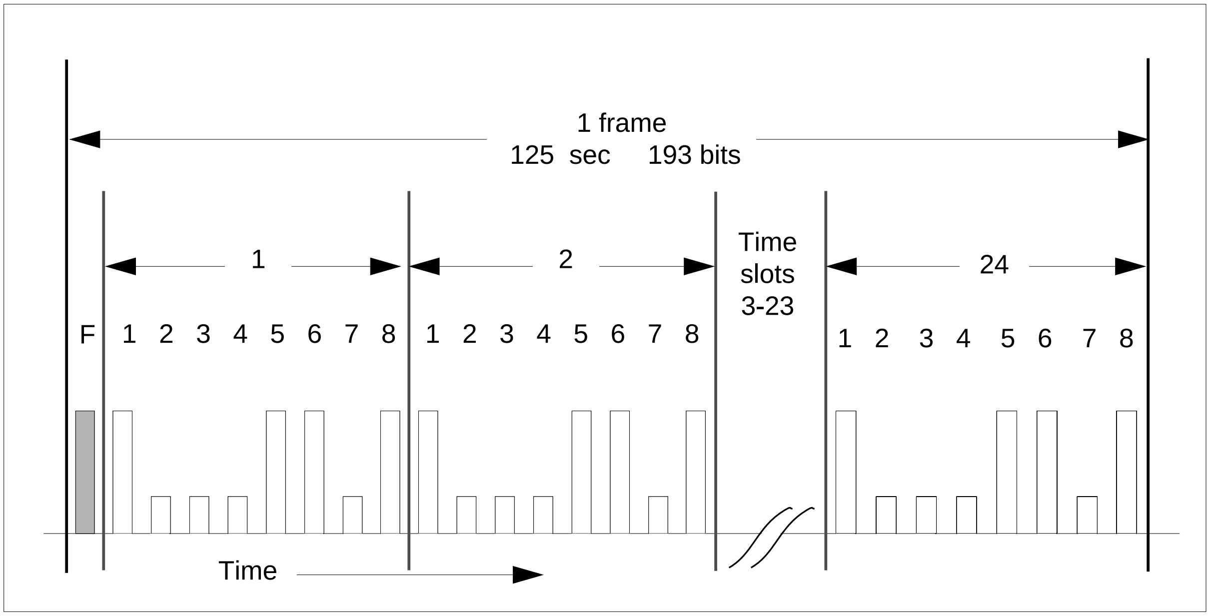
4.1 Introduction

The carrier and the CI signals at the NI are in either the superframe (SF) or the extended superframe (ESF) format. The same framing format is used in both directions of transmission.

4.2 Frame format definition

A frame is a set of 192 information digit time slots preceded by a one-digit time slot containing a framing bit (F bit), for a total of 193 digit time slots. The 192 information digit time slots may be partitioned into 24 eight-bit time slots, as shown in Figure 2-8.

Figure 2-8
DS-1 frame bit assignment



4.3 Superframe format definition

A superframe consists of twelve consecutive frames as shown in Table 1-3. The superframe format is a structure in which the F bits are used for framing only. In the superframe format, the F bits are divided into two groups

- terminal framing (Ft) bits, used to identify frame boundaries
- signaling framing (Fs) bits, used to identify superframe boundaries. (When the 192 digit time slots are channelized, the Fs bits are used to identify the robbed-bit signaling frames and associated signaling channels A and B.)

The F-bit position, with respect to every group of 192 information bits is always maintained from NI to NI or from NI to central office (CO).

Table 1-3
Superframe format

Frame no.	F bits			Bit use in each time slot		Signaling bit use options	
	Bit no.	Terminal framing bit (Ft)	Signaling framing bit (Fs)	Traffic	Signaling	T	Signaling channel
1	0	1	-	1-8	-		
2	193	-	0	1-8	-		
3	386	0	-	1-8	-		
4	579	-	0	1-8	-		
5	772	1	-	1-8	-		
6	965	-	1	1-7	8	-	A
7	1158	0	-	1-8	-		
8	1351	-	1	1-8	-		
9	1544	1	-	1-8	-		
10	1737	-	1	1-8	-		
11	1930	0	-	1-8	-		
12	2123	-	0	1-7	8	-	B

Note 1: Frame 1 is transmitted first.

Note 2: Frames 6 and 12 are called signaling frames.

Note 3: Option T - traffic (bit 8 is not used for signaling).

4.4 Extended superframe format

An extended superframe (ESF) consists of twenty-four consecutive frames. The ESF is a structure in which the F bits are used as shown below and in Table 1-4

- A 2 kbit/s framing pattern sequence (FPS) channel is used to identify the frame and the extended superframe boundaries. (When the 192 information digit time slots are channelized, the FPS bits are used to identify the robbed-bit signaling frames and the associated signaling channels, A, B, C and D.)
- A 4 kbit/s data link (DL) channel. When idle, the DL channel contains continuous repetitions of the data link idle code — 0111 1110.
- A 2 kbit/s cyclic redundancy check (CRC) channel which carries the CRC-6 code. The CRC-6 bits from ESF frame N that are transmitted in ESF frame (N+1) are determined as follows:
  - For the purpose of CRC-6 calculation only, every F bit is set to “1” in ESF(N), that is, the ESF just preceding ESF(N+1). ESF(N) is altered in no other way.
  - The resulting 4632 bits of ESF(N) are used, in order of occurrence, to construct a polynomial in “x” such that bit 0 of ESF(N) is the coefficient of the term x^{4631} and bit 4631 of ESF(N) is the coefficient of the term x^0 .
  - The polynomial is multiplied by the factor x^6, and the result is divided, modulo 2, by the generator polynomial x^6+x+1. The coefficients of the remainder polynomial are used, in order of occurrence, as the ordered set of check bits, C1 through C6, for ESF(N+1). The ordering is such that the coefficient of the term x^5 in the remainder polynomial is check bit C1 and the coefficient of the term x^0 in the remainder polynomial is check bit C6.
  - The check bits C1 through C6 contained in any ESF frame are always those associated with the content of the ESF frame immediately preceding the one in which the check bits occur. When there is no immediately preceding ESF frame, the check bits may be assigned any value.

Table 1-4
Extended superframe format

Frame no.	F bits				Bit use in each time slot		Signaling bit use options	
	Bit no.	FPS	DL	CRC	Traffic	Signal’g	T	Signal’g channel
1	0	-	m	-	1-8	-		
2	193	-	-	C1	1-8	-		
3	386	-	m	-	1-8	-		
4	579	0	-	-	1-8	-		
5	772	-	m	-	1-8	-		
6	965	-	-	C2	1-7	8	-	A
7	1158	-	m	-	1-8	-		
8	1351	0	-	-	1-8	-		
9	1544	-	m	-	1-8	-		
10	1737	-	-	C3	1-8	-		
11	1930	-	m	-	1-8	-		
12	2123	1	-	-	1-7	8	-	B
13	2316	-	m	-	1-8	-		
14	2509	-	-	C4	1-8	-		
15	2702	-	m	-	1-8	-		
16	2895	0	-	-	1-8	-		
17	3088	-	m	-	1-8	-		
18	3281	-	-	C5	1-7	8	-	A
19	3474	-	m	-	1-8	-		
20	3667	1	-	-	1-8	-		
21	3860	-	m	-	1-8	-		
22	4053	-	-	C6	1-8	-		
23	4246	-	m	-	1-8	-		
24	4439	1	-	-	1-7	8	-	B

Note 1: Frame 1 is transmitted first.

Note 2: Frames 6, 12, 18, and 24 are denoted signaling frames.

Note 3: FPS is the Framing Pattern Sequence (...001011...).

Note 4: DL is the 4 kbit/s Data Link (“m” bits).

Note 5: CRC is the CRC-6 Cyclic Redundancy Check (bits C1 to C6).

Note 6: Option T is traffic (bit 8 is not used for signaling).

4.5 Idle codes

4.5.1 Codes for idle channels and idle slots

A keep-alive signal is applied to idle channels to ensure that no more than 80 consecutive “0”s are transmitted. The keep alive signal is removed when the pulse density returns to the requirements described in section 3.6.

The keep alive signal is an unframed, continuous repetition of the channel idle code — 0111 1111.

4.5.2 Interframe (layer 2) timefill

Contiguous HDLC flags are transmitted on the D-channel when its layer 2 has no frames to send.

Chapter 2-5:
Layer 1 clear channel capability

5.1 Clear channel capability

To provide DS-1 clear channel capability (CCC), a DS-1 signal with unconstrained information bits is altered by some method to meet the pulse density requirements specified in section 3.6. The method used to provide DS-1 CCC is the same in both directions of transmission. The long-term method of providing DS-1 CCC will be B8ZS. DS-1 CCC is a necessary, but not a sufficient condition for providing clear channel capabilities end-to-end for customers.

Chapter 2-6: Layer 1 maintenance

Maintenance messages and signals are transmitted in-band in the superframe format (SF) and in the data link layer in the extended superframe (ESF) format.

6.1 Remote alarm indication

The remote alarm indication (RAI) signal — also called the Yellow Alarm — is transmitted in the outgoing direction when a DS-1 terminal determines that it has lost the incoming signal. The RAI signal is transmitted to the interface as follows:

- In the superframe format, the RAI signal is transmitted for the duration of the alarm condition or for at least one second, whichever is greater. For the duration of the alarm, bit 2 in every eight-bit time slot is a “0”.
- In the extended superframe format, the RAI signal is transmitted for the duration of the alarm condition or for at least one second, whichever is greater. For the duration of the alarm, a repeating 16-bit pattern consisting of eight “1”s followed by eight “0”s (1111 1111 0000 0000) is transmitted continuously on the ESF data link.
- For either framing format, the minimum time between the end of one transmission and the beginning of another transmission is one second. Certain services provided by the network may require longer time intervals than these minimum values, and may require unequal “on” and “off” intervals, or both.

6.2 Alarm indication signal (AIS)

An alarm indication signal (AIS) should be transmitted forward upon a loss of an originating signal, or when any action is taken that would cause a service disruption. The AIS is removed when the condition triggering the AIS is terminated. The AIS is an unframed, all “1”s signal. The presence of the AIS signal may indicate the loss of network synchronization.

6.3 Loopback

Customers have the option to use the CI with or without loopback.

The protocol currently in use by the carriers for network access to the CI loopback feature is in-band signaling control. This protocol may also be used for CI-to-CI testing. Only the CI may respond to the in-band control loopback codes described in this section.

With in-band signaling control, the loopback operates upon receipt of specific framed pulse patterns. The loopback pulse codes and functions are:

- Activate: A framed DS-1 signal consisting of repetitions of four “0”s followed by a “1” (00001), lasting for at least 5 seconds, with the frame alignment bits overwriting the pattern.
- Deactivate: A framed DS-1 signal consisting of repetitions of two “0”s following by a “1” (001), lasting for at least 5 seconds, with the frame alignment bits overwriting the pattern[1].

The loopback also operates upon receipt of the patterns described above without framing to accommodate imbedded equipment which sends unframed (non-standard) in-band control signals. With the CI loopback feature activated, the customer's signal is interrupted and the DS-1signal received from the network is transmitted back to the network. The looped signal must be regenerated by the CI without change in framing format or removal of bipolar violations.

Line loopbacks and payload loopbacks as described in ANSI T1.408 are not supported by the network. Loopback on a DMS-100 is activated and deactivated from a MAP terminal.

6.4 ESF maintenance

6.4.1 Introduction

The extended superframe format incorporates a block error detection code (CRC-6) and a data link (DL) channel that allow carrier maintenance of DS-1 transmission facilities. The following sections specify the functions that are necessary in the CI to support monitoring of digital circuits.

Errors in the transmission received by the CI may be detected by

- detecting CRC violations, by comparing a locally calculated CRC with the CRC encoded in the received signal
- detecting errors in the framing bit pattern, or detecting the loss of a frame
- detecting line code violations (non-B8ZS bipolar violations)

---

[1] It should be noted that embedded network equipment exists which may be activated by the loopback code and block the code from reaching the CI, requiring manual intervention to deactivate the loopback.

- detecting controlled slips (for CIs that are components of a synchronized network)

The presence of all or a subset of these error types can indicate the location of the impairment, and thus is required maintenance information. The CI monitors the incoming signal for these conditions.

Once each second, the CI reports the parameters over the DL channel as specified in the following sections. These reports ensure that the quality of transmission, as received at the CI, is reported. The reports are sent over the DL channel using bit-oriented signals.

6.4.2 Transmission measurement parameters

During periods of ideal transmission, none of these events occur. If the CI detects, or does not detect, any of these conditions, it shall report as specified in section 6.4.3. The reports are based on one-second intervals.

The one-second timing intervals may be derived from the DS-1 signal, or from a separate, equally accurate (± 32 ppm) source. The phase of the one-second periods with respect to the occurrence of error events is arbitrary. That is, the one-second timing does not depend on the time of occurrence of any error event. These events identify details of transmission errors received at the CI.

The events that are detected and reported are

- no event
- CRC error
- severely-errored frames

The events that may be detected and reported are

- frame synchronization bit error
- line code violation
- controlled slip

These are defined as follows:

6.4.2.1 CRC error event

A CRC error event is reported if the received CRC code for a particular frame is not identical to the corresponding locally calculated code.

6.4.2.2 Severely errored framing event

A severely errored framing event is reported if two or more framing bit pattern errors occur within a 3 ms period. Contiguous 3 ms intervals are examined. The 3 ms period may coincide with the extended superframe period.

6.4.2.3 Frame synchronization bit error event

A frame synchronization bit error event is the occurrence of a received framing-bit-pattern error.

6.4.2.4 Line code violation event

A line code violation event occurs when a bipolar violation is received for an AMI-coded signal. For a B8ZS-coded signal, a line code violation event occurs when a bipolar violation is received and this violation is not part of an associated zero-substitution code.

6.4.2.5 Controlled slip event

A controlled slip event is the occurrence of a replication or deletion of DS-1 frames by the receiving terminal. A controlled slip occurs when there is a difference between the timing of a synchronous receiving terminal and that of the received signal of such a magnitude as to exhaust the buffer capability of the synchronous terminal.

6.4.3 ESF data link

There are two categories of bit-oriented messages — priority messages, and command and response messages.

Message-oriented codewords are used to carry performance monitoring information (see ANSI T1.408, ISDN primary rate—customer installation metallic interfaces Layer 1 specification, 1990). Message-oriented codewords based on LAPD protocol are not supported by the network.

6.4.3.1 Priority messages

Priority messages indicate a service-affecting condition. The only priority message generated by the network is an RAI — a yellow alarm. It is transmitted continuously until the cause no longer exists.

6.4.3.2 Command and response messages

Command and response messages are transmitted to perform various functions. The various command and response messages include

- loopback activate
- loopback deactivate
- protection switch line “x” (0 < x < 28)
- protection switch acknowledge
- protection switch release

These are currently not supported by the network although it is recommended that user equipment support these for future compatibility.

6.4.4 ESF bit-oriented data link communication

Data link bit-oriented messages shall be of the format:

0xxx xxx0 1111 1111

with the rightmost bit transmitted first. Table 2-5 lists two categories of bit-oriented message functions and their associated 16-bit codewords. Codewords for priority messages are repeated continually until the condition which initiated the message is removed. The minimum duration is as specified for RAI in section 6.1. Command/response codewords are repeated at least 10 times.

6.4.4.1 Protection switching codewords

The “switch line” codes in Table 1-5 use the five least significant “x” bits in the second octet of the codeword to indicate the number of the line, 1 through 27, to be switched to a protection line.

Table 1-5
Assigned Bit-oriented data-link messages

Priority Messages	Codeword	
RAI (Yellow alarm)	000 0000	0111 11111
Loopback retention	001 0101	0111 11111

Command and Response Messages	Codeword	
Line loopback (Ia) activate	000 0111	0111 11111
Line loopback (Ia) deactivate	001 1100	0111 11111
Line loopback (Ib) activate	001 0000	0111 11111
Payload loopback activate	000 1010	0111 11111
Payload loopback deactivate	001 1001	0111 11111
Network use loopback activate	000 1001	0111 11111
Universal loopback deactivate	001 0111	0111 11111
CI loopback activate	001 0111	0111 11111
Protection switch line 1	010 0001	0111 11111
Protection switch line 2	010 0010	0111 11111
Protection switch line 3	010 0011	0111 11111
....	...	...
Protection switch line 27	011 1011	0111 11111
Protection switch acknowledge	000 1100	0111 11111
Protection switch release	001 0011	0111 11111
Synchronization	001 1000	0111 11111
Synchronization	000 0110	0111 11111
Synchronization	001 0001	0111 11111
Synchronization	001 0100	0111 11111

Note 1: The rightmost bit in each code word is transmitted first.

Note 2: The protection switch line codes of the form 01x xxxx 0111 1111 use the five x-bits to indicate the number of the line (1 to 27) to be switched to a protection line.

Note 3: Only RAI is supported by the network; other values are reserved.

Chapter 2-7:
Layer 1 connector arrangements

7.1 Connector arrangements

All connections at the network interface use one of three Universal Service Ordering Code (USOC) connectors (RJ48C, RJ48X, or RJ48M) (FCC Rules and Regulations, Sub-part F of Part 68, supplemented by Public Notice 2526, February 10, 1986). The physical arrangement of these connectors is shown in Figure 2-9, Figure 2-10, and Figure 2-11.

Figure 2-9
Connector pin assignment (RJ48C)

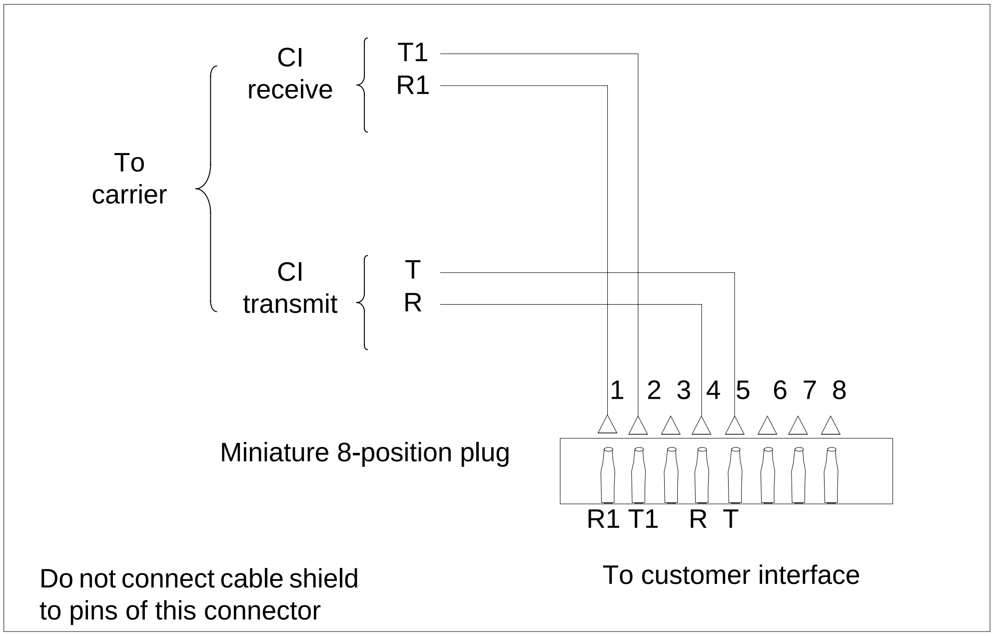


Figure 2-10
Connector pin assignment (RJ48X)

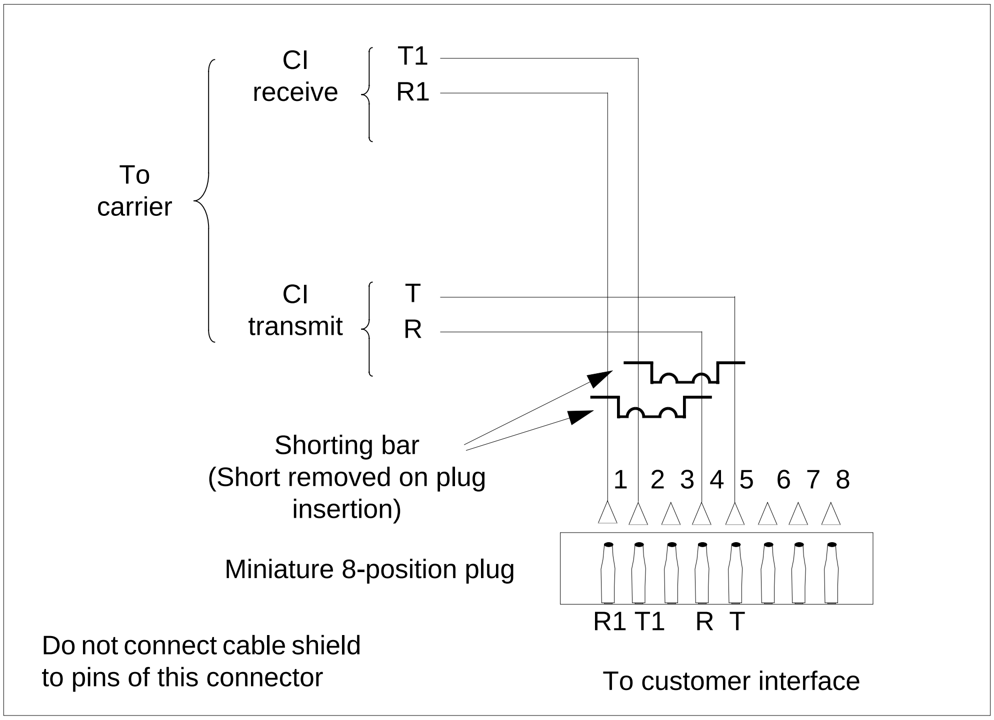
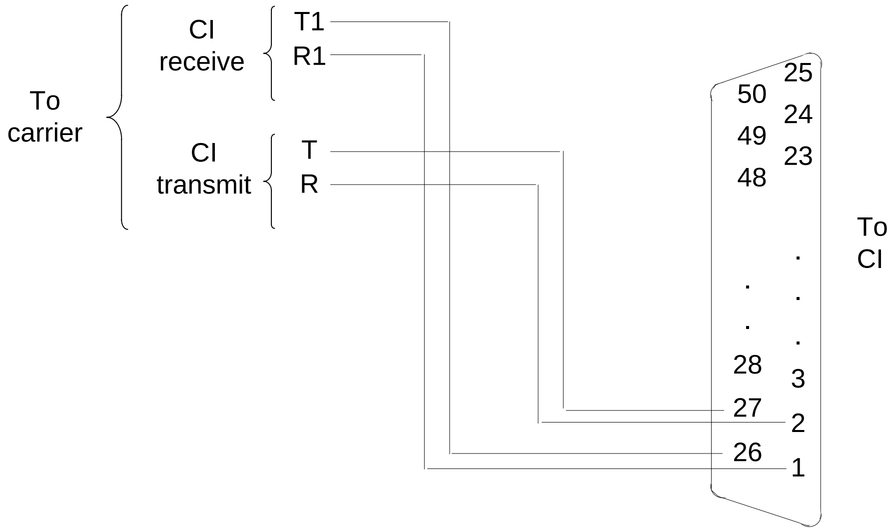


Figure 2-11
Connector pin assignment (RJ48M)



Connector pin number				
Line	**T1**	**R1**	**T**	**R**
1	26	1	27	2
2	29	4	30	5
3	32	7	33	8
4	35	10	36	11
5	38	13	39	14
6	41	16	42	17
7	44	19	45	20
8	47	22	48	23

Do not connect cable shield to pins of this connector

Section 3:
Layer 2 specification for primary rate interfaces

Chapter 3-1:
Introduction to Layer 2 3-5

Chapter 3-2:
Layer 2 frame structure 3-9

Chapter 3-3:

Layer 2 elements of procedures 3-15

Chapter 3-6:
Occurrence of MDL-Error-Indication 3-57

Chapter 3-7:
Layer 2 SDL diagrams 3-61

Chapter 3-1: Introduction to Layer 2

1.1 Scope

This section defines the link access protocol for the D channel (LAPD) of the ISDN primary rate interface (PRI).

In particular, it specifies:

- the peer-to-peer protocol for the transfer of information and control between any pair of service access points on the data link layer
- the interactions between the data link layer[1] and Layer 3, and between the data link layer and the physical layer (Layer 1).

LAPD, in the Open Systems Interconnection (OSI) reference model, is the Layer 2 protocol for the interface. It is independent of transmission rate, and requires a duplex, bit-transparent D-channel. The purpose of LAPD is to convey information between Layer 3 entities across the ISDN primary rate interface using the D-channel. The protocol defines the procedures required to establish, maintain, and disconnect the link.

The LAPD procedures in this section are suitable for all applications of the ISDN primary rate interface. For example, private branch exchange (PBX) to central office (CO).

1.2 Feature summary

The LAPD features that are supported are:

- Point-to-point, acknowledged, multiple frame information transfer.

---

[1] The term “data link layer” is used in the main text of this specification. However, the terms “Layer 2”and “L2”are used as abbreviations. Similarly, in accordance with Recommendations Q.930 (I.450) and Q.931 (I.451), the term “layer 3”is used to indicate the layer above the data link layer.

All references to “layer management entity” or “connection management entity” refer to those entities at the data link layer.

- Service access point identifier (SAPI) of 0, and terminal endpoint identifier (TEI) of 0 (fixed TEI).
- TEI administration procedures are limited to those interactions that do not involve peer entities. For example, assignment of a TEI value by the user-side management entity to the user-side data link layer entity do not involve interactions with the network side.
- Default parameter values.

Features in ANSI T1.602 that are not supported are as follows:

- Unnumbered information (UI) commands, and the *DL-Unit-Data* primitive.
- Broadcast procedures (that is, TEI 127 is not supported).
- Management information transfer (that is SAPI 63, Identity Remove message, and *MDL-Unit-Data* primitive).
- TEI removal procedure (the network and user can not request that the other end remove its TEI).
- Exchange identification (XID) procedures.
- MPH primitives (used for communication between the management entity and Layer 1).
- Deactivation procedures.

1.3 Standards compatibility

This data link layer specification is based on *ANSI T1.602, ISDN signaling specification for application at the user-network interface — Layer 2 specification*, and is a subset of the *CCITT Recommendation Q.920(I.440), ISDN user-network interface data link layer — general aspects*, and the *CCITT Recommendation Q.921(I.441), ISDN user-network interface data link layer specification.*

1.4 Overview description of LAPD functions and procedures

The purpose of LAPD is to convey information between Layer 3 entities across the ISDN PRI using the D-channel.

All data link layer messages are transmitted in frames which are delimited by flags. A flag is a unique bit pattern.

LAPD includes functions for:

- Provisioning of one or more data link connections on a D-channel. Discrimination between the data link connections is by means of a data link connection identifier (DLCI) contained in each frame.

- Frame delimiting, alignment, and transparency, that allows a sequence of bits transmitted over a D-channel to be recognized as a frame.
- Sequence controlling, to maintain the sequential order of frames across a data link connection.
- Detection of transmission, format, and operational errors on a data link connection.
- Recovery from detected transmission, format, and operational errors.
- Notification to the management entity of unrecoverable errors.
- Flow control.

Data-link-layer functions provide the means for information transfer between multiple combinations of data link connection endpoints. In the case of PRI, the information is transferred through point-to-point data link connections in which each frame is directed to a single endpoint.

1.5 Protocol service definition

The data link layer provides services to Layer 3 and the management of the data link layer (Layer 2). It uses the services provided by the physical layer (Layer 1) and by layer management.

1.5.1 Services provided to Layer 3

The specification of the interactions with Layer 3 (primitives) provides a description of the services that the data link layer, plus the physical layer offer to Layer 3, as viewed from Layer 3.

The information transfer service is based on acknowledged information transfer at the data link layer.

The characteristics of the service are as follows:

- provision of a data link connection between Layer 3 entities for acknowledged information transfer of Layer 3 message units
- identification of data link connection endpoints
- sequence integrity of data link layer message units in the absence of malfunctions
- notification to the peer entity in the case of errors; for example, loss of sequence
- notification to the management entity of unrecoverable errors detected by the data link layer
- flow control

The primitives associated with the acknowledged information transfer services are:

- *DL-Data-Request* and *-Indication* — for transferring data
- *DL-Establish-Request* and *-Indication* — for establishing multiple-frame operation
- *DL-Release-Request*, *-Indication*, and *-Confirm* — for terminating multiple-frame operation

1.5.2 Administrative services

The administrative services functions are:

- assignment and removal of TEI values
- notification of errors

These services are considered to be provided conceptually by layer management either on the user side or on the network side. The primitives associated with these services are:

- *MDL-Assign-Request* and *-Indication* — for assigning TEI value

  These primitives are used to send a TEI value obtained from the layer manager. The layer manager passes the TEI value to the data link layer in order that the user data-link-layer entities can begin to communicate with the network data-link-layer entities.
- *MDL-Remove-Request* — for removing TEI value

  This primitive is used to send a layer manager request for removal of a TEI value that has previously been assigned using the *MDL-Assign* primitives.
- *MDL-Error-Indication* and *-Response* — used for error notification.

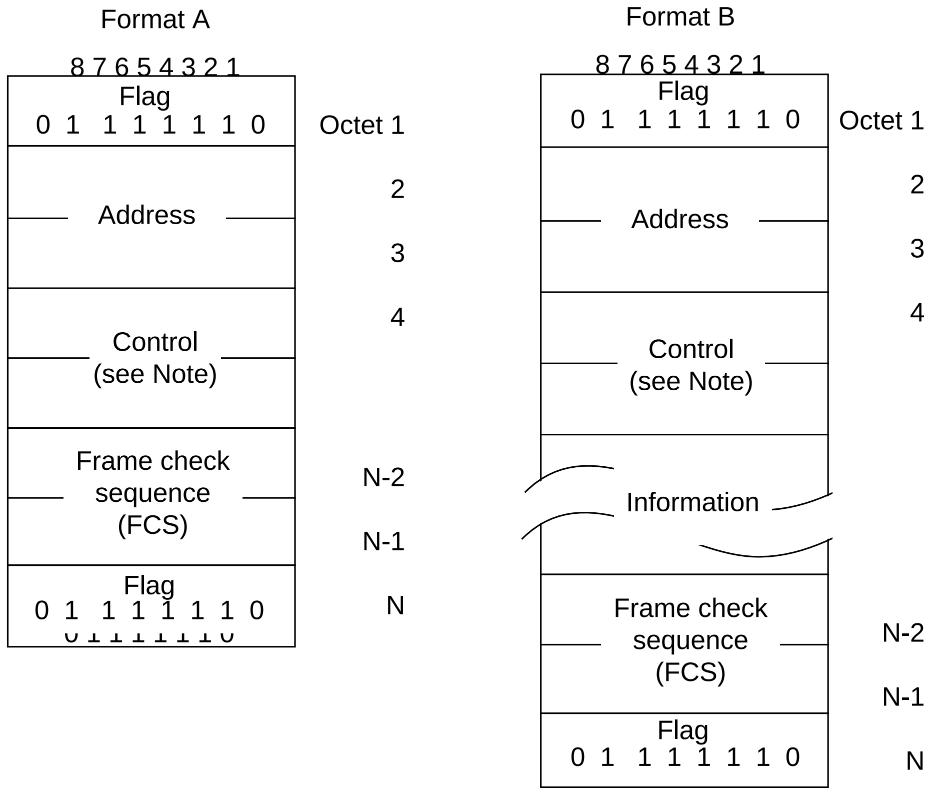
  These primitives are used to report errors between the layer manager and the data-link-layer entities.

Chapter 3-2:
Layer 2 frame structure

2.1 Introduction

All peer-to-peer exchanges at the data link layer conform to one of the formats shown in Figure 3-1. Format A is used for frames that do not have an information field. Format B is used for frames that do contain an information field.

Figure 3-1
Frame formats



Note: Acknowledged operation (modulo 128)	— 2 octets for frames with sequence numbers
	— 1 octet for frames without sequence numbers

2.2 Flag sequence

All frames start and end with a flag sequence that consists of one “0” bit followed by six contiguous “1” bits and one “0” bit (0111 1110). The flag preceding the address field is called the opening flag. The flag following the Frame Check Sequence (FCS) field is called the closing flag. The closing flag may also serve as the opening flag of the next frame in some applications.

When the layer 2 entity has no frames to transmit, it sends contiguous HDLC flag sequences (0111 1110). The receiving equipment should also be capable of receiving an interframe abort. This consists of one “0” bit followed by seven contiguous “1” bits (0111 1111).

2.3 Address field

The address field consists of 2 octets as shown in Figure 3-1. The address field identifies the intended receiver of a command frame and the transmitter of a response frame. The format of the address field is defined in section 3.2 on page 3-15.

2.4 Control field

Depending on the type of operation, the control field consists of 1 or 2 octets as shown in Figure 3-1. This field is used to identify the type of command and response. The format of the control field is defined in section 3.4 on page 3-17.

2.5 Information field

The information field of a frame, when present, follows the control field and precedes the frame check sequence as shown in Figure 3-1. The contents of the information field consist of an integral number of octets which hold a message from layer 3.

The maximum number of octets in the information field is a system parameter, which is described in section 5.9.3 on page 3-53.

2.6 Transparency

A transmitting data-link-layer entity examines the frame content between the opening and closing flag sequences, (address, control, information and FCS fields). It inserts a “0” bit after all sequences of five contiguous “1” bits (including the last five bits of the FCS) to ensure that a flag or an abort sequence is not simulated within the frame.

At the receiving end, a similar data-link-layer entity examines the frame contents between the opening and closing flag sequences and discards any “0” bit which directly follows five contiguous “1” bits.

2.7 Frame checking sequence (FCS) field

The FCS field is a 16-bit sequence. It is the “1”s complement of the sum (modulo 2) of the following formulas:

- the remainder of $(x^k)(x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ divided (modulo 2) by the generator polynomial $x^{16} + x^{12} + x^5 + 1$, where “k” is the number of bits in the frame existing between, but not including, the final bit of the opening flag and the first bit of the FCS, excluding bits inserted for transparency
- the remainder of the division (modulo 2) by the generator polynomial $x^{16} + x^{12} + x^5 + 1$, of the product of x^{16} by the content of the frame existing between, but not including, the final bit of the opening flag and the first bit of the FCS, excluding bits inserted for transparency

As a typical implementation at the transmitter, the initial content of the register of the device computing the remainder of the division is preset to all “1”s. This is modified by division by the generator polynomial (as described above) of the address, control and information fields; the “1”s complement of the resulting remainder is transmitted as the16-bit FCS.

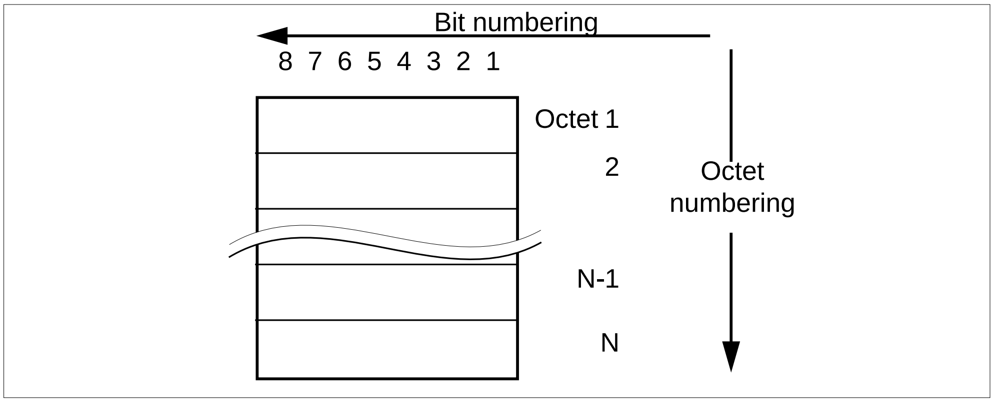
As a typical implementation at the receiver, the initial content of the register of the device computing the remainder is preset to all “1”s. The final remainder, after multiplication by x and division (modulo 2) by the generator polynomial $x^{16} + x^{12} + x^5 + 1$ of the serial incoming protected bits and the FCS, is ‘0001 1101 0000 1111’(x^{15} through x^0, respectively) in the absence of transmission errors.

2.8 Format convention

2.8.1 Numbering convention

The basic frame numbering convention used is shown in Figure 3-2. The bits are grouped into octets.

Figure 3-2
Format convention



2.8.2 Order of bit transmission

The octets are transmitted in ascending numerical order. Within an octet, bit 1 is the first bit to be transmitted.

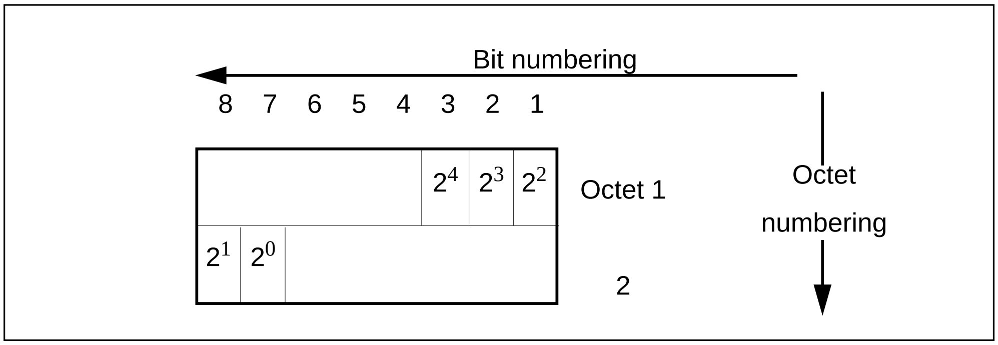
2.8.3 Field mapping convention

When a field is contained within a single octet, the lowest bit number of the field represents the lowest order value.

When a field spans more than one octet, the order of bit values progressively decreases as the octet number increases within each octet. The lowest bit number associated with the field represents the lower order value.

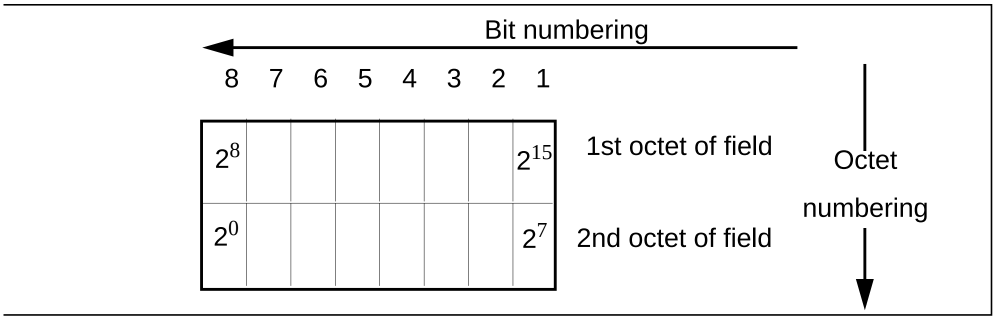
For example, a bit number can be identified as a couple (o, b) where “o” is the octet number and “b” is the relative bit number within the octet. Figure 3-2 shows a field that spans from bit (1, 3) to bit (2, 7). The high order bit of the field is mapped on bit (1, 3) and the low order bit is mapped on bit (2, 7).

Figure 3-3
Field mapping convention



An exception to the preceding field mapping convention is the data-link-layer frame check sequence (FCS) field, which spans two octets. In this case, bit 1 of the first octet is the high order bit and bit 8 of the second octet is the low order bit (see Figure 3-5).

Figure 3-4
FCS mapping convention



2.9 Invalid frames

An invalid frame is a frame which has one or more of the following properties:

- it is not properly bounded by two flags
- it has fewer than 6 octets between flags of frames that contain sequence numbers and fewer than 5 octets between flags of frames that do not contain sequence numbers
- it does not consist of an integral number of octets prior to zero bit insertion or following zero bit extractions
- it contains a frame-check sequence error
- it contains a single octet address field
- it contains a service access point identifier (SAPI) which is not supported by the receiver

Invalid frames are discarded without notification to the sender. No action is taken as the result of the invalid frame.

2.10 Frame abort

Receipt of seven or more continuous “1” bits is interpreted as an abort message and the data-link-layer entity ignores the frame currently being received.

Chapter 3-3:

Layer 2 elements of procedures

3.1 Introduction

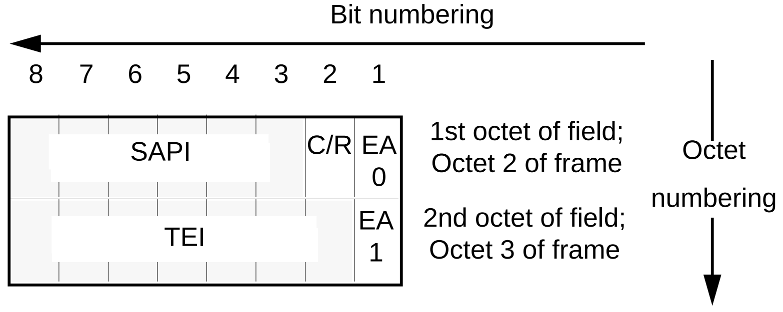
This chapter defines the commands and responses that are used on the data link connections carried on the D-channel.

Procedures are derived from these elements and are described in Chapter 3-5: "Definition of peer-to-peer procedures for Layer 2".

3.2 Address field format

The address field format shown in Figure 3-5 contains the address field extension bits, a command and response indication bit (C/R), a data-link-layer Service Access Point Identifier (SAPI) subfield, and a Terminal Endpoint Identifier (TEI) subfield.

Figure 3-5
Address field format



EA	Address field extension bit
C/R	Command and response indication bit
SAPI	Service access point identifier
TEI	Terminal endpoint identifier

3.3 Address field variables

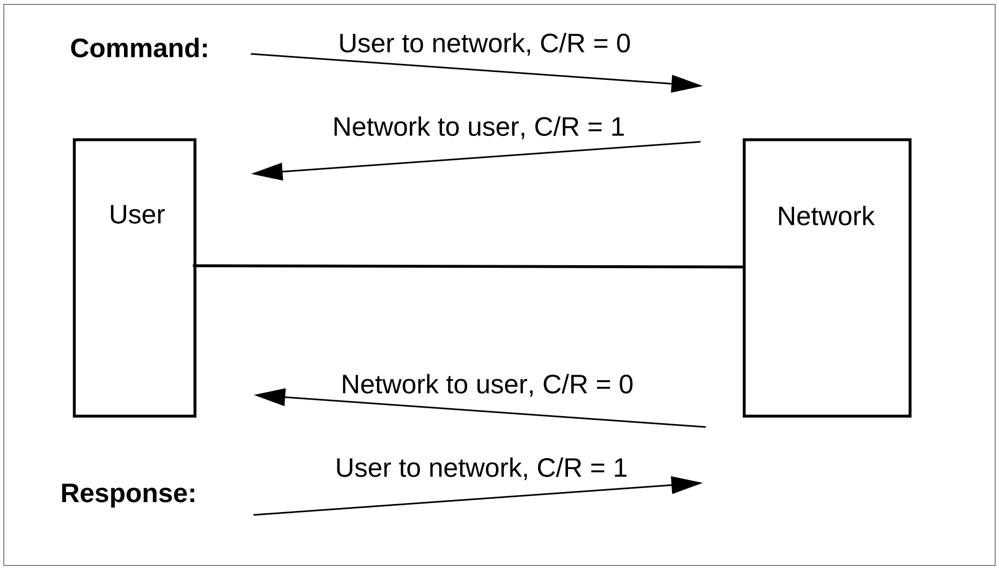
3.3.1 Address field extension bit (EA)

The address field range is extended by reserving the first transmitted bit of the address field octets to indicate the final octet of the address field. The presence of a “1” in the first bit of an address-field octet signals that it is the final octet of the address field. The double-octet address field for LAPD operation has bit 1 of the first octet set to “0” and bit 1 of the second address octet set to “1”.

3.3.2 Command response field bit (C/R)

The C/R bit identifies a frame as either a command or a response. The user side sends commands with the C/R bit set to “0”, and responses with the C/R bit set to “1”. The network side does the opposite; that is commands are sent with the C/R bit set to “1”, and responses are sent with the C/R bit set to “0”. The combinations for the network side and user side are shown in Figure 3-6.

Figure 3-6
C/R field bit usage



3.3.3 Service access point identifier (SAPI)

The SAPI identifies an endpoint at which data-link-layer services are provided by a data-link-layer entity to a Layer 3 or management entity. Consequently, the SAPI specifies a data-link-layer entity that should process a data-link-layer frame and also a Layer 3 or management entity which is to receive information carried by the data-link-layer frame.

The SAPI allows 64 (2^5) service access points to be specified. In the address field octet containing the SAPI, bit 3 is the least significant binary digit and bit 8 is the most significant. The SAPI values are allocated as shown in Figure 3-7.

Figure 3-7
Allocation of SAPI values

SAPI value	Related Layer 3 or management entity
0	Call control procedures
All others	Reserved for future standardization

3.3.4 Terminal end-point identifier (TEI)

The TEI for a point-to-point data link connection may be associated with a single item of terminal equipment (TE). A TE contains one TEI for point-to-point data transfer. The TEI subfield allows 128 (2^6)values to be specified. where bit 2 of the address field octet containing the TEI is the least significant binary digit and bit 8 is the most significant binary digit.

The TEI values from 0 to 126 are used for the point-to-point data link connections associated with the addressed SAP. The TEI subfield bit pattern “111 1111” (127) is reserved for assignment to the broadcast data link connection. This value is not supported.

The user side is assigned one TEI value, that is, the value of 0. The TEI is assigned at the time of subscription (and consequently described also as fixed or non-automatic TEI equipment), and may be entered into the TE, for example, by the user or manufacturer.

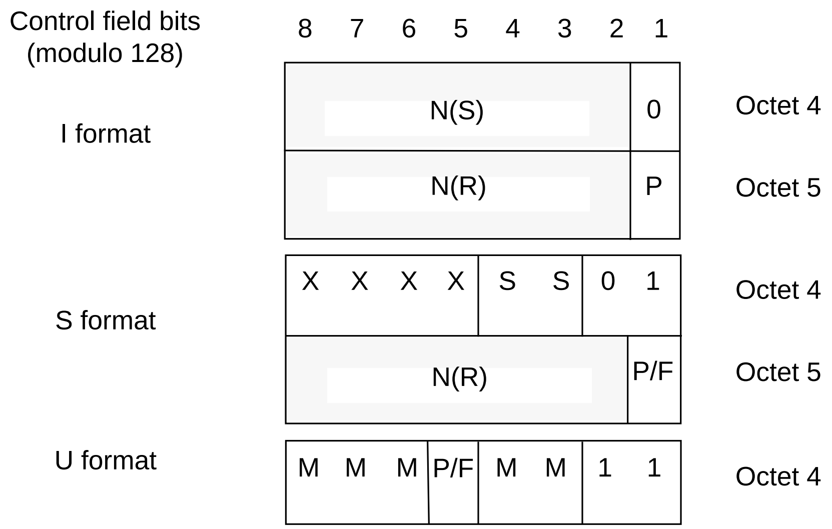
3.4 Control field formats

The control field identifies the type of frame. It can be either a command or a response frame. The control field contains sequence numbers where applicable. Three types of control field formats are specified:

- numbered information transfer (I format)
- supervisory function (S format)
- unnumbered information transfers and control functions (U format).

The control field formats are shown in Figure 3-8.

Figure 3-8
Control field formats



N(S)	Transmitter send sequence number	M	Modifier function bit
N(R)	Transmitter receive sequence number	P/F	Poll bit when issued as a command, final bit when issued as a response
S	Supervisory function bit	X	Reserved and set to “0”

3.4.1 Information transfer format — I

The I format is used for frames that transfer information between Layer 3 entities. The functions of N(S), N(R) and P (defined in section 3.5) are independent. Each I frame has an N(S) sequence number and an N(R) sequence number which may or may not acknowledge additional I frames received by the data-link-layer entity and a P bit that may be set to “0” or “1”.

The use of N(S), N(R), and P bits are defined in Chapter 3-5: "Definition of peer-to-peer procedures for Layer 2".

3.4.2 Supervisory format — S

The S format is used for frames to perform data link supervisory control functions such as

- acknowledging I frames
- requesting retransmission of I frames
- requesting a temporary suspension of transmission of I frames

The functions of N(R) and P/F are independent. Each supervisory frame has an N(R) sequence number which may or may not acknowledge additional

I frames received by the data-link-layer entity and a P/F bit that may be set to “0” or “1”.

3.4.3 Unnumbered format — U

The U format is used for frames that provide additional data link control functions. This format does not contain any sequence numbers. It includes a P/F bit that may be set to “0” or “1”. Unnumbered frames have a one-octet-sized control field.

3.5 Control field parameters and associated state variables

The various parameters associated with the control field formats are described in this section.

The coding of the bits within these parameters is such that the lowest numbered bit within the parameter field is the least significant bit.

3.5.1 Poll/final (P/F) bit

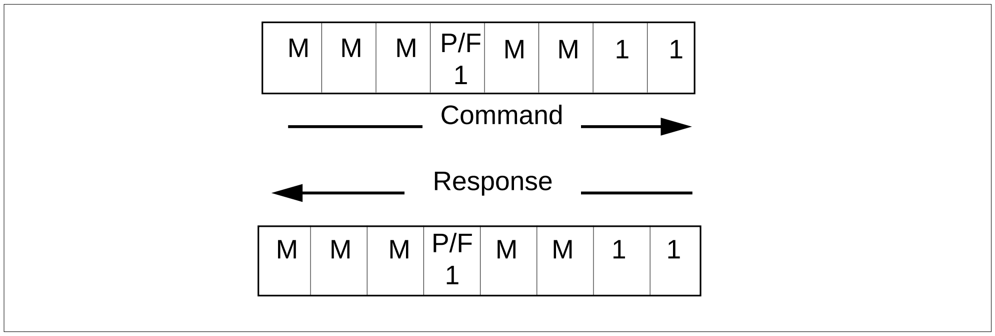
All frames contain a poll/final (P/F) bit. The P/F bit is used in both command and response frames. In command frames, the P/F bit is called the P bit. In response frames it is called the F bit.

The P bit set to ‘1’ is used by a data link layer entity to solicit (poll) a response frame from the peer data link layer entity.

When the F bit set to “1”, this indicates that the frame is a response from a data-link-layer entity sent as a result of a soliciting (poll) command.

The use of the P/F bit is fully described in Chapter 3-5: "Definition of peer-to-peer procedures for Layer 2".

Figure 3-9
Example of P/F bit for U-format frames



3.5.2 Multiple frame operation — variables and sequence numbers

This section describes all the variables and sequence numbers that are used when frames are transmitted. Figure 3-10 shows how these numbers progress as different frames are sent.

3.5.2.1 Modulus

Each I frame is sequentially numbered and may have a value 0 through modulus minus 1. The modulus is 128, and the sequence numbers cycle through the entire range, 0 through 127.

3.5.2.2 Send state variable, V(S)

When using I-frame commands, each point-to-point data link connection endpoint has an associated send state variable [V(S)]. The send state variable denotes the sequence number of the next in-sequence I frame that the end point transmits.

The send state variable can take on the value 0 through modulus minus 1. The value of the send state variable is incremented by 1 with each successive I-frame transmission. It cannot exceed V(A) by more than the maximum number of outstanding I frames, “k”. The value of “k” ranges from 1 through 127.

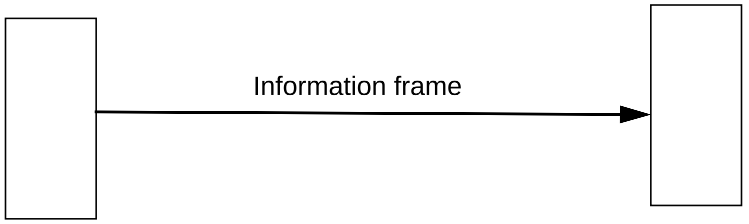
3.5.2.3 Acknowledge state variable, V(A)

When using I-frame commands and Supervisory frame commands and responses, each point-to-point data link connection endpoint has an associated acknowledge state variable [V(A)]. The acknowledge state variable identifies the last frame that has been acknowledged by its peer.

N(S) of last acknowledged I frame = V(A) - 1

The acknowledge state variable can take on the value 0 through modulus minus 1. The value of the acknowledge state variable is updated whenever a frame with a valid receive sequence number [N(R)] is received from its peer. A valid N(R) has a value in the range $V(A) \leq N(R) \leq V(S)$.

Figure 3-10
Variable and sequence number progression



First frame sent
V(S) = 1   In frame 1   Assume k = 2 in this example
V(A) = 1   N(S) = 1
V(R) = 1   N(R) = 1

Second frame sent
V(S) = 2   In frame 2
V(A) = 1   N(S) = 2
V(R) = 1   N(R) = 1

Third frame to be sent
V(S) = 3   In frame 3
V(A) = 1   N(S) = 3   Frame cannot be sent until
V(R) = 1   N(R) = 1   an acknowledge is returned
because
V(S) [=3] - V(A) [=1]   k [=2]

When 1st acknowledge frame returned:	When 2nd acknowledge frame returned for both frames sent:
V(S) = 2	V(S) = 2
V(A) = 2	V(A) = 3
V(R) = 1	V(R) = 1

3.5.2.4 Send sequence number, N(S)

Only I frames contain send sequence numbers [N(S)]. When an in-sequence I frame is transmitted, the value of the send sequence number [N(S)] in the frame is set equal to the value of the send state variable [V(S)].

3.5.2.5 Receive state variable, V(R)

When using I frame commands and supervisory frame commands and responses, each point-to-point data link connection endpoint has an associated receive state variable [V(R)].

The receive state variable [V(R)] denotes the sequence number of the next in-sequence I frame expected to be received. The receive state variable can take on the value 0 through modulus minus 1. The value of the receive state variable is incremented by one when each error free, in-sequence I frame is received provided its N(S) value equals the receive state variable [V(R)].

Figure 3-11
Layer 2 commands and responses

Format	Commands	Responses	Encoding								Octet No.
			8	7	6	5	4	3	2	1	
Information transfer	I (Information)		N(S)							0	4
			N(R)							P	5
Supervisory	RR (Receive ready)	RR	0	0	0	0	0	0	0	1	4
			N(R)							P/F	5
	RNR (Receive not ready)	RNR	0	0	0	0	0	0	0	1	4
			N(R)							P/F	5
	REJ (Reject)	REJ	0	0	0	0	1	0	0	1	4
			N(R)							P/F	5
Unnumbered	SABME*		0	1	1	P	1	1	1	1	4
		DM (Disconnect mode)	0	0	0	F	1	1	1	1	4
	DISC (Disconnect)		0	1	0	P	0	0	1	1	4
		UA (Unnumbered acknowledge)	0	1	1	F	0	0	1	1	4
		FRMR (Frame reject)	1	0	0	F	0	1	1	1	4

*Set asynchronous balanced mode extended

3.5.2.6 Receive sequence number, N(R)

All I frames and supervisory frames contain N(R), the expected send sequence number of the next received I frame. When any I or S frame is transmitted, the value N(R) in that frame is set equal to the current value of the receive state variable [V(R)]. N(R) indicates that the data-link-layer entity transmitting the

N(R) has correctly received all I frames numbered up to and including N(R) - 1.

3.6 Frame types

3.6.1 Commands and responses

This section describes the commands and responses that are used by either the user or the network data-link-layer entities. Each data link connection supports all the commands and responses identified below.

Only point-to-point, acknowledged, multiple frame information transfer is supported. Frame types associated with other information transfer modes are discarded. No other action is taken.

For purposes of the LAPD procedures in each application, the supervisory function bit encoding “11” and those encodings of the modifier function bits in Figure 3-8 not identified in Figure 3-11 are identified as undefined command and response control fields .

3.6.2 Information (I) command

The information (I) command is used to transfer, across a data link connection, sequentially numbered frames containing information fields provided by layer 3. This command is used in the multiple frame operation on point-to-point data link connections.

3.6.3 Set asynchronous balanced mode extended (SABME) command

The SABME unnumbered command is used to place the addressed user side or network side into modulo 128 multiple frame acknowledged operation.

No information field is permitted with the SABME command. A data link layer entity confirms acceptance of a SABME command by the transmission at the first opportunity of a UA or DM response. Upon acceptance of this command, the data link layer entity’s send state variable V(S), acknowledge state variable V(A), and receive state variable V(R) are cleared (set to zero). The transmission of an SABME command indicates the clearance of all exception conditions.

Previously transmitted I frames that are unacknowledged when this command is processed remain unacknowledged and are discarded. It is the responsibility of a higher level (for example, Layer 3) or the management entity to recover any such loss of information.

3.6.4 Disconnect (DISC) command

The DISC unnumbered command is transmitted to terminate multiple frame operation.

No information field can be present in the DISC command frame. The data-link-layer entity receiving the DISC command confirms the acceptance of a DISC command by transmitting a UA response. The data-link-layer entity sending the DISC command terminates the multiple frame operation when it receives an acknowledging UA or DM response.

Previously transmitted I frames that are unacknowledged when this command is processed remain unacknowledged and are discarded. It is the responsibility of a higher level (for example, Layer 3) or the management entity to recover any such loss of information.

3.6.5 Unnumbered information (UI) command

Not supported in this specification.

3.6.6 Receive ready (RR) command and response

The RR supervisory frame is used by a data-link-layer entity to

- indicate it is ready to receive an I frame
- acknowledge previously received I frames numbered up to and including N(R) - 1
- clear a busy condition that was indicated by the earlier transmission of an RNR frame by that same data-link-layer entity

In addition to indicating the status of a data-link-layer entity, the RR command, with the P bit set to “1” is used by the data-link-layer entity to ask for the status of its peer data-link-layer entity.

3.6.7 Reject (REJ) command and response

The REJ supervisory frame is used by a data-link-layer entity to request retransmission of I frames starting with the frame numbered N(R). The value of N(R) in the REJ frame acknowledges that I frames numbered up to and including N(R) - 1 have been received. New I frames pending initial transmission are transmitted following the retransmitted I frame(s).

Only one REJ exception condition for a given direction of information transfer is established at a time. The REJ exception condition is reset when an I frame with an N(S) equal to the N(R) of the REJ frame is received.

The transmission of a REJ frame also indicates that the busy condition has cleared on a sending data-link-layer entity. The busy state would normally have been signalled by the transmission of an RNR frame by that same data-link-layer entity.

In addition to indicating the status of a data-link-layer entity, the REJ command (with the P bit set to “1”) is used by the data-link-layer entity to ask for the status of its peer data-link-layer entity.

3.6.8 Receive not ready (RNR) command and response

The RNR supervisory frame is used by a data-link-layer entity to indicate a busy condition. That is, a temporary inability to accept additional incoming I frames. The value of the receive sequence number [N(R)] in the RNR frame acknowledges I frames numbered up to and including [N(R) - 1].

In addition to indicating the status of a data-link-layer entity, the RNR command — with the P bit set to “1” — may be used by the data-link-layer entity to enquire about the status of its peer data-link-layer entity.

3.6.9 Unnumbered acknowledgment (UA) response

The UA response is used by a data-link-layer entity to acknowledge the receipt and acceptance of the mode-setting commands, SABME or DISC. Received mode-setting commands are not processed until the UA response is transmitted. The UA response frame does not contain an information field.

The transmission of the UA response is also used to indicate the clearance of any busy condition that was reported by the earlier transmission of an RNR frame by that same data-link-layer entity.

3.6.10 Disconnected mode (DM) response

The DM response is used by a data-link-layer entity to report to its peer that the data link layer is in a state such that multiple frame operation cannot be performed. The DM response frame is not numbered and does not contain an information field.

3.6.11 Frame reject (FRMR) response

The FRMR unnumbered response may be received by a data link layer entity as a report of an error condition not recoverable by retransmission of the identical frame; that is, at least one of the following error conditions, resulting from the receipt of a valid frame:

- A frame containing a command or response control field that is not defined or is not implemented.An undefined or unimplemented control or response field is any control field code not identified in Figure 3-11.
- A supervisory or unnumbered frame of incorrect length. A frame containing an information field that is not permitted, with exception to the following message types; SABME, DISC, UA, RR, RNR, and REJ. For these messages, the frame is simply ignored.
- A frame received with an invalid receive sequence number [N(R)]. A valid N(R) value is one that is in the range $V(A) \leq N(R) \leq V(S)$.

If such an error occurs, an information field immediately following the control field is returned, consisting of five octets. This response provides the reason for the FRMR response. This information field format is shown in Figure 3-12.

Figure 3-12
FRMR information field format for extended (modulo 128) operation

8	7	6	5	4	3	2	1	
Rejected frame control field								Octet 5
								Octet 6
V(S)							0	Octet 7
V(R)							C/R	Octet 8
0	0	0	0	Z	Y	X	W	Octet 9

- The rejected frame control field is the control field of the received frame which causes rejection. When the rejected frame is not numbered, the control field of the rejected frame is positioned in octet 5, with octet 6 set to “0000 0000”.
- V(S) is the value of the current send state variable (on the user side or network side) that is reporting the rejection condition.
- C/R is set to “1” if the rejected frame is a response
- V(R) is the value of the current receive state variable (on the user side or network side) that is reporting the rejection condition.
- W set to “1” indicates that the control field received and returned in octets 5 and 6 is undefined or not implemented.
- X set to “1” indicates that the control field received and returned in octets 5 and 6 is considered invalid because the frame contained an information field which is not permitted with this frame, or the frame is a supervisory or unnumbered frame of incorrect length. Bit W is set to “1” in conjunction with this bit.
- Y set to “1” indicates that the information field received exceeds the maximum established information field length (N201) of the user side or network side reporting the rejection condition.
- Z set to “1” indicates that the control field received and returned in octets 5 and 6 contains an invalid N(R).
- Octet 7, bit 1, and octet 9, bits 5 through 8, are set to “0”.

Note: DMS implementation does not generate FRMR frame under any conditions. However, it responds to a received FRMR frame as specified in this document.

3.6.12 Exchange identification (XID) command/response

Not supported in this specification.

Chapter 3-4:
Layer 2 elements for layer-to-layer communication

4.1 Introduction

Communication between layers and between the data link layer and the management entity is accomplished by means of primitives.

Primitives represent, in an abstract way, the logical exchange of information and control between the data link layer and adjacent layers. They do not specify or constrain implementations.

Primitives consist of commands and their respective responses associated with the services requested of a lower layer. The general syntax of a primitive is:

Interface- Generic name - Type: Parameters

4.2 Interface

The interface part of the primitive determines the interface across which the primitive flows. For ISDN PRI, the following interfaces are defined:

- DL defines communication between Layer 3 and the data link layer
- PH defines communication between the data link layer and the physical layer
- MDL defines communication between the layer management and the data link layer

4.3 Generic names

The generic name specifies the activity that should be performed by the primitive. Table 2-1 illustrates the primitives defined in this chapter. (Note that some of the primitives do not have associated parameters.) A list of all the primitives and their uses follows Table 2-1.

Table 2-1
Primitives associated with the data link layer

Generic name	Type				Parameters		Message unit contents
	Request	Indication	Response	Confirm	Priority indicator	Message unit	
Layer 3-to-Layer 2 boundary							
DL-Establish	X	X	-	X	-	-	
DL-Release	X	X	-	X	-	-	
DL-DM-Release	X	-	-	-	-	-	
DL-Data	X	X	-	-	-	X	Layer 3 peer-to-peer message
Management entity-to-Layer 2 boundary							
MDL-Assign	X	X	-	-	-	X	TEI value - CES
MDL-Remove	X	-	-	-	-	X	TEI value - CES
MDL-Error	-	X	X	-	-	X	Reason for error
Later 2-to-Layer 1 boundary							
PH-Data	X	X	-	-	X	X	Layer 2 peer-to-peer message

4.3.1 DL-Establish

The *DL-Establish* primitives are used to request, indicate, and confirm the outcome of the procedures used to establish multiple-frame operation.

4.3.2 DL-Release

The *DL-Release* primitives are used to request, indicate, and confirm the outcome of the procedures for terminating a previously established multiple-frame operation. These primitives are also used to report unsuccessful attempts to establish multiple-frame operation.

4.3.3 DL-DM-Release

The *DL-DM-Release* primitives are equivalent to a *DL-Release* request. These primitives cause the Layer-2 entity to respond to a SABME command with a DM response. This primitive is used in the D-channel backup procedures (see 11.6 Annex F - Backup D-channel service).

4.3.4 DL-Data

The *DL-Data* primitives are used to request and indicate layer-3 messages which are to be transmitted, or have been received by the data link layer. These primitives are only used if the Layer-3 messages are transmitted using the acknowledged information transfer service.

4.3.5 MDL-Assign

The *MDL-Assign* primitives are used by the layer management entity to request that the data link layer associate the TEI value contained within the message portion of the primitive with the specified connection endpoint suffix (CES), across all SAPIs.

In addition, an *MDL-Assign* primitive is used by the data link layer to indicate to a layer management entity that a TEI value needs to be associated with the CES specified in the primitive message unit.

4.3.6 MDL-Remove

The *MDL-Remove* primitives are used by the layer management entity to request that the data link layer remove the association of the specified TEI value with the specified CES, across all SAPIs. The TEI and CES are specified in the *MDL-Remove* primitive message unit.

4.3.7 MDL-Error

The *MDL-Error* primitives are used to indicate to the connection management entity that one of the following has been detected:

- an error associated with a previous management function request
- an error in a communication with the data link layer peer entity, which cannot be corrected by the data link layer

4.3.8 PH-Data

The *PH-Data* primitives are used to request and indicate message units containing frames used for data link layer peer-to-peer communications passed to and from the physical layer.

4.4 Primitive types

The primitive types defined in this specification are defined in the following sections.

4.4.1 Request

The *Request* primitive type is used when a higher layer or a management entity is requesting a service from the next lower layer.

4.4.2 Indication

The *Indication* primitive type is used by a layer providing a service to inform the next higher layer or layer management.

4.4.3 Response

The *Response* primitive type is used by layer management as a consequence of the *Indication* primitive type.

4.4.4 Confirm

The *Confirm* primitive type is used by the layer providing the requested service to confirm that the activity has been completed.

4.5 Parameter definition

4.5.1 Priority indicator

Since several service access points (SAPs) may exist on the network side or on the user side, protocol message units sent by one SAP may contend with those of other SAPs for the physical resources available for message transfer.

The priority indicator is used to determine which message unit has greater priority when contention exists. The priority indicator is only needed on the user side. It is used to distinguish message units sent by the SAP (with a SAPI value of “0”) from all other message units.

4.5.2 Message unit

The message unit contains additional layer-to-layer information concerning actions and results associated with requests. For *Data* primitives, the message unit contains the requesting layer peer-to-peer messages. For example, the *DL-Data* message unit contains Layer 3 information. The *PH-Data* message unit contains the data link frame.

> ***Note:*** The operations across the Layer 2-to-Layer 3 boundary are such that the layer sending the *DL-Data* primitive assumes a temporal order of the bits within the message unit. It is also assumed that the layer receiving the primitive can reconstruct the message with its assumed temporal order.

4.6 Primitive procedures

Primitive procedures specify the interactions used (between adjacent layers of the protocol) to invoke and provide a service. The service primitives represent the elements of the procedures. This section specifies the interactions between Layer 3 and the data link layer.

The states of a data link connection endpoint may be derived from the internal states of the data link layer entity supporting this type of a data link connection.

The data link connection endpoint states for point-to-point data link connection endpoints are as follows:

- link connection released
- awaiting establish

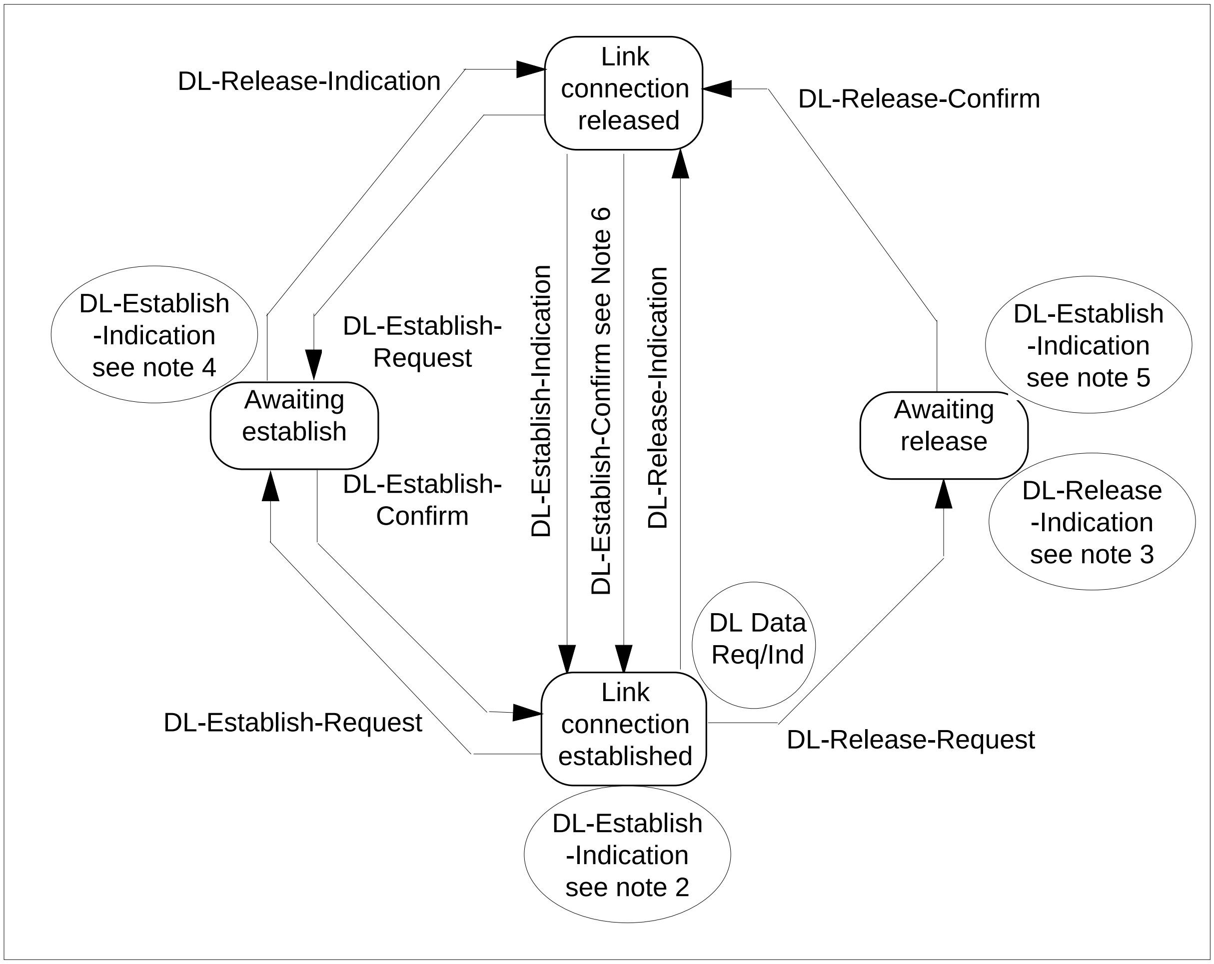
- awaiting release
- link connection established

The primitives provide the procedures to specify, conceptually, how a data link service user can invoke a service.

The possible overall sequences of primitives at a point-to-point data link connection endpoint are shown in the state transition diagram (Figure 3-13) The sequences are related to the states at one point-to-point data link connection endpoint.

The *Link connection released* and *Link connection established* states are stable states. The *Awaiting establish* and *Awaiting release* states are transition states.

Figure 3-13
State transition diagram for sequences of primitives at a point-to-point data link connection endpoint as seen by Layer 3



Note 1: If the data link layer entity issues a *DL-Establish-Indication* primitive, (for instance, if the data link layer is initiated or the peer system initiated re-establishment), a *DL-Release-Confirm* primitive, or a *DL-Release-Indication* primitive, all the data link service data units representing *DL-Data-Request*s are discarded.

Note 2: This primitive notifies Layer 3 that the link is re-established.

Note 3: This primitive is generated if a *DL-Release-Request* collides with a *DL-Release-Indication*.

Note 4: This primitive is generated if a *DL-Establish-Request* collides with a *DL-Establish-Indication*.

Note 5: This primitive is generated if a *DL-Release-Request* collides with a *DL-Establish-Indication*.

Note 6: This primitive is generated if a *DL-Establish-Request* (generated if Layer 3 attempts to re-establish the link) collides with a *DL-Release-Indication*. Since this *DL-Release-Indication* is not related to the *DL-Establish-Request*, the data link layer establishes the link and issue a *DL-Establish-Confirm*.

Chapter 3-5:
Definition of peer-to-peer procedures for Layer 2

This chapter specifies the procedures used by the data-link-layer entities.

The elements of procedure (frame types) which apply to point-to-point, acknowledged, and multiple-frame information transfer are:

- Set asynchronous balanced mode extended (SABME) command
- Unnumbered acknowledgment (UA) response
- Disconnected mode (DM) response
- Disconnect (DISC) command
- Receive ready (RR) command and response
- Receive not ready (RNR) command and response
- Reject (REJ) command and response
- Information (I) command
- Frame reject (FRMR) response

5.1 Procedure for use of the P/F bit

5.1.1 Unacknowledged information transfer

Not supported in this specification.

5.1.2 Acknowledged multiple-frame information transfer

A data-link-layer entity receiving an SABME, DISC, RR, RNR, REJ, or I-frame with the P bit set to “1”, sets the F bit to “1” in the next response frame it transmits, as shown in Table 2-2.

Table 2-2
Immediate response operation of the P/F bit

Command received with P bit = “1”	Response transmitted with F bit = “1”
SABME, DISC	UA, DM
I, RR, RNR, REJ	RR, RNR, REJ

5.2 Procedures for unacknowledged information transfer

Not supported in this specification.

5.3 Terminal endpoint identifier (TEI) management procedures

User equipment in the TEI-unassigned state enters the TEI-assigned state when layer management assigns a TEI value of “0” to that equipment. The state change is carried out when layer management issues an *MDL-Assign-Request* primitive.

User equipment in the TEI-assigned state enters the TEI-unassigned state when layer management removes the TEI from that equipment. The TEI is removed when layer management issues an *MDL-Remove-Request* primitive.

5.4 Automatic negotiation of data-link-layer parameters

Not supported in this specification.

5.5 Procedures for establishment and release of multiple frame operation

5.5.1 Establishment of multiple frame operation

Only the extended multiple-frame operation (modulo 128 sequencing) is supported for PRI.

The following procedures are used to establish multiple-frame operation between the network and a designated user entity.

Layer 3 requests establishment of multiple frame operation by the using the *DL-Establish-Request* primitive. Re-establishment may be initiated by the data-link-layer procedures defined in section 5.7 on page 3-49. All frames (other than unnumbered frames) received during the establishment procedures are ignored.

5.5.1.1 Establishment procedures

A data-link-layer entity initiates a request for multiple frame operation by transmitting the set asynchronous balanced mode extended (SABME) command. The SABME command:

- clears all existing exception conditions

- resets the retransmission counter to zero
- starts timer T200. (Timer T200 is defined in section 5.9.1 on page 3-53.) All mode setting commands are transmitted with the P bit set to “1”

Establishment procedures initiated by Layer 3 imply that all outstanding *DL-Data-Requests* and all I-frames in queues are discarded.

Having received a SABME command, and provided it can enter the multiple frame established state, the data-link-layer entity

- responds with an unnumbered acknowledgment (UA) response with the F bit is set to the same binary value (“0” or “1”) as the P bit in the received SABME command
- sets the send state variable V(S), the receive state variable V(R), and the acknowledge state variable V(A) to “0”
- enters the multiple-frame established state and inform Layer 3 using the *DL-Establish-Indication* primitive
- clears all existing exception conditions
- clears any existing peer receiver busy condition
- starts timer T203. (Timer T203 is defined in section 5.9.8 on page 3-53.)

If the data-link-layer entity cannot enter the multiple-frame established state, it responds to the SABME command with a Disconnected mode (DM) response. The F bit is set to the same binary value (“0” or “1”) as the P bit in the received SABME command.

If a UA response with the F bit set to “1” is received by the originator of the SABME command, the originator:

- resets timer T200
- starts timer T203
- sets the send state variable V(S), the receive state variable V(R), and the acknowledge state variable V(A) to “0”
- enters the multiple-frame established state and informs Layer 3 using the *DL-Establish-Confirm* primitive

If a DM response with the F bit set to “1” is received by the originator of the SABME command, the originator:

- informs Layer 3 that it has received this command, using the *DL-Release-Indication* primitive
- resets timer T200
- enters the TEI-assigned state

If a DM response with the F bit set to “0” is received by the originator of the SABME command, the originator ignores the response.

If a *DL-Release-Request* primitive is received during re-establishment of the data link layer, it is serviced on completion of the establishment mode-setting operation.

5.5.1.2 Procedure on expiry of timer T200

If timer T200 expires before the UA or DM response (with the F bit set to “1”) is received, the data-link-layer entity

- retransmits the SABME command
- restarts timer T200
- increments the retransmission counter

After retransmission of the SABME command N200 time, the data link layer entity indicates this to Layer 3 and the connection management entity by using the *DL-Release-Indication* and *MDL-Error-Indication* primitives, respectively. After discarding all outstanding *DL-Data-Request* primitives and all I-frames in the queue, the data-link-layer entity enters the TEI-assigned state.

The value of N200 is defined in section 5.9.2 on page 3-53.

5.5.2 Information transfer

I-frames and supervisory frames are transmitted and received (according to the procedures described in section 5.6 on page 3-41) if

- UA is transmitted in response to a received SABME command, or
- UA response is received in response to a transmitted SABME command.

If a SABME command is received while in the multiple-frame established state, the data-link-layer entity goes through the re-establishment procedures described in section 5.7 on page 3-49.

5.5.3 Termination of multiple frame operation

5.5.3.1 General

The following procedures are used to terminate the multiple-frame operation between the network and a designated user entity.

A Layer-3 entity can request termination of the multiple frame operation by using the *DL-Release-Request* primitive.

All frames, other than the unnumbered frames received during the release procedures, are ignored. All outstanding *DL-Data-Request* primitives, and all I-frames in the queue, are discarded.

If there is a persistent Layer 1 failure, the data-link-layer entity

- discards all I queues
- delivers a *DL-Release-Confirm* primitive to Layer 3, if a *DL-Release-Request* primitive is outstanding, otherwise it delivers a *DL-Release-Indication* primitive to Layer 3

5.5.3.2 Release procedure

A data-link-layer entity can initiate a request for release of the multiple-frame operation by transmitting the Disconnect (DISC) command with the P bit set to “1”. Timer T200 is started and the retransmission counter is reset to zero.

If a data-link-layer entity receives a DISC command while in the multiple-frame established state, or the timer recovery state, it transmits a UA response with the F bit set to the same binary value (“0” or “1”) as the P bit in the received DISC command. A *DL-Release-Indication* primitive is passed to Layer 3 and the entity enters the TEI-assigned state.

If the originator of the DISC command receives one of the following, it enters the TEI-assigned state and timer T200 is reset:

- a UA response with the F bit set to “1”
- a DM response with the F bit set to “1” (indicating that the peer data-link-layer entity is already in the TEI-assigned state)

The data-link-layer entity which issued the DISC command notifies Layer 3 that it is now in the TEI-assigned state using the *DL-Release-Confirm* primitive. The conditions relating to the TEI-assigned state are defined in section 5.5.4 on page 3-40.

5.5.3.3 Procedure on expiry of timer T200

If timer T200 expires before a UA or DM response with the F bit set to “1” is received, the originator of the DISC command

- retransmits the DISC command as defined above
- restarts the retransmission timer (T200)
- increments the retransmission counter.

If the data link layer entity has not received the correct response as defined in section 5.5.3.2 on page 3-39 after N200 attempts to recover, the data link layer

- sends an *MDL-Error-Indication* primitive to the managemnet entity
- enters the TEI-assigned state
- notifies layer 3 by means of the *DL-Release-Confirm* primitive

5.5.4 TEI-assigned state

While in the TEI-assigned state, the data link layer responds to the various commands, as follows:

- DISC command received: A disconnected mode (DM) response is transmitted with the F bit set to the binary value (“0” or “1”) of the received P bit.
- SABME command received: The entity tries to enter the multiple-frame operation state as described in section 5.5.1 on page 3-36.
- Unsolicited DM response (with the F bit set to “0”) received: The entity tries to enter the multiple-frame operation state as described in section 5.5.1 on page 3-36, or, if it cannot, it ignores the DM response.
- Unsolicited UA response received: The entity issues an *MDL-Error-Indication* primitive.

All other frame types are ignored by the entity and are discarded.

5.5.5 Collision of unnumbered commands and responses

5.5.5.1 Identical transmitted and received commands

If the transmitted and received unnumbered commands (SABME or DISC) are the same, the data-link-layer entities send the UA response at the earliest possible opportunity.

The entity receiving the UA response enters the indicated state. The data-link-layer entities each notify their respective Layer 3 entity using the appropriate *Confirm* primitive.

5.5.5.2 Different transmitted and received commands

If the transmitted and received unnumbered commands (SABME or DISC) are different, the data-link-layer entities issue a DM response at the earliest possible opportunity.

The entity receiving a DM response (with the F bit set to “1”) enters the TEI-assigned state and notifies its Layer 3 using the appropriate primitive.

The entity receiving the DISC command issues a *DL-Release-Indication* primitive while the other entity issues a *DL-Release-Confirm* primitive.

5.5.6 Unsolicited DM response and SABME or DISC command

When a DM response (with the F bit set to “0”) is received by a data-link-layer entity, a collision between a transmitted SABME or DISC command and the unsolicited DM response may have occurred. This is caused (typically) when the user equipment applies a protocol procedure according to X.25 LAPB to ask for a mode-setting command. (See the reference *CCITT Recommendation X.25, 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*.)

In order to avoid misinterpretation of the DM response received, a data-link-layer entity always sends the SABME or DISC command with the P bit set to “1”.

If a DM response (with the F bit set to “0”) collides with a SABME or DISC command, the DM response is ignored.

5.6 Procedures for information transfer in multiple frame operation

The procedures for transmitting I-frames are defined in the following sections. The term “transmission of an I-frame” and its equivalents, refer to the delivery of an I frame by the data link layer to the physical layer.

5.6.1 Transmitting I-frames

Information is received by the data-link-layer entity from Layer 3 using the *DL-Data-Request* primitive. This information is transmitted between peer entities in an I-frame. The control field parameters N(S) and N(R) in the I-frame are assigned the values of the send and receive state variables V(S) and V(R), respectively. The value of the send state variable V(S) is incremented by one at the end of the transmission of the I-frame.

If the retransmission timer, T200, is not running at the time of transmission of an I-frame, it is started. If the timer T200 expires before an acknowledgment is received by the sending entity, the procedures defined in section 5.6.7 on page 3-48 are followed.

If:
Send state variable V(S) = Acknowledge state variable V(A)
+ k (where k is the maximum number of
outstanding I-frames),
the data-link-layer entity does not transmit any new I-frames. It may retransmit an I-frame as a result of the error recovery procedures described in section 5.6.4 on page 3-43 and section 5.6.7 on page 3-48.

When the network side or user side is in the own-receiver busy[1] condition, it may still transmit I-frames, provided that a peer-receiver busy condition does not exist.

> ***Note:*** Any *DL-Data-Request* primitives received while in the timer recovery condition are queued.

---

[1] The term own- or peer-receiver busy refers to the peer-to-peer flow control state in the data-link-layer entities.

5.6.2 Receiving I-frames

Independent of a timer recovery condition, when a data-link-layer entity is not in an own-receiver busy condition, and receives a valid I-frame, whose send sequence number N(S) is equal to the current receive state variable V(R), the data-link-layer entity

- passes the information field of this frame to Layer 3 using the *DL-Data-Indication* primitive.
- increments its receive state variable V(R) by one.

The following actions are performed depending on the value of the P bit.

5.6.2.1 P bit set to “1”

If the P bit of the received I-frame is set to “1”, the data-link-layer entity responds to its peer in one of the following ways:

- If the data-link-layer entity receiving the I-frame is still not in an own receiver busy condition, it sends an RR response (with the F bit set to “1”).
- If the data-link-layer entity receiving the I-frame enters an own receiver busy condition upon receipt of the I-frame, it sends an RNR response (with the F bit set to “1”).

5.6.2.2 P bit set to “0”

If the P bit of the received I-frame is set to “0” and

- if the data-link-layer entity is still not in an own-receiver busy condition:
    - — if no I-frame is available for transmission, or if an I-frame is available for transmission but a peer receiver busy condition exists, the data-link-layer entity transmits an RR response (with the F bit set to “0”).
    - — if an I-frame is available for transmission and no peer receiver busy condition exists, the data-link-layer entity transmits the I-frame with the value of N(R) set to the current value of V(R).
- if, on receipt of this I-frame, the data-link-layer entity is now in an own-receiver busy condition, it transmits an RNR response (with the F bit set to “0”).

When the data-link-layer entity is in an own receiver busy condition, it processes any received I-frame according to the procedures defined in section 5.6.6 on page 3-47.

5.6.3 Sending and receiving acknowledgments

5.6.3.1 Sending acknowledgments

Whenever a data-link-layer entity transmits an I-frame or a supervisory frame, the value of N(R) is set equal to the value of V(R).

5.6.3.2 Receiving acknowledgment

On receipt of a valid I-frame or supervisory frame (RR, RNR, or REJ) — even in the own receiver busy or timer (T200) recovery condition — the data-link-layer entity treats the receive sequence number [N(R)] contained in this frame as an acknowledgment for all the I-frames it has transmitted with a send sequence number [N(S)] up to and including the received N(R)-1.

The value of the acknowledge state variable V(A) is set to the value of N(R).

The data-link-layer entity resets timer T200 on receipt of one of the following

- a valid I-frame
- a supervisory frame with the receive sequence number [N(R)] higher than V(A) (actually acknowledging some I-frames)
- a REJ frame with an N(R) equal to V(A)

  Note 1: If a supervisory frame with the P bit set to “1” has been transmitted and not acknowledged, timer T200 is not reset.

  Note 2: Upon receipt of a valid I-frame, timer T200 is not reset if the data-link-layer entity is in the peer receiver busy condition.

If timer T200 has been reset by the receipt of an I, RR, or RNR frame, and if there are outstanding I-frames still unacknowledged, the data-link-layer entity restarts timer T200. If the timer then expires, the data-link-layer entity attempts to recover as defined in section 5.6.7 on page 3-48.

If timer T200 has been reset by the receipt of a REJ frame, the data-link-layer entity retransmit any outstanding frames as described in section 5.6.4 on page 3-43.

5.6.4 Receiving REJ frames

On receipt of a valid REJ frame, the data-link-layer entity carries out the following

- if the data-link-layer entity is not in the timer recovery condition, the data-link-layer entity
  - — clears any existing peer receiver busy condition
  - — sets its send state variable V(S) and its acknowledge state variable V(A) to the value of the N(R) contained in the REJ frame control field
  - — stops timer T200
  - — starts timer T203
  - — if it was a REJ command frame with the P bit set to “1”, it transmits an appropriate supervisory response frame[1] with the F bit set to “1”

  - — transmits the corresponding I-frame as soon as possible, as defined in section 5.6.1 on page 3-41, taking into account the conditions in section 5.6.4.1 on page 3-45
  - — notifies the management entity that a protocol violation has occurred by use of the *MDL-Error-Indication* primitive, if it was a REJ response frame with the F bit set to “1”.

- If the data-link-layer entity is in the timer recovery condition and it was a REJ response frame with the F bit set to “1”, the data-link-layer entity
  - — clears any existing peer receiver busy condition
  - — sets its send state variable V(S) and its acknowledge state variable V(A) to the value of N(R) contained in the REJ frame control field
  - — stops timer T200
  - — starts timer T203
  - — enters the multiple-frame-established state
  - — transmits the corresponding I-frame as soon as possible, as defined in section 5.6.1 on page 3-41, taking into account the conditions in section 5.6.4.1 on page 3-45
- If the data-link-layer entity is in the timer recovery condition and it was a REJ frame, other than a REJ response frame with the F bit set to “1”, the data-link-layer entity
  - — clears any existing peer receiver busy condition
  - — sets its acknowledge state variable V(A) to the value of the N(R) contained in the REJ frame control field
  - — if it was a REJ command frame with the P bit set to “1”, it transmits an appropriate supervisory response frame with the F bit set to “1”. See footnote 1 on page 3-44 for a definition of the appropriate supervisory frame.

---

[1] If the data-link-layer entity is not in an own receiver busy condition and is in a Reject exception condition (that is, an N(S) sequence error has been received, and a REJ frame has been transmitted, but the requested I-frame has not been received), the appropriate supervisory frame is the RR frame.

If the data-link-layer entity is not in an own receiver busy condition, but is in an N(S) sequence error exception condition, (that is, an N(S) sequence error has been received but a REJ frame has not been transmitted), the appropriate supervisory frame is the REJ frame.

If the data-link-layer entity is in its own receiver busy condition, the appropriate supervisory frame is the RNR frame.

Otherwise, the appropriate supervisory frame is the RR frame.

5.6.4.1 Transmission of I-frames

When I-frames are transmitted the following conditions are taken into account:

- If the data-link-layer entity is transmitting a supervisory frame when it receives the REJ frame, it completes that transmission before commencing transmission of the requested I-frame.
- If the data-link-layer entity is transmitting a SABME command, a DISC command, a UA response, or a DM response when it receives the REJ frame, it ignores the request for retransmission.
- If the data-link-layer is not transmitting a frame when the REJ frame is received, it immediately commences transmission of the requested I-frame.

All outstanding unacknowledged I-frames, commencing with the I-frame identified in the received REJ frame are transmitted. Other I-frames not yet transmitted may be transmitted following the retransmitted I-frames.

5.6.5 Receiving RNR

If the data-link-layer entity is not engaged in a mode setting operation, after receiving a valid RNR command or response, it sets a peer receiver busy condition and then

- if it was an RNR command (with the P bit set to “1”) and the data-link-layer entity is *not* in an own receiver busy condition, it responds with an RR response (with the F bit set to “1”)
- if it was an RNR command (with the P bit set to “1”) and the data-link-layer entity *is* in an own receiver busy condition, it responds with an RNR response (with the F bit set to “1”)
- if it was an RNR response (with the F bit set to “1”) any existing timer recovery condition is cleared and the receive sequence number [N(R)] contained in the RNR response is used to update the send state variable [V(S)]

The data-link-layer entity takes note of the peer receiver busy condition and does not transmit any I-frames to the peer which has indicated the busy condition.

> ***Note:*** The receive sequence number [N(R)] in any RR or RNR command frame — irrespective of the setting of the P bit — is *not* used to update the send state variable [V(S)].

The data-link-layer entity then

- treats the receive sequence number [N(R)] contained in the received RNR frame as an acknowledgment for all the I-frames that have been (re)transmitted with an N(S) up to and including N(R) - 1. It sets its acknowledge state variable [V(A)] to the value of the N(R) contained in the RNR frame.
- restarts timer T200 unless a supervisory response frame (with the F bit set to “1”) is still expected

If timer T200 expires, the data-link-layer entity

- if it is not yet in a timer recovery condition, enters the timer recovery condition, and resets the retransmission count variable,,
- if it is already in a timer recovery condition, adds one to its retransmission count variable.

The data-link-layer entity then

- if the value of the retransmission count variable is less than N200:
    - transmits an appropriate supervisory command (with the P bit set to “1”). See footnote 1 on page 3-44 for a definition of the appropriate supervisory frame.
    - restarts timer T200
- If the value of the retransmission count variable is equal to N200, the data-link-layer entity
    - initiates a re-establishment procedure as described in section 5.7 on page 3-49.
    - indicates re-establishment is occurring by sending the *MDL-Error-Indication* primitive to the management entity.

The data-link-layer entity receiving the supervisory frame (with the P bit set to “1”) responds, at the earliest opportunity, with an appropriate supervisory response frame (with the F bit set to “1”), to indicate whether or not its own receiver busy condition still exists. See footnote 1 on page 3-44 for a definition of the appropriate supervisory frame.

When the supervisory response frame (with the F bit set to “1”) is received, the data-link-layer entity resets timer T200 and

- if the response is an RR or REJ response, the peer receiver busy condition is cleared and the data link entity may transmit new I-frames or retransmit I-frames
- if the response is an RNR response, the data-link-layer entity receiving the response proceeds as indicated in the first paragraph of this description

If a supervisory command (RR, RNR, or REJ, with the P bit set to “0”or “1”) or a supervisory response frame (RR, RNR, or REJ, with the F bit set to “0”) is received during the enquiry process, the data-link-layer entity carries out one of the following:

- If the supervisory frame is an RR or REJ command frame or an RR or REJ response frame (with the F bit set to “0”) the data-link-layer entity clears the peer receiver busy condition. I-frames are not (re)transmitted until the appropriate supervisory response frame (with the F bit set to “1”) is received, or timer T200 expires.
- If the supervisory frame is an RR or REJ command frame (with the P bit set to “1”) the data-link-layer entity transmits the appropriate supervisory response frame (with the F bit set to “1”). See footnote 1 on page 3-44 for a definition of the appropriate supervisory frame. I-frames are not (re)transmitted until the appropriate supervisory response frame (with the F bit set to “1”) is received, or timer T200 expires.
- If the supervisory frame is an RNR command frame or an RNR response frame (with the F bit set to “0”) the data-link-layer entity retains the peer receiver busy condition.
- If the supervisory frame received is an RNR command (with the P bit set to “1”) the data-link-layer entity transmits the appropriate supervisory response frame (with the F bit set to “1”). See footnote 1 on page 3-44 for a definition of the appropriate supervisory frame.

When a SABME command is received, the data-link-layer entity clears the peer receiver busy condition.

5.6.6 Data link layer own receiver busy condition

When the data-link-layer entity enters an own receiver busy condition, it transmits a receiver not ready (RNR) frame at the earliest opportunity.

The RNR frame may be one of the following:

- an RNR response (with the F bit set to “0”)
- an RNR response (with the F bit set to “1”) if the busy condition occurs when a command frame (with the P bit set to “1”) is received
- an RNR command (with the P bit set to “1”) if the busy condition occurs when timer T200 expires

All I-frames (with the P bit set to “0”) that are received, are discarded after the acknowledge state variable [V(A)] is updated.

All supervisory frames (with the P/F bit set to “0”) that are received are processed, including updating the acknowledge state variable [V(A)].

All I-frames (with the P bit set to “1”) that are received are discarded, after the acknowledge state variable [V(A)] is updated. An RNR response frame (with the F bit set to “1”) is transmitted.

All supervisory frames (with the P bit set to “1”) that are received are processed including updating the acknowledge state variable [V(A)]. An RNR response (with the F bit set to “1”) is transmitted.

To indicate to the peer data-link-layer entity that the own receiver busy condition has been cleared, the data-link-layer entity transmits one of the following:

- an RR frame
- if a previously detected N(S) sequence error has not been reported, an REJ frame with the N(R) set to the current value of the receive state variable [V(R)]

The transmission of a SABME command or a UA response (in reply to a SABME command) also indicates to the peer data-link-layer entity that the own receiver busy condition has been cleared.

5.6.7 Waiting acknowledgment

The data-link-layer entity maintains an internal retransmission count variable.

If timer T200 expires, the data-link-layer entity

- if it is *not* in the timer recovery condition, enters the timer recovery condition and resets the retransmission count variable
- if it *is* in the timer recovery condition, adds one to its retransmission count variable,

The data-link-layer entity then

- if the value of the retransmission count variable is less than N200:
  - — restarts timer T200, and, either
    - – transmits an appropriate supervisory command (with the P bit set to “1”) (see footnote 1 on page 3-44 for a definition of the appropriate supervisory frame)
    - – retransmits the last transmitted I-frame [V(S) - 1] (with the P bit set to “1”)
- if the value of the retransmission count variable is equal to N200
  - — initiates a re-establishment procedure as defined in section 5.7 on page 3-49
  - — indicates this to the management entity by issuing the *MDL-Error-Indication* primitive

The timer recovery condition is cleared when the data-link-layer entity receives a valid supervisory frame response (with the F bit set to “1”).

If the receive sequence number [N(R)] of the received supervisory frame is within the range from its current acknowledge state variable [V(A)] to its current send state variable [V(S)] inclusive, it sets its send state variable [V(S)] to the value of the received N(R).

Timer T200 is reset if the received supervisory frame response is an RR or REJ response. After the timer is reset, the data-link-layer entity resumes I-frame (re)transmission, as appropriate.

Timer T200 is reset and restarted if the received supervisory response is an RNR response. This allows the enquiry process, described in section 5.6.5 on page 3-45, to proceed.

5.7 Re-establishment of multiple frame operation

5.7.1 Criteria for re-establishment

To re-establish the multiple-frame mode of operation, one or more of the following conditions must be satisfied:

- while in the multiple-frame mode of operation, a SABME command is received
- a *DL-Establish-Request* primitive is received from Layer 3
- while in the timer recovery condition, the occurrence of N200 retransmission failures
- the occurrence of a frame rejection condition as identified in section 5.8.5 on page 3-51
- while in the multiple-frame mode of operation, an FRMR response frame is received
- while in the multiple-frame mode of operation, an unsolicited DM response (with the F bit set to “0”) is received
- while in a timer recovery condition, a DM response (with the F bit set to “1”) is received

5.7.2 Procedures

In all re-establishment situations, the data-link-layer entity follows the procedures defined in section 5.5.1 on page 3-36. Any locally generated condition that causes re-establishment procedures to be started, causes a SABME command to be transmitted.

For data-link-layer- and peer-initiated re-establishment, the data-link-layer entity also

- issues an *MDL-Error-Indication* primitive to the management entity

- if the send state variable [V(S)] > acknowledge state variable [V(A)], issues a *DL-Establish-Indication* primitive to Layer 3, and discards all I queues prior to re-establishing the call

For Layer 3-initiated re-establishment, or if a *DL-Establish-Request* primitive occurs before re-establishment, the *DL-Establish-Confirm* primitive is used.

5.8 Exception condition reporting and recovery

Exception conditions may occur as the result of physical layer errors or data-link-layer procedural errors.

The error recovery procedures which are available to effect recovery following the detection of an exception condition at the data link layer are defined in the following sections.

5.8.1 Send sequence number [N(S)] sequence error

A send sequence number [N(S)] sequence error exception condition occurs in the receiver when a valid I-frame is received in which the send sequence number [N(S)] is not equal to the receive state variable [V(R)].

All information fields of all I-frames whose N(S) does not equal V(R) are discarded.

The receiver does not acknowledge the I-frame causing the sequence error or increment its receive state variable [V(R)]. It does not acknowledge any I-frames which may follow. Recovery from this condition is indicated when an I-frame with the correct send sequence number [N(S)] is received.

A data-link-layer entity which receives one or more I-frames having sequence errors which are otherwise error free, or subsequent supervisory frames (RR, RNR, and REJ), uses the control field information contained in the N(R) field and the P or F bit to perform data link control functions. For example, it receives acknowledgment of previously transmitted I frames and causes the data-link-layer entity to respond if the P bit is set to “1”. Therefore, the retransmitted I-frame may contain an N(R) field value and P bit that are updated from (and different from) those contained in the originally transmitted I-frame.

The REJ frame is used by a receiving data-link-layer entity to initiate an exception condition recovery (retransmission) following the detection of an N(S) sequence error. Only one REJ exception condition for a given direction of information transfer can be established at any one time.

When a data-link-layer entity receives a REJ command or response it initiates sequential transmission (retransmission) of all I-frames starting with the I frame indicated by the N(R) contained in the REJ frame.

A REJ exception condition is cleared when the requested I-frame is received or when a SABME or DISC command is received.

5.8.2 Receive sequence number [N(R)] sequence error

A receive sequence number [N(R)] sequence error exception condition occurs in the transmitter when a valid supervisory frame or I-frame is received which contains an invalid receive sequence number [N(R)] value.

A valid N(R) is one that is in the range: $V(A) \le N(R) \le V(S)$

The information field contained in an I-frame that is in sequence and is error-free may be delivered to Layer 3 using the *DL-Data-Indication* primitive.

The data-link-layer entity informs the management entity of this exception condition using the MDL-*Error-Indication* primitive, and initiates re-establishment according to the procedures defined in section 5.7 on page 3-49.

5.8.3 Timer recovery condition

If a data-link-layer entity, due to a transmission error, does not receive a single I-frame or the last I-frame(s) in a sequence of I-frames, it cannot detect an out-of-sequence exception condition and therefore, does not transmit a REJ frame.

The data-link-layer entity which transmitted the unacknowledged I-frame(s), on the expiry of timer T200 takes the recovery action defined in section 5.6.7 on page 3-48 to determine which I-frame(s) must be re-transmitted.

5.8.4 Invalid frame condition

Any frame received which is invalid is discarded. No other action is taken as a result of that frame being received. Invalid frames are defined in section 2.9 on page 3-13 and section 3.6 on page 3-23.

5.8.5 Frame rejection condition

A frame rejection condition occurs when undefined commands or response frames are received. See section 3.6.1 on page 3-23 and section 3.6.11 on page 3-25 for a listing of such commands and responses

When a frame rejection condition occurs while in multiple-frame mode of operation, the data-link-layer entity

- issues an *MDL-Error-Indication* primitive
- initiates re-establishment, as described in section 5.7 on page 3-49

5.8.6 Receipt of an FRMR response frame

When an FRMR response frame is received, while in the multiple-frame mode of operation, the data-link-layer entity

- issues an *MDL-Error-Indication* primitive

- initiates re-establishment as described in section 5.7 on page 3-49

5.8.7 Unsolicited response frames

The action taken on the receipt of an unsolicited response frame is defined in Table 2-3.

5.8.8 Multiple assignment of a TEI value

Not supported in this specification.

Table 2-3
Action on receipt of an unsolicited response frame

Unsolicited response frame	TEI assigned	Awaiting estab-lishment	Awaiting release	Multiple frames modes of operation	
				Established mode	Timer recovery condition
UA response: F = 1	Issue MEI	Solicited	Solicited	Issue MEI	Issue MEI
UA response: F = 0	Issue MEI	Issue MEI	Issue MEI	Issue MEI	Issue MEI
DM response: F = 1	Ignore	Solicited	Solicited	Issue MEI	Re-establish Issue MEI
DM response: F = 0	Establish	Ignore	Ignore	Re-establish Issue MEI	Re-establish Issue MEI
Supervisory response: F = 1	Ignore	Ignore	Ignore	Issue MEI	Solicited
Supervisory response: F = 0	Ignore	Ignore	Ignore	Solicited	Solicited

Key:

Issue MEI	Issue *MDL-Error-Indication* primitive to Layer 3
Ignore	Ignore response
Establish	Establish multiple-frame mode of operation
Re-establish	Re-establish multiple-frame mode of operation

5.9 List of system parameters

The system parameters listed below are associated with each individual service access point (SAP).

The parameter values are assigned when the data link is configured. Only default values of the parameters are supported by the network.

5.9.1 Timer T200

The default value for timer T200, at the end of which transmission of a frame may be initiated according to the procedures described in section 5.6 on page 3-41, is one second.

> ***Note:*** The proper operation of the procedure requires that the time-out for timer T200 be set greater than the maximum time between transmission of command frames and the reception of their corresponding response or acknowledgment frames.

5.9.2 Maximum number of retransmissions, N200

The default value of N200 is 3.

5.9.3 Maximum number of octets in an information field, (N201)

The maximum number of octets that can be inserted into a frame is set using the system parameter N201.

The default value of N201 is 260 octets.

5.9.4 Maximum number of transmissions of an identity request message, (N202)

Not supported in this specification.

5.9.5 Maximum number of outstanding I-frames, k

The maximum number (k) of sequentially numbered I-frames that may be outstanding (that is, unacknowledged) at any given time is a system parameter that does not exceed 127.

The default value is 7.

5.9.6 TEI identity check timer, T201

Not supported in this specification.

5.9.7 Timer, T202

Not supported in this specification.

5.9.8 Data link verification timer, T203

The data link verification timer, T203, is used to set the maximum period that the data link is allowed to remain active without frames being exchanged.

The default value of timer T203 is 10 seconds.

5.10 Data-link-layer monitor function

5.10.1 General

The procedural elements defined in this chapter allow for the supervision of the data-link-layer resource. This section describes procedures which may be used to provide this supervision function.

5.10.2 Data link layer supervision in the multiple-frame-established state

The following procedures propose a solution which is already identified in the HDLC classes of procedures. Connection verification is a service provided by the data link layer to Layer 3. This implies that Layer 3 is informed in case of a failure only. Furthermore, the procedure may be incorporated in the “normal” exchange of information and may become more efficient than a procedure based on the involvement of Layer 3.

The procedure is based on supervisory command frames (RR command, RNR command) and the data link verification timer (T203). It operates in the multiple-frame-established state as follows.

If there are no frames being exchanged on the data link connection (neither new or outstanding I-frames, or supervisory frames with the P bit set to “1”) there is no means to detect a faulty data link connection condition, or to detect if the user equipment has been unplugged. The data link verification timer (T203) represents the maximum time allowed without frames being exchanged.

If timer T203 expires, a supervisory command (with the P bit set to “1”) is transmitted.

Such a procedure is protected against transmission errors by making use of the procedures associated with the timer T200 and the maximum number of retransmissions, N200.

5.10.3 Connection verification procedures

5.10.3.1 Start of data link verification timer, T203

The data link verification timer, T203 is started

- when the multiple-frame-established state is entered
- AND, whenever timer T200 is stopped while in the multiple-frame established state (that is, T200 and T203 are never running concurrently)

When an I or supervisory frame is received, timer T203 is restarted if timer T200 is not to be started.

5.10.3.2 Stop of data link verification timer, T203

The data link verification timer, T203, is stopped

- when in the multiple-frame established state, timer T200 is started (see note), *and*
- when leaving the multiple-frame established state.

Note: These two conditions mean that timer T203 is only started whenever T200 is stopped and not restarted.

5.10.3.3 Expiry of timer T203

If timer T203 expires — and timer T200 is neither running or expired — the data-link-layer entity

- sets the retransmission count variable to zero
- enters the timer recovery state
- transmits a supervisory-type command (with the P bit set to “1”) as follows:
  - if there is *not* a receiver busy condition (own receiver not busy), it transmits an RR command
  - if there *is* a receiver busy condition (own receiver busy), it transmits an RNR command
- starts timer T200
- sends an *MDL-Error-Indication* primitive to layer management after N200 retransmissions

Chapter 3-6: Occurrence of *MDL-Error-Indication*

6.1 Introduction

The *MDL-Error-Indication* primitive is used to notify the management entity of the data link layer of error situations. The error situations for which this primitive is generated are shown in Table 2-4.

The associated error parameter contains the error code that describes the unique error conditions. The table also identifies the associated management actions that are taken by the network and should be taken by the user side, for the various types of error reported.

The following paragraphs provide a key to the information contained in Table 2-4.

Error code

The *Error code* column gives the identification value for each error situation that is included as a parameter with the *MDL-Error-Indication* primitive.

Error condition and affected states

The *Error condition* column together with the *Affected states* column describes the unique protocol error events and the state of the data link layer entity at the time that the *MDL-Error-Indication* primitive is generated.

Network management action

For each error condition, the *Network management action* column describes the preferred action taken by the network management entity.

User management action

This column describes the preferred action taken by the user side management entity on a given error condition.

6.2 Preferred management actions

The various preferred management actions on an error situation may be described as one of the following:

- Error Log
  - This suggests that the network side management entity has the preferred action of logging the event in an error counter. The length and the operation of the counter mechanisms for the error situations are implementation dependent.
- TEI Remove
  - This suggests that the user side layer management entity may directly remove its TEI value from service.

In most of the described error situations, there is either no action to be taken on the user side layer management or the action to be taken by the user side is implementation dependent. It is therefore a user side option to incorporate any form of error counter to log or store the reported event.

If action is taken, the layer management entity has to take into account that the data link layer has initiated a recovery procedure.

Table 2-4
Management entity actions for MDL-Error-Indications.

Error code	Error condition	Affected states *	Network management action	User management action
Receipt of unsolicited response (error codes A through E)				
A	Supervisory frame (F = 1)	7	Error log	Implementation dependent
B	DM frame (F = 1)	7, 8	Error log	Implementation dependent
C	UA frame (F = 1)	4, 7, 8	Error log	Implementation dependent
D	UA frame (F = 0)	4, 5, 6, 7, 8	Error log	Implementation dependent
E	Receipt of DM response (F =0)	7, 8	Error log	Implementation dependent
Peer initiated re-establishment (error code F)				
F	SABME frame	7, 8	Error log	Implementation dependent
Unsuccessful retransmission (after N200 retries) (error codes G through I)				
G	SABME frame	5	Error log	Implementation dependent
H	DISC frame	6	Error log	Implementation dependent
I	Status enquiry	8	Error log	Implementation dependent
Other errors (error codes J through O)				
J	N(R) error	7, 8	Error log	Implementation dependent
K	Receipt of FRMR response	7, 8	Error log	Implementation dependent
L	Receipt of non-implemented frame	4, 5, 6, 7, 8	Error log	Implementation dependent
M	Receipt of I field not permitted	4, 5, 6, 7, 8	Error log	Implementation dependent
N	Receipt of frame with wrong size	4, 5, 6, 7, 8	Error log	Implementation dependent
O	N201 error	4, 5, 6, 7, 8	Error log	Implementation dependent

Chapter 3-7: Layer 2 SDL diagrams

To assist in the understanding of the data link layer, this chapter provides an example of a detailed SDL (Specification and description language) diagram of the point-to-point procedures.

This representation does not describe all of the possible actions of the data link layer entity. In particular, the non-partitioned representation does not show all possible interactions and imposes an order in the sequence of events that may not be necessary. A non-partitioned representation was chosen to minimize complexity in the SDL representation. This SDL representation should not therefore constrain implementations from exploiting the full flexibility of the procedures as presented within the text of this specification. The text description of the procedures is definitive.

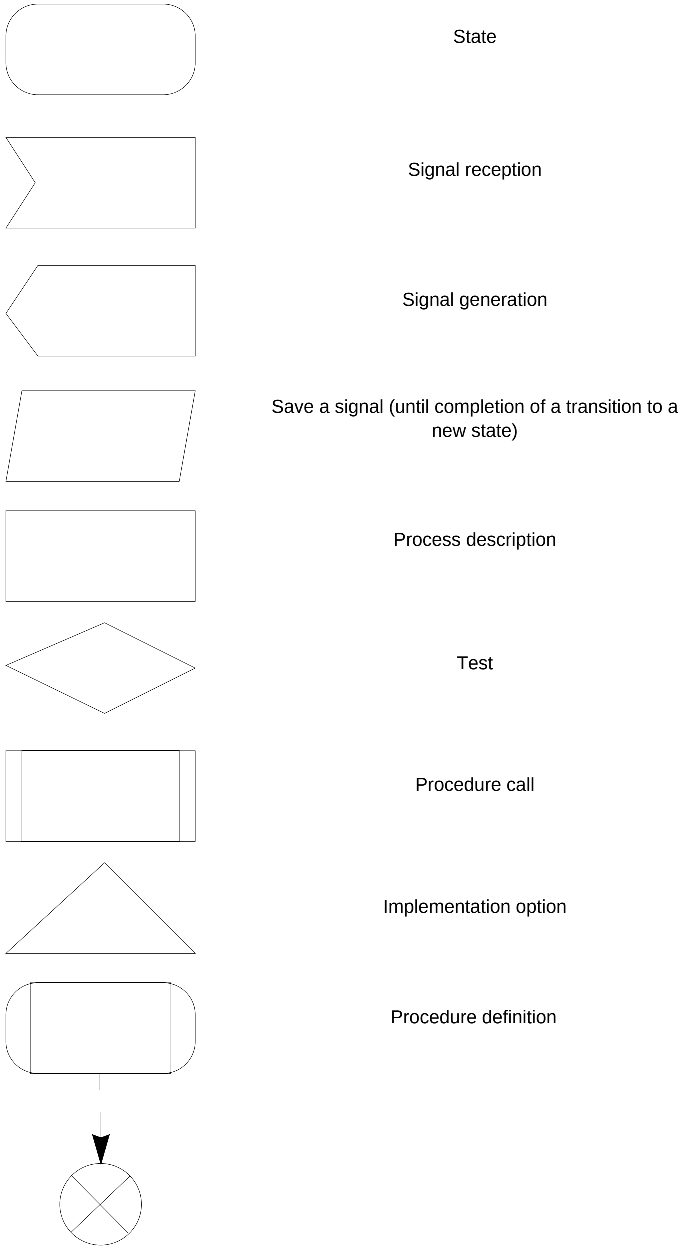
The representation is a peer-to-peer model of the point-to-point procedures of the data-link layer and is applicable to the data-link-layer entities at both the user and network sides for all ranges of TEI values.

7.1 Use of queues

To enable a satisfactory representation of the data-link-layer entity, conceptual queues for the I-frame transmission has been explicitly brought out. These conceptual queues are finite but unbounded and should in no way restrict the implementation of the point-to-point procedures. An additional signal has been provided (I frame queued up) to initiate the servicing of these queues.

Figure 3-14 shows the symbols and abbreviations used in the SDL representations. Full descriptions of their meanings and application can be found in the CCITT Z series of recommendations.

Figure 3-14
SDL symbol key



***	To mark an event or signal required as a result of the representation approach adopted, which is local to the data link layer entity
RC	Retransmission counter
A - O	Used to represent the MDL-Error-Indication signals as defined in Chapter 3-6. Where multiple codes are shown, only one applies

Figure 3-15
State transition diagram

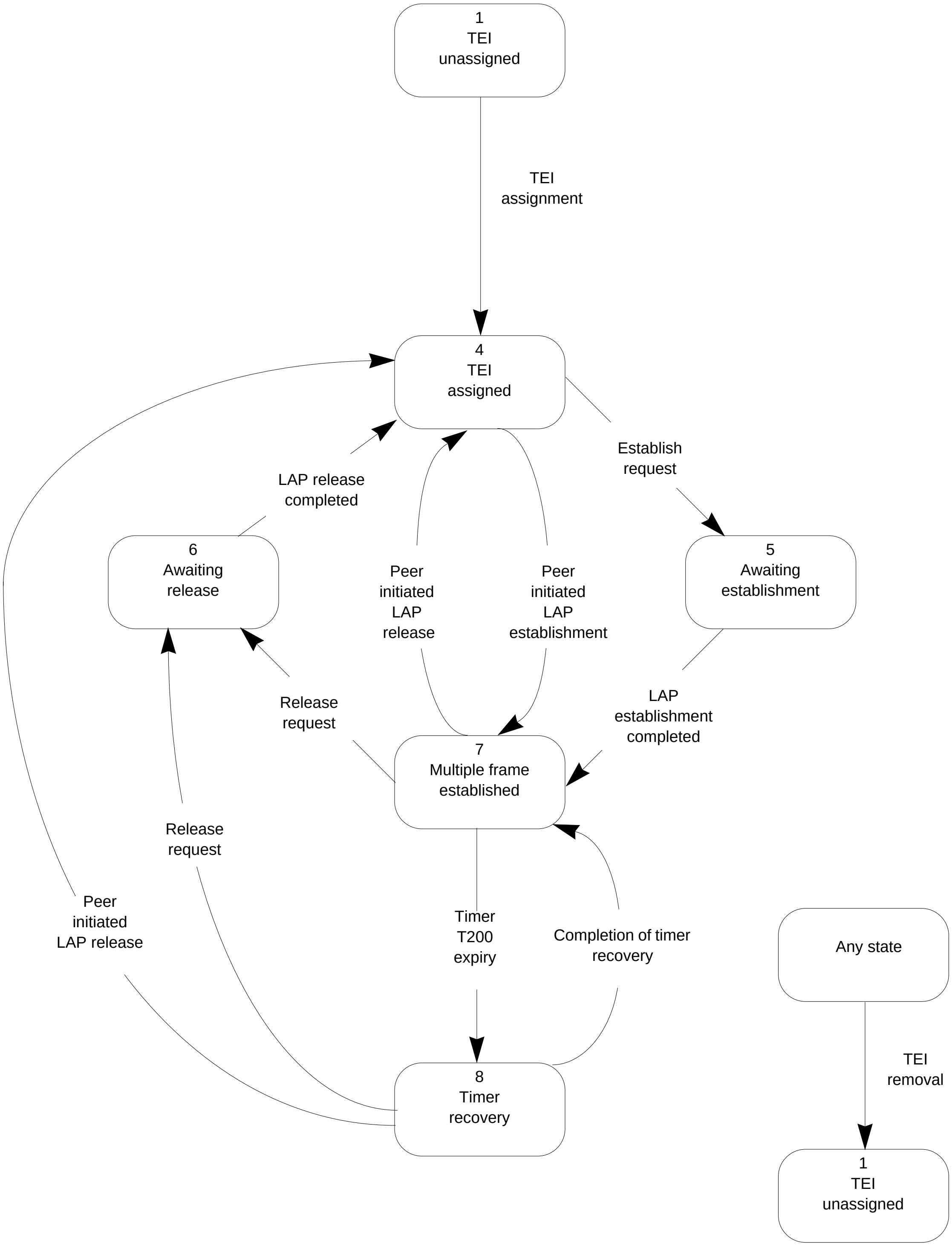


Figure 3-16
Layer 2 SDL diagrams (1 of 22)

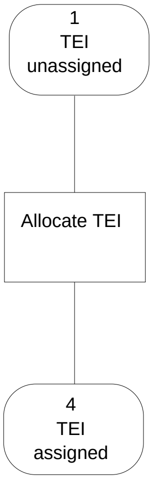


Figure 3-17
Layer 2 SDL diagrams (2 of 22)

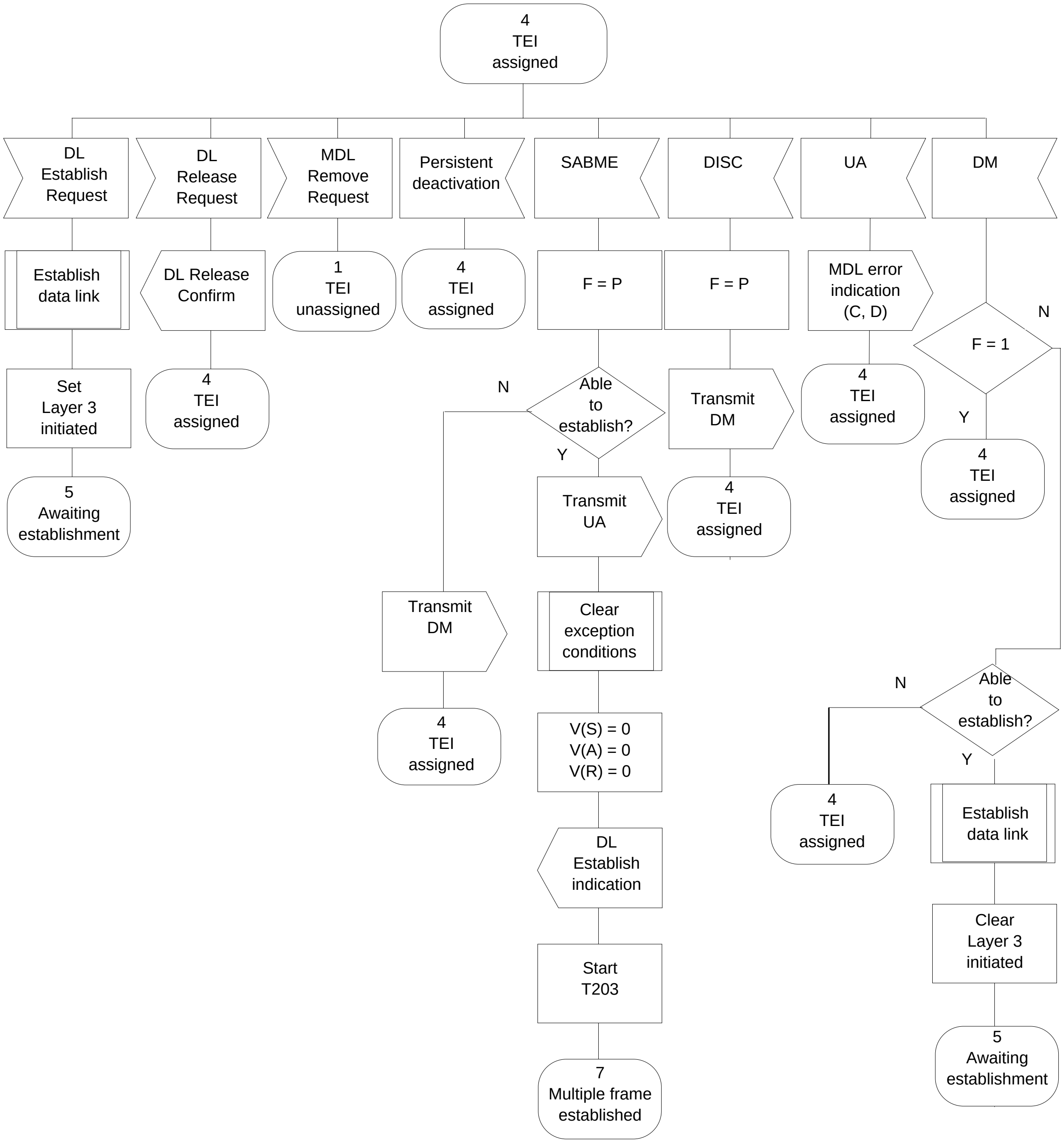
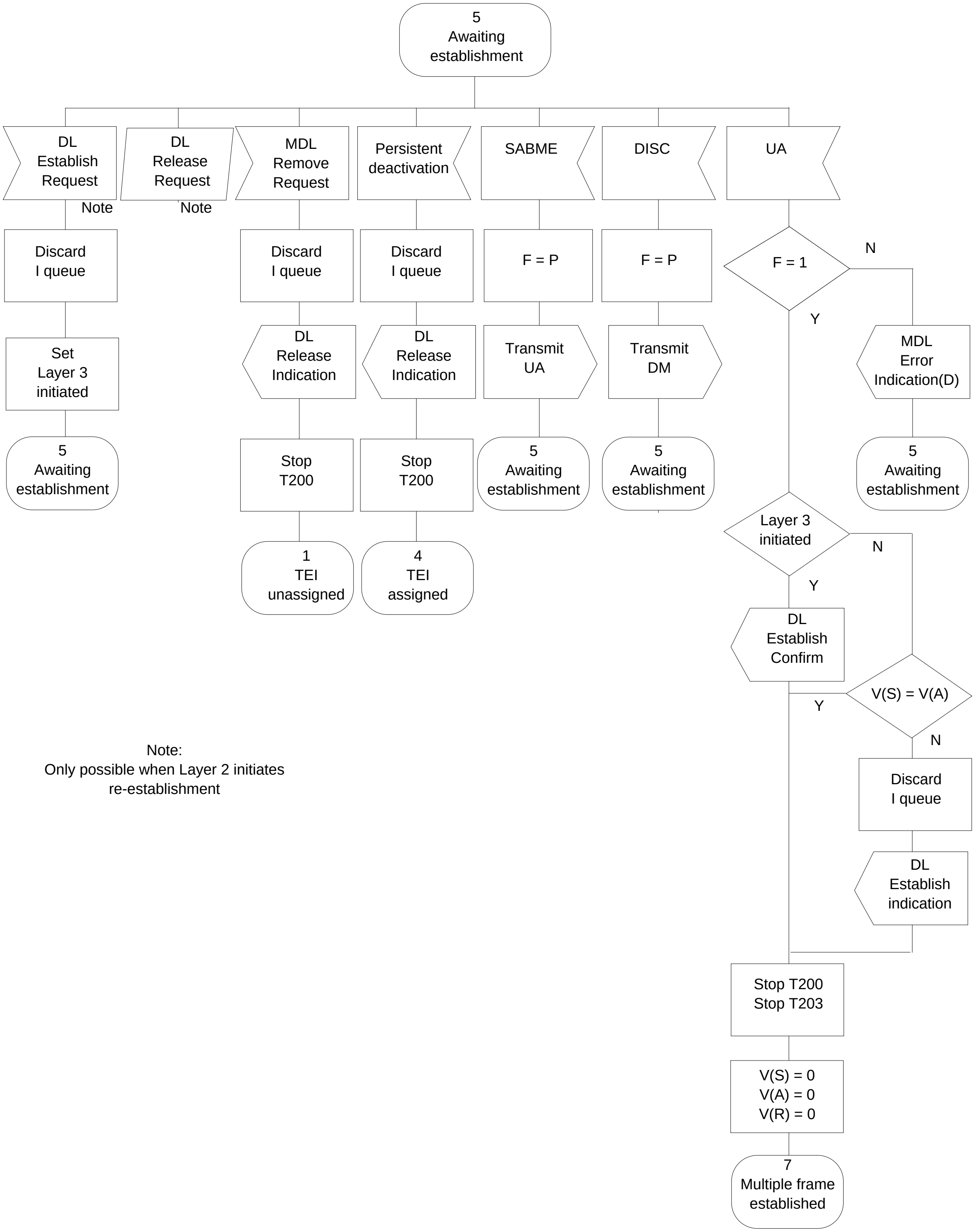
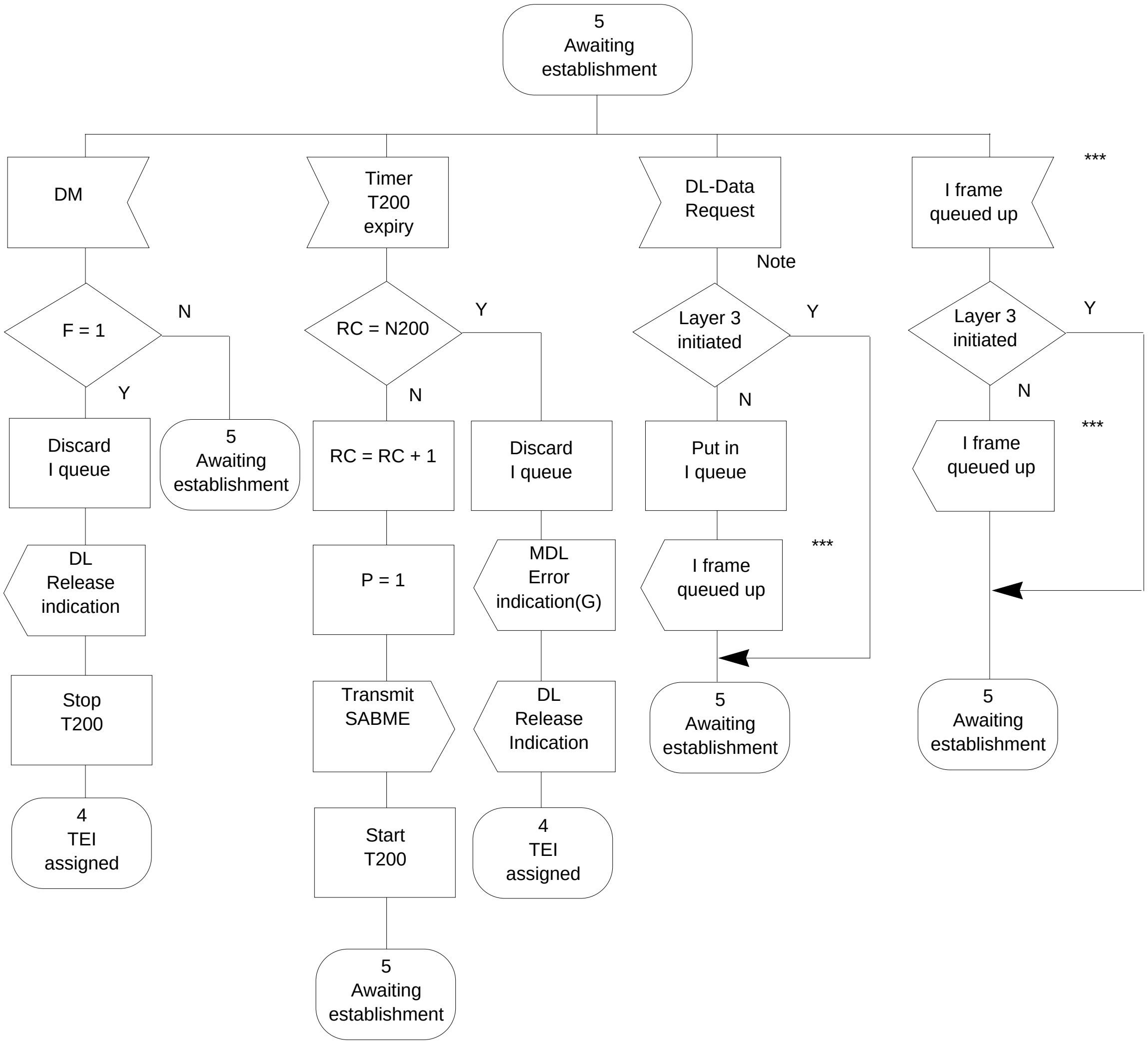


Figure 3-18
Layer 2 SDL diagrams (3 of 22)



Note:
Only possible when Layer 2 initiates
re-establishment

Figure 3-19
Layer 2 SDL diagrams (4 of 22)



Note:
Only possible when Layer 2 initiates
re-establishment

Figure 3-20
Layer 2 SDL diagrams (5 of 22)

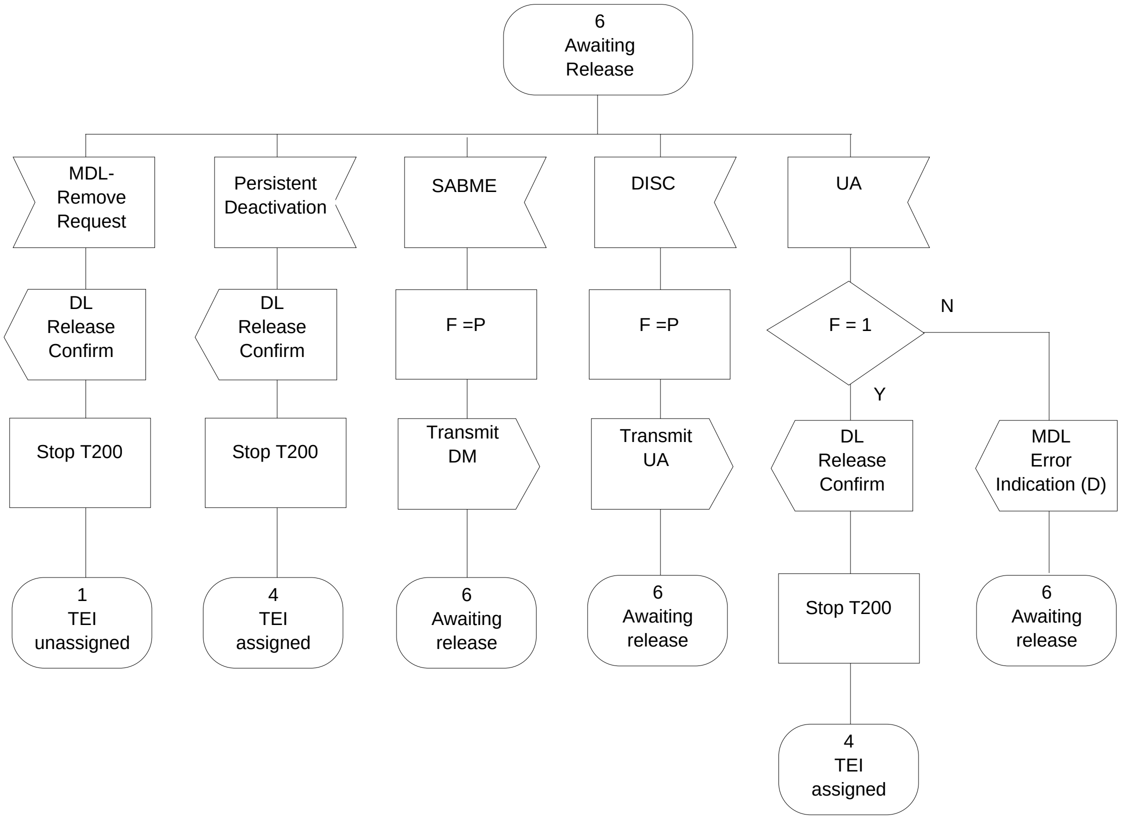


Figure 3-21
Layer 2 SDL diagrams (6 of 22)

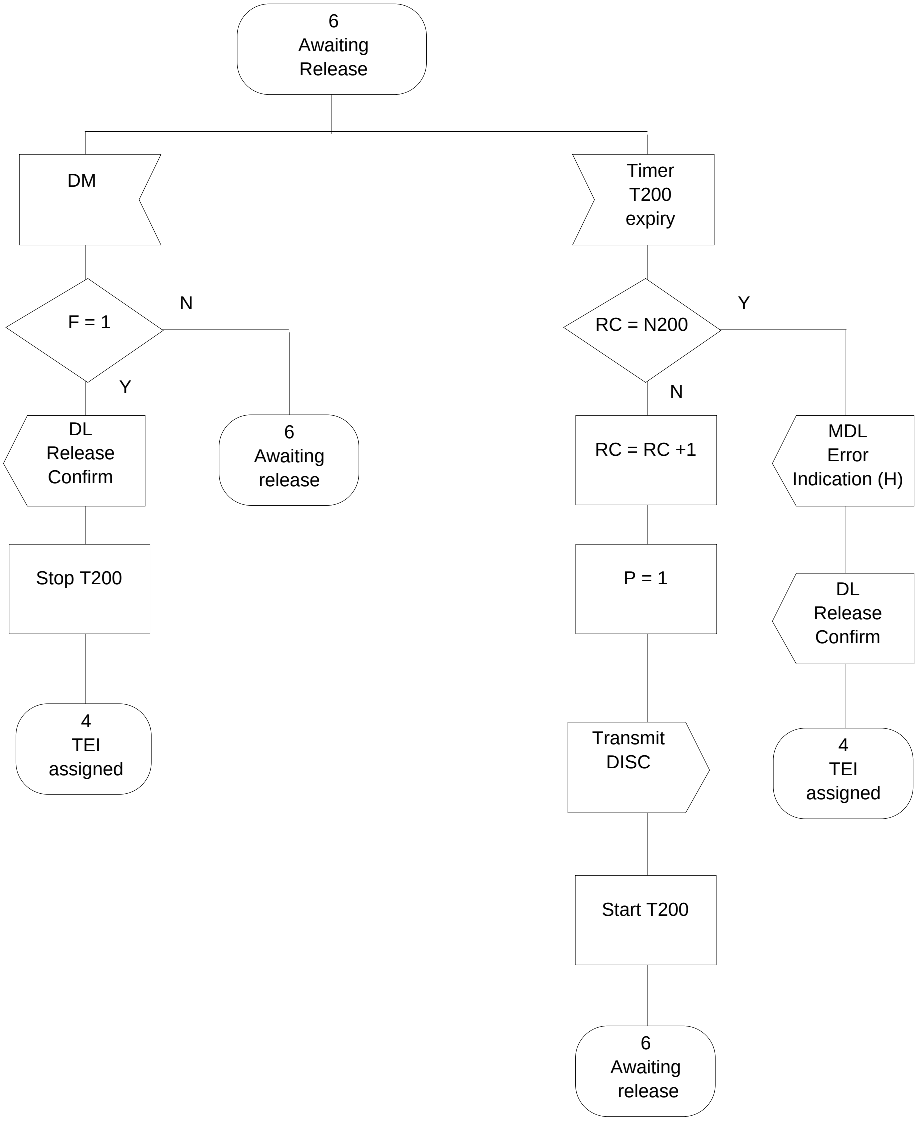
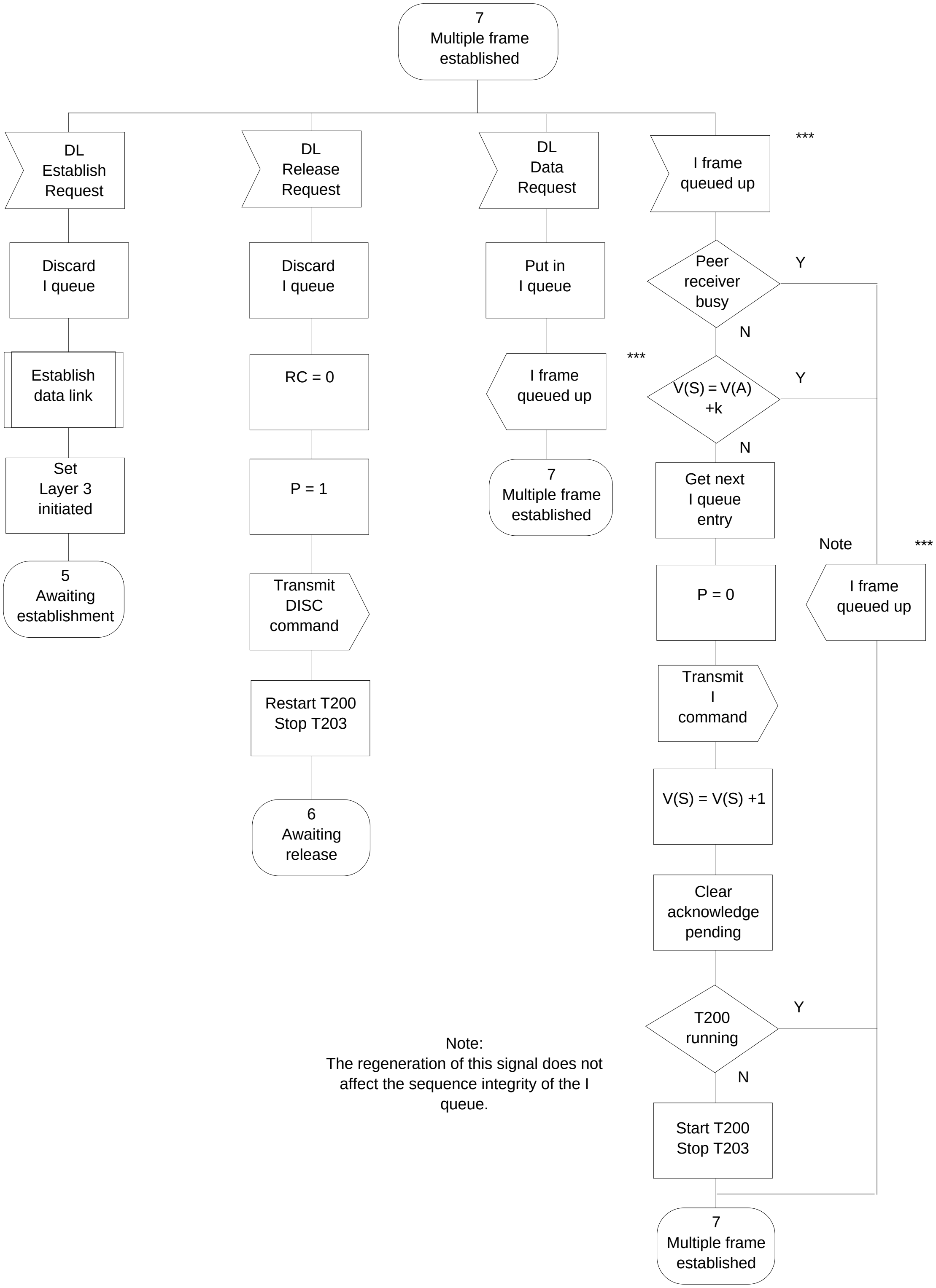
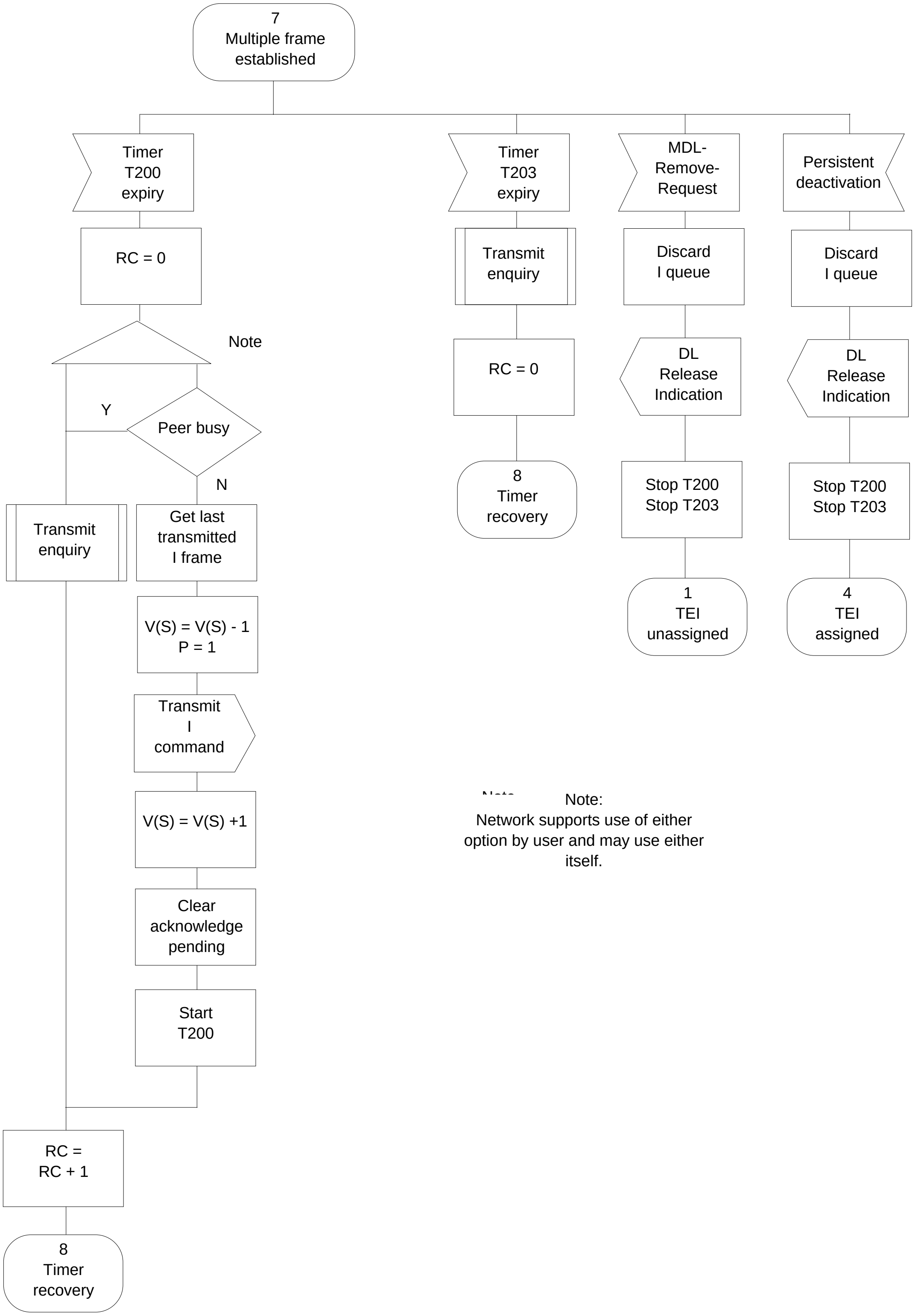


Figure 3-22
Layer 2 SDL diagrams (7 of 22)



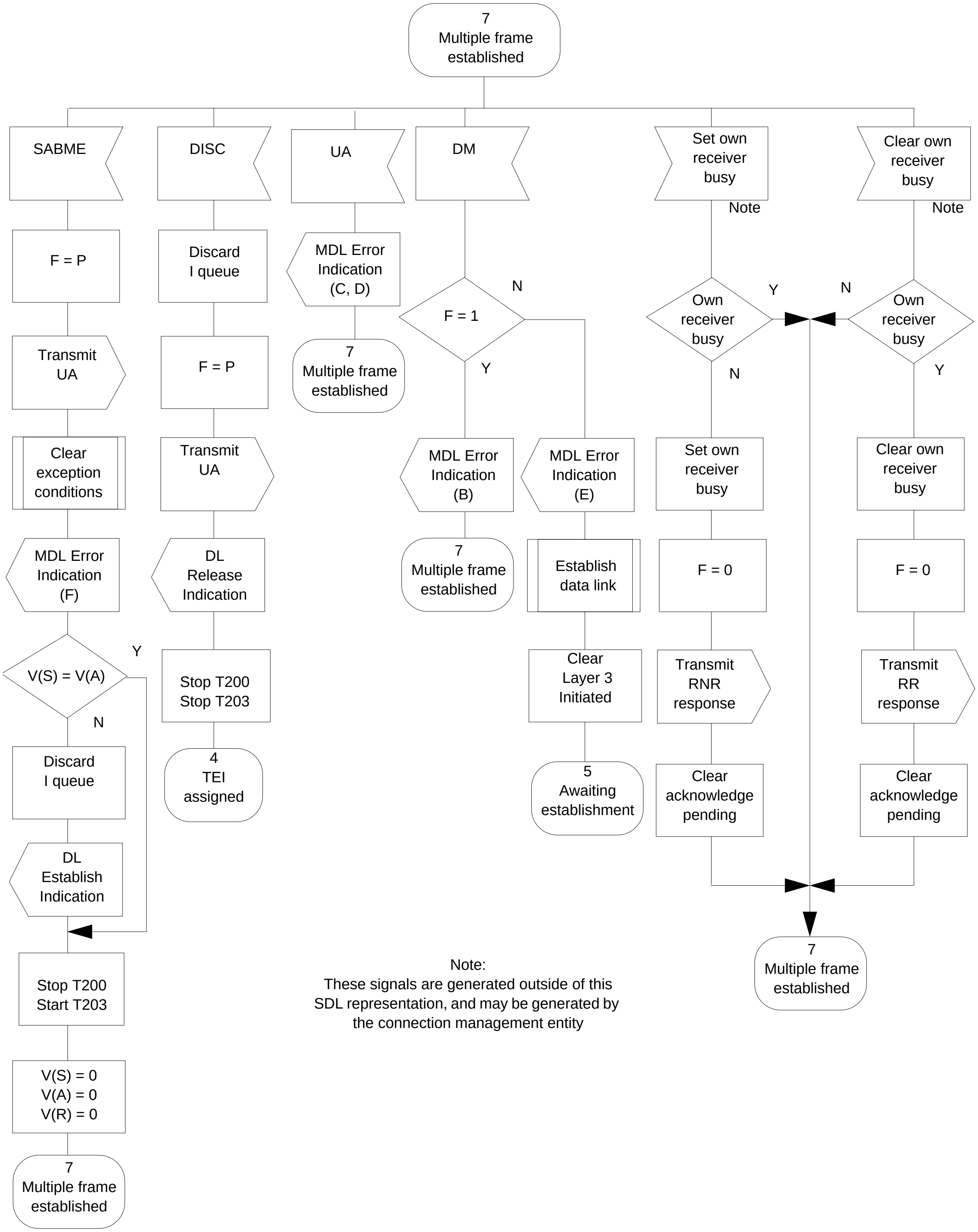
Note:
The regeneration of this signal does not affect the sequence integrity of the I queue.

Figure 3-23
Layer 2 SDL diagrams (8 of 22)



Note:
Network supports use of either option by user and may use either itself.

Figure 3-24
Layer 2 SDL diagrams (9 of 22)



Note:
These signals are generated outside of this SDL representation, and may be generated by the connection management entity

Figure 3-25
Layer 2 SDL diagrams (10 of 22)

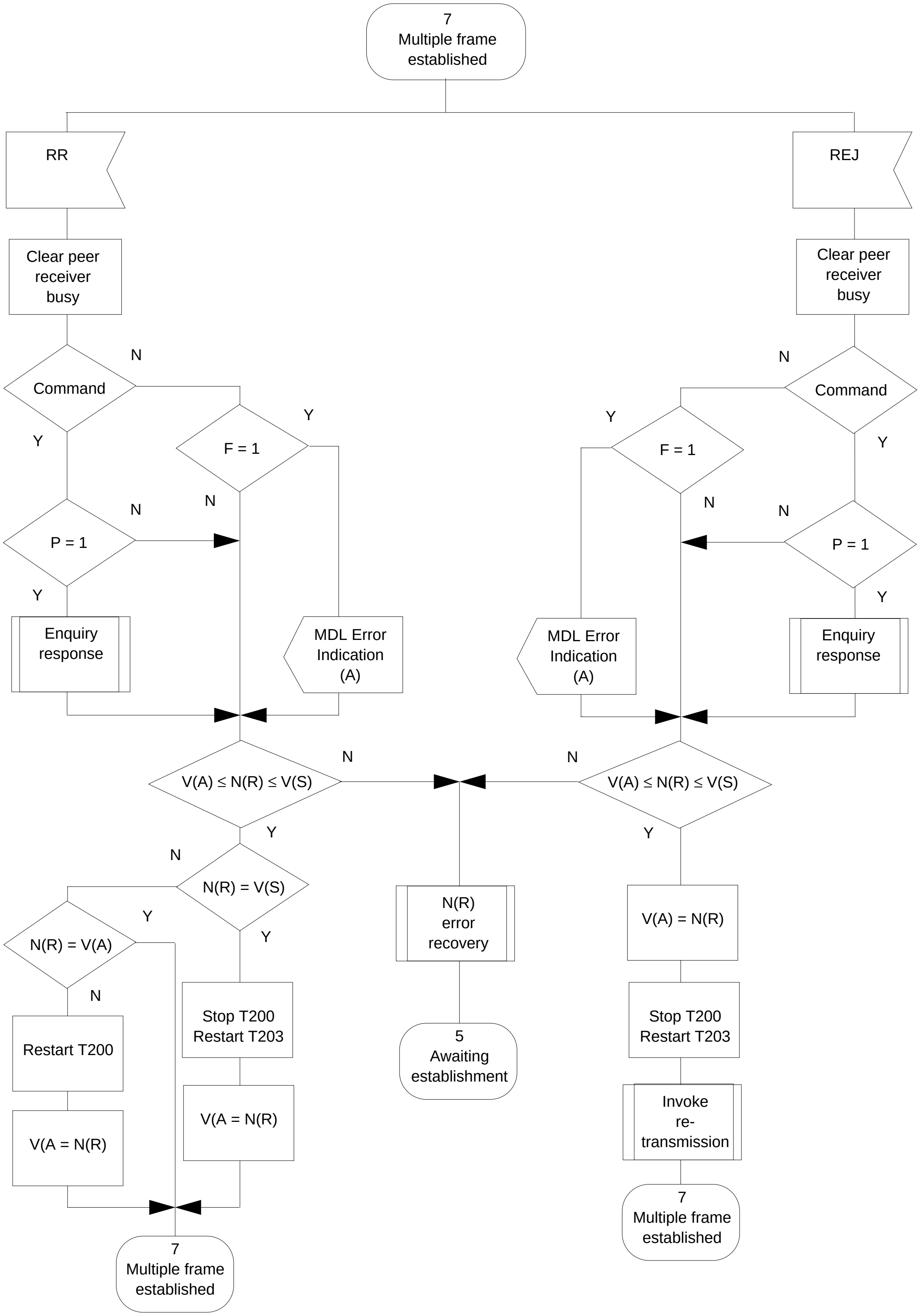


Figure 3-26
Layer 2 SDL diagrams (11 of 22)

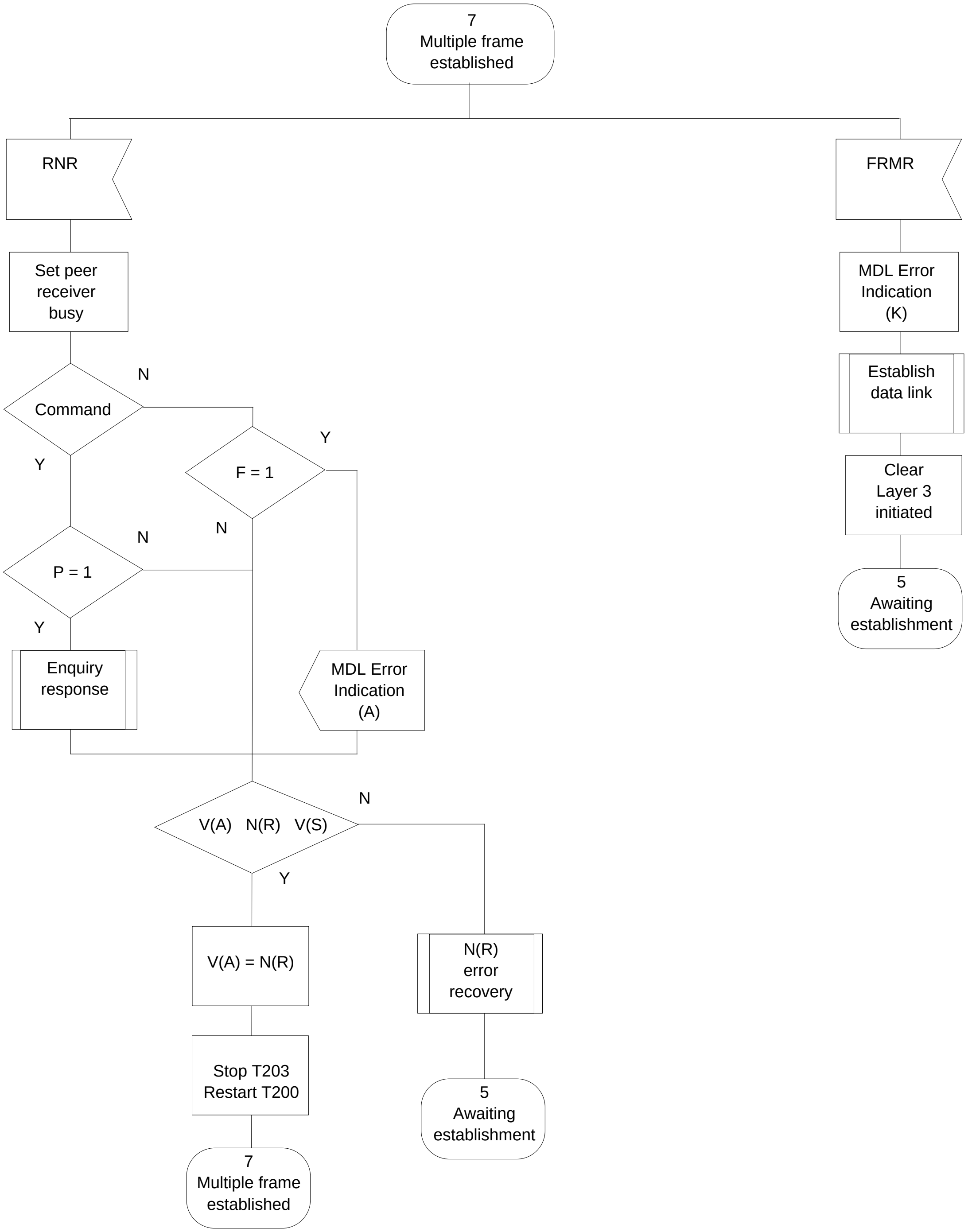


Figure 3-27
Layer 2 SDL diagrams (12 of 22)

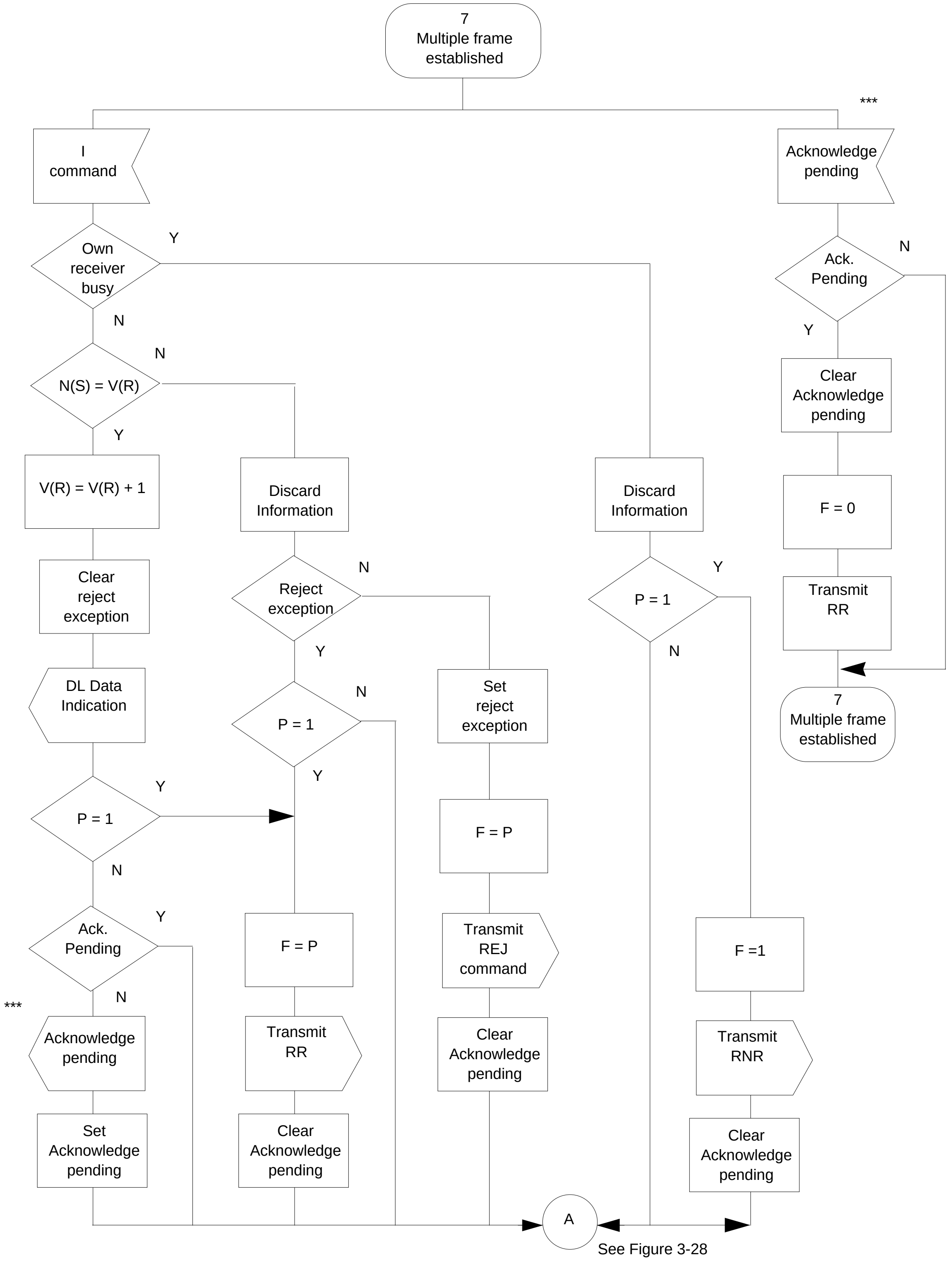


Figure 3-28
Layer 2 SDL diagrams (13 of 22)

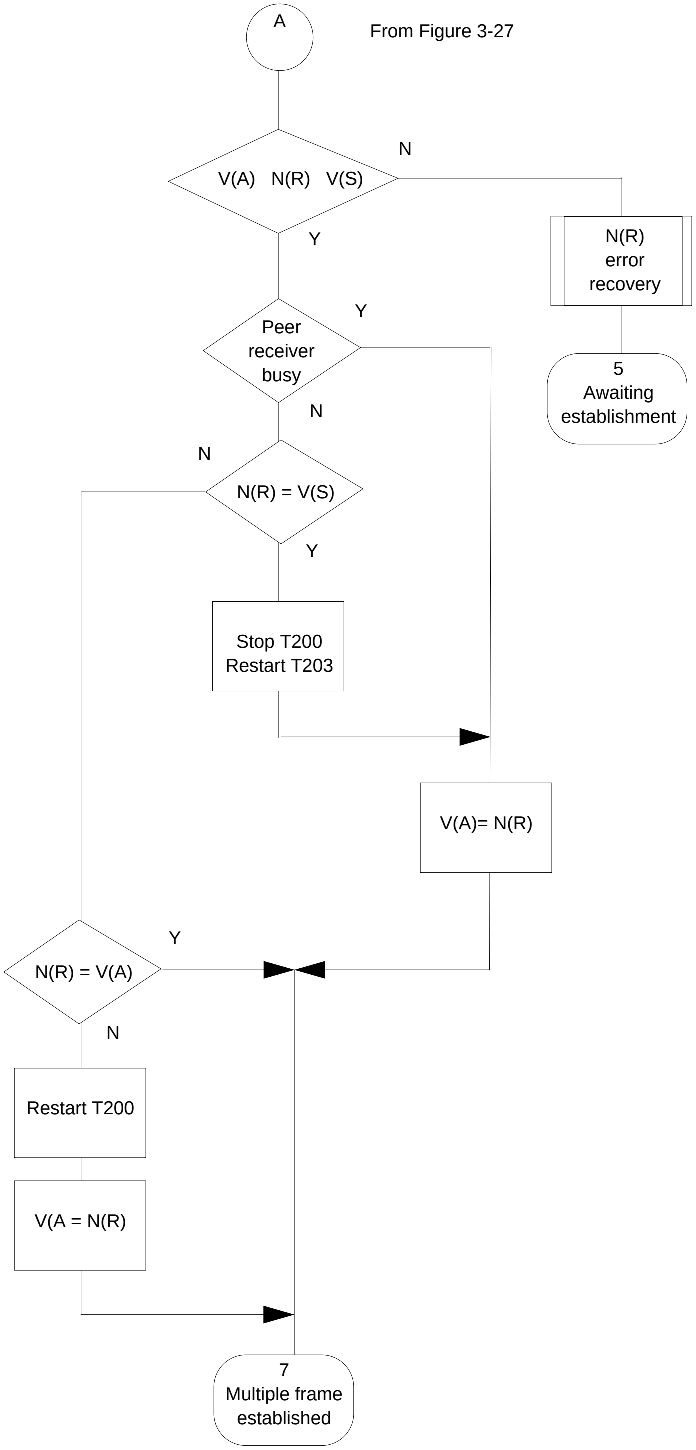


Figure 3-29
Layer 2 SDL diagrams (14 of 22)

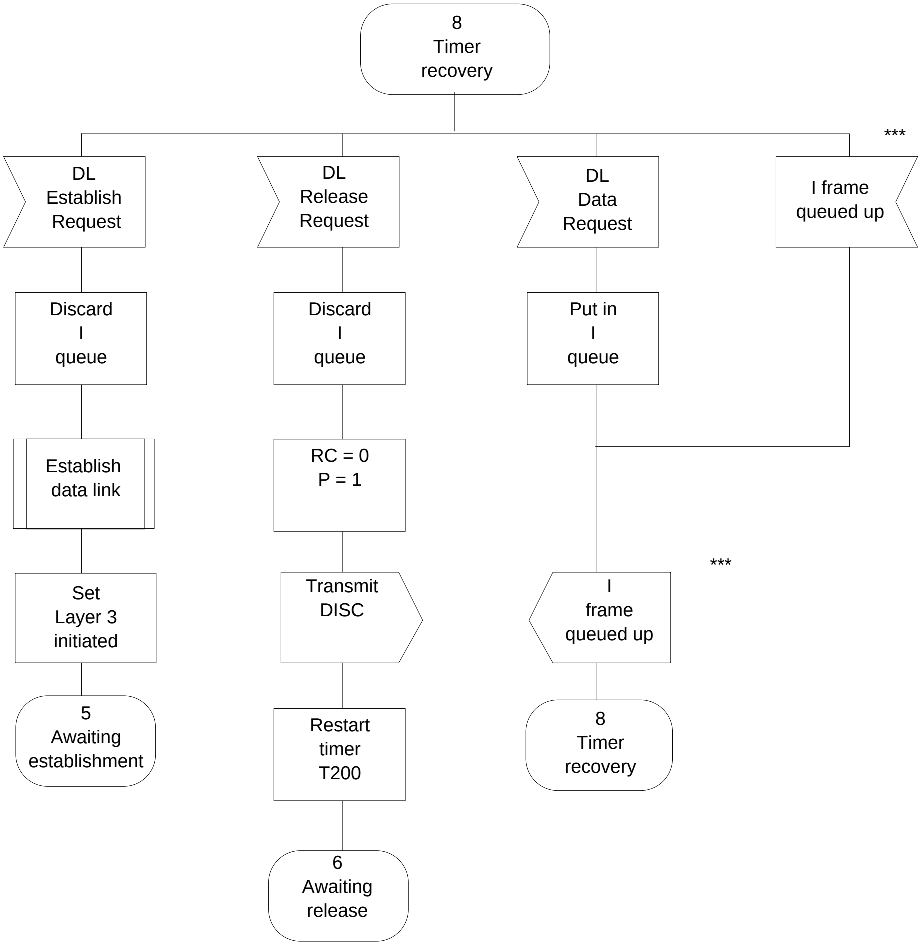
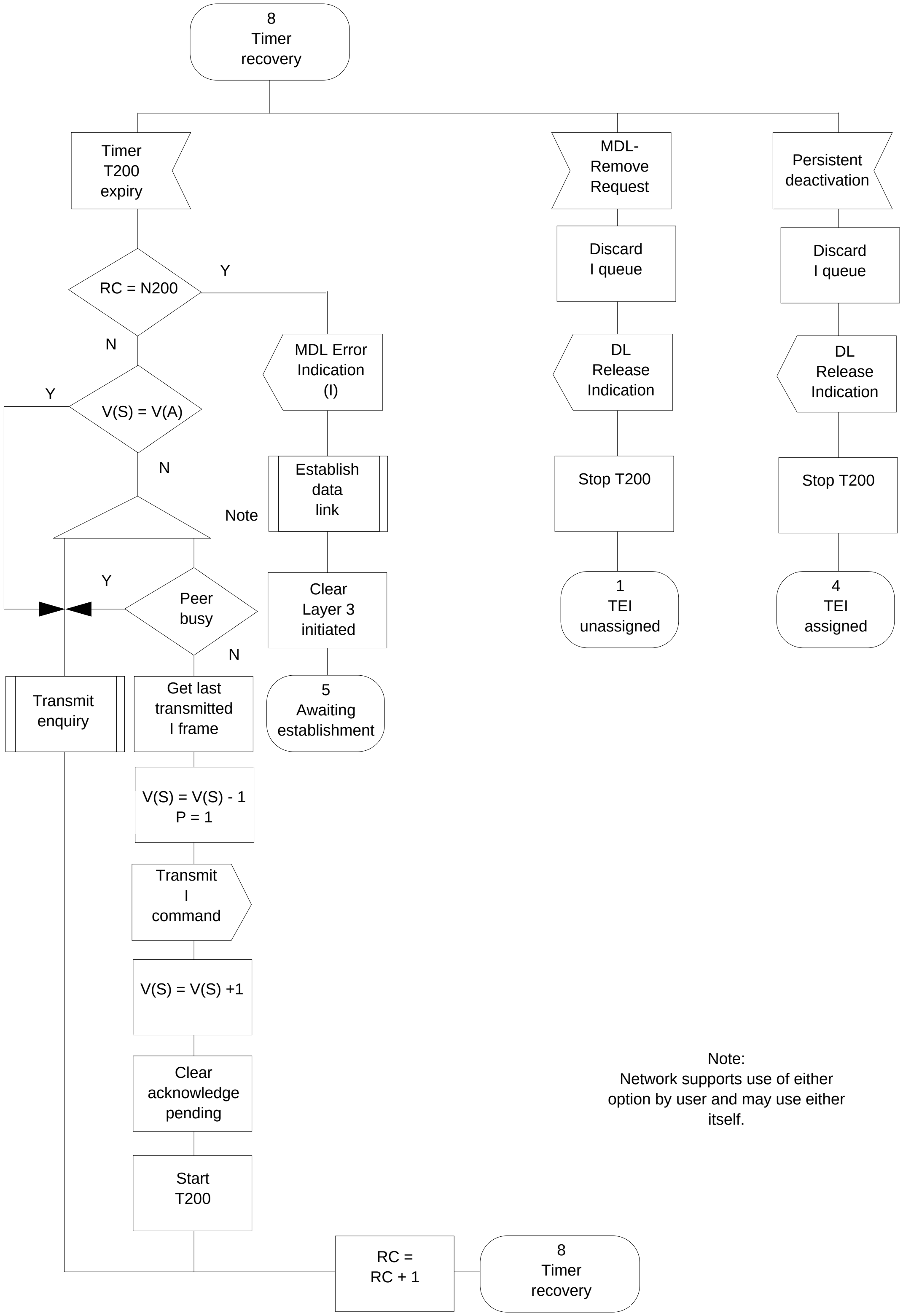


Figure 3-30
Layer 2 SDL diagrams (15 of 22)



Note:
Network supports use of either option by user and may use either itself.

Figure 3-31
Layer 2 SDL diagrams (16 of 22)

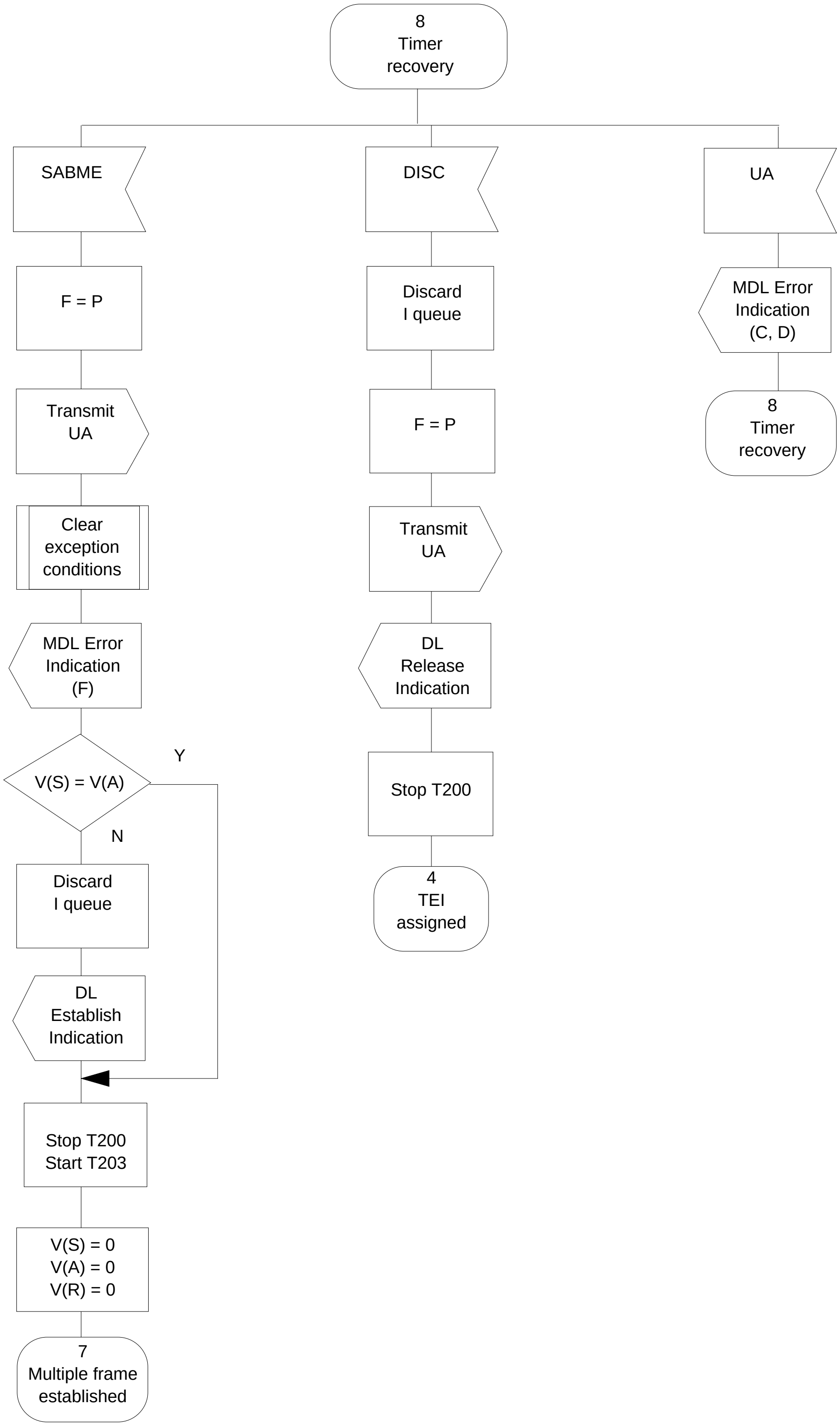
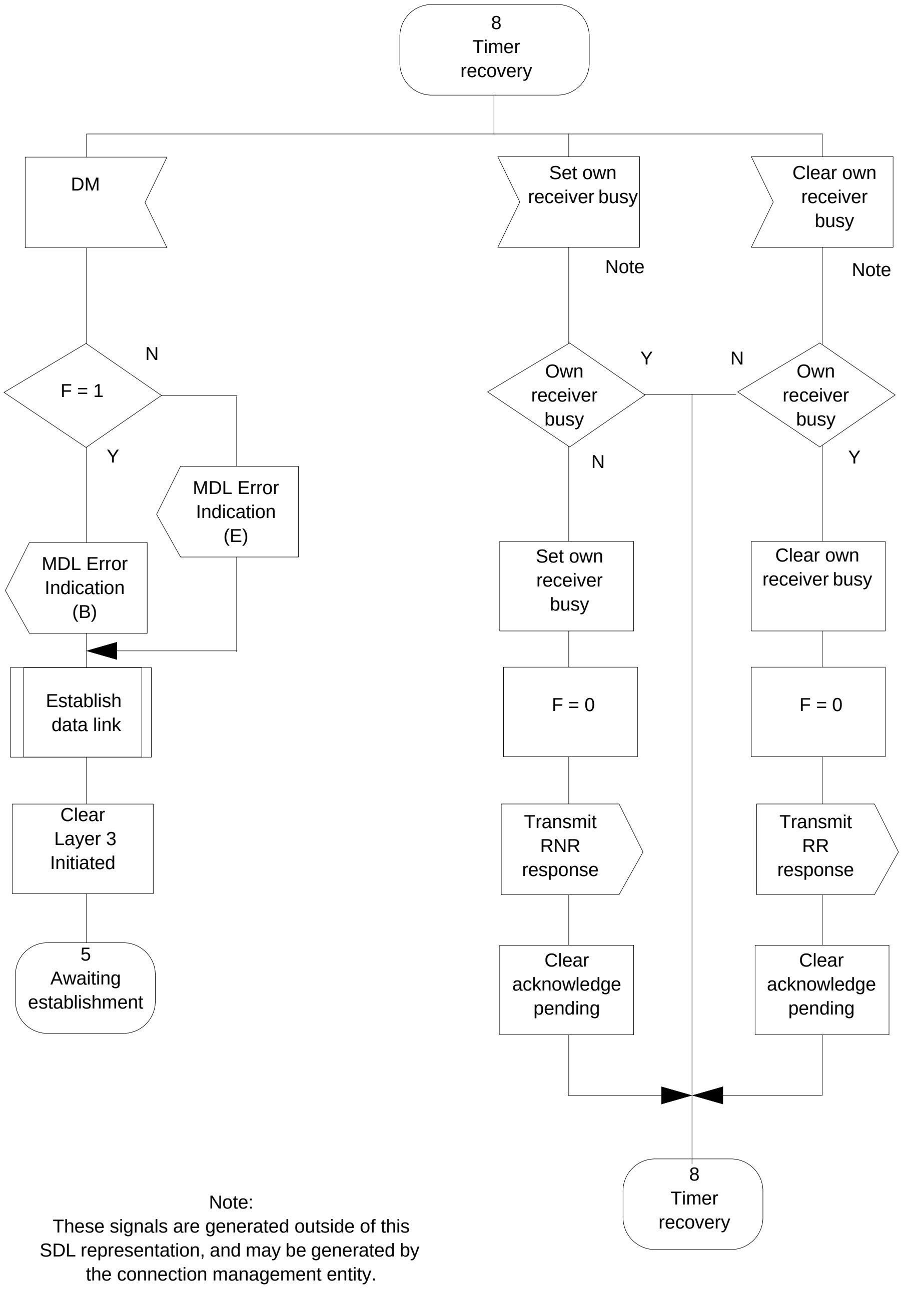


Figure 3-32
Layer 2 SDL diagrams (17 of 22)



Note:
These signals are generated outside of this SDL representation, and may be generated by the connection management entity.

Figure 3-33
Layer 2 SDL diagrams (18 of 22)

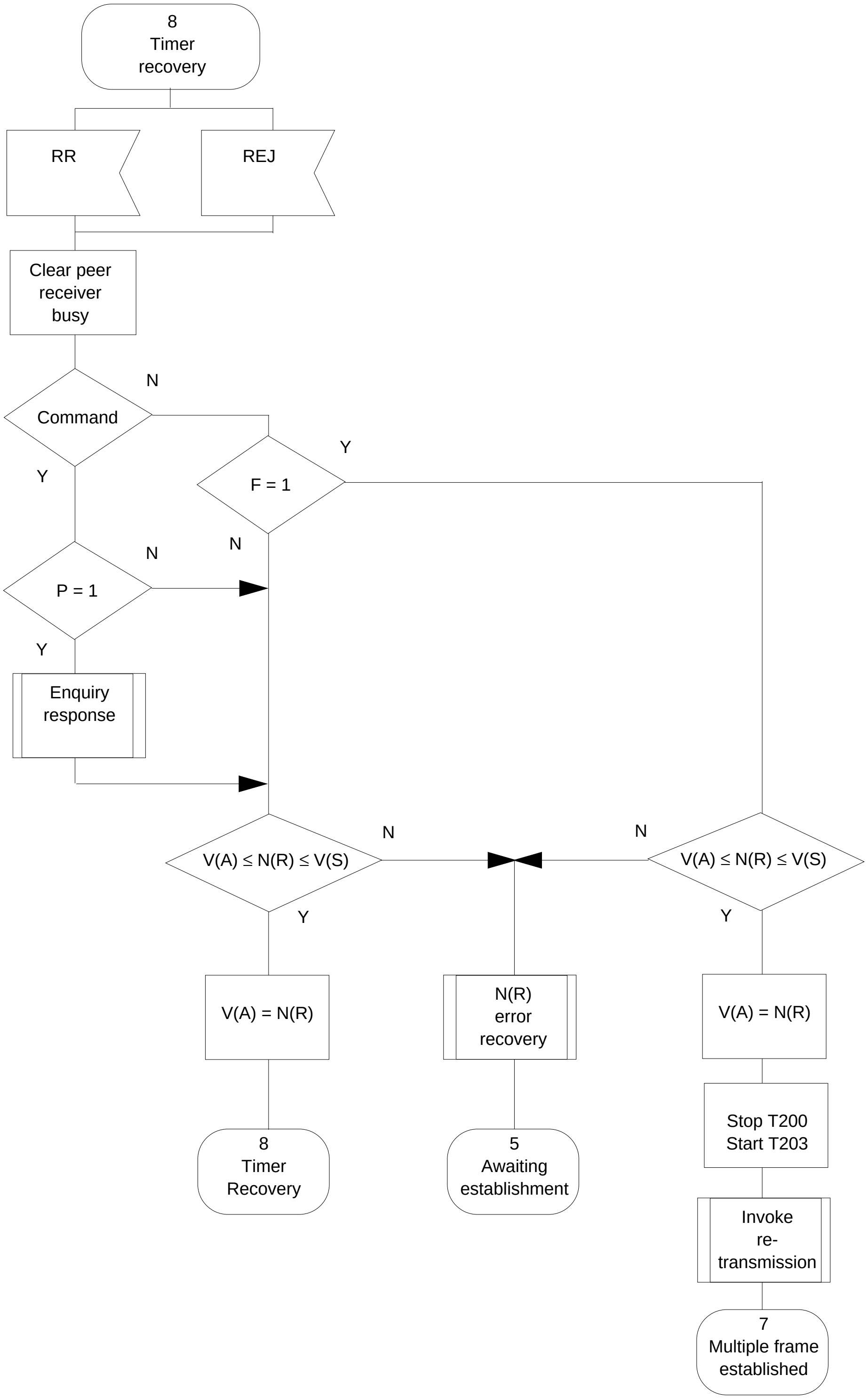


Figure 3-34
Layer 2 SDL diagrams (19 of 22)

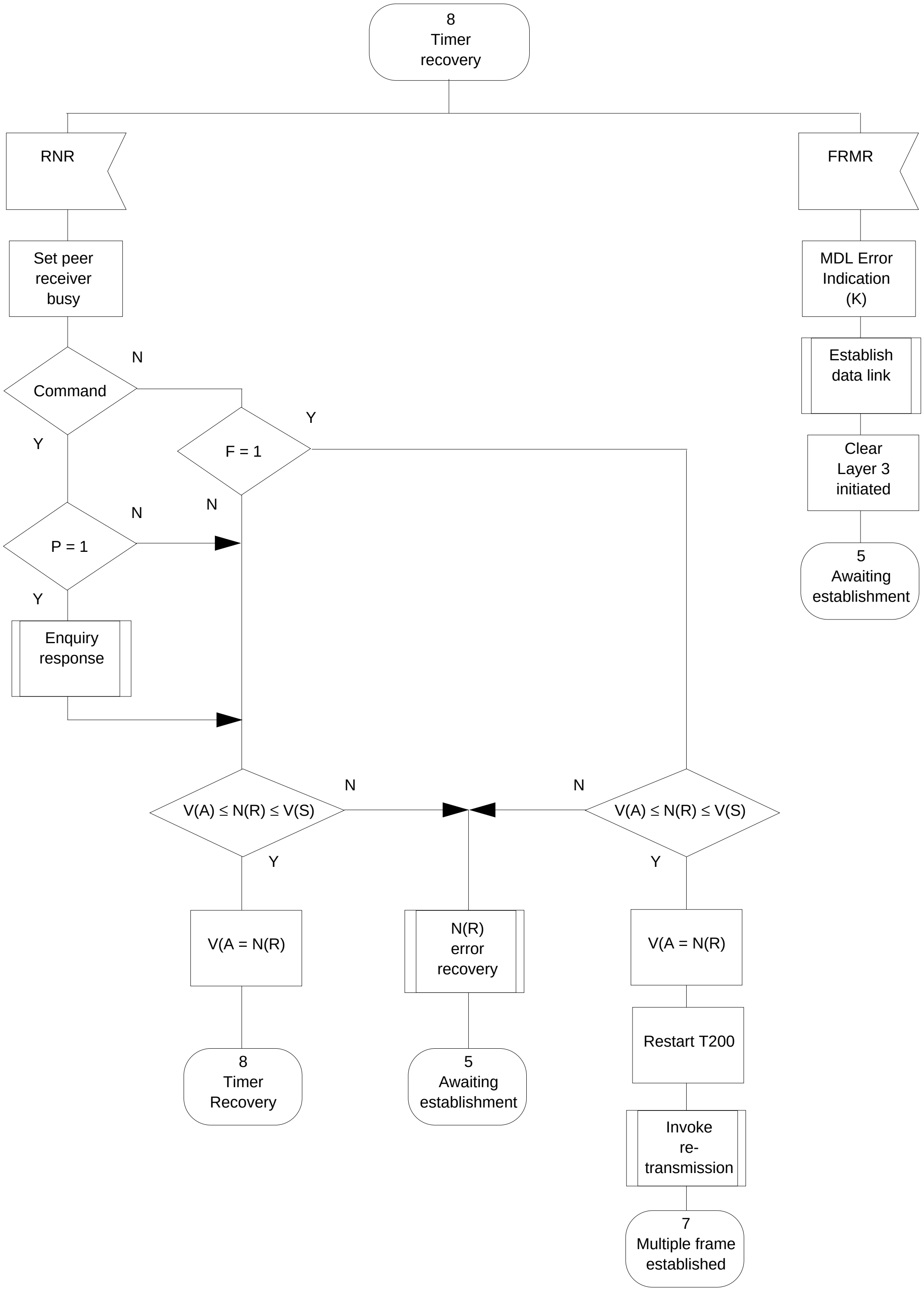


Figure 3-35
Layer 2 SDL diagrams (20 of 22)

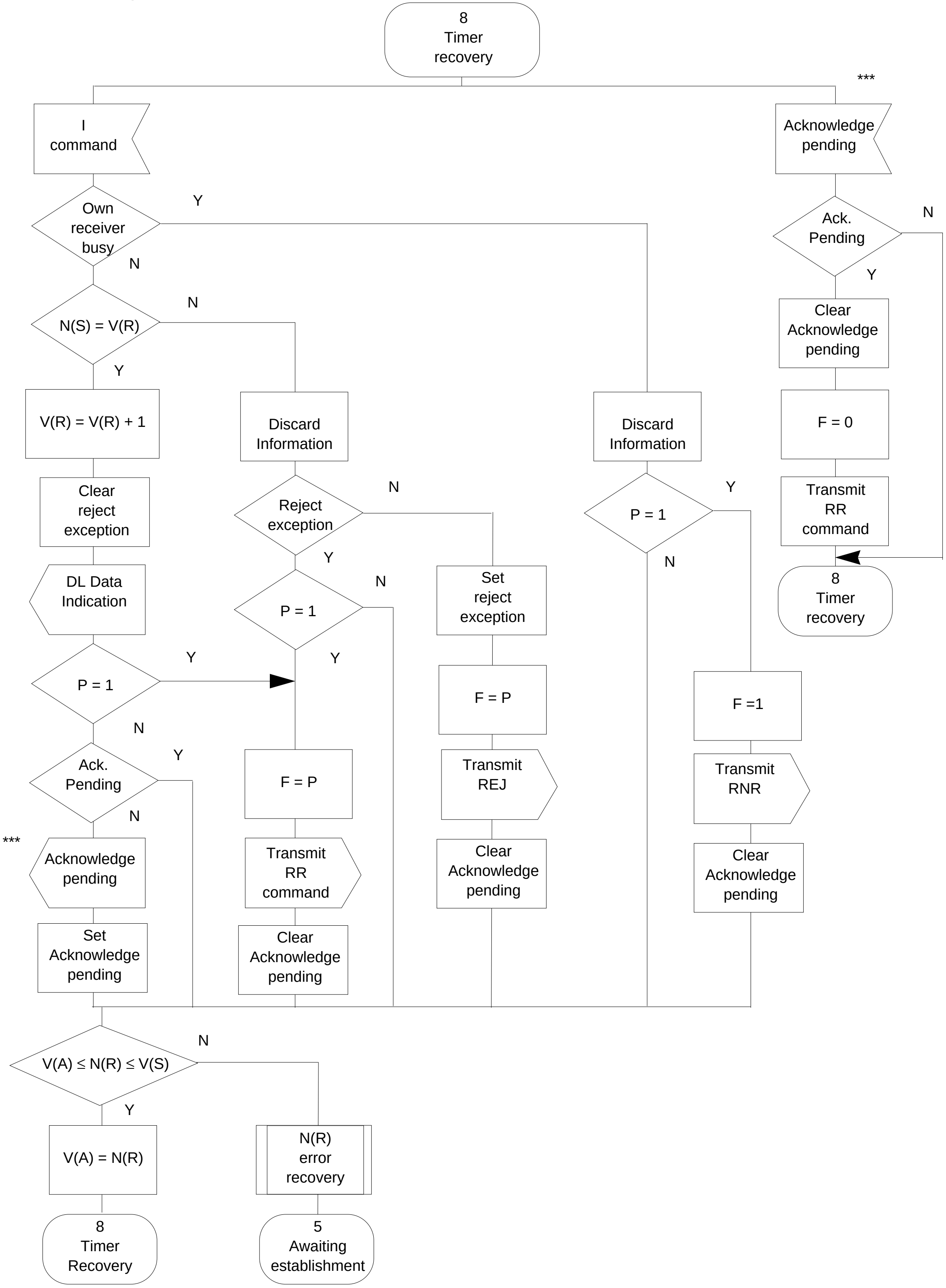
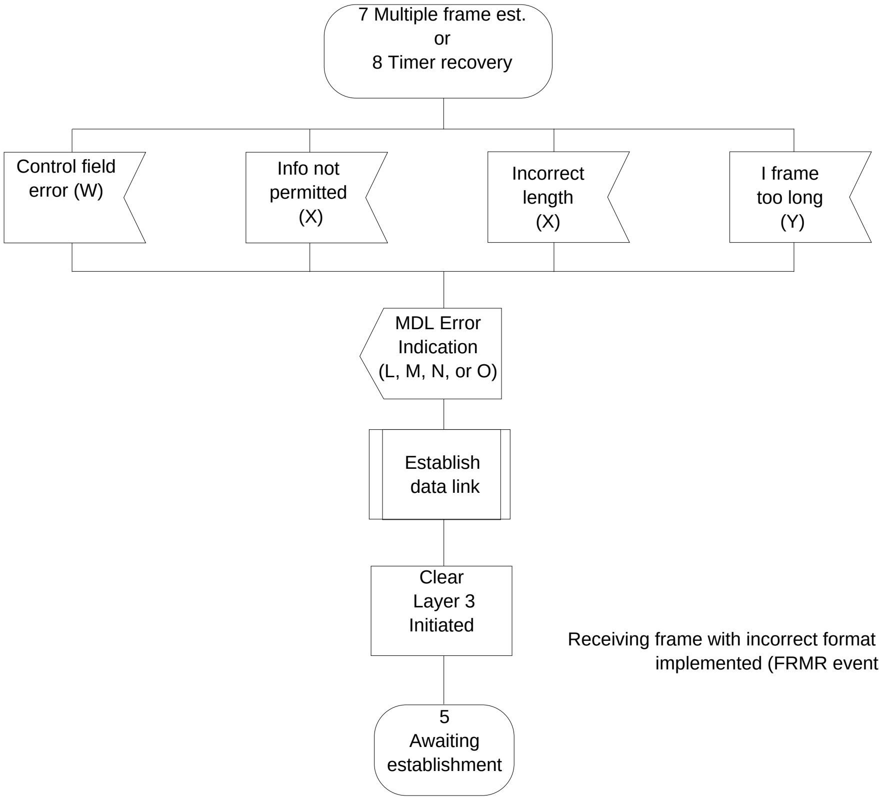
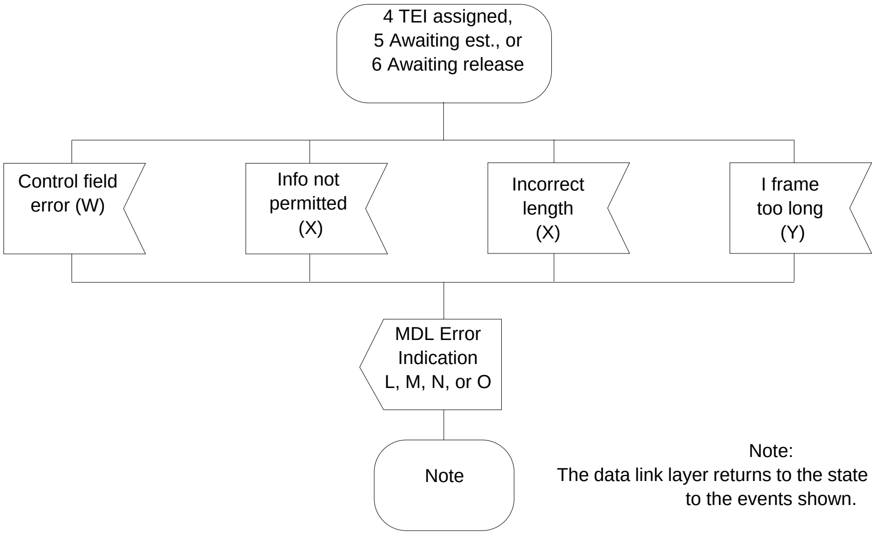


Figure 3-36
Layer 2 SDL diagrams (21 of 22)

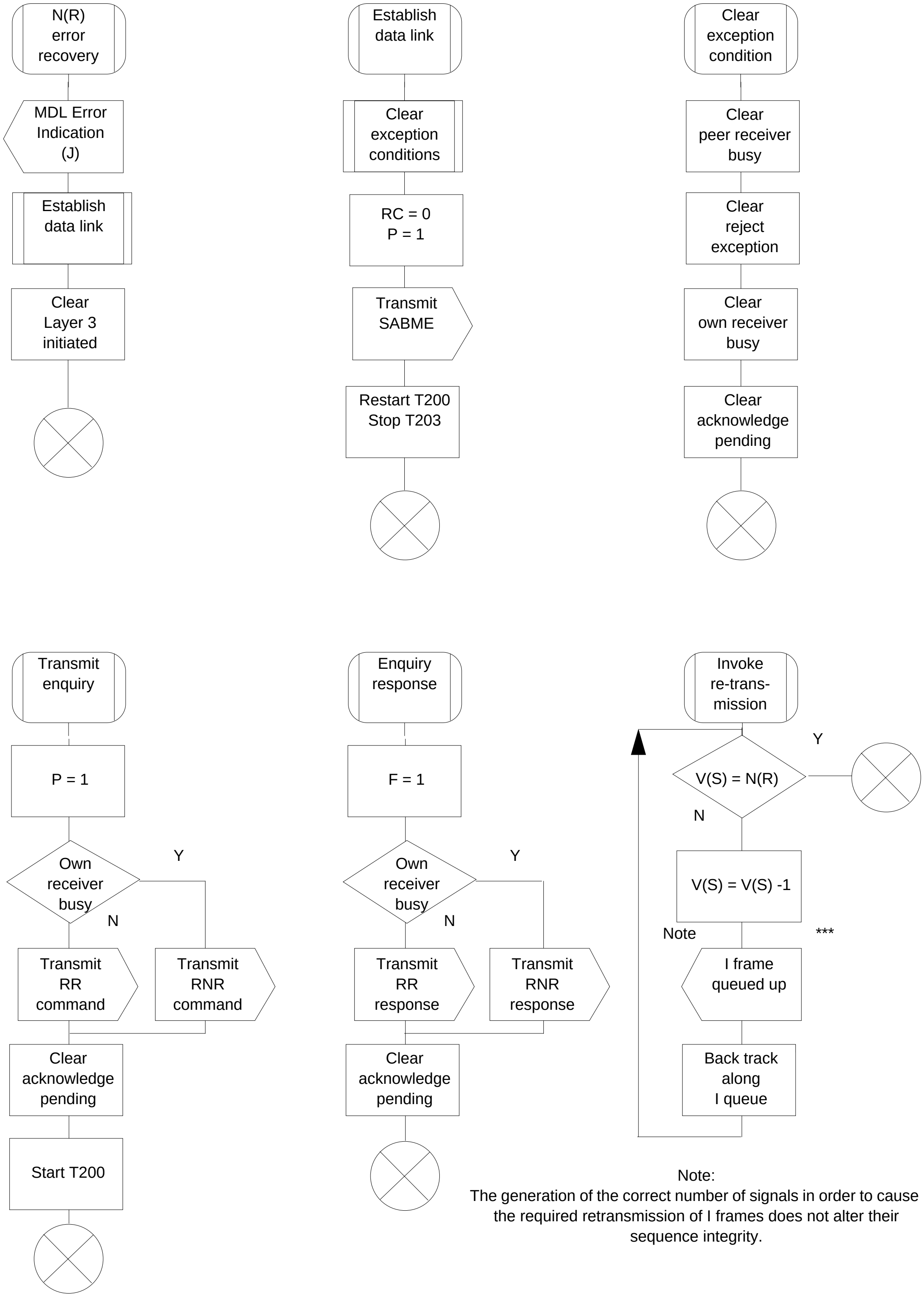


Receiving frame with incorrect format or frame not implemented (FRMR events)



Note:
The data link layer returns to the state it was in prior to the events shown.

Figure 3-37
Layer 2 SDL diagrams (22 of 22)



Note:
The generation of the correct number of signals in order to cause the required retransmission of I frames does not alter their sequence integrity.

Section 4:
Layer 3 call control signaling

Chapter 4-1:
Introduction 4-5

Chapter 4-2:
Layer 3 overview of call control 4-7

Chapter 4-3:
Layer 3 message functional definitions 4-11

Chapter 4-4:
Layer 3 message formats 4-37

Chapter 4-5:
Layer 3 call control procedures 4-113

Chapter 4-8:
B-channel maintenance 4-153

Chapter 4-9:
Connectionless signaling procedures 4-159

Chapter 4-10:
Layer 3 list of system parameters 4-161

Chapter 4-11:
Annexes 4-167

Chapter 4-1: Introduction

1.1 Scope

Section 4 defines the call signaling protocol for DMS-100 to CPE applications using an Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI). This call control signaling specification is based on the general format and procedures found in CCITT Recommendation Q.931 (I.451), ISDN user-network interface Layer 3-specification and ANSI T1.607, Layer 3 signaling specification for circuit switched bearer services.

The format of this section is similar to the standards to assist with reader comprehension. Additional messages, procedures, and parameter encodings have been provided in order to satisfy the signaling requirements of the interface.

Section 4 specifies the procedures for establishing, maintaining, and clearing network connections at the ISDN user-network interface for support of circuit-switched calls. These procedures are defined in terms of messages exchanged over the D-channel of a PRI. This part also describes the protocol structure on which supplementary services are based. Procedures for the operation of supplementary services are defined in Section 5.

References in the text to “network side” equipment are to be understood as relating to a DMS-100 Central Office (CO).

1.2 Conformance

Products conforming to this specification support all mandatory procedures and information elements outlined in Chapters 2 through 8 inclusive of this section of the specification.

It is intended that the call signaling protocol be fully symmetric to enable direct user-to-user communication. In order to achieve this objective, several options are incorporated in the specification as described in Annex D.

Chapter 4-2: Layer 3 overview of call control

In this chapter, call states are defined for circuit switched calls in section 2.1 on page 4-7 and for the interface in section 2.2 on page 4-10.

Section 2.1 defines the basic call control states that individual calls may have. These definitions do not apply to the state of the interface itself, any attached equipment, the D-channel, or the logical links used for signaling on the D-channel. Because several calls may exist simultaneously at a user-network interface, and each call may be in a different state, the state of the interface itself cannot be unambiguously defined.

Detailed descriptions of the procedures for call control are given in Chapter 4-5: "Layer 3 overview of call control" in terms of:

- The messages which are transferred across the user-network interface (defined in Chapter 4-3: "Layer 3 message functional definitions").
- The information processing and actions that take place at the user side and the network side.

Overview and detailed specification and description language (SDL) diagrams for call control of circuit-switched calls are contained in Annex A "Annex A: Layer 3 SDL diagrams".

In this specification, the terms “incoming” and “outgoing” are used to describe the call as viewed by the user side of the interface.

2.1 Circuit switched calls

This section defines the basic call control states for circuit switched calls.

2.1.1 Call states on the network or user side of the interface

The states which may exist on the user side or on the network side of the user-network interface are defined in Table 3-1.

Table 3-1
Call states

State no.	State name	User side	Network side	Definition
0	Null	U0	N0	No call exists.
1	Call initiated	U1	N1	This state exists for an outgoing call, when the user requests call establishment from the network, but the network has not responded. On the network side, this state exists when the network has received a call establishment request, but has not yet responded.
3	Outgoing call proceeding	U3	N3	This state exists for an outgoing call when the user has received acknowledgement that the network has received all call information necessary to effect call establishment. On the network side, this state exists when the network has sent acknowledgement that it has received all call information necessary to effect call establishment.
4	Call delivered	U4	N4	This state exists for an outgoing call when the calling user has received an indication that the remote user has been alerted. On the network side, this state exists for an outgoing call when the network has indicated that the remote user has been alerted.
6	Call present	U6	N6	This state exists for an incoming call when the user has received a call establishment request but has not yet responded. On the network side, this state exists when the network has sent a call establishment request, but has not yet received a satisfactory response.
7	Call received	U7	N7	This state exists for an incoming call when the user has initiated alerting but has not yet answered. On the network side, this state is entered when the network receives an indication that the user has initiated alerting, but has not yet answered.
8	Connect request	U8	N8	This state exists for an incoming call when the user has answered the call and is waiting to be awarded the call. On the network side, this state exists when the network has received an answer but the network has not awarded the call.

Table 3-1
Call states (Continued)

State no.	State name	User side	Network side	Definition
9	Incoming call proceeding	U9	N9	This state exists for an incoming call when the user has sent acknowledgement that the user has received all call information necessary to effect call establishment. On the network side, this state exists when the network has received acknowledgement that the user has received all call information necessary to effect call establishment.
10	Active	U10	N10	This state exists for an incoming call when the user has received an acknowledgement from the network that the user has been awarded the call. This state exists for an outgoing call when the user has received an indication that the remote user has answered the call. That is, the call is in an end-to-end communication mode.
11	Disconnect request	U11	N11	This state exists when the user has requested the network to clear the end-to-end connection (if any) and is waiting for a response. This state exists on the network from the time that the network has received the call clearing request from the user.
12	Disconnect indication	U12	N12	This state exists when the user has received an invitation to disconnect because the network has disconnected the end-to-end connection (if any). On the network side, this state is entered when the network has disconnected the call, and sent an invitation to disconnect to the user-network connection.
19	Release request	U19	N19	This state exists when the user has requested the network to release the call and is waiting for a response. On the network side, this state exists when the network has requested the user to release and is waiting for a response

2.2 States associated with the global call reference

This section defines the states that the protocol may adopt using the global call reference. The procedures for use of the global call reference for restart procedures are contained in section 5.7 on page 4-132.

There is only one global call reference per interface.

The states which may exist on the user side and the network side of the user-network interface are defined in Table 3-2.

Table 3-2
Call states associated with global call reference

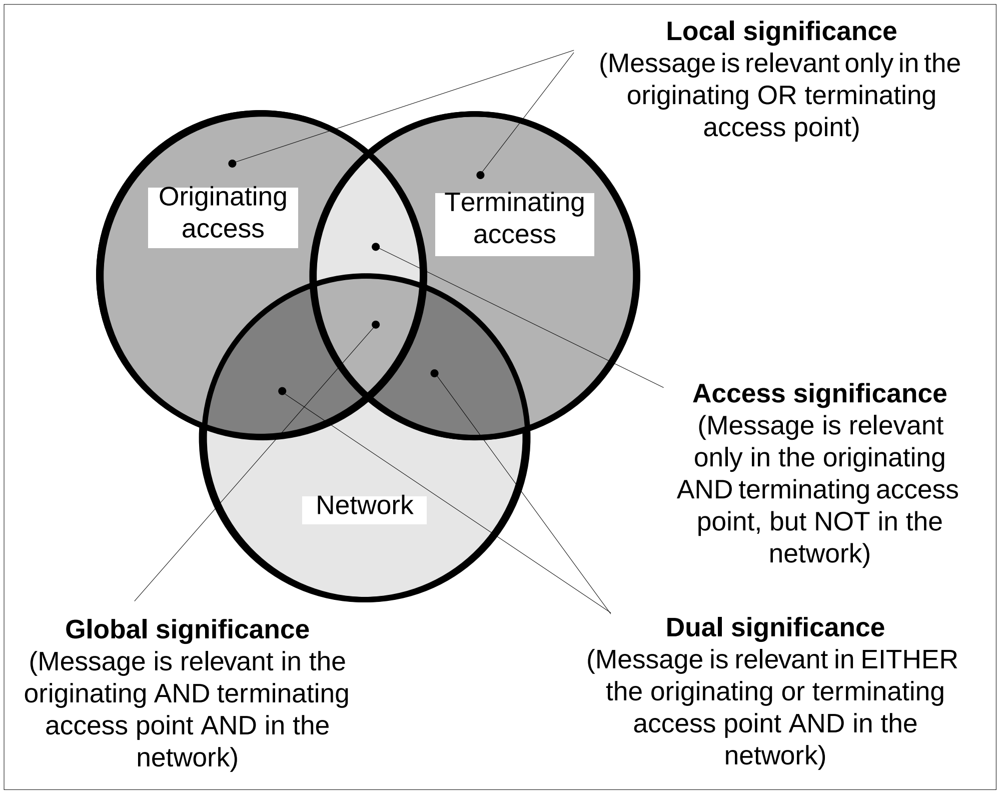
State no.	State name	User side	Network side	Definition
0	Null	Rest 0	Rest 0	No transaction exists.
1	Restart request	Rest 1	Rest 1	On the user side, this state exists for a restart transaction when the user has sent a restart request but has not yet received an acknowledgement response from the network. On the network side, this state exists when the network has sent a restart request, but has not yet received an acknowledgement response from the user.
2	Restart	Rest 2	Rest 2	On the user side, this state exists when a request for a restart has been received from the network and responses have not yet been received from all locally active call references. Similarly, on the network side, this state exists when a request for a restart has been received from the user, but a response has not yet been received from all locally active call references.

Chapter 4-3:
Layer 3 message functional definitions

This chapter provides an overview of the Layer 3 message structure, providing the functional definition and information content (that is, the semantics) of each message. Each definition includes:

- A brief description of the message direction and use, including the significance of the message with respect to the originating access point, the terminating access point and the network, as shown in Figure 4-1.

Figure 4-1
Message significance within the network



- A table listing the codeset 0 and codeset 6 information elements in the order of their appearance in the message. The relative order of information elements is the same for all message types. For each information element the table indicates
  - the reference to the section where the information element is described
  - the direction in which the information element may be sent, that is, user to network (“u->n”), network to user (“n->u”), or “both” directions
  - whether inclusion is mandatory (“M”) or optional (“O”), with a reference to notes explaining the circumstances under which the information element is included
  - the length of the information element (or permissible range of lengths), in octets

  Note: Certain messages contain information elements from codeset 6 and the corresponding locking *Shift* information element which complies with the coding rules specified in section 4.5.2 on page 4-45 to section 4.5.4 on page 4-46. These information elements are listed in the appropriate tables in this chapter.

- Further explanatory notes, as necessary.

3.1 Messages for circuit mode connection control

Table 3-3 summarizes the messages for circuit-mode connection control.

Table 3-3
Messages for circuit-mode connection control

Call establishment messages	**Reference**
ALERTING	section 3.1.1 on page 4-14
CALL PROCEEDING	section 3.1.2 on page 4-15
CONNECT	section 3.1.3 on page 4-16
CONNECT ACKNOWLEDGE	section 3.1.4 on page 4-17
PROGRESS	section 3.1.7 on page 4-21
SETUP	section 3.1.10 on page 4-24
Call clearing messages	
DISCONNECT	section 3.1.5 on page 4-18
RELEASE	section 3.1.8 on page 4-22
RELEASE COMPLETE	section 3.1.9 on page 4-23
Miscellaneous messages	
NOTIFY	section 3.1.6 on page 4-19
STATUS	section 3.1.11 on page 4-26
STATUS ENQUIRY	section 3.1.12 on page 4-27

3.1.1 ALERTING

This message is sent by the called user to the network and by the network to the calling user to indicate that called user alerting has been initiated.

Table 3-4
ALERTING **message content**

Message type: *ALERTING* **Significance:** Global **Direction:** Both				
Information element	**Reference**	**Direction**	**Type**	**Length**
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Channel identification	section 4.5.11 on page 4-66	both (see Note 1)	O (see Note 2)	2 - 6
Facility	section 4.5.15 on page 4-76	both	O (see Note 3)	see Note 4
Progress indicator	section 4.5.22 on page 4-107	n->u	O (see Note 5)	2 - 4

Note 1: Included in the network-to-user direction for support of the procedures in Annex D.

Note 2: Mandatory if this message is the first message in response to *SETUP*.

Note 3: Used for supplementary services described in Section 5.

Note 4: The length depends on the supplementary service provided.

Note 5: Included in connection with the provision of in-band information and patterns.

3.1.2 CALL PROCEEDING

This message is sent by the called user to the network or by the network to the calling user to indicate that the requested call establishment has been initiated and no more call establishment information can be accepted.

Table 3-5
CALL PROCEEDING **message content**

Message type: *CALL PROCEEDING* **Significance:** Local **Direction:** Both				
Information element	**Reference**	**Direction**	**Type**	**Length**
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Channel identification	section 4.5.11 on page 4-66	both	M	5- 6

3.1.3 CONNECT

This message is sent by the called user to the network and by the network to the calling user to indicate call acceptance by the called user.

Table 3-6
CONNECT **message content**

Message type: *CONNECT*

Significance: Global

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Channel identification	section 4.5.11 on page 4-66	both (see Note 1)	O (see Note 2)	2 - 6

Note 1: Included in the network-to-user direction for support of the procedures in Annex D.

Note 2: Mandatory if this message is the first message in response to *SETUP.*

3.1.4 CONNECT ACKNOWLEDGE

This message is sent by the network to the called user to indicate the user has been awarded the call. It may also be sent by the calling user to the network to allow symmetrical call control procedures.

Table 3-7
CONNECT ACKNOWLEDGE **message content**

Message type: *CONNECT ACKNOWLEDGE*

Significance: Local

Direction: Both

Information element	**Reference**	**Direction**	**Type**	**Length**
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1

3.1.5 DISCONNECT

This message is sent by the user to request the network to clear an end-to-end connection or is sent by the network to indicate that the end-to-end connection is cleared.

Table 3-8
DISCONNECT **message content**

Message type: *DISCONNECT* **Significance**: Global **Direction:** Both				
Information element	**Reference**	**Direction**	**Type**	**Length**
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Cause	section 4.5.9 on page 4-61	both	M	4 - 10 (see Note 1)

Note 1: The network does not generate more than two octets of diagnostics.

3.1.6 NOTIFY

This message is sent by the user or the network to indicate information pertaining to a call.

Table 3-9
NOTIFY **message content**

Message type: *NOTIFY*

Significance: Global

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Cause	section 4.5.9 on page 4-61	both	O (see Note 1)	2 - 10 (see Note 2)
Connected number	section 4.5.12 on page 4-70	both	O (see Note 3)	2 - 16
Progress indicator	section 4.5.22 on page 4-107	both	O (see Note 4)	2 - 4
Notification indicator	section 4.5.18 on page 4-100	both	M	3
Display	section 4.5.14 on page 4-74	both	O (see Note 3)	2 - 18
Information request	section 4.5.16 on page 4-96	both	O (see Note 3)	2 - 4
Calling party number	section 4.5.8 on page 4-59	both	O (see Note 3)	2 - 16
Redirection number	section 4.5.24 on page 4-110	both	O (see Note 3)	2 - 17

Note 1: Included by the user or the network to provide additional information concerning the provision of in-band information or patterns.

Note 2: The network does not generate more than two octets of diagnostics.

Note 3: Used for supplementary services described in Section 5.

Note 4: Progress indicator is sent if in-band tones are required to be provided, or interworking is encountered. Otherwise it is not included.

3.1.7 PROGRESS

This message is sent by the user or the network to indicate the progress of a call in the event of interworking or in relation with the provision of in-band information or patterns.

Table 3-10
PROGRESS **message content**

Message type: *PROGRESS*

Significance: Global

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Cause	section 4.5.9 on page 4-61	both	O (see Note 1)	2 - 10 (see Note 2)
Progress indicator	section 4.5.22 on page 4-107	both	M	4
Facility	section 4.5.22 on page 4-76	both	O(see Note 3)	(see Note 3)

Note 1: Included by the user or the network to provide additional information concerning the provision of in-band information or patterns.

Note 2: The network does not generate more than two octets of diagnostics.

Note 3: Used for RLT (Release Link Trunk). The length depends on the supplementary service provided.

3.1.8 RELEASE

This message is sent by the user or the network to indicate that the equipment sending the message has disconnected the channel (if any) and intends to release the channel and the call reference, and that the receiving equipment should release the channel and prepare to release the call reference after sending a *RELEASE COMPLETE* message.

Table 3-11
RELEASE **message content**

Message type: *RELEASE* **Significance:** Local (see Note 1) **Direction:** Both				
Information element	**Reference**	**Direction**	**Type**	**Length**
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Cause	section 4.5.9 on page 4-61	both	O (see Note 2)	2 - 10 (see Note 3)

Note 1: This message has local significance. However, it may carry information of global significance when used as the first call clearing message.

Note 2: Mandatory in the first call clearing message, including when the *RELEASE* message is sent as a result of an error handling condition.

Note 3: The network does not generate more than two octets of diagnostics.

3.1.9 RELEASE COMPLETE

This message is sent by the user or the network to indicate that the equipment sending the message has released the channel (if any) and call reference. The channel is available for reuse, and the receiving equipment releases the call reference.

Table 3-12
RELEASE COMPLETE **message content**

Message type: *RELEASE COMPLETE*

Significance: Local (see Note 1)

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Cause	section 4.5.9 on page 4-61	both	O (see Note 2)	2 - 10 (see Note 3)

Note 1: This message has local significance. However, it may carry information of global significance when used as the first call clearing message.

Note 2: Mandatory in the first call clearing message, including when the *RELEASE COMPLETE* message is sent as a result of an error handling condition.

Note 3: The network does not generate more than two octets of diagnostics.

3.1.10 SETUP

This message is sent by the calling user to the network and by the network to the called user to initiate call establishment.

Table 3-13
SETUP **message content**

Message type: *SETUP*

Significance: Global

Direction: Both

Information element	**Reference**	**Direction**	**Type**	**Length**
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Bearer capability	section 4.5.5 on page 4-48	both	M	4 - 8
Channel identification	section 4.5.11 on page 4-66	both	M	5 - 6
Facility	section 4.5.15 on page 4-76	both	O (see Note 1)	(see Note 2)
Progress indicator	section 4.5.22 on page 4-107	both	O (see Note 3)	2 - 4
Network-specific facilities	section 4.5.17 on page 4-98	both	O (see Note 4)	2 - 7
Display	section 4.5.14 on page 4-74	both	O (see Note 1)	2 - 18
Calling party number	section 4.5.8 on page 4-59	both	O (see Note 5)	2 - 16
Called party number	section 4.5.7 on page 4-56	both	O (see Note 6)	2 - 27
Original called number	section 4.5.21 on page 4-103	both	O (see Note 1)	2 - 18
Transit network selection	section 4.5.26 on page 4-112	u->n	O (see Note 7)	2 - 7

Note 1: Used for supplementary services described in Section 5.

Note 2: The length depends on the supplementary service provided.

Note 3: Included in the event of interworking or in connection with the provision of in-band information or patterns.

Note 4: Included by the calling user or the network to indicate network-specific facilities information (see Annex E).

Note 5: May be included by the calling user or the network to identify the calling user.

Note 6: Mandatory in u->n direction. Only included in the n->u direction as described in Section 5.

Note 7: Included by the calling user to select a particular transit network (see Annex C).

3.1.11 STATUS

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 error conditions as described in section 5.9 on page 4-134.

Table 3-14
STATUS **message content**

Message type: *STATUS*

Significance: Local

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Cause	section 4.5.9 on page 4-61	both	M	4 - 10 (see Note 1)
Call state	section 4.5.6 on page 4-54	both	M	3

Note 1: The network does not generate more than two octets of diagnostics.

3.1.12 STATUS ENQUIRY

This message is sent by the user or the network at any time during a call to solicit a *STATUS* message from the peer Layer 3 entity. Sending a *STATUS* message in response to a *STATUS ENQUIRY* message is mandatory.

Table 3-15
STATUS ENQUIRY **message content**

Message type: *STATUS ENQUIRY*

Significance: Local

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M	2 - 3
Message type	section 4.4 on page 4-41	both	M	1

3.2 Messages used with the global call reference

Table 3-16 summarizes the messages which may use the global call reference as defined in paragraph 4.3 on page 4-38 in Chapter 4-4:

Table 3-16
Messages used with the global call reference

Message	Reference
RESTART	section 3.2.1 on page 4-29
RESTART ACKNOWLEDGE	section 3.2.2 on page 4-30
SERVICE	section 3.2.3 on page 4-31
SERVICE ACKNOWLEDGE	section 3.2.4 on page 4-32
STATUS	section 3.2.5 on page 4-33

3.2.1 RESTART

This message is sent by the user or the network to request the recipient to restart (that is, return to an idle condition) the indicated channel or interfaces.

Table 3-17
RESTART **message content**

Message type: *RESTART* **Significance:** Local **Direction:** Both				
Information element	**Reference**	**Direction**	**Type**	**Length**
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M (see Note 1)	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Channel identification	section 4.5.11 on page 4-66	both	O (see Note 2)	2 - 6
Restart indicator	section 4.5.25 on page 4-111	both	M	3

Note 1: This message is sent with the global call reference as defined in section 4.3 on page 4-38.

Note 2: Included when necessary to indicate the particular channel to be restarted.

3.2.2 RESTART ACKNOWLEDGE

This message is sent to acknowledge the receipt of the *RESTART* message and to indicate that the requested restart is complete.

Table 3-18
RESTART ACKNOWLEDGE **message content**

Message type: *RESTART ACKNOWLEDGE* **Significance:** Local **Direction:** Both				
Information element	**Reference**	**Direction**	**Type**	**Length**
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M (see Note 1)	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Channel identification	section 4.5.11 on page 4-66	both	O (see Note 2)	2 - 6
Restart indicator	section 4.5.25 on page 4-111	both	M	3

Note 1: This message is sent with the global call reference as defined in section 4.3 on page 4-38.

Note 2: Included when necessary to indicate the particular channel which has been restarted.

3.2.3 SERVICE

This message is sent by either the user or the network and is used to change the current status of a channel to one of the following states: In Service, Maintenance, or Out of Service.

Table 3-19
SERVICE **message content**

Message type: *SERVICE*

Significance: Local

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	section 4.2 on page 4-38	both	M (see Note 1)	1
Call reference	section 4.3 on page 4-38	both	M (see Note 2)	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Change status	section 4.5.10 on page 4-65	both	M	3
Channel identification	section 4.5.11 on page 4-66	both	M	3 - 6

Note 1: This message is sent with the protocol discriminator for maintenance messages as defined in section 4.2 on page 4-38.

Note 2: This message is sent with the global call reference as defined in section 4.3 on page 4-38.

3.2.4 SERVICE ACKNOWLEDGE

This message is sent by either the user or the network and is used as the acknowledgement for the change of state indicated in the *SERVICE* message.

Table 3-20
SERVICE ACKNOWLEDGE **message content**

Message type: *SERVICE ACKNOWLEDGE*

Significance: Local

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	section 4.2 on page 4-38	both	M (see Note 1)	1
Call reference	section 4.3 on page 4-38	both	M (see Note 2)	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Change status	section 4.5.10 on page 4-65	both	M	3
Channel identification	section 4.5.11 on page 4-66	both	M	3 - 6

Note 1: This message is sent with the protocol discriminator for maintenance messages as defined in section 4.2 on page 4-38.

Note 2: This message is sent with the global call reference as defined in section 4.3 on page 4-38.

3.2.5 STATUS

This message may be sent by either the user or the network at any time when an unexpected or unrecognized message with a global call reference is received.

Table 3-21
STATUS **message content**

Message type: *STATUS* **Significance:** Local **Direction:** Both				
Information element	**Reference**	**Direction**	**Type**	**Length**
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M (see Note 1)	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Cause	section 4.5.9 on page 4-61	both	M	4 - 10 (see Note 2)
Call state	section 4.5.6 on page 4-54	both	M	3

Note 1: This message is sent with the global call reference as defined in section 4.3 on page 4-38.

Note 2: The network does not generate more than one octet of diagnostics.

3.3 Messages for connectionless signaling

Table 3-22 summarizes the messages used for connectionless signaling.

Table 3-22
Messages for connectionless signaling

Message	Reference
FACILITY	section 3.3.1 on page 4-35
FACILITY REJECT	section 3.3.2 on page 4-36

3.3.1 FACILITY

The *FACILITY* message is used to transfer higher layer protocols (for example, TCAP) using connectionless signaling.

Table 3-23
FACILITY **message content**

Message type: *FACILITY*

Significance: Global

Direction: Both

Information element	**Reference**	**Direction**	**Type**	**Length**
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M (see Note 1,4)	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Locking Shift to codeset 6	section 4.5.3 on page 4-46	both	M	1
Origination	section 4.5.20 on page 4-102	both	M	8 - 17
Destination	section 4.5.13 on page 4-71	both	M	8 - 17
Options	section 4.5.19 on page 4-101	both	O (see Note 2)	2 - 3
Facility	section 4.5.15 on page 4-76	both	M	(see Note 3)

Note 1: The null call reference is used for the *FACILITY* message (see section 4.3 on page 4-38). The call reference does not have end to end significance.

Note 2: Used for supplementary services described in Section 5.

Note 3: The length depends on the supplementary service provided.

Note 4: For RLT (Release Link Trunk), the FACILITY message includes actual call reference.

3.3.2 FACILITY REJECT

The *FACILITY REJECT* message is sent to the originator of the *FACILITY* message whenever it is not possible to route the *FACILITY* message.

Table 3-24
FACILITY REJECT **message content**

Message type: *FACILITY REJECT*

Significance: Global

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol discriminator	section 4.2 on page 4-38	both	M	1
Call reference	section 4.3 on page 4-38	both	M (see Note 1)	2 - 3
Message type	section 4.4 on page 4-41	both	M	1
Locking Shift to codeset 6	section 4.5.3 on page 4-46	both	M	1
Origination	section 4.5.20 on page 4-102	both	M	8 - 17
Destination	section 4.5.13 on page 4-71	both	M	8 - 17
Reason for return	section 4.5.23 on page 4-109	both	M	3
Facility	section 4.5.15 on page 4-76	both	M	(see Note 2)

Note 1: The null call reference is used for the *FACILITY REJECT* message (see section 4.3 on page 4-38). The call reference does not have end to end significance.

Note 2: The length depends on the supplementary service provided.

Chapter 4-4: Layer 3 message formats

4.1 Overview

Within this protocol, every message consists of the following parts:

- protocol discriminator
- call reference
- message type
- other information elements, as required

The first three parts are common to all messages and are always present, while the last part is specific to each message type. This organization is illustrated in Figure 4-2.

Figure 4-2
General message organization

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
Protocol discriminator								1
0	0	0	0	Length of call reference value				2
Call reference value								3
0	Message type							etc.
Other information elements as required								

A particular message may contain more information than particular (user or network) equipment needs or can understand. All equipment should be able to ignore any extra information present in a message which is not required for the proper operation of that equipment. For example, a user may ignore the calling party number if that number is of no interest to the user when a *SETUP* message is received.

Unless specified otherwise, a particular information element is present only once in a given message.

The term “default” implies that the value defined should be used in the absence of any assignment, or the negotiation of alternative values.

The messages are sent as an ordered set of octets. In the following figures, the message contents are shown with a consistent bit and octet numbering pattern. Within each octet, bit “1” is transmitted first, followed by bits “2” through “8”. Similarly, the octet shown at the top of each figure is sent first.

When a field extends over more than one octet, the order of bit values progressively decreases as the octet number increases. The least significant bit of the field is represented by the lowest numbered bit of the highest numbered octet of that field.

4.2 Protocol discriminator

The *Protocol discriminator* information element is used to distinguish the user-to-network call control messages from other messages. In this specification, only two values are allowed; one for maintenance messages and one for call control messages, as shown in Figure 4-3.

The *Protocol discriminator* information element is the first part of every message.

Figure 4-3
Q.931 protocol discriminator coding

8 7 6 5	**4 3 2 1**	
0 0 0 0	0 0 1 1	Maintenance messages
0 0 0 0	1 0 0 0	Q.931 (I.451) user-to-network call control message

All other values are reserved.

4.3 Call reference

The *Call reference* information element is used to identify the call request at the local user-network interface to which the particular message applies. The *Call reference* information element does not have end-to-end significance.

The *Call reference* information element is the second part of every message, and is shown in Figure 4-4. The length of the *Call reference* information element is indicated in octet 1, bits 1 through 4. The default maximum length of the *Call reference* information element value field is two octets. The *Call* *reference* information element includes the length of the call reference value, the call reference value and the call reference flag.

Figure 4-4
Call reference information element

Bit 8	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Octet**
0	0	0	0	Length of call reference value				1
Flag	Call reference value							2 ... 3

The actions taken by the receiver are based on the Call reference value and are independent of the length of the *Call reference* information element.

The Call reference value may be one or two octets long. A call reference with a numerical value up to 127 may be encoded using one or two octets. The network always uses two octets for the Call reference value.

Call reference values are assigned by the originating side of the interface for a call. These values are unique to the originating side only within a particular D-channel Layer 2 logical link connection. The call reference value is assigned at the beginning of a call and remains fixed for the duration of the call.

When a call ends, the associated call reference value may be reassigned to a later call. Two identical call reference values on the same D-channel Layer 2 logical link connection may be used when each value is associated with a call originated at opposite ends of the link.

The call reference flag is used to identify which end of the Layer 2 logical link originated a call reference. The call reference flag (bit 8 of octet 2) is set to one of the following:

- “0”, indicating that the message is sent from the side that originated the call reference.
- “1”, indicating that the message is sent to the side that originated the call reference.

The call reference flag is used to resolve simultaneous attempts to allocate the same call reference value. The call reference flag also applies to functions which use the global call reference (for example, restart procedures).

A *Call reference* information element containing a dummy (null) call reference is one octet long and is coded “0000 0000”, as shown in Figure 4-5.

The null call reference is used for the *FACILITY* and *FACILITY REJECT* messages which are used in connectionless signaling.

Figure 4-5
Dummy (null) call reference

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
				Length of call reference value				1
0	0	0	0	0	0	0	0	

The numerical value of the global call reference is zero (see Figure 4-6 and Figure 4-7). The equipment receiving a message containing the global call reference should interpret the message as pertaining to all call references on the associated Layer 2 data link connection identifier. The messages which can use the global call reference value are defined in section 3.2 on page 4-28.

Figure 4-6
Global call reference (1 octet value)

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
				Length of call reference value				1
0	0	0	0	0	0	0	1	
Flag (0/1)	0	0	0	0	0	0	0	2

Figure 4-7
Global call reference (2 octet value)

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
				Length of call reference value				1
0	0	0	0	0	0	1	0	
Flag (0/1)	0	0	0	0	0	0	0	2
0	0	0	0	0	0	0	0	3

4.4 Message type

The purpose of the *Message type* information element is to identify the function of the message being sent.

The *Message type* information element is the third part of every message. The coding of the information element is shown in Figure 4-8.

Figure 4-8
Message type information element

Bit 8	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Octet**
0	Message type							1

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	-	-	-	-	-	**Call establishment messages**
			0	0	0	0	1	Alerting
			0	0	0	1	0	Call Proceeding
			0	0	1	1	1	Connect
			0	1	1	1	1	Connect Acknowledge
			0	0	0	1	1	Progress
			0	0	1	0	1	Setup
0	1	0	-	-	-	-	-	**Call clearing messages**
			0	0	1	0	1	Disconnect
			0	1	1	0	1	Release
			1	1	0	1	0	Release Complete
			0	0	1	1	0	Restart
			0	1	1	1	0	Restart Acknowledge
0	1	1	-	-	-	-	-	**Miscellaneous messages**
			0	0	0	1	0	Facility (connectionless)
			1	0	0	1	0	Facility reject (connectionless)
			0	1	1	1	0	Notify
			1	1	1	0	1	Status
			1	0	1	0	1	Status Enquiry

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	-	-	-	-	-	**Maintenance messages (see Note 1)**
			0	1	1	1	1	Service
			0	0	1	1	1	Service acknowledge

Note 1: The maintenance messages protocol discriminator is “0000 0011”.

4.5 Other information elements

4.5.1 Coding rules

The coding of other information elements follows the coding rules described below. These rules are formulated to allow each piece of equipment which processes a message to find information elements important to it, and to ignore information elements not important to that equipment.

Two categories of information elements are defined:

- single octet information elements (see Figure 4-9)
- variable length information elements (see Figure 4-10)

Figure 4-9
Single octet nformation element format

Bit 8	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Octet**
1	Information element identifier			Contents of information element				1

Figure 4-10
Variable length information element format

Bit 8	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Octet**
0	Information element identifier							1
Length of contents of information element, octets 3 through n								2
Contents of information element								3 ... n

The descriptions of the following information elements are organized in alphabetical order. However, there is a particular order of appearance for each information element in a message within each codeset (see section 4.5.2 on page 4-45).

The code values of the information element identifier for the variable length formats are assigned in ascending numerical order, according to the actual order of appearance of each information element in a message. This allows the receiving equipment to detect the presence or absence of a particular information element without scanning through an entire message. Single octet information elements may appear at any point in the message.

Where the description of information elements in this specification contains spare bits, these bits are indicated as being set to “0”. In order to allow compatibility with future implementations, messages are not rejected because a spare bit is set to “1”.

The second octet of a variable length information element indicates the total length of the contents of that information element regardless of the coding of the first octet (that is, the length starting with octet 3). The second octet is a binary coding of the number of octets of the contents, with bit 1 as the least significant bit.

A variable length information element may be present, but empty. For example, a *SETUP* message may contain a *Called party number* information element, which has a content of zero length. This should be interpreted by the receiver as equivalent to that information element being absent. Similarly, an absent information element should be interpreted by the receiver as equivalent to that information element being empty.

The following rules apply for the coding of variable length information elements from octet 3 and above:

- The first digit in the octet number identifies one octet or a group of octets.
- Each octet group is a self-contained entity. The internal structure of an octet group may be defined in alternative ways.
- An octet group is formed by using an extension mechanism. The preferred extension mechanism is to extend an octet (N) through the next octet(s) (Na, Nb, ...) by using bit 8 in each octet as an extension bit. The bit value “0” indicates that the octet group continues through the next octet. The bit value “1” indicates that this octet is the last octet. If an octet (Nb) is present, then the preceding octets (N and Na) must be present.

  In the format descriptions (appearing in the later sections of this chapter), bit 8 is marked “0/1 Ext” if another octet may follow. Bit 8 is marked “1 Ext” if this is the last octet in the extension domain.
- In addition to the extension mechanism defined above, an octet (N) may be extended through the next octet(s) (N.1, N.2 ...) by indications in bits 7 through 1 (of octet N).
- The two extension mechanisms described above may be combined.

- Optional octets are marked with asterisks (*).

Figure 4-11
Codeset 0 information element identifiers

8	7	6	5	4	3	2	1		
1	:	:	:	:	:	:	:	**Single octet information element**	
	0	0	1	-	-	-	-	Shift	(Note 1)
0	:	:	:	:	:	:	:	**Variable length information element**	
	0	0	0	0	0	0	1	Change status	(Note 2)
	0	0	0	0	1	0	0	Bearer capability	
	0	0	0	1	0	0	0	Cause	(Note 3)
	0	0	0	1	1	0	0	Connected number	
	0	0	1	0	1	0	0	Call state	
	0	0	1	1	0	0	0	Channel identification	
	0	0	1	1	1	0	0	Facility	
	0	0	1	1	1	1	0	Progress indicator	
	0	1	0	0	0	0	0	Network-specific facilities	
	0	1	0	0	1	1	1	Notification indicator	
	0	1	0	1	0	0	0	Display	(Note 4)
	0	1	1	0	0	1	0	Information request	
	1	1	0	1	1	0	0	Calling party number	
	1	1	1	0	0	0	0	Called party number	
	1	1	1	0	0	1	1	Original called number	
	1	1	1	0	1	1	0	Redirection number	
	1	1	1	1	0	0	0	Transit network selection	
	1	1	1	1	0	0	1	Restart indicator	

All other values are reserved. (Note 5)

Note 1: This information element may be repeated.

Note 2: This information element is used exclusively by messages with a maintenance protocol discriminator.

Note 3: This information element may be repeated once.

Note 4: This information element may be repeated twice.

Note 5: The reserved values with bits 5 to 8 coded “0000” are for future information elements for which comprehension by the receiver is required (see section 5.9.7.1 on page 4-139).

Figure 4-12
Codeset 6 information element identifiers

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	:	:	:	:	:	:	:	**Variable length information element**
	0	0	0	0	0	0	1	Origination
	0	0	0	0	0	1	0	Destination
	0	0	0	1	0	1	0	Options
	0	0	0	1	0	0	1	Reason for return
	0	0	1	1	1	0	0	Facility

4.5.2 Extension of codesets

There are a number of possible information element identifier values using the formatting rules described in the previous section. There are a possible 128 values for the variable length information element format and at least 8 values for the single octet information element format.

It is possible to expand this structure to eight codesets with at least 133 information element identifier values each. One common value in the single octet format is employed in each codeset to allow shifting from one codeset to another. The content of this *Shift* information element identifies the codeset to be used for the next information element or elements. The codeset in use at any given time is referred to as the “active codeset”. By convention, codeset 0 is the initially active codeset.

Two codeset shifting procedures are defined: locking and non-locking shift (see 4.5.3 and 4.5.4). Only the locking shift procedure is supported.

The coding rules specified in section 4.5.1 on page 4-42 apply to information elements belonging to any active codeset.

Transitions from one active codeset to another (that is, by means of the locking shift procedure) may only be made to a codeset with a higher numerical value than the codeset being left.

User or network equipment should have the capability to recognize a *Shift* information element and determine the length of the following information element. The equipment need not be able to interpret and act upon the contents of the information element. This enables the equipment to determine the start of a subsequent information element.

Codeset 6 is reserved for information elements specific to the local network (either public or private). These information elements do not have significance across the boundaries between local networks, or across a national or international boundary. Therefore, codeset 6 information elements are treated as if they were unrecognized information elements beyond the local network boundary. (See the procedures in section 5.9.7 on page 4-139.)

4.5.3 Locking shift procedure

The locking shift procedure employs a locking *Shift* information element to indicate the new active codeset. The specified codeset remains active until another locking *Shift* information element is encountered which specifies the use of another codeset.

For example, codeset 0 is active at the start of message content analysis. If a locking *Shift* information element to codeset 6 is encountered, the next information elements are interpreted according to the information element identifiers assigned in codeset 6. Codeset 6 remains active until another *Shift* information element is encountered.

The locking shift is valid only within the message which contains the locking *Shift* information element. At the start of every message content analysis, the active codeset is codeset 0. The locking *Shift* information element uses the single octet information element format, as shown in Figure 4-13.

Figure 4-13
Locking shift

8	7	6	5	4	3	2	1	
1	0	0	1	0	1	1	0	Codeset 6

4.5.4 Non-locking shift procedure

The non-locking shift procedure provides a temporary shift to the specified lower or higher codeset.

Sending of a non-locking *Shift* information element is not supported by this specification. A user or network receiving a message containing a non-locking *Shift* information element recognizes the non-locking *Shift* information element and ignores the information element following it. The non-locking *Shift* information element and the information element following it are discarded and procedures for unrecognized information element are followed for the information element following the non-locking *Shift* information element.

Figure 4-14
Non-locking shift

8	7	6	5	4	3	2	1	
1	0	0	1	1	x	x	x	x is “0” or “1”

4.5.5 Bearer capability

The purpose of the *Bearer capability* information element is to indicate a CCITT Recommendation I.231 bearer service to be provided by the network. The use of the *Bearer capability* information element in relation to compatibility checking is described in Annex B.

No default bearer capability is assumed by the absence of this information element.

The maximum length of this information element is 8 octets.

Figure 4-15
Bearer capability information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
0	Bearer capability information element identifier 0	0	0	0	1	0	0	1
Length of information element								2
Ext. 1	Coding standard		Information transfer capability					3
Ext. 0 / 1	Transfer mode		Information transfer rate					4
Ext. 0 / 1	Structure			Configuration		Establishment		4a* (see Note 1)
Ext 1	Symmetry		Information transfer rate (Destination ->Origination)					4b* (see Note 1)
Ext 1	Rate multiplier							4.1* (see Note 2)
Ext. 0 / 1	Layer 1 identifier 0	1	User information layer 1 protocol					5*
Ext. 1	Spare 0	0	User rate					5a* (see Note 3)

Note 1: These octets are ignored if present.

Note 2: This octet is required if octet 4 indicates multirate (64 kbit/s base rate). Otherwise it is not present.

Note 3: This octet is present if octet 5 indicates CCITT standardized rate adaption V.110 / X.30.

Coding standard (octet 3)

7 6	
0 0	CCITT standard as in Recommendation Q.931

All other values are reserved.

Information transfer capability (octet 3)

5 4 3 2 1	
0 0 0 0 0	Speech
0 1 0 0 0	Unrestricted digital information
0 1 0 0 1	Restricted Digital Information
1 0 0 0 0	3.1 kHz audio (see Note)

All other values are reserved.

Note: 3.1 kHz audio receives identical treatment to speech.

Transfer mode (octet 4)

7 6	
0 0	Circuit mode

All other values are reserved.

Information transfer rate (octet 4)

5 4 3 2 1	
1 0 0 0 0	64 kbit/s
1 0 0 1 1	384 kbit/s
1 0 1 0 1	1536 kbit/s
1 1 0 0 0	Multirate (64 kbit/s base rate)

All other values are reserved.

Structure (Octet 4a)

7 6 5	
0 0 1	8 kHz integrity (see Note)

All other values are reserved.

> ***Note:*** This attribute should be interpretted as “time slot sequence integrity” for multirate, 384 kbit/s and 1536 kbit/s information transfer rates.

Octet 4a is ignored if received and the value of the structure attribute is assumed to be:

Transfer Mode	Transfer Capability	Structure
circuit	Speech	8 kHz integrity
circuit	Unrestricted digital	8 kHz integrity
circuit	Restricted digital	8 kHz integrity
circuit	3.1 kHz audio	8 kHz integrity

Configuration (octet 4a)

4 3	
0 0	Point-to-point

All other values are reserved.

As octet 4a is ignored the configuration is assumed to be point-to-point.

Establishment (octet 4a)

2 1	
0 0	Demand

All other values are reserved.

As octet 4a is ignored the method of establishment is assumed to be demand.

Symmetry (octet 4b)

7	6	
0	0	bidirectional symmetric

All other values are reserved.

As octet 4b is ignored the bearer capability is assumed to be bi-directional symmetric at the information transfer rate specified in octet 4.

Rate multiplier (octet 4.1)

7	6	5	4	3	2	1	
0	0	0	0	0	1	0	128 kbit/s (n=2)
0	0	0	0	0	1	1	192 kbit/s (n=3)
			•				
			•				
0	0	1	0	1	1	1	1472 kbit/s (n=23)
0	0	1	1	0	0	0	1536 kbit/s (n=24)

All other values are reserved.

User Information Layer 1 Protocol (octet 5)

5	4	3	2	1	
0	0	0	0	1	CCITT standardized rate adaption V.110/X.30. This implies the presence of octet 5a.
0	0	0	1	0	Recommendation G.711 Mu-law Speech

All other values are reserved.

If the information transfer capability is “unrestricted digital information” or “restricted digital information” and if the user information layer 1 protocol is not to be identified to the network, then octet 5 is omitted. Otherwise, octet 5 is present.

User Rate (octet 5a)

5	4	3	2	1	Synchronous Rate
0	1	1	1	1	56 kbit/s

All other values are reserved.

4.5.5.1 Examples of bearer capability encoding

The encoding of this information element for the bearer services supported by DMS-100 are:

Attribute	Encoding	Octet
(1) Speech		
Transfer capability = speech	1 00 00000	3
Transfer mode and rate = circuit-mode, 64 kbit/s	1 00 10000	4
Layer 1 protocol identifier = Mu law	1 01 00010	5
Octet 5a is not present		
(2) 64 kbit/s unrestricted digital, rate adapted from 56 kbit/s, circuit mode		
Transfer capability = unrestricted digital	1 00 01000	3
Transfer mode and rate = circuit-mode, 64 kbit/s	1 00 10000	4
Layer 1 protocol ID = Rate adaption	0 01 00001	5
Data rate = 56 kbit/s	1 00 01111	5a
(3) 64 kbit/s clear, unrestricted digital, circuit-mode		
Transfer capability = unrestricted digital	1 00 01000	3
Transfer mode and rate = circuit-mode, 64 kbit/s	1 00 10000	4
Octets 5 and 5a are not present		
(4) 64 kbit/s restricted digital, circuit-mode		
Transfer capability = restricted digital	1 00 01001	3
Transfer mode and rate = circuit-mode, 64 kbit/s	1 00 10000	4
Octets 5 and 5a are not present		

Attribute	Encoding	Octet
(5) 3.1 kHz audio		
Transfer capability = 3.1 kHz audio	1 00 10000	3
Transfer mode and rate = circuit-mode, 64 kbit/s	1 00 10000	4
Layer 1 protocol ID = Mu-law	1 01 00010	5
Octet 5a is not present		
(6) 384 kbit/s unrestricted digital, circuit mode		
Transfer capability = unrestricted digital	1 00 01000	3
Transfer mode and rate = circuit-mode, 384 kbit/s	1 00 10011	4
Octets 5 and 5a are not present		
(7) 1536 kbit/s unrestricted digital, circuit mode		
Transfer capability = unrestricted digital	1 00 01000	3
Transfer mode and rate = circuit-mode, 1536 kbit/s	1 00 10101	4
Octets 5 and 5a are not present		
(8) Multirate (64 kbit/s base rate) unrestricted digital, circuit mode		
Transfer capability = unrestricted digital	1 00 01000	3
Transfer mode and rate = circuit-mode, multirate	1 00 11000	4
Rate multiplier = n (2 - 24)	1 00 XXXXX	4.1
Octets 5 and 5a are not present		

4.5.6 Call state

The purpose of the *Call state* information element is to describe the current status of a call (see section 2.2 on page 4-10) or a global interface state (see section 2.2 on page 4-10).

The maximum length of this information element is 3 octets.

Figure 4-16
Call state information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
	Call state information element identifier							1
0	0	0	1	0	1	0	0	
Length of information element								2
0	0	0	0	0	0	0	1	
Coding standard		Call state or global call state value (state value is coded in binary)						3

Coding standard (octet 3)

8 7	
0 0	CCITT standard as in Recommendation Q.931

All other values are reserved.

Call state value (octet 3)

6 5	4 3 2 1	State no.	User state	Network state
0 0	0 0 0 0	0	Null	Null
0 0	0 0 0 1	1	Call initiated	Call initiated
0 0	0 0 1 1	3	Outgoing call proceeding	Outgoing call proceeding
0 0	0 1 0 0	4	Call delivered	Call delivered
0 0	0 1 1 0	6	Call present	Call present
0 0	0 1 1 1	7	Call received	Call received
0 0	1 0 0 0	8	Connect request	Connect request
0 0	1 0 0 1	9	Incoming call proceeding	Incoming call proceeding
0 0	1 0 1 0	10	Active	Active
0 0	1 0 1 1	11	Disconnect request	Disconnect request

6	**5**	**4**	**3**	**2**	**1**	**State no.**	**User state**	**Network state**
0	0	1	1	0	0	12	Disconnect indication	Disconnect indication
0	1	0	0	1	1	19	Release request	Release request

Global interface state value (octet 3)

6	**5**	**4**	**3**	**2**	**1**	**State no.**	**User state**	**Network states**
0	0	0	0	0	0	0	REST 0 - Null	REST 0 - Null
1	1	1	1	0	1	1	REST 1 - Restart request	REST 1 - Restart request
1	1	1	1	1	0	2	REST 2 - Restart	REST 2 - Restart

All other values are reserved.

4.5.7 Called party number

The purpose of the *Called party number* information element is to identify the called party of a call.

The maximum length of this information element is 27 octets.

Figure 4-17
Called party number information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
0	Called party number information element identifier							1
	1	1	1	0	0	0	0	
Length of information element								2
1 Ext.	Type of number			Numbering plan identification				3
0 Spare	Number digits (IA5 characters, see Note)							4 ...n

Note: The number digits appear starting at octet 4 in the same order in which they would be entered, that is, the number digit which would be entered first is located in octet 4.

Type of number (octet 3)

7 6 5	Type of number
0 0 0	Unknown
0 0 1	International number
0 1 0	National number
1 0 0	Subscriber number

All other values are reserved.

Numbering plan identification (octet 3)

4 3 2 1	Numbering plan
0 0 0 0	Unknown
0 0 0 1	ISDN/Telephony numbering plan (E.164/E.163)
1 0 0 1	Private numbering plan

All other values are reserved.

Number digit coding (octet 4...n)

7 6 5	4 3 2 1	Address digit value
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
0 1 0	1 0 1 0	*
0 1 0	0 0 1 1	#

All other values are reserved.

4.5.7.1 Valid combinations of TON and NPI for call routing

The following combination of type of number (TON) and numbering plan identification (NPI) are supported for call routing:

- Unknown/Unknown
- International number in ISDN/Telephony numbering plan (E.164/E.163)
- National number in ISDN/Telephony numbering plan (E.164/E.163)
- Subscriber number in ISDN/Telephony numbering plan (E.164/E.163)
- Subscriber number in Private numbering plan (call routing in the Private numbering plan is based on customer specific translations).

4.5.7.2 Examples of encoding

The expected encoding of the *Called party number* information element for public network calls originated by a PRI user is shown in Table 3-25 on page 4-58. It is assumed that a carrier, where required, is part of the called party number digits, and not specified with a *Transit network selection* information element.

Table 3-25
Called party number encoding

Public Network Dialing Plan (prefixed by 9 in Centrex)	Called Party Number		
	Type of Number	Numbering Plan Ident'n	Digits
NXX-XXXX	Subscriber	E.164	NXX XXXX
NPA NXX-XXXX	National	E.164	NPA NXX XXXX
0	Subscriber	E.164	0
01 + CC + N(S)N	International	E.164	01 CC N(S)N
011 + CC + N(S)N	International	E.164	011 CC N(S)N
N11 (e.g. 411, 611, etc.)	Subscriber	E.164	N11
10TNS + NXX-XXXX	Subscriber	E.164	10TNS NXX XXXX
10TNS + NPA + NXX-XXXX	National	E.164	10TNS NPA NXX XXXX
10TNS + 0 + NXX-XXXX	Subscriber	E.164	10TNS 0 NXX XXXX
10TNS + 0 + NPA + NXX-XXXX	National	E.164	10TNS 0 NPA NXX XXXX
10TNS + 01 + CC + N(S)N	International	E.164	10TNS 01 CC N(S)N
10TNS + 0	Subscriber	E.164	10TNS 0
00	Subscriber	E.164	00

Note 1: "N" represents digits 2 - 9.

Note 2: "X" represents digits 0 - 9.

Note 3: "NPA" represents a 3 digit Numbering Plan Area:

— 'N' represents digits 2 - 9

— 'P' represents either 0 or 1

— 'A' represents digits 2 - 9

Note 4: "TNS" (Transit Network Selection) represents a 3 or 4 digit carrier identification code. Each TNS digit can be from 0 to 9.

4.5.8 Calling party number

The purpose of the *Calling party number* information element is to identify the origin of a call.

The maximum length of the information element is 16 octets.

Figure 4-18
Calling party number information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
	Calling party number information element identifier							1
0	1	1	0	1	1	0	0	
Length of information element								2
Ext. 0/1	Type of number			Numbering plan identification				3
Ext.	Presentation indicator		Spare			Screening indicator		3a*
1			0	0	0			
Spare 0	Number digits (IA5 characters)							4 … n

Note: The contents of this information element, other than octet 3a, are coded as shown for the *Called party number* information element in section 4.5.7 on page 4-56.

Presentation indicator (octet 3a)

7 6	
0 0	Presentation allowed
0 1	Presentation restricted
1 0	Number not available
1 1	Reserved

Note: If octet 3a is omitted:

— “Presentation allowed” is the default in the network -> user direction.

— Subscription default is assumed in the user -> network direction.

Screening indicator (octet 3a)

2	1	
0	0	User provided, not screened
0	1	User provided, verified and passed (see Note 1)
1	0	User provided, verified and failed (see Note 1)
1	1	Network provided

Note 1: This encoding is treated by the network as “user provided, not screened”.

Note 2: If octet 3a is omitted, “user provided, not screened” is the default.

4.5.9 Cause

The purpose of the *Cause* information element is to describe the reason for generating certain messages, to provide diagnostic information in the event of procedural errors and to indicate the location of the cause originator.

The maximum length of this information element is 10 octets. The network generates no more than 6 octets.

The *Cause* information element may be repeated once in a message but only the first cause value is transferred to the remote user through the network. Diagnostic information is not available for every cause.

Figure 4-19
Cause information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
	Cause information element identifier							1
0	0	0	0	1	0	0	0	
Length of information element								2
Ext.	Coding standard		Spare	Location				3
1			0					
Ext.	Cause value							4
1	Class			Value				
Diagnostics (if any)								5*

Coding standard (octet 3)

7 6	
0 0	CCITT standardized coding

All other values are reserved.

Location (octet 3)

4	3	2	1	
0	0	0	0	User
0	0	0	1	Private network serving the local user
0	0	1	0	Public network serving the local user
0	0	1	1	Transit network
0	1	0	0	Public network serving the remote user
0	1	0	1	Private network serving the remote user
0	1	1	1	International network

All other values are reserved.

> ***Note:*** The location code generated by the DMS-100 is datafillable. The allowable values are: user; private network serving the local user; and public network serving the local user. All location codes that are received are passed through to the terminating interface without alteration.

Cause value (octet 4)

The cause value is divided into two fields, a class (bits 5 through 7) and a value within the class (bits 1 through 4). The class indicates the general nature of the event.

Class (000)	Normal event
Class (001)	Normal event
Class (010)	Resource unavailable
Class (011)	Service or option not available
Class (100)	Service or option not implemented
Class (101)	Invalid message (for example, parameter out of range)
Class (110)	Protocol error (for example, unknown message)
Class (111)	Interworking

Diagnostics (octet 5)

Diagnostic information is not available for every cause. The inclusion of diagnostics is optional. When the network provides diagnostics, they are a maximum of two octets long with one octet providing a locking *Shift* information element identifier (if appropriate) to indicate a codeset other than codeset 0.

The cause values are listed below and further defined in Annex G.

Table 3-26
Cause value definitions

Cause value		Cause no.	Cause (and definition)	Diagnostics
Class	Value			
7 6 5	4 3 2 1			
		Normal event class		
0 0 0	0 0 0 1	1	Unallocated (unassigned) number	
0 0 0	0 0 1 0	2	No route to specified transit network	
0 0 0	0 0 1 1	3	No route to destination	
0 0 0	0 1 1 0	6	Channel unacceptable	
0 0 1	0 0 0 0	16	Normal call clearing	
0 0 1	0 0 0 1	17	User busy	
0 0 1	0 0 1 0	18	No user responding	
0 0 1	0 0 1 1	19	No answer from user (user alerted)	
0 0 1	0 1 0 1	21	Call rejected	
0 0 1	0 1 1 0	22	Number changed	
0 0 1	1 0 1 1	27	Destination out of order	
0 0 1	1 1 0 0	28	Invalid number format (address incomplete)	
0 0 1	1 1 0 1	29	Facility rejected	
0 0 1	1 1 1 0	30	Response to STATUS ENQUIRY	
0 0 1	1 1 1 1	31	Normal, unspecified	
		Resource unavailable class		
0 1 0	0 0 1 0	34	No circuit/channel available	
0 1 0	1 0 0 1	41	Temporary failure	
0 1 0	1 0 1 0	42	Switch equipment congestion	
0 1 0	1 0 1 1	43	Access information discarded	
0 1 0	1 1 0 0	44	Requested circuit/channel not available	
0 1 0	1 1 1 1	47	Resources unavailable, unspecified	
		Service or option not available class		
0 1 1	0 0 1 0	50	Requested facility not subscribed	
0 1 1	0 1 1 0	54	Incoming calls barred	
0 1 1	1 0 0 1	57	Bearer capability not authorized	
0 1 1	1 0 1 0	58	Bearer capability not presently available	

Table 3-26
Cause value definitions (Continued)

Cause value		Cause no.	Cause (and definition)	Diagnostics
Class	**Value**			
7 6 5	**4 3 2 1**			
0 1 1	1 1 1 1	63	Service or option not available, unspecified	
			Service or option not implemented class	
1 0 0	0 0 0 1	65	Bearer capability not implemented	
1 0 0	0 0 1 0	66	Channel type not implemented	
1 0 0	0 1 1 0	70	Only restricted digital information bearer capability is available	
1 0 0	1 1 1 1	79	Service or option not implemented, unspecified	
			Invalid message class	
1 0 1	0 0 0 1	81	Invalid call reference value	
1 0 1	0 0 1 0	82	Identified channel does not exist	
1 0 1	1 0 0 0	88	Incompatible destination	
1 0 1	1 0 1 0	90	Destination address missing, and direct call not subscribed	
1 0 1	1 1 1 1	95	Invalid message, unspecified	
			Protocol error class	
1 1 0	0 0 0 0	96	Mandatory information element is missing	Information element identifier
1 1 0	0 0 0 1	97	Message type non-existent or not implemented	Message type
1 1 0	0 0 1 1	99	Information element non-existent or not implemented	Information element identifier
1 1 0	0 1 0 0	100	Invalid information element contents	Information element identifier
1 1 0	0 1 0 1	101	Message not compatible with call state	Message type
1 1 0	0 1 1 0	102	Recovery on timer expiry	
1 1 0	1 1 1 1	111	Protocol error, unspecified	
			Interworking class	
1 1 1	1 1 1 1	127	Interworking, unspecified	

All other values are reserved.

4.5.10 Change status

The purpose of the *Change status* information element is to change the current status of either an interface or channel to one of the following states: “in service”, “maintenance” or “out of service”.

The *Change status* information element is used with the maintenance protocol discriminator.

The maximum length of this information element is 3 octets.

Figure 4-20
Change status information element

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th><th>Octet</th></tr>
<tr><td rowspan="2">0</td><td colspan="7">Change status information element identifier</td><td rowspan="2">1</td></tr>
<tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Length of information element</td><td>2</td></tr>
<tr><td>Ext.
1</td><td>Prefer-ence</td><td colspan="3">Spare
0 0 0</td><td colspan="3">New status</td><td>3</td></tr>
</table>

Preference (octet 3)

7	
0	Reserved
1	Channel

New Status (octet 3)

3	2	1	
0	0	0	In service
0	0	1	Maintenance (see Note)
0	1	0	Out of service

All other values are reserved.

Note: This encoding is treated by the network as “Out of service”.

4.5.11 Channel identification

The purpose of the *Channel identification* information element is to identify a channel within the interface controlled by these signaling procedures.

The maximum length for this information element is 8 octets.

Figure 4-21
Channel identification information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
	Channel identification information element identifier							1
0	0	0	1	1	0	0	0	
Length of information element								2
Ext. 1	Interface identifier present	Interface type 1	Spare 0	Preferred / Exclusive	D-channel indicator 0	Information channel selection 0	1	3
Ext. 1	Interface identifier							3.1* (see Note 1)
Ext. 1	Coding standard 0	0	Number/ Map	Channel type /Map element type				3.2* (see Note 3)
Channel number / Slot map (see Note 2)								3.3* (see Note 3)

Note 1: When the “interface identifier present” field in octet 3 indicates “interface implicitly identified”, octet 3.1 is omitted.

Note 2: When the channel number format is used, bit 8 is set to “1”.

Note 3: These octets are omitted when the entire interface is to be identified (for example, when the 1536 kbit/s information transfer rate is specified in the *Bearer capability* information element.

Interface identifier present (octet 3, bit 7)

7	
0	Interface implicitly identified (see Note 1)
1	Interface explicitly identified in octet 3.1 (interface identifier).

Note 1: The interface which includes the D-channel carrying this information element is indicated.

Note 2: When the interface is implicitly identified, octet 3.1 is omitted.

Interface type (octet 3, bit 6)

6	
0	Reserved
1	Primary rate interface

Preferred / Exclusive (octet 3, bit 4)

4	
0	Indicated channel is preferred
1	Exclusive; only the indicated channel is acceptable

Note: Preferred/exclusive has significance only for B-channel selection. They are both treated as exclusive by this specification.

D-channel indicator (octet 3, bit 3)

3	
0	Channel identified is not the D-channel
1	Channel identified is the D-channel

Note: D-channel indication has significance in D-channel use. No other information affects D-channel use.

Information channel selection (octet 3, bits 1 and 2)

2	1	Primary interface
0	0	No channel
0	1	As indicated in the following octets

All other values are reserved.

Interface identifier (octet 3.1)

Binary code in the range 0 to 31 assigned to the interface at subscription time.

> ***Note:*** When the interface is implicitly identified, octet 3.1 is omitted.

Coding standard (octet 3.2)

7 6	
0 0	CCITT Standardized coding

All other values are reserved.

Number / Map (octet 3.2)

5	
0	Channel is indicated by the number in the following octet
1	Channel is indicated by the slot map in the following octets

> ***Note 1:*** When the information transfer rate is 64 kbit/s the channel number is used.
>
> ***Note 2:*** The slot map is used only when the information transfer rate is 384 kbit/s or multirate (64 kbit/s base rate). The slot map is not used for restart procedures or maintenance procedures.

Channel type / Map element type (octet 3.2)

4 3 2 1	
0 0 1 1	B-channel units

All other values are reserved.

Channel number (octet 3.3)

The binary number that is assigned to the channel. For B-channels, the channel number equals the time slot number.

> ***Note:*** Either “Channel number” or “Slot map” is used exclusively, depending on the “Number / Map” information.

Slot map (octet 3.3)

Bit positions in the slot map corresponding to time slots used by the channel are set to “1”. The remaining bits are set to “0”.

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
24	23	22	21	20	19	18	17	3.3.1
16	15	14	13	12	11	10	9	3.3.2
8	7	6	5	4	3	2	1	3.3.3

4.5.12 Connected number

The purpose of the *Connected number* information element is to identify the responding party to a call. The connected number may be different from the calling or called party number(s) because of changes (e.g. call redirection) during the lifetime of the call.

The maximum length of the information element is 16 octets.

Figure 4-22
Connected number information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
	Connected number information element identifier							1
0	0	0	0	1	1	0	0	
Length of information element								2
Ext.	Type of number			Numbering plan identification				3
0/1								
Ext.	Presentation indicator		Spare			Screening indicator		3a*
1			0	0	0			
Spare	Number digits (IA5 characters)							4 ... n
0								

Note 1: The contents of this information element are coded as shown for the *Calling party number* information element in section 4.5.8 on page 4-59.

4.5.13 Destination

The purpose of the *Destination* information element is to identify the destination of a connectionless signaling message. This information element is located in codeset 6.

The maximum length of the information element is 17 octets.

Figure 4-23
Destination information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
	Destination information element identifier							1
0	0	0	0	0	0	1	0	
Length of information element								2
Ext. 1	Type of routing				Encoding			3
Ext. 0/1	Private network identifier							3.1*
Ext. 0/1	Private network identifier (continued)							3.1a*
Ext. 1	Private network identifier (continued)							3.1b*
Length of routing information								4
Routing information								5 ... n

Type of routing (octet 3)

7	6	5	4	
0	0	0	0	Spare
0	0	0	1	Private number
0	0	1	0	Public number (Recommendation E.164)
0	0	1	1	CCS7 point code

All other values are reserved.

Encoding (octet 3)

3	2	1	
0	0	0	Spare
0	0	1	BCD odd
0	1	0	BCD even
0	1	1	Binary
1	0	0	IA5

All other values are reserved.

Private network identifier (octets 3.1 to 3.1b, bits 1 to 7)

This field is present if the type of routing field identifies a private number. Contained in this field is a binary number identifying the private network. The field may consist of one, two or three octets. The least significant bit is bit 1 of octet 3.1 and the most significant bit is bit 7 of the octet 3.1b. If octet 3.1b is present only bit 1 is part of the private network identifier; bits 2 to 7 should contain all zeroes.

Length of routing information (octet 4)

This field specifies the length in octets of the routing information field.

Routing information (octet 5)

7 6 5	4 3 2 1	Character
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
0 1 0	1 0 1 0	*
0 1 0	0 0 1 1	#

This field identifies the number that is used for routing of the *Facility* information element to the appropriate node. The routing information field is encoded using IA5 characters. The IA5 digits are coded in bits 1 to 7, and bit 8 is spare (that is, set to “0”).

4.5.14 Display

The purpose of the *Display* information element is to supply information that may be displayed by the user.

The *Display* information element may be repeated twice in a message to support supplementary services such as Network Name (see Section 5 for further information).

The maximum length of the information element is 18 octets. If the receiver of the information element cannot handle all the display information, the information element should be truncated.

Figure 4-24
Display information element

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th><th>Octet</th></tr>
<tr><td rowspan="2">0</td><td colspan="7">Display information element identifier</td><td rowspan="2">1</td></tr>
<tr><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td colspan="8">Length of information element</td><td>2</td></tr>
<tr><td>Ext.
1</td><td colspan="3">Associated information</td><td colspan="4">Display type</td><td>3</td></tr>
<tr><td>Spare
0</td><td colspan="7">Display information (IA5 characters)</td><td>4 ... n</td></tr>
</table>

Associated information (octet 3)

7 6 5	
0 0 1	Requested
0 1 1	Included

All other values are reserved.

Display type (octet 3)

4	3	2	1	
0	0	0	1	Calling party name
0	0	1	0	Connected party name
0	1	0	1	Original called party name

All other values are reserved.

Display information (octet 4, etc.)

Display information is a string of IA5 characters, starting in octet 4. The IA5 characters are coded in bits 1 to 7, and bit 8 is spare (that is, set to “0”).

4.5.15 Facility

The purpose of the *Facility* information element is to indicate the invocation and operation of supplementary services identified by the corresponding operation value within the *Facility* information element.

The maximum length of the information element depends on the service provided.

Figure 4-25
Facility information element

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th><th>Octet</th></tr>
<tr><td rowspan="2">0</td><td colspan="7">Facility information element identifier</td><td rowspan="2">1</td></tr>
<tr><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td></tr>
<tr><td colspan="8">Length of information element</td><td>2</td></tr>
<tr><td>Ext.
0/1</td><td colspan="2">Spare
0 0</td><td colspan="5">Service discriminator</td><td>3*</td></tr>
<tr><td>Ext.
1</td><td colspan="7">Service identifier</td><td>3a</td></tr>
<tr><td colspan="8">User data</td><td>4 ... n</td></tr>
</table>

Service discriminator (octet 3)

5	4	3	2	1	
1	0	0	0	1	Supplementary services (ROSE)
1	0	0	1	0	Supplementary services (TCAP)

All other values are reserved.

Note: Octet 3 is not included for the Network Ring Again service.

Service Identifier (octet 3a)

7	6	5	4	3	2	1	
0	1	1	1	1	1	0	Release Link Trunk (RLT)
1	1	1	0	0	0	0	Network Message Service (NMS)
1	1	1	1	1	1	0	Network Automatic Call Distribution (NACD)
1	1	1	1	1	1	1	Network Ring Again (NRAG)

All other values are reserved.

4.5.15.1 ROSE user data (octet 4, etc.)

If the service discriminator field indicates ROSE, the user data field contains ROSE protocol. The ROSE protocol is defined in the ANSI T1.610 standard.

Component

A component is a sequence of data elements each of which is made up of a tag, a length and contents. There are 4 types of components, each identified by a unique component tag.

The following components are supported:

- Invoke
- Return result
- Return error
- Reject

ROSE components are also referred to in section 12.3.2 on page 5-124.

The structure of each type of component is shown in Figure 4-26 through Figure 4-29.

Figure 4-26
Invoke component

Invoke Component		Reference	Mandatory Indication	Octet Group
Component type tag		Page 4-82	Mandatory	4
Component length (see Note 1)		Page 4-81		5
	Invoke identifier tag	Page 4-82	Mandatory	6
	Invoke identifier length	Page 4-81		7
	Invoke identifier			8
	Linked value tag	Page 4-82	Optional	9
	Linked value length	Page 4-81		10
	Linked value			11
	Operation value tag	Page 4-83	Mandatory	12
	Operation value length	Page 4-81		13
	Operation value	(see Note 3)		14
	Argument (see Note 2)	Page 4-85	Optional	15
		(see Note 3)		etc.

Note 1: The component length is coded to indicate the number of octets contained in the component, excluding the component type tag and the component length octets.

Note 2: This is a parameter of the Invoke component type.

Note 3: The coding is service dependent.

Figure 4-27
Return Result component

Return Result Component	Reference	Mandatory Indication	Octet Group
Component type tag	Page 4-82	Mandatory	4
Component length (see Note 1)	Page 4-81		5
Invoke identifier tag	Page 4-82	Mandatory	6
Invoke identifier length	Page 4-81		7
Invoke identifier			8
Sequence tag	Page 4-85	Optional	9
Sequence length (see Note 4)		(see Note 1)	10
Operation value tag	Page 4-83	Optional	11
Operation value length	Page 4-81		12
Operation value	(see Note 6)	(see Note 2)	13
Result (see Note 5)	Page 4-82	Optional	14
	(see Note 6)		etc.

Note 1: If the Return result component does not include any result, then the sequence and operational value are omitted. "Component types" on page 4-82 shows the coding for the sequence tag.

Note 2: If a result is included, the operation value is mandatory and is the first element in the sequence.

Note 3: The component length is coded to indicate the number of octets contained in the component, excluding the component type tag and the component length octets.

Note 4: The sequence length is coded to indicate the number of octets contained in the sequence, excluding the sequence type tag and the sequence length octets.

Note 5: This is a parameter of the Return result component type.

Note 6: The coding is service dependent.

Figure 4-28
Return error component

Return Error Component		Reference	Mandatory Indication	Octet Group
Component type tag		Page 4-82	Mandatory	4
Component length (see Note 1)		Page 4-81		5
	Invoke identifier tag	Page 4-82	Mandatory	6
	Invoke identifier length	Page 4-81		7
	Invoke identifier			8
	Error value tag	Page 4-83	Mandatory	9
	Error value length	Page 4-81		10
	Error value			11
	Parameter	Page 4-85	Optional	12
	(see Note 2)	(see Note 3)		etc.

Note 1: The component length is coded to indicate the number of octets contained in the component, excluding the component type tag and the component length octets.

Note 2: This is a parameter of the Return result component type.

Note 3: The coding is service dependent.

Figure 4-29
Reject component

Reject Component		Reference	Mandatory Indication	Octet Group
Component type tag		Page 4-82	Mandatory	4
Component length (Note)		Page 4-81		5
	Invoke identifier tag	Page 4-82	Mandatory	6
	Invoke identifier length	Page 4-81		7
	Invoke identifier			8
	Problem tag	Page 4-83	Mandatory	9
	Problem length	Page 4-81		10
	Problem	Page 4-83		11

Note: The component length is coded to indicate the number of octets contained in the component, excluding the component type tag and the component length octets.

Length of each component or data element

Lengths up to 127 octets are coded using the short form of the length field. The length format is set to “0” and the remaining 7 bits are the length of the contents in octets. Bit 7 is the most significant bit (MSB) and bit 1 is the least significant bit (LSB).

Figure 4-30
Format of the length field (short form)

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
Length format 0	Length of contents						
	MSB						LSB

Lengths greater than 127 octets are coded using the long form of the length field. The length format is set to “1” and the remaining 7 bits of the first octet are the length of the length field, less this first octet. Bit 7 is the most significant bit (MSB) and bit 1 is the least significant bit (LSB) of this first octet. The remaining octets (maximum of 2) are the length of the contents in octets. Bit 8 of the second octet is the most significant bit (MSB) and bit 1 of the last octet is the least significant bit (LSB). The length of contents should be coded using the minimum number of octets, with no leading octets having the value 0.

Figure 4-31
Format of the length field (long form)

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
Length Format 1	MSB			(Length field size) - 1			LSB	1
MSB				Length of contents			LSB	2 ... 3

Note: The network may use the long form of the length field for lengths less than 128 octets for some constructor data elements.

Component types

Every component is specified with a component type tag. The following table contains the tags for the component types.

Component type tags

8	7	6	5	4	3	2	1	
1	0	1	0	0	0	0	1	Invoke
1	0	1	0	0	0	1	0	Return result
1	0	1	0	0	0	1	1	Return error
1	0	1	0	0	1	0	0	Reject

Component identifiers

An invoke identifier is used to identify an operation invocation and is reflected in the Return result or Return error that responds to it. An Invoke may refer to another Invoke through the linked identifier. When a protocol error occurs, the invoke identifier is reflected in the Reject component, but if it is not available, a null is returned. Invoke and linked identifiers are one octet long. The null has zero length.

The component identifiers, invoke identifier and linked identifier, are unique within a call reference. That is, the same identifiers can be used simultaneously in separate call references without ambiguity.

Component identifier tags

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	1	0	Invoke identifier
1	0	0	0	0	0	0	0	Linked identifier
0	0	0	0	0	1	0	1	Null

Operations

The operation value specifies the service or operation being requested. An operation value is an integer value and its meaning is specific to each service. Operation values are unique within each service discriminator.

Operation value tags

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	1	0	Operation value — Integer

Supplementary services operation values

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	1	1	1	1	1	1	0	NACD Receive info (7E05 hex)
0	0	0	0	0	1	0	1	

Errors

Operations report errors as specified for each operation.

Error value tags

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	1	0	Error value — Integer

Problems

Protocol problems are indicated in groups. The first of the following tables specifies the tags for these groups. The remaining tables specify the problem values associated with each problem group.

Problem tags

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
1	0	0	0	0	0	0	0	General problem
1	0	0	0	0	0	0	1	Invoke problem
1	0	0	0	0	0	1	0	Return result problem
1	0	0	0	0	0	1	1	Return error problem

General problems

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	Unrecognized component
0	0	0	0	0	0	0	1	Mistyped component
0	0	0	0	0	0	1	0	Badly structured component

Invoke problems

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	Duplicate invocation
0	0	0	0	0	0	0	1	Unrecognized operation
0	0	0	0	0	0	1	0	Mistyped argument
0	0	0	0	0	0	1	1	Resource limitation
0	0	0	0	0	1	0	0	Initiator releasing
0	0	0	0	0	1	0	1	Unrecognized linked identifier
0	0	0	0	0	1	1	0	Linked response unexpected
0	0	0	0	0	1	1	1	Unexpected child operation

Return result problems

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	Unrecognized invocation
0	0	0	0	0	0	0	1	Result response unexpected
0	0	0	0	0	0	1	0	Mistyped result

Return error problem

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	Unrecognized invocation
0	0	0	0	0	0	0	1	Error response unexpected
0	0	0	0	0	0	1	0	Unrecognized error
0	0	0	0	0	0	1	1	Unexpected error
0	0	0	0	0	1	0	0	Mistyped parameter

Parameters

Parameters included with a component (that is, argument of Invoke, result of Return result or parameter of Return error) are indicated in the operation specification. They may include optional and default parameters. Parameters are one of the following:

- a sequence of parameters
- a set of parameters
- a specific parameter with its own tag
- null (absent)

If more than one parameter is required, they follow a sequence or set tag, as specified for the operation. Each parameter in a set or sequence is allowed to be a set or sequence.

Sequence and set tags

8 7 6 5	4 3 2 1	
0 0 1 1	0 0 0 0	Sequence tag
0 0 1 1	0 0 0 1	Set tag

4.5.15.2 TCAP user data (octet 4, etc.)

If the service discriminator field indicates TCAP, then the user data field contains TCAP protocol. The TCAP protocol is defined in the ANSI T1.114 standard.

This section provides an overview of the common elements of the TCAP protocol. The application specific information is described in Section 5.

Each data element in a TCAP message is encoded using a sequence of octets logically divided into an Identifier, Length of contents, and Contents. The Identifier distinguishes one type from another and governs the interpretation of the Contents. The Length of contents specifies the length of the contents. The Contents contains the primary information being conveyed by the data element.

Identifier

All Identifiers use bits 8 and 7 to indicate the identifier class. The coding of the identifier class is shown in Table 3-27.

Table 3-27
Identifier class

Class	Bits 8 7	Usage
Universal	0 0	Universal
Application-wide	0 1	International TCAP
Context-specific	1 0	Context specific
Private use	1 1	National TCAP / Private TCAP

Bit 6 is used to indicate whether the data type is “primitive” or “constructor”. A primitive type is one whose structure is atomic (that is, one value only). A constructor type is one whose content is a series of data elements (that is, a recursive definition of a single value or a sequence of values).

Bits 5 to 1 of the Identifier octet represent an identifier code that distinguishes one data type from another of the same class.

Identifier codes in the range “00000” to “11110” are provided in one octet.

The extension mechanism is to code bits 5 to 1 as “11111”. If bit 8 of the extension octet is set to “0”, no further octets are used. All preceding extension octets must have bit 8 set to “1”. The resultant Identifier consists of bits 7 to 1 of each extension octet, with the first extension octet being the most significant.

When the Private use class is specified, bits 5 to 1 of the first Identifier octet are reserved for national use only. The extended formats are shared between private TCAP and national TCAP usage. If bit 7 of the second octet is set to “0”, a nationally assigned Identifier is implied. If bit 7 is set to “1”, a privately assigned Identifier is implied.

Length of contents

The Length of contents field is coded to indicate the number of octets in the contents. The length does not include the Identifier or the Length of contents.

When the contents are longer than 127 octets, the long form of the Length of Contents is used. The long form is from 2 to 127 octets long. Bit 8 of the first octet has the value “1”. Bits 7 to 1 of the first octet encode a number one less than the size of the Length of Contents field (in octets) as an unsigned binary number whose most significant (MSB) and least significant bit (LSB) are bit 7 and 1, respectively. The length itself is encoded as an unsigned binary number whose MSB and LSB are bit 8 of the second octet and bit 1 of the last octet, respectively. This binary number is encoded in the fewest possible octets, with no leading octets having the value 0.

TCAP message structure

A TCAP message consists of a Transaction Portion and one or more Components. Figure 4-32 shows the message structure format.

Figure 4-32
General TCAP message structure

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th><th></th></tr>
<tr><td colspan="8">Package type identifier</td><td rowspan="7">Transaction Portion</td></tr>
<tr><td colspan="8">Total TCAP message length</td></tr>
<tr><td colspan="8">Transaction ID identifier</td></tr>
<tr><td colspan="8">Transaction ID length</td></tr>
<tr><td colspan="8">Transaction IDs</td></tr>
<tr><td colspan="8">Component sequence identifier</td></tr>
<tr><td colspan="8">Component sequence length</td></tr>
<tr><td colspan="8">Component A</td><td rowspan="3">Component Portion</td></tr>
<tr><td colspan="8">. . . . .</td></tr>
<tr><td colspan="8">Component n</td></tr>
</table>

Package type identifier

This one octet field is mandatory for all TCAP messages. It identifies the type of message that is being sent. The four package types which are used are:

- Query with Permission
  - — This package type is used to establish a transaction.
- Conversation with Permission
  - — This package type is used once the transaction has been established, and further communication between the switches is expected.
- Response
  - — This package type is used to complete the transaction.
- Unidirectional
  - — This package type is used when no transaction exists or is required.

Total TCAP message length

This field may be from 1 to 127 octets long. If the TCAP message is less then 127 octets, this field is one octet long. If the message length is greater then 127 octets then the length itself is encoded in two or more octets.

Transaction ID identifier

Transaction IDs are assigned to a TCAP message to permit transaction association.

Transaction ID length

The Transaction ID length is the total length in octets used by the Transaction IDs in a TCAP message. The value of the length is determined by the combined length of the originating and responding Transaction IDs combined. It may be 0, 4 or 8 octets in length.

Transaction IDs

Depending on the Package type there may be zero or more transaction IDs present in this parameter. In TCAP there are only two types of transaction IDs. Table 3-28 shows the relationship between the package type and the transaction ID.

Table 3-28
Transaction ID's and package types

Package type identifier	Originating Transaction ID	Responding Transaction ID
Unidirectional	No	No
Query with Permission	Yes	No
Response	No	Yes
Conversation with Permission	Yes	Yes

Originating transaction ID

This field contains the Transaction ID assigned by the originator. When present, it consists of four octets and is the first of the Transaction IDs when both Originating and Terminating transaction IDs are present.

Responding transaction ID

This field contains the Transaction ID assigned by the responder. The Responding transaction ID has the same format and length as the Originating transaction ID.

Component sequence identifier

This field identifies the following Component sequence and is coded national, constructor with Identifier code 8 (“11101000”).

Component sequence length

This field encodes the total length in octets of the Component sequence. It may be from 1 to 127 octets in length, as described in the Total TCAP message length parameter.

Component type identifier

The Component type is coded national, constructor, as shown in Table 3-29.

Table 3-29
Component type identifier encoding

Component type identifier	8 7 6 5 4 3 2 1
Invoke (last)	1 1 1 0 1 0 0 1
Return Result (last)	1 1 1 0 1 0 1 0
Return Error	1 1 1 0 1 0 1 1
Reject	1 1 1 0 1 1 0 0
Invoke (not last)	1 1 1 0 1 1 0 1

Component structures

The structures of Invoke, Return result, Return error and Reject components are shown in Figure 4-33 through Figure 4-36.

Figure 4-33
Invoke component structure

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th></tr>
<tr><td colspan="8">Component type identifier</td></tr>
<tr><td colspan="8">Component length</td></tr>
<tr><td colspan="8">Component ID identifier</td></tr>
<tr><td colspan="8">Component ID length</td></tr>
<tr><td colspan="8">Component IDs</td></tr>
<tr><td colspan="8">Operation code identifier</td></tr>
<tr><td colspan="8">Operation code length</td></tr>
<tr><td colspan="8">Operation code</td></tr>
<tr><td colspan="8">Parameter set/sequence identifier</td></tr>
<tr><td colspan="8">Parameter set/sequence length</td></tr>
<tr><td colspan="8">Parameter set/sequence</td></tr>
</table>

Figure 4-34
Return result component structure

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th></tr>
<tr><td colspan="8">Component type identifier</td></tr>
<tr><td colspan="8">Component length</td></tr>
<tr><td colspan="8">Component ID identifier</td></tr>
<tr><td colspan="8">Component ID length</td></tr>
<tr><td colspan="8">Component IDs</td></tr>
<tr><td colspan="8">Parameter set/sequence identifier</td></tr>
<tr><td colspan="8">Parameter set/sequence length</td></tr>
<tr><td colspan="8">Parameter set/sequence</td></tr>
</table>

Figure 4-35
Return error component structure

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th></tr>
<tr><td colspan="8">Component type identifier</td></tr>
<tr><td colspan="8">Component length</td></tr>
<tr><td colspan="8">Component ID identifier</td></tr>
<tr><td colspan="8">Component ID length</td></tr>
<tr><td colspan="8">Component IDs</td></tr>
<tr><td colspan="8">Error code identifier</td></tr>
<tr><td colspan="8">Error code length</td></tr>
<tr><td colspan="8">Error code</td></tr>
<tr><td colspan="8">Parameter set/sequence identifier</td></tr>
<tr><td colspan="8">Parameter set/sequence length</td></tr>
<tr><td colspan="8">Parameter set/sequence</td></tr>
</table>

Figure 4-36
Reject component structure

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th></tr>
<tr><td colspan="8">Component type identifier</td></tr>
<tr><td colspan="8">Component length</td></tr>
<tr><td colspan="8">Component ID identifier</td></tr>
<tr><td colspan="8">Component ID length</td></tr>
<tr><td colspan="8">Component IDs</td></tr>
<tr><td colspan="8">Problem code identifier</td></tr>
<tr><td colspan="8">Problem code length</td></tr>
<tr><td colspan="8">Problem code</td></tr>
<tr><td colspan="8">Parameter set/sequence identifier</td></tr>
<tr><td colspan="8">Parameter set/sequence length</td></tr>
<tr><td colspan="8">Parameter set/sequence</td></tr>
</table>

Component length

This field specifies how many additional octets are in this component.

Component ID identifier

The Component ID identifier is coded national, primitive, with identifier code 15 (“11001111”).

Component ID length

The Component ID length indicates the total length of the Component IDs. The length may be 0, 1 or 2 octets.

Component IDs

The number of Component IDs is determined by the Component type and is shown in Table 3-30.

Table 3-30
Component IDs versus component type

Component type	Invoke ID	Correlation ID
Invoke (last)	Optional (see Note)	Reflected
Return Result	Absent	Reflected
Return Error	Absent	Reflected
Reject	Absent	Reflected
Invoke (not last)	Optional (see Note)	Reflected

Note: Mandatory when the Correlation ID is present

Where the “reflected” status is indicated for Correlation IDs, the IDs are mandatory only if an Invoke ID was present in the corresponding Invoke component.

Invoke ID

The Invoke ID is assigned to a component initiating an operation. It is optional and, if present, is one octet long.

Correlation ID

The Correlation ID is assigned to components sent in response to another component. It is mandatory when the received Component had an Invoke ID. It is optional and, if present, is one octet long.

Operation code identifier

This Operation code identifier identifies the Operation code that follows as being either National TCAP or Private TCAP. It is coded national, primitive, as in Table 3-31.

Table 3-31
Operation code identifier encoding

Operation code identifier	8 7 6 5	4 3 2 1
National TCAP	1 1 0 1	0 0 0 0
Private TCAP	1 1 0 1	0 0 0 1

Operation code length

This field specifies the length of the Operation code. It is 2 octets long.

Operation code

The Operation code is partitioned into an operation family followed by a specifier associated with each operation family member. The length of the operation family field and specifier field are one octet each.

The operation codes are application specific information.

Error code identifier

This Error code identifier identifies the Error code that follows as being either National TCAP or Private TCAP. It is coded national, primitive, as shown in Table 3-32.

Table 3-32
Error code identifier encoding

Error code identifier	8 7 6 5 4 3 2 1
National TCAP	1 1 0 1 0 0 1 1
Private TCAP	1 1 0 1 0 1 0 0

Error code length

This field specifies the length of the Error code. The Error code is one octet long.

Error code

This provides the reason why a specific operation could not be completed successfully. The Error codes are application specific information.

Problem code identifier

This field indicates that a Problem code follows. It is coded national, primitive, as shown in Table 3-33.

Table 3-33
Problem code identifier encoding

	8 7 6 5 4 3 2 1
Problem code identifier	1 1 0 1 0 1 0 1

Problem code length

This field specifies the length of the Problem code. It is two octets long.

Problem code

This field indicates the reason the component or transaction portion was rejected. The Problem code is partitioned into a Problem type followed by a

Problem specifier associated with each Problem type. The lengths of the Problem type field and Problem specifier field are one octet each.

The Problem type values are coded as shown in Table 3-34. The Problem specifier values are coded as shown in Table 3-35.

Table 3-34
Problem types

Problem type	8 7 6 5	4 3 2 1
General	0 0 0 0	0 0 0 1
Invoke	0 0 0 0	0 0 1 0
Return Result	0 0 0 0	0 0 1 1
Return Error	0 0 0 0	0 1 0 0

Table 3-35
Problem specifiers

Problem type	Problem specifier	8 7 6 5	4 3 2 1
General	Unrecognized component	0 0 0 0	0 0 0 1
General	Incorrect component portion	0 0 0 0	0 0 1 0
General	Badly structured component portion	0 0 0 0	0 0 1 1
Invoke	Duplicate invoke ID	0 0 0 0	0 0 0 1
Invoke	Unrecognized operation	0 0 0 0	0 0 1 0
Invoke	Incorrect parameter	0 0 0 0	0 0 1 1
Invoke	Unrecognized correlation ID	0 0 0 0	0 1 0 0
Return Result	Unrecognized correlation ID	0 0 0 0	0 0 0 1
Return Result	Unexpected return result	0 0 0 0	0 0 1 0
Return Result	Incorrect parameter	0 0 0 0	0 0 1 1
Return Error	Unrecognized correlation ID	0 0 0 0	0 0 0 1
Return Error	Unexpected return error	0 0 0 0	0 0 1 0
Return Error	Unrecognized error	0 0 0 0	0 0 1 1
Return Error	Unexpected error	0 0 0 0	0 1 0 0
Return Error	Incorrect parameter	0 0 0 0	0 1 0 1

Parameter set identifier

This field indicates that a set of Parameters is to follow. It is coded as national, constructor, as shown in Table 3-36.

Table 3-36
Parameter set identifier encoding

	8 7 6 5	**4 3 2 1**
Parameter set identifier	1 1 1 1	0 0 1 0

Parameter set length

This field indicates the total length in octets of the Parameter set.

Parameter sequence identifier

This field indicates that a sequence of Parameters is to follow. It is coded as universal, constructor, as shown in Table 3-37.

Table 3-37
Parameter sequence identifier encoding

	8 7 6 5	**4 3 2 1**
Parameter sequence identifier	0 0 1 1	0 0 0 0

Parameter sequence length

This length indicates the total length in octets of the Parameter sequence.

Parameters

The Parameter identifiers and contents are application specific information.

4.5.16 Information request

The purpose of the *Information request* information element is to provide the capability for requesting additional information and to signal completion of the information request.

The maximum length of the information element is 4 octets.

Figure 4-37
Information request information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
0	Information request information element identifier							1
	0	1	1	0	0	1	0	
Length of information element								2
Ext. 0/1	Information request indicator	Type of information						3
Ext. 1	Information specifics							3a

Information request indicator (octet 3)

7	
0	Information request completed
1	Prompt for additional information

Type of information (octet 3)

6 5	4 3 2 1	
0 0	0 0 0 0	Undefined
0 0	0 0 0 1	Authorization code
0 0	0 0 1 0	Address digits
0 0	0 0 1 1	Terminal identification

All other values are reserved.

Information specifics (Octet 3a)

7	6	5	4	3	2	1	
0	0	0	0	0	0	0	Dialed number (default)
0	0	0	0	0	0	1	Calling party number
0	0	0	0	0	1	0	Connected number
0	0	1	0	0	0	0	Redirecting number and indicators
0	0	1	0	0	0	1	Redirection number and indicators
0	0	1	0	0	1	0	Redirecting number without reason indicator
0	0	1	0	0	1	1	Redirection number without reason indicator
0	1	1	0	0	0	0	Information denied
0	1	1	0	0	0	1	Information not available

All other values are reserved.

4.5.17 Network-specific facilities

The purpose of the *Network-specific facilities* information element is to indicate which network facilities are being invoked.

The maximum length of this information element is 7 octets.

Figure 4-38
Network-specific facilities information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
	Network-specific facilities information element identifier							1
0	0	1	0	0	0	0	0	
Length of information element								2
Length of network identification								3
Ext. 1	Type of network identification			Network identification plan				3.1* (Note)
Spare 0	Network identification characters (IA5)							3.2* (Note)
Ext. 0/1	Expansion 1	Service / Feature	Binary facility coding value					4
Ext. 0/1	Service identifier							4a*
Ext. 0/1	Service identifier (continued)							4b*
Ext. 1	Service identifier (continued)							4c*

Note: These octets are ignored.

Length of network identification (octet 3)

This field contains the length, in octets, of the network identification found in octet 3.1 and the repetition of octet 3.2. Octets 3.1 and 3.2 are ignored if present, and the local serving network determines access to the requested facility.

Expansion (octet 4)

7	
0	Reserved
1	Last octet of description

Service / Feature (octet 4)

6	
0	Reserved
1	Service

Binary facility coding value (octet 4)

All defined Binary facility coding value settings are valid for both public (E.164) and private numbering plans. An invalid encoding results in network determined treatment.

5	**4**	**3**	**2**	**1**	
0	0	0	0	1	Private
0	0	0	1	0	Inwats
0	0	0	1	1	Outwats
0	0	1	0	0	Foreign exchange (FX)
0	0	1	0	1	Tie trunk (TIE)

All other values are reserved.

Service identifier (octets 4a to 4c)

The service identifier is used to identify a specific trunk route or Outwats zone. The most significant bit is bit 7 in octet 4a. The least significant bit is bit 1 of octet 4c. If all three octets are present (4a, 4b and 4c), only the least significant 15 bits are used (that is, bit 1 of octet 4a, bits 1 to 7 of octet 4b, and bits 1 to 7 of octet 4c). In this case, bits 2 to 7 of octet 4a are coded all zeroes.

4.5.18 Notification indicator

The purpose of the *Notification indicator* information element is to indicate information pertaining to a call.

The maximum length of the information element is 3 octets.

Figure 4-39
Notification Indicator information element

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th><th>Octet</th></tr>
<tr><td rowspan="2">0</td><td colspan="7">Notification indicator information element identifier</td><td rowspan="2">1</td></tr>
<tr><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td colspan="8">Length of information element</td><td>2</td></tr>
<tr><td>Ext.
1</td><td colspan="7">Notification description</td><td>3</td></tr>
</table>

Notification description (octet 3)

7	6	5	4	3	2	1	
1	1	1	0	0	0	1	Call information/event

All other values are reserved.

4.5.19 Options

The purpose of the *Options* information element is to select options for a connectionless *FACILITY* message. This information element is located in codeset 6.

The maximum length of the information element is 3 octets.

Figure 4-40
Options information element

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th><th>Octet</th></tr>
<tr><td rowspan="2">0</td><td colspan="7">Options information element identifier</td><td rowspan="2">1</td></tr>
<tr><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>1</td><td>0</td></tr>
<tr><td colspan="8">Length of information element</td><td>2</td></tr>
<tr><td>Ext.
1</td><td colspan="7">Options value</td><td>3</td></tr>
</table>

Options Value (octet 3)

7 6 5	4 3 2 1	
0 0 0	0 0 0 1	Return message on error

All other values are reserved.

4.5.20 Origination

The purpose of the *Origination* information element is to identify the origin of the connectionless signaling message. This information element is located in codeset 6.

The maximum length of the information element is 17 octets.

Figure 4-41
Origination information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
	Origination information element identifier							1
0	0	0	0	0	0	0	1	
Length of information element								2
Ext. 1	Type of routing			Encoding				3
Ext. 0/1	Private network identifier							3.1*
Ext. 0/1	Private network identifier (continued)							3.1a*
Ext. 1	Private network identifier (continued)							3.1b*
Length of routing information								4
Routing information								5 ... n

Note: The contents of this information element are coded as shown for the *Destination* information element in section 4.5.13 on page 4-71.

4.5.21 Original called number

The purpose of the *Original called number* information element is to identify the original called party when call redirection has occurred.

The maximum length of the information element is 18 octets.

Figure 4-42
Original called number information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
	Original called number information element identifier							1
0	1	1	1	0	0	1	1	
Length of information element								2
Ext.	Type of number			Numbering plan identification				3
0/1								
Ext.	Presentation indicator		Spare			Screening indicator		3a*
0/1			0	0	0			
Ext.	Spare			Original redirection reason				3b*
0/1	0	0	0					
Ext.	CFNR indicator	Spare			Redirection counter			3c*
1		0	0	0				
Spare	Number digits (IA5 characters)							4 ... n
0								

Type of number (octet 3)

7 6 5	
0 0 0	Unknown
0 0 1	International number
0 1 0	National number
1 0 0	Subscriber number

All other values are reserved.

Numbering plan identification (octet 3)

4 3 2 1	
0 0 0 0	Unknown
0 0 0 1	ISDN/Telephony numbering plan (E.163/E.164)
1 0 0 1	Private numbering plan

All other values are reserved.

Presentation Indicator (octet 3a)

7 6	
0 0	Presentation allowed
0 1	Presentation restricted (default)
1 0	Number not available

All other values are reserved.

Screening indicator (octet 3a)

2 1	
0 0	User provided, not screened
0 1	User provided, verified and passed (Note)
1 0	User provided, verified and failed (Note)
1 1	Network provided (default)

Note: This value is treated by the network as “user provided, not screened”.

Original redirection reason (octet 3b)

4 3 2 1	
0 0 0 0	No reason supplied
0 0 0 1	Call forwarding busy
0 0 1 0	Call forwarding no reply
1 1 0 1	Call transfer
1 1 1 0	Call pickup
1 1 1 1	Call forwarding unconditional

All other values are reserved.

Redirection counter (octet 3c)

3 2 1	
0 0 0	Counter = 0 (default)
0 0 1	Counter = 1
0 1 0	Counter = 2
0 1 1	Counter = 3
1 0 0	Counter = 4
1 0 1	Counter = 5

All other values are reserved.

Call forwarding no reply undergone indicator (octet 3c)

7	
0	False (default)
1	True

Number digits (octet 4 ...n)

7 6 5	4 3 2 1	Address digit value
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
0 1 0	1 0 1 0	*
0 1 0	0 0 1 1	#

All other values are reserved.

4.5.22 Progress indicator

The *Progress indicator* information element is used to describe an event which has occurred during the life of a call.

The maximum length of the information element is 4 octets.

Figure 4-43
Progress information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
0	Progress indicator information element identifier							1
	0	0	1	1	1	1	0	
Length of information element								2
Ext. 1	Coding standard		Spare 0	Location				3
Ext. 1	Progress description							4

Coding standard (octet 3)

7	6	
0	0	CCITT standard

All other values are reserved.

Location (octet 3)

4	3	2	1	
0	0	0	0	User
0	0	0	1	Private network serving the local user
0	0	1	0	Public network serving the local user
0	0	1	1	Transit network
0	1	0	0	Public network serving the remote user
0	1	0	1	Private network serving the remote user

All other values are reserved.

> ***Note:*** The location code generated by the DMS-100 is datafillable. The allowable values are: user; private network serving the local user; and public network serving the local user. All valid location codes that are received are passed through to the terminating interface without alteration.

Progress description (octet 4)

7	6	5	4	3	2	1	Number	
0	0	0	0	0	0	1	1	Call is not end-to-end ISDN; further call progress information may be available in-band
0	0	0	1	0	0	0	8	In-band information or pattern is now available

All other values are reserved.

4.5.23 Reason for return

The purpose of the *Reason for return* information element is to identify the reason for not being able to route a connectionless *FACILITY* message to the destination. This information element is located in codeset 6.

The maximum length of the information element is 3 octets.

Figure 4-44
Reason for return information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
	Reason for return information element identifier							
0	0	0	0	1	0	0	1	1
Length of information element								2
Ext. 1	Diagnostic							3

Diagnostic (octet 3)

7 6 5	4 3 2 1	
0 0 0	0 0 0 1	No translation for address of such nature
0 0 0	0 0 1 0	No translation for this specific address
0 0 0	0 0 1 1	Application congestion
0 0 0	0 1 0 0	Application failure
0 0 0	0 1 0 1	Unequipped application
0 0 0	0 1 1 0	Network failure
0 0 0	0 1 1 1	Network congestion
0 0 0	1 0 0 0	
to		Spare
1 1 1	1 1 1 1	

4.5.24 Redirection number

The purpose of the *Redirection number* information element is to identify the number to which call redirection or diversion should be or has been invoked.

The maximum length of the information element is 17 octets.

Figure 4-45
Redirection number information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
	Redirection number information element identifier							1
0	1	1	1	0	1	1	0	
Length of information element								2
Ext.	Type of number			Numbering plan identification				3
0/1								
Ext.	Presentation indicator		Spare			Screening indicator		3a*
0/1			0	0	0			
Ext.	Spare			Reason for redirection				3b*
0/1	0	0	0					
Spare	Number digits (IA5 characters)							4 ... n
0								

Note: The contents of this information element, other than octet 3b, are coded as shown for the *Calling party number* information element in section 4.5.8 on page 4-59.

Reason for Redirection (octet 3b)

4	3	2	1	
0	0	0	1	Call forwarding busy
0	0	1	0	Call forwarding no reply
1	1	0	1	Call transfer
1	1	1	0	Call pickup
1	1	1	1	Call forwarding unconditional

All other values are reserved.

4.5.25 Restart indicator

The purpose of the *Restart indicator* information element is to identify the class of the facility (that is, channel or all interfaces) to be restarted.

Figure 4-46
Restart indicator information element

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th><th>Octet</th></tr>
<tr><td rowspan="2">0</td><td colspan="7">Restart indicator information element identifier</td><td rowspan="2">1</td></tr>
<tr><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Length of information element</td><td>2</td></tr>
<tr><td>Ext.</td><td colspan="4">Spare</td><td colspan="3" rowspan="2">Class</td><td rowspan="2">3</td></tr>
<tr><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
</table>

Class (octet 3)

3	2	1	
0	0	0	Indicated channel (see Note)
1	1	1	All channels associated with the D-channel

All other values are reserved.

Note: The *Channel identification* information element must be included and indicates which channel is to be restarted.

4.5.26 Transit network selection

The purpose of the *Transit network selection* information element is to identify the requested transit network. This information element should not be included in a *SETUP* message when a *Network-specific facilities* information element is present or the presubscribed carrier is to be used.

The maximum length of the information element is 7 octets.

Figure 4-47
Transit network selection information element

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
0	Transit network selection information element identifier							1
	1	1	1	1	0	0	0	
Length of information element								2
Ext. 1	Type of network identification			Network identification plan				3
Spare 0	Network identification (IA5 characters)							4 ... n

Type of Network identification (octet 3)

7 6 5	
0 0 0	User specified
0 1 0	National network identification

All other values are reserved.

Network identification Plan (octet 3)

4 3 2 1	
0 0 0 0	Unknown
0 0 0 1	Carrier identification code
0 0 1 0	User specific

All other values are reserved.

Network Identification Characters (octet 4)

These IA5 characters are organized according to the network identification plan specified in octet 3.

Chapter 4-5: Layer 3 call control procedures

This chapter describes the procedures that define the flow of messages across a primary rate interface between an ISDN user and the network. The call states referred to in this chapter refer to

- states seen by the network
- states seen by the user
- states which are common to both user and network

Unless noted, all states described in the following text should be understood as common. (See section 2.1.1 on page 4-8 for user and network call states.)

Detailed Specification and Description Language (SDL) diagrams for the procedures specified in this section are contained in Annex A. If there is an ambiguity in the narrative text, the SDL diagrams should be used to resolve the conflict. If the text and SDL are in disagreement, the text should be considered correct.

> ***Note:*** This chapter describes the sequence of messages associated with the control of circuit-switched connections. Annex D contains optional extensions to the user-side procedures for symmetric call-control signaling.

Before these procedures are invoked, Layer 3 must be established on an active D-channel (see Chapter 4-7: D-channel maintenance). All Layer 3 messages are sent to the data link layer using a *DL-Data-Request* primitive. The data link services described in the Layer 2 procedures (Section 3 of this specification) are assumed.

The *Call reference* information element contained in all messages exchanged across the user-network interface contains the call reference value specified in the *SETUP* message delivered by the network. In selecting a call reference, the dummy (null) call reference is not used.

5.1 Call establishment at the originating interface

5.1.1 Call request procedure

A user initiates call establishment by transferring a *SETUP* message across the user-network interface.

Following the transmission of the *SETUP* message, the call is considered by the user to be in the *Call initiated* state. The message always contains a *Call reference* information element, selected according to the procedures given in section 4.3 on page 4-38. In selecting a call reference, the dummy call reference value is not used. The *Bearer capability, Channel identification* and *Called party number* information elements are mandatory in the *SETUP* message.

If the user knows all appropriate channels controlled by the D-channel are in use, it does not send a *SETUP* message across the user-network interface. If the user does not monitor the status of the channels in use, it may send a *SETUP* message when all channels are busy.

The *SETUP* message contains all of the call information necessary for call establishment.

5.1.2 B-channel selection — originating

In the *SETUP* message, the user indicates one of the following using the *Channel identification* information element

- channel is indicated, no acceptable alternative
- channel is indicated, any alternative is acceptable

If no *Channel identification* information element is included, the procedures in section 5.9.6.1 on page 4-138 for a missing mandatory information element are followed. In both cases, if the indicated channel is available, the network selects it for the call.

The selected B-channel is indicated in the first message returned by the network in response to the *SETUP* message (that is, a *CALL PROCEEDING* message). After transmitting this message, the network activates the selected B-channel connection.

The user need not attach until it receives a *CALL PROCEEDING*, *PROGRESS*, or *ALERTING* message with a *Progress indicator* information element with one of the following *Progress description* values:

- #1 “Call is not end-to-end ISDN; further call progress information may be available in-band”
- #8 “Inband information or appropriate pattern is now available”

Prior to this time, the network does not assume that the user has attached to the B-channel. After this time, the user is connected to the B-channel, provided the equipment does not generate local tones. Upon receipt of the *CONNECT* message, the user attaches to the B-channel (if it has not already done so).

If the specified B-channel is not available, the network

- sends a *RELEASE COMPLETE* message with *Cause* value #44 “Requested circuit/channel not available”
- enters the *Null* state

Reasons for B-channel non-availability include another call isallocated to the same B-channel or the B-channel is out of service (see Chapter 4-8: B-channel maintenance).

5.1.3 Invalid call information

If, following the receipt of the *SETUP* message, the network determines that the call information received from the user is invalid (for example, an invalid number is sent), the network initiates call clearing in accordance with section 5.3 on page 4-122. The *Cause* value returned is one of the following:

- #1 “Unallocated (unassigned) number”
- #3 “No route to destination”
- #22 “Number changed”
- #28 “Invalid number format (address incomplete)”

5.1.4 Call proceeding

If the network determines that the *SETUP* message contains all the information required from the user to establish the call and that access to the requested service is authorized and available, the network:

- sends a *CALL PROCEEDING* message to the user to acknowledge the *SETUP* message and to indicate that the call is being processed
- enters the *Outgoing call proceeding* state

When the user receives the *CALL PROCEEDING* message, the user also enters the *Outgoing call proceeding* state.

If the network determines that a requested service is not authorized or is not available, the network initiates call clearing in accordance with section 5.3 on page 4-122. The network returns one of the following *Cause* values:

- #34 “No circuit/channel available”
- #57 “Bearer capability not authorized”
- #58 “Bearer capability not presently available”

- #63 “Service or option not available, unspecified”
- #65 “Bearer capability not implemented”

5.1.5 Notification of interworking at the originating interface

During call establishment, the call may leave the ISDN environment (for example, because of interworking with non-ISDN facilities). When this situation occurs, a *Progress indicator* information element is returned to the calling user in the *PROGRESS* message:

The *Progress indicator* information element in the message sent to the user has *Progress description* value #1 “Call is not end-to-end ISDN; further call progress information may be available in-band”.

On receipt of the *Progress indicator* information element in the *PROGRESS* message, the calling user does not change state, but any supervisory timers are stopped. The user connects to (if not connected already) and then monitors the B-channel for further in-band information.

If the interface at which the *Progress indicator* originates is where the call enters the ISDN environment from a non-ISDN environment, any *SETUP* message sent to the network includes a *Progress indicator* information with *Progress description* value #1 “Call is not end-to-end ISDN ; further call progress information may be available in-band”.

5.1.6 Call confirmation indication

Upon receiving an indication that user alerting has been initiated at the called address, the network

- sends an *ALERTING* message across the user-network interface to the calling user
- enters the *Call delivered* state

The *ALERTING* message contains a *Progress indicator* information element with *Progress description* value #8 “In-band information or appropriate pattern is now available” if the bearer capability is “speech” or “3.1 kHz Audio”. When the user receives the *ALERTING* message, it enters the *Call delivered* state.

5.1.7 Call connected

Upon receiving an indication that the call has been accepted, the network

- sends a *CONNECT* message across the user-network interface to the calling user
- enters the *Active* state

The *CONNECT* message indicates to the calling user that a connection has been established through the network.

On receipt of the *CONNECT* message, the calling user

- (optionally) sends a *CONNECT ACKNOWLEDGE* message
- enters the *Active* state

The network takes no action on receipt of a *CONNECT ACKNOWLEDGE* message if the call is in the *Active* state.

5.1.8 Call rejection

Upon receiving an indication that the network or the called user is unable to accept the call, the network initiates clearing at the originating user-network interface as described in section 5.3 on page 4-122 using the cause value provided by the terminating network or the called user.

5.1.9 Transit network selection

When the *Transit network selection* information element is present, the call is processed according to Annex C.

5.2 Call establishment at the destination interface

5.2.1 Network response to an incoming call

The network indicates the arrival of a call at the user-network interface by transferring a *SETUP* message across the interface. This message is sent if the network can select an idle B-channel.

In addition to the mandatory information elements, the *SETUP* message may include any of the optional information elements described in section 3.1.10 on page 4-24.

After sending the *SETUP* message, the network

- starts timer T303
- enters the *Call present* state

The *SETUP* message contains all the information required by the called user to process the call. Upon receipt of a *SETUP* message, the user enters the *Call present* state.

If no response to the *SETUP* message is received by the network before the first expiry of timer T303

- the *network retransmits the SETUP* message
- timer T303 is restarted

5.2.2 Compatibility checking

A user receiving a *SETUP* message performs compatibility checking before responding to the *SETUP* message. Any reference to “user” in this chapter implicitly refers to compatible user equipment. Annex B defines compatibility checking to be performed by users upon receiving a *SETUP* message.

An incompatible user responds to the *SETUP* message as follows

- sends to the network a *RELEASE COMPLETE* message with *Cause* value #88 “Incompatible destination”
- enters the *Null* state

The network processes the *RELEASE COMPLETE* message as described in section 5.2.4.3 on page 4-119.

5.2.3 B-channel selection — destination

In the *SETUP* message, the network indicates the B-channel to be used, with no acceptable alternative, for the call. If the indicated channel is acceptable, the user equipment selects it for the call.

If the B-channel indicated in the first response message is not the channel offered by the network, the network clears the call by sending a *RELEASE* message with *Cause* value #6 “Channel unacceptable” (see section 5.3.2 on page 4-122).

When a B-channel has been accepted by the user, that channel may be connected to by the user.

If the indicated B-channel is not available, the user

- sends a *RELEASE COMPLETE* message with *Cause* value #44 “Requested circuit/channel not available”
- enters the *Null* state

Reasons for B-channel non-availability include another call isallocated to the same B-channel or the B-channel is out of service (see Chapter 4-8: B-channel maintenance).

5.2.4 Call confirmation

5.2.4.1 Response to *Setup*

When the user determines that sufficient call setup information has been received and compatibility requirements (see Annex B) have been satisfied, the user responds with a *CALL PROCEEDING,* an *ALERTING*, or a *CONNECT* message. It enters the *Incoming call proceeding, Call received,* or *Connect request* state, respectively.

> ***Note:*** The *CALL PROCEEDING* message may be sent by a user that does not respond to a *SETUP* message with an *ALERTING, CONNECT,* or *RELEASE COMPLETE* message before expiration of timer T303.

An incompatible user responds by

- sending a *RELEASE COMPLETE* message with *Cause* value #88 “Incompatible destination”
- entering the *Null* state

The network processes this *RELEASE COMPLETE* message in accordance with the procedures described in section 5.2.4.3 on page 4-119.

A busy user that satisfies the compatibility requirements indicated in the *SETUP* message normally responds with a *RELEASE COMPLETE* message with *Cause* value #17 “User busy”. The network processes this *RELEASE COMPLETE* message in accordance with the procedures described in section 5.2.4.3 on page 4-119.

If the user chooses to refuse the call, it

- sends a *RELEASE COMPLETE* message with the *Cause* value #21 “Call rejected”
- enters the *Null* state

The network processes this *RELEASE COMPLETE* message in accordance with the procedures described in section 5.2.4.3 on page 4-119.

5.2.4.2 Receipt of *Call proceeding* and *Alerting*

Upon receipt of the *CALL PROCEEDING* message from a user, the network

- stops timer T303
- starts timer T310
- enters the *Incoming call proceeding* state

Upon receipt of the *ALERTING* message from a user, the network

- stop timers T303 or T310 (if running)
- starts timer T301
- enters the *Call received* state
- sends a corresponding *ALERTING* message to the calling user

If the received *ALERTING* message is the first response to the *SETUP* message it contains the *Channel identification* information element.

5.2.4.3 Called user clearing during incoming call establishment

If a *RELEASE COMPLETE* or *DISCONNECT* message is received before a *CONNECT* message, the network

- stops timer T301, T303 or T310 (if running)

- continues to clear the user as described in section 5.3.3 on page 4-122
- clears the call to the calling user with the *Cause* value received in the *RELEASE COMPLETE* or *DISCONNECT* message

5.2.4.4 Call failure

If the network does not receive any response to the retransmitted *SETUP* message prior to the expiration of timer T303, the network

- initiates clearing procedures towards the calling user with *Cause* value #18 “No user responding”
- initiates clearing procedures towards the called user in accordance with the procedures defined in section 5.3.4 on page 4-125 using *Cause* value #102 “Recovery on timer expiry”.

If the network has received a *CALL PROCEEDING* message, but does not receive an *ALERTING*, *CONNECT*, or *DISCONNECT* message prior to the expiration of timer T310, the network

- initiates clearing procedures toward the calling user with *Cause* value #18 “No user responding”
- initiates clearing procedures towards the called user in accordance with the procedures defined in section 5.3.4 on page 4-125 using *Cause* value #102 “Recovery on timer expiry”

If the network receives an *ALERTING* message, but does not receive a *CONNECT* or *DISCONNECT* message prior to the expiration of timer T301, the network

- initiates clearing procedures toward the calling user with *Cause* value #19 “No answer from user (user alerted)”
- initiates clearing procedures towards the called user in accordance with the procedures defined in section 5.3.4 on page 4-125 using *Cause* value #102 “Recovery on timer expiry”

5.2.5 Notification of interworking at the terminating interface

During call establishment, a call may enter a non-ISDN environment because, for example

- the ISDN network is interworking with another network
- the call may be from or to a non-ISDN user

When this occurs, the point at which the call enters the non-ISDN environment causes a *Progress indicator* information element to be included in the *SETUP* message that is sent to the called user. The information element has *Progress description* value #1 “Call is not end-to-end ISDN; further call progress information may be available inband”.

On receipt of *Progress indicator* information element with *Progress description* value #1, the called user connects to the B-channel in accordance with the procedures defined in section 5.2.7 on page 4-121.

In addition, the called user notifies the calling party if the call has left the ISDN environment within the called user's premises and the possible availability of in-band call progress information. When such situations occur, a *Progress indication* information element is sent by the user to the network in the *PROGRESS* message. The *Progress indicator* information element contains the *Cause* value #1 "Call is not end-to-end ISDN; further call progress information may be available in-band".

On receipt of the *Progress indicator* information element in a *PROGRESS* message, the network does not change state but any supervisory timers are stopped.

5.2.6 Call accept

A user indicates acceptance of an incoming call by sending a *CONNECT* message to the network. When the *CONNECT* message is sent, the user starts timer T313 (the value of timer T313 is specified in Table 3-40 on page 4-164). If an *ALERTING* message has previously been sent to the network, the *CONNECT* message may contain only the *Call reference* information element.

If a call can be accepted using the B-channel indicated in the *SETUP* message, and no user alerting is required, a *CONNECT* message may be sent without a previous *ALERTING* message. If the *CONNECT* message is the first response to the *SETUP* message, it contains the *Channel identification* information element.

5.2.7 Active indication

On receipt of the first *CONNECT* message, the network

- stops timers T301, T303 and T310 (if running)
- completes the circuit-switched path to the selected B-channel
- sends a *CONNECT ACKNOWLEDGE* message to the user
- initiates procedures to send a *CONNECT* message towards the calling user
- enters the *Active* state

The *CONNECT ACKNOWLEDGE* message indicates completion of the circuit-switched connection. There is no guarantee of an end-to-end connection until a *CONNECT* message is received at the calling user interface.

Upon receipt of the *CONNECT ACKNOWLEDGE* message, the called user:

- stops timer T313

- enters the *Active* state

If timer T313 expires prior to receipt of a *CONNECT ACKNOWLEDGE* message, the called user initiates clearing toward the network in accordance with the procedures defined in section 5.3.3 on page 4-122 with cause #102 “Recovery on timer expiry”.

A user that has received the *SETUP* message may connect to the B-channel as soon as channel selection has been completed.

5.3 Call clearing

5.3.1 Terminology

The following terms are used in the description of the clearing procedures:

- A channel is *connected* when the channel is part of a circuit-switched ISDN connection established according to this specification.
- A channel is *disconnected* when the channel is no longer part of a circuit-switched ISDN connection, but is not yet available for use in a new connection.
- A channel is *released* when the channel is not part of a circuit-switched ISDN connection and is available for use in a new connection. Similarly, a call reference that is *released* is available for reuse.

5.3.2 Exception conditions

Under normal conditions, call clearing is usually initiated when the user or the network sends a *DISCONNECT* message and follows the procedures defined in section 5.3.3 on page 4-122 or section 5.3.4 on page 4-125, respectively. The only exceptions to this rule are as follows:

- In response to a *SETUP* message, the user or network can reject a call (for example, 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
- Unsuccessful termination of the B-channel selection procedure (see section 5.2.3 on page 4-118 and section 5.1.2 on page 4-114) by the side offering the call. The call is cleared by sending a *RELEASE* message as described in section 5.3.3 on page 4-122 and section 5.3.4 on page 4-125. The *RELEASE* message includes *Cause* value #6 “Channel unacceptable”.

5.3.3 Clearing initiated by the user

Apart from the exception conditions identified in section 5.3.2 on page 4-122 and section 5.9 on page 4-134, the user initiates clearing by

- sending a *DISCONNECT* message

- starting timer T305 (the value of timer T305 is specified in Table 3-40 on page 4-164)
- disconnecting the B-channel
- entering the *Disconect request* state

> ***Note:*** When a user initiates call clearing by sending a *RELEASE* message, the procedures described in section 5.3.4 on page 4-125 are followed.

When the network receives a *DISCONNECT* message from the user, it

- enters the *Disconnect request* state
- disconnects the B-channel and to initiate procedures for clearing the network connection to the remote user

When the B-channel used for the call has been disconnected, the network

- sends a *RELEASE* message to the user
- starts timer T308 (the value of timer T308 is specified in)
- enters the *Release request* state

> ***Note:*** The *RELEASE* message has only local significance and does not imply an acknowledgement of clearing from the remote user.

On receipt of the *RELEASE* message, the user

- cancels timer T305
- releases the B-channel
- sends a *RELEASE COMPLETE* message
- releases the call reference
- enters the *Null* state

Following the receipt of a *RELEASE COMPLETE* message from the user, the network

- stops timer T308
- releases both the B-channel and the call reference
- enters the *Null* state

If a *RELEASE COMPLETE* message is not received by the network before the first expiry of timer T308, the *RELEASE* message is retransmitted and timer T308 is restarted. If no *RELEASE COMPLETE* message is received from the user before T308 expires a second time, the network

- places the B-channel in a maintenance state
- releases the call reference
- enters the *Null* state

If timer T305 expires, the user

- sends a *RELEASE* message to the network with the cause number originally contained in the *DISCONNECT* message
- starts timer T308
- enters the *Release request* state

The user may include in the *RELEASE* message a second *Cause* information element with *Cause* value #102 “Recovery on timer expiry”.

If user timer T308 expires for the first time, the user

- retransmits the *RELEASE* message
- restarts timer T308

The user may include in the *RELEASE* message a second *Cause* information element with the *Cause* value #102 “Recovery on timer expiry”.

If no *RELEASE COMPLETE* message is received from the network before timer T308 expires a second time, the user

- may place the B-channel in a maintenance state
- releases the call reference
- enters the *Null* state

> ***Note:*** The restart procedures contained in section 5.7 on page 4-132 may be used on B-channels in the maintenance state.

5.3.3.1 Cause Screening

When an initial call clearing message is received by the terminating interface with a cause other than the ones which result in a reroute attempt or inband treatment, the terminating interface normally sends a clearing message to the originating interface with the cause received. However cause values that only have significance locally are mapped to a more generalized one for the DMS-100 platform. Table 3-38 on page 4-125 shows the causes that are affected.

When one of these causes is received at the terminating interface, cause #41, “temporary failure”, is substituted.

Table 3-38 Cause screening table

Received cause
6. Channel unacceptable
30. Response to status enquiry
45. Preempt[a]
81. Invalid call reference value
82. Identified channel does not exist[b]
90. Destination address missing
95. Invalid message unspecified
96. Mandatory information element is missing
97. Message type nonexistent or not implemented
99. Information element nonexistent or not implemented
100. Invalid information element contents
101. Message not compatible with state
102. Recovery on timer expiry
111. Protocol error, unspecified

[a] This cause is screened for PRI trunks that are **not** AUTOVON agents.

[b] screening is done ONLY if the remote interface (remote interface refers to the PRI trunk connected to the other end of the terminating interface) is NOT controlled by an MSL-1 PBX.

5.3.4 Clearing initiated by the network

Apart from the exceptions identified in section 5.3.2 on page 4-122 and section 5.9 on page 4-134, the network initiates clearing by

- sending a *DISCONNECT* message
- entering the *Disconnect indication* state

When the network initiates clearing by sending a *RELEASE* message, the procedures in section 5.3.3 on page 4-122 are followed.

5.3.4.1 Clearing when tones or announcements provided

When tones or announcements are provided in conjunction with call clearing, the network sends a *PROGRESS message* (see section 5.4 on page 4-129).

If a call originating on a PRI trunk cannot be completed, a clearing message, containing an appropriate cause, is generally sent back to the calling interface. In some cases, however, an inband treatment (a tone or an announcement) may be preferable, instead of immediately clearing the call.

Inband treatment procedures apply only for originating PRI calls with a bearer capability (BC) of speech or 3.1-kHz audio. Inband treatment is available when normally, a DISCONNECT or RELEASE COMPLETE message containing either cause #1, “unallocated (unassigned) number”,or cause #27, “destination out of order”, would be sent to the calling interface. Inband treatment can also be applied if the terminating interface receives a call clearing message containing cause #1, “unallocated (unassigned) number”.

Subscribing to this option enables inband treatment procedures for originating PRI calls with a bearer capability (BC) of speech or 3.1-kHz audio for the following scenarios:

- The call attempt results in a DMS treatment of VACT (vacant code), UNDN (unassigned number), or BLDN (blank directory number). (Normally, a DISCONNECT or RELEASE COMPLETE message containing cause #1, “unallocated (unassigned) number”, would be sent to the calling interface.)
- The terminating interface receives a call clearing message containing cause #1, “unallocated (unassigned) number”.
- The call attempt results in a DMS treatment of TRBL (trouble intercept). (Normally, a DISCONNECT or RELEASE COMPLETE message containing cause #27, “destination out of order”, would be sent to the calling interface.)

For these cases, when inband treatment is subscribed to, the originating interface will send the calling interface a PROGRESS message containing progress indicator #8, and either cause #1 or cause #27 (as appropriate), and a tone or an announcement will be supplied over the allocated b-channel.

5.3.4.2 Clearing when tones or announcements not provided

When tones or announcements are not provided, the network initiates clearing by

- sending a *DISCONNECT* message
- starting timer T305
- disconnecting the B-channel

- entering the *Disconnect indication* state

On receipt of the *DISCONNECT* message the user

- disconnects the B-channel
- sends a *RELEASE* message
- starts timer T308
- enters the *Release request* state

On receipt of the *RELEASE* message, the network

- stops timer T305
- releases the B-channel
- sends a *RELEASE COMPLETE* message
- releases the call reference
- enters the *Null* state

If timer T305 expires, the network

- sends a *RELEASE* message to the user with the *Cause* value originally contained in the *DISCONNECT* message
- starts timer T308
- enters the *Release request* state

5.3.4.3 Completion of clearing

Following the receipt of a *RELEASE COMPLETE* message from the user, the network

- stops timer T308
- releases both the B-channel and the call reference
- enters the *Null* state

If a *RELEASE COMPLETE* message is *not* received by the network before the first expiry of timer T308, the network

- retransmits the *RELEASE* message
- restarts timer T308

If no *RELEASE COMPLETE* message is received from the user before timer T308 expires a second time, the network

- places the B-channel in a maintenance state
- releases the call reference

- enters the *Null* state

If a *RELEASE COMPLETE* message is not received by the user before the first expiry of timer T308, the user

- retransmits the *RELEASE* message
- restarts timer T308

The user may include in the *RELEASE* message a second *Cause* information element with the *Cause* value #102 “Recovery on timer expiry”.

If a *RELEASE COMPLETE* message is not received from the network before T308 expires a second time, the user

- may place the B-channel in a maintenance state
- releases the call reference
- enters the *Null* state

  Note: The restart procedures contained in section 5.7 on page 4-132 may be used on B-channels in the maintenance state.

5.3.5 Clear collision

Clear collision occurs when both the user and the network simultaneously transfer *DISCONNECT* messages specifying the same call reference value. When the network receives a *DISCONNECT* message while in the *Disconnect indication* state, the network

- stops timer T305
- sends a *RELEASE* message
- starts timer T308
- enters the *Release request* state.

Similarly, when the user receives a *DISCONNECT* message while in the *Disconnect request* state, the user

- stops timer T305
- disconnects the B-channel (if not disconnected)
- sends a *RELEASE* message
- starts timer T308
- enters the *Release request* state

Clear collision can also occur when both sides simultaneously transfer *RELEASE* messages related to the same call reference value. The entity receiving such a *RELEASE* message while within the *Release request* state

- stops timer T308
- releases the call reference and B-channel, if appropriate
- enters the *Null* state (without sending or receiving a *RELEASE COMPLETE* message)

5.4 In-band tones and announcements

Inband treatment procedures apply only for PRI calls with a bearer capability (BC) of speech or 3.1-kHz audio. When in-band tones or announcements not associated with a call state change are to be provided before reaching the *Active* state, a *PROGRESS message* is returned with the application of the in-band tone or announcement. The *PROGRESS* message contains the *Progress indicator* information element with *Progress description* value #8 “In-band information or appropriate pattern now available”.

> ***Note:*** When the *PROGRESS message* is used, the user may initiate call clearing as a result of the applied in-band tone or announcement, according to procedures in section 5.3.3 on page 4-122.

5.5 Interworking with existing networks

Although the method of functional out-of-band signaling is unique to ISDN facilities, it is essential to preserve the same human interface for calls that are routed over these facilities, and to allow for interworking with non-ISDN interfaces. Methods for providing audible ringback, user busy tones, and announcements are essential to preserving the traditional human interface for telephony calls.

These procedures identify the agent responsible for generating in-band busy and audible ringback tones. The agent generates the tones for calls that are within an ISDN network as well as calls between ISDN and non-ISDN networks.

Three call scenarios are considered:

- The call has been delivered successfully to the terminating user, who is being alerted.
- The call is unsuccessful because the terminating user is busy.
- The call requires that network-provided tones or announcements be sent to the calling user.

In addition, three types of network connections need to be considered

- Type 1, within ISDN

- Type 2, from non-ISDN to ISDN
- Type 3, from ISDN to non-ISDN

For these procedures, the non-ISDN network provides tones and announcements as currently implemented regardless of the network connection and call scenario. An ISDN exchange acts independently of the three network connections, that is, it is independent of the possible existence and character of interworking.

The terms *originating exchange* and *terminating exchange* are used in the following description to refer to equipment such as private branch exchanges (PBXs) or central offices (COs) that are closest to the respective end users. An intermediate exchange is a PBX or CO situated between the originating and terminating exchanges.

5.5.1 Generation of audible ringback tones

The terminating exchange (either ISDN or non-ISDN) is responsible for the generation of audible ringback tones for all three types of network connections, as described above.

Calls terminating on ISDN facilities

This section describes procedures for calls involving network connections that remain in the ISDN network (Type 1) or are from non-ISDN networks but terminate on an ISDN network (Type 2).

In order to remain consistent with the pre-ISDN implementation, audible ringback tone is provided by the terminating exchange.

For Type 1 connections, audible ringback is generated by the terminating exchange.

For Type 2 connections, the following procedure is performed

- the terminating exchange determines it is a type 2 call by the presence of the *Progress indicator* information element in the *SETUP* message, having *Progress description* value #1 “Call is not end-to-end ISDN ; further call progress information may be available in-band”.
- if the call proceeds through the network and successfully reaches the terminating exchange, the terminating exchange
  - determines if the endpoint terminal is available
  - if so, alerts the end-user terminal, propagates the alerting indicator back to the originating exchange and provides in-band audible ringback tone
  - when the terminal at the terminating exchange answers the call by sending a *CONNECT* message (or equivalent “off-hook”

indication) audible ringback is removed, and the *CONNECT* message is propagated back towards the originating exchange

ISDN to non-ISDN calls

For Type 3 connections, interworking occurs at the interworking exchange. When the interworking condition is detected, it is the responsibility of the interworking exchange to send a *PROGRESS message* towards the originating side of the interface. The *PROGRESS message* contains the *Progress indicator* information element having *Progress description* value #1 “Call is not end-to-end ISDN; further call progress information may be available in-band”.

The *PROGRESS* message indicates that the call has left the ISDN network and that audible ringback is provided in-band from the terminating exchange. Further, the interworking exchange monitors the outgoing non-ISDN trunking facilities for answer and disconnect supervision. These conditions, upon detection, are translated into *CONNECT* or *DISCONNECT* messages, respectively, for the ISDN side of the call.

5.5.2 Generation of busy tones

In-band busy tones are generated as close as possible to the calling user, allowing network resources used to reach the terminating exchange to be released. In the case of some features, for example Call Completion with Trunk Optimization (CCTO), the point closest to the calling user, at which busy tones may be applied, may not be the originating exchange. The user can subscribe to have the network provide busy tone as a subscription option.

ISDN to ISDN (Type 1 network connection)

Upon notification that the called user is busy, the terminating exchange sends a *DISCONNECT* message with *Cause* value #17 “User busy” towards the originating side. In response to this message, the originating exchange disconnects the B-channel and generates the in-band busy tone locally.

Non-ISDN to ISDN (Type 2 network connection)

As above, upon notification that the called user is busy, the terminating exchange sends a *DISCONNECT* message with cause #17, “User busy” towards the originating side. In response to this message, the interworking exchange generates the in-band busy tone towards the originating user.

ISDN to non-ISDN (Type 3 network connection)

For a Type 3 connection, the busy tone is generated by the terminating exchange. A *PROGRESS message* with *Progress indicator* information element containing *Progress description* value #1 is sent towards the originating user by the interworking exchange indicating that the call is not end-to-end ISDN and that call progress information is only available in-band.

5.5.3 Announcements

Calls within an ISDN may still have treatment applied, involving in-band information, for example, tones or voice announcements.

The cut-through procedures ensure that in-band tones will be heard by users, if provided. Therefore, the network or user may insert in-band tones or announcements before reaching the *Active* state, after sending a *PROGRESS* message.

5.6 Channel cut-through procedures

Originating and intermediate switches connect to the agreed upon information channel upon successful B-channel selection. The terminating switch connects to the agreed upon information channel upon receipt of an “off-hook” indication (that is, equivalent to the *CONNECT* message) from the terminating user.

The definitions of originating, intermediate, and terminating exchanges are as defined in section 5.5 on page 4-129.

5.7 Restart procedure

The restart procedure is used to return channels and interfaces to an idle condition. The procedure is invoked

- after a data link reset following a data link failure (that is, after expiry of timer T309) — all interfaces restart
- following expiry of timer T308 for a second time, caused by the absence of a response to the *RELEASE* message — single interface restart
- on data link establishment at time of system initialization — all interfaces restart

- when adding or returning B channels to service from a Maintainance or Out of Service State

5.7.1 Sending Restart

A *RESTART* message is sent by the network or user to return one channel or all interfaces to the *Null* state. The *Channel identification* information element must be present in the *RESTART* message when a specified channel is returned to the idle condition.

After transmitting the *RESTART* message, the sender

- starts timer T316
- enters the *Restart request* state

When the *RESTART ACKNOWLEDGE* message is received by the sender of the *RESTART* message, which specifies the corresponding channel or all interfaces

- timer T316 is stopped (this frees the channels and call reference values for reuse)
- enters the *Null* state

If a *RESTART ACKNOWLEDGE* message is not received prior to the expiry of timer T316, one or more *RESTART* messages are periodically sent until a *RESTART ACKNOWLEDGE* message is returned. Until a valid response is received, no calls are allowed on the specified channel or interfaces by the originator of the *RESTART* message.

After two unsuccessful restart attempts, an indication will be provided to the appropriate maintenance entity. The channel or interface is considered to be in an out-of-service condition until maintenance action has been taken. Further restart attempts may be made.

The *RESTART* and *RESTART ACKNOWLEDGE* messages contain the global call reference value (see section 4.3 on page 4-38) with which the *Restart request* state is associated. These messages are transferred using the *DL-Data-Request* primitive.

5.7.2 Receipt of Restart

After receiving a *RESTART* message, the recipient

- enters the *Restart* state
- initiates the appropriate internal actions to return the specified channel or interfaces to the idle condition, and calls to the *Null* state
- after completion of internal clearing, a *RESTART ACKNOWLEDGE* message is transmitted to the originator, specifying the same channel or all interfaces as received in the *RESTART* message
- enters the *Null* state

> ***Note1:*** Even if all calls are in the *Null* state and all channels are in the idle condition, the receiving entity transmits a *RESTART ACKNOWLEDGE* message to the originator of the *RESTART* message.
>
> ***Note2:*** Restart Acknowledge is not sent to the originator after receiving the global restart message with restart indicator set to 7 (all channels associated with D channel) in the call states N12, and N19.

If the network receives a restart message with restart indicator IE set to 0 (meaning the channel to be restarted is indicated in the channel identification

IE) and the channel identification IE does not have the channel number to restart, then the message is ignored and no action is taken.

An unsolicited Restart Acknowledge message is discarded by the recipient(in order to keep up existing calls).

5.8 Call collisions

Call collisions cannot occur in the network. Any simultaneous incoming or outgoing calls are managed separately and are assigned different call references.

Channel selection conflicts may occur if an incoming call and outgoing call select the same channel. This is resolved by the network through the channel selection mechanisms described in section 5.1.2 on page 4-114 and section 5.2.3 on page 4-118.

In such conflicts, the network gives priority to the incoming call over the outgoing call request received from the user.

The network clears the outgoing call if the B-channel cannot be

- allocated by the network
- accepted by the user originating the call

5.9 Handling of error conditions

All procedures transferring signaling information by using the protocol discriminator of “Q.931 user-network call control messages” are applicable only to those messages which pass the checks described in section 5.9.1 on page 4-134 through section 5.9.7 on page 4-139.

Errors found in messages using the maintenance protocol discriminator, described in section 4.2 on page 4-38, cause the message to be ignored, that is, as if the message had never been received.

The network establishes a threshold for the number of messages which are either unrecognized, not expected or discarded per call. The network releases calls if the threshold of eight is exceeded, according to the procedures of section 5.3.4 on page 4-125 using *Cause* #111 “protocol error, unspecified”.

The procedures in section 5.9.1 on page 4-134 through section 5.9.7 on page 4-139 are listed in order of precedence.

5.9.1 Protocol discrimination error

When a message is received with a protocol discriminator coded other than “Q.931 user-network call control message” or “Maintenance messages”, that message is ignored.

5.9.2 Message too short error

When a message is received that is too short to contain a complete *Message type* information element, that message is ignored.

5.9.3 Call reference error

5.9.3.1 Invalid call reference format

In the *Call reference* information element, if octet 1, bits 5 through 8 are not set to "0000", the message is ignored.

In the *Call reference* information element, if octet 1, bits 1 through 4 indicate a length greater than the maximum length supported by the receiving equipment, the message is ignored. (See section 4.3 on page 4-38 for further details.)

5.9.3.2 Call reference procedural errors

- Whenever any message except *SETUP*, *RELEASE COMPLETE*, *STATUS*, or *STATUS ENQUIRY* is received specifying a call reference which is not recognized as relating to an active call or to a call in progress, the receiver initiates clearing. Clearing is initiated by sending a *RELEASE COMPLETE* message with *Cause* value #81 "Invalid call reference value". This message specifies the call reference value of the received message. The receiver remains in the *Null* state.
- When a *RELEASE COMPLETE* message is received specifying a call reference value which is not recognized as relating to an active call or to a call in progress, no action is taken.
- When a *SETUP* message is received specifying a call reference value which is not recognized as relating to an active call or to a call in progress, and with a call reference flag incorrectly set to "1", the message is ignored.
- When a *SETUP* message is received specifying a call reference value which is recognized as relating to an active call or to a call in progress, this message is ignored.
- When any message except *RESTART*, *RESTART ACKNOWLEDGE* or *STATUS* is received using the global call reference, no action is taken. A *STATUS* message using the global call reference with a call state indicating the current state associated with the global call reference and a *Cause* value #81 "Invalid call reference value" is returned.
- When a *STATUS* message is received specifying a call reference value which is not recognized as relating to an active call or to a call in progress, the procedures in section 5.9.11 on page 4-143 are followed.
- When a *STATUS ENQUIRY* message is received specifying a call reference value which is not recognized as relating to an active call or to a call in progress, a *STATUS* message is returned indicating the *Null* call state with *Cause* value #30 "Response to Status enquiry".

5.9.4 Message type or message sequence errors

Whenever an unexpected message, except *RELEASE*, *RELEASE COMPLETE*, *CONNECT_ACK* or an unrecognized message is received in any state other than the *Null* state, a *STATUS* message is returned with one of the following *Cause* values

- #97 “Message type non-existent or not implemented”
- #101 “Message not compatible with call state”

However, there are exceptions to the above procedure:

- When the network or the user receives an unexpected *RELEASE* message (for example, if the *DISCONNECT* message is corrupted by undetected transmission errors). In this case, no *STATUS* message is sent.
    - When the network receives an unexpected *RELEASE* message, the network
        - disconnects and releases the B-channel
        - clears the network connection and the call to the remote user with the *Cause* value in the *RELEASE* message sent by the user or, if not included, *Cause* value #31 “Normal, unspecified”
        - returns a *RELEASE COMPLETE* message to the user
        - releases the call reference
        - stops all timers
        - enters the *Null* state
    - When the user receives an unexpected *RELEASE* message, the user
        - disconnects and releases the B-channel
        - returns a *RELEASE COMPLETE* message to the network
        - releases the call reference
        - stops all timers
        - enters the *Null* state
- When the network or the user receives an unexpected *RELEASE COMPLETE* message
    - When the network receives an unexpected *RELEASE COMPLETE* message, the network
        - disconnects and releases the B-channel
        - clears the network connection and the call to the remote user with the *Cause* value indicated by the user or, if not included, *Cause* value #111 “Protocol error, unspecified”

    - releases the call reference
    - stops all timers
    - enters the *Null* state

  - Whenever the user receives an unexpected *RELEASE COMPLETE* message, the user
    - disconnects and releases the B-channel
    - releases the call reference
    - stops all timers
    - enters the *Null* state

- When a *NOTIFY* message is received which is in error
  - the recipient ignores the message, since, in general, the reception of a *NOTIFY* message does not cause the generation of a *STATUS* message.

- When the network or the user receives an unexpected connect_ack message in the call state N12 (Disconnect indication), no action is taken; message is ignored. In any other states, a STATUS message is sent with cause #101.

5.9.5 General information element errors

The general information element error procedures may also apply to information elements in codesets other than 0. The diagnostics in the *Cause* information element may indicate information elements other than those in codeset 0 by applying the locking shift procedures as described in section 4.5 on page 4-42.

5.9.5.1 Information element out-of-sequence error

A variable length information element which has a code value lower than the code value of the variable length information element preceding it is considered as an out-of-sequence information element.

If a message with an out-of-sequence information element (mandatory or non-mandatory IE) is received, the network will ignore the message.

5.9.5.2 Duplicated information elements error

If an information element is repeated in a message in which repetition of the information element is not permitted, only the contents of the information element appearing first are handled. All subsequent repetitions of the information element are ignored.

When repetition of information elements is permitted, only the contents of permitted information elements are handled. If the limit on repetition of information elements is exceeded, the contents of information elements appearing first up to the limit of repetitions are handled. All subsequent repetitions of the information element are ignored.

> ***Note:*** There are some legitimate exceptions in which all entries of the duplicate IE will be handled up to the maximum limit allowed.

5.9.6 Mandatory information element errors

5.9.6.1 Mandatory information element missing

When a message other than *SETUP*, *DISCONNECT*, *RELEASE* or *RELEASE COMPLETE* is received that has one or more mandatory information elements missing, no action is taken on this message and no state change occurs. A *STATUS* message is returned with *Cause* value #96 “Mandatory information element is missing”.

When a *SETUP* or *RELEASE* message is received that has one or more mandatory information elements missing, a *RELEASE COMPLETE* message with *Cause* value #96 “Mandatory information element is missing” is returned.

When a *DISCONNECT* message is received with the *Cause* information element missing, the actions taken are same as if a *DISCONNECT* message with *Cause* value #31 “Normal, unspecified” was received (see section 5.3 on page 4-122). The exception is that the *RELEASE* message sent to the user has *Cause* value #96 “Mandatory information element is missing”.

When a *RELEASE COMPLETE* message is received with a *Cause* information element missing, it is assumed that a *RELEASE COMPLETE* message has been received with *Cause* value #31 “Normal, unspecified”.

5.9.6.2 Mandatory information element content error

When a message other than *SETUP*, *DISCONNECT*, *RELEASE* or *RELEASE COMPLETE* is received that has one or more mandatory information elements with invalid content, no action is taken on this message and no state change occurs. A *STATUS* message is returned with *Cause* value #100 “Invalid information element contents”.

When a *SETUP* or *RELEASE* message is received that has one or more mandatory information elements with invalid content, a *RELEASE COMPLETE* message is returned with *Cause* value #100 “Invalid information element contents”.

When a *DISCONNECT* message is received with invalid content of the *Cause* information element, the action taken is the same as if a *DISCONNECT* message with *Cause* value #31 “Normal, unspecified” was received (see section 5.3 on page 4-122). The exception is that the *RELEASE* message sent on the local interface has *Cause* value #100 “Invalid information element contents”.

When a *RELEASE COMPLETE* message is received with invalid content of the *Cause* information element, it is assumed that a *RELEASE COMPLETE* message was received with *Cause* value #31 “Normal, unspecified”.

Information elements with a length exceeding the maximum length are treated as information elements with content error.

Receipt of an information element which has been truncated (for example, the length of IE is more than it receives) would lead to ignoring the message by the network, and no state change should occur.

5.9.7 Non-mandatory information element errors

The following sections identify actions on information elements not recognized as mandatory.

5.9.7.1 Unrecognized information elements

Unrecognized information elements are non-mandatory information elements whose information element identifiers are not implemented by the receiver of the information element.

When a message is received which has one or more unrecognized information elements, the receiving entity checks whether any are encoded to indicate “comprehension required”. If any unrecognized information element is encoded to indicate “comprehension required”, the procedures in section 5.9.6.1 on page 4-138 are followed. That is, as if a missing mandatory information element error condition had occurred.

If all unrecognized information elements are not encoded to indicate “comprehension required”, the receiving entity proceeds as follows:

- Action is taken on the message and those information elements which are recognized and have valid content.
- When the received message is other than *DISCONNECT*, *RELEASE* or *RELEASE COMPLETE*, a *STATUS* message is returned by the network and may be returned by the user. It has one *Cause* information element. The *STATUS* message indicates the call state in which the receiver detected the error. The *Cause* information element has *Cause* value #99 “Information element non-existent or not implemented”, and the diagnostic field contains the information element identifier of each unrecognized information element. The network sends only the first unrecognized information element identifier in the diagnostic field.
- Subsequent actions are determined by the sender of the unrecognized information elements. If a clearing message contains an unrecognized information element, the error is reported to the local user as follows:
    - — When a *DISCONNECT* message is received that has an unrecognized information element, a *RELEASE* message is returned with *Cause*

value #99 “Information element non-existent or not implemented”. The *Cause* information element diagnostic field, if present, contains the information element identifier for each information element which was unrecognized. The network sends only the first unrecognized information element identifier in the diagnostic field.

— When a *RELEASE* message is received that has an unrecognized information element, a *RELEASE COMPLETE* message is returned with *Cause* value #99 “Information element non-existent or not implemented”. The *Cause* information element diagnostic field contains the first information element identifier that is unrecognized. The network sends only the first unrecognized information element identifier in the diagnostic field.

— When a *RELEASE COMPLETE* message is received that has an unrecognized information element, no action is taken on the unrecognized information.

Note: The diagnostic of *Cause* value #99 facilitates the decision in selecting an appropriate recovery procedure at the reception of a *STATUS* message. Therefore, it is recommended that the user provide *Cause* value #99 with diagnostics if it expects the network to take appropriate action at the receipt of a *STATUS* message, although inclusion of the diagnostics is optional.

5.9.7.2 Non-mandatory information element content error

When a message is received that has one or more non-mandatory information elements with invalid content, action is taken on the message and those information elements that are recognized and have valid content.

A *STATUS* message is returned by the network and may be returned by the user containing one *Cause* information element. If the message containing one or more non-mandatory information elements with invalid content is a *RELEASE COMPLETE* message, no *STATUS* message is returned.

The *STATUS* message indicates the call state in which the receiver detected the error. The *Cause* information element has *Cause* value #100 “Invalid information element contents”. The diagnostic field, if present, contains the information element identifier of the information elements that have invalid contents. The network sends only the first information element which had invalid contents in the diagnostic field.

Information elements with a length exceeding the maximum length (see Chapter 4-3) are treated as information elements with content error.

Receipt of an information element which has been truncated (for example, the length of IE is more than it receives) would lead to ignoring the message by the network, and no state change should occur.

5.9.8 Data link reset

Whenever Layer 3 is informed of a spontaneous data link layer reset by means of the *DL-Establish-Indication* primitive, the following procedures are carried out:

- For calls in the disestablishment phase (states N11, N12, N19, U11, U12 or U19), no action is taken.
- Calls in the establishment phase (states N1, N3, N4, N6, N7, N8, N9, U1, U3, U4, U6, U7, U8 or U9) are cleared according to the procedures in section 5.3 on page 4-122.
- For calls in the active state (state N10), a *STATUS ENQUIRY* is sent from the network to the user. For calls in the active state (state U10), a *STATUS ENQUIRY* may be sent from the user to the network. (See section 5.9.10 on page 4-142 and section 5.9.11 on page 4-143 for further information.)

5.9.9 Data link failure

Whenever Layer 3 is notified by its data link entity by means of the *DL-Release-Indication* primitive that there is a data link layer malfunction, the following procedures are performed:

- Any calls not in an active state are cleared internally.
- For any call in the active state without a timer running, timer T309 is started (if timer T309 is implemented).

  Note: If timer T309 is already running, it is not restarted.

Layer 3 requests a Layer 2 re-establishment by sending a *DL-Establish-Request* primitive. When informed of Layer 2 re-establishment by means of the *DL-Establish-Confirm* primitive, Layer 3 stops timer T309, and

- either sends out a *STATUS* message with *Cause* value #31 “Normal, unspecified” to report the current state to the peer entity
- OR, sends out a *STATUS ENQUIRY* message to verify the call state of the peer entity (see section 5.9.10 on page 4-142)

If timer T309 expires prior to data link re-establishment, the network

- clears the network connection and call to the remote user with *Cause* value #27 “Destination out of order”
- disconnects and releases the B-channel
- releases the call reference
- enters the *Null* state

The implementation of timer T309 on the user side is optional, but is mandatory on the network side. If timer T309 expires prior to data link establishment, the user:

- clears the attached connection (if any) with *Cause* #27 “Destination out of order”
- disconnects and releases the B-channel
- releases the call reference
- enters the *Null* state

When a back-up D-channel is available, the back-up D-channel procedures, as specified in Annex F, are used.

5.9.10 Status enquiry procedure

Whenever an entity wishes to check the call state at a peer entity, a *STATUS ENQUIRY* message is sent requesting the call state. This may, in particular, apply to procedural error conditions described in section 5.9.8 on page 4-141 and section 5.9.9 on page 4-141.

After sending the *STATUS ENQUIRY* message, timer T322 is started in anticipation of receiving a *STATUS* message. While timer T322 is running only one outstanding request for call state information can exist. Therefore, if timer T322 is already running, it is not restarted. If a clearing message is received before timer T322 expires, timer T322 is stopped, and call clearing continues.

When a *STATUS ENQUIRY* message is received, the receiver responds with a *STATUS* message, reporting the current call state and *Cause* value #30 “Response to status enquiry”. Receipt of the *STATUS ENQUIRY* message does not result in a state change.

The sending or receipt of the *STATUS* message in such a situation does not directly affect the call state of either the sender or receiver. The side having received the *STATUS* message inspects the *Cause* information element. If a *STATUS* message is received that contains *Cause* #30 “Response to status enquiry”, timer T322 is stopped and the appropriate actions taken, based on the information in the *STATUS* message, relative to the current state of the receiver. On the network side, the call is cleared if the state of the incoming *STATUS* message is not compatible with the network state.

Further “appropriate actions” taken by a user are implementation dependent. However, the actions described in the following sections apply.

If timer T322 expires (that is, no *STATUS* message was received) the *STATUS ENQUIRY* message may be retransmitted one or more times until a response is received. The number of times a *STATUS ENQUIRY* message is retransmitted by the user is an implementation dependent value. The network does not retransmit the *STATUS ENQUIRY* message. The call is cleared to the local interface with *Cause* value #41 “Temporary failure”, if the *STATUS ENQUIRY* is retransmitted the maximum number of times. If appropriate, the network also clears the network connection, using *Cause* value #41 “Temporary failure”.

5.9.11 Receiving a *STATUS* message

When a *STATUS* message reporting an incompatible state is received, if the receiving entity determines that the state mismatch is a valid error condition (see Note below) it carries out one of the following procedures:

- Clears the call by sending the appropriate clearing message with *Cause* value #101 “Message not compatible with call state”.
- Takes other actions that attempt to recover from the mismatch. These actions are implementation dependent. The network sends a *STATUS ENQUIRY* message when the received state is incompatible, as described in section 5.9.10 on page 4-142.

Note: The sending and receiving state machines are dynamic, and valid state mismatches can occur due to message flow during the status enquiry and response stage. Further, one or both entities may not implement all call states.

The determination of which states are incompatible is an implementation option for the user.

The network considers the following states to be incompatible:

- If a *STATUS* message indicating any call state except the *Null* state is received in the *Null* state, the receiving entity sends a *RELEASE COMPLETE* message with *Cause* value #101 “Message not compatible with call state”. The receiving entity remains in the *Null* state.
- If a *STATUS* message indicating any call state except the *Null* state is received in the *Release request* state, no action is taken.
- If a *STATUS* message indicating the *Null* state is received in any state except the *Null* state, the receiver releases all resources and enters the *Null* state. When in the *Null* state, the receiver of a *STATUS* message that indicates the *Null* state takes no action other than to discard the message.
- If a *STATUS* message indicating any call state except the *Active* state is received in the *Active* state, a *STATUS ENQUIRY* message is sent.

A *STATUS* message may be received indicating a compatible call state but which has one of the following *Cause* values:

- #96 “Mandatory information element is missing”
- #97 “Message type non-existent or not implemented”

- #99 “Information element non-existent or not implemented”
- #100 “Invalid information element contents”.

The actions taken by the user are an implementation option. If other procedures are not defined, the receiver clears the call with the appropriate procedure defined in section 5.3 on page 4-122. It uses the *Cause* value specified in the received *STATUS* message. The network clears the call only when receiving a *Cause* value #96 “Mandatory information element is missing”.

On receipt of a *STATUS* message specifying a global call reference and reporting an incompatible state in the *Restart request* or *Restart* state, the receiving Layer 3 entity informs layer management and takes no further action on this message.

When in the *Null* state, if a *STATUS* message is received with the global call reference, no action is taken.

Chapter 4-6:
Circuit-mode multirate, 384 kbit/s, 1536 kbit/s procedures

This chapter describes extensions to the procedures in Chapter 4-5 to support the following, additional circuit-mode bearer capabilities

- multirate (64 kbit/s base rate, and a rate multiplier of 2 to 24)
- 384 kbit/s (H0 channel)
- 1536 kbit/s (H11 channel)

Users subscribe to one of the following channel-selection options to access the above bearer capabilities

- fixed - H0 and H11 channels, where H0 channels use one of the following set of contiguous time slots: 1 to 6, 7 to 12, 13 to 18 or 19 to 24
- floating - H0 and H11 channels, and multirate, where H0 channels use contiguous time slots as per the “fixed” option and the time slots for multirate are also contiguous
- flexible - H0 and H11 channels, and multirate, where H0 channels and multirate can use either contiguous or non-contiguous time slots

6.1 Call establishment at the originating interface

6.1.1 Compatibility information

The *Bearer capability* information element is described in section 4.5.5 on page 4-48. The following coding is used when selecting a multirate, 384 kbit/s or 1536 kbit/s bearer capability

- Information transfer capability of “Unrestricted digital information”
- Transfer mode of “Circuit mode”
- Information transfer rate of “Multirate (64 kbit/s base rate)”, “384 kbit/s” or “1536 kbit/s”
- Octet 4.1, and the Rate Multiplier field, is included if the Information transfer rate is “Multirate (64 kbit/s base rate)”

If the user subscribes to the “fixed” channel selection option, the only allowed Information transfer rates are “384 kbit/s” and “1536 kbit/s”. If the user subscribes to the “floating” or “flexible” channel-selection options, access to 384 kbit/s and 1536 kbit/s services is supported by providing an Information transfer rate of “Multirate (64 kbit/s base rate)” and a Rate multiplier of 6 or 24, respectively.

If the user is not an authorized subscriber of the multirate, 384 kbit/s or 1536 kbit/s circuit-mode bearer capabilites, a *RELEASE COMPLETE* message with *Cause* value #57 “Bearer capability not authorized” is sent by the network, following the procedures in section 5.3 on page 4-122.

6.1.2 Channel selection

The *Channel identification* information element in the *SETUP* message indentifies the channels selected for multirate, 384 kbit/s and 1536 kbit/s circuit-mode bearer capabilities. The *Channel identification* information element is described in section 4.5.11 on page 4-66. All the selected channels are on one DS-1 interface. The procedures in section 5.1.2 on page 4-114 are followed to complete the channel selection.

The number of channels identified corresponds to the Information transfer rate and Rate multiplier fields of the *Bearer capability* information element. If the contents of the Bearer capability and Channel identification information elements do not match, the procedures in section 5.9.6.2 on page 4-138 are performed.

If a multirate (rate multiplier of 24) or 1536 kbit/s (H11 channel) call is requested (that is, 24 64 kbit/s time slots), octets 3.2 and 3.3 of the *Channel identification* information element are not included.

If a multirate (rate multiplier of 2 through 23) or 384 kbit/s (H0 channel) call is requested, the slot map in the *Channel identification* information element identifes the 64 kbit/s time slots used for the call.

If the channels requested by the user are available, the network selects them for the call.

If any specified channel is not available, a *RELEASE COMPLETE* message with *Cause* value #44 “Requested circuit/channel not available” is sent by the network, following the procedures in section 5.3 on page 4-122.

6.2 Call establishment at the destination interface

6.2.1 Compatibility information

The *Bearer capability* information element is described in section 4.5.5 on page 4-48. The following coding is used when selecting a multirate, 384 kbit/s or 1536 kbit/s bearer capability

- Information transfer capability of "Unrestricted digital information"
- Transfer mode of "Circuit mode"
- Information transfer rate of "Multirate (64 kbit/s base rate)", "384 kbit/s" or "1536 kbit/s"
- Octet 4.1, and the Rate Multiplier field, is included if the Information transfer rate is "Multirate (64 kbit/s base rate)"

If the information transfer rate is 384 kbit/s or 1536 kbit/s, and the user subscribes to the "fixed" channel selection option, the *Bearer capability* information element is coded with an Information transfer rate of "384 kbit/s" or "1536 kbit/s", respectively.

When the information transfer rate is 384 kbit/s or 1536 kbit/s, and the user subscribes to the "floating" or "flexible" channel selection option, the *Bearer capability* information element is coded with an Information transfer rate of "Multirate (64 kbit/s base rate)" and a Rate multiplier of 6 or 24, respectively.

If the user is not an authorized subscriber of the multirate, 384 kbit/s or 1536 kbit/s circuit-mode bearer capabilites, the network clears the call to the remote user with *Cause* value #57 "Bearer capability not authorized".

6.2.2 Channel selection

The *Channel identification* information element in the *SETUP* message indentifies the channels selected for multirate, 384 kbit/s and 1536 kbit/s circuit-mode bearer capabilities. The *Channel identification* information element is described in section 4.5.11 on page 4-66. All the selected channels are on one DS-1 interface. The procedures in section 5.1.2 on page 4-114 are followed to complete the channel selection.

The number of channels identified corresponds to the Information transfer rate and Rate multiplier fields of the *Bearer capability* information element. If the contents of the Bearer capability and Channel identification information elements do not match, the procedures in are performed.

If a multirate (rate multiplier of 24) or 1536 kbit/s (H11 channel) call is requested (that is, 24 64 kbit/s time slots), octets 3.2 and 3.3 of the *Channel identification* information element are not included.

If a multirate (rate multiplier of 2 through 23) or 384 kbit/s (H0 channel) call is requested, the slot map in the *Channel identification* information element identifes the 64 kbit/s time slots used for the call.

If the channels requested by the network are available, the user selects them for the call.

If any specified channel is not available, a *RELEASE COMPLETE* message with *Cause* value #44 “Requested circuit/channel not available” is sent by the user, following the procedures in section 5.3 on page 4-122.

If there are insufficient channels on a single interface to support the information transfer rate requested, the network clears the call to the remote user with *Cause* value #34 “No circuit/channel available”.

6.3 Channel selection conflict

Channel selection conflict occurs when the channels selected for an incoming and outgoing call do not constitute two disjoint sets of time slots. When channel selection conflict occurs, the procedures in section 5.8 on page 4-134 are followed.

To minimize channel selection conflicts, the network does and the user should support channel selection algorithm options of selecting the lowest idle channels or highest idle channels. The user and the network would be assigned complementary channel selection algorithms (for example, the user selects the lowest idle channels and the network selects the highest idle channels).

6.4 Tones and announcements

No tones and announcements are provided for the multirate, 384 kbit/s and 1536 kbit/s bearer capabilities.

6.5 Call clearing

When the call is cleared, by the user or the network, all channels associated with the call are cleared following the procedures in section 5.3 on page 4-122.

6.6 Restart procedures

B-channels can be restarted irrespective of their usage within a multirate, 384 kbit/s or 1536 kbit/s call. If a single B-channel is restarted, Layer 3

- returns all the channels associated with the call to the idle state
- releases the call reference
- enters the *Null* state

The procedures in section 5.7 on page 4-132 are followed when call clearing is complete.

Chapter 4-7: D-channel maintenance

This chapter describes the D-channel maintenance procedures that are supported between the user and the network. These procedures describe the relationship between the ISDN PRI D-channel, Layer 3 establishment, maintenance actions and normal call control.

Section 3 of this specification describes the primitives used for communication between Layer 3 and Layer 2, and the associated Layer 2 procedures.

Additional procedures for Backup D-Channel service are described in Annex F.

7.1 D-channel states

In order of decreasing availability, the allowed D-channel states are defined below.

IS	In Service. In this state, the D-channel is available for transfer of call control and other Layer 3 messages.
OOS	Out Of Service. In this state, the D-channel is not available and the maintenance entity periodically attempts to move the D-channel to the IS state.
MB	Maintenance Busy. The attributes of this state are the same as MOOS except that moves to and from this state are performed automatically by maintenance procedures, rather than by manual intervention.
MOOS	Manual Out Of Service. In this state, the D-channel is not available. Only manual intervention on the near-end can move the D-channel to a more available state.
INB	Installation Busy. This is the D-channel state when it is first provisioned, or when service changes are being made to the interface. In other respects, this state is identical to MOOS.

7.2 Timers

The following timers are defined for D-channel maintenance.

T3DW This timer determines the maximum time that a maintenance entity waits for a *DL-Establish-Confirm* or *DL-Establish-Indication* primitive after sending a *DL-Establish-Request* primitive. The value of this timer in the network is 5 seconds. The value of this timer on the user side is not critical, but should be greater than N200 x T200 (see Section 3) to ensure that Layer 2 establishment has failed.

T3MB This timer is used to prevent Layer 2 establishment immediately after a Layer 1 failure. The value of this timer in the network is 5 seconds. The value of this timer on the user side is not critical but is recommended to be the same as the network value.

7.3 Procedures

D-channel maintenance procedures are initiated by one of the following actions

- initialization of an ISDN PRI
- manual intervention to add or remove Layer 3 (D-channel) from service
- automatic detection of D-channel failure or recovery

The procedures in section 5.9.8 on page 4-141 and in section 5.9.9 on page 4-141 are referenced where there are interactions between the D-channel maintenance procedures and call control.

7.3.1 D-channel installation

One channel (typically, time slot 24) is assigned as the D-channel when an ISDN PRI is initially provisioned. When installed, the D-channel is in the INB state. While in the INB state, attempts by the far-end of the interface to establish a Layer 2 connection are rejected. Manual intervention is required to move the D-channel from the INB state to the MOOS state.

7.3.2 Service changes

In order for the network to allow changes to the PRI service parameters (for example, provisioning B-channels associated with the PRI), the D-channel must be in the INB state. This helps to ensure that unintended side-effects do not occur as a result of automatic procedures that could move the D-channel to the IS state. Similarly, the user side should also ensure that Layer 3 is not established while service changes are being made.

On the network side, the D-channel must be in the MOOS state before it can be manually moved to the INB state. Similarly, when the D-channel is in the INB state, it can only be moved to the MOOS state.

7.3.3 Establishing an In Service D-channel

To begin the transfer of normal Layer 3 messages across the user-network interface requires the establishment of, first Layer 2 and then Layer 3. These procedures are described in this section.

7.3.3.1 Layer 2 establishment

D-channel establishment is initiated by manual intervention on the near-end of the interface to move the D-channel state from MOOS to OOS. When the D-channel moves to the OOS state, Layer 3 first

- sends a *DL-Establish-Request* primitive to Layer 2
- starts timer T3DW

If timer T3DW expires, the Layer 3 entity in the network resends the *DL-Establish-Request* primitive periodically, approximately every 120 seconds, although the first interval may be shorter. The user may also periodically request Layer 2 establishment.

When Layer 3 receives a *DL-Establish-Confirm* or *DL-Establish-Indication* primitive from Layer 2, and the D-channel state is OOS, Layer 3 establishment can proceed, as described below. If running, timer T3DW is stopped. If a *DL-Establish-Indication* primitive is received when the D-channel state is less available than OOS, Layer 3 responds with a *DL-Release-Request* primitive.

If Layer 3 receives a *DL-Establish-Indication* primitive from Layer 2 when the D-channel is in the IS state, a data link reset has occurred. In this case, Layer 3 clears all calls which are not in the *Active* state, following the procedures in section 5.9.8 on page 4-141. The D-channel remains in the IS state.

7.3.3.2 Layer 3 establishment

When Layer 2 is successfully established, as described above, Layer 3

- initiates and waits for successful completion of an all interfaces restart (see section 5.7 on page 4-132), if timer T309 is not running
- stops timer T309, if it is running
- moves the D-channel to the IS state

Once the D-channel is in the IS state, Layer 3 establishment is complete and normal call control procedures are allowed.

7.3.4 Layer 3 failure

If Layer 3 receives a *DL-Release-Indication* primitive from Layer 2 when the D-channel state is IS, Layer 3

- clears all calls which are not in the *Active* state, following the procedures in section 5.9.9 on page 4-141
- starts timer T309, if any calls are in the *Active* state and the timer is not already running
- starts timer T3DW
- moves the D-channel to the OOS state

The procedures in section 7.3.3.1 on page 4-151 are then followed in an attempt to re-establish the D-channel.

If Layer 3 receives a failure indication from Layer 1 when the D-channel state is IS, Layer 3 follows the same procedure as described above, with the following differences

- timer T3MB is started instead of timer T3DW
- the D-channel is moved to the MB state instead of the OOS state

When timer T3MB expires, Layer 3

- sends a *DL-Establish-Request* primitive to Layer 2
- starts timer T3DW
- moves the D-channel to the OOS state

7.3.5 Layer 3 removal

Layer 3 can be removed from service by manual intervention to move the D-channel state to MOOS. When this occurs, Layer 3

- clears all calls
- sends a *DL-Release-Request* primitive to Layer 2, if the D-channel state is IS
- starts timer T3DW, if it is not running
- moves the D-channel to the MOOS state

When timer T3DW expires and the D-channel is still in the MOOS state, no action is taken.

Chapter 4-8: B-channel maintenance

This chapter describes the B-channel maintenance procedures that are supported between the user and the network. These procedures provide for the transfer of individual B-channels between in service, out of service, and maintenance conditions.

8.1 B-channel states

In order of decreasing availability, the allowed B-channel states are defined below.

- In service: the B-channel can be allocated to a call by Layer 3 call control
- Out of service: the B-channel is not available for use by Layer 3 call control

The Out of service state is further categoried to identify which end of the interface initiated to move to that state. The possible categories are

- near-end
- far-end

These categories are used to ensure that only the side of the interface which initiated the move to Out of service state can subsequently move the B-channel to the In service state.

8.2 Timers

The following, additional timer is defined for use by B-channel maintenance.

T3M1 This timer determines the maximum time that a maintenance entity waits for a response to a *SERVICE* message. The value of this timer in the network is nominally120 seconds, but can be lesser or greater depending on other network activity. The value of this timer on the user side is not critical, but the same value as is used by the network is recommended.

8.3 Procedures

B-channel maintenance procedures are initiated by one of the following actions

- addition and initialization of an ISDN PRI
- manual intervention to add or remove B-channels or DS-1 links on an ISDN PRI
- automatic detection of B-channel failure or recovery
- receipt of maintenance messages from the far-end of the interface

As described in the following procedures, performance of the above B-channel maintenance actions may require the use of *SERVICE* and *SERVICE ACKNOWLEDGE* messages. When sending these messages, the protocol discriminator in the *Protocol discriminator* information element is set to “Maintenance messages” and the global call reference is used. At Layer 2, the same SAPI as for normal call control (“0”) is used.

8.3.1 Layer 3 establishment

Sending and reception of Layer 3 B-channel maintenance messages is only possible when Layer 3 is established on a D-channel associated with the ISDN PRI. Other maintenance actions that do not require the exchange of maintenance messages are allowed when no Layer 3 link is established on a D-channel. See Chapter 4-7: “D-channel maintenance” for Layer 3 establishment procedures.

When Layer 3 of an ISDN PRI is not established, that is, there is no active D-channel, all of its B-channels are in the Out of service state. Movement to this state is considered to have been initiated by the near-end of the interface.

When Layer 3 is subsequently established, all of its B-channels automatically change to the In service state, without any exchange of B-channel maintenance messages. B-channels which were not in the In service state previous to a Layer 3 failure, typically as a result of manual maintenance intervention, do not change state when Layer 3 is established.

8.3.2 Adding B-channels to service

This procedure is followed when one or more B-channels, including one or more DS-1 links, are added to service on an ISDN PRI. That is, the current state of each B-channel is Maintenance or Out of service.

This procedure is typically used for B-channels which are newly provisioned or were previously removed from service. This procedure may be used by the user, but is not used by the network, if the Layer 1 entity had previously detected a failure condition which prevented continued use of one or more B-channels, and a D-channel remained active. When Layer 1 recovers, the network moves the affected B-channels to the In service state, without the exchange of maintenance messages.

For each B-channel being added to service, the initiating side of the interface

- initiates and completes a single-channel restart for the individual B-channel, following the procedures in section 5.7 on page 4-132
- sends a *SERVICE* message to the responding side of the interface containing
  - a *Channel identification* information element which identifies the individual B-channel
  - a *Change status* information element with the Preference field set to “Channel” and the New status field set to “In service”

When the responding side of the interface receives the above *SERVICE* message, it checks the service availability of the indicated B-channel. If it can be successfully moved to the In service state, the responding side

- sends a *SERVICE ACKNOWLEDGE* message to the initiating side of the interface containing
  - a *Channel identification* information element which identifies the individual B-channel
  - a *Change status* information element with the Preference field set to “Channel” and the New status field set to “In service”
- changes the state of the B-channel to In service, and considers the state change to have been initiated by the far-end

If the responding side, due to local conditions, can not move the indicated B-channel to the In service state (for example, it was placed out of service by the near-end), it

- sends a *SERVICE ACKNOWLEDGE* message to the initiating side of the interface, as described above, but with the New status field of the *Change status* information element set to “Out of service”
- does not change the state of the B-channel

If the initiating side of the interface receives a *SERVICE ACKNOWLEDGE* message for the B-channel before timer T3M1 expires, it

- changes the B-channel state to that specified in the received *Change status* information element

If the new B-channel state is Out of service, the initiating side of the interface considers the state change to have been intiated by the far-end.

8.3.3 Removing B-channels from service

This procedure is followed when one or more B-channels, including one or more DS-1 links, are removed from service on an ISDN PRI. That is, the current state of each B-channel is In service.

This procedure is typically used for B-channels which are no longer subscribed to by the customer or for testing purposes. This procedure is used by the user, but is not used by the network, if the Layer 1 entity detects a failure condition which prevents continued use of one or more B-channels, and a D-channel remains active. When Layer 1 fails, the network moves the affected B-channels to the Out of service state, without the exchange of maintenance messages.

For each B-channel being removed from service, the initiating side of the interface

- sends a *SERVICE* message to the responding side of the interface containing
    - a *Channel identification* information element which identifies the individual B-channel
    - a *Change status* information element with the Preference field set to “Channel” and the New status field set to “Out of service”
- changes the state of the B-channel to Out of service

When the responding side of the interface receives the above *SERVICE* message, it checks the state of the indicated B-channel. If the current B-channel state is In service, the responding side

- sends a *SERVICE ACKNOWLEDGE* message to the initiating side of the interface containing
    - a *Channel identification* information element which identifies the individual B-channel
    - a *Change status* information element with the Preference field set to “Channel” and the New status field set to “Out of service”
- changes the state of the B-channel to Out of service, and considers the state change to have been initiated by the far-end

If the B-channel state at the responding side is currently Out of service, the responding side

- sends a *SERVICE ACKNOWLEDGE* message to the initiating side of the interface, as described above, but with the New status field of the *Change status* information element set to “Out of service”

- leaves the B-channel state as Out of service, and does not alter the category of the Out of service state (whether near-end or far-end)

If the initiating side of the interface receives a *SERVICE ACKNOWLEDGE* message for the B-channel before timer T3M1 expires, it

- changes the B-channel state to that specified in the received *Change status* information element, if it is not already in that state

  Note: The state specified in the received *Change status* information element may not be the one requested in the *SERVICE* message, depending on conditions at the responding side of the interface.

If the new B-channel state is Out of service, the initiating side of the interface considers the state change to have been intiated by itself (near-end).

8.3.4 Maintenance action on an active B-channel

B-channel states and call control states are independent. That is, call control and maintenance action can be performed independently.

Due to this independence, it is possible to have unexpected actions occur if care is not taken to avoid maintenance action on a B-channel associated with an active call reference. For example, placing test tones on a B-channel which has been placed in an Out of service state while there is an existing user call on that B-channel.

Before initiating maintenance action on a B-channel, other than either side of the interface initiating the lowering of the B-channel state from In service (see section 8.3.3 on page 4-156), the user should restart the B-channel or otherwise clear any active call associated with that B-channel. In the least intrusive case, an existing call can be allowed to clear normally, resulting in no direct user impact, after which no new calls can be established

8.4 Error procedures

8.4.1 Message structure

A *SERVICE* or *SERVICE ACKNOWLEDGE* message is ignored if one of the following conditions is true

- the *Protocol discriminator* information element is not coded as “Maintenance messages”; the procedures in section 5.9 on page 4-134 apply if it is coded as “Q.931 user-to-network call control message”
- a mandatory information element is missing
- a mandatory information element has content error

8.4.2 Unexpected *SERVICE ACKNOWLEDGE* message

If the state of the bearer channel was changed by the near end, for example DMS-100, then an unexpected SERVICE ACKNOWLEDGE Message will be handled as follow:

- If the change status field matches the network state, then the SERVICE ACKNOWLEDGE Message will be ignored.
- If the change status field does not match the network state then a SERVICE Message will be sent by the DMS-100 with the change status field set to the state the network thinks the bearer channel is in and Timer T3M1 is started.

If the state of the bear channel was changed by the far end, then an unexpected Service Acknowledge message will be ignored by the network.

8.4.3 *SERVICE* message collision

If a *SERVICE* message is received for a B-channel while timer T3M1 is running, a *SERVICE* message collision has occurred. The following procedure ensures that the final state of the B-channel at both sides of the interface is equal to the state with the lowest availability of those in the *SERVICE* messages sent by each side of the interface.

If the new state sent in the *SERVICE* message is “In-Service”, the side which detects the collision

- stops timer T3M1
- responds to the received *SERVICE* message with a *SERVICE ACKNOWLEDGE* message with the New status field of the *Change status* information element set to the state in the received *SERVICE* message
- changes the B-channel state to that specified in the received *Change status* information element, if it is not already in that state; if the final state is Out of service, it is considered to have been initiated by the far-end of the interface

If the new state sent in the *SERVICE* message is “Out-of-Service”, the side which detects the collision

- stops timer T3M1
- responds to the received *SERVICE* message with a *SERVICE ACKNOWLEDGE* message with the New status field of the *Change status* information element set to “Out-of-Service”
- leaves the B-channel state as Out of service, and does not alter the state category (whether near-end or far-end)

Chapter 4-9: Connectionless signaling procedures

This chapter describes the procedures which are used to perform connectionless signaling on a PRI. Connectionless signaling is defined as a form of non-call associated signaling, that is, signaling not associated with a call. The procedures are connectionless in that no signaling connection is established at the network layer (the null call reference is used).

The *FACILITY* and *FACILITY REJECT* messages with a null call reference are used to transport the application information between the originating and terminating nodes. The application protocol that is used (for example, TCAP) is contained in the *Facility* information element of the *FACILITY* and *FACILITY REJECT* messages.

9.1 Routing procedures

The routing information for connectionless messages is contained in the *Origination* and *Destination* information elements. The *Origination* information element identifies the node originating the connectionless message and the *Destination* information element identifies the node at which the connectionless message terminates.

A node receiving a connectionless message determines if the received *Destination* information element identifies the node itself or another node. If the *Destination* information element identifies the node itself, the *Facility* information element is processed. If the *Destination* information element does not identify the node itself, then the same connectionless message is sent from the intermediate node towards the terminating node over the appropriate PRI.

If the *Destination* information element contains a private number, the Private network identifier field uniquely identifes the private network with which the routing information is associated.

Messages sent from the terminating node to the originating node follow the same procedure as described above, but with the *Destination* and *Origination* information elements being interchanged.

9.2 Error procedures

The application at the originating node determines whether the return message on error option is selected. If it is not selected, the *Options* information element is not included in the *FACILITY* message.

If a node is unable to route the *FACILITY* message to the terminating node or appropriate application, then a *FACILITY REJECT* message is returned to the originator if the following conditions are satisfied

- the *Options* information element is contained in the *FACILITY* message
- the return message on error option is specified in the *Options* information element

Otherwise the FACILITY message is discarded.

The *FACILITY REJECT* message contains the error condition in a *Reason for return* information element.

If a *FACILITY REJECT* message can not be sent to the originator for any reason, the *FACILITY* message is discarded and no further action is taken.

The recovery procedures that may be performed as a result of a message not being delivered are application specific.

9.3 Application protocol

The application protocol that is used in connectionless signaling for supplementary services in Section 5 of this specification is the Transaction Capabilities Application Part (TCAP) protocol as defined in ANSI standard T1.114. The TCAP protocol is carried in the *FACILITY* and *FACILITY REJECT* messages within the *Facility* information element.

Chapter 4-10:
Layer 3 list of system parameters

10.1 Timers

This section lists all the timers associated with the Layer 3 primary rate interface. The description of timers in the following tables should be considered a brief summary. The detailed procedures for timer usage are found in Chapter 4-5 through Chapter 4-8, which contain the definitive descriptions.

The timer values shown in Table 3-39 on page 4-162 are the defaults used by the network side of the interface. The timers are modifiable by the telephone operating company.

The timer values shown in Table 3-40 on page 4-164 are the recommended values for the user side of the interface. The user side table is included for reference and guidance only.

.

Table 3-39
Timers on the network side of the interface

Timer number	Default time-out value	State	When started	When stopped (normally)	Action taken on expiry	Cross Reference
T301	180 s	N7	On receiving *ALERT* message	On receiving *CONNECT* message	Clear call.	Mandatory
First start of T303	4 s	N6	On sending *SETUP* message	On receiving *CALL PROCEEDING, ALERT, CONNECT,* or *RELEASE COMPLETE* message	Resend *SETUP* message. Restart T303. If *RELEASE COMPLETE* message is received, clear the call	Mandatory
Second start of T303	4 s	N6	On resending *SETUP* message	On receiving *CALL PROCEEDING, ALERT, CONNECT, RELEASE COMPLETE* message	Clear network connection.	Mandatory
T305	30 s	N12	On sending *DISCONNECT* message	On receiving *RELEASE* or *DISCONNECT* message	Send *RELEASE* message.	Mandatory
First start of T308	4 s	N19	On sending *RELEASE* message	On receiving *RELEASE* or *RELEASE COMPLETE* message	Resend *RELEASE* message. Restart T308.	Mandatory
Second start of T308	4 s	N19	On resending *RELEASE* message	On receiving *RELEASE* or *RELEASE COMPLETE* message	Place B-channel in maintenance condition. Release call reference	Mandatory
T309	90 s	Any stable state	Data link disconnection. Calls in stable state not lost	Data link reconnected	Clear network connection. Release B-channel and call reference	Mandatory

Table 3-39
Timers on the network side of the interface (Continued)

Timer number	Default time-out value	State	When started	When stopped (normally)	Action taken on expiry	Cross Reference
T310	10 s	N9	On receiving *CALL PROCEEDING* message	On receiving *ALERT, CONNECT, PROGRESS* or *DISCONNECT* message	Clear call in accordance with section 5.2.4.3 on page 4-119.	Mandatory
T316	120 s	Restart Request	On sending *RESTART* message	On receiving *RESTART ACKNOWLEDGE* message	*RESTART* may be retransmitted several times	Mandatory
T321	40 s	Any call state	D-channel failure	Response to Layer 3 message received	Send *DL-Establish-Request* on both D-channels.	Mandatory when Annex F is implemented, otherwise optional
T322	4 s	Any call state	On sending *STATUS ENQUIRY* message	On receiving *STATUS, DISCONNECT, RELEASE,* or *RELEASE COMPLETE* message	Initiate call clearing.	Mandatory

Table 3-40
Timers on the user side of the interface

Timer number	Default time-out value	State	When started	When stopped (normally)	Action taken on expiry	Cross Reference
T301	180 s	U7	On receiving *ALERT* message	On receiving *CONNECT* message	Initiate call clearing	Optional
First start of T303	4 s	U1	On sending *SETUP* message	On receiving *CALL PROCEEDING, ALERTING, CONNECT,* or *RELEASE COMPLETE* message	Resend *SETUP* message. Restart T303. If *RELEASE COMPLETE* has been received, initiate call clearing	Mandatory when Annex D is implemented, otherwise optional
Second start of T303	4 s	U1	On re-sending *SETUP* message	On receiving *CALL PROCEEDING, ALERTING, CONNECT, RELEASE COMPLETE* message	Clear internal connection. Send *RELEASE COMPLETE* message. Enter *Null* state	Mandatory when Annex D is implemented, otherwise optional
T305	30 s	U11	On sending *DISCONNECT* message	On receiving *RELEASE* or *DISCONNECT* message	Send *RELEASE* message.	Mandatory
First start of T308	4 s	U19	On sending *RELEASE* message	On receiving *RELEASE* or *RELEASE COMPLETE* message	Resend *RELEASE* message. Restart T308	Mandatory
Second start of T308	4 s	U19	On re-sending *RELEASE* message	On receiving *RELEASE* or *RELEASE COMPLETE* message	Place B-channel in maintenance condition. Release call reference.	Mandatory
T309	90 s	Any stable state	Data link disconnection Calls in stable state not lost	Data link reconnected	Release network connection. Release B-channel and call reference.	Optional

Table 3-40
Timers on the user side of the interface (Continued)

Timer number	Default time-out value	State	When started	When stopped (normally)	Action taken on expiry	Cross Reference
T310	10 s	U3	On receiving *CALL PROCEEDING*	On receiving *ALERTING, CONNECT, PROGRESS,* or *DISCONNECT* message	Send *DISCONNECT* message.	Mandatory when Annex D is implemented, otherwise optional
T313	4 s	U8	On sending *CONNECT* message	On receiving *CONNECT ACKNOWLEDGE* message	Send *DISCONNECT* message	Mandatory
T316	120 s	Restart Request	On sending *RESTART* message	On receiving *RESTART ACKNOWLEDGE* message	*RESTART* may be retransmitted several times.	Mandatory
T321	40 s	Any call state	D-channel failure	Response to Layer 3 message received	Send *DL-Establish-Request* on both D-channels.	Mandatory when Annex F is implemented, otherwise optional
T322	4 s	Any call state	On sending *STATUS ENQUIRY* message	Receipt of *STATUS, DISCONNECT, RELEASE,* or *RELEASE COMPLETE* message	*STATUS ENQUIRY* may be retransmitted several times.	Mandatory

Chapter 4-11: Annexes

11.1 Annex A: Layer 3 SDL diagrams

This section includes overview and detailed SDL diagrams which show Layer 3 protocol control for circuit-switched basic calls. In the event of conflict between these diagrams and the text in the previous chapters of this Section, the text should be considered as the definitive source. Similarly, in the event of conflict between overview SDL and detailed SDL diagrams, the detailed SDL diagrams should be the considered as the definitive source.

Figure 4-48
Key to Layer 3 protocol control SDL diagrams (network side)

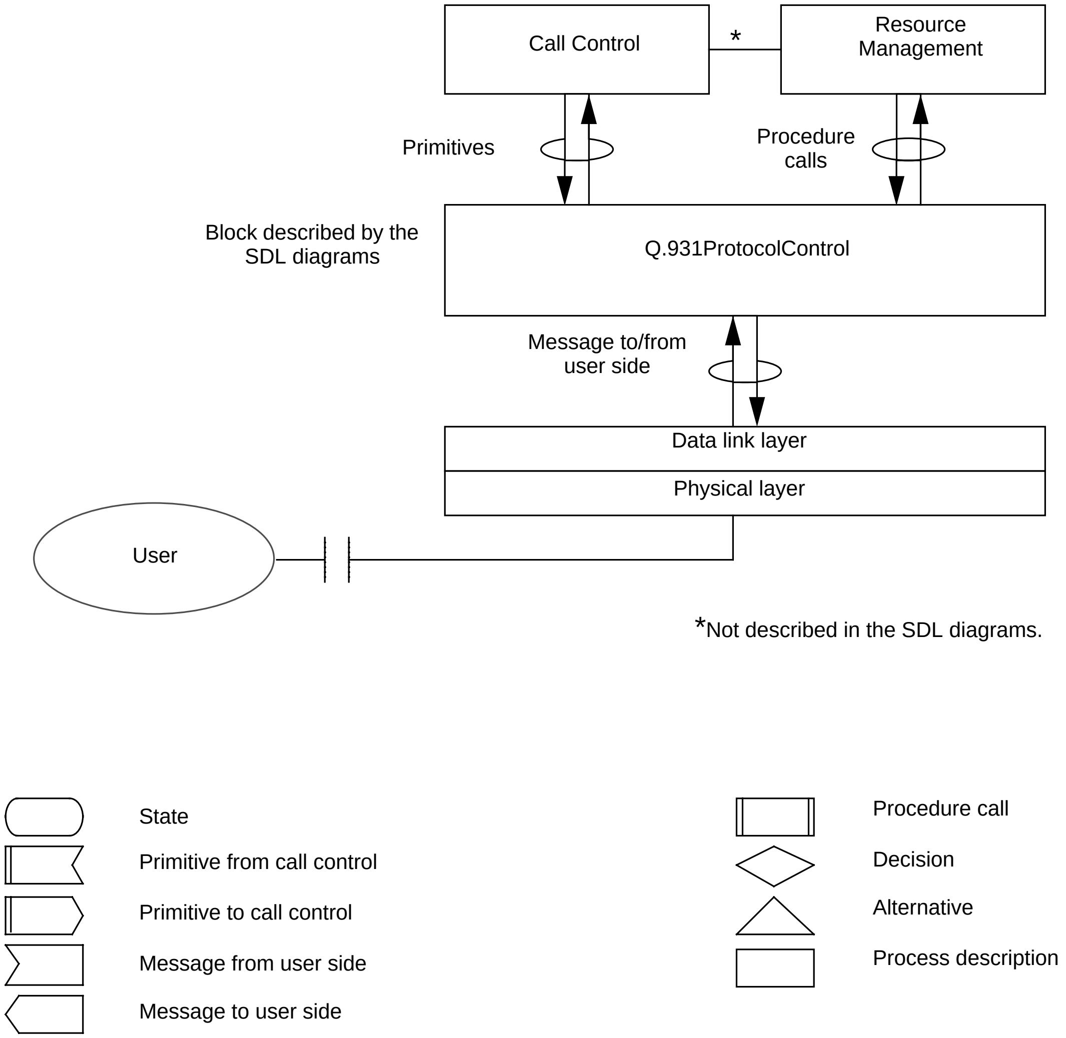
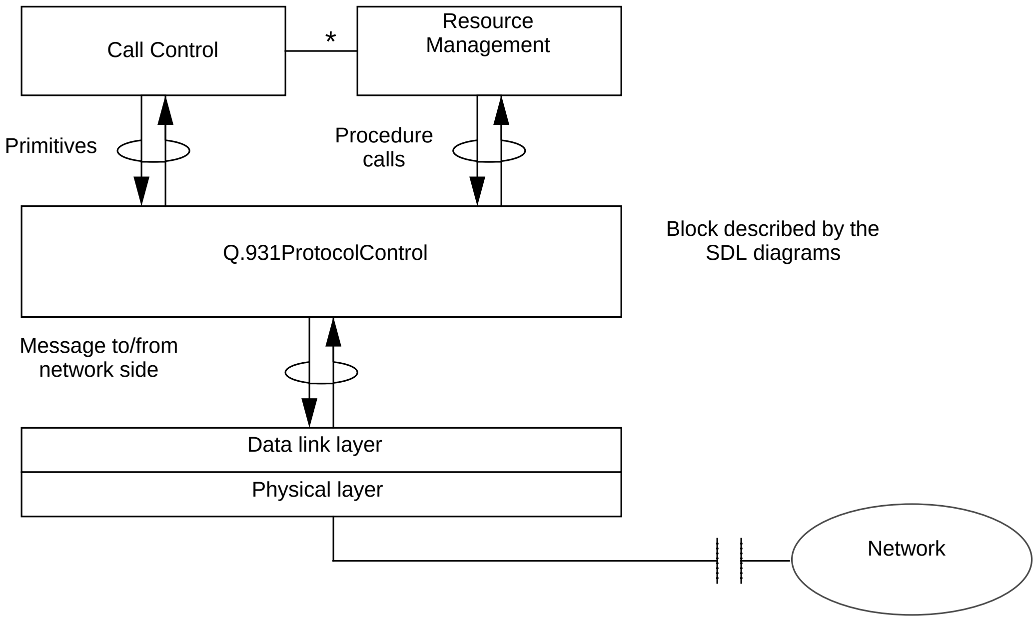


Figure 4-49
Key to Layer 3 protocol control SDL diagrams (user side)



*Not described in the SDL diagrams.

Figure 4-50
Overview protocol control: user side (1 of 5)
Outgoing setup procedure (1 of 2)

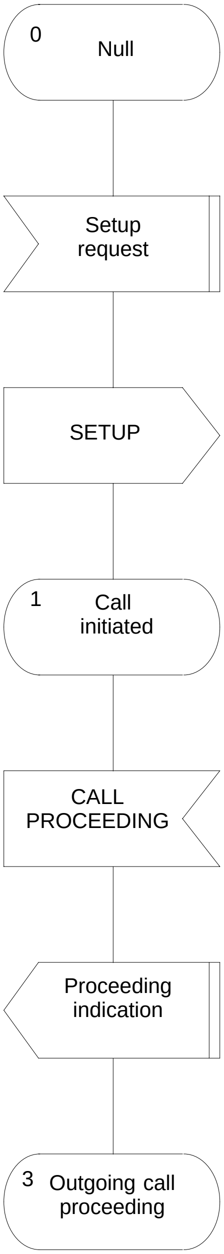


Figure 4-51
Overview protocol control: user side (2 of 5)
Outgoing setup procedure (2 of 2)

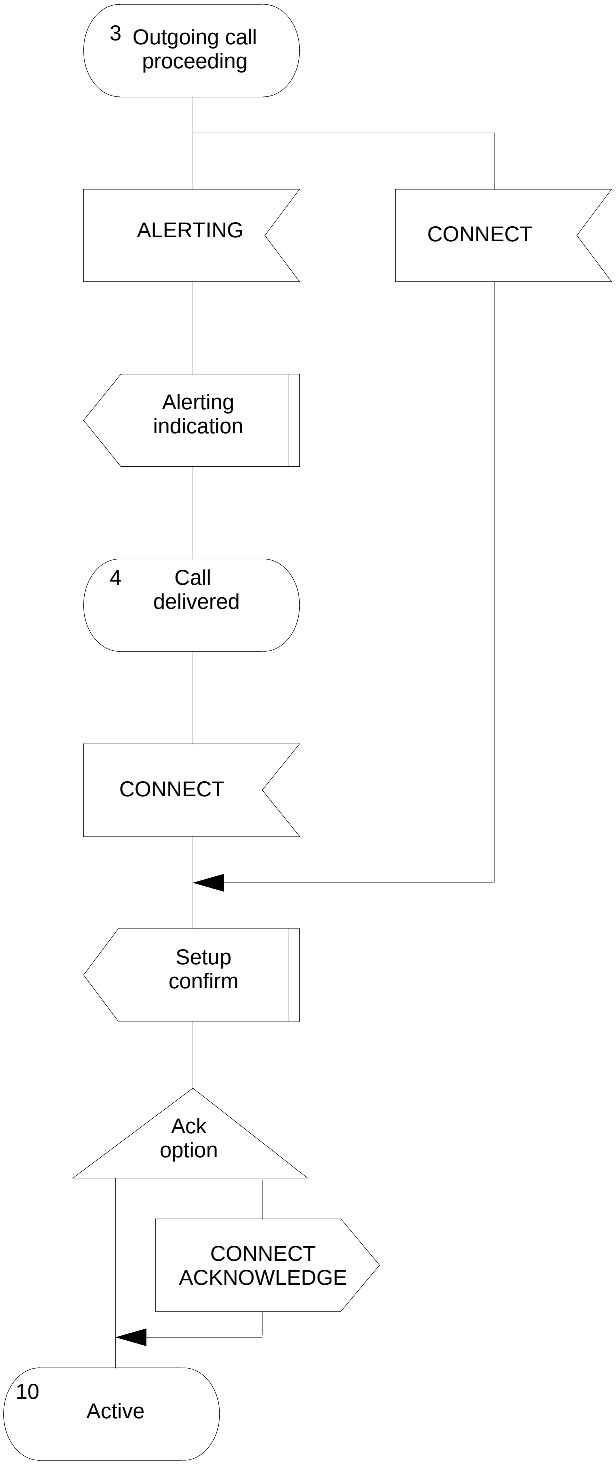


Figure 4-52
Overview protocol control: user side (3 of 5)
Incoming setup procedure (1 of 2)

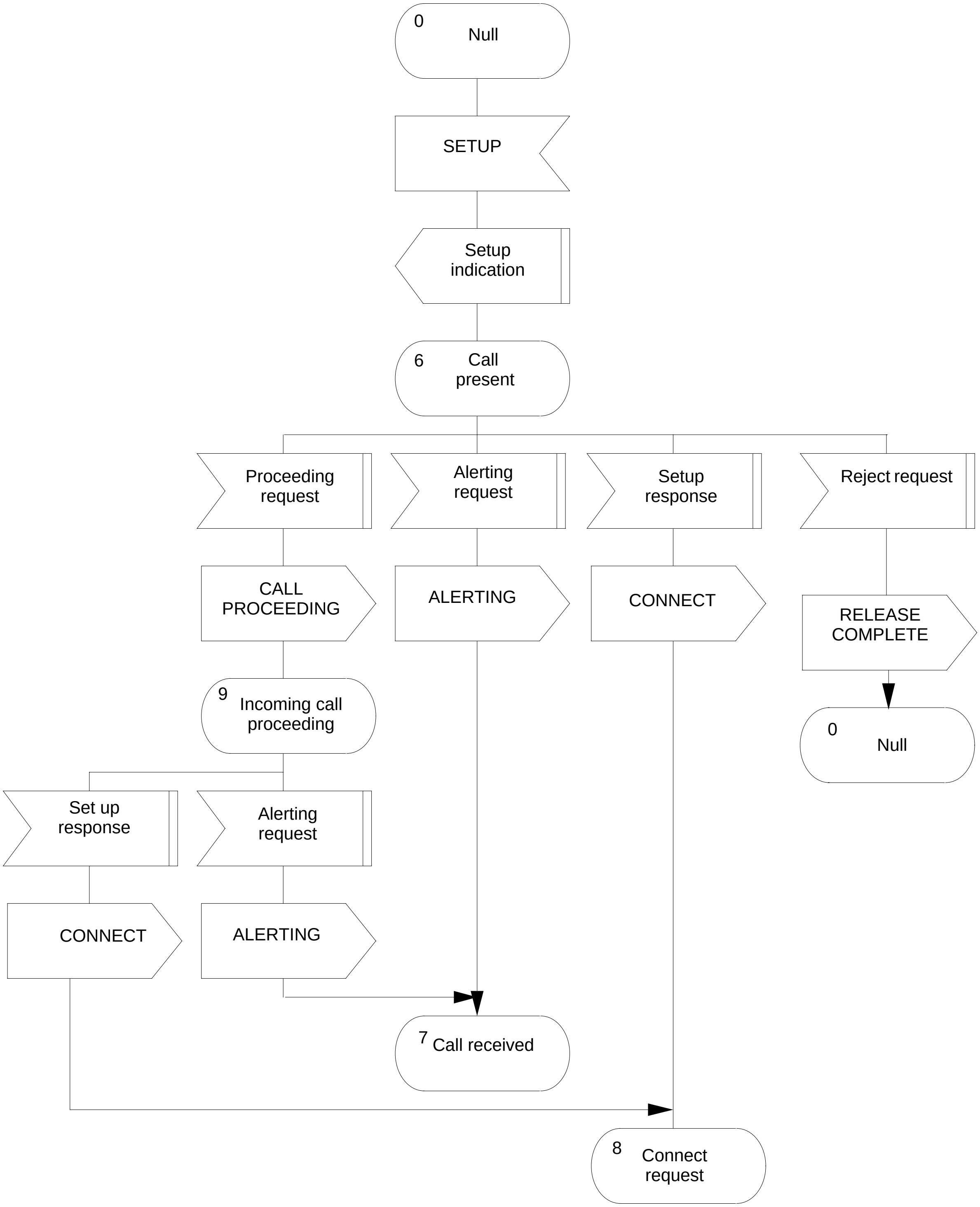


Figure 4-53
Overview protocol control: user side (4 of 5)
Incoming setup procedure (2 of 2)

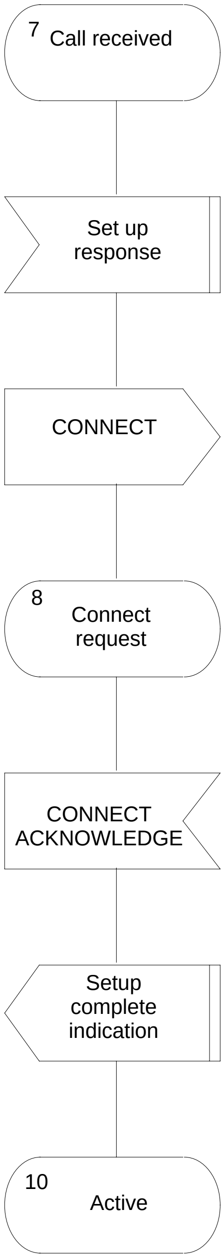


Figure 4-54
Overview protocol control: user side (5 of 5)
Clearing procedure

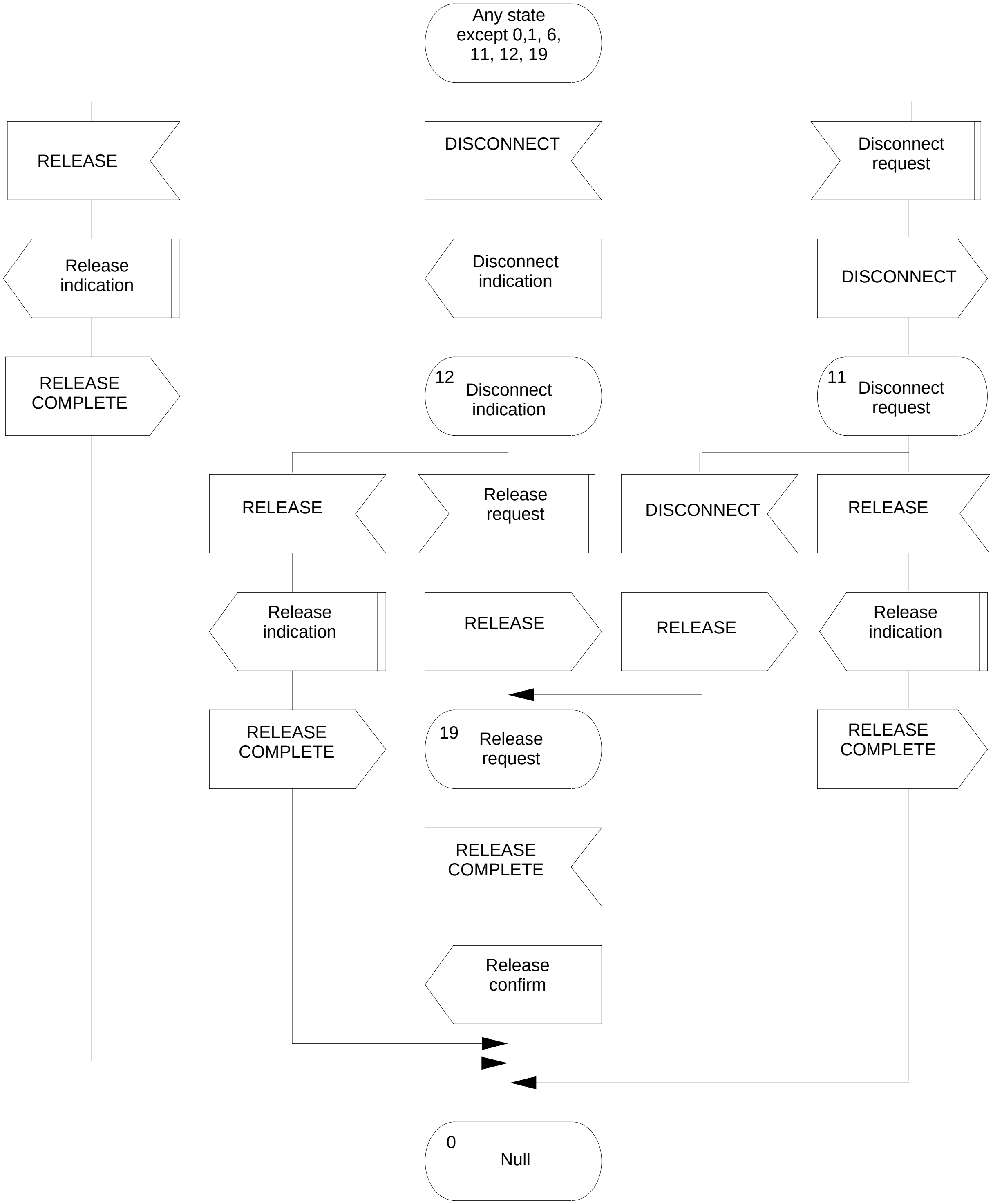


Figure 4-55
Detailed protocol control: User side (1 of 15)

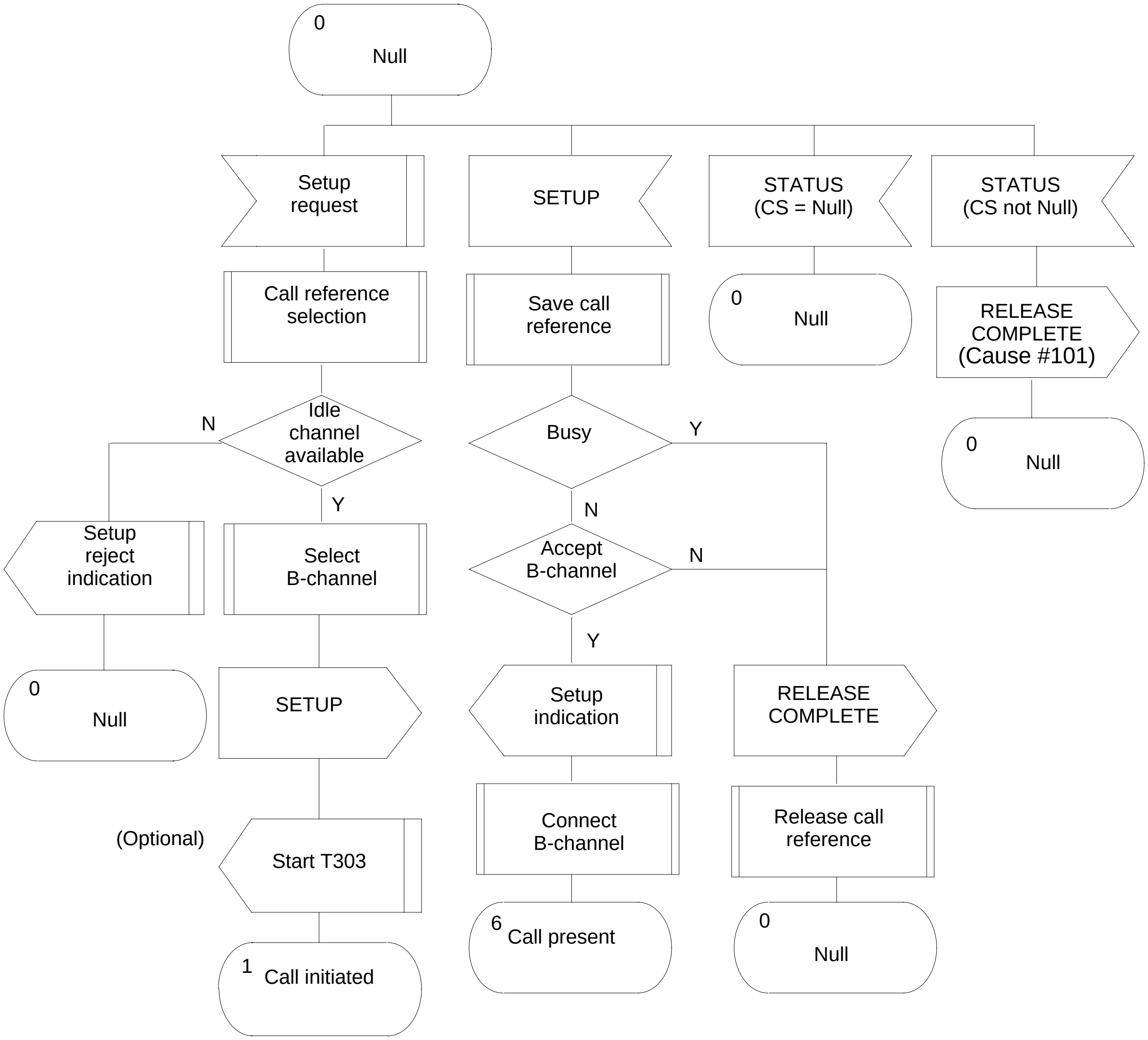


Figure 4-56
Detailed protocol control: User side (2 of 15)

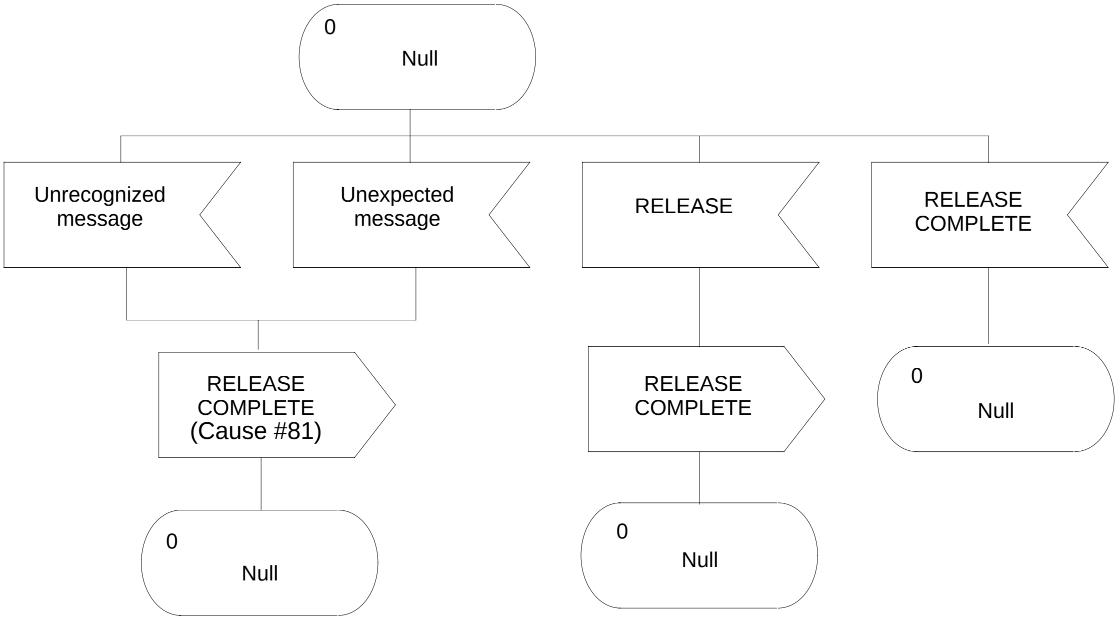


Figure 4-57
Detailed protocol control: User side (3 of 15)

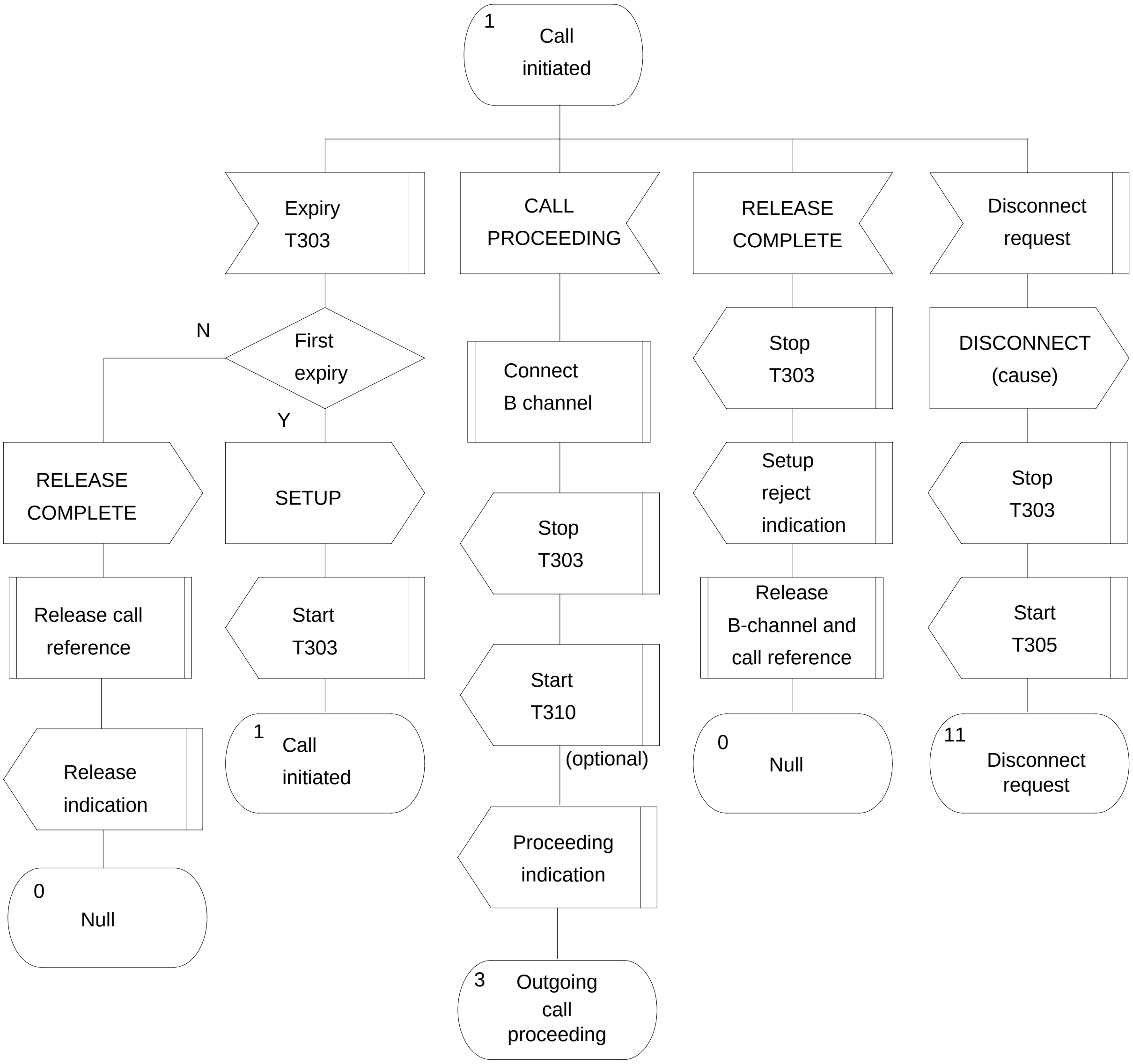


Figure 4-58
Detailed protocol control: User side (4 of 15)

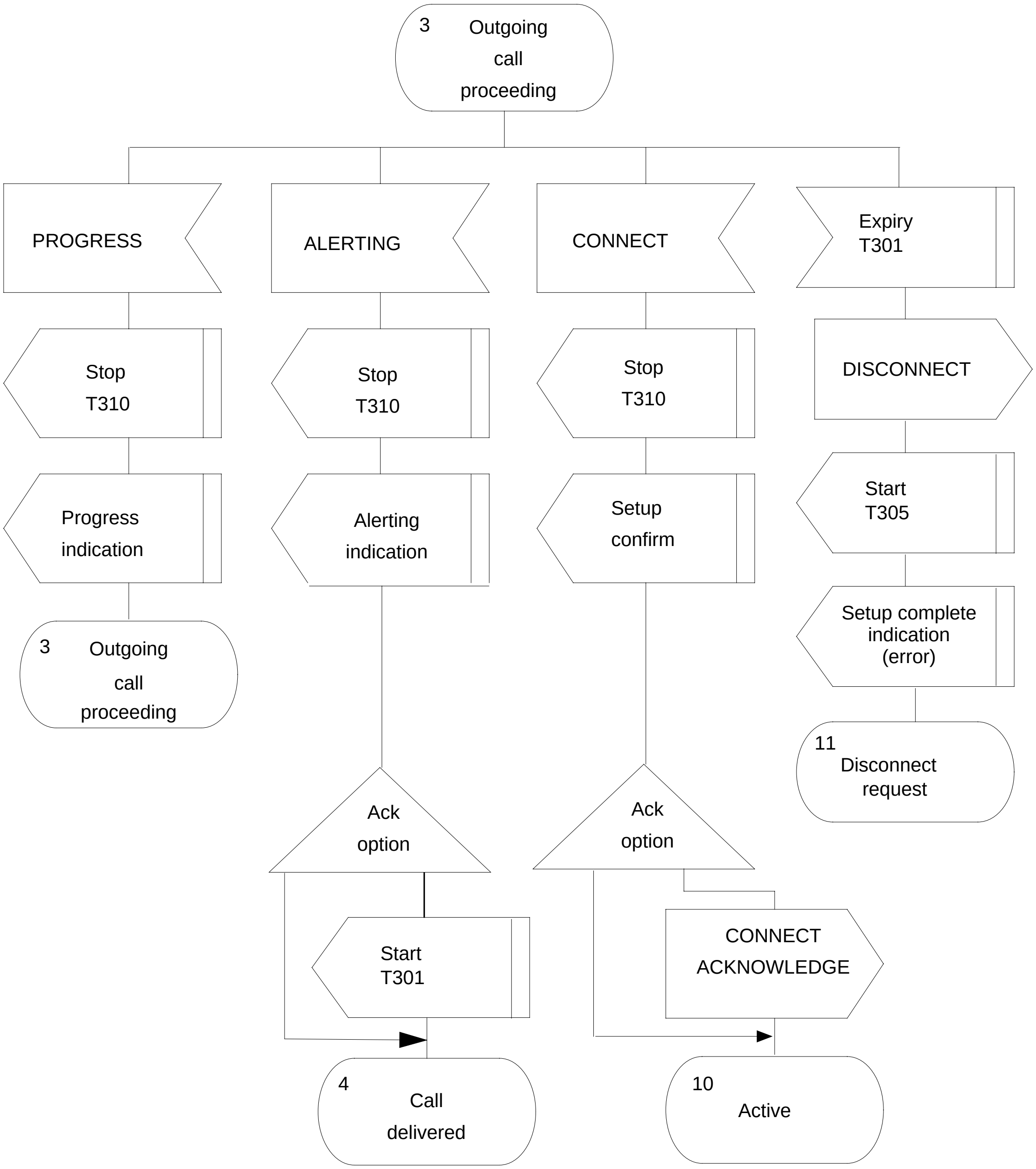


Figure 4-59
Detailed protocol control: User side (5 of 15)

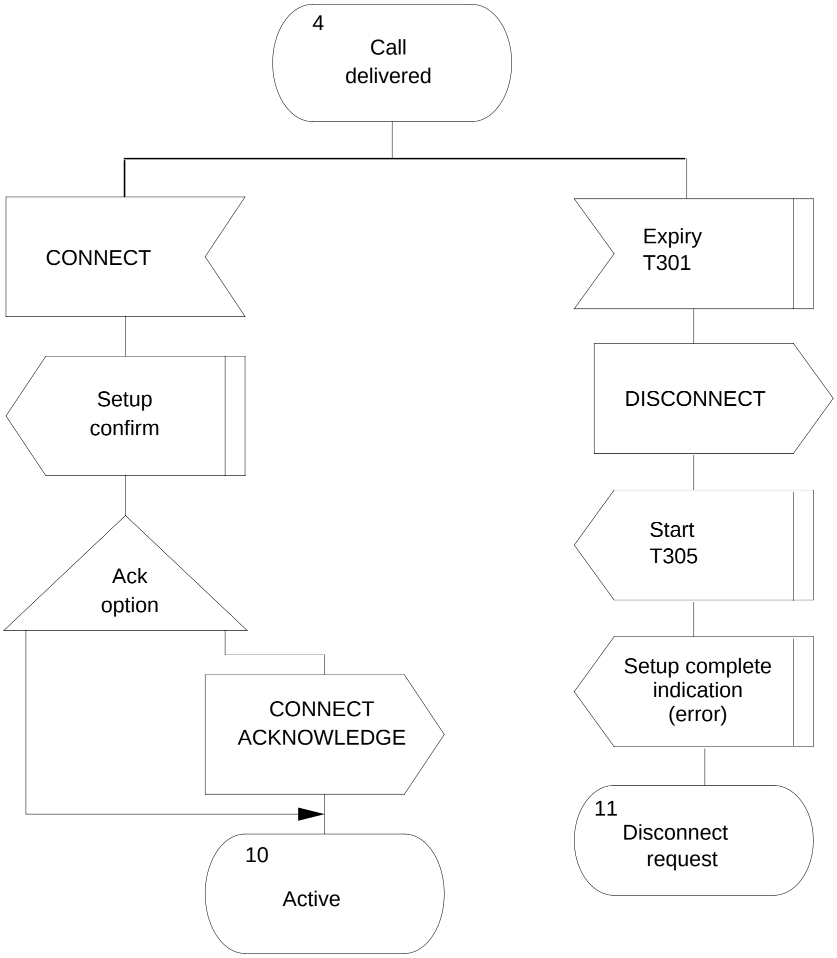


Figure 4-60
Detailed protocol control: User side (6 of 15)

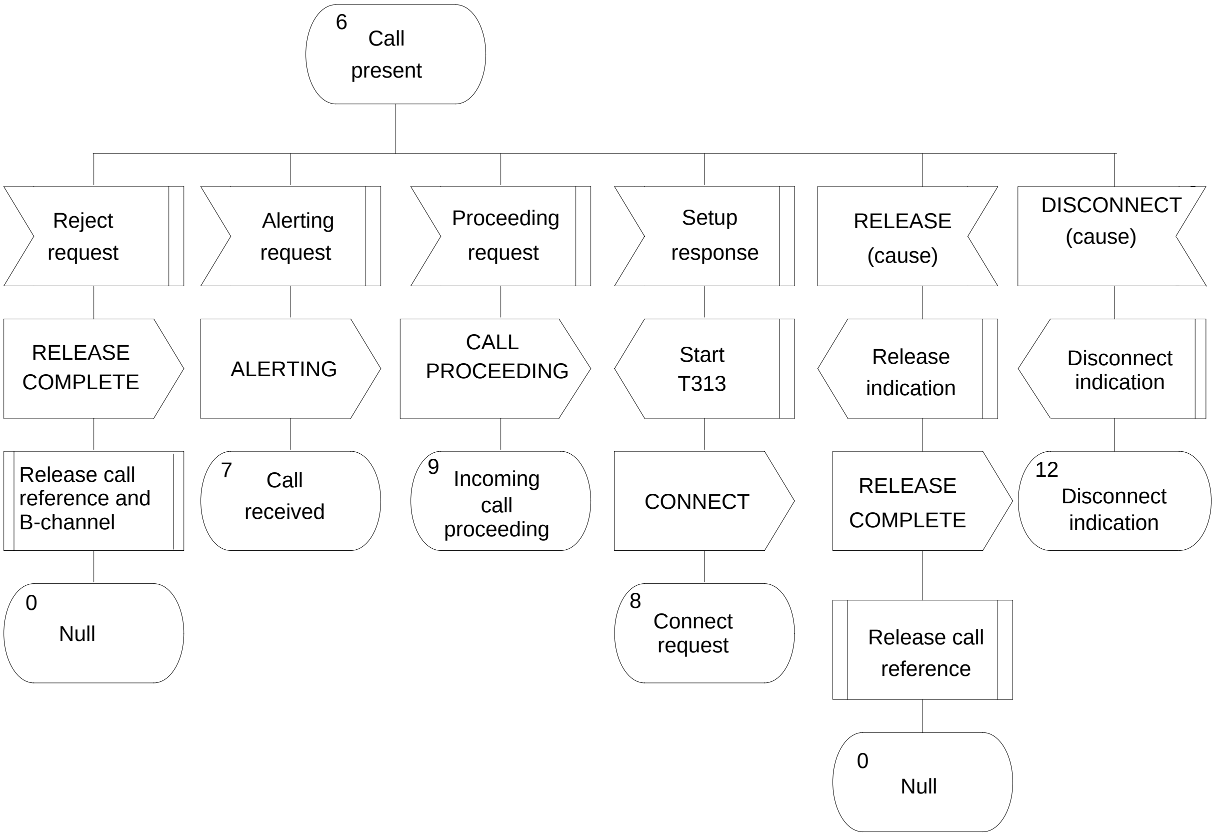


Figure 4-61
Detailed protocol control: User side (7 of 15)

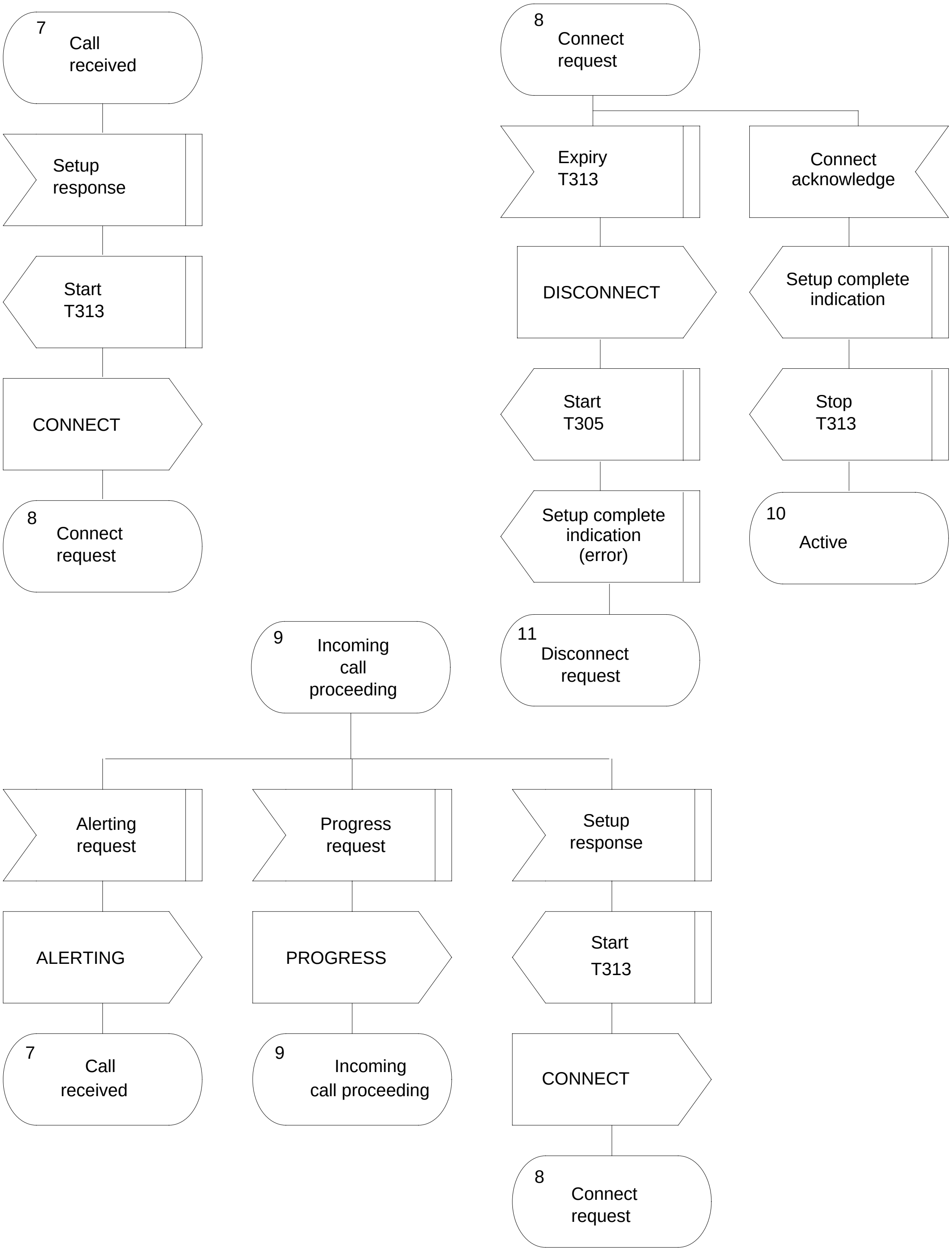
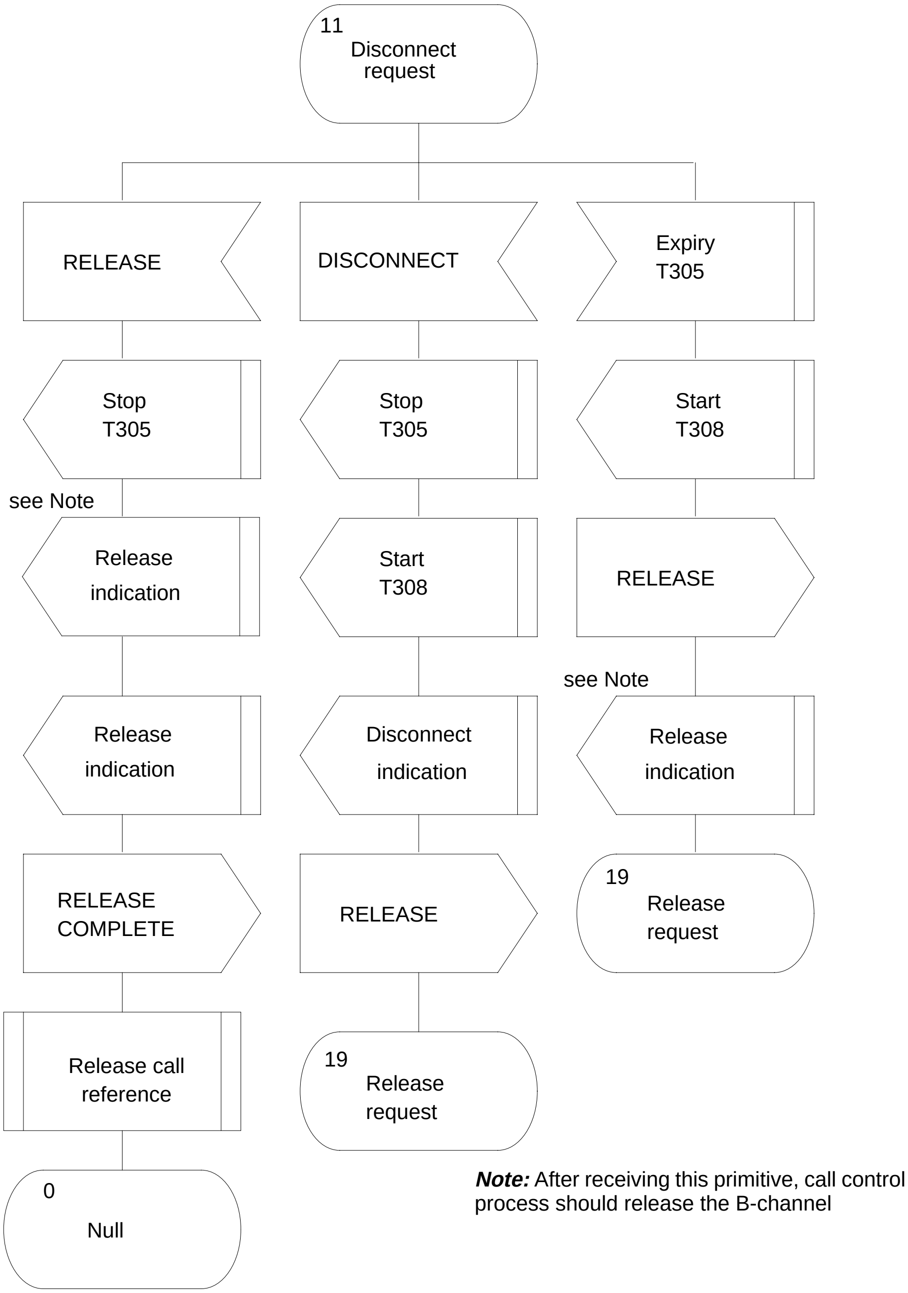
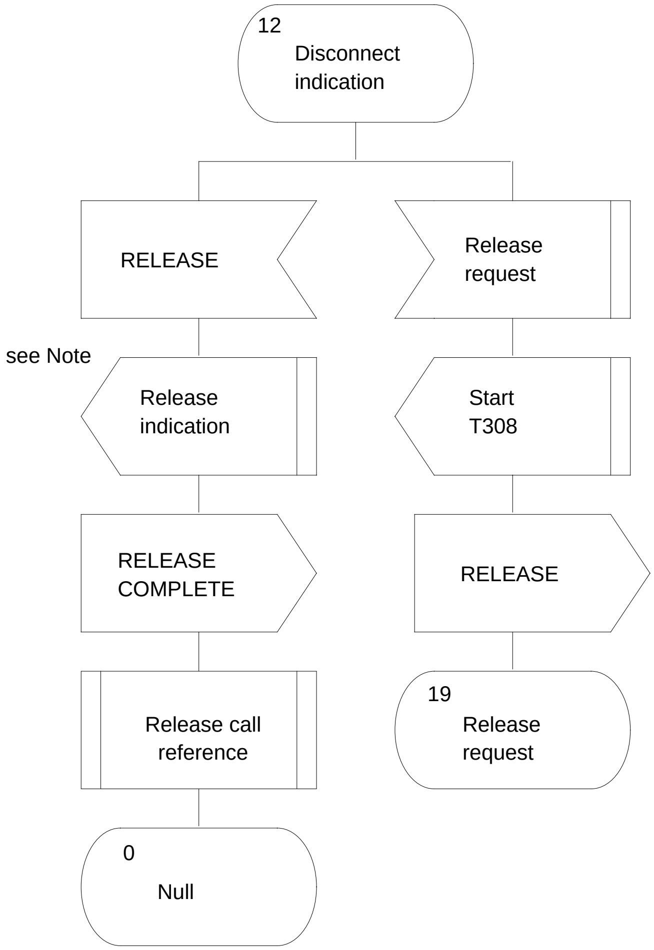


Figure 4-62
Detailed protocol control: User side (8 of 15)



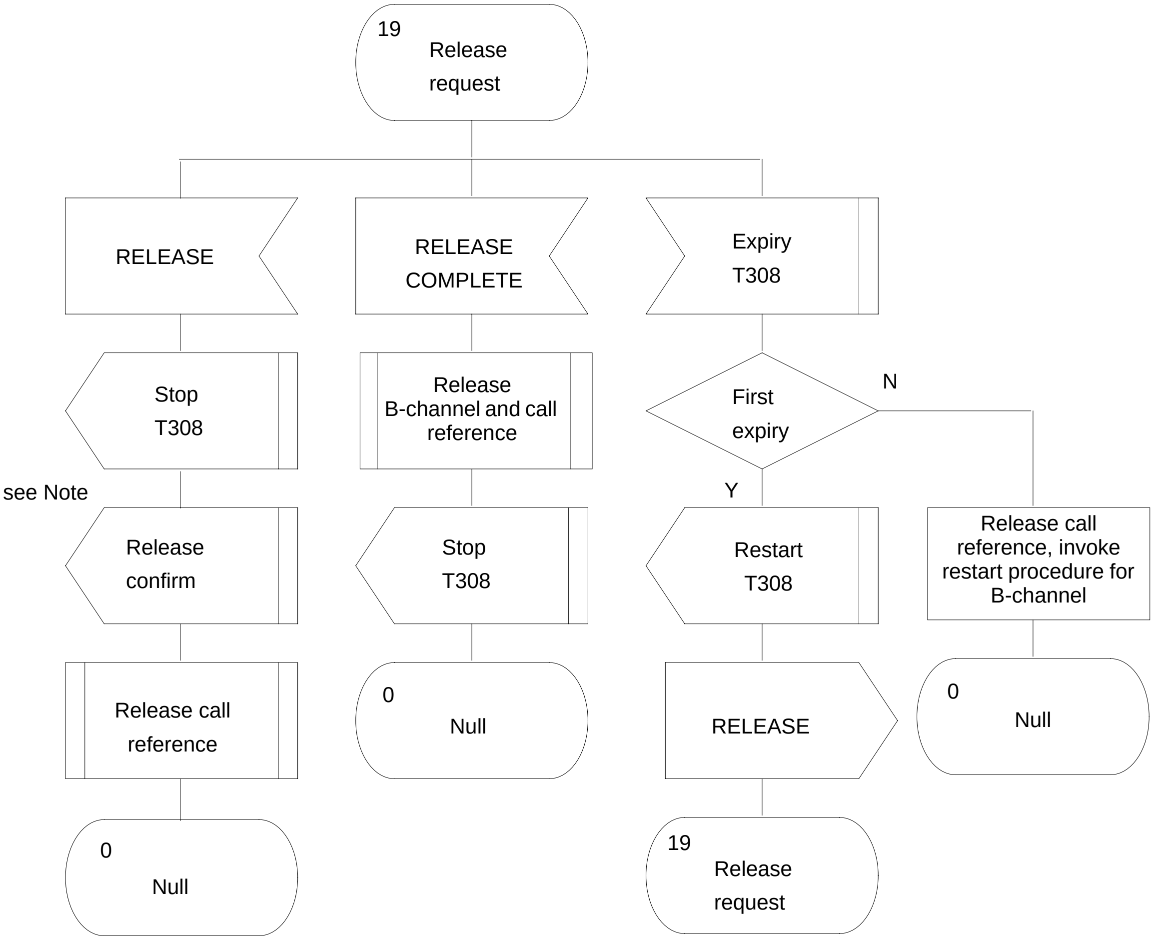
Note: After receiving this primitive, call control process should release the B-channel

Figure 4-63
Detailed protocol control: User side (9 of 15)



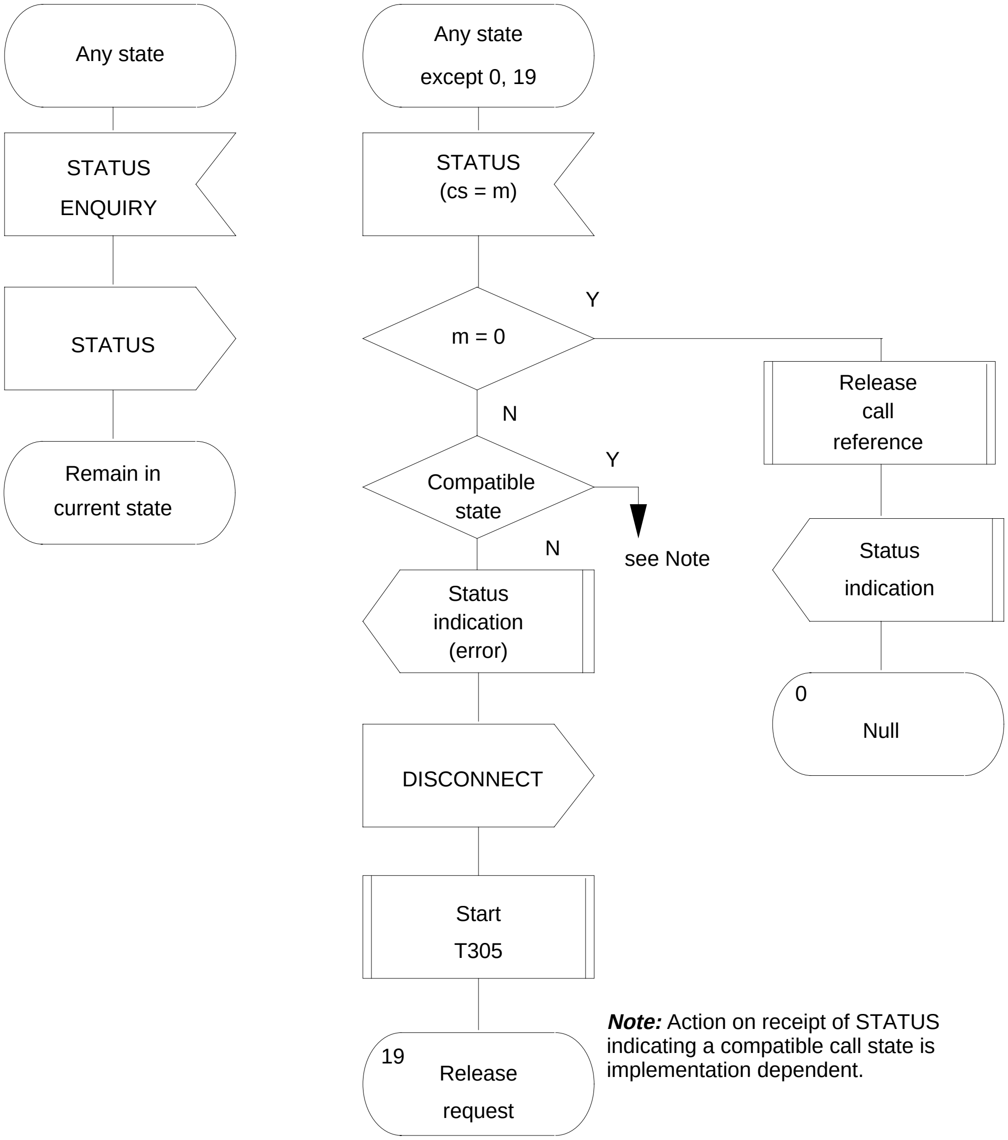
Note: After receiving this primitive, call control process should release the B-channel

Figure 4-64
Detailed protocol control: User side (10 of 15)



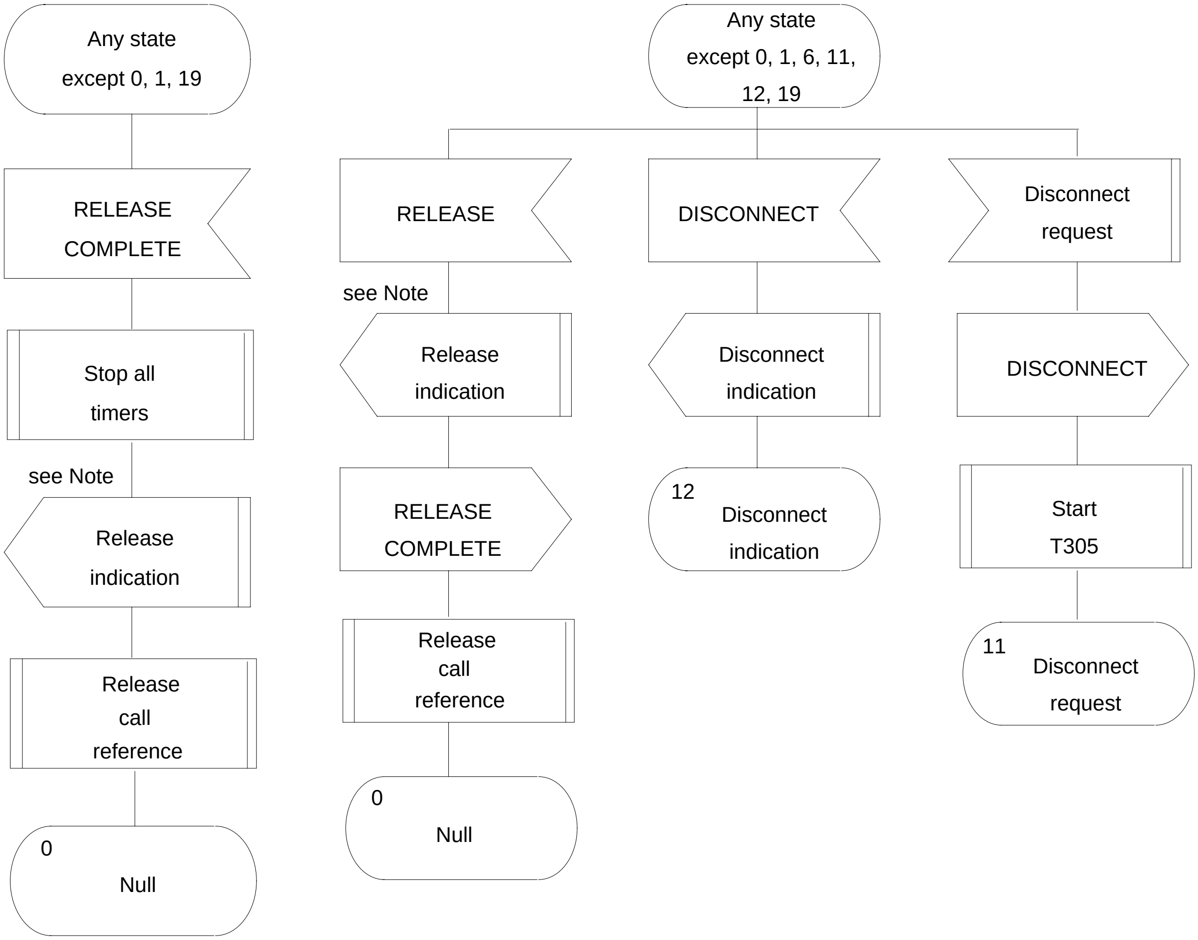
Note: After receiving this primitive, call control process should release the B-channel

Figure 4-65
Detailed protocol control: User side (11 of 15)



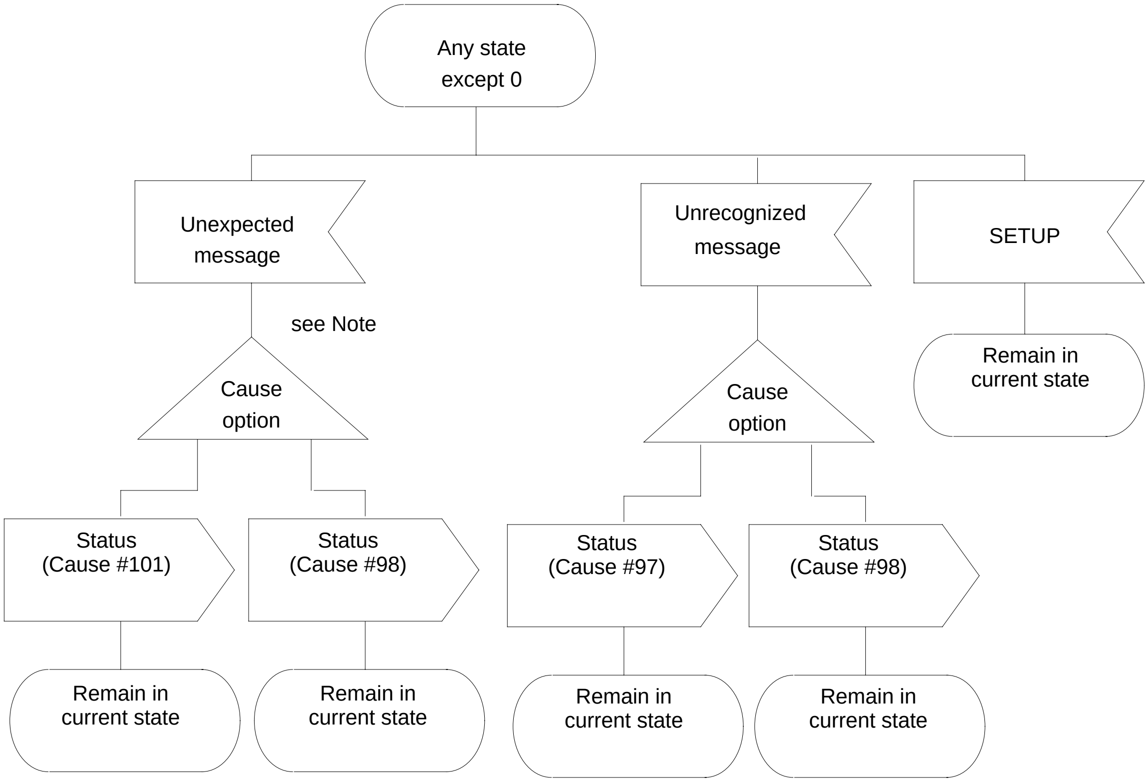
Note: Action on receipt of STATUS indicating a compatible call state is implementation dependent.

Figure 4-66
Detailed protocol control: User side (12 of 15)



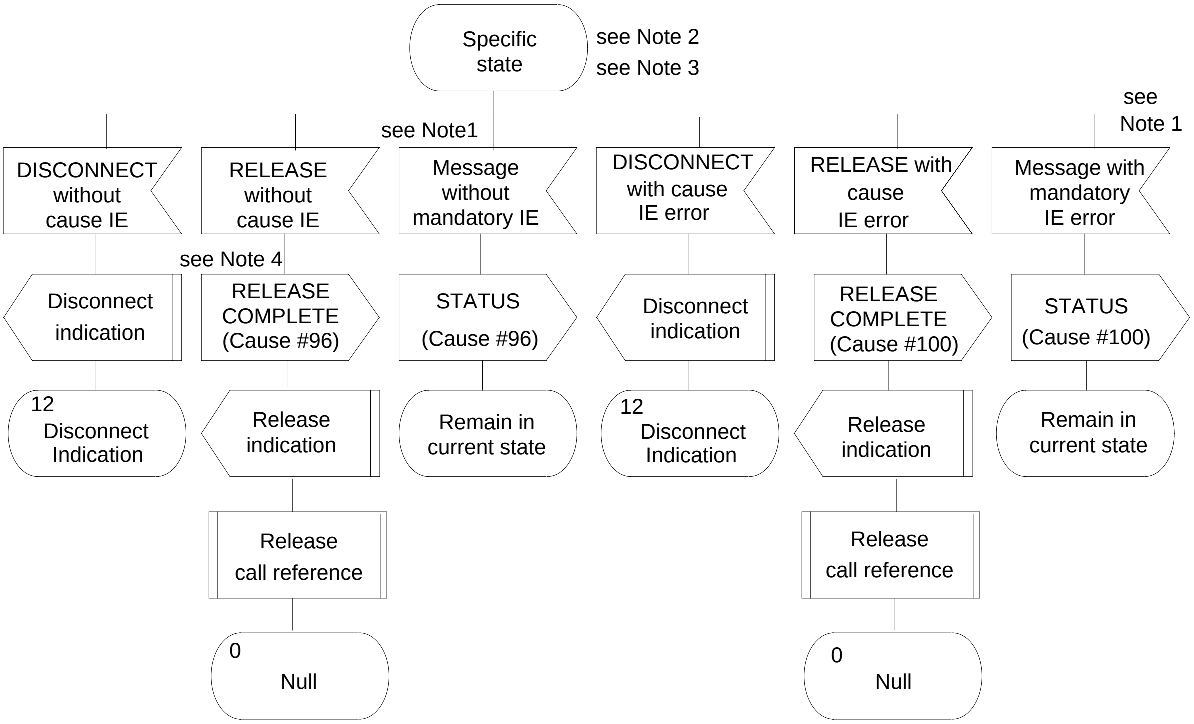
Note: After receiving this primitive, call control process should release the B-channel

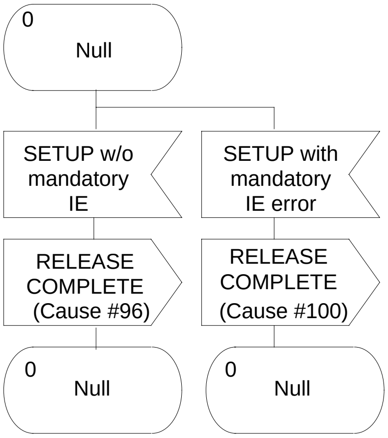
Figure 4-67
Detailed protocol control: User side (13 of 15)



Note: Except RELEASE or RELEASE COMPLETE

Figure 4-68
Detailed protocol control: User side (14 of 15)





Note 1: Except SETUP, RELEASE COMPLETE and DISCONNECT.

Note 2: These messages are recognized by the user and are expected messages in the state.

Note 3: See procedures for specific states.

Note 4: Release the B channel.

Figure 4-69
Detailed protocol control: User side (15 of 15)

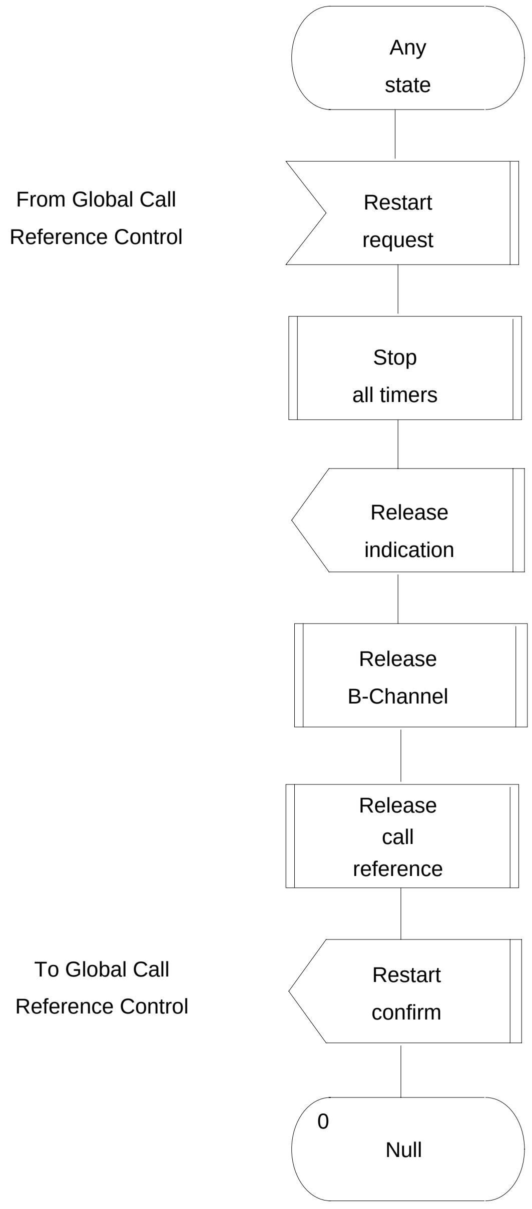
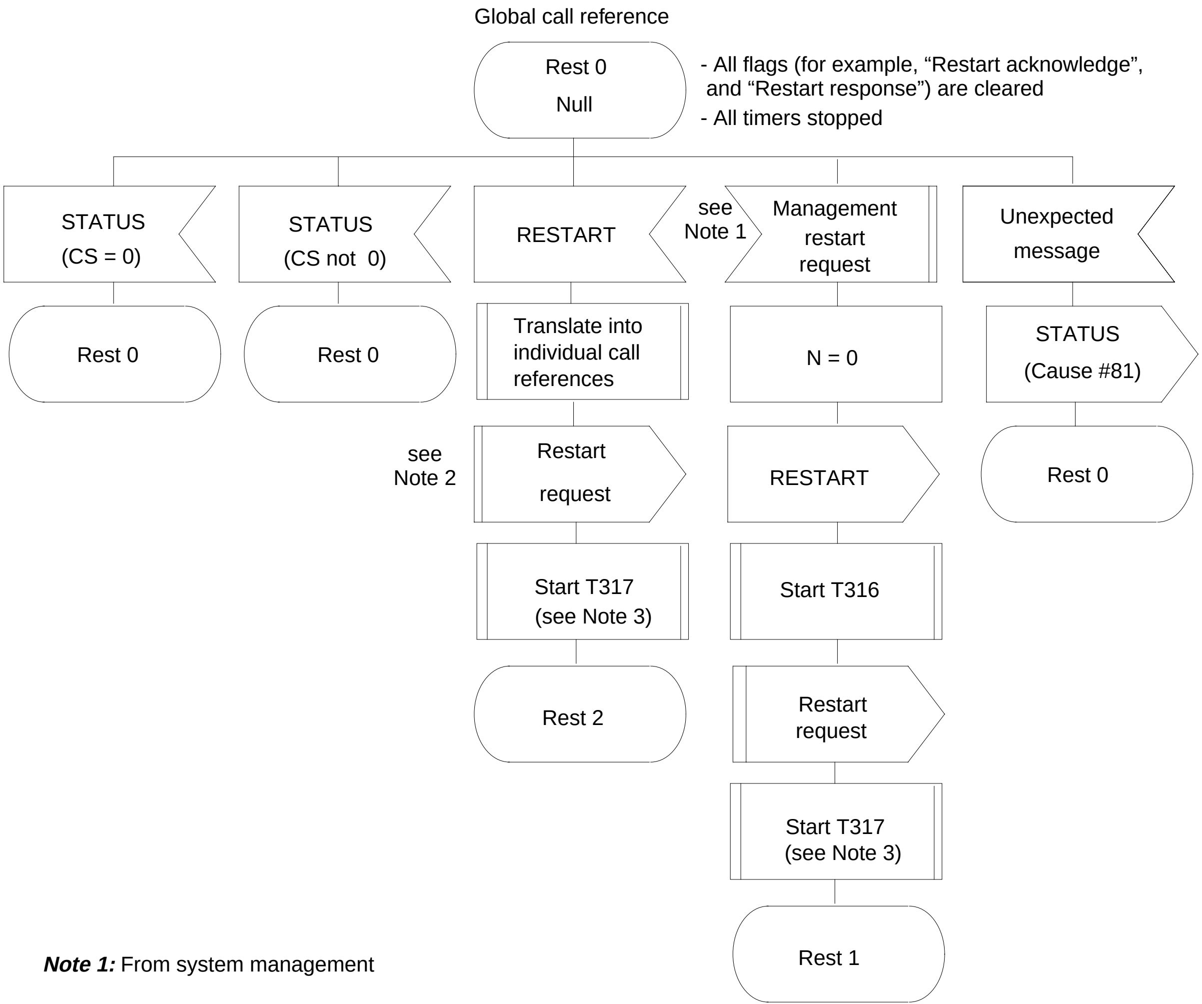


Figure 4-70
Detailed protocol control for the global call reference (1 of 4)



Note 1: From system management

Note 2: To Q.931 protocol control (related call reference)

Note 3: The value of T317 is implementation dependent.

Figure 4-71
Detailed protocol control for the global call reference (2 of 4)

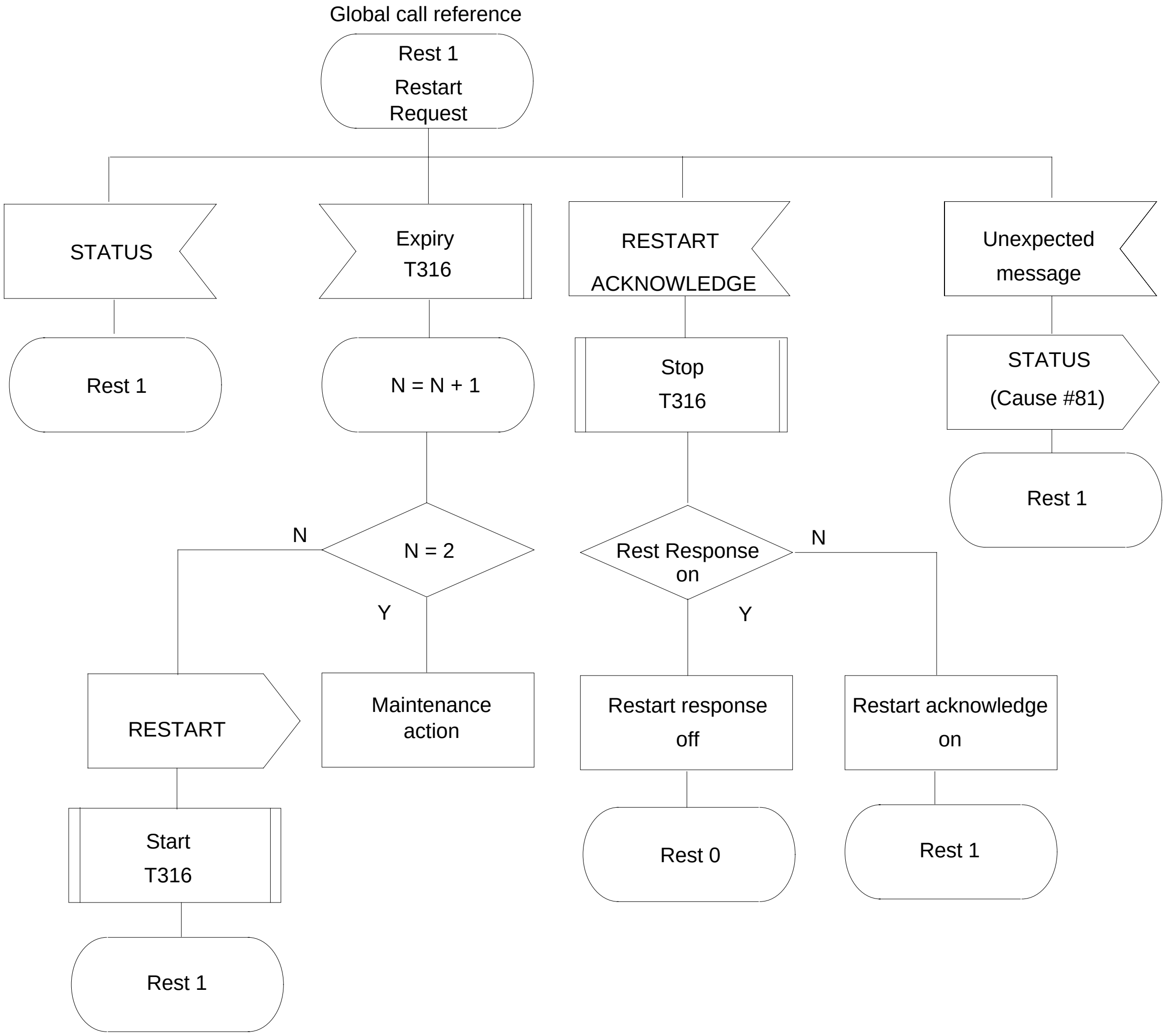


Figure 4-72
Detailed protocol control for the global call reference (3 of 4)

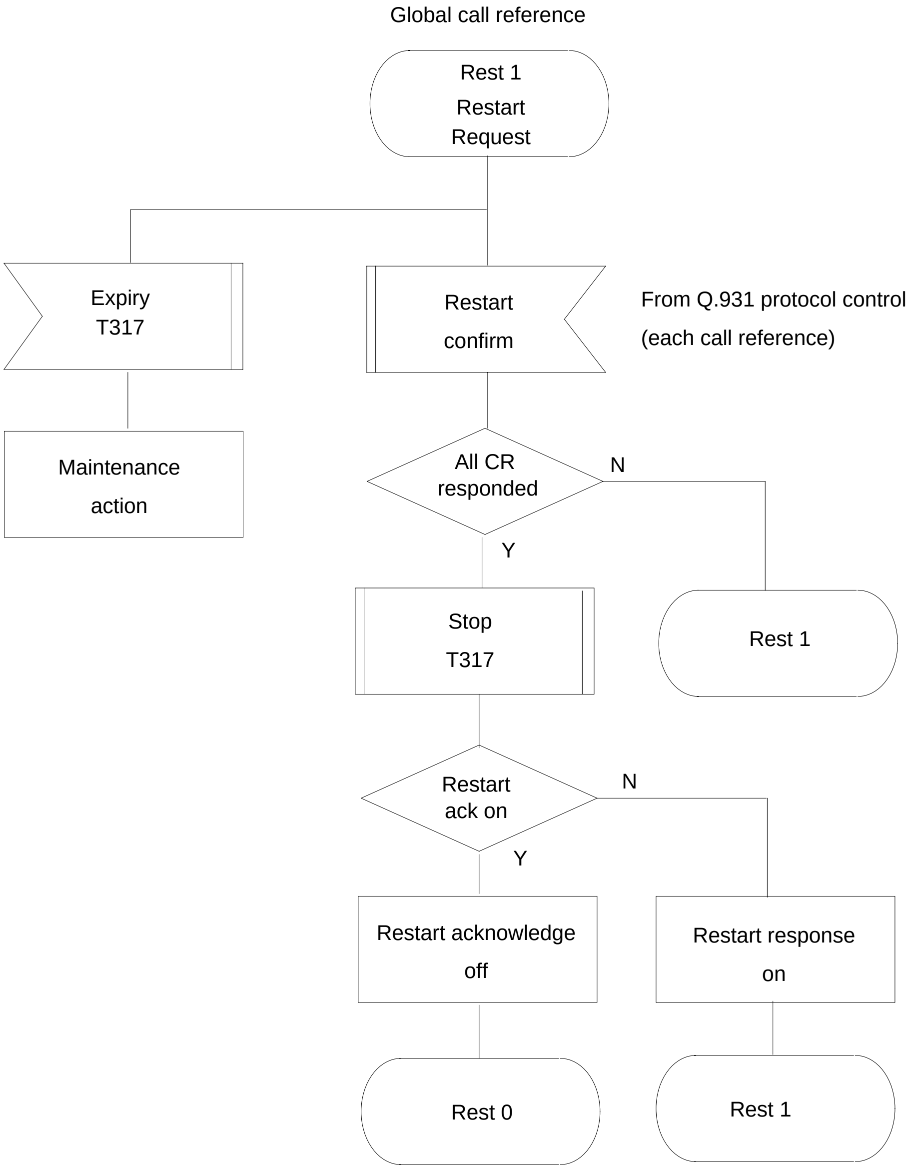


Figure 4-73
Detailed protocol control for the global call reference (4 of 4)

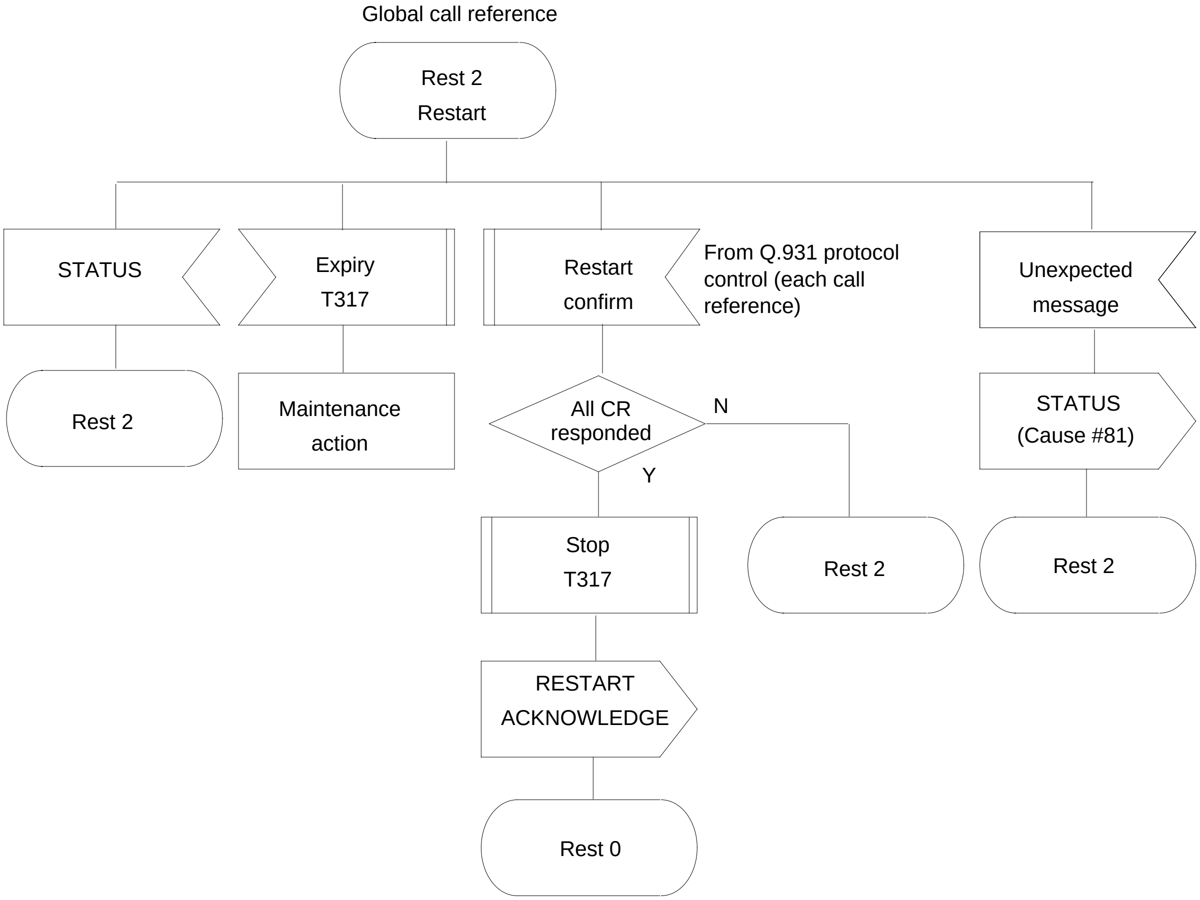


Figure 4-74
Overview protocol control: Network side (1 of 6)
Outgoing setup procedure (1 of 2)

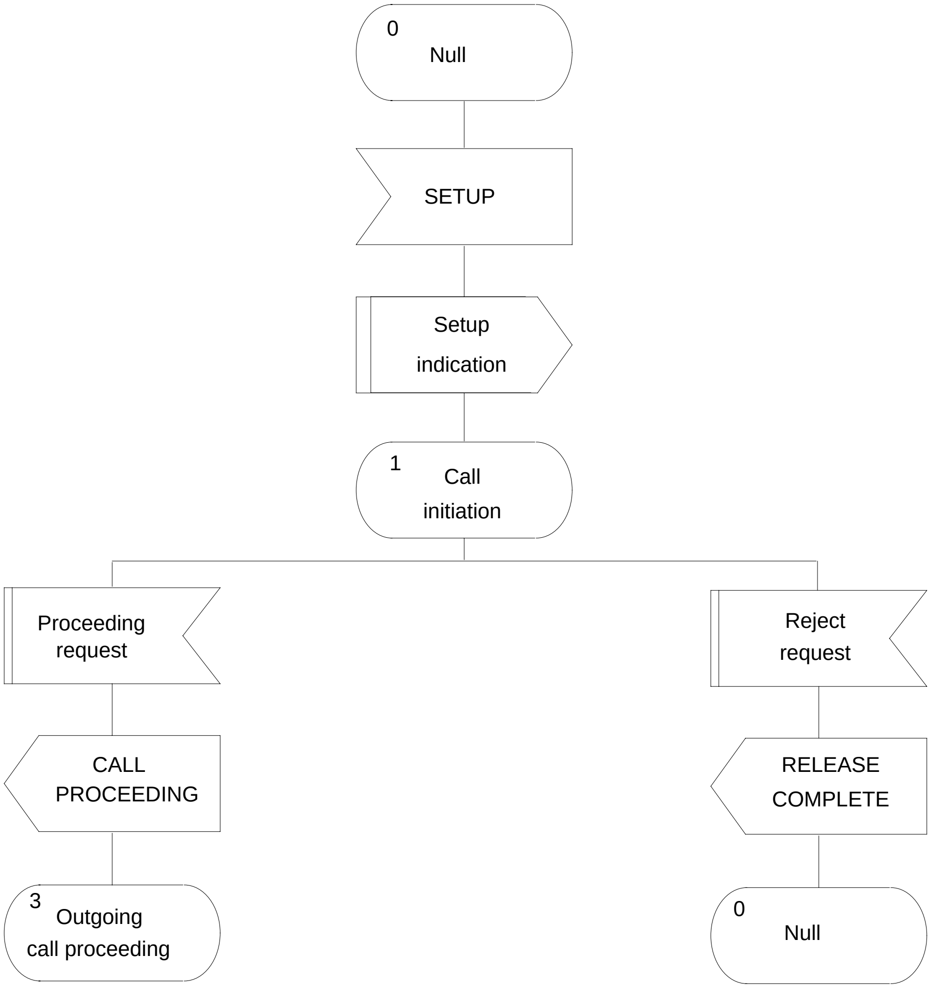


Figure 4-75
Overview protocol control: Network side (2 of 6)
Outgoing setup procedure (2 of 2)

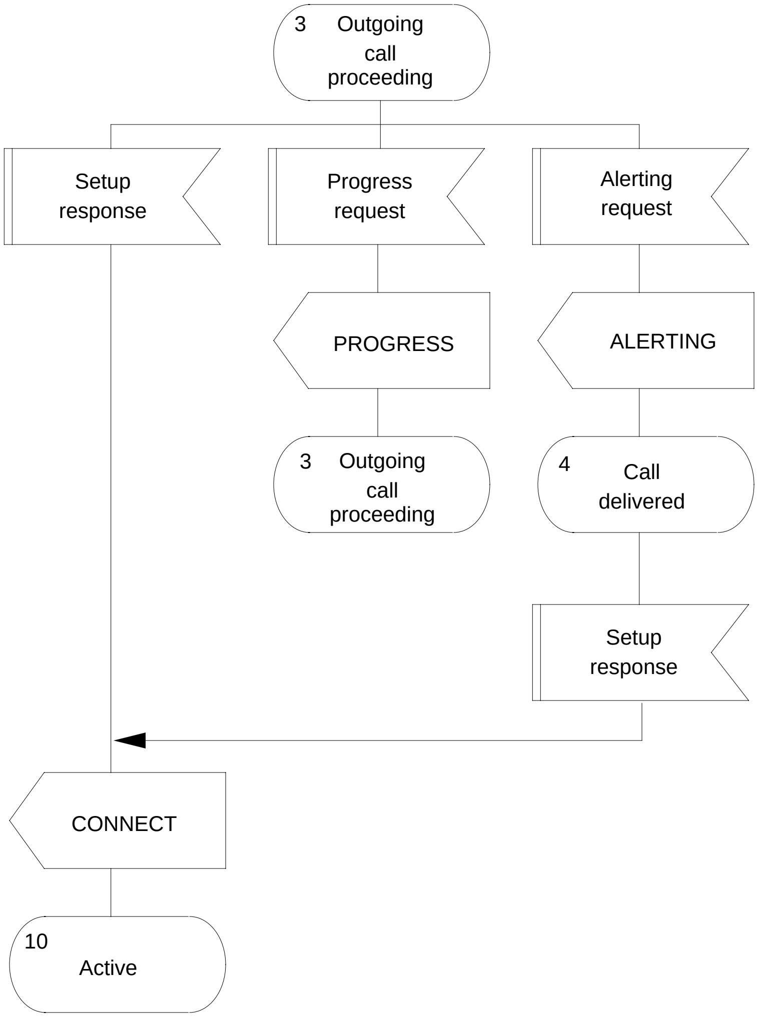


Figure 4-76
Overview protocol control: Network side (3 of 6)
Incoming setup procedure (1 of 2)

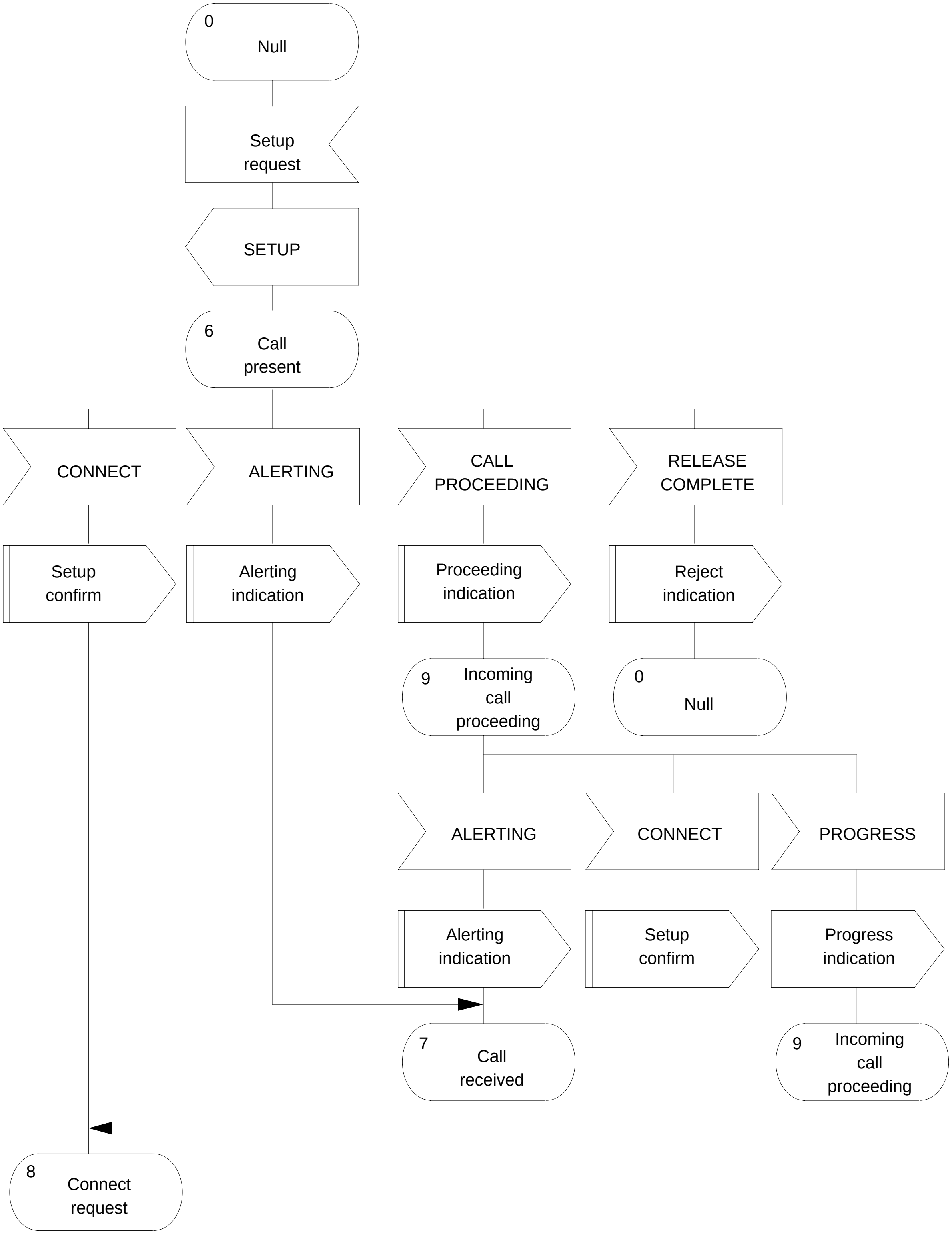


Figure 4-77
Overview protocol control: Network side (4 of 6)
Incoming setup procedure (2 of 2)

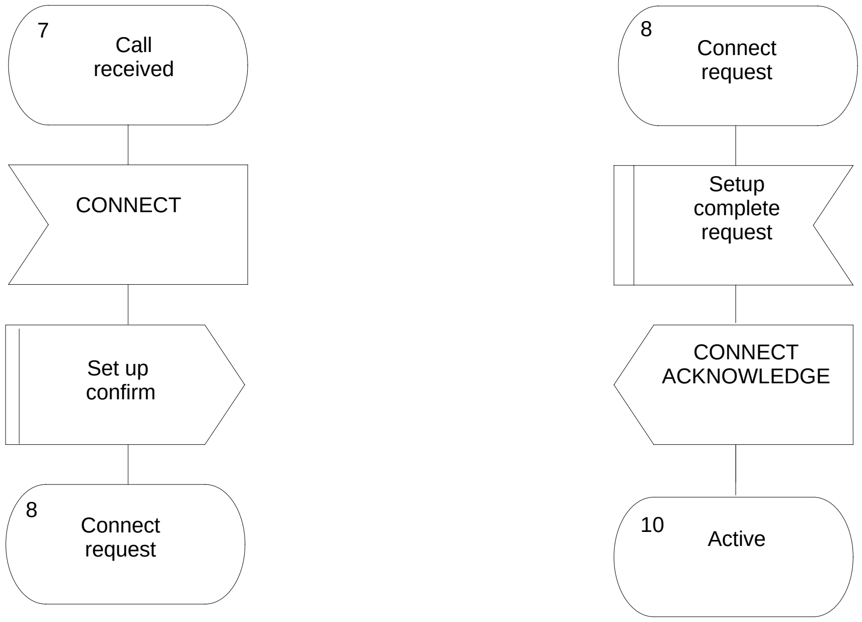


Figure 4-78
Overview protocol control: Network side (5 of 6)
Clearing procedure (1 of 2)

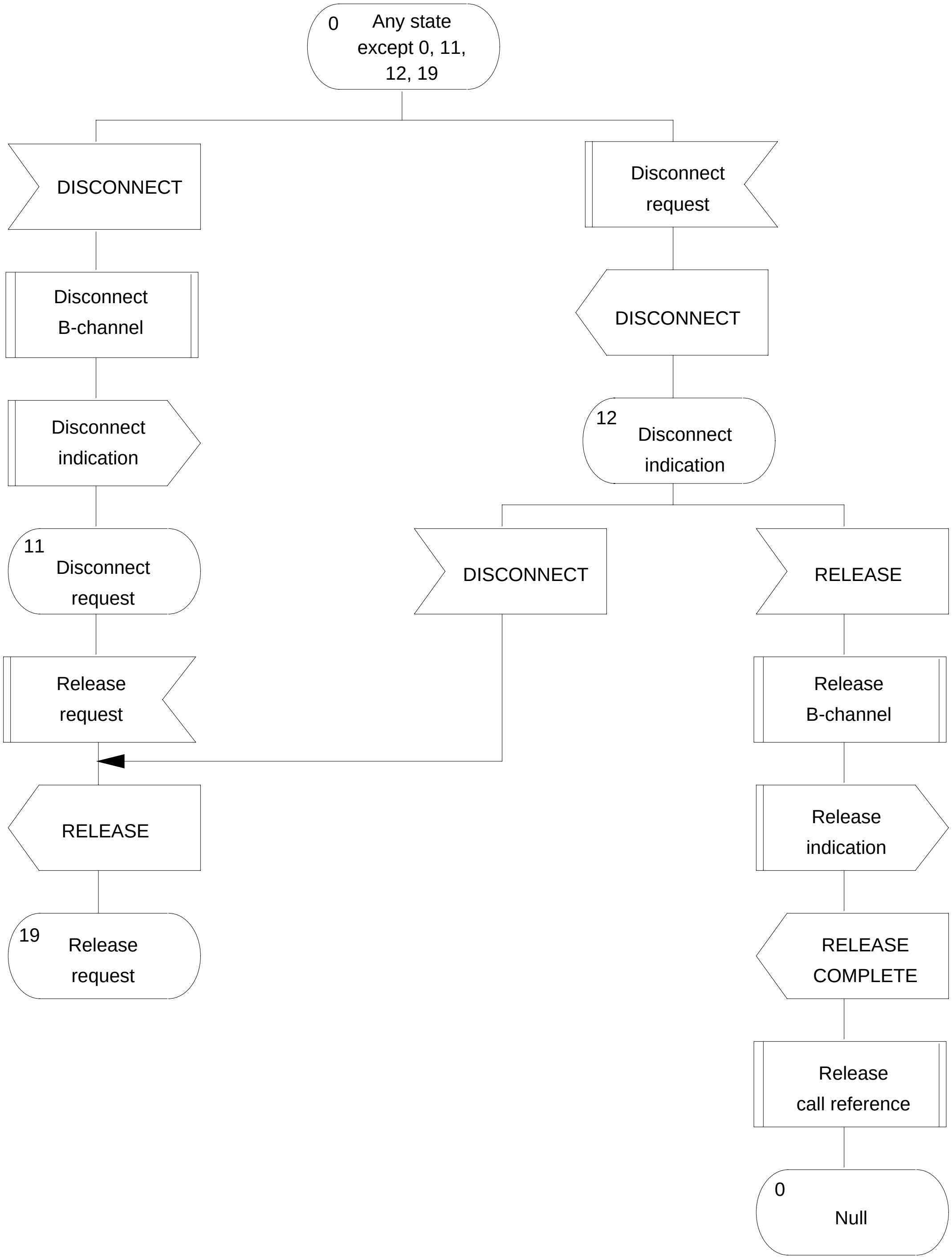


Figure 4-79
Overview protocol control: Network side (6 of 6)
Clearing procedure (2 of 2)

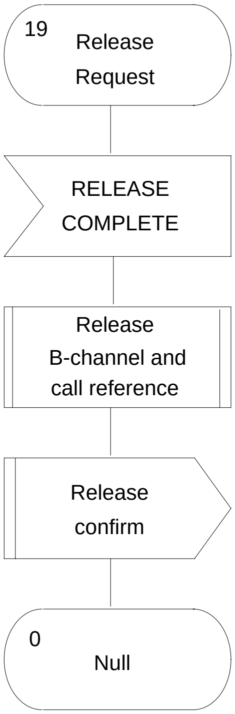


Figure 4-80
Detailed protocol control: Network side (1 of 18)

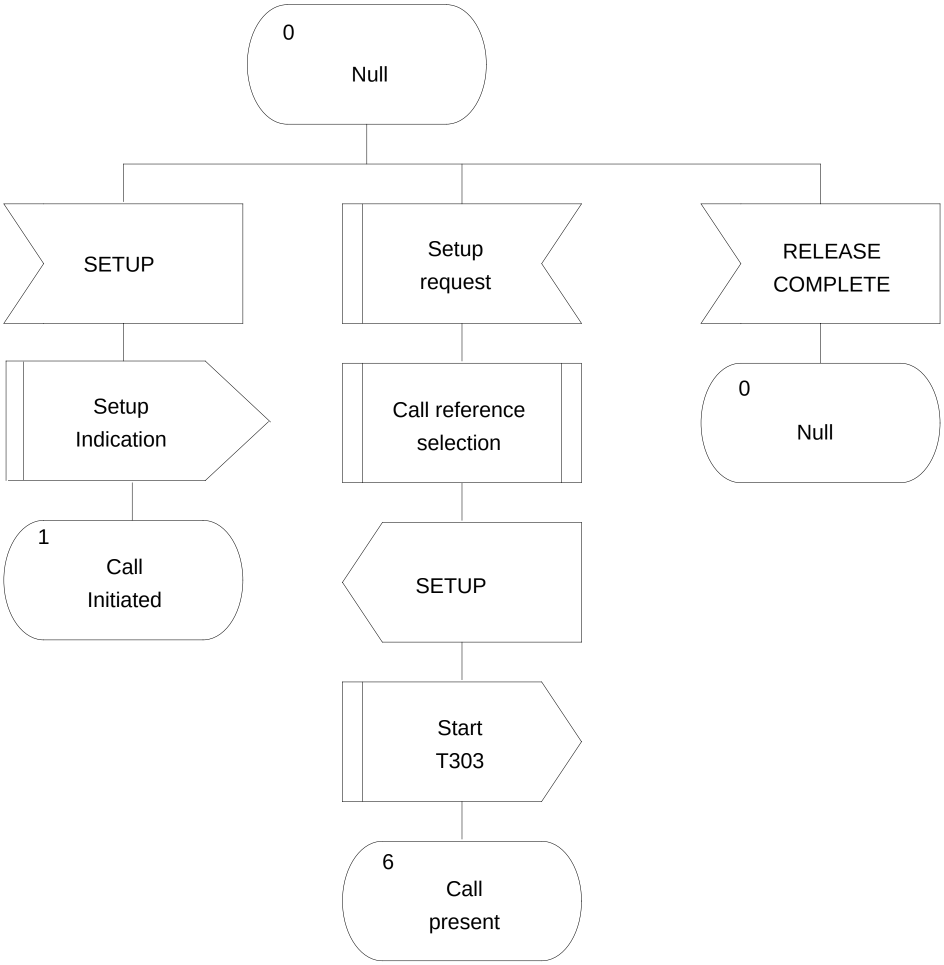


Figure 4-81
Detailed protocol control: Network side (2 of 18)

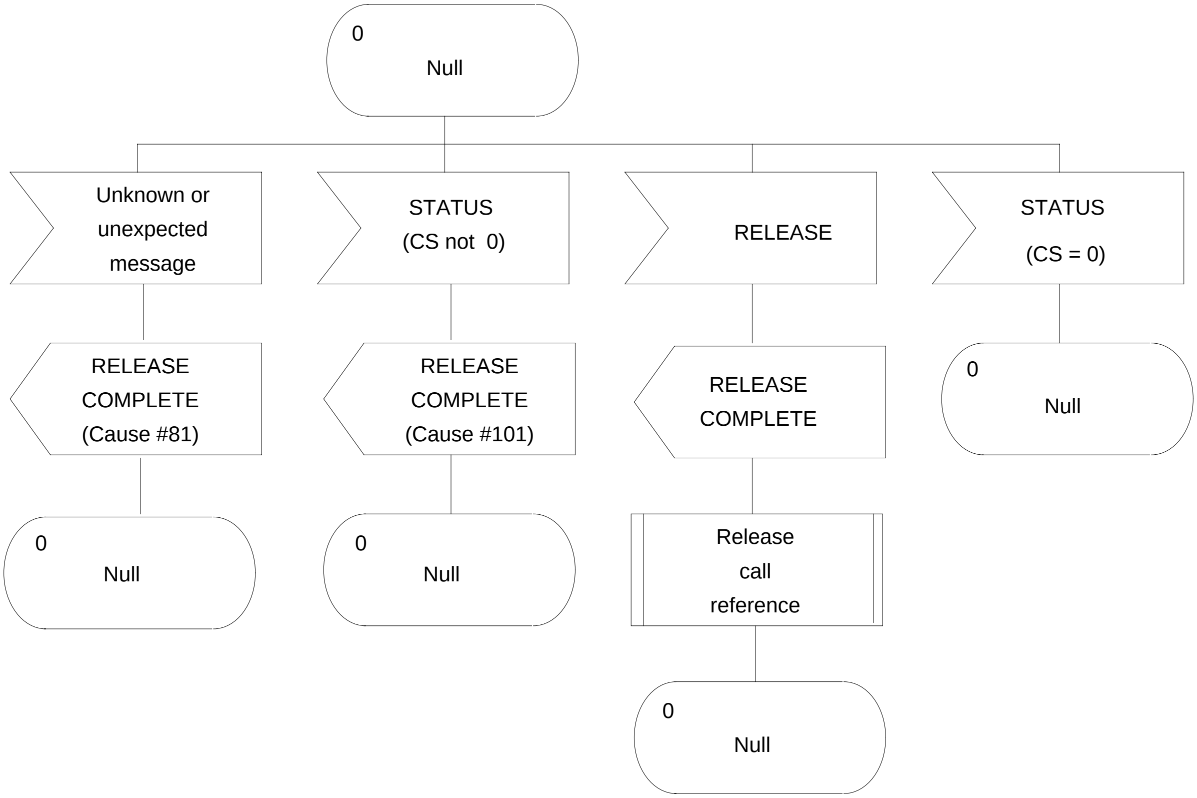


Figure 4-82
Detailed protocol control: Network side (3 of 18)

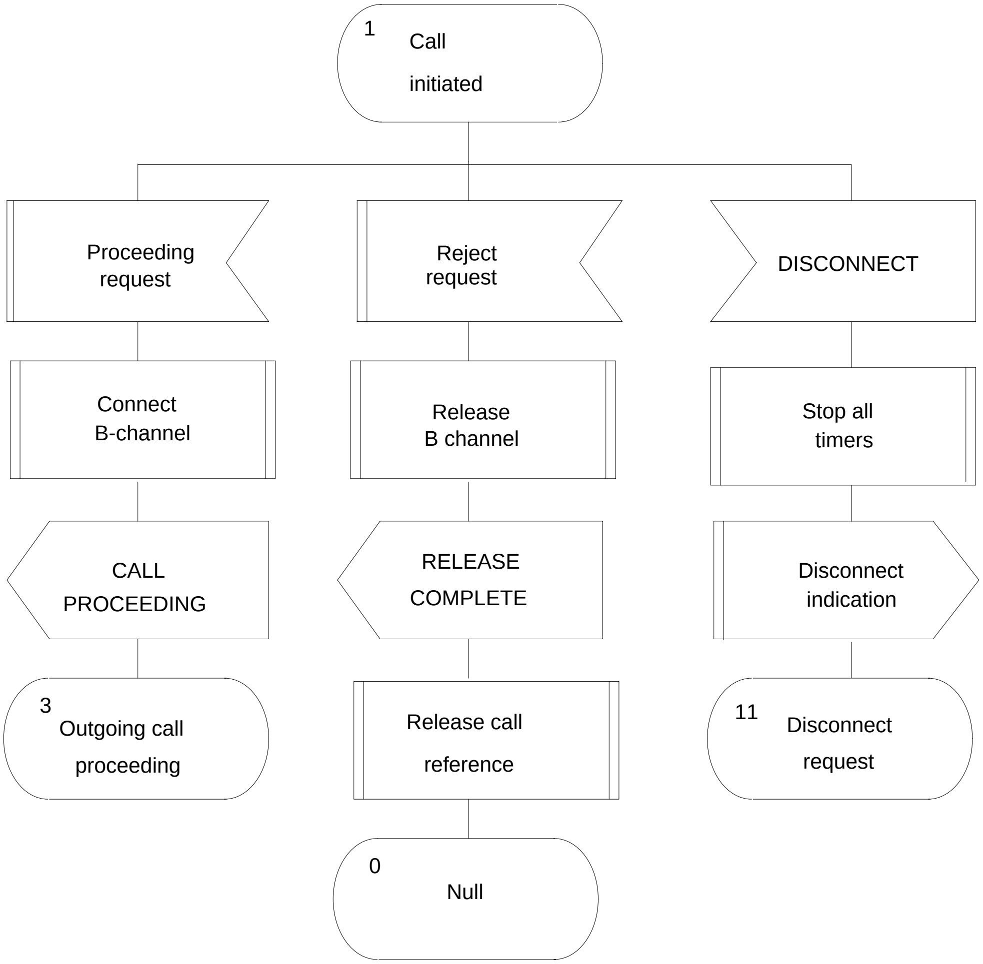


Figure 4-83
Detailed protocol control: Network side (4 of 18)

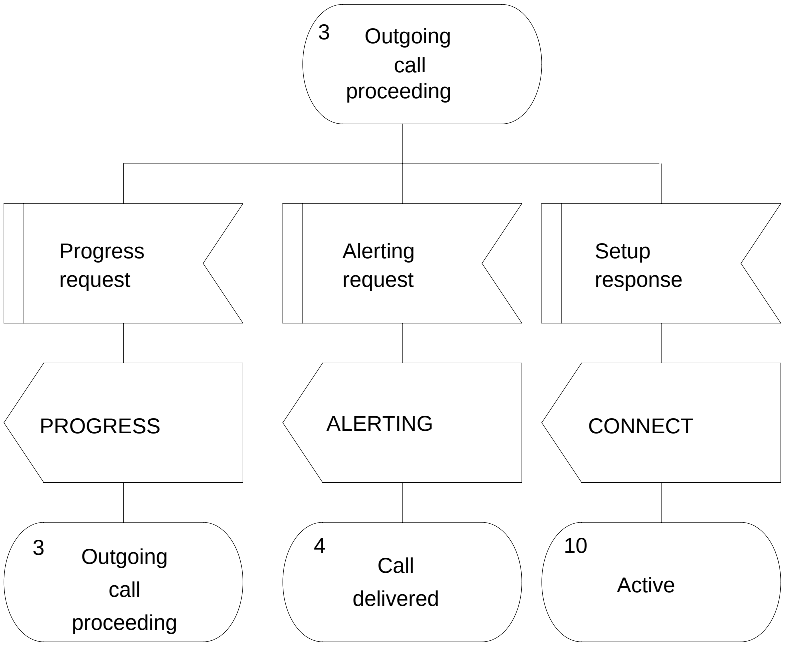


Figure 4-84
Detailed protocol control: Network side (5 of 18)

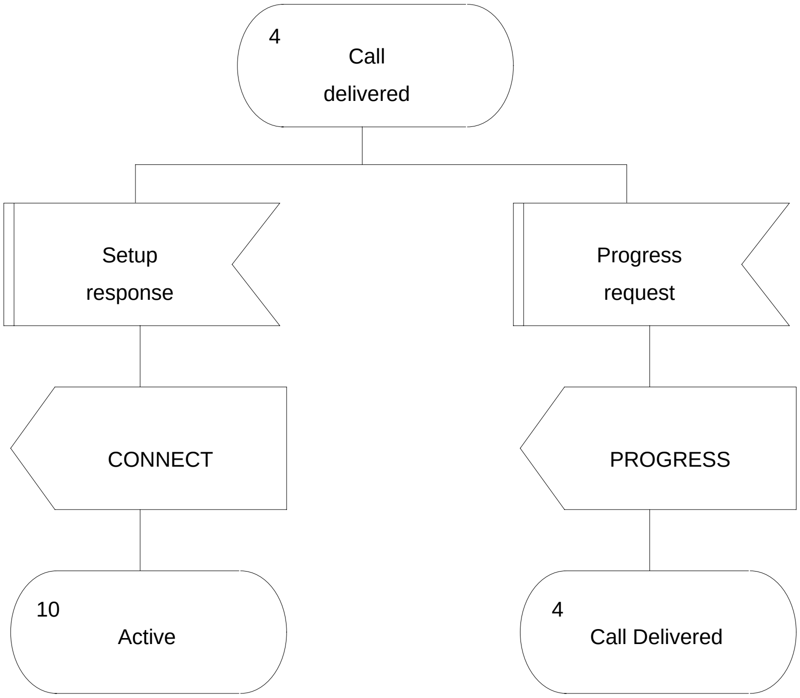


Figure 4-85
Detailed protocol control: Network side (6 of 18)

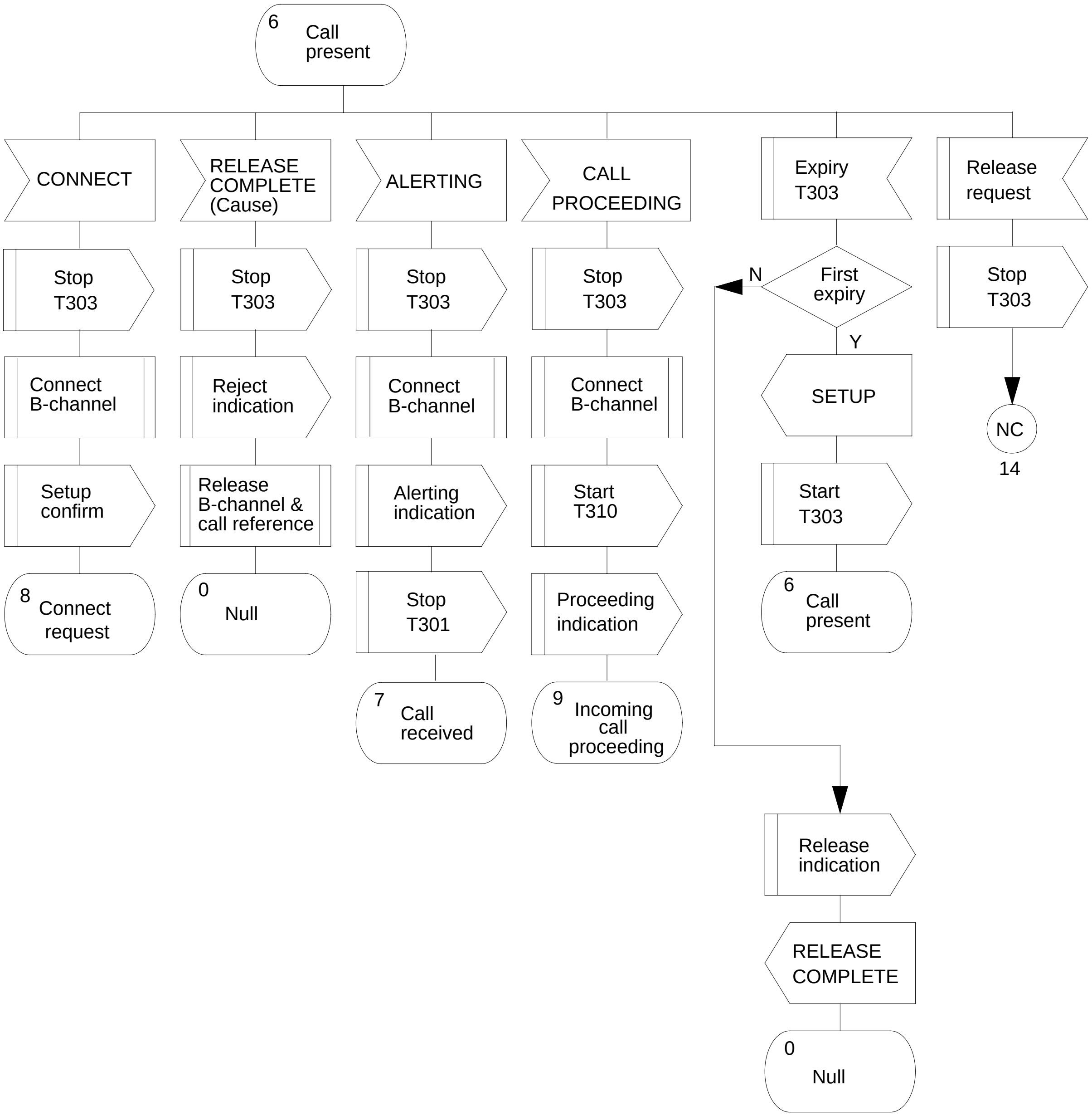


Figure 4-86
Detailed protocol control: Network side (7 of 18)

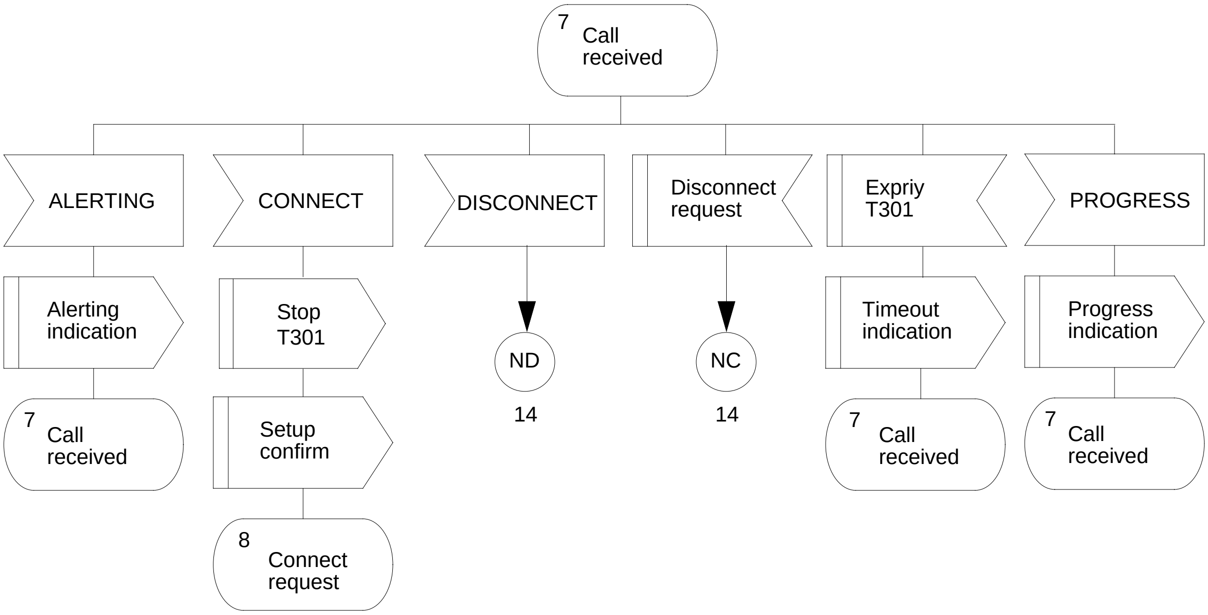


Figure 4-87
Detailed protocol control: Network side (8 of 18)

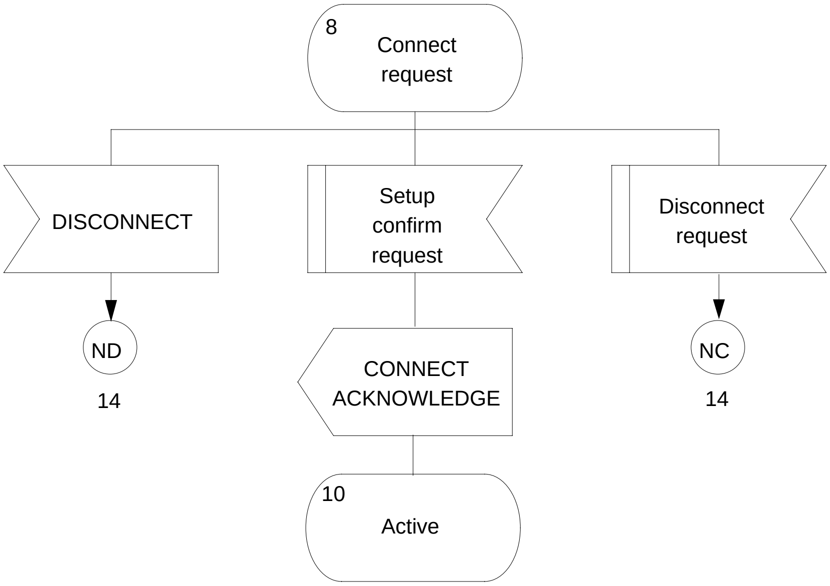


Figure 4-88
Detailed protocol control: Network side (9 of 18)

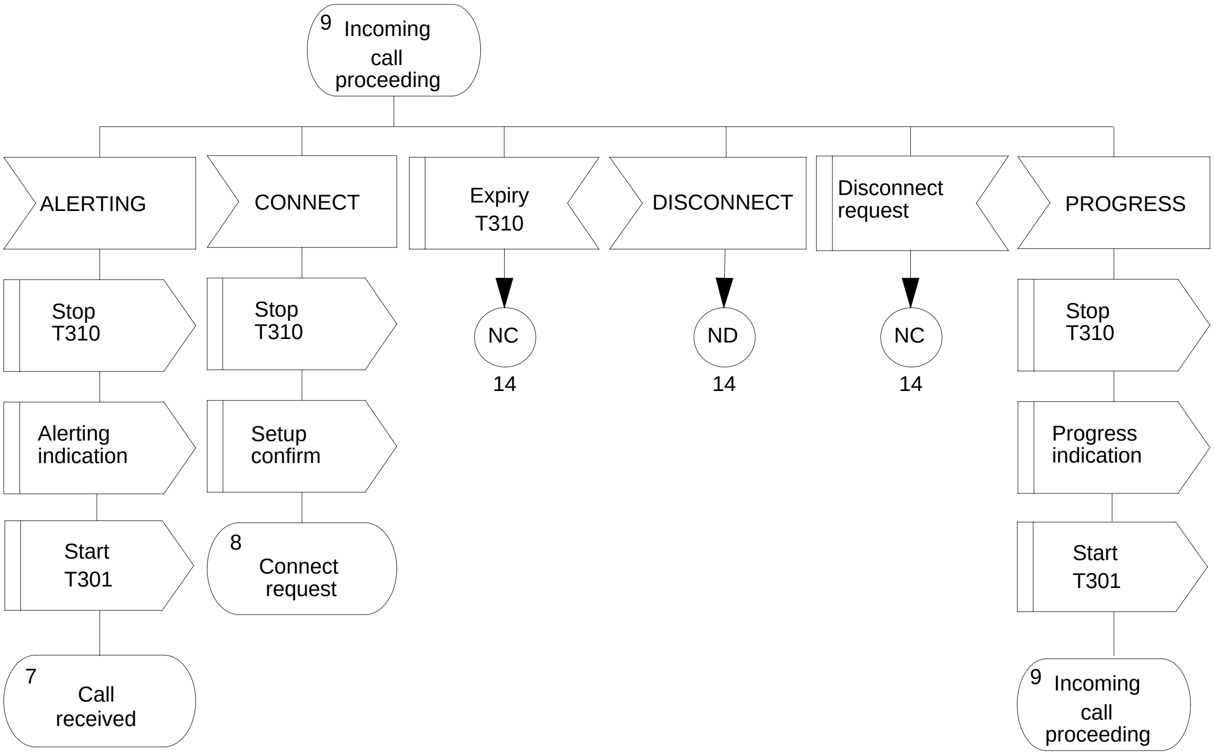


Figure 4-89
Detailed protocol control: Network side (10 of 18)

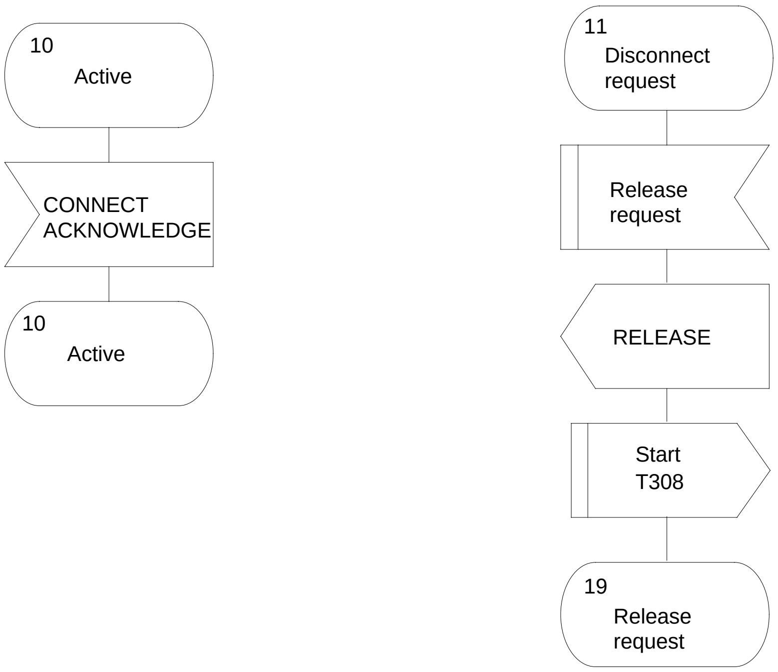


Figure 4-90
Detailed protocol control: Network side (11 of 18)

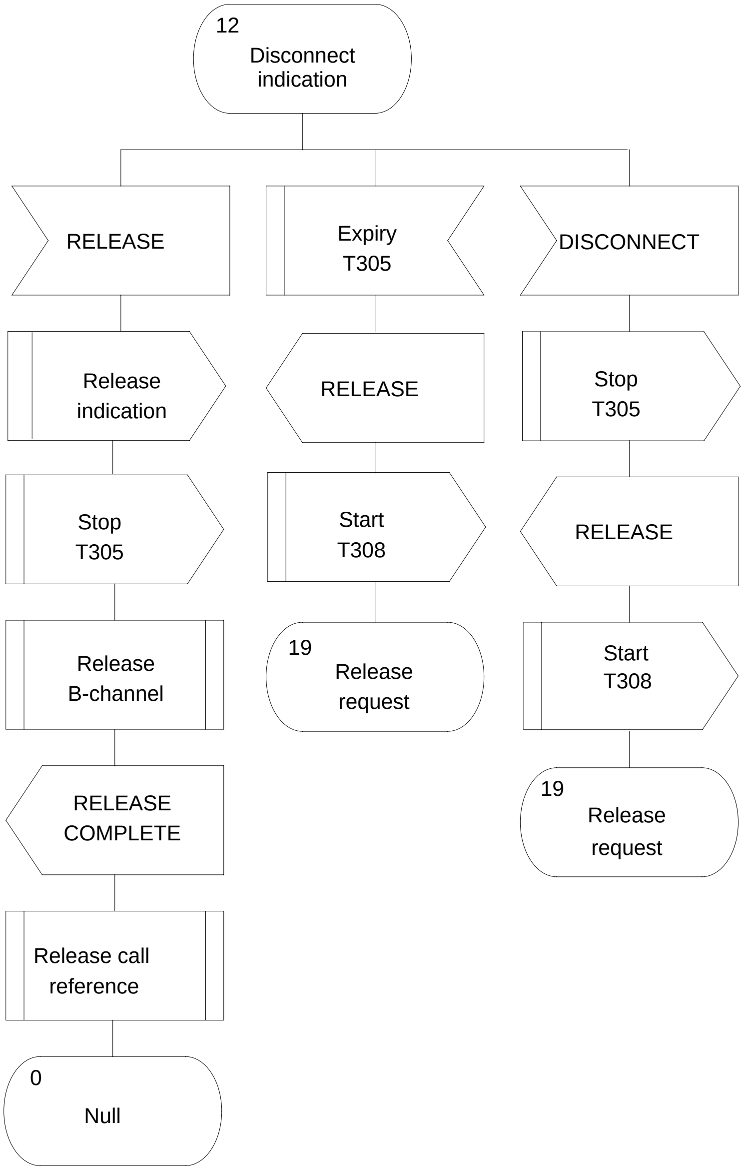


Figure 4-91
Detailed protocol control: Network side (12 of 18)

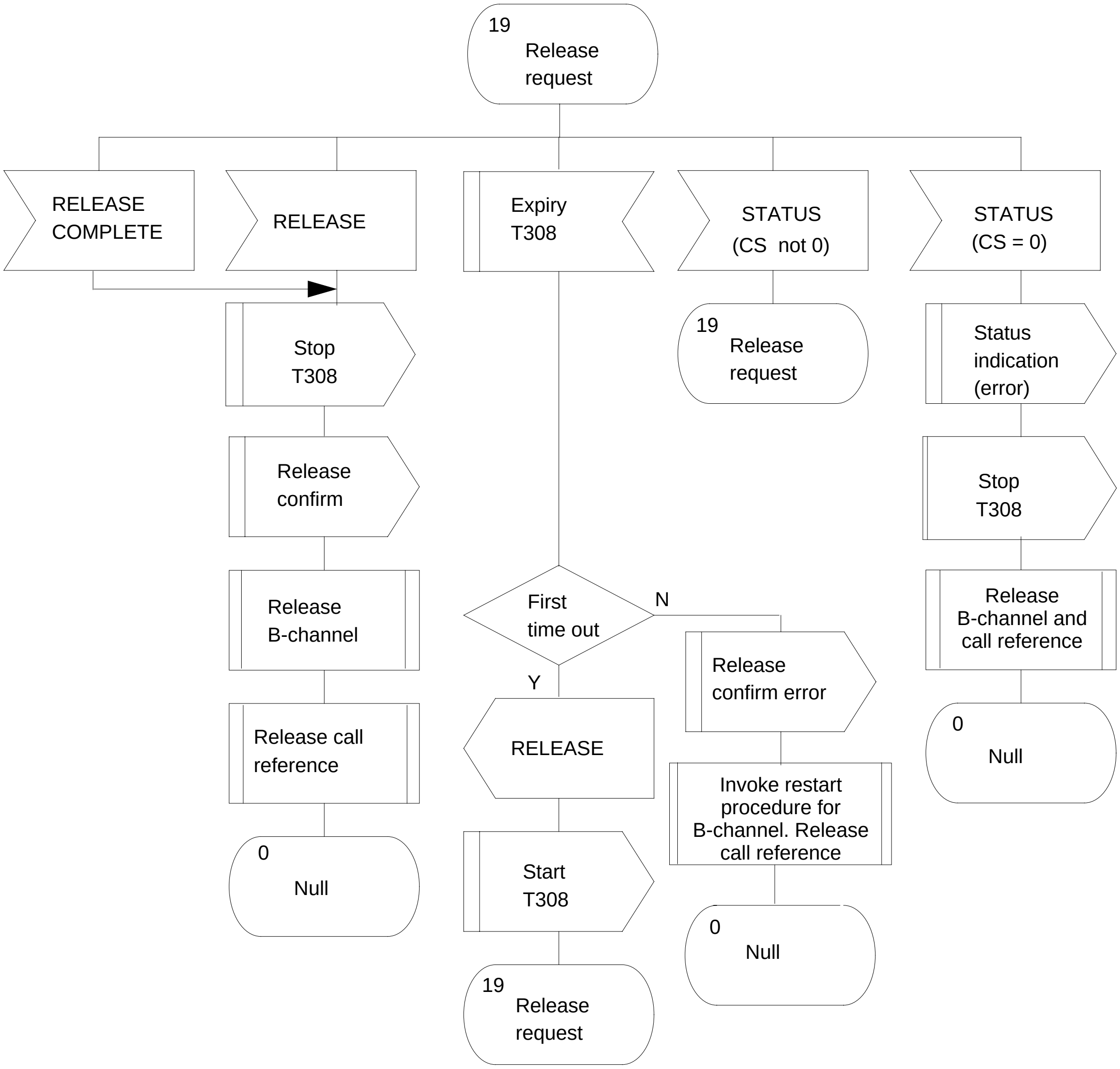


Figure 4-92
Detailed protocol control: Network side (13 of 18)

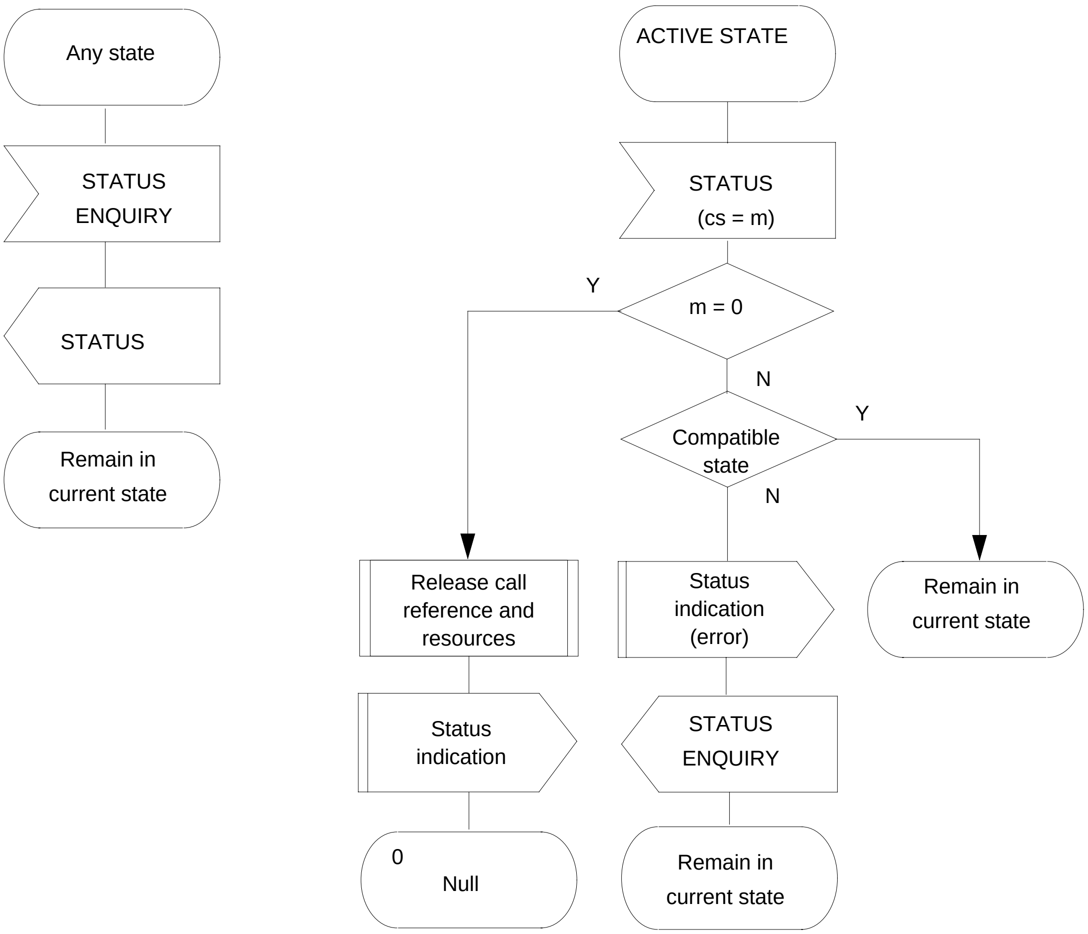


Figure 4-93 Detailed protocol control: Network side (14 of 18)

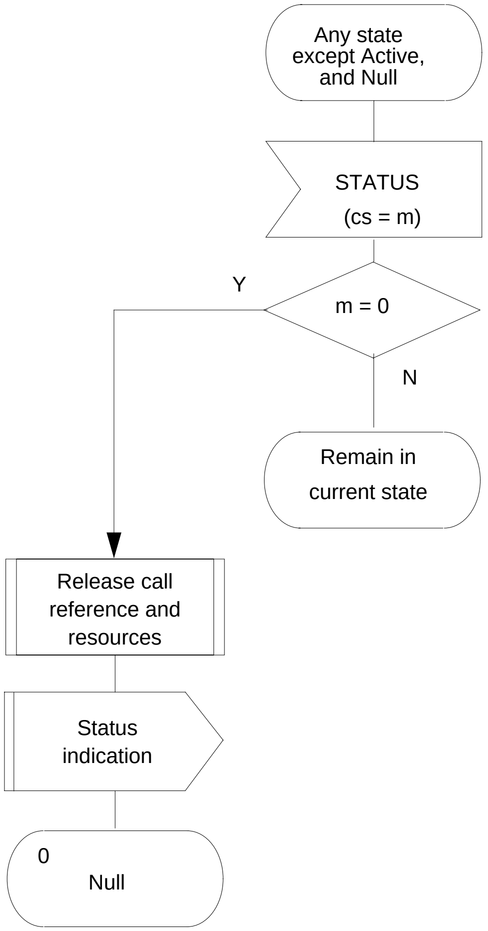


Figure 4-94
Detailed protocol control: Network side (15 of 18)

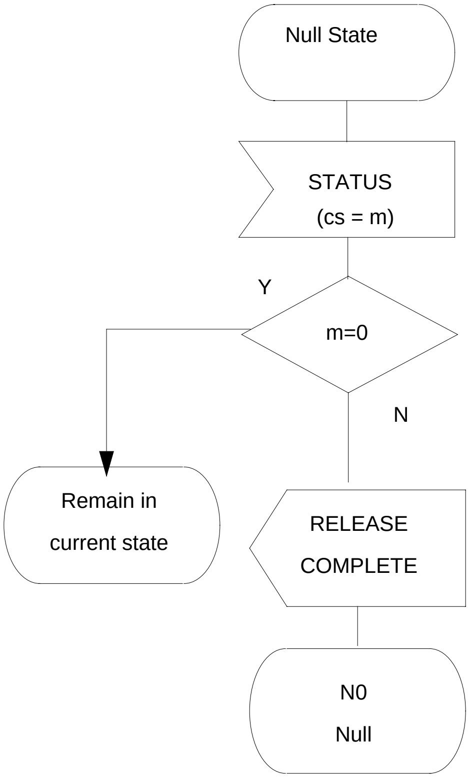


Figure 4-95
Detailed protocol control: Network side (16 of 18)

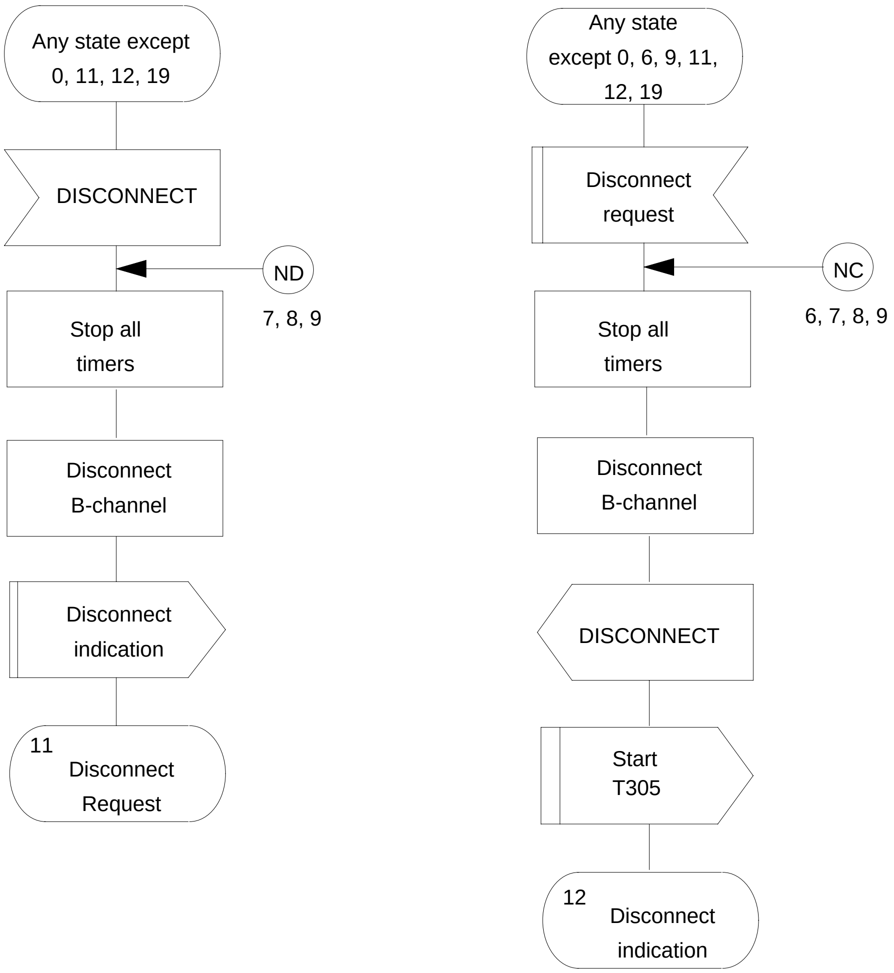
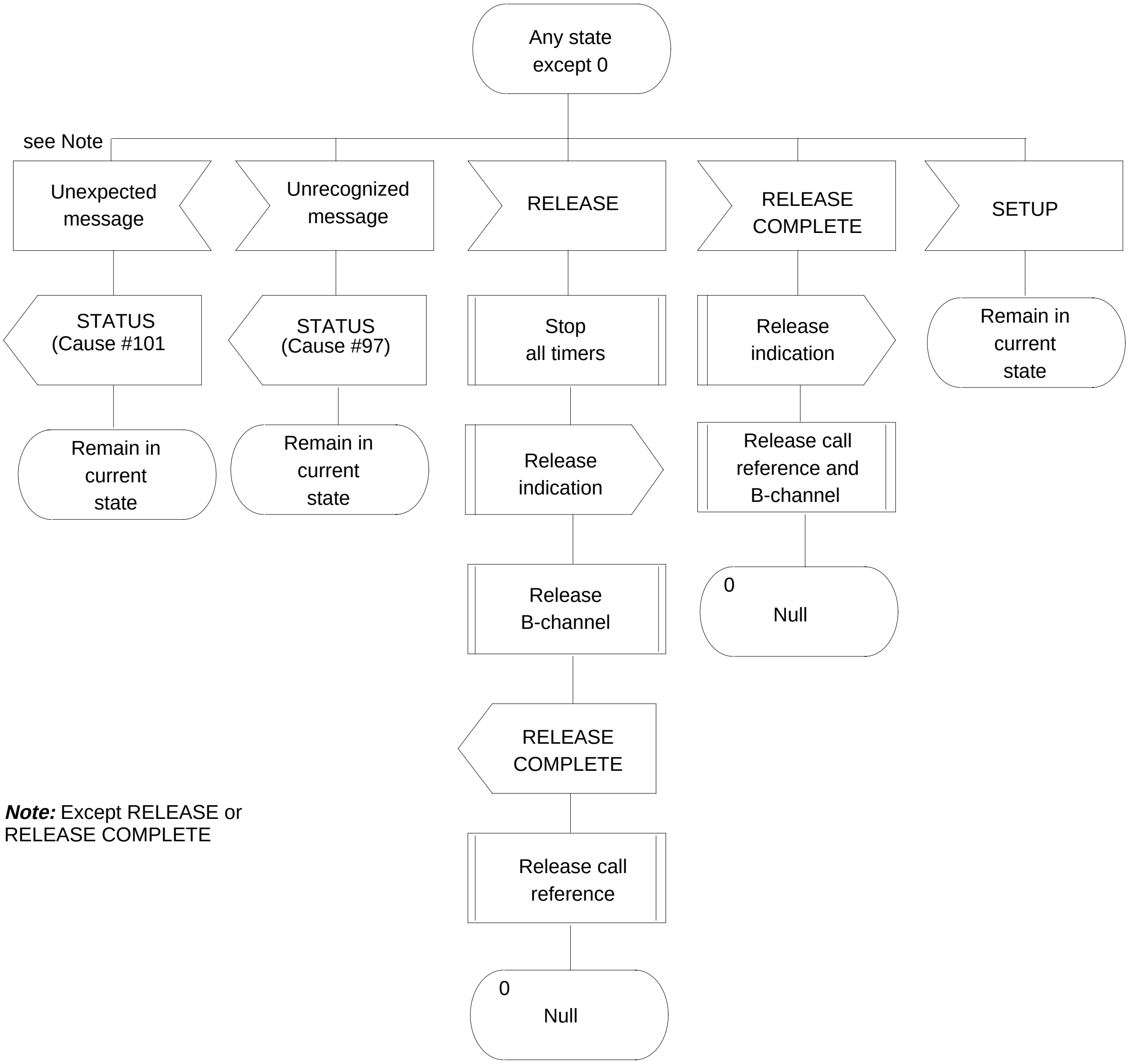
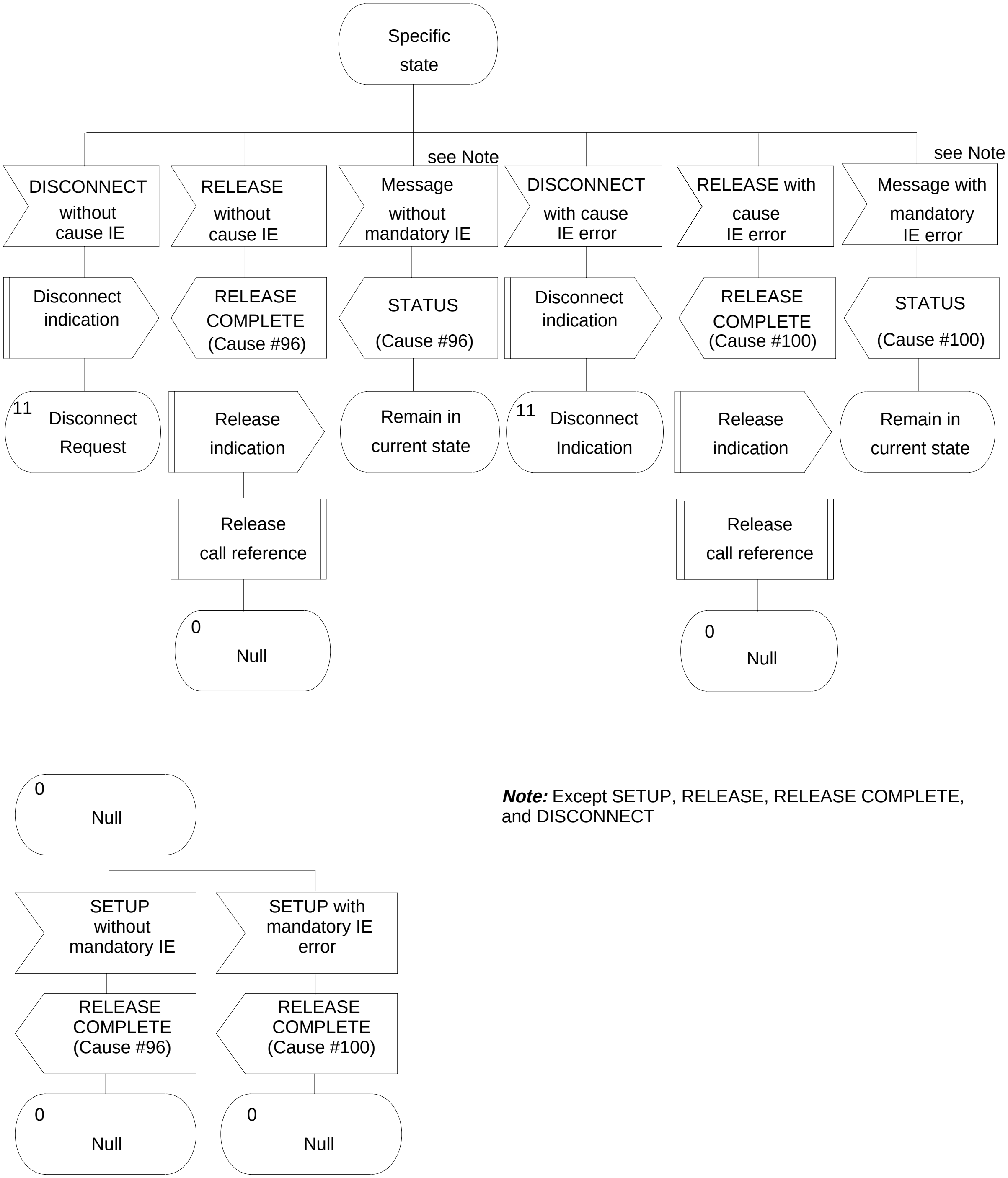


Figure 4-96
Detailed protocol control: Network side (17 of 18)



Note: Except RELEASE or RELEASE COMPLETE

Figure 4-97
Detailed protocol control: Network side (18 of 18)



Note: Except SETUP, RELEASE, RELEASE COMPLETE, and DISCONNECT

11.2 Annex B - Compatibility checking

11.2.1 Calling side compatibility checking

At the calling side, the network checks that the bearer service requested by the calling user in the *Bearer capability* information element matches the bearer services provided to that user by the network. If a mismatch is detected, the network rejects the call using one of the causes listed in section 5.1.4 on page 4-115.

11.2.2 Called side compatibility checking

When the network is providing a bearer service at the called side, the user checks that the bearer service offered by the network in the *Bearer capability* information element matches the bearer services that the user can support. If a mismatch is detected, the user either ignores the offered call or rejects it using *Cause* value #88 “Incompatible destination”.

11.3 Annex C - Transit network selection

The Transit Network Selection procedures are described in Section 5 of this specification.

11.4 Annex D - Extensions for symmetric call operation

Symmetric call operation, or peer-to-peer call operation, is 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 and Centrex-to-Centrex.

This Annex describes the user side procedures for symmetric call operation. The network side procedures remain unchanged. The procedures described in Chapter 4-5 for the user side are normally followed. Where additional procedures are required, they are described below.

11.4.1 Additional message handling

In symmetric applications, the *SETUP* message contains a *Channel identification* information element indicating a particular B-channel to be used for the call. A point-to-point data link is used to carry the *SETUP* message.

11.4.1.1 Call request

The initiator of the call follows the network side procedures described in section 5.2.1 on page 4-117, including the mandatory use of timer T303.

11.4.1.2 B-channel selection - symmetric interface

The *SETUP* message indicates one of the following channel selection alternatives

- channel is indicated, no acceptable alternative, or
- channel is indicated, any alternative is acceptable.

If the indicated channel is acceptable and available, the recipient of the *SETUP* message

- reserves it for the call
- sends a *CALL PROCEEDING* message, indicating the selected B-channel in a *Channel identification* information element
- enters the *Incoming Call Proceeding* state

> ***Note:*** If an *ALERTING* or a *CONNECT* message is received in response to a *SETUP* message, the call is not cleared. Although these are acceptable responses, a *CALL PROCEEDING* message is the recommended response to a *SETUP* message.

If the indicated B-channel is not acceptable or is unavailable, the recipient of the *SETUP* message

- sends a *RELEASE COMPLETE* message containing a *Cause* information element with the *Cause* value #44 “Requested circuit/channel not available”

- remains in the *Null* state.

If the channel indicated in a *CALL PROCEEDING* message is unacceptable to the initiator of the call, it clears the call in accordance with section 5.3 on page 4-122.

> ***Note:*** If an *ALERTING* or a *CONNECT* message is received in response to a *SETUP* message, the call is not cleared. Although these are acceptable responses, a *CALL PROCEEDING* message is the recommended response to a *SETUP* message.

11.4.1.3 Invalid call information

The recipient of a *SETUP* message follows the network side procedures described in section 5.1.3 on page 4-115.

11.4.1.4 Call confirmation

On receiving a *SETUP* message, the receiver enters the *Call Present* state. Valid responses to the *SETUP* message are a *CALL PROCEEDING* or a *RELEASE COMPLETE* message.

> ***Note:*** If an *ALERTING* or a *CONNECT* message is received in response to a *SETUP* message, the call is not cleared. Although these are acceptable responses, a *CALL PROCEEDING* message is the recommended response to a *SETUP* message.

Receipt of Call Proceeding and Alerting

The initiator of a call follows the network side procedures described in section 5.2.4.2 on page 4-119.

Clearing during incoming call establishment

The initiator of a call follows the network side procedures described in section 5.2.4.3 on page 4-119.

Call failure

The initiator of a call follows the network side procedures described in section 5.2.4.4 on page 4-120.

11.4.1.5 Clearing by the called user employing user-provided tones and announcements

When tones or announcements are provided in conjunction with call clearing, the node providing the in-band treatment sends a *PROGRESS* message.

11.4.1.6 Active indication

Upon receipt of a *CONNECT* message, the initiator of the call responds with a *CONNECT ACKNOWLEDGE* message and enter the *Active* state (see the network side procedures in section 5.2.7 on page 4-121).

11.4.1.7 Normal call clearing

The recipient of a *DISCONNECT* message follows the network side procedures described in section 5.3.3 on page 4-122.

11.4.2 Timers for call establishment

The optional user side timers described in Table 3-40 on page 4-164 are implemented, including the associated procedures described in Chapter 4-5 for actions on timer expiry.

11.5 Annex E - Network specific facility selection

These procedures are in Section 5 of this specification, in the description of Integrated Services Access.

11.6 Annex F - Backup D-channel service

The Backup D-Channel service is optional for PRI configurations which consist of more than one DS-1 interface. That is, configurations where the D-channel supports call control signaling for channels on a DS-1 other than that which contains the D-channel (or, non-facility associated signaling).

The Backup D-Channel service increases PRI reliability by automatically moving Layer 3 signaling to a standby D-channel when the DS-1 containing the active (that is, In Service) D-Channel fails. For this reason, both designated D-channels must be provisioned on different DS-1 interfaces.

Switching between D-channels can also be initiated by manual intervention. This may be done, for example, when the DS-1 interface with the active D-channel is to be removed from service temporarily for maintenance.

The procedures in this annex are supplemental to those described in Chapter 4-7: D-channel maintenance, which describes maintenance procedures for PRI configurations with a single D-channel.

11.6.1 D-channel states

In order of decreasing availability, the allowed D-channel states are defined below. Only those states which are not defined for single D-channel maintenance procedures are fully defined here.

IS	In Service
WAIT	Wait. In this state the maintenance entity has initiated moving the D-channel to the IS state and is waiting for confirmation from the other end of the interface.
STBY	Standby. The D-channel is available for transfer of Layer 3 messages, but the other D-channel is currently in the IS state.
OOS	Out Of Service
MB	Maintenance Busy. In addition to its use for single D-channel maintenance, the MB state is also used by Backup D-channel service procedures.
MOOS	Manual Out Of Service
INB	Installation Busy

In addition to the above states, the D-channel on the lowest numbered DS-1 interface is labelled the “primary” D-channel (D1) and the other is the “secondary” D-channel (D2). In the procedures which follow, the states of the two D-channels are often indicated in the format “(D1 state, D2 state)”. For example, (IS,STBY).

Only one D-channel can be in the IS state at any one time. In these procedures, the D-channel in the IS state is also referred to as the “in service” or “active” D-channel. The D-channel which is not in the IS state is not available for user data, for example, it can not serve as a B-channel.

11.6.2 Timers

The following timers are defined for use by Backup D-channel service. These timers are only described where they differ in use from single D-channel maintenance, or only apply to Backup D-channel service.

T3DW	
T3MB	This timer is used to guard against the far end attempting to activate a failed D-channel while the near end is attempting to activate the backup D-channel.
T321	This timer is the maximum amount of time that Layer 3 waits for a response to a *SERVICE* message. The value of this timer in the network is 40 seconds. The value of this timer on the user side is not critical but is recommended to be the same value as in the network.

11.6.3 Protocol

The procedures in this annex use the *SERVICE* and *SERVICE ACKNOWLEDGE* messages. These messages are defined in Section 3 of this specification.

The global call reference is used for all *SERVICE* and *SERVICE ACKNOWLEDGE* messages.

The *Channel identification* information element is described in Section 3 of this specification. Coding of this information element for Backup D-channel procedures follows

- Interface Identifier Present field is set to “Explicit interface identification” or “Implicit interface identification”, as appropriate
- Interface Type field is set to “Primary rate interface”
- Preferred/Exclusive field is not used, and is ignored if received
- D-channel Indicator field is set to “Channel identified is the D-channel”
- Information Channel Selection field is set to “No channel” and is ignored if received.

- Interface Identifier field must be set (present only if the interface is explicitly identified).

The *Change status* information element is coded as follows

- Preference field set to “Channel”
- New Status field set to “In service”

Incorrectly coded *SERVICE* and *SERVICE ACKNOWLEDGE* messages received from the far end are ignored.

11.6.4 Procedures

The procedures for Backup D-channel service differ from those for single D-channel maintenance as follows

- automatically move a backup D-channel to the IS state when the active D-channel fails
- additional Layer 3 maintenance procedures are needed to make a D-channel available for service after Layer 2 is successfully established
- resolution of race conditions when both D-channels are simultaneously available for service

In the majority of cases, the procedures in the following sections work symmetrically for both D1 and D2. In cases where symmetry does not apply, it is explicitly stated.

11.6.4.1 Service changes

Service changes can only be made when the D-channels are in the (INB,INB) states. Please refer to section 7.3.2 on page 4-150 for further details.

11.6.4.2 Establishing an In Service D-channel

The procedures in section 7.3.3 on page 4-151 are followed except where modified below.

Layer 2 establishment begins when one or both D-channels are moved from the MOOS to the OOS state. If both D-channels are moved from MOOS to OOS at the same time, the network initiates Layer 2 establishment on D1 shortly before D2 in order to preferentially establish Layer 3 on D1.

When Layer 2 is established on a D-channel, and the other D-channel is not in the IS, WAIT or STBY state, Layer 3 establishment begins. This requires coordination with the far end of the interface to agree on which D-channel will be used for Layer 3. To accomplish this coordination, Layer 3

- sends a *SERVICE* message on the D-channel, containing a *Change status* information element with a New Status of “In service”
- starts timer T321

- moves the D-channel to the WAIT state

If a *SERVICE* or *SERVICE ACKNOWLEDGE* message containing a *Change status* information element with a New Status of “In Service” is received on the waiting D-channel before timer T321 expires, Layer 3

- stops timer T321
- if the other D-channel is in the MB state, Layer 3
  - — stops timer T3MB for the other D-channel
  - — moves the other D-channel to the OOS state
  - — attempts to establish Layer 2 on the other D-channel following the procedures in section 11.6.4.3 on page 4-228
- if the message received on the waiting D-channel is *SERVICE*, a *SERVICE ACKNOWLEDGE* message is sent containing a *Change status* information element with a New Status of “In service”
- initiates and waits for successful completion of an all interface restart (see section 5.7 on page 4-132)
- stops timer T309, if it is running
- moves the D-channel to the IS state, thus making it the active D-channel

If timer T3MB for the failed D-channel expires, while the waiting D-channel is in the WAIT state, the failed D-channel is moved to the OOS state in an attempt to re-establish Layer 2, following the procedures in section 11.6.4.3 on page 4-228. If Layer 2 is successfully established, the previously failed D-channel is moved to the STBY state.

If timer T321 expires or a *DL-Release-Indication* primitive is received from Layer 2 for the waiting D-channel, it is declared as having failed and the procedures in section 11.6.4.3 on page 4-228 are followed.

11.6.4.3 Layer 3 failure

Layer 3 failure on either D-channel occurs when Layer 3 receives a *DL-Release-Indication* primitive from Layer 2, or Layer 3 receives a failure indication from Layer 1. This is potentially service-affecting when the failure occurs on an in-service D-channel.

If a D-channel failure occurs when it is in the IS or WAIT state, Layer 3

- stops timer T321, if it is running
- clears all calls which are not in the *Active* state, following the procedures in section 5.9.9 on page 4-141
- starts timer T309, if any calls are in the *Active* state and the timer is not already running

If the failed D-channel is in the IS or WAIT state and the backup D-channel is in the STBY or OOS state, Layer 3

- starts timer T3MB for the failed D-channel
- moves the failed D-channel to the MB state
- if the backup D-channel is in the STBY state, the procedures in section 11.6.4.5 on page 4-229 are followed

If the backup D-channel is not in either the STBY or OOS state, or when timer T3MB on the failed D-channel expires, Layer 3

- sends a *DL-Establish-Request* primitive to Layer 2 on the failed D-channel
- starts timer T3DW for the failed D-channel
- moves the failed D-channel to the OOS state

11.6.4.4 Layer 3 removal

Layer 3 can be removed from service by manual intervention to move one or both D-channels to the MOOS state, following the procedures in section 7.3.5 on page 4-152. If this occurs when the D-channel is in the IS or WAIT state and the other D-channel is in the STBY state, the procedures in section 11.6.4.5 are followed.

11.6.4.5 D-channel switch-over

The active D-channel can be changed from D1 to D2, or vice versa, when initiated by one of the following actions

- automatically, on detection of failure of the active D-channel, that is, receipt of a *DL-Release-Indication* primitive from Layer 2 (see section 11.6.4.3 on page 4-228)
- automatically, on receiving a *SERVICE* message on the backup D-channel, which must be in the STBY state, containing a *Change status* information element with a New Status of “In service”
- by manual intervention (see section 11.6.4.4 on page 4-229)

If switch-over is initiated by receipt of a *SERVICE* message on the backup D-channel, and the backup D-channel is D1, that is (STBY,IS), the maintenance entity

- sends a *SERVICE ACKNOWLEDGE* message on D1, containing a *Change status* information element with a New Status of “In service”
- starts timer T3MB for D2
- moves the D-channel states to (IS,MB)

A *SERVICE* message received on D2 is ignored when it is the backup D-channel.

If a *SERVICE* message is received on an in-service D-channel containing a *Change status* information element with a New Status of “In service”, Layer 3 sends a *SERVICE ACKNOWLEDGE* message to the far end, but no other action is taken.

When the backup D-channel is in the STBY state, it is only necessary to establish Layer 3, following the procedures in section 11.6.4.2 on page 4-227. Layer 2 is already established.

11.7 Annex G - Cause definitions

The following list contains definitions for each of the causes values used in this specification.

Normal class

- Cause 1 - Unallocated (Unassigned) Number

  This cause indicates that the destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned (allocated).

- Cause 2 - No route to specified transit network

  This cause indicates that the equipment sending this cause has received a request to route the call through a particular transit network which it does not recognize. The equipment sending this cause does not recognize the transit network either because the transit network does not exist or because that particular transit network, while it does exist, does not serve the equipment which is sending this cause.

- Cause 3 - No route to destination

  This cause indicates that the called user cannot be reached because the network through which the call has been routed does not serve the destination desired.

- Cause 6 - Channel unacceptable

  This cause indicates the channel most recently identified is not acceptable to the sending entity for use in this call.

- Cause 16 - Normal call clearing

  This cause indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared.

- Cause 17 - User busy

  This cause is used when the called user is unable to accept another call because another call or calls is occupying the resources required to handle the new call.

- Cause 18 - No user responding

  This cause is used when a user does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated.

- Cause 19 - No answer from user (user alerted)

  This cause is used when a user has provided an alerting indication but has not provided a connect indication within a prescribed period of time.

- Cause 21 - Call rejected

  This cause indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible.

- Cause 22 - Number changed

  This cause is returned to a user when the called number, indicated by the calling user, is no longer assigned.

- Cause 27 - Destination out of order

  This cause indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term “not functioning correctly” indicates that a signaling message was unable to be delivered to the remote user; for example a physical layer or data link layer failure at the remote user, user equipment off-line, etc.

- Cause 28 - Invalid number format (address incomplete)

  This cause indicates that the destination indicated by the calling user cannot be reached because the number is not in a valid format or is not complete.

- Cause 29 - Facility Rejected

  This cause is returned when a facility requested by the user cannot be provided by the network.

- Cause 30 - Response to *STATUS ENQUIRY*

  This cause is included in the *STATUS* message when the reason for generating the *STATUS* message was the prior receipt of a *STATUS ENQUIRY* message.

- Cause 31 - Normal, unspecified

  This cause is used to report a normal event only when no other cause in the normal class applies.

Resource unavailable class

- Cause 34 - No circuit/channel available

  This cause indicates that there is no appropriate circuit/channel, presently available, to handle the call.

- Cause 41 - Temporary failure

  This cause indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time. For example, the user may wish to try another call attempt almost immediately.

- Cause 42 - Switching equipment congestion

  This cause indicates that the switching equipment generating this cause is experiencing a period of high traffic.

- Cause 43 - Access information discarded

  This cause indicates that the network could not deliver access information to the remote user as requested.

- Cause 44 - Requested circuit/channel not available

  This cause indicates that the channel requested by the user during local channel negotiation is not currently available. For example,, in use or out of service for maintenance.

- Cause 47 - Resources unavailable, unspecified

  This cause is used to report a resource unavailable event only when no other cause in the resource unavailable class applies.

Service or option not available class

- Cause 50 - Requested facility not subscribed

  This cause indicates that the user has not subscribed to this facility and therefore cannot access the facility at this time.

- Cause 54 - Incoming calls barred

  This cause indicates that the called user does not accept the call delivered in the *SETUP* message.

- Cause 57 - Bearer capability not authorized

  This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but the user is not authorized to use.

- Cause 58 - Bearer capability not presently available

  This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but which is not available at this time.

- Cause 63 - Service or option not available, unspecified

  This cause is used to report a service or option not available event only when no other cause in the service or option not available class applies.

Service or option not implemented class

- Cause 65 - Bearer capability not implemented

  This cause indicates that the equipment sending this cause does not support the bearer capability requested.

- Cause 66 - Channel type not implemented

  This cause indicates that the equipment sending this cause does not support the channel type requested.

- Cause 70 - Only restricted digital information bearer capability is available

  This cause indicates that the user has requested an unrestricted bearer service but that the equipment sending this cause only supports the restricted version of the requested bearer capability.

- Cause 79 - Service or option not implemented, unspecified

  This cause is used to report a service or option not implemented event only when no other cause in the service or option not implemented class applies.

Invalid message class

- Cause 81 - Invalid call reference value

  This cause indicates that the equipment sending this cause has received a message with a call reference which is not currently in use on the user-network interface.

- Cause 82 - Identified channel does not exist

  This cause indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example, if a user has subscribed to those channels on a primary rate interface numbered from 1 to 12 and the user equipment or the network attempts to use channels 13 through 23, this cause is generated.

- Cause 88 - Incompatible destination

  This cause indicates that the equipment sending this cause has received a request to establish a call to a destination in which the required attributes cannot be accommodated (for example, data rate).

- Cause 90 - Destination address missing

  This cause indicates that the called party address is missing.

- Cause 95 - Invalid message, unspecified

  This cause is used to report an invalid message event only when no other cause in the invalid message class applies.

Protocol error class

- Cause 96 - Mandatory information element is missing

  This cause indicates that the equipment sending this cause has received a message which is missing an information element which must be present in the message before that message can be processed.

- Cause 97 - Message type non-existent or not implemented

  This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined, or defined but not implemented, by the equipment sending this cause.

- Cause 99 - Information element non-existent or not implemented

  This cause indicates that the equipment sending this cause has received a message which includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the equipment sending the cause. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.

- Cause 100 - Invalid information element contents

  This cause indicates that the equipment sending this cause has received an information element which it has implemented, however, one or more of the fields in the information element are coded in a way which has not been implemented by the equipment sending this cause.

- Cause 101 - Message not compatible with call state

  This cause indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state, or that a *STATUS* message was received indicating an incompatible call state.

- Cause 102 - Recovery on timer expiry

  This cause indicates that a procedure has been initiated by the expiry of a timer in association with error handling procedures.

- Cause 111 - Protocol error, unspecified

  This cause is used to report a protocol error event only when no other cause in the protocol error class applies.

Interworking class

- Cause 127 - Interworking, unspecified

  This cause indicates that there has been interworking with a network which does not provide causes for actions it takes. Thus, the precise cause for a message which is being sent cannot be ascertained.

Section 5: Supplementary Services

Chapter 5-1: Introduction 5-5

Chapter 5-5:
Network name 5-37

Chapter 5-6:
Network ring again 5-59

Chapter 5-7:
Network automatic call distribution 5-73

Chapter 5-8:
Equal access 5-93

Chapter 5-9:
Special number service 5-97

Chapter 5-10:
Integrated services access 5-99

Chapter 5-11:
Network message service 5-103

Chapter 5-12:
Release Link Trunk (RLT) 5-115

Chapter 5-1: Introduction

The ISDN Primary Rate Interface (PRI) services described in this section are those offered by the DMS-100 (the network) to a PRI user (for example, a PBX).

The PRI services fall into the following two categories

- user services
- administration services

User services are the service requirements and protocol to support services visible to the PRI user. As such, for some of the services, the requirements are similar to those for CCS7 (Common Channel Signaling System No. 7). Specific differences between PRI and CCS7 requirements for a particular service reflect structural and procedural differences between PRI and CCS7, where PRI is a user-network (access) relationship and CCS7 is an intra-network relationship.

Administration services deal with the administration and control of an ISDN PRI, and are additional to product specific OAM services. PRI administration services differ from the user services in that they are not selected by users and have no direct signaling and control implications.

1.1 PRI user services

1.1.1 Calling number delivery

The Calling Number Delivery (CND) service provides the directory number of the calling party for calls terminating on a PRI. CND is available as an option on a per ISDN PRI basis.

When the CND option is active, the calling party number will be contained in the *Calling party number* information element and is delivered in the *SETUP* message, unless the calling party number is restricted or is not available. The number is not available when a call is routed over certain existing signaling systems (for example, MF). If a call encounters interworking, the *Calling* *party number* information element is sent with an indication of “number not available due to interworking” and no digits. If the calling party has requested that the number not be displayed, the *Calling party number* information element will be delivered with the presentation indicator set to “restricted” . The digits will be delivered as determined by the CPN Screening subscription option.

1.1.2 Called number delivery

The Called Number Delivery service provides the called number for calls terminating on a PRI. Called Number Delivery is available as an option on each ISDN PRI. When this option is subscribed, the *Called party number* information element is included in the *SETUP* message and contains the called party’s number.

1.1.3 Network redirection and reason

The Network Redirection and Reason service informs the calling and called parties about any redirections that may occur during the life of a call.

The following redirection services are supported

- Call Forwarding Universal (CFU)
- Call Forwarding Busy (CFB)
- Call Forwarding No Reply (CFNR)
- Call Transfer
- Call Pickup

Features of the Network Redirection and Reason service are described below.

1.1.3.1 Notification of redirection before answer

The calling party will be informed of the reason for redirection and the directory number of the new destination by means of the *Redirection number* information element in the *NOTIFY* message.

1.1.3.2 Notification of redirection after answer

The connected parties will be informed of the reason for redirection and the directory number of the new connected party by means of the *Connected number* information element in the *NOTIFY* message.

1.1.3.3 Notification of redirected call

The new destination of a redirected call will be informed of the original destination and the reason for redirection by means of the *Original called number* information element, delivered in the *SETUP* message.

1.1.4 Network name

The Network Name service allows the transport of the calling, redirecting and called parties' names across the PRI. The service allows an originating node to receive the name of the terminating party, and to deliver the originator's name to the terminating node. When a call is redirected, the name of the connected party is also delivered.

1.1.5 Network ring again

The Network Ring Again service allows a calling user to be notified when a busy called party becomes idle. For example, a user (A) encountering a busy user (B) can monitor that user and be recalled when it becomes idle. If user (A) accepts the recall, the original call will be set up again automatically.

1.1.6 Network automatic call distribution

The Network Automatic Call Distribution service provides the capability to distribute incoming calls to a set of answering positions (agent positions). These positions can be on a local node or on remote nodes, where each node can be served by a PBX or by Centrex. Information which is exchanged between nodes is used to determine the best routing to evenly distribute calls among the answering positions.

1.1.7 Equal access

The Equal Access service provides PRI users with equal access to carrier networks (for example, IEC networks) for public network calls.

1.1.7.1 Transit network selection on a per call basis

Transit network selection on a per call basis allows the user to specify the preferred carrier on each call. The carrier selection may be accomplished by using the equal access dialing plan in the *Called party number* information element (for example, 10XXX+ dialing) or by including a *Transit network selection* information element in the *SETUP* message.

1.1.7.2 Default transit network selection

A default carrier is selected by the network if a carrier is not explicitly provided by the user in the call setup request and one is needed for the call. In this case, the network will provide the default carrier to which to route the call. The default carrier is selectable for each PRI.

1.1.8 Special number services

The Special Number services enable a PRI user to access any special number services available in the public network. These special numbers may not conform to any of the numbering plans. As such they are specified in the public network dialing plan to access certain network services (for example, "0" for operator services and "411" for directory information).

The special number digits are sent by the user in the *Called party number* information element in a *SETUP* message. The called party number will be coded as conforming to the E.164 numbering plan (for example, an NPI of "E.164" and a type of number of "unknown").

All special numbers accessible to public network subscribers can be accessed over PRI. These include

- 0
- 411
- 911
- 611
- 1-800
- 1-900
- 0+ (operator assisted calls)

1.1.9 Integrated services access

Integrated Services Access (ISA) permits one PRI interface to replace several dedicated trunk groups, resulting in efficiencies and simplified administration. ISA provides the capability to signal information which specifies the specific trunk type needed to complete a call. While the individual services continue to exist in the network for INWATS, OUTWATS, TIE and FX calls, a single PRI connection allows access to all of these services (see on page 5-9). ISA is supported for both incoming and outgoing calls on a PRI.

An ISA call follows normal call control procedures. The *Network specific facilities* (NSF) and *Called party number* (CDN) information elements within the *SETUP* message are used to select the appropriate service.

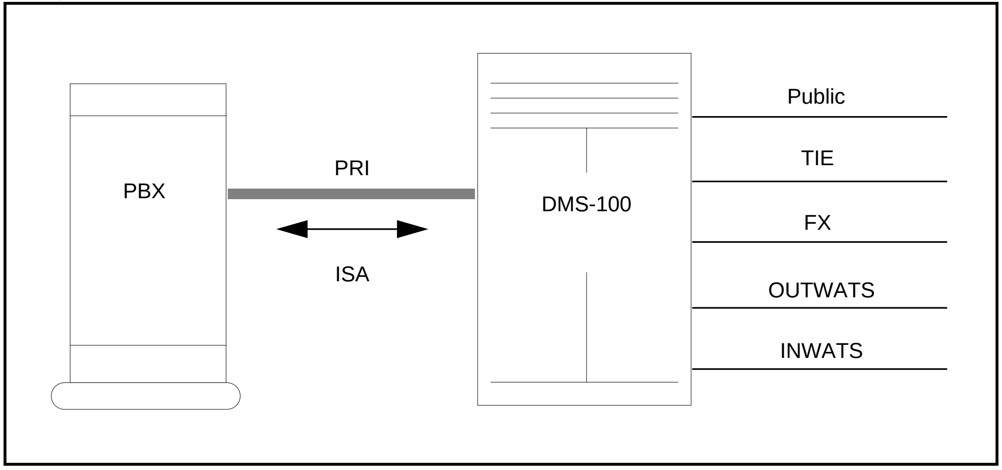
The following services are supported:

OUTWATS	OUTWATS is a service provided by telephone companies which permits a customer to originate calls to destinations in specific geographical areas, sometimes identified as a zone or band. The user may request a specific zone or band number.
INWATS	INWATS is a form of a long distance service which allows a subscriber to receive calls originating within specified service areas (zones or bands) without a charge to the caller. Typically, the caller dials a 1-800 number to identify the call as an INWATS call.
FX	Foreign Exchange (FX) is a dedicated line service between the customer's location and a remote public network exchange.

This service provides the equivalent of local service at the distant exchange.

TIE	These are private dedicated facilities between two private network switches (for example, PBX and Centrex).
PRIVATE	Private calls allow PRI users to access customer-specific routing and number translations.
PUBLIC	Public calls allow PRI users to access the public switched network.

Figure 5-1
Integrated Services Access



1.1.10 Network message service

The following types of Network Message Service are supported:

- Network Message Waiting Indicator

  Network Message Waiting Indicator (NMWI) allows a Message Service on one node to active or deactivate the message waiting indicator of a subscriber located at a different node.

- Network Executive Message Waiting

  Network Executive Message Waiting (NEMW) allows the DMS-100 Executive Message Waiting (EMW) feature on one node to activate the message waiting indicator of a subscriber located at a different node.

1.1.11 Release Link Trunk (RLT)

This feature provides RLT on PRI trunks on the network side. RLT is a feature available on an optional basis which optimizes the usage of NTNA PRI trunks.

The following is a typical usage for RLT. Please note that many other scenarios are possible. In this scenario, User A calls User B. This call is referred to as Call 1. Call 1 is routed through the DMS-100 to the PBX. User B then forwards or transfers the call to User C, requesting RLT. This call (Call 2) is routed through the same DMS-100 (see Figure 5-2 on page 5-10).

Figure 5-2
Typical Usage of RLT

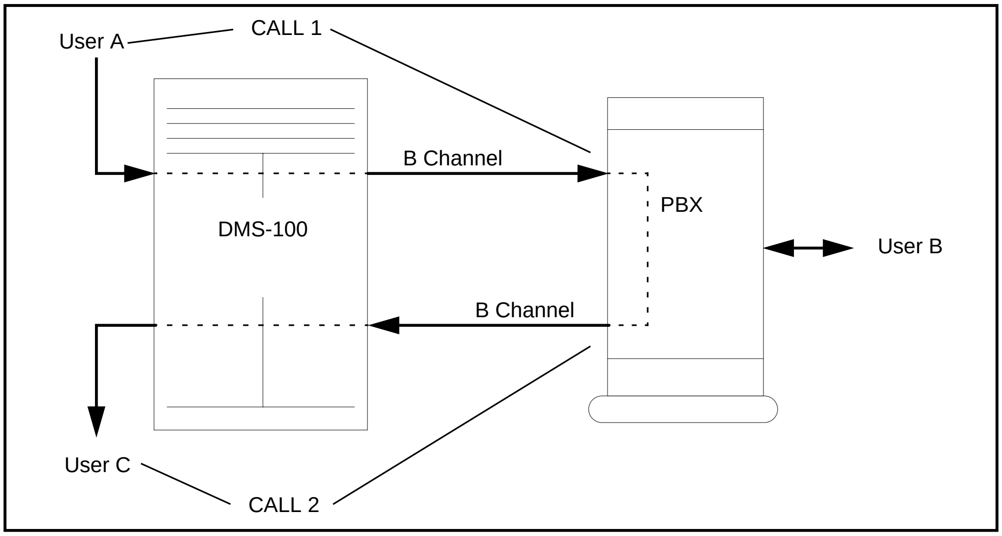
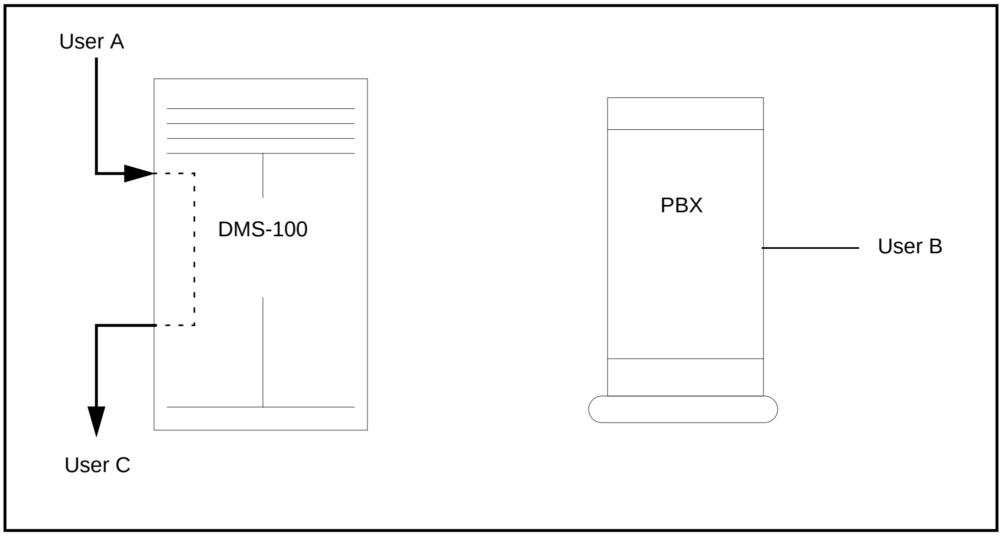


Figure 5-3
Result of Invoking RLT



When the call to User C is connected, RLT is invoked. The call is bridged between User A and User C at the DMS-100 and the PRI trunks to the PBX are released (see Figure 5-3 on page 5-10).

This feature will implement the network side of RLT only. The user side of RLT will not be implemented on the DMS-100. Any CPE device may be used with this feature if it follows the same user side RLT protocol as described in “Chapter 5-12: Release Link Trunk (RLT)”.

1.2 Administration services

1.2.1 Backup D-Channel

The Backup D-Channel service increases the reliability of signaling for non-facility associated signaling, that is, when a single D-channel is used to provide call control signaling for more than one DS-1 interface. This service provides a procedure for employing a standby D-channel which is used if the primary D-channel fails. All active calls are maintained during the switch-over to the standby D-channel.

The Backup D-Channel service is available as an option on a per ISDN PRI basis. See Section 4 of this specification for further information on this service.

1.2.2 Private network hop-off

The Private Network Hop-off service allows users of a logical private network to use the private network to route public network calls as far as possible before “hopping off” into the public network. The objective of this service is to optimize use of reserved private network capacity (for example, tie trunks).

Hopping off to the public network implies that the destination address is translated, if necessary, to an equivalent public numbering plan number (E.164) and that public network billing will apply from the hop off point.

1.2.3 Private network overflow

The Private Network Overflow service allows overflow from a private network to public network facilities. That is, private network calls will automatically overflow to the public network when congestion is encountered on the private network circuits.

For example, if the limit for private calls types on a PRI is at capacity and another private network call is made, the overflow would use B-channel capacity reserved for public call types.

Overflow to the public network implies that the destination address is translated to an equivalent public number (E.164) and that public network billing will apply.

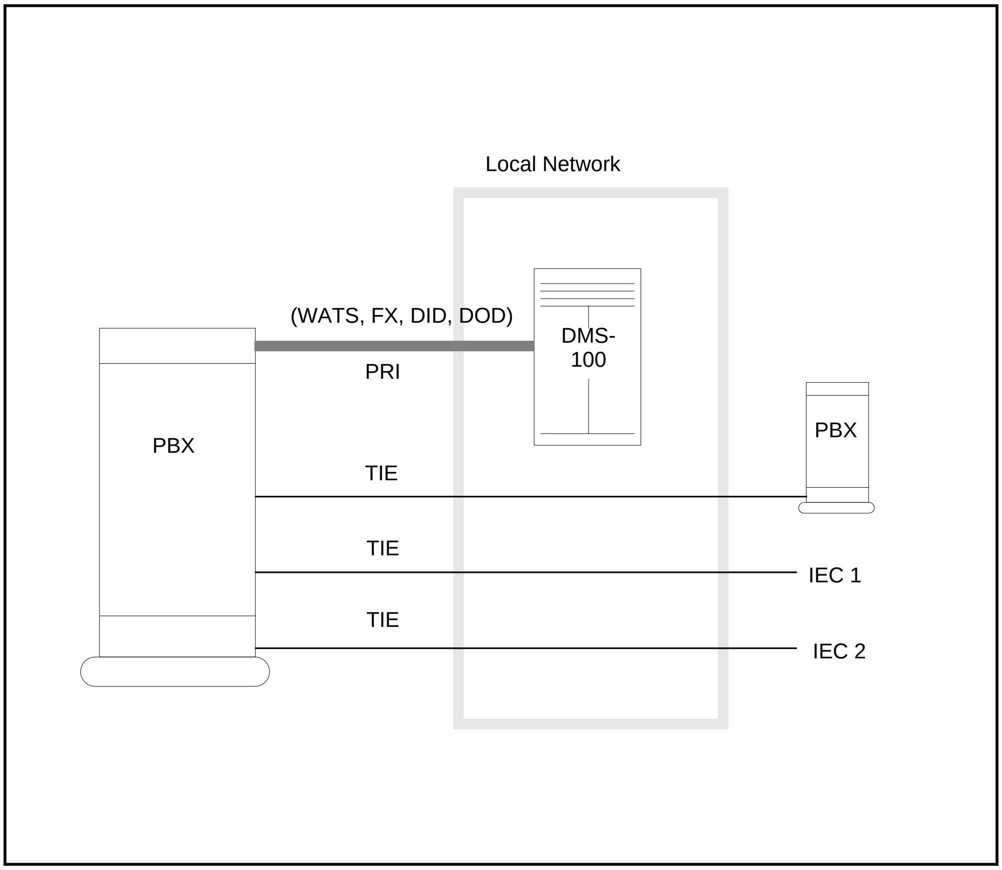
1.2.4 Integrated trunk access

Integrated Trunk Access (ITA) is a service for joint logical administration of an ISDN PRI, A/B signaling trunks and permanent DS-0 connections on a DS-1. That is, not all the channels on a DS-1 are used by PRI. Signaling for the non-PRI DS-0 channels does not utilize the PRI D-channel.

In ITA service, the non-PRI DS-0 channels only share the physical layer of the DS-1 connection. Thus, ITA is similar to a dedicated trunk environment, but where the individual physical wire connections are placed on individual DS-0 channels on a DS-1. Some of the DS-0 channels on the same DS-1 may be associated with a PRI.

In a dedicated trunk environment, network trunking requires dedicated, reserved trunks for different types of calls (for example, FX, WATS and tie trunks), as shown in Figure 5-4 on page 5-12.

Figure 5-4
Dedicated Trunk Environment



ISDN PRI can be related to these existing trunk types in two ways:

- Services coexisting with PRI (see Figure 5-5 on page 5-13)

  The DS-1 facility containing a PRI (N x B-channels + D-channel) may also be shared by A/B signaling DS-0 trunks, including FX, WATS and tie trunks.

- Services encompassed by PRI (see Figure 5-6 on page 5-14)

  The PRI is used to replace the access portion of these dedicated trunks, although the dedicated trunk facilities remain in the network. From the PRI user point of view this means replacing the A/B signaling with PRI D-channel signaling and replacing the dedicated trunks with PRI controlled B-channels. (see section 1.1.9 on page 5-8).

Figure 5-5
ITA - services coexisting with PRI

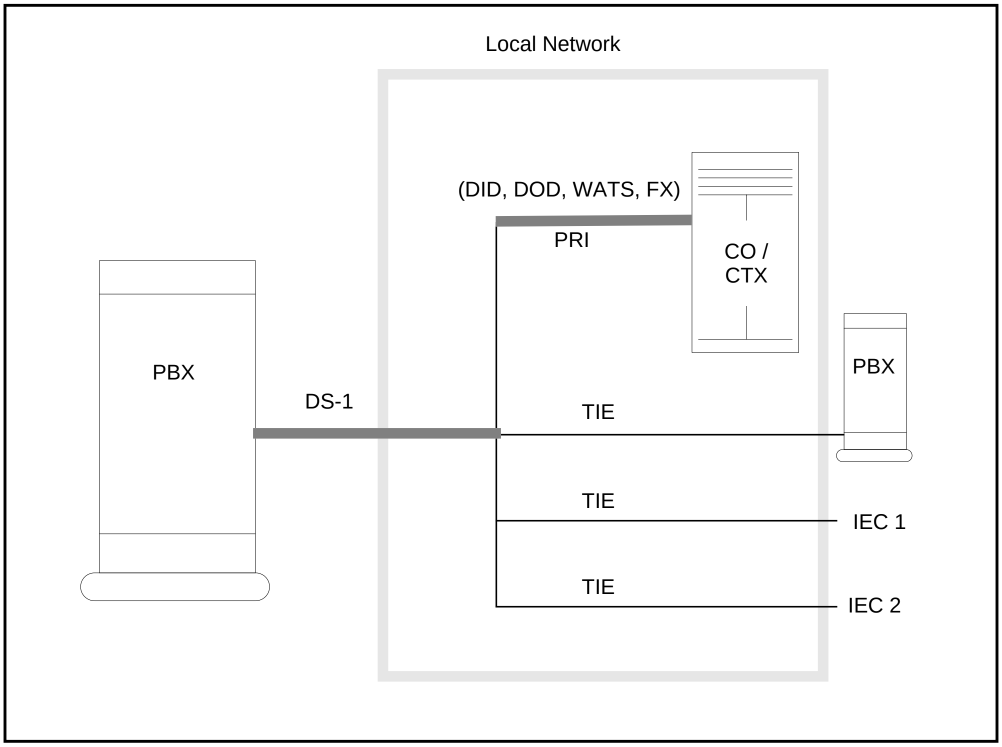
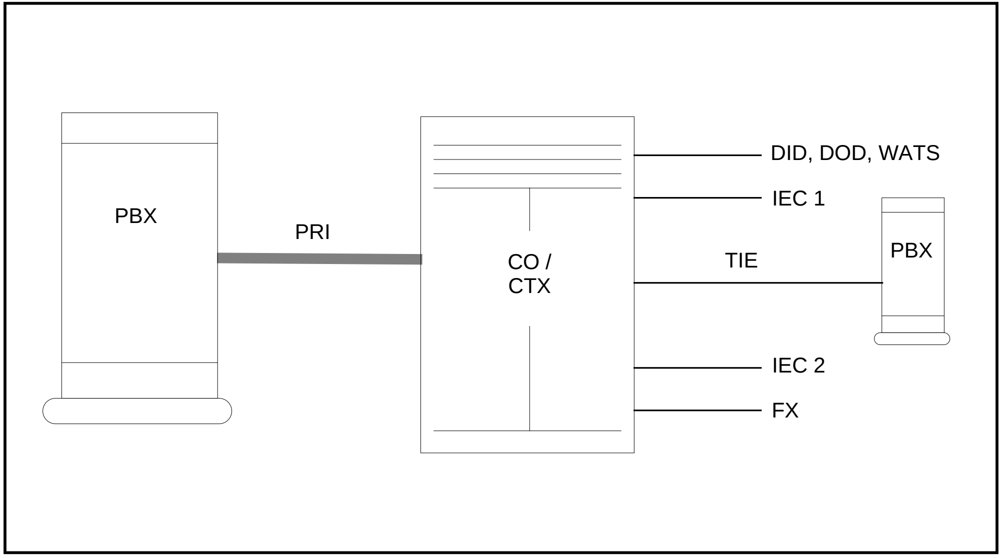


Figure 5-6
ITA - services encompassed by PRI



Chapter 5-2:
Calling number delivery

The procedures for Calling Number Delivery (CND) service cover the requirements for both when the PRI user provides a calling number as part of a call setup request and when the network delivers a calling number as part of a call setup request. These procedures include the requirements for calling party number privacy.

The procedures for CND service are consistent among PRI, BRI, Centrex and public network users. For interworking with CLASS CND service, the entire PRI is considered by the network to be one user, that is, there is no differentiation among individual users on a PRI.

The calling party's number is included in the *SETUP* message in the *Calling party number* information element. The *SETUP* message and the *Calling party number* information element are described in Section 4 of this specification.

2.1 Receipt of a call setup request from the calling user

The actions on receipt of a call setup request from a PRI user is dependent on the values of the Presentation Indicator (PI), the Screening Indicator (SI), and calling party number digits (CPN) in the *Calling party number* information element (CPN).

2.1.1 User includes the PI and SI

For the case where CPN screening is not activated, the network sets the Screening Indicator (SI) to "User-provided, not screened". The digit string in the user provided CPN is not screened by the network, and may therefore contain any user desired set of characters. The TON and NPI remain as received in the SETUP message. For public network calls from a PBX it is recommended that the user at least provides the Listed Directory Number (LDN) of the PBX.

For the case where CPN screening is activated, the CPN may either pass or fail the screening.

If the CPN passes screening, the SI is set to “User Provided, Verified and Passed”. All other CPN IE fields remain unchanged (i.e. TON, NPI and Number Digits). The number which has been screened may or may not have been edited, depending upon whether the editing option was activated.

If the CPN fails screening, then a network provided default DN is used to identify the calling party. TON is set to “National”, NPI is set to “E.164”, and SI is set to “Network Provided”.

> ***Note:*** A PI of “Number not available” should be coded by the user when the CPN is either not valid or no digits are included.
>
> ***Note:*** The network may ignore the PI received from the user and set it to “Presentation restricted” for certain types of calls, at the discretion of the service provider.
>
> ***Note:*** CPN editing may occur prior to CPN screening for the case of origination from a non-ISDN agent. If a CPN is edited, CPN screening must follow.

2.1.2 User does not include the PI and SI

The network sets the PI to “Presentation allowed” and the SI to “User-provided, not screened”, “User Provided, Verified and Passed”, or “Network Provided”, depending upon which scenario occurs as outlined in Section 2.1.

2.1.3 User does not include the *Calling party number* information element

The network sets calling party information as follows

- the numbering plan identifier (NPI) is set to “E.164”
- the type of number (TON) is set to “National”
- the network supplies a default CPN to uniquely identify the interface
- the PI is set to “Presentation allowed”
- the SI is set to “Network provided”

2.2 Progress of calling party information through the network

The calling party information provided by the user, and possibly as altered by the procedures in section 2.1 on page 5-15, is normally passed unmodified through the network to the terminating network switch. Exceptions to this general rule are described below.

2.2.1 Interworking

When interworking with a non-ISDN network which is not capable of transporting the CPN, PI or SI information, this information is discarded. For example, this can occur when interworking with an MF trunk.

When a call originates from a non-ISDN network which does not support the CPN, PI, or SI information, the terminating ISDN network may be able to reconstitute the CPN, and possibly the PI and SI. This can be done since some non-ISDN networks are capable of transporting a calling party number. Otherwise, the ISDN network sets the PI to “Number not available”, the SI to “Network provided”, and the CPN is omitted.

> ***Note:*** For an ISDN PRI being used for private network calls, if the CPN, PI and SI are not available, the NPI is set to “Private numbering plan”, the TON to “Unknown” and the CPN is omitted.

2.2.2 Private network overflow

If the private network capacity is exceeded at any point and the private network call (NPI of “Private”) is to be routed through the public network (as caused by use of the Private Network Overflow service), the called party number is translated to a public network number with an NPI of “E.164”. A private CPN may undergo the same type of translation to a public network number (NPI of “E.164”), or, if this is not possible, the private CPN may be discarded or marked by the network with a PI of “Presentation restricted”.

The reasons for performing the above number translations are:

- To ensure that the called party is aware that public network call tariffs apply to the call.
- The keep the calling and called party numbers aligned, that is, within the same numbering plan. Otherwise, if call redirection occurs, the eventual delivery of private numbers may be meaningless.
- Billing records can be associated with a valid public network number.

2.3 Delivery of a call setup request to the called user

If a CPN is available, the delivery of the CPN is determined by the received Presentation Indicator (PI) and by the network CPN Screening option. The PI and SI, if available, are delivered as received. The calling party information is included in a *Calling party number* information element in the *SETUP* message sent to the called user.

The network uses the following procedure to determine whether the CPN should be delivered to the terminating user:

- CPN Screening is “Always”

  CPN digits are always delivered over the PRI, even if the PI is “Presentation restricted”.

- CPN Screening is “Never”

  A *Calling party number* information element is not delivered over the PRI, regardless of the PI value.

- CPN Screening is “Screen”

  CPN digits are delivered over the PRI only if the PI is “Presentation allowed”.

Chapter 5-3: Called number delivery

If a called user subscribes to this service, the *Called party number* information element is included in the *SETUP* message on each terminating call. The coding of the *Called party number* information element is described in Section 4 of this specification.

The Numbering Plan Identification (NPI) and Type of Number (TON) fields are coded as received from the originating user.

If the originating user is non-ISDN or from a PRI not using ISA, the NPI and TON are inferred from the received called party number digits, as follows:

- If the call comes from private facilities, the NPI is set to “Private numbering plan” and the TON is set to “Subscriber number”.
- If the call comes from public facilities, the NPI is set to “ISDN/ Telephony numbering plan (E.164/E.163)” and the TON is set to
  - “International number”, if the number of digits in the called number is greater than 10
  - “National number”, if the number of digits in the called number is equal to 10
  - “Subscriber number”, if the number of digits in the called number is less than 10

If a called user does not subscribe to this service, the terminating *SETUP* message does not contain a *Called party number* information element.

Chapter 5-4: Network redirection and reason

This section describes the protocol and procedures for the Network Redirection and Reason service. Only the differences from PRI basic call are shown. (See Section 4 of this specification for basic call protocol and procedures.)

The following types of call redirection are supported:

- Call Forwarding Universal (CFU): all calls to a called party are redirected to another destination
- Call Forwarding Busy (CFB): all calls to a called party are redirected to another destination if the called party is busy
- Call Forwarding No Reply (CFNR): Calls to a called party are redirected to another destination if the called party does not answer the call within a preset time after the start of alerting
- Call Pickup: Calls to a called party are redirected to another destination when the user at that destination picks up the alerting call
- Call Transfer: An active call is redirected to a new destination

Network redirection and reason service extends basic call in the following ways

- notification to the users of call redirection, when it occurs
- notification to the called party, when a call is offered, of previous call redirections during the call history
- exchange of connected numbers after call transfer

Notifications of previous redirections when a call is offered is accomplished with an *Original called number* information element in the *SETUP* message. A description of the *Original called number* information element is in section 4.5.21 on page 4-103. This information is only provided when one of the call forwarding services occurs (CFU, CFB or CFNR).

Notifications of call redirection, when it occurs, and exchange of connected numbers after call transfer are accomplished with *NOTIFY* messages. The required information is carried in one of, or a combination of, the following information elements

- *Redirection numbe*r (see section 4.5.24 on page 4-110)
- *Information request* (see section 4.5.16 on page 4-96)
- *Connected number* (see section 4.5.12 on page 4-70)

Connected numbers are only sent at the request of another node.

The *NOTIFY* message can be sent before the *ALERTING* message for CFU and CFB, after the *ALERTING* message for CFNR and Call Pickup, and after the *CONNECT* message for Call Transfer.

Multiple call redirections could result in more than one *NOTIFY* message being sent.

Redirection information may not be available if the call leaves the ISDN network. In this case, a *PROGRESS* message is sent to the calling party with a *Progress indicator* information element with *Progress description* value #1 “Call is not end-to-end ISDN; further call progress information may be available in-band”.

For the Network Redirection and Reason service, the *NOTIFY* message always contains a *Notification indicator* information element with a *Notification description* of “Call information/event”.

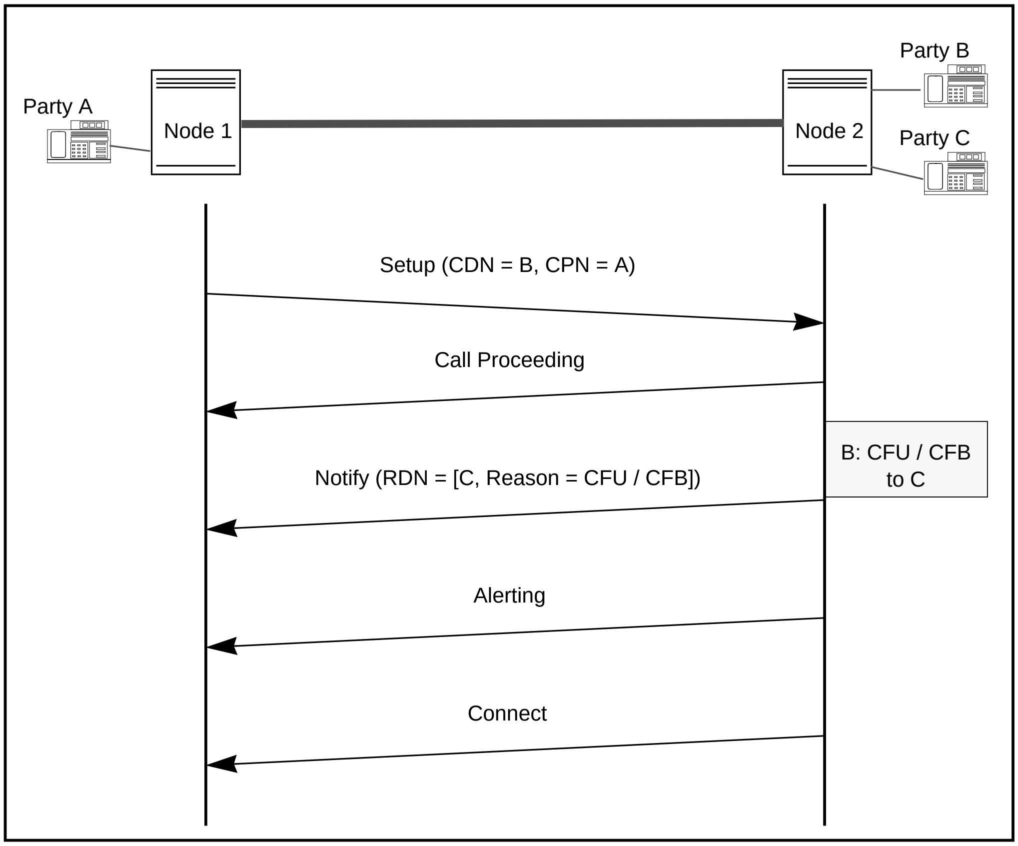
4.1 Call forwarding universal and call forwarding busy

As shown in Figure 5-7, party A calls party B over a PRI, and the call is redirected to party C using CFU or CFB (parties B and C are on the same node). The terminating node sends a *NOTIFY* message to party A containing the *Redirection number* information element (RDN) coded as follows:

- Type of Number - “Unknown” or “National”
- Numbering Plan Identification - “Private” or “E.164”
- Presentation Indicator - “Presentation allowed” or “Presentation restricted”
- Screening Indicator - “Network provided” or “User-provided not screened”
- Reason for Redirection - “Call Forwarding Busy” or “Call Forwarding Universal”
- Number Digits - party C’s number

The *NOTIFY* message is sent after the *CALL PROCEEDING* message.

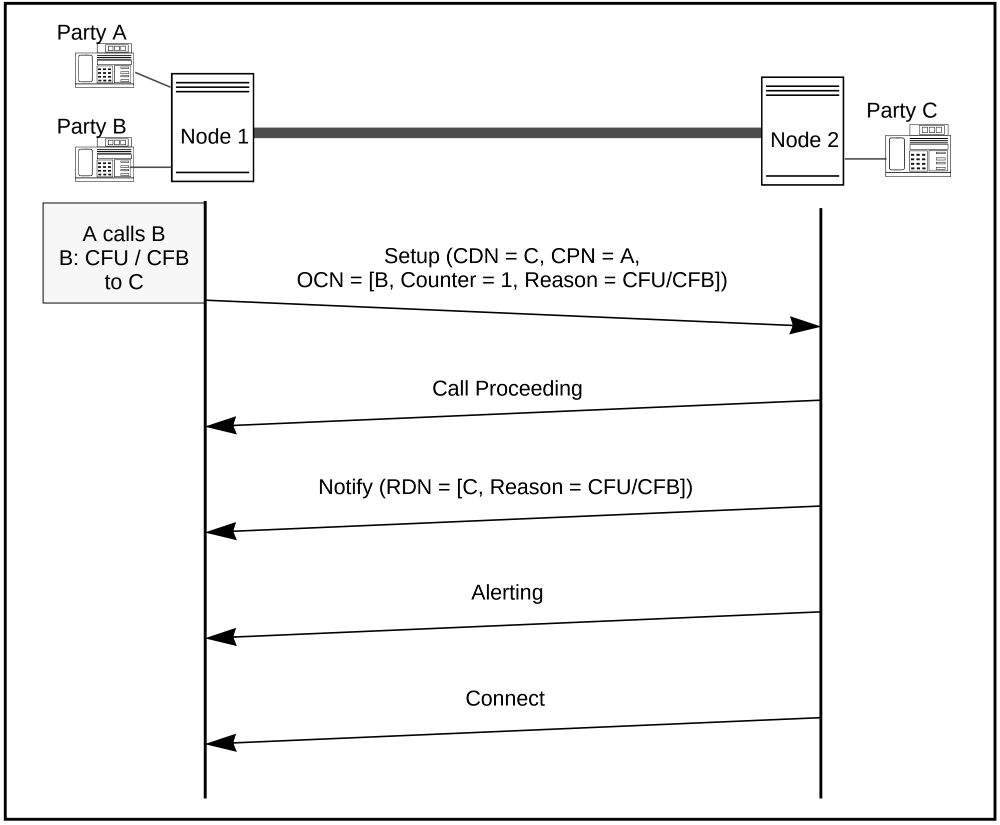
Figure 5-7
Call forward universal (CFU) or call forward busy (CFB) at a remote node



As shown in Figure 5-8, party A calls party B and is redirected to party C over a PRI using CFU or CFB. The *SETUP* message sent to party C includes the *Original called number* information element coded as follows:

- Type of Number - “Unknown” or “National”
- Numbering Plan Identification - “Private” or “E.164”
- Presentation Indicator - “Presentation allowed” or “Presentation restricted”
- Screening Indicator - “Network provided” or “User-provided not screened”
- Original Redirection Reason - “CFB” or “CFU”
- Redirection Counter - 1
- CFNR indicator - “False”
- Number Digits - party B’s number

Figure 5-8
Call forward universal (CFU) or call forward busy (CFB) at a local node



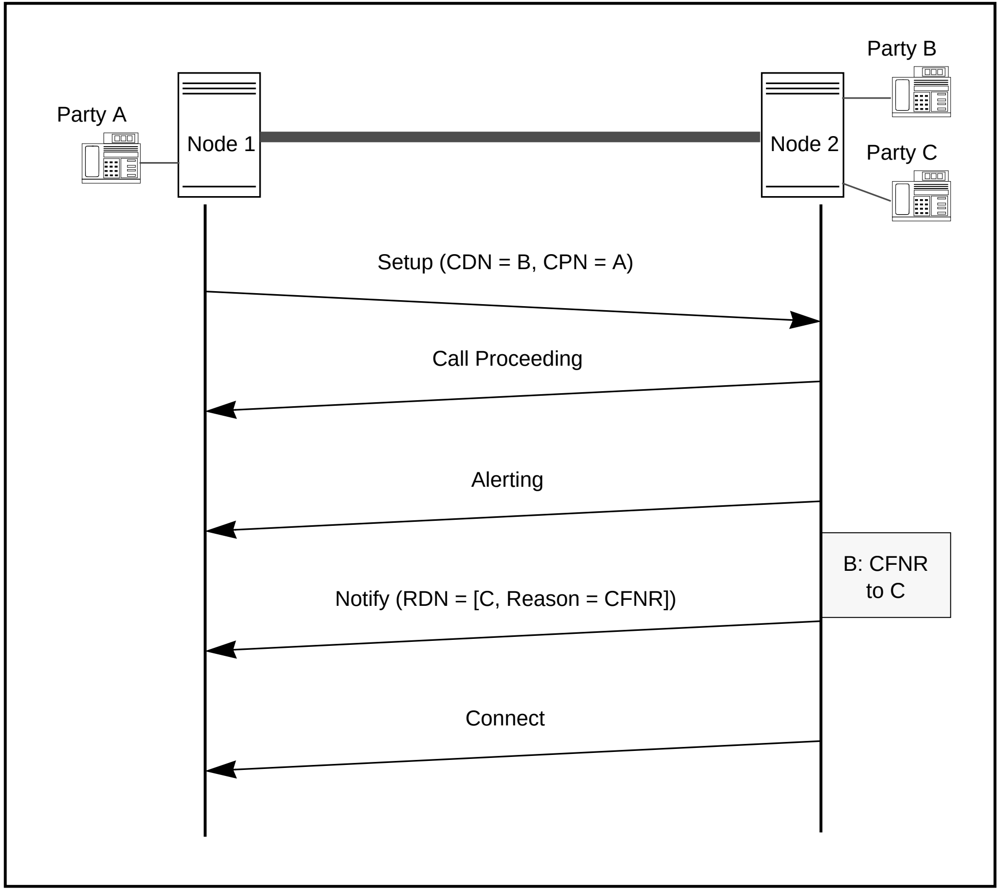
4.2 Call forwarding no reply

As shown in Figure 5-9, party A calls party B over a PRI, and the call is redirected to Party C using CFNR, where parties B and C are on the same node. The terminating node sends a *NOTIFY* message to party A containing the *Redirection number* information element coded as follows:

- Type of Number - “Unknown” or “National”
- Numbering Plan Identification - “Private” or “E.164”
- Presentation Indicator - “Presentation allowed” or “Presentation restricted”
- Screening Indicator - “Network provided” or “User-provided not screened”
- Reason for Redirection - “Call Forwarding No Reply”
- Number Digits - party C’s number

The *NOTIFY* message is sent after the *ALERTING* message.

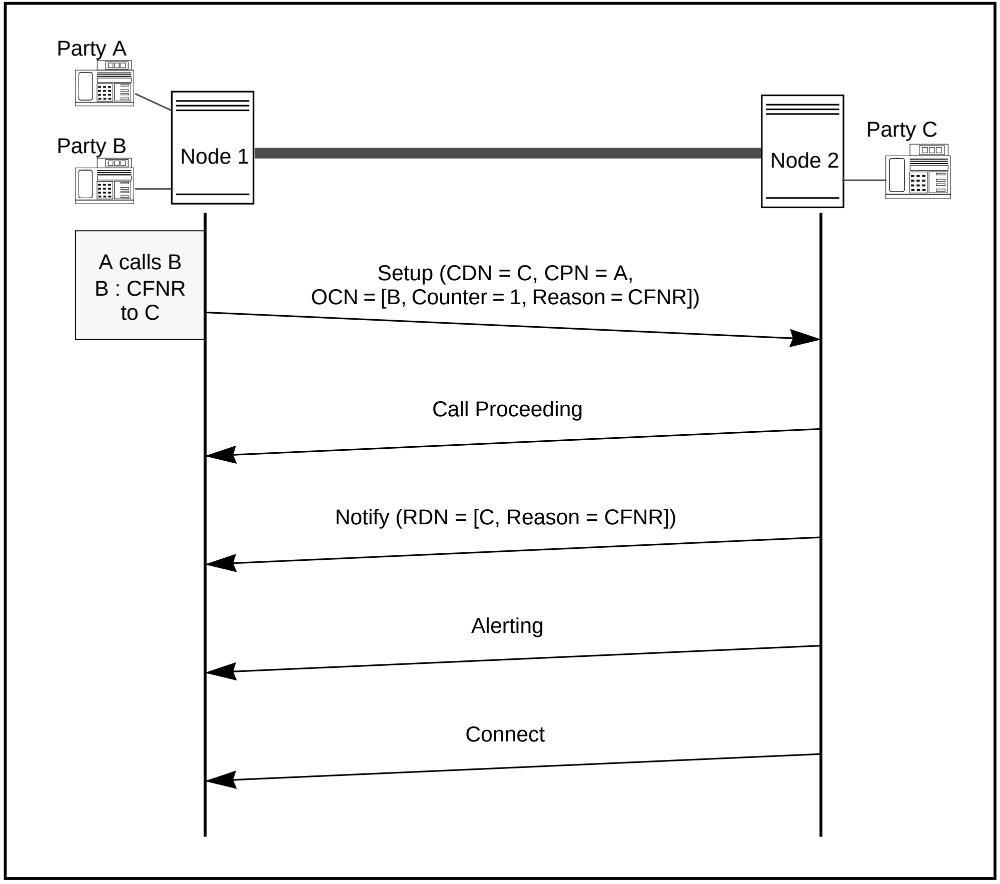
Figure 5-9
Call forward no reply (CFNR) at a remote node



As shown in Figure 5-10, party A calls party B and is redirected to party C over a PRI using CFNR. The *SETUP* message sent to party C will include the *Original called number* information element coded as follows:

- Type of Number - “Unknown” or “National”
- Numbering Plan Identification - “Private” or “E.164”
- Presentation Indicator - “Presentation allowed” or “Presentation restricted”
- Screening Indicator - “Network provided” or “User-provided not screened”
- Original Redirection Reason - “Call Forwarding No Reply”
- Redirection Counter - 1
- CFNR indicator - “True”
- Number Digits - party B’s number

Figure 5-10
Call forward no reply (CFNR) at a local node



4.3 Multiple call forwarding

If a call undergoes multiple call forwardings, (for example, party A calls party B, is then forwarded to party C, and is then forwarded to party D) the original called number and the calling party number remain unchanged (parties B and A, respectively).

The redirection counter is incremented each time a forwarding occurs. The redirection information which is returned to the originating node always contains the directory number of the user that finally accepts the call (party D).

When the redirection limit is exceeded (that is, the sixth or greater redirection), the call is cleared by sending a *DISCONNECT* message. The *Cause* value in the *Cause* information element is dependent on the type of call forwarding that would cause the limit to be exceeded:

- Call Forwarding Universal - *Cause* value #18 “No user responding”
- Call Forwarding Busy - *Cause* value #17 “User busy”

If the last reason for redirection is Call Forward No Reply, call forwarding is not inhibited even if the redirection limit is exceeded.

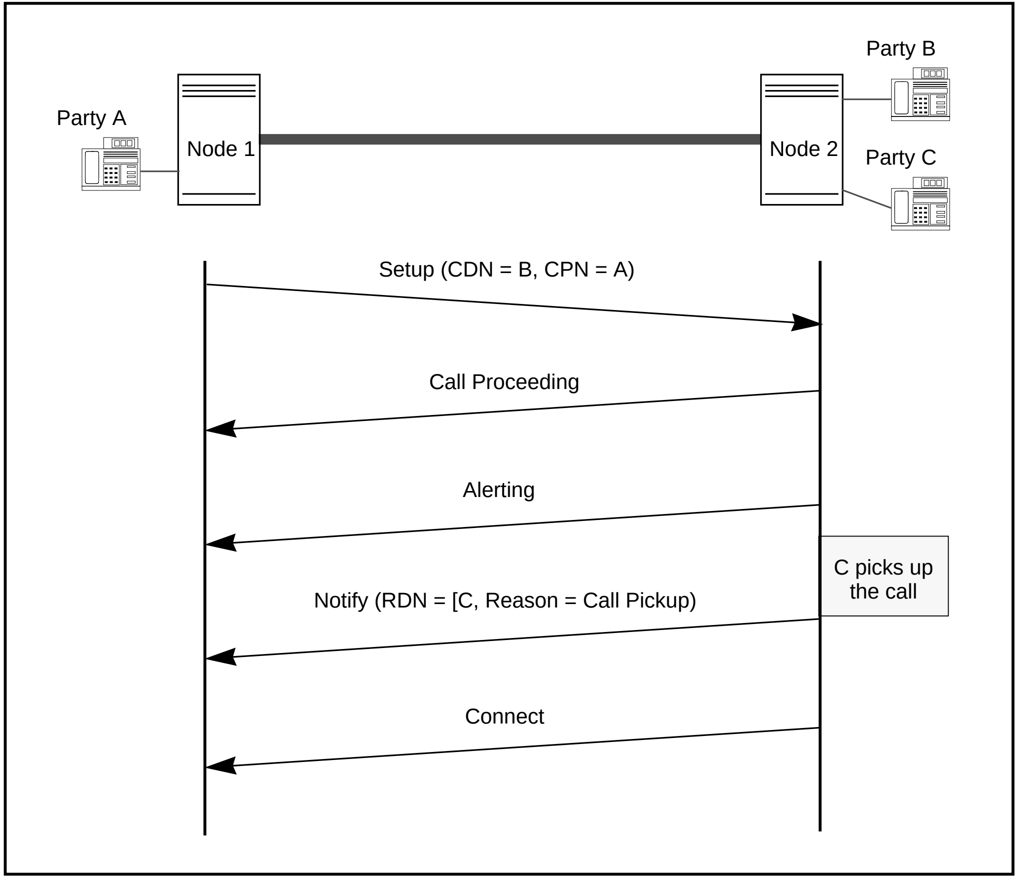
4.4 Call pickup

As shown in Figure 5-11, party A calls party B over a PRI, and party C activates call pickup during the alerting phase of the call (parties B and C are in the same call pickup group). The terminating node sends a *NOTIFY* message to party A with a *Redirection number* information element coded as follows:

- Type of Number - “Unknown” or “National”
- Numbering Plan Identification - “Private” or “E.164”
- Presentation Indicator - “Presentation allowed” or “Presentation restricted”
- Screening Indicator - “Network provided” or “User-provided not screened”
- Reason for Redirection - “Call Pickup”
- Number Digits - party C’s number

The *NOTIFY* message is sent after the *ALERTING* message.

Figure 5-11
Call pickup at the remote node



4.5 Call transfer

As shown in Figure 5-12 on page 5-30, a call between parties A and B, over a PRI, is transferred by B to party C, where parties B and C are on the same node). When party B releases the call (after the CONNECT message from party C) node 2 sends a *NOTIFY* message to party A containing a *Redirection number* information element coded as follows:

- Type of Number - “Unknown”
- Numbering Plan Identification - “E.164”
- Presentation Indicator - “Presentation allowed”
- Screening Indicator - “Network provided”
- Reason for Redirection - “Call transfer”
- Number Digits - no digits are included

After transfer, the connected number may be requested by sending a *NOTIFY* message containing an *Information request* information element coded as follows:

- Information Request Indicator - “Request for additional information”
- General Type of Information - “Address digits”
- Information Specifics - “Connected number”

The connected number is returned in a *NOTIFY* message with the *Connected number* information element coded as follows:

- Type of Number - “Unknown” or “National”
- Numbering Plan Identification - “Private” or “E.164”
- Presentation Indicator - “Presentation allowed” or “Presentation restricted”
- Screening Indicator - “Network provided” or “User-provided not screened”
- Number Digits - party C’s number

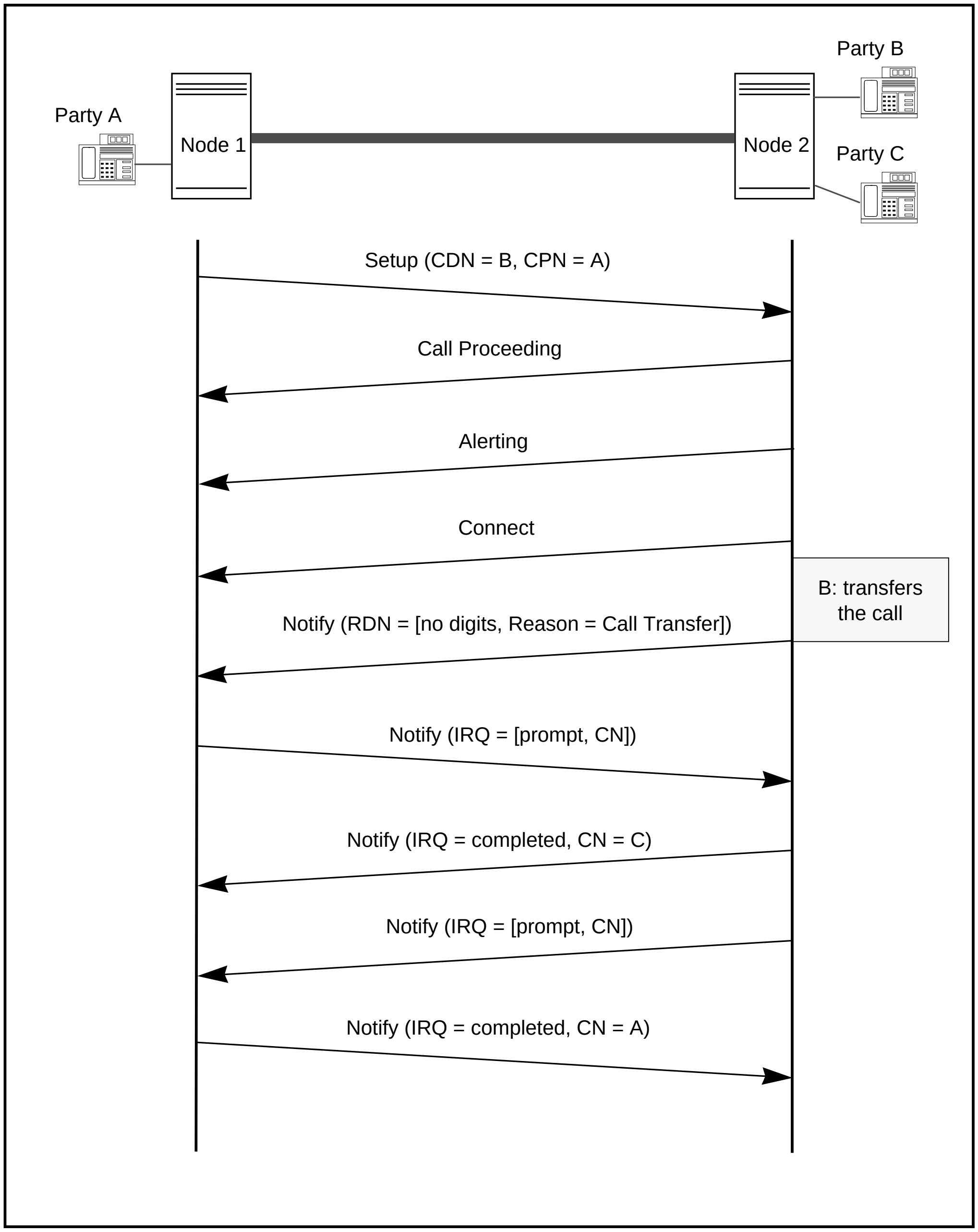
The *Information request* information element in the *NOTIFY* message is coded as follows:

- Information Request Indicator - “Information request completed”
- General Type of Information - “Address digits”
- Information Specifics - “Connected number”

Node 2 may also request the connected number for party A by coding a request in the *NOTIFY* message. The connected number for party A would then be returned in a *NOTIFY* message.

> ***Note:*** The message flow after the call transfer occurs is not dependent on who originated the call between parties A and B.

Figure 5-12
Call transfer at the remote node



As shown in Figure 5-13 on page 5-32, a call between parties A and B is transferred by B to party C over a PRI. When party B releases the call, the node 1 sends a *NOTIFY* message to party C containing the *Redirection number* information element coded as follows:

- Numbering Plan Identification - “E.164”
- Presentation Indicator - “Presentation allowed”
- Screening Indicator - “Network provided”
- Reason for Redirection - “Call transfer”
- Number Digits - no digits are included

The connected number may then be requested by sending a *NOTIFY* message containing an *Information request* information element coded as follows:

- Information Request Indicator - “Request for additional information”
- General Type of Information - “Address digits”
- Information Specifics - “Connected number”

The connected number is returned in a *NOTIFY* message with the *Connected number* information element coded as follows:

- Type of Number - “Unknown” or “National”
- Numbering Plan Identification - “Private” or “E.164”
- Presentation Indicator - “Presentation allowed” or “Presentation restricted”
- Screening Indicator - “Network provided” or “User-provided not screened”
- Number Digits - party C’s number

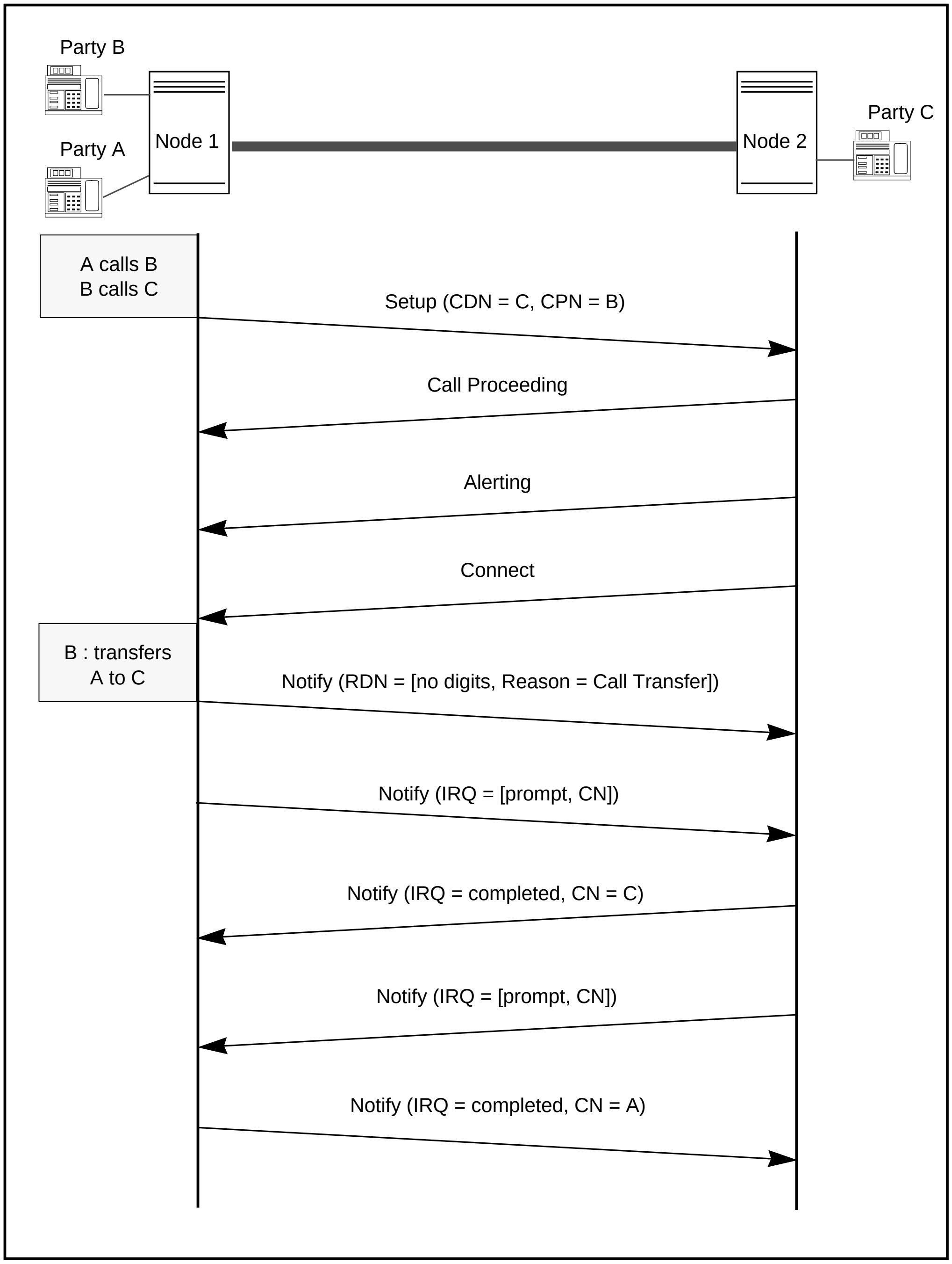
The Information request information element in the *NOTIFY* message will be encoded as:

- Information Request Indicator - “Information request completed”
- General Type of Information - “Address digits”
- Information Specifics - “Connected number”

Node 2 may also request the connected number by sending a request in the *NOTIFY* message. The connected number for party A is returned in a *NOTIFY* message.

> ***Note:*** The message flow for the consultation call between parties B and C follows normal call control procedures.

Figure 5-13
Call transfer at the local node



As shown in Figure 5-14 on page 5-34, a call between parties A and B, over PRI, is transferred by B to party C over PRI. Party B releases the call, which transfers party A to party C. Node 2 sends a *NOTIFY* message to both nodes 1 and 3 containing the reason for redirection (call transfer).

The connected number may be requested by node 1 with a *NOTIFY* message containing an *Information request* information element coded as follows:

- Information Request Indicator - “Request for additional information”
- General Type of Information - “Address digits”
- Information Specifics - “Connected Number”

The connected number is returned in a *NOTIFY* message from node 3 with the *Connected number* information element coded as follows:

- Type of Number - “Unknown” or “National”
- Numbering Plan Identification - “Private” or “E.164”
- Presentation Indicator - “Presentation allowed” or “Presentation restricted”
- Screening Indicator - “Network provided” or “User-provided not screened”
- Number Digits - party C’s number

The Information request information element in the *NOTIFY* message will be coded as follows:

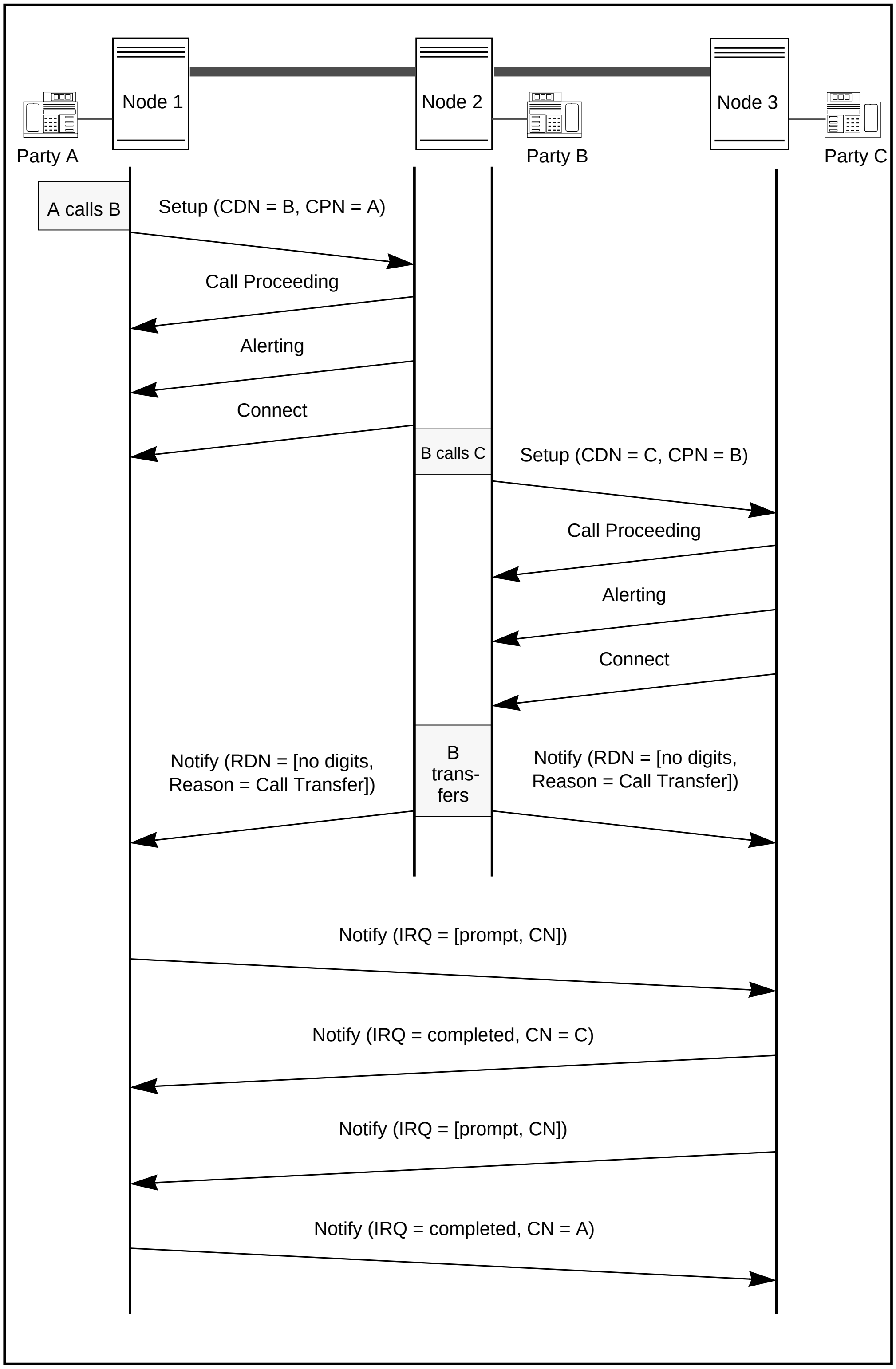
- Information Request Indicator - “Information request completed”
- General Type of Information - “Address digits”
- Information Specifics - “Connected number”

Node 3 may also request the connected number by sending a *NOTIFY* message to node 1. The connected number for party A will be returned in a *NOTIFY* message.

> ***Note:*** The message flow for the consultation call between parties B and C follows normal call control procedures.

> ***Note:*** After B transfers the call, node 2 continues to relay messages between nodes 1 and 2.

Figure 5-14
Call transfer at an intermediate node



4.6 Interworking

If interworking is encountered with a non-ISDN trunk (that is, not PRI or CCS7), or an ISDN trunk which does not support the Network Redirection and Reason service, then all redirection information may not be delivered to, nor received from, the terminating node.

The redirection counter may be discarded when interworking is encountered. The network assumes that a call incoming from an interworking point has not undergone any redirections, that is, the redirection counter will be set to one when the first redirection occurs within the ISDN environment.

Requests for connected number will not receive any response when interworking is encountered.

Interworking does not impact normal call processing except that redirection information may not be available to the PRI user.

Chapter 5-5: Network name

This section describes how the Network Name service is provided. The Network Name service allows the names associated with the parties of a call to be transported across a PRI.

There are two methods of exchanging name information across PRI

- query method
- setup method

Nodes which exchange name information should use the same exchange method, that is, setup or query. For more flexibility, especially where the network may contain a large number a nodes, if the name information is not provided by the setup method for a particular call, the query method could be used as an alternative procedure.

In the query method, the name information is provided only in response to a request. The request is made with a *Display* information element in either a *SETUP* or a *NOTIFY* message. The name information in the response to the query is coded in a *Display* information element in a *NOTIFY* message.

When a call is redirected, the name of the new connected party can be provided to the calling party. Up to one request and two names can be included in a *NOTIFY* message. This allows the transport of the names associated with the calling party, the original called party and the connected party.

In the setup method, name information is automatically sent, if available, without explicit requests. Name information is sent in a *Display* information elements in either a *SETUP* or *NOTIFY* message.

Name information may not always be available. If this occurs in the query method, the response *Display* information element will contain an indication that the name information is not available. In the setup method, no *Display* information element is sent in this case.

When a call is redirected, the name information transported can include the calling party, the new connected party and the original called party names. Interactions with the Network Redirection and Reason service are described in section 5.4 on page 5-41.

In the following procedures, when a *NOTIFY* message is to be sent, the *Notification indicator* information element is mandatory. The *Notification description* field is coded as “Call information/event”.

5.1 Query method

An originating node requests the called party’s name by including a *Display* information element in the *SETUP* message, coded as follows:

- Associated Information - “Requested”
- Display Type - “Connected party name”
- Display Information - not included

The terminating node responds by sending a *NOTIFY* message with a *Display* information element containing the called party’s name. The terminating node requests the calling party’s name by including another *Display* information element in the *NOTIFY* message.

The *Display* information element containing the called party’s name is coded as follows:

- Associated Information - “Included”
- Display Type - “Connected party name”
- Display Information - name of called party

The *Display* information element requesting the calling party’s name is coded as follows:

- Associated Information - “Requested”
- Display Type - “Calling party name”
- Display Information - not included

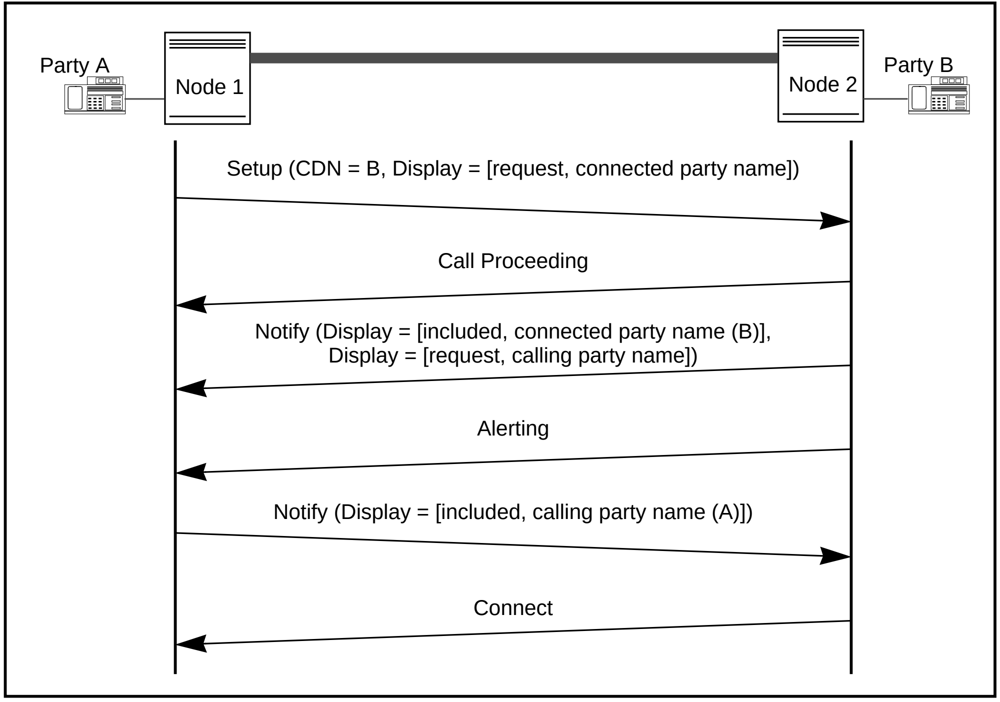
The terminating node can request the calling party’s name even if the originating node does not request the called party’s name in the *SETUP* message. In this case, the terminating node only includes one *Display* information element in the *NOTIFY* message, requesting the calling party’s name, as described above.

The originating node responds to the request for the calling party's name by sending a *NOTIFY* message with a *Display* information element coded as follows:

- Associated Information - “Included”
- Display Type - “Calling party name”
- Display Information - name of calling party

See Figure 5-15 on page 5-39 for the query method message flow.

Figure 5-15
Network name - query method



5.2 Setup method

The originating node includes the calling party's name in a *Display* information element included in the *SETUP* message. The *Display* information element is coded as follows:

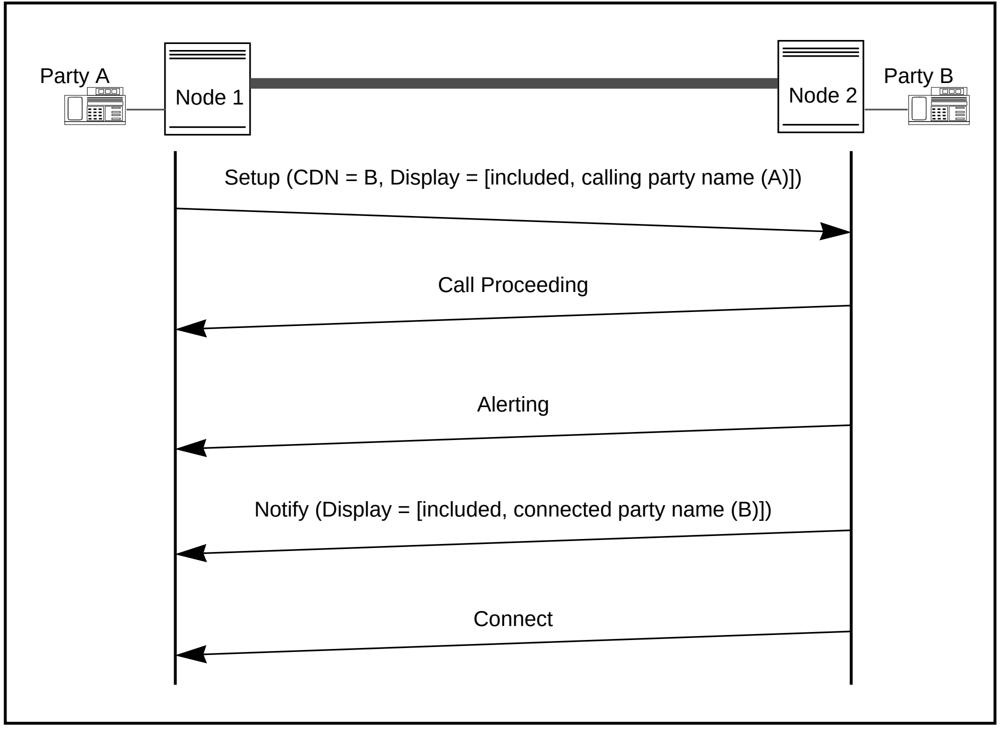
- Associated Information - “Included”
- Display Type - “Calling party name”
- Display Information - name of the calling party

The terminating node sends the called party’s name in a *Display* information element included in a *NOTIFY* message. The *Display* information element is coded as follows:

- Associated Information - “Included”
- Display Type - “Connected party name”
- Display Information - name of the called party

See Figure 5-16 on page 5-40 for the setup method message flow.

Figure 5-16
Network Name - setup method



5.3 Restrictions

The maximum length of a name included in the *Display* information element is 15 characters.

Name information may not always be available. A request for name information when it is not available is ignored, and the call continues normally.

In the case of multiple call forwarding, only the calling and original called parties’ names are available. That is, the names of subsequent redirecting parties are not available.

5.4 Interactions with network redirection and reason service

The procedures and message flows in this section mainly show only the additions to those shown in Chapter 5-4, as a result of Network Name service interactions. Please refer to the corresponding procedures and message flows in Chapter 5-4 to supplement those in this section in order to achieve a full understanding of the interactions in this section..

5.4.1 Call forwarding universal and call forwarding busy

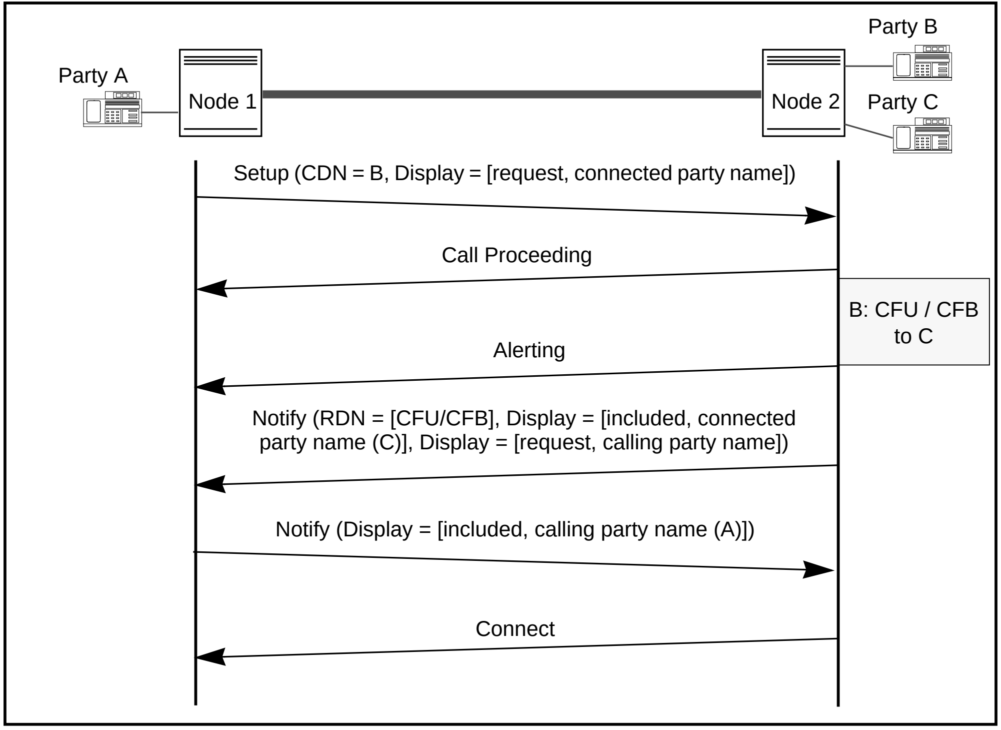
5.4.1.1 Query method

As shown in Figure 5-17, party A calls party B over a PRI, and the call is redirected to party C using Call Forwarding Universal (CFU) or Call Forwarding Busy (CFB). The terminating node sends a *NOTIFY* message containing a *Redirection number* information element. If the originating node included a request for the called party's name in the original *SETUP* message, this *NOTIFY* message will include, in addition to the redirection information

- a *Display* information element, coded as "Connected party name" and including party C's name
- a second *Display* information element, if needed, coded as a request for the calling party's name

The originating switch sends the calling party's name in a *Display* information element in a *NOTIFY* message.

Figure 5-17
Network name (query method): CFU/CFB at the remote node

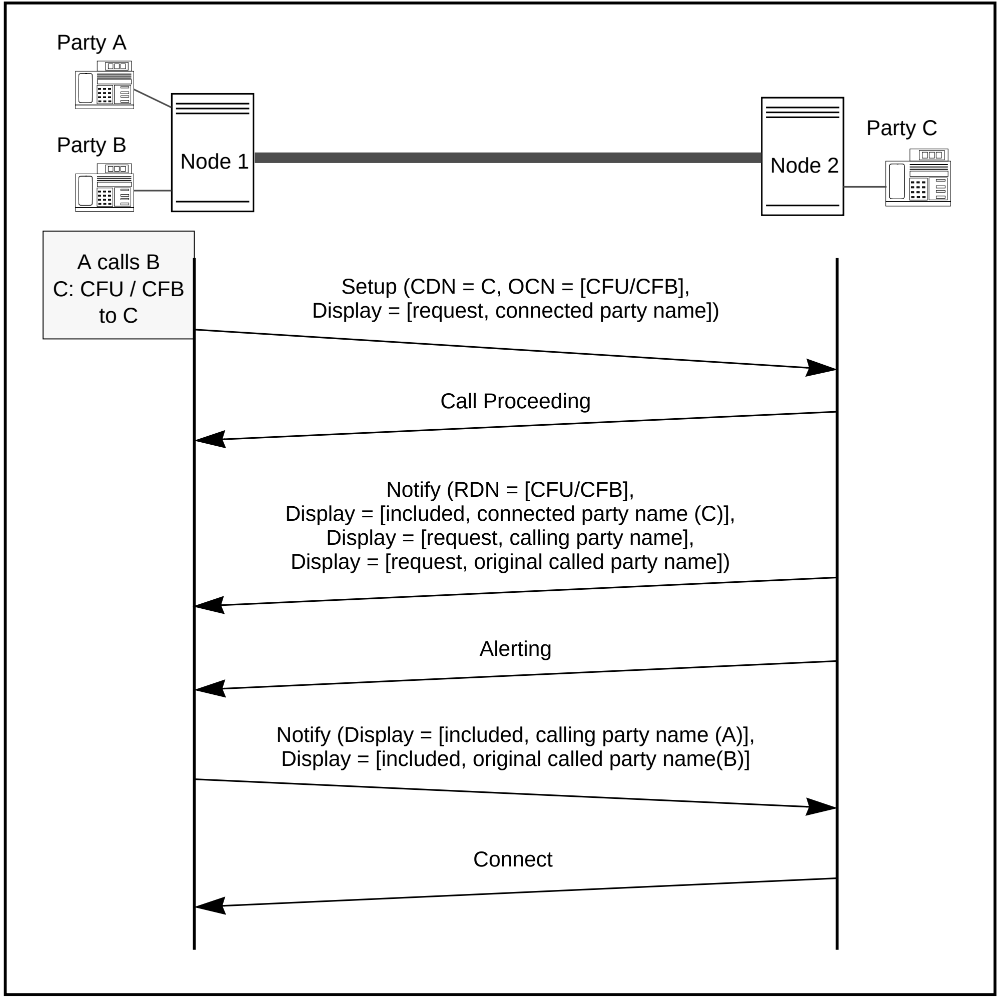


As shown in Figure 5-18, party A calls party B and is redirected to party C over a PRI with CFU or CFB. The *SETUP* message sent to party C contains a request for the connected party name. The terminating node responds with a *NOTIFY* message which includes, in addition to the redirection information

- a *Display* information element, coded as “Connected party name” and including party C’s name
- a second Display information element, if needed, coded as a request for the calling party’s name
- a third Display information element, if needed, coded as a request for the original called party’s name

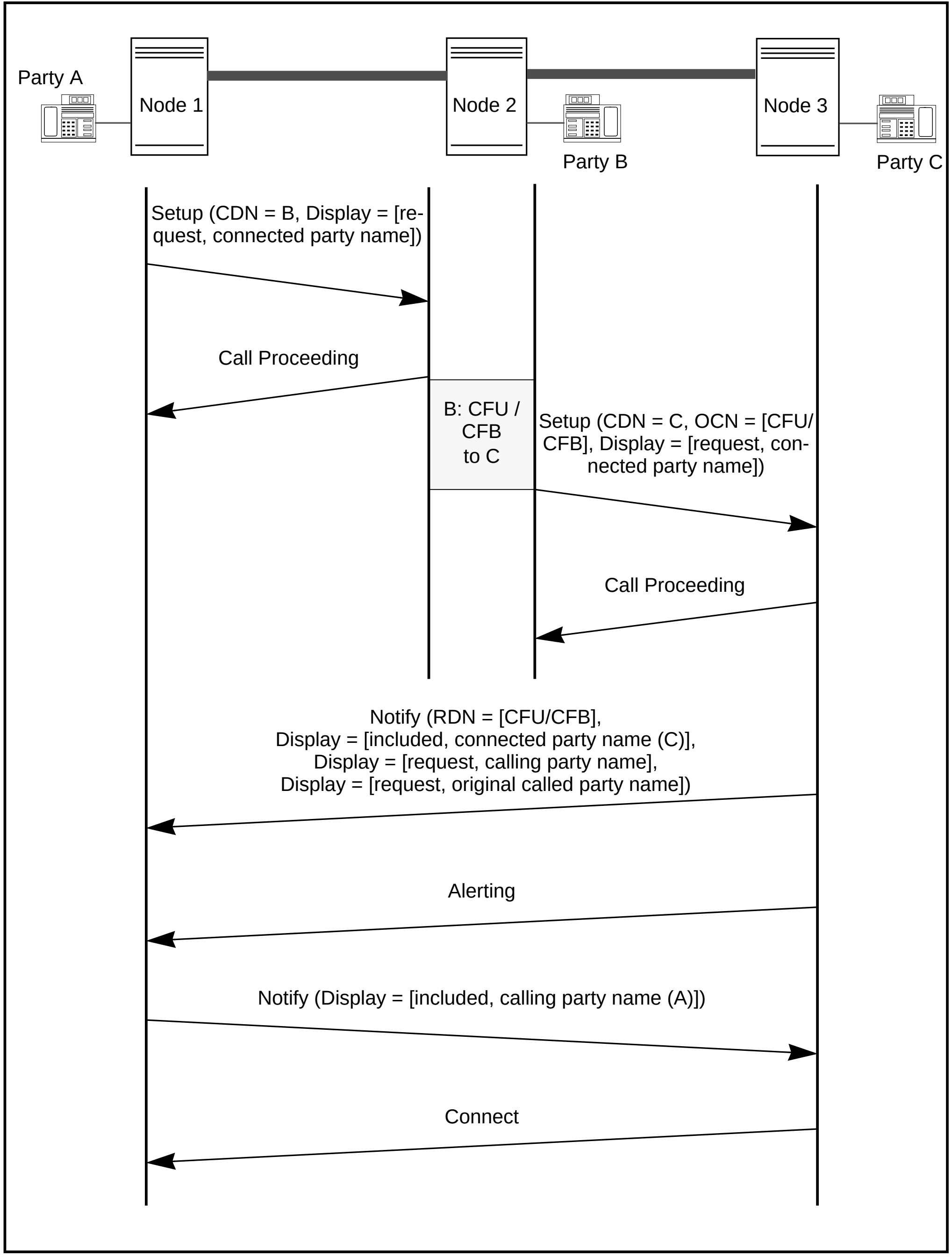
If requested to do so, the originating switch sends the calling party’s name and the original called party’s name in two *Display* information elements in a *NOTIFY* message.

Figure 5-18
Network name (query method): CFU/CFB at the local node



The original called party's name is not available if parties A, B and C are all on different nodes. For example, as shown in Figure 5-19, party A calls party B over a PRI, and the call is redirected to party C over another PRI. The originating node has access to the connected party's name (C) and the terminating node has access to the calling party's name (A), but the name of the original called party's name (B) is not available to either party A or party C.

Figure 5-19
Network name (query method): CFU/CFB at an intermediate node



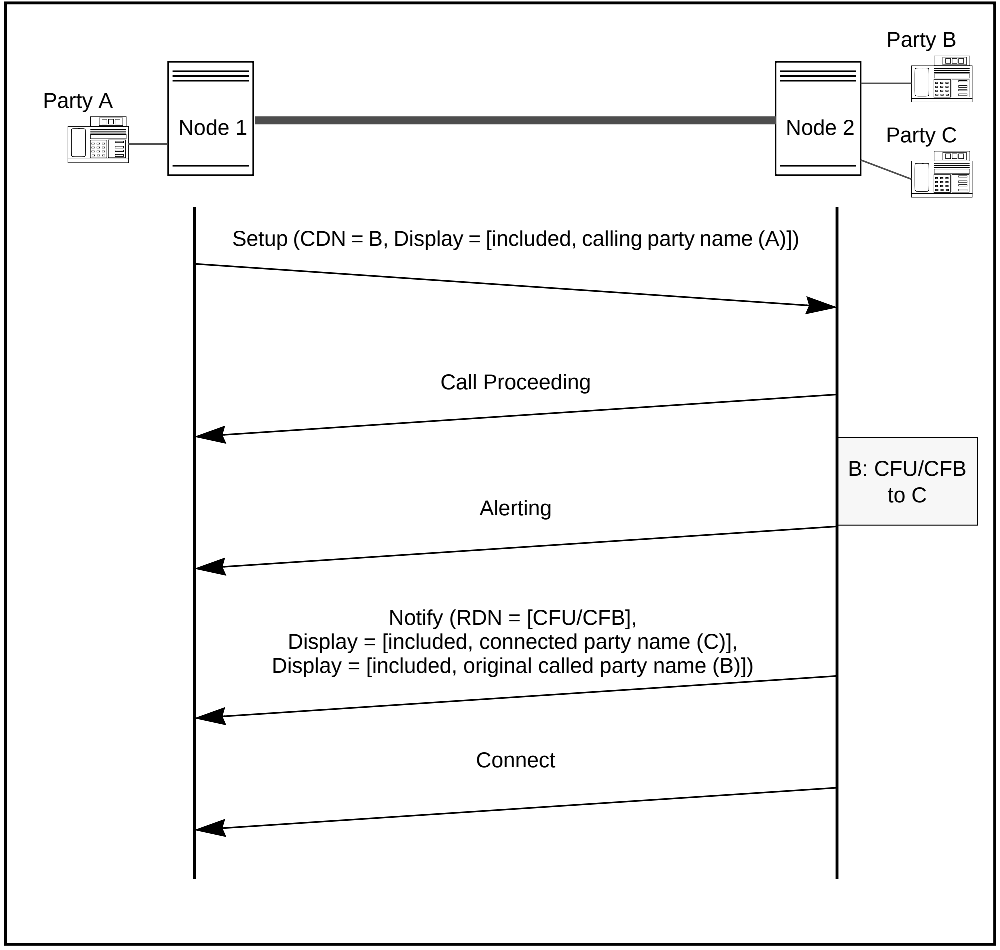
5.4.1.2 Setup method

As shown in Figure 5-20, party A calls party B over a PRI, and the call is redirected to party C with Call Forwarding Universal (CFU) or Call Forwarding Busy (CFB). The originating node sends a *SETUP* message including a *Display* information element coded as “Calling party name” and including party A’s name.

The terminating node responds with a *NOTIFY* message containing redirection information and the following

- a *Display* information element coded as “Connected party name” and including party C’s name
- a *Display* information element coded as “Original called party name” and including party B’s name

Figure 5-20
Network name (setup method): CFU/CFB at the remote node

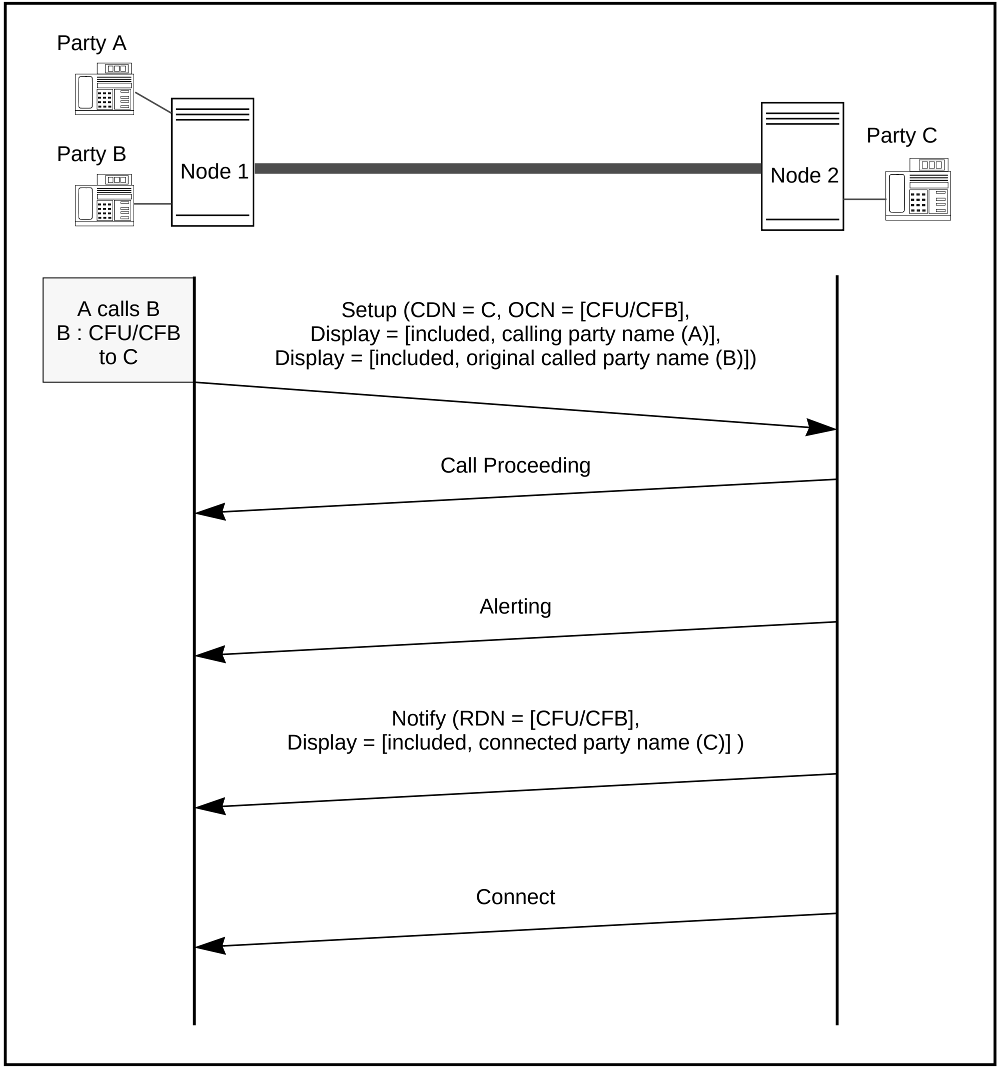


As shown in Figure 5-21, party A calls party B and is redirected to party C over a PRI with CFU or CFB. The originating node sends a *SETUP* message containing redirection information, and the following

- a *Display* information element coded as “Calling party name” and including party A’s name.
- a *Display* information element coded as “Original called party name” and including party B’s name

The terminating node responds with a NOTIFY message containing redirection information and a *Display* information element coded as “Connected party name” and including party C’s name.

Figure 5-21
Network name (setup method): CFU/CFB at the local node



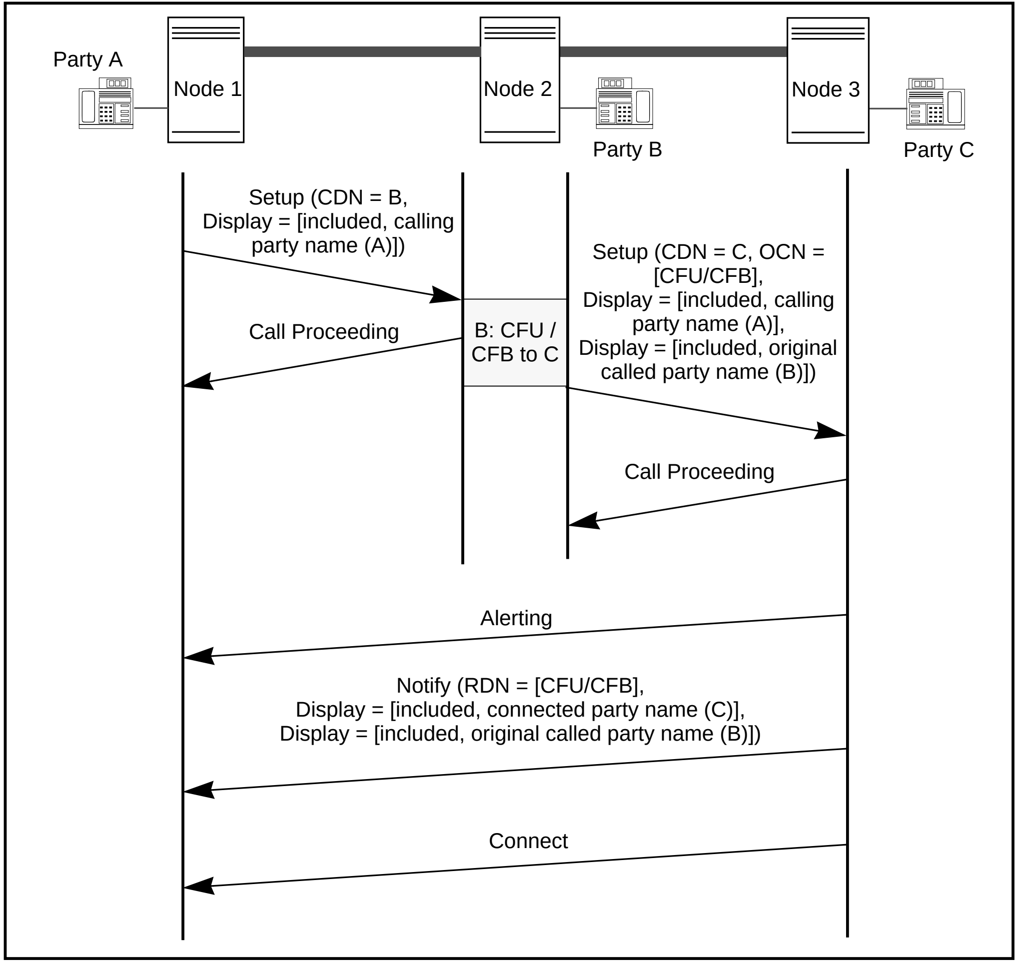
As shown in Figure 5-22, party A calls party B over a PRI and is redirected over another PRI to party C. The originating node sends a *SETUP* message containing a *Display* information element coded as “Calling party name” and including party A’s name.

Node 2 sends a *SETUP* message to Node 3, containing redirection information, a *Display* information element as described above and a second *Display* information element coded as “Original called party name” and including party B’s name.

The terminating node responds by sending a *NOTIFY* message with redirection information, and the following

- a *Display* information element, coded as “Connected party name” and including party C’s name
- a *Display* information element, coded as “Original called party name” and including party B’s name

Figure 5-22
Network name (setup method): CFU/CFB at an intermediate node



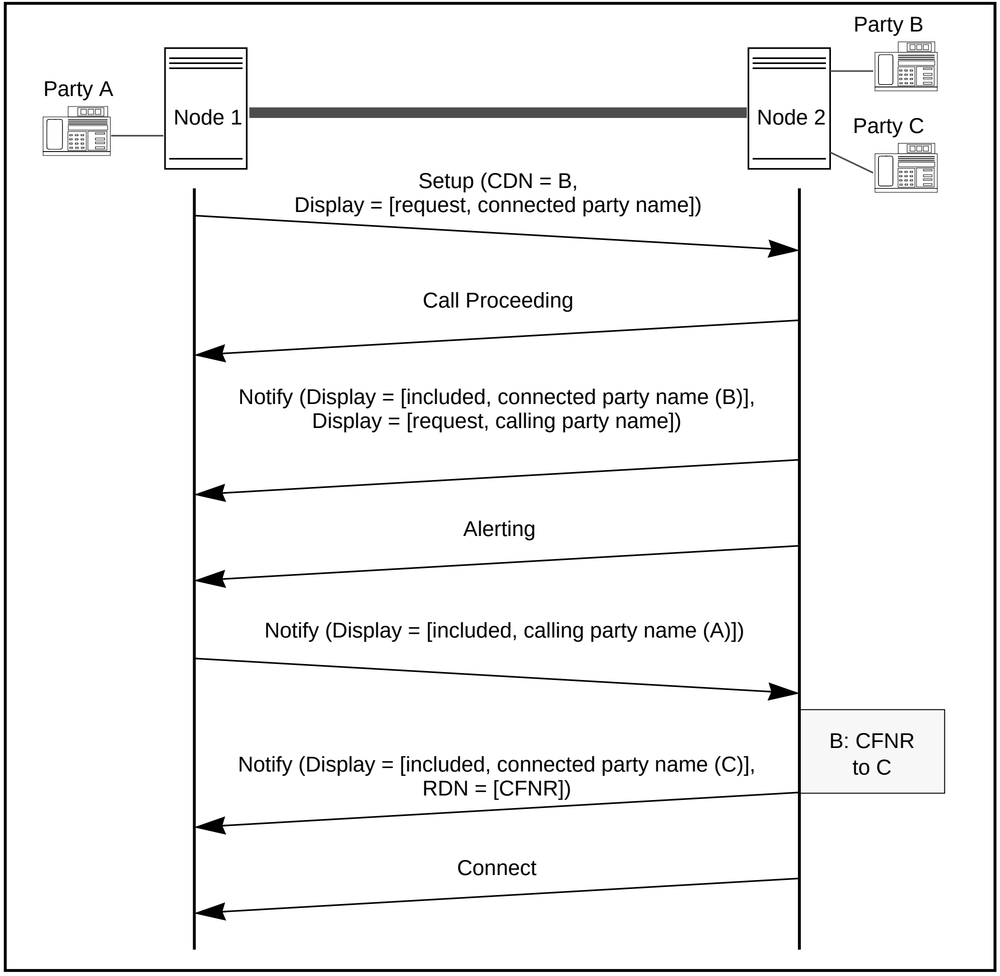
5.4.2 Call forwarding no reply

5.4.2.1 Query method

As shown in Figure 5-23, party A calls party B over a PRI, and the call is redirected to party C with Call Forwarding No Reply (CFNR). The terminating node sends a *NOTIFY* message containing the redirection information. If the originating node included a request for the connected party name in the original *SETUP* message, the *NOTIFY* message will include, in addition to the redirection information, a *Display* information element, coded as “Connected party name” and including party C’s name.

> ***Note:*** During the setup of the initial call from party A to party B, normal network name procedures are followed.

Figure 5-23
Network name (query Method): CFNR at the remote node

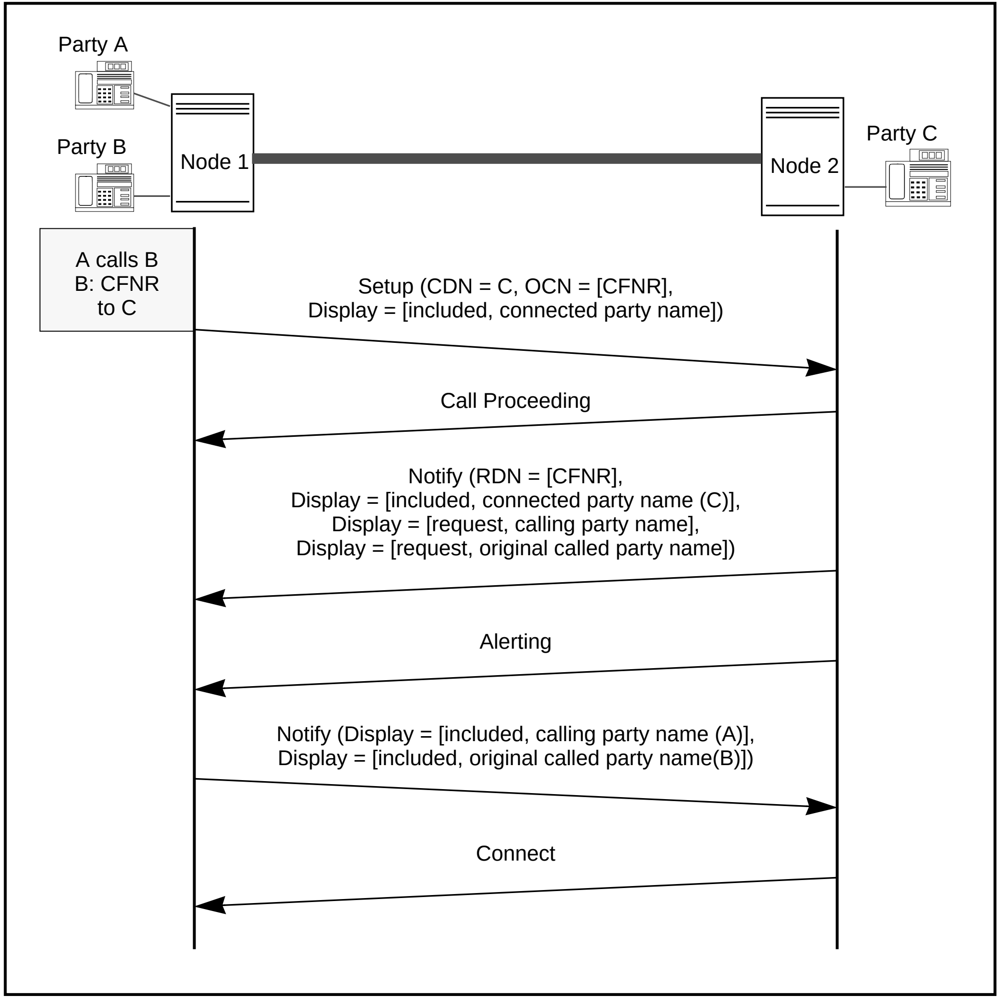


As shown in Figure 5-24, party A calls Party B and is redirected to party C over a PRI with CFNR. If the *SETUP* message sent to party C contains a request for the connected party name, the terminating node responds with a *NOTIFY* message which includes, in addition to the redirection information

- a *Display* information element, coded as “Connected party name” and including party C’s name
- a second *Display* information element, if needed, coded as a request for the calling party’s name
- a third *Display* information element, if needed, coded as a request for the original called party’s name

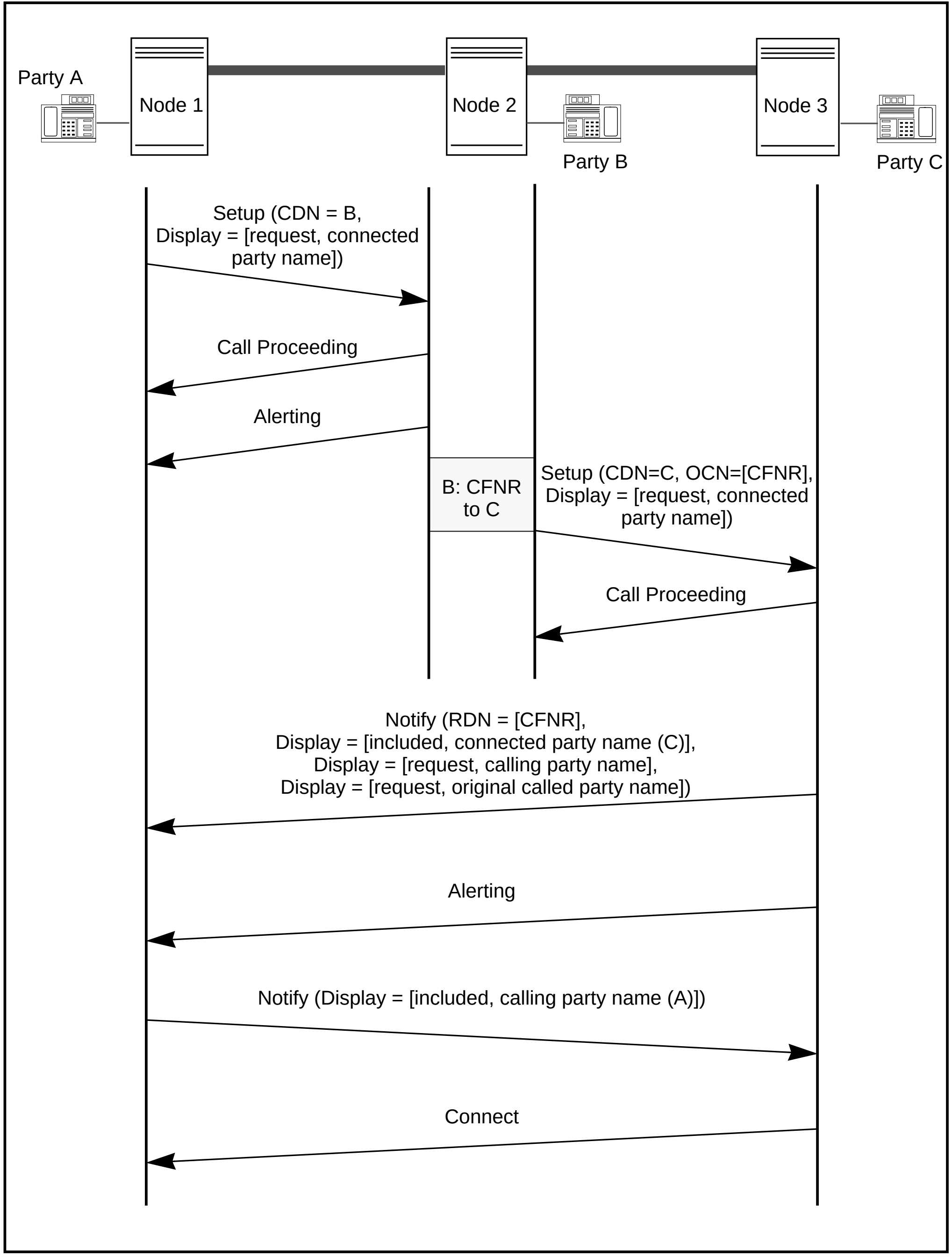
The originating switch sends a *NOTIFY* message including the calling party’s name and the original called party’s name in two *Display* information elements.

Figure 5-24
Network name (query method): CFNR at the local node



The original called party's name is not available when parties A, B and C are all on different nodes. As shown in Figure 5-25, party A calls party B over a PRI, and the call is redirected to party C over another PRI. Node 1 has access to the connected party's name (C) and node 3 has access to the calling party's name (A), but the original called party's name (B) is not available to either party A or party C.

Figure 5-25
Network name (query method): CFNR at an intermediate node



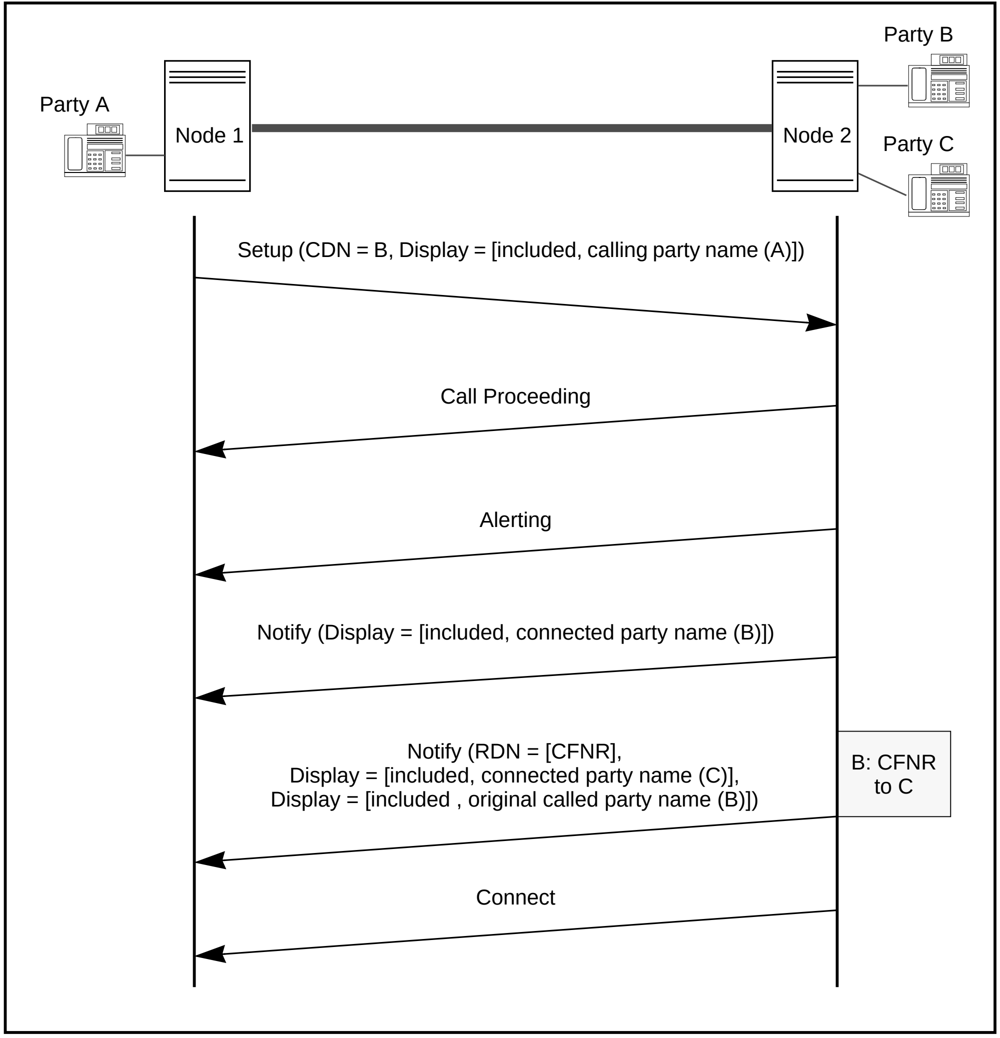
5.4.2.2 Setup method

As shown in Figure 5-26, party A calls party B over a PRI, and the call is redirected to party C with Call Forwarding No Reply (CFNR). The terminating node responds with a *NOTIFY* message containing, in addition to redirection information

- a *Display* information element, coded as “Connected party name” and including party C’s name
- a *Display* information element, coded as “Original called party name” and including party B’s name

During the setup of the initial call from party A to party B, normal network name procedures are followed.

Figure 5-26
Network name (setup method): CFNR at the remote node

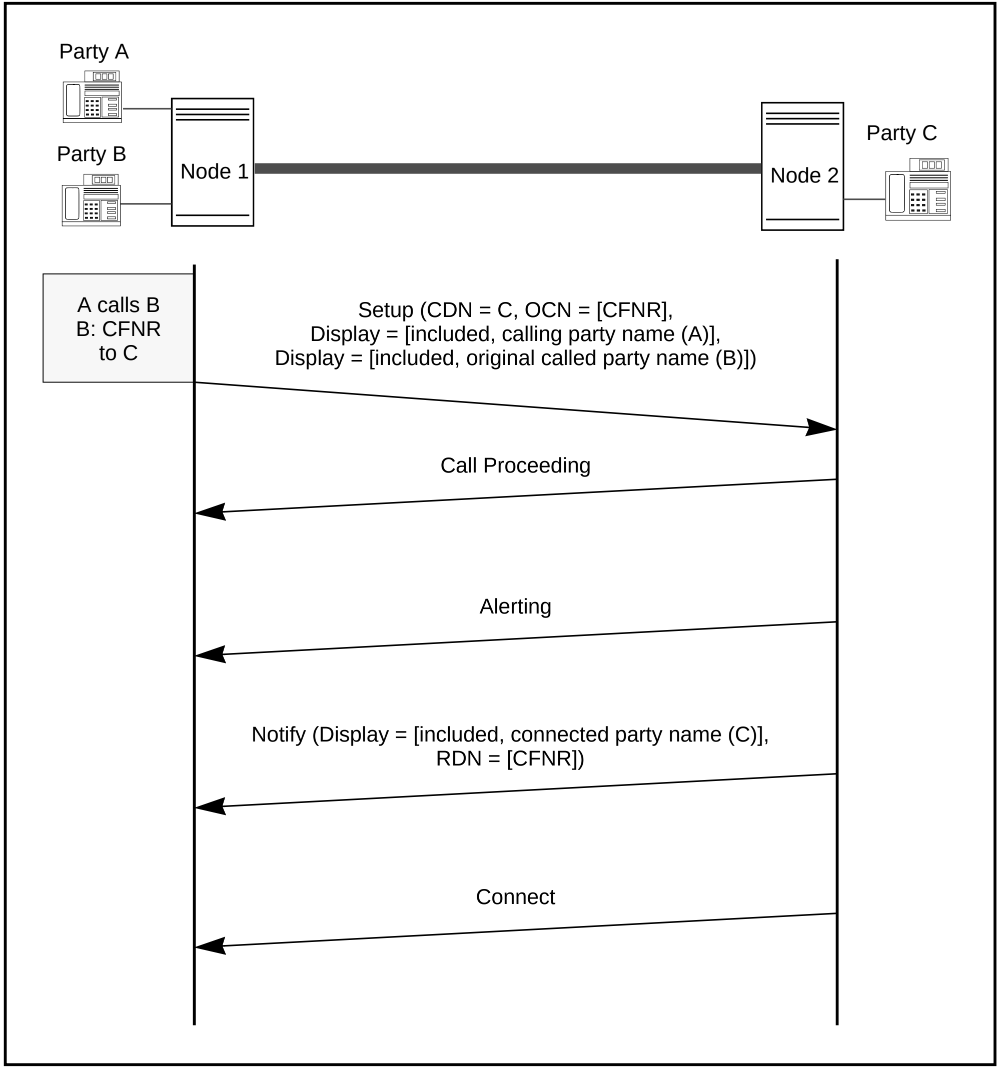


As shown in Figure 5-27, party A calls party B and is redirected to party C over a PRI with CFNR. The *SETUP* message sent to party C contains, in addition to redirection information

- a *Display* information element, coded as “Calling party name” and including party A’s name
- a *Display* information element, coded as “Original called party name” and including party B’s name

The terminating node will then respond with a *NOTIFY* message containing, in addition to redirection information, a *Display* information element, coded as “Connected party pame” and including party C’s name.

Figure 5-27
Network name (setup method): CFNR at the local node



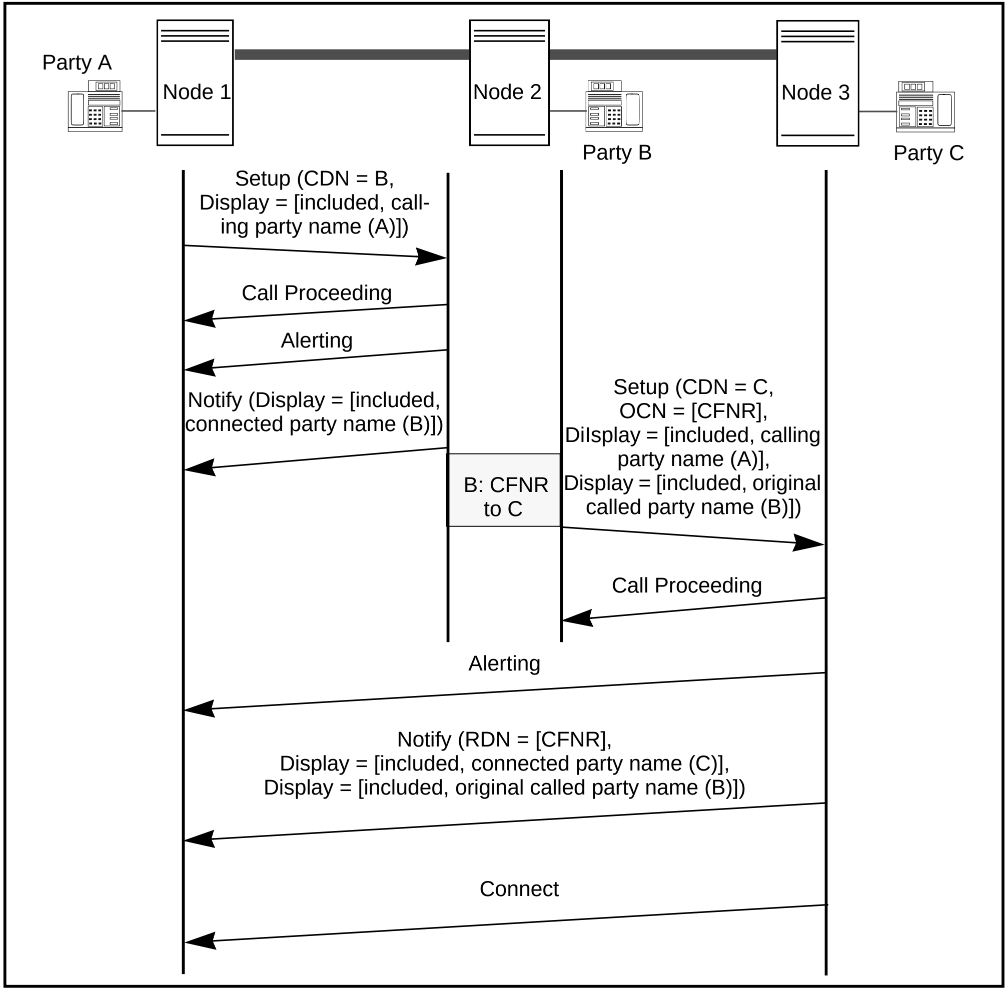
As shown in Figure 5-28, party A calls party B over a PRI, and is redirected over another PRI to party C with CFNR. The *SETUP* message sent by node 2 contains, in addition to redirection information

- a *Display* information element, coded as “Calling party name” and including party A’s name
- a *Display* information element, coded as “Original called party name” and including party B’s name

The terminating node responds with a *NOTIFY* message containing, in addition to redirection information,

- a *Display* information element, coded as “Connected party name” and including party C’s name
- a *Display* information element, coded as “Original called party name” and including party B’s name

Figure 5-28
Network name (setup method): CFNR at an intermediate node

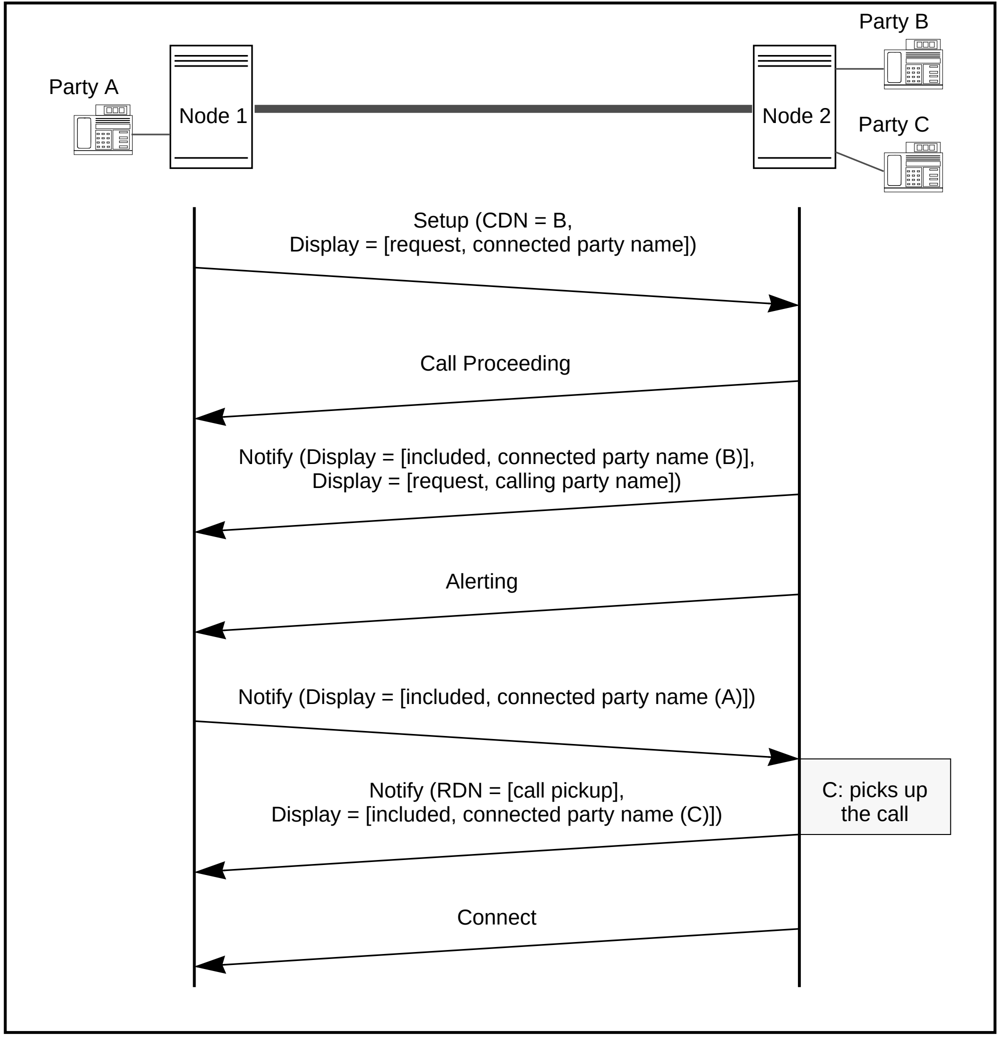


5.4.3 Call pickup

5.4.3.1 Query method

As shown in Figure 5-29, party A calls party B over a PRI, and party C activates Call Pickup during the alerting phase of the call (parties B and C are in a call pickup group). The terminating node sends a *NOTIFY* message containing the reason for redirection. If the *SETUP* message sent to party B contained a request for the called party's name, the *NOTIFY* message includes a *Display* information element, coded as "Connected party name" and containing party C's name.

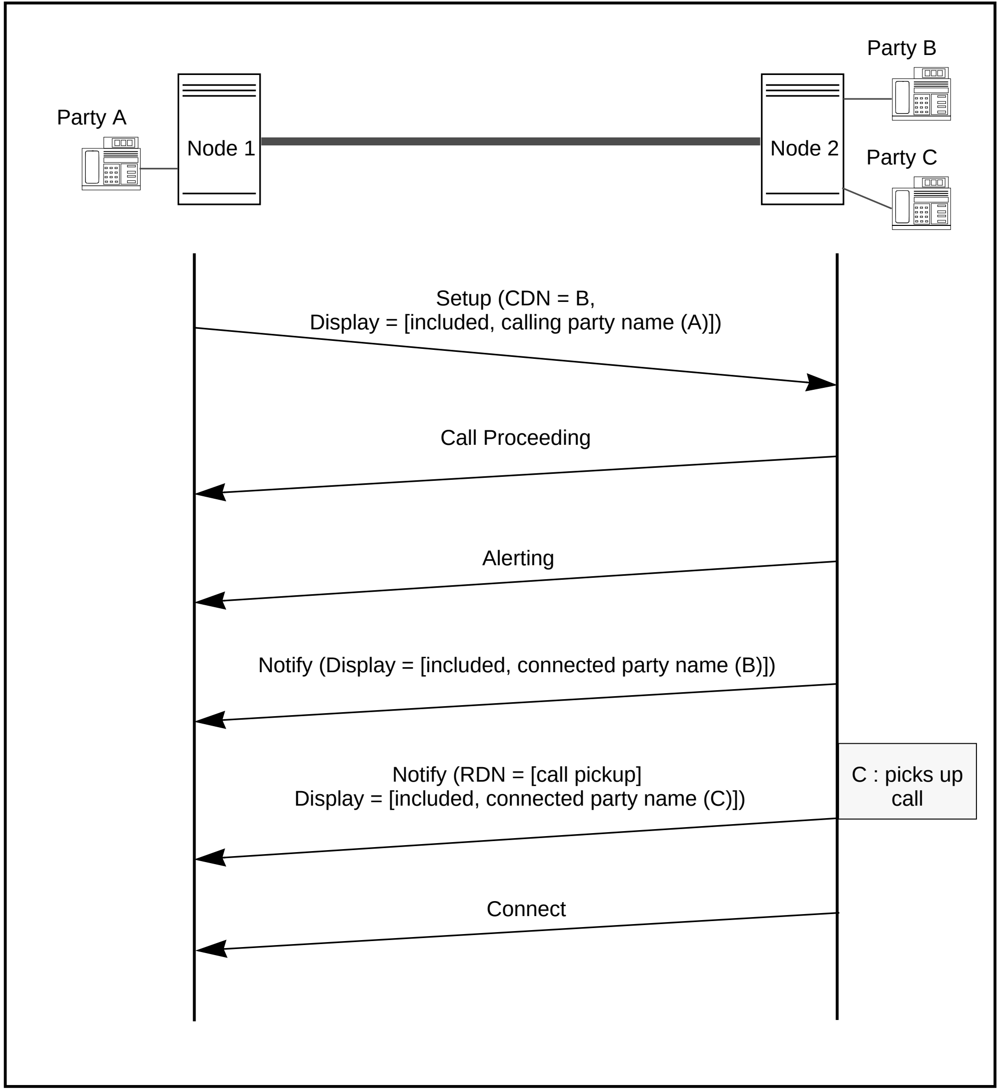
Figure 5-29
Network name (query method): Call Pickup at the remote node



5.4.3.2 Setup method

As shown in Figure 5-30, party A calls party B over a PRI, and party C activates call pickup during the alerting phase of the call (parties B and C are in a call pickup group). The terminating node sends a *NOTIFY* message containing the reason for redirection and a *Display* information element, coded as “Connected party name” and including party C’s name.

Figure 5-30
Network name (setup method): Call Pickup at the remote node



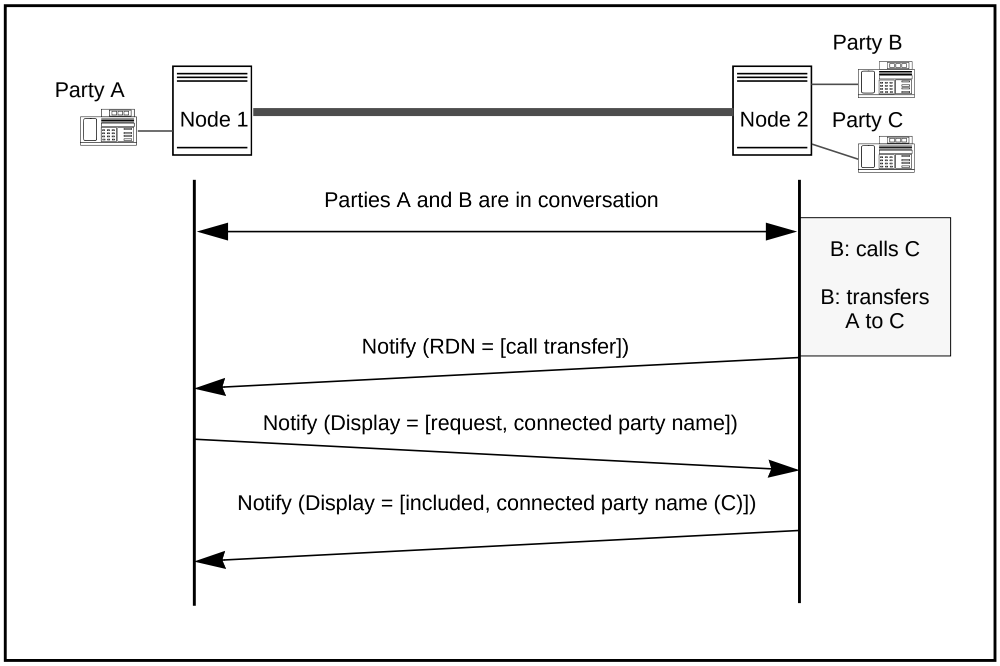
5.4.4 Call transfer

As shown in Figure 5-31, a call between parties A and B over a PRI is transferred by party B to party C. The terminating node sends a *NOTIFY* message containing the reason for redirection. The name exchange after the call transfer is not dependent on which node originated the call.

After the originating node receives the redirection information, it sends a *NOTIFY* message containing an information request for the connected party's number. In addition to this, the *NOTIFY* message includes a *Display* information element, coded as a request for the connected party's name.

The terminating node responds with a *NOTIFY* message containing the connected party's name in a *Display* information element.

Figure 5-31
Network name: Call Transfer at the remote node

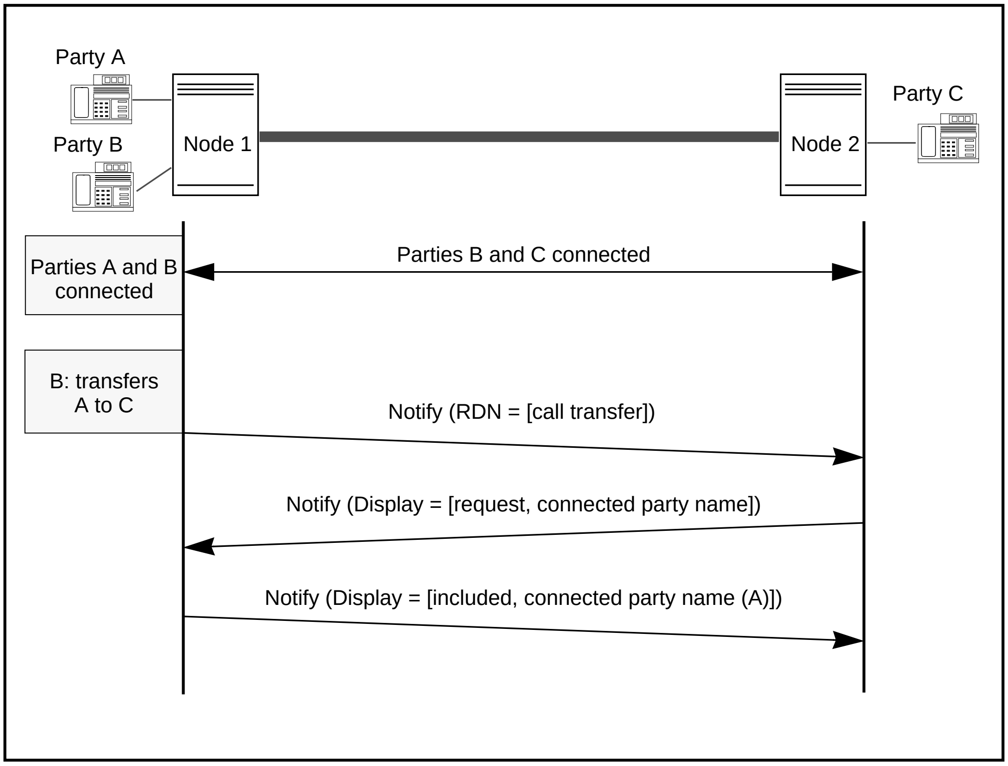


As shown in Figure 5-32, a call between parties A and B on the same node is transferred by party B over a PRI to party C. Normal network name procedures are followed during the consultation call from party B to party C. The name exchange after the call transfer is not dependent on which node originated the call.

When the call is transferred, a *NOTIFY* message is sent by the originating node containing the reason for redirection. If the terminating node requires the connected party name, it sends a *NOTIFY* message which contains, in addition to other requests (such as connected party number), a *Display* information element, coded as a request for the connected party's name.

The originating node sends a *NOTIFY* message with a *Display* information element containing the connected party's name.

Figure 5-32
Network name: Call Transfer at the local node

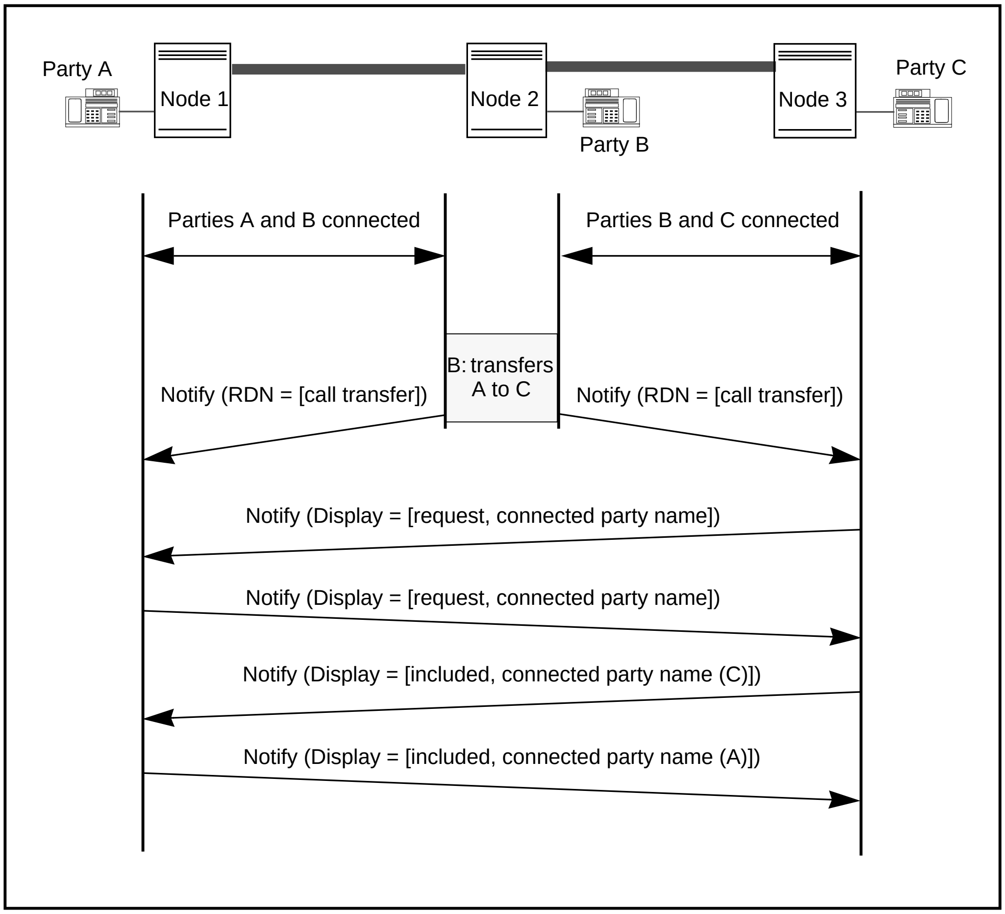


As shown in Figure 5-33, parties A and B are connected over a PRI, and the call is transferred by party B over another PRI to party C. The intermediate node sends a *NOTIFY* message to each node indicating the reason for redirection. The name exchange after the call transfer is not dependent on which nodes originated the calls.

If either party A or party C requires the connected party’s name, its node sends a *NOTIFY* message with a *Display* information element requesting the connected party’s name. The other node sends a *NOTIFY* message with a *Display* information element containing the connected party’s name.

Figure 5-33 shows simultaneous requests for the connected party’s name from both parties A and C.

Figure 5-33
Network name: Call Transfer at an intermediate node



5.5 Error procedures

Normal error procedures are followed, as described in Chapter 4-5. For example, if a *Display* information element is incorrectly coded it is ignored, following the procedures in 4.5 5.9.7.2 on page 4-140.

If a name is not available, a request for the name is ignored and the call continues normally. If no response to a name request is received, the call continues normally.

5.6 Interworking

If interworking is encountered with a non-ISDN facility (that is, not PRI or CCS7), or an ISDN trunk which does not support the procedures in this section, name exchange does not occur across the interworking point. For example, if party A calls party B over a PRI, and party B redirects the call to party C across a non-ISDN facility, name exchange procedures are allowed between parties A and B. However, no name exchange is allowed between party C and parties A or B.

The above restriction applies to all call scenarios that encounter interworking.

Chapter 5-6: Network ring again

The Network Ring Again service (NRAG) simplifies the ability of a caller to reach a called party who is busy. NRAG does this by monitoring the status of the busy party, notifiying the caller when the called party becomes idle and then automatically initiating a new call to the called party.

PRI support of NRAG allows the calling and called parties to be on different nodes. Both parties must be either Centrex or PBX lines, and in the same customer group. Neither party can be an ordinary public network user.

6.1 Overview

When party A calls party B over a PRI, and party B is busy, the call is cleared. Party A, if subscribed to NRAG, can then invoke NRAG service. Party B’s node will then monitor party B’s status and notify party A’s node when party B becomes idle. Notification is delayed briefly to ensure that party B does not immediately initiate a new call after becoming idle.

When the notification is received by party A’s node, party A is informed and must accept the NRAG recall within a certain time. If party A accepts the recall, party A’s node initiates a call to party B, identical to party’s original call attempt. If party A does not accept the recall, the NRAG request is cancelled.

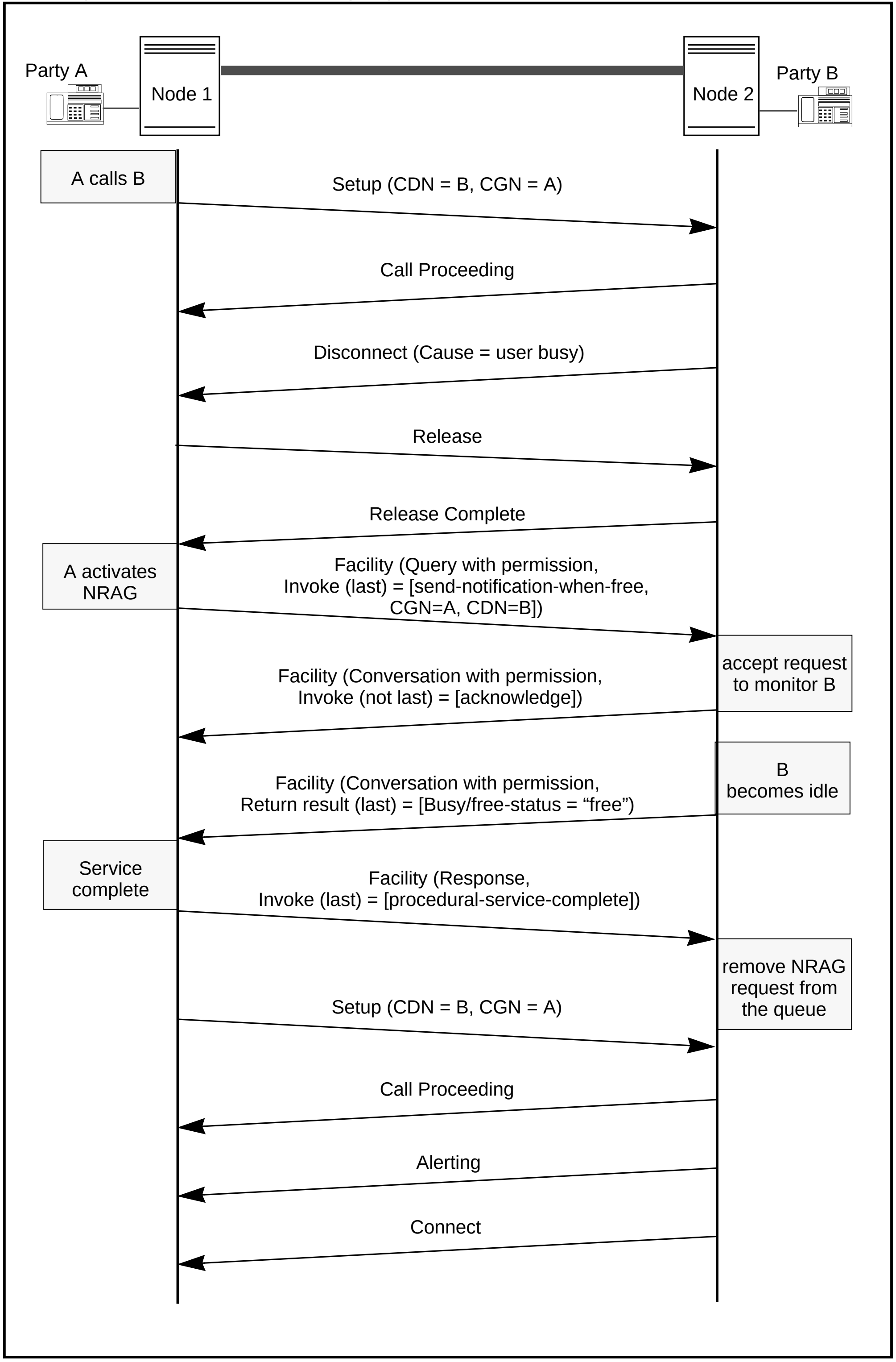
A single busy called party can have multiple NRAG requests queued against it simultaneously. When the called party becomes idle, the first party in the queue is notified. If that queued party does not reattempt a call within a specified time, the queue entry is removed and the next party in the queue is notified.

A calling party can have only one outstanding NRAG request pending at any one time.

Figure 5-34 on page 5-61 shows the message flow for an ordinary, successful NRAG request, as described above.

The following sections describe the protocol and procedures for NRAG in detail.

Figure 5-34
Message flow for Network Ring Again service



6.2 Protocol

NRAG protocol consists of the following elements, each of which is described in detail in the following sections

- *FACILITY* and *FACILITY REJECT* messages for connectionless signaling procedures
- the following information elements, all of which are in codeset 6
    - Facility
    - Origination
    - Destination
    - Options
    - Reason for return
- TCAP protocol
- timers

The detailed structure and coding of the *FACILITY* and *FACILITY REJECT* messages, the above list of information elements and TCAP protocol are described in Section 4 of this specification. Only their specific application to NRAG is described in this section.

6.2.1 *FACILITY* and *FACILITY REJECT* messages

FACILITY and *FACILITY REJECT* are the only messages used to carry the NRAG protocol. These messages are described in Section 4 of this specification.

6.2.2 Information elements

The *Facility* information element in the *FACILITY* and *FACILITY REJECT* messages is coded as follows

- octet 3, which contains the Service discriminator, is not included
- Service identifier is “Network Ring Again (NRAG)”
- User data contains a TCAP message pertaining to NRAG

The *Origination* and *Destination* information elements are coded as required to identify the calling and called party’s nodes, respectively.

The *Options* information element may be included in the *FACILITY* message if the originating node wants to be notified if an error occurs in the routing of the *FACILITY* message. Otherwise, the originating node receives no notification if the *FACILITY* message is not routed successfully. The options value field is coded as “Return message on error”.

The *Reason for return* information element is included in a *FACILITY REJECT* message if a *FACILITY* message could not be successfully routed and the originator of the *FACILITY* message included an *Options* information element, as described above. The diagnostic field in the *Reason for return* information element indicates the problem encountered.

6.2.3 TCAP protocol

This section discusses the operations, error codes and parameters that NRAG uses in TCAP messages between the originating and terminating nodes. The general TCAP message structure is described in Section Chapter 4-4: 4.5.15.2 on page 4-85.

6.2.3.1 Operations

The operations associated with the NRAG service are described in this section. The operation codes for these operations are all defined in private TCAP, using the private TCAP operation code.

The detailed definition of the operations is described using macros. An operation macro consists of the following

- A parameter list to be included in the component, as indicated by the keyword PARAMETERSET followed by the parameter list. The list may be empty or contain default or optional parameters.
- The RESULT keyword indicates that a Return result component is sent in response to the operation when it is successfully invoked. The result may have parameters. Absence of RESULT indicates that a successful outcome is not reported.
- The ERRORS keyword indicates that a Return error component is sent in response to the operation if it is not successfully invoked. ERRORS is followed by a list of the possible error codes. Absence of ERRORS indicates that an unsuccessful outcome is not reported.
- The RESPONSEOPERATIONS keyword indicates other operations that are allowed in response to this operation. RESPONSEOPERATIONS is followed by the list of allowed operations. Absence of RESPONSEOPERATIONS indicates that no other operations are linked to this one.
- The numerical operation value is shown following the “::=” symbol.

send-notification-when-party-free

The originating node uses this operation to initiate the NRAG service, by requesting the terminating node to monitor the busy/idle status of the terminating party. The terminating node is expected to respond when the terminating party becomes idle or the monitoring duration is exceeded. If the terminating node cannot perform the requested operation, an appropriate error indication is returned.

```
send-notification-when-party-free      OPERATION

PARAMETERSET      {  calling-number Digits      OPTIONAL,
                     called-number Digits       OPTIONAL,
                     Duration                   OPTIONAL,
                     Business-group-data        OPTIONAL,
                     Context                    OPTIONAL   }

RESULT            {  Busy/free-status   }

ERRORS            {  unexpected-data-value,
                     unavailable-network-resource,
                     missing-customer-record,
                     data-unavailable,
                     terminating-switch-cant-scan,
                     feature-incompatible,
                     timer-expired   }

RESPONSEOPERATIONS              {  acknowledge  }

:: =      8601  --(hex)
```

acknowledge

The terminating node uses this operation in response to the originating node when a send-notification-when-party-free operation is successfully invoked. This operation has no parameters and no response is expected.

```
acknowledge                            OPERATION

PARAMETERSET                           {   }

:: =      0806  --(hex)
```

operation-control-cancel

The originating node uses this operation to cancel the NRAG request. The reason for the cancellation is included. No response is expected.

```
operation-control-cancel               OPERATION

PARAMETERSET      {  Cancel-reason,
                     Component-id }

:: =      0901  --(hex)
```

procedural-report-error

The originating node uses this operation to indicate that there is invalid data present in a response from the terminating node. The content of the erroneous parameter is included. No response is expected.

```
procedural-report-error              OPERATION

PARAMETERSET                         {  problem-data ANY }

:: =      0803  --(hex)
```

procedural-service-complete

The originating node uses this operation to indicate that the originating party has accepted the NRAG recall request. This operation has no parameters and no response is expected.

```
procedural-service-complete          OPERATION

PARAMETERSET                         {   }

:: =      0804  --(hex)
```

procedural-service-no-longer-available

The terminating node uses this operation if the terminating party’s line is not in service or NRAG is not supported for that party. This operation has no parameters and no response is expected.

```
procedural-service-no-longer-available        OPERATION

PARAMETERSET                                  {   }

:: =      0805  --(hex)
```

6.2.3.2 Errors

The errors associated with NRAG operations are described in this section. The Return error component contains an error code to identify the reason for unsuccessful completion of an invoked operation. The error codes are defined in both national and private TCAP. National TCAP error codes are defined in ANSI T1.114. Private TCAP error codes are described in this section.

The detailed definitions of the errors are described using macros. An error macro consists of the following

- the PARAMETERSET keyword indicates whether there are any parameters associated with the error
- the numerical error value is shown following the “::=” symbol

terminating-switch-cant-scan

The terminating node rejects the NRAG request due to feature interactions, unavailable resources or other reasons.

```
terminating-switch-cant-scan          ERROR

PARAMETERSET                          {  }

:: =      252
```

feature-incompatible

Data in the Invoke component for the requested operation is invalid.

```
feature-incompatible                  ERROR

PARAMETERSET                          {  }

:: =      253
```

timer-expired

The duration timer, T7, at the terminating node expires. The duration can be provided by the originating node in the send-notification-when-party-free operation.

```
timer-expired                         ERROR

PARAMETERSET                          {  }

:: =      251
```

6.2.3.3 Parameters

This section describes all the parameters used by the operations and errors defined for NRAG. Private TCAP parameters are defined in this section. National TCAP parameters are defined in ANSI T1.114, but their usage for NRAG is shown in this section.

Digits

The Digits parameter is defined in National TCAP. It consists of the following fields:

- Type of digits - coded as “destination number” for the called number, and coded as “calling DN” for the calling number
- Nature of number - “not applicable”
- Encoding scheme - “BCD”
- Numbering plan

- Number of digits present
- Digits

Busy/free status

The Busy/free-status parameter indicates whether an identified party is free (idle) or busy.

The Busy/free status parameter is defined in private TCAP.

```
Busy/free-status  :: =   [ PRIVATE 75 ]        IMPLICIT INTEGER
                                               { free (0),
                                                 busy (1) }
```

Duration

The Duration parameter indicates the amount of time to monitor the busy/free status of an identified party. The parameter is coded in BCD (binary coded decimal) as follows

- octet 1 - hours (2 digits)
- octet 2 - minutes (2 digits)
- octet 3 - seconds (2 digits)

The Duration parameter is defined in private TCAP.

```
Duration  :: =   [ PRIVATE 125 ]       IMPLICIT OCTET STRING
```

Business-group-data

The Business-group-data parameter contains the customer group ID of an identified party. This parameter is required for validity checking since NRAG is only valid within the same customer group.

The Business-group-data parameter is defined in private TCAP.

```
Business-group-data  :: =           [ PRIVATE 117 ]
                                    IMPLICIT OCTET STRING
```

Context

The Context parameter identifies the service requesting an operation to be performed.

The Context parameter is defined in private TCAP.

```
Context  :: =   [ PRIVATE 124 ]     IMPLICIT INTEGER
                                    {nRAG (127)}
```

Component-id

The Component-id parameter is defined in Private TCAP. This parameter contains an invoke identifier.

ComponentId :: = [PRIVATE 72] IMPLICIT INTEGER

Cancel-reason

The Cancel-reason parameter contains the reason for cancelling the “send-notification-when-party-free” operation.

The Cancel-reason parameter is defined in private TCAP.

Cancel-reason :: = [PRIVATE 123] IMPLICIT INTEGER
{ user-cancelled (0),
duration-timer (1) }

6.2.4 Timers

The following timers are defined for use with NRAG.

T-GT	Guard Timer - Used by the terminating node to delay notification to the queued NRAG party when the monitored party becomes idle. This delay ensures that the monitored party remains idle. T-GT can range from 0 to 6 seconds.
T-QAT	Queue Advance Timer - Used by the terminating node to remove an NRAG queue entry, after having sent notification that the monitored party is idle. T-QAT should be set greater than T2. T-QAT can range from 0 to 40 seconds.
T2	Used by the originating node to determine if the called party responds to the NRAG recall request. T2 can range from 8 to 32 seconds.
T5	Used by the originating node to determine if the terminating node fails to respond to the NRAG invocation request. T5 can range from 2 to 10 seconds.
T6	Used by the originating node to limit the duration of the wait for the monitored party to become idle. T6 can range from 5 to 30 minutes.
T7	Used by the terminating node to limit the duration of the wait for the monitored party to become idle. T7 should be set greater than the sum of T6 and T2. T7 can range from 5 to 31 minutes.

6.3 Procedures

The details for coding the TCAP packages and components mentioned in the following procedures are described in section 6.2 on page 5-62.

6.3.1 Actions at the originating node

When a called party is busy, the terminating node clears the call by sending a *DISCONNECT* message with a *Cause* information element containing *Cause* value #17 “User busy”. If the calling party subscribes to NRAG, NRAG can be invoked by the calling party.

The originating node sends a TCAP Query with permission package to the terminating node with the following content

- a new Transaction ID
- an Invoke (last) component, with the operation send-notification-when-party-free
- the parameters within the operation contain the calling and called parties numbers, the business group identification and the originating node’s duration timer (T6)

The originating node then starts timer T5. If timer T5 expires, the above TCAP message is sent again, but with a new Transaction ID. If timer T5 expires a second time, NRAG is cancelled and the Transaction ID is released.

If the originating node receives a TCAP Conversation with permission package, with the same Transaction ID as the previously sent Query with permission package, and containing an Invoke (not last) component with an acknowledge operation, the originating node

- stops timer T5
- sends an NRAG activation confirmation to the invoking party
- starts timer T6

If timer T6 expires, the originating node

- sends a TCAP Response package to the terminating node containing an Invoke (last) component with the operation operation-control-cancel, and a Cancel-reason parameter is set to “duration-timer”
- releases the Transaction ID

If the originating node receives a TCAP Conversation with permission package containing a Return result (last) component with the Busy/free-status parameter set to “free”, and timer T6 has not expired, the originating node

- stops timer T6
- sends to the invoking party an NRAG recall indication
- sends a TCAP Response package to the terminating node containing an Invoke (last) component with the operation procedural-service-complete
- starts timer T2

- releases the Transaction ID

If the invoking party is busy, the above procedures are not performed. That is, no recall attempt is made. When the invoking party becomes idle, the originating node sends a Conversation with permission package to the terminating node containing an Invoke (last) component with the operation send-notification-when-party-free. No parameters are included and the Transaction ID is unchanged. Timer T5 is started and the originating node follows the above procedures, except that a Return result may be received in this case without first receiving an acknowledge operation.

If timer T2 expires, the originating node

- stops the NRAG recall to the invoking party
- cancels the NRAG invocation

If the invoking party accepts the NRAG recall, the originating node

- stops timer T2
- establishes a new call to the called party, using the contents of the original *SETUP* message

If the called party is busy, the calling party can choose to invoke NRAG again. That is, the originating node does not do this automatically.

If the invoking NRAG party decides to cancel the NRAG request before its operation is complete, the originating node

- sends a TCAP Response package to the terminating node containing an Invoke (last) component with the operation operation-control-cancel, and a Cancel-reason parameter set to “user-cancelled”
- releases the Transaction ID

6.3.2 Actions at the terminating node

When the terminating node receives a TCAP Query with permission package containing an Invoke (last) component with the operation send-notification-when-party-free, the terminating node

- allocates the Transaction ID
- places the monitor request in the NRAG queue for the identified party
- sends a TCAP Conversation with permission package to the originating node, containing an Invoke (not last) component with the acknowledge operation
- starts timer T7; timer T7 is set to the lesser of the received Duration parameter (if present) and the terminating node’s default value for timer T7

When the monitored party becomes free (idle), timer T-GT is started. If the monitored party is still free when the timer expires, the terminating node

- starts timer T-QAT
- sends a TCAP Conversation with permission package to the originating node, containing a Return result (last) component with the Busy/free-status parameter set to “free”

If, while timer T-QAT is running, the terminating node receives a TCAP Response package from the originating node, containing an Invoke (last) operation with the operation procedural-service-complete, the terminating node

- stops timer T7
- releases the Transaction ID

Calls to the monitored party from other than the invoking NRAG party, and calls originated by the monitored party, are not rejected while timer T-QAT is running. Thus, a new call from the invoking NRAG party may not complete.

If timer T7 expires, timer T-QAT expires or the terminating node receives a TCAP Response package from the originating node, containing an Invoke (last) component with the operation operation-control-cancel, the terminating node

- stops all timers
- if timer T7 or T-QAT expired, sends a TCAP Response package to the originating node, containing a Return error component with the error code “timer-expired”
- removes the queue entry for the invoking NRAG party
- releases the Transaction ID
- acts on the next NRAG queue entry, if one exists, by notifying the associated invoking party that the monitored party is free, following the procedures above

6.3.3 Error procedures

Errors are reported with either a TCAP Response or a Unidirectional package. Since a message containing the TCAP Unidirectional package does not require a transaction ID, this package is used when

- a protocol error makes the Transaction ID impossible to determine
- the error occurred in a TCAP Response package; since this package ends the TCAP transaction, the other node has already released the Transaction ID

In all other cases, a TCAP Response package is used to report the error.

Two types of errors can occur during a TCAP transaction

- protocol errors
- application errors

6.3.3.1 Protocol errors

Protocol errors are caused by incorrectly coded TCAP packages. These include errors in the format of a component, invalid or duplicate component IDs or an invalid parameter format. Protocol errors are reported with a Reject component. The Reject component contains a problem code to describe the protocol error. Problem code definitions can be found in Section 4 of this specification.

> ***Note:*** A protocol error occurs in cases where a TCAP package is sent to a node that has already released the Transaction ID. For example, if timers T6 and T7 expire simultaneously at the originating and terminating nodes, respectively.

6.3.3.2 Application errors

Application errors are those errors which are specific to NRAG operations. Application errors are only detected if the TCAP package, and the included component, do not contain protocol errors. Application errors are reported in a TCAP package (as described above), containing a Return error component with one of the error codes described in section 6.2.3.2 on page 5-65. The Transaction ID, if allocated, is released.

If the application error occurs in a TCAP Response package, it is reported in a TCAP Unidirectional package containing an Invoke (last) component with the operation procedural-report-error. The problem-data parameter contains the parameter that was in error.

Chapter 5-7: Network automatic call distribution

The Network Automatic Call Distribution (NACD) service provides the capability to distribute incoming calls among a set of NACD groups. Each NACD group may have one or more agents. Each NACD group can be on the local node or on remote nodes. The NACD service exchanges information between nodes to determine the best routing for each call to, for example, evenly distribute calls among NACD groups.

7.1 Overview

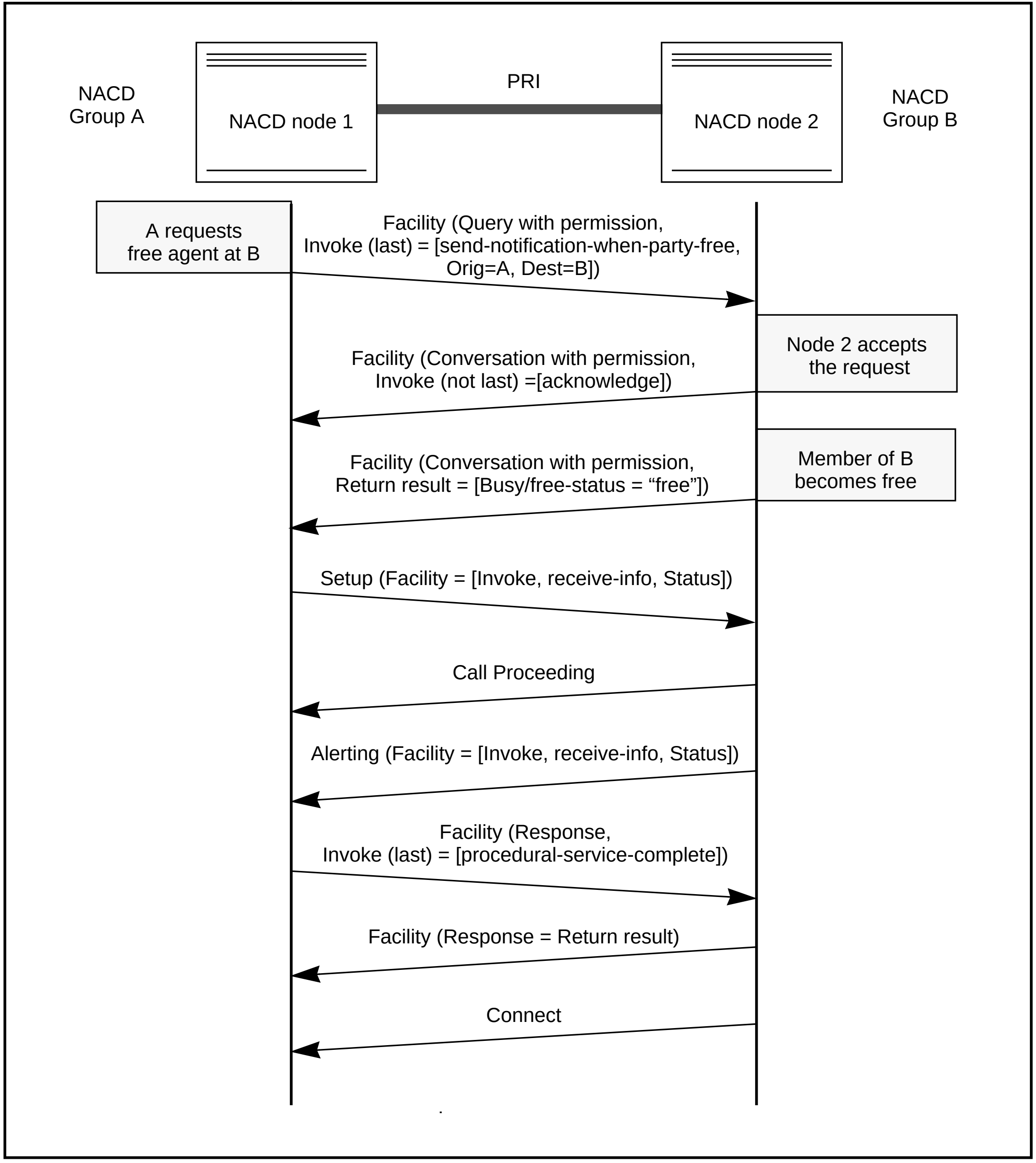
The NACD service uses ISDN PRI connections between nodes supporting NACD to perform the following functions

- regular (periodic) broadcast of load status information from one NACD group to other NACD groups
- notification to other NACD groups when an NACD group is no longer able to handle additional calls
- queuing on a destination node for a free NACD agent when the originating NACD group has no available agents to handle an incoming call
- rerouting of an incoming call to an NACD group located on a different node
- notification to other NACD groups when an NACD group is added or removed from service

The load status information (LSI) is an integer which indicates the relative availability of an NACD group to handle additional calls. An LSI of 0 indicates that an NACD group has no free agents. The term resource index (RI) is used interchangably with LSI in this chapter.

Figure 5-35 on page 5-74 shows a sample message flow for rerouting an incoming call between NACD groups over PRI after first queuing for a free agent at the destination NACD group.

Figure 5-35
Message flow for request rerouting of an NACD call



7.2 Protocol

NACD protocol consists of the following elements, each of which is described in detail in the following sections

- *SETUP* and *ALERTING* messages for call-associated signaling procedures
- *FACILITY* and *FACILITY REJECT* messages for connectionless signaling procedures
- the following information elements, all of which are in codeset 6

  - Facility
  - Origination
  - Destination
  - Options
  - Reason for return

- TCAP protocol
- ROSE protocol
- timers

The detailed structure and coding of the *FACILITY* and *FACILITY REJECT* messages, the above list of information elements, TCAP protocol and ROSE protocol are described in Section 4 of this specification. Only their specific application to NACD is described in this section.

7.2.1 *FACILITY* and *FACILITY REJECT* messages

FACILITY and *FACILITY REJECT* messages are used to carry the NACD TCAP protocol. The *SETUP* and *ALERTING* messages are used to carry the call-associated ROSE components. These messages are described in Section 4 of this specification.

7.2.2 Information elements

The *Facility* information element in the *FACILITY* and *FACILITY REJECT* messages is coded as follows

- Service discriminator is “Supplementary services (TCAP)”
- Service identifier is “Network Automatic Call Distribution (NACD)”
- User data contains a TCAP message component pertaining to NACD

The *Facility* information element in the *SETUP* and *ALERTING* messages is coded as follows

- Service discriminator is “Supplementary services (ROSE)”
- Service identifier is “Network Automatic Call Distribution (NACD)”
- User data contains a ROSE component pertaining to NACD

The *Origination* and *Destination* information elements are coded as required to identify the calling and called party’s nodes, respectively.

The *Options* information element may be included in the *FACILITY* message if the originating node wants to be notified if an error occurs in the routing of the *FACILITY* message. Otherwise, the originating node receives no notification if the *FACILITY* message is not routed successfully. The options value field is coded as “Return message on error”.

The *Reason for return* information element is included in a *FACILITY REJECT* message if a *FACILITY* message could not be successfully routed and the originator of the *FACILITY* message included an *Options* information element, as described above. The diagnostic field in the *Reason for return* information element indicates the problem encountered.

7.2.3 ROSE protocol

This section discusses the operations, error codes and parameters that NACD uses in ROSE call-associated messages between the originating and terminating nodes. The general ROSE message structure is described in Section Chapter 4-4: 4.5.15.1 on page 4-77.

7.2.3.1 Operations

The operations associated with the NACD service are described in this section. The detailed definition of the operations is described using macros. An operation macro consists of the following

- If the operation has parameters, a parameter list is included, as indicated by the keyword ARGUMENT followed by the parameter list. The list may contain default or optional parameters.
- The RESULT keyword indicates that a Return result component is sent in response to the operation when it is successfully invoked. The result may have parameters. Absence of RESULT indicates that a successful outcome is not reported.
- The ERRORS keyword indicates that a Return error component is sent in response to the operation if it is not successfully invoked. ERRORS is followed by a list of the possible error codes. Absence of ERRORS indicates that an unsuccessful outcome is not reported.
- The numerical operation value is shown following the “::=” symbol.

Receive info operation

The receive info operation is included in call control messages when a call is rerouted.

```
receive-info    OPERATION
                ARGUMENT      {  CallType       OPTIONAL,
                                 CallPriority   OPTIONAL,
                                 Status         OPTIONAL,
                                 TransactionId  OPTIONAL}

                :: =     7E05     --(hex)
```

7.2.3.2 Errors

There are no ROSE error components defined for NACD.

7.2.3.3 Parameters

This section describes all the parameters used by the ROSE operations and errors defined for NACD.

CallType

The call type “immediate-reroute” indicates that the call was immediately rerouted, without being queued. Call type “time-reroute” indicates that the call was queued at the original NACD group before being rerouted. Call type “immediate-then-time-reroute” indicates that the call was both immediately rerouted and queued at the original NACD group.

```
CallType          :: =      [ APPLICATION 0 ] IMPLICIT INTEGER
                            {  direct-incoming (0),
                               immediate-reroute (1),
                               time-reroute (2),
                               immediate-then-time-reroute (3)}
```

CallPriority

The call priority is an integer value ranging from 0 to 3, where 0 is the highest priority.

```
CallPriority      :: =      [ APPLICATION 1 ] IMPLICIT INTEGER
                            (0 .. 3)
```

Status

The Status parameter contains the Load Status Information (LSI or Resource Index) of the sending NACD group. A value of 0 indicates that no more calls should be rerouted to that group.

```
Status            :: =      [ APPLICATION 5 ] IMPLICIT INTEGER
```

TransactionId

The transaction id is 4 octets long and contains a TCAP transaction id.

```
TransactionId     :: =      [ 7 ] IMPLICIT OCTET STRING
```

7.2.4 TCAP protocol

This section discusses the operations, error codes and parameters that NACD uses in TCAP messages between the originating and terminating nodes. The general TCAP message structure is described in Section Chapter 4-4: 4.5.15.2 on page 4-85.

7.2.4.1 Operations

The operations associated with the NACD service are described in this section. The operation codes for these operations are all defined in private TCAP, using the private TCAP operation code.

The detailed definition of the operations is described using macros. An operation macro consists of the following

- A parameter list to be included in the component, as indicated by the keyword PARAMETERSET followed by the parameter list. The list may be empty or contain default or optional parameters.
- The RESULT keyword indicates that a Return result component is sent in response to the operation when it is successfully invoked. The result may have parameters. Absence of RESULT indicates that a successful outcome is not reported.
- The ERRORS keyword indicates that a Return error component is sent in response to the operation if it is not successfully invoked. ERRORS is followed by a list of the possible error codes. Absence of ERRORS indicates that an unsuccessful outcome is not reported.
- The RESPONSEOPERATIONS keyword indicates other operations that are allowed in response to this operation. RESPONSEOPERATIONS is followed by the list of allowed operations. Absence of RESPONSEOPERATIONS indicates that no other operations are linked to this one.
- The numerical operation value is shown following the “::=” symbol.

status-update

An NACD node uses this operation to notify a destination NACD group of the originating NACD group’s status. No response is expected.

```
status-update                OPERATION

PARAMETERSET           {  orig-NACD-DN digits,
                          dest-NACD-DN digits,
                          Status                    OPTIONAL }

:: =        7E03    --(hex)
```

status-exchange

An NACD node uses this operation to exchange status information between originating and a terminating NACD groups. The operation includes the originating group’s status and the response contains the terminating group’s status.

```
status-exchange                  OPERATION

PARAMETERSET           {  orig-NACD-DN digits,
                          dest-NACD-DN digits,
                          Status }

RESULT                 { Status }

:: =        FE04    --(hex)
```

send-notification-when-party-free

This operation is used by an originating NACD group to monitor a destination NACD group until an agent becomes available. The terminating node is expected to respond when a terminating agent becomes idle or the monitoring duration is exceeded. If the terminating node cannot perform the requested operation, an appropriate error indication is returned.

```
send-notification-when-party-free       OPERATION

PARAMETERSET        {   orig-NACD-DN Digits     OPTIONAL,
                        dest-NACD-DN Digits     OPTIONAL,
                        CallType,
                        CallPriority,
                        TimeInQueue,
                        Context,
                        Status                  OPTIONAL   }

RESULT              {   Busy/free-status   }

ERRORS              {   unexpected-data-value,
                        unavailable-network-resource,
                        missing-customer-record,
                        data-unavailable,
                        terminating-switch-cant-scan,
                        feature-incompatible,
                        queue-full,
                        night-service,
                        timer-expired   }

RESPONSEOPERATIONS                  {  acknowledge  }

:: =        8601  --(hex)
```

acknowledge

The terminating node uses this operation in response to the originating node when a send-notification-when-party-free operation is successfully invoked.

The status of the terminating NACD group is optionally included as a parameter.

```
acknowledge                 OPERATION

PARAMETERSET          { Status                   OPTIONAL }

:: =      0806    --(hex)
```

operation-control-cancel

The originating node uses this operation to cancel an NACD monitor request. The reason for the cancellation, and optionally the terminating NACD group's status, is included.

```
operation-control-cancel    OPERATION

PARAMETERSET        {  Cancel-reason,
                       Component-id,
                       Status                    OPTIONAL }

RESULT

:: =      0901    --(hex)
```

procedural-service-complete

The originating node uses this operation to inform the terminating switch that the NACD monitor operation is complete and that the call has been redirected to the terminating NACD group. The status of the originating NACD group is optionally included in the operation.

```
procedural-service-complete OPERATION

PARAMETERSET        { Status          OPTIONAL}

RESULT

:: =      0804    --(hex)
```

procedural-report-error

The originating node uses this operation to indicate that there is invalid data present in a response from the terminating node. The content of the erroneous parameter is included. No response is expected.

```
procedural-report-error          OPERATION

PARAMETERSET          {  problem-data ANY }

:: =       0803  --(hex)
```

7.2.4.2 Errors

The errors associated with NACD operations are described in this section. The Return error component contains an error code to identify the reason for unsuccessful completion of an invoked operation. The error codes are defined in both national and private TCAP. National TCAP error codes are defined in ANSI T1.114. Private TCAP error codes are described in this section.

The detailed definitions of the errors are described using macros. An error macro consists of the following

- the PARAMETERSET keyword indicates whether there are any parameters associated with the error
- the numerical error value is shown following the "::=" symbol

terminating-switch-cant-scan

The terminating switch rejects the NACD monitor request due to feature interactions, unavailable resources or other reasons.

```
terminating-switch-cant-scan    ERROR

PARAMETERSET                    { }

:: =       252
```

feature-incompatible

Data in the Invoke component for the requested operation is invalid.

```
feature-incompatible            ERROR

PARAMETERSET                    { }

:: =       253
```

queue-full

```
queue-full                      ERROR

PARAMETERSET                    { }

:: =       8
```

night-service

```
night-service                ERROR

PARAMETERSET                 { }

:: =      251
```

timer-expired

The duration timer, T2, at the terminating node expires.

```
timer-expired                ERROR

PARAMETERSET                 { }

:: =      10
```

7.2.4.3 Parameters

This section describes all the parameters used by the operations and errors defined for NACD. Private TCAP parameters are defined in this section. National TCAP parameters are defined in ANSI T1.114, but their usage for NACD is shown in this section.

CallType

The CallType parameter is defined in Private TCAP. This parameter is used to indicate the type of the call for which a transfer request is being made. The call type definitions are in section 7.2.3.3 on page 5-77.

```
CallType        :: =      [ PRIVATE 64 ] IMPLICIT INTEGER
                          {  direct-incoming (0),
                             immediate-reroute (1),
                             time-reroute (2),
                             immediate-then-time-reroute (3) }
```

CallPriority

The CallPriority parameter is defined in Private TCAP. See section 7.2.3.3 on page 5-77 for its description.

```
CallPriority    :: =      [ PRIVATE 65 ] IMPLICIT INTEGER
```

TimeInQueue

The TimeInQueue parameter is defined in Private TCAP. This parameter is used to indicate the time, in seconds, that the call has been queued at the original NACD group before a reroute request.

```
TimeInQueue     :: =      [ PRIVATE 66 ] IMPLICIT INTEGER
```

Context

The Context parameter is defined in Private TCAP. This parameter is used to indicate which service is requesting the operation. For NACD service, this parameter is always set to “nACD”.

```
Context          :: =     [ PRIVATE 67 ] IMPLICIT INTEGER
                          {  nACD (126) }
```

Status

The Status parameter is defined in Private TCAP. This parameter provides the LSI (load status information, or resource index) of one NACD group to another NACD group. A value of 0 indicates that no more calls should be rerouted to that group.

```
Status           :: =     [ PRIVATE 69 ] IMPLICIT INTEGER
```

CancelReason

The CancelReason parameter is defined in Private TCAP. This parameter is used to provide the reason for cancelling the send-notification-when-party-free operation.

```
CancelReason     :: =     [ PRIVATE 71 ] IMPLICIT INTEGER
                          {  user-cancelled (0),
                             duration-timer (1),
                             call-answered (2),
                             reserve-timer (3) }
```

ComponentId

The ComponentId parameter is defined in Private TCAP. This parameter contains an invoke identifier.

```
ComponentId      :: =     [ PRIVATE 72 ] IMPLICIT INTEGER
```

Digits

The Digits parameter is defined in Private or National TCAP. This parameter contains the number of a party in an NACD call or of an NACD group. Use of the private or national tag for the Digits parameter depends on the coding of the Type of Digits field, as shown below.

```
Digits    :: =    [ PRIVATE 73 ] IMPLICIT OCTET STRING
                                                  -- private

Digits    :: =    [ 4 ] IMPLICIT OCTET STRING     -- national
```

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
Type of digits								1
Nature of Number								2
Numbering Plan				Encoding				3
Number of Digits								4
Digits								5 ... n

Type of digits (octet 1)

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	1	Called party number (national)
1	1	1	1	1	0	1	0	Originating NACD group (private)
1	1	1	1	1	1	0	0	Destination NACD group (private)

All other values are reserved.

Nature of Number (octet 2)

8	7	6	5	4	3	2	1	
-	-	-	-	-	-	-	0	National number
-	-	-	-	-	-	-	1	International number
-	-	-	-	-	-	0	-	Presentation allowed
-	-	-	-	-	-	1	-	Presentation restricted

All other values are reserved.

Note: Only the “National number” and “Presentation allowed” codings are supported.

Numbering Plan (octet 3)

8 7 6 5	
0 0 0 0	Unknown or not applicable
0 0 0 1	ISDN Numbering
0 0 1 0	Telephony Numbering

All other values are reserved.

Note: Only the “Unknown or not applicable” coding is supported.

Encoding (octet 3)

4 3 2 1	
0 0 0 1	BCD (Binary Coded Decimal)
0 0 1 0	IA5 (Internaqtional Alphabet 5)

All other values are reserved.

Note: Only the “BCD” coding is supported.

Number of Digits (octet 4)

Number of digits in the Digits field.

Digits (octet 5)

Each octet contains one IA5 digit (in bits 7 to 1) or two BCD digits (in bits 4 to 1 and bits 8 to 5) in each octet. For BCD encoding, the high-order (first) digit is placed in bits 4 to 1. If there is an odd number of BCD digits, bits 8 to 5 of the last octet are ignored.

Digit	**IA5 : 7 6 5 4 3 2 1**	**BCD : 8 7 6 5**
		4 3 2 1
0	0 1 1 0 0 0 0	0 0 0 0
1	0 1 1 0 0 0 1	0 0 0 1
2	0 1 1 0 0 1 0	0 0 1 0
3	0 1 1 0 0 1 1	0 0 1 1
4	0 1 1 0 1 0 0	0 1 0 0
5	0 1 1 0 1 0 1	0 1 0 1
6	0 1 1 0 1 1 0	0 1 1 0
7	0 1 1 0 1 1 1	0 1 1 1
8	0 1 1 1 0 0 0	1 0 0 0
9	0 1 1 1 0 0 1	1 0 0 1
*	0 1 0 1 0 1 0	1 1 0 1
#	0 1 0 0 0 1 1	1 1 1 0

7.2.5 Timer values

The following timers are defined for use with NACD.

T1	Resend Timer - This is the time a node waits for a response to a TCAP Query package. This timer can be restarted one time for each sent TCAP Query package. The value of timer T1 is 5 seconds.
T2	Duration Timer - This is the time an NACD agent can be reserved for a rerouted NACD call. The value of timer T2 is 15 seconds.
T4	Sanity Timer - This is the maximum time that a transaction can remain active on the terminating node. The value of timer T4 is 30 seconds.
T5	Originator Cancel Timer - This is the time the originating node waits for a response to a TCAP Query package containing an

operation-control-cancel or procedural-service-complete operation. The value of timer T5 is 5 seconds.

7.3 Procedures

7.3.1 Adding a new NACD group

When a new NACD group is added, it is the responsibility of the other NACD groups to establish a dialog with the new group. Once this initial dialog is complete, calls can be rerouted to the new group.

To establish the dialog, an originating NACD group sends a TCAP Query with permission package to the terminating node (that is, the node with the new NACD group) with the following content

- a new Transaction ID
- an Invoke (last) component, with the operation status-exchange
- identification of the originating and destination NACD groups in the orig-NACD-DN and dest-NACD-DN parameters
- a Status parameter containing the load status information of the originating NACD group

The originating node then starts timer T1. If timer T1 expires, the old Transaction ID is released and the above TCAP package is sent again, but with a new Transaction ID. If timer T1 expires a second time, the operation is cancelled and the Transaction ID is released.

When the destination NACD group receives the above TCAP package, and the originating NACD group is not known, no further action is taken. If the originating NACD group is known, the terminating node sends a TCAP Response package to the originating node with the following content

- a Return result (last) component
- a Status parameter containing the load status information of the destination NACD group

When the originating node receives the above Response package while timer T1 is running, it

- stops timer T1
- releases the Transaction ID
- allows reroutes to the destination NACD group, assuming the received load status information allows it

If timer T1 is not running when the TCAP Response package is received, the originating node ignores it.

7.3.2 Broadcast of load status information

An NACD group broadcasts its load status information (LSI) to all other known NACD groups under the following circumstances

- removal of the NACD group
- the NACD group is busy, and can not accept reroute requests from other groups
- periodically, to ensure that other NACD groups have its up to date load status information

An originating node broadcasts an NACD groups status by sending to each known NACD group a TCAP Unidirectional package with the following content

- a new Transaction ID
- an Invoke (last) component, with the operation status-update
- a Status parameter with the load status information (LSI) of the originating NACD group (the LSI is 0 if the NACD is being deleted or is busy)

No reply is expected.

7.3.3 Direct reroute

A direct reroute on an incoming call to an NACD group to another NACD group occurs under one of the following circumstances

- original NACD group is overloaded, that is, can not service the call
- the call queues for too long at the original NACD group
- on successful completion of a request reroute to a destination NACD group

The protocol for a direct reroute operation is performed with ROSE components within the call control messages (*SETUP* and *ALERTING*) associated with the rerouted call. In addition, when call forwarding is used to reroute the call, the procedures and protocol in Chapter 5-4: Network redirection and reason, apply.

The *SETUP* message sent to the terminating node for a direct rerouted NACD call, which did not first undergo request rerouting, contains a ROSE Invoke component with the following content

- operation of receive-info
- a CallType parameter with the appropriate reason for the reroute
- a CallPriority parameter with the priority of the rerouted call
- a Status parameter with the load status information of the originating NACD group

If the call was first request rerouted, the Invoke component with the receive-info operation contains just one parameter, TransactionId, with the TCAP Transaction ID associated with the request reroute procedure.

The *ALERTING* message sent to the originating node contains a ROSE Invoke component with the following content

- operation of receive-info
- a Status parameter with the load status information of the destination NACD group

7.3.4 Request reroute

An originating NACD group performs a request reroute when it decides to queue an incoming NACD call to wait for a free agent on a destination NACD group.

7.3.4.1 Actions at the originating node

The originating node sends a TCAP Query with permission package to the terminating node with the following content

- a new Transaction ID
- an Invoke (last) component, with the operation send-notification-when-party-free
- the parameters within the operation contain the numbers of the originating and destination NACD groups, the call type, call priority, length of time that the call has already been queued, the context of the operation (that is, NACD) and the load status information of the originating NACD group

The originating node then starts timers T1. If timer T1 expires, the old Transaction ID is released and the above TCAP message is sent again, but with a new Transaction ID. If timer T1 expires a second time, the request reroute operation is cancelled and the Transaction ID is released.

If the originating node receives a TCAP Response package containing a Return error component, the originating node

- stops timer T1
- releases the Transaction ID
- cancels the request reroute operation

If the originating node receives a TCAP Conversation with permission package containing an Invoke (not last) component with an acknowledge operation, the originating node

- stops timer T1
- sends confirmation to the originating NACD group

If an agent at the originating NACD group becomes available to process the call or the caller abandons, the originating NACD group cancels the request reroute. In this case, the originating node

- sends a TCAP Response package to the terminating node containing an Invoke (last) component with the operation operation-control-cancel, and a Cancel-reason parameter set to “call-answered” or “user-abandoned”
- starts timer T5

If timer T5 expires, the originating node sends an error indication to the terminating node.

If the originating node receives a TCAP Response package containing a Return result component, before timer T5 expires, the originating node

- stops timer T5
- releases the Transaction ID

If the originating node receives a TCAP Conversation with permission package containing a Return result (last) component with the Busy/free-status parameter set to “free”, the originating node

- sends to the originating NACD group an indication that an agent at the destination NACD group is available
- sends a TCAP Response package to the terminating node containing an Invoke (last) component with the operation procedural-service-complete
- starts timer T5

If timer T5 expires, the originating node cancels the NACD request reroute operation, and sends an error indication to the terminating node.

If the originating node receives a TCAP Response package containing a Return result (last) component, before timer T5 expires, the originating node

- stops timer T5
- releases the Transaction ID
- redirects the incoming NACD call to the destination NACD group, using the direct reroute procedures in section 7.3.3 on page 5-88

7.3.4.2 Actions at the terminating node

When the terminating node receives a TCAP Query with permission package containing an Invoke (last) component with the operation send-notification-when-party-free, the terminating node

- allocates the Transaction ID
- verifies the information received and that the originating NACD group is allowed to queue for a free agent on the destination NACD group

- places the monitor request in the queue for the destination NACD group
- sends a TCAP Conversation with permission package to the originating node, containing an Invoke (not last) component with the acknowledge operation
- starts timer T4

If the queue request is rejected, the terminating node sends a TCAP Response package to the originating node containing a Return error component with the reason for the rejection (for example, night service or queue full). The Transaction ID is released.

When the monitored party becomes free (idle), the terminating node

- reserves the NACD agent for the rerouted call
- starts timer T2
- sends a TCAP Conversation with permission package to the originating node containing a Return result (last) component with the Busy/free-status parameter set to “free”

If, while timer T2 is running, the terminating node receives a TCAP Response package from the originating node containing an Invoke (last) operation with the operation procedural-service-complete, the terminating node waits for a direct reroute from the originating to the terminating NACD group.

If a direct reroute arrives before timer T2 or timer T4 expires, the terminating node

- stops timers T2 and T4
- completes the call to the reserved NACD agent
- removes the NACD agent reservation and queue entry
- releases the Transaction ID

Calls to the monitored NACD agent from other than the originating NACD group are rejected while timer T2 is running.

If timer T2 or T4 expires, or the terminating node receives a TCAP Response package from the originating node, containing an Invoke (last) component with the operation operation-control-cancel, the terminating node

- stops all timers
- if timer T2 or T4 expired, sends a TCAP Response package to the originating node, containing a Return error component with the error code “timer-expired”
- removes the NACD agent reservation and queue entry

- releases the Transaction ID

7.3.5 ROSE error procedures

There is ROSE protocol associated with NACD procedures. ROSE components which are not coded properly or are not acted on are ignored.

7.3.6 TCAP error procedures

Errors are reported with either a TCAP Response or a Unidirectional package. Since a message containing the TCAP Unidirectional package does not require a transaction ID, this package is used when

- a protocol error makes the Transaction ID impossible to determine
- the error occurred in a TCAP Response package; since this package ends the TCAP transaction, the other node has already released the Transaction ID

In all other cases, a TCAP Response package is used to report the error.

Two types of errors can occur during a TCAP transaction

- protocol errors
- application errors

7.3.6.1 Protocol errors

Protocol errors are caused by incorrectly coded TCAP packages. These include errors in the format of a component, invalid or duplicate component IDs or an invalid parameter format. Protocol errors are reported with a Reject component. The Reject component contains a problem code to describe the protocol error. Problem code definitions can be found in Section 4 of this specification.

> ***Note:*** A protocol error occurs in cases where a TCAP package is sent to a node that has already released the Transaction ID.

7.3.6.2 Application errors

Application errors are those errors which are specific to NACD operations. Application errors are only detected if the TCAP package, and the included component, do not contain protocol errors. Application errors are reported in a TCAP package (as described above), containing a Return error component with one of the error codes described in section 6.2.3.2 on page 5-65. The Transaction ID, if allocated, is released.

If the application error occurs in a TCAP Response package, it is reported in a TCAP Unidirectional package containing an Invoke (last) component with the operation procedural-report-error. The problem-data parameter contains the parameter that was in error.

Chapter 5-8: Equal access

Equal Access service allows a PRI user to select a specific carrier for calls to the public network. Not all calls require carrier selection, depending on the geographical separation between the calling and called parties and regulatory requirements.

Equal Access service can be used in conjunction with any call setup request, whether it is an ordinary basic call or there are interactions with other supplementary services.

Carrier selection can be performed by the PRI user in one of the following ways

- on a per call basis
- subscribed default
- network-determined

In the ISDN, the carrier code provided explicitly by the user or selected by default, is conveyed and used for routing until the point of entry into the selected carrier network, at which point it is typically discarded.

This section describes how Equal Access service can be accessed by PRI users.

8.1 Transit network selection on a per call basis

The PRI user can specify that a specific carrier (for example, inter-exchange carrier) be used on a per call basis. This is accomplished by including one of the following in the *SETUP* message

- using the equal access dialing plan in the *Called party number* information element
- using a *Transit network selection* (TNS) information element in the *SETUP* message.

The equal access dialing plan consists of special prefix digits before the public number of the called station. For example “10XXX” in the U.S., where “XXX” is the code assigned to the selected carrier. In addition to 10-digit public numbers, “10XXX-0+” or “10XXX-0-” dialing can be used to reach a carrier’s operator service. Other special numbers to reach other carrier services may also be available, but these are beyond the scope of this specification.

If a TNS is included in the *SETUP* message, it is coded as follows

- Type of Network Identification - “National”
- Network Identification Plan - “Carrier identification code”
- Network Identification Characters - the 3 or 4 digit code of the selected carrier, coded as IA5 characters (leading zeros are significant and must be included)

If a TNS is included in the *SETUP* message, but the call (as indicated by the *Called party number* information element) does not require carrier routing to complete, the TNS is ignored by the network.

8.2 Default transit network selection

If the user does not include a *Transit network selection* information element (TNS) in the *SETUP* message and there is no carrier specified in the *Called party number* information element, and the call must be routed via a carrier , a default carrier will be selected by the originating network switch. For public calls, the default carrier can be

- subscribed to by the customer, on an interface basis
- if there is no customer or interface subscription default, a network-determined default is used

For private calls, the default carrier is selected through translations. The subscribed default carrier for private and public calls may be different.

8.3 Interworking

The Equal Access service supports interworking with non-ISDN public network facilities, in those networks which support equal access. That is, the carrier identification code is carried in the non-ISDN portion of the public network (for example, Feature Group D signaling).

8.4 Error Procedures

If a carrier selection is required for a call, and the user includes in the *SETUP* message

- both a TNS and equal access dialing in the *Called party number* information element
- or, the carrier identification code in the TNS or *Called party number* information element is incorrect

The network clears the call by sending a *RELEASE COMPLETE* message with a *Cause* information element containing *Cause* value #2 “No route to specified transit network”.

Chapter 5-9:
Special number service

Each special number service is handled in a specific manner within the network. In general, the special numbers do not conform to any numbering plan, therefore their meaning is determined by the network supplying PRI service. Use of the special number routes the call to the requested service.

This specification does not specify in detail how to provide these services as there are no specific PRI requirements. Access to these services is via the public network dialing plan, as coded in the *Called party number* information element in the *SETUP* message.

There may be charges for the Special Number Services as tariffed by the network provider. PRI users may wish to consult with their local network provider before using these services.

Special Number Services can include, but are not necessarily limited to, the following

• 0	public network operator
• 411	directory information
• 611	repair service
• 911	emergency
• 1-800	automatic reverse charging for toll calls
• 1-900	special business services
• 0+	operator assisted calls

Chapter 5-10: Integrated services access

Integrated Services Access (ISA) permits a PRI to replace several dedicated trunk groups, resulting in efficiencies and simplified administration. ISA provides the capability to signal information, on a per call basis, which specifies the specific service needed to complete a call.

Dedicated facilities continue to exist in the network for these services, but a single PRI connection allows access to all of these facilities. ISA supports calls for both incoming and outgoing services.

10.1 Services supported

An ISA call follows normal call control procedures as described in Part 4 of this specification. Information provided in the Network specific facilities (NSF) and the Called party number information elements, within the *SETUP* message, is used to select the appropriate service.

The following services are supported.

OUTWATS	OUTWATS is a service provided by telephone companies which permits a customer to originate calls to telephones in a specific geographical area, sometimes identified by a zone or band. The PRI user may request a specific band number.
INWATS	INWATS is a public long distance service which allows a subscriber to receive calls originating within specified service areas without a charge to the caller. Typically the caller would dial a 1-800 number.
FX	Foreign Exchange (FX) service connects a customer's location to a remote public exchange. This service provides the equivalent of local service at the remote exchange.
TIE	These are private, dedicated facilities between two private network switches, either Centrex or PBX.

PRIVATE	Private calls allow PRI users to access customer-specific routing and number translations.
PUBLIC	Public calls allow PRI users to access the public switched network.

10.2 Procedures

The *Network specific facilities* information element (NSF) is an optional information element which can be included in the *SETUP* message in both the network-to-user and user-to-network directions. The format of the NSF is described in Section 4 of this specification.

For ISA service, the following are mandatory fields in the NSF

- Service Selector (Binary Facility Coding Value)
- Service Identifier

The following NSF fields are never generated by the network, and are ignored if received from the user

- Type of Network Identification
- Network Identification Plan
- Network Identification Characters (IA5 Characters)

In addition to the NSF, the Numbering Plan Identification (NPI) in the *Called party number* information element is also used for call routing. By default, when the NPI is “E.164”, the public switched network will be used to route the call. When the NPI is “Private”, the dialing plan is determined by customer-specific translations in the network. These translations may include the use of MSN digit strings. Reserved private facilities (for example, TIE) may be selected.

It is possible to originate and terminate both public and private calls without the use of ISA. If an NSF if not included in the *SETUP* message, the public or private nature of the call is determined by the NPI in the *Called party number* information element, as described above.

10.2.1 Call originations

Calls originated by the PRI user specify the type of service they wish to access with the Network specific facilities information element (NSF) in the *SETUP* message. The NSF contains the following fields

- a Service Selector (Binary Code Facility Coding Value) which specifies the type of service requested (FX, TIE, OUTWATS, PUBLIC or PRIVATE)

- a Service Identifier to identify a specific facility (for example, trunk identifier or OUTWATS zone) to be used to route the call; the allowed Service Identifier values for each service selector are arranged between the telephone company and the user

On receipt of an NSF with a valid Service Selector, the network routes the call primarily based on the Service Selector and the Service Identifier, rather than other information (for example, the *Called party number* information element). Checks are also made to ensure that other information in the *SETUP* message (for example, the *Bearer capability* information element) is consistent with the facilities selected.

Specific routing procedures must be arranged between the telephone company and the user.

10.2.2 Call terminations

Calls terminating to a PRI which subscribes to ISA include an indication of the type of service being used by including a *Network specific facilities* information element (NSF) in the *SETUP* message. The NSF contains the following fields

- a Service Selector (Binary Code Facility Coding Value) which specifies the type of service used (FX, TIE, INWATS, PUBLIC or PRIVATE)
- a Service Identifier to identify a specific facility (for example, trunk identifier) used for the call; the allowed Service Identifier values for each service selector are arranged between the telephone company and the user

10.3 Error procedures

If the information contained in the *Network specific facilities* information element is incorrectly coded, the network ignores the information element and attempts to route the call without it. There is no notification to the user that the NSF has been discarded.

Chapter 5-11:
Network message service

Network Message Service (NMS) allows a user to indicated to another user that there is a message waiting. The two users can be on different nodes, where the nodes are interconnected with PRI.

This section describes the ISDN PRI protocol impacts of NMS. Service-specific operational details of NMS (including both NMWI and NEMW) are not included.

11.1 Overview

The following types of Network Message Service are supported:

Network message waiting indicator (NMWI)

NMWI allows a Message Service on one node to activate or deactivate the message waiting indicator of a user located at a different node. When a user sees the message waiting indicator, he or she can access the Message Service to retrieve any messages. Typically, once all messages have been retrieved, the Message Service uses NMWI to deactivate the user’s message waiting indicator.

Network executive message waiting (NEMW)

NEMW allows the DMS-100 Centrex Executive Message Waiting (EMW) feature of a user to activate the message waiting indicator of a user located at a different node. With EMW, the calling party can indicate to the called party, when the called party is busy or unavailable, that he or she has called. The called party, on seeing the EMW indicator on the terminal, can retrieve the identity of all calling users who have used EMW or NEMW, or of Message Services which have messages waiting for them.

Figure 5-36
Message flow for Network Message Service - NMWI

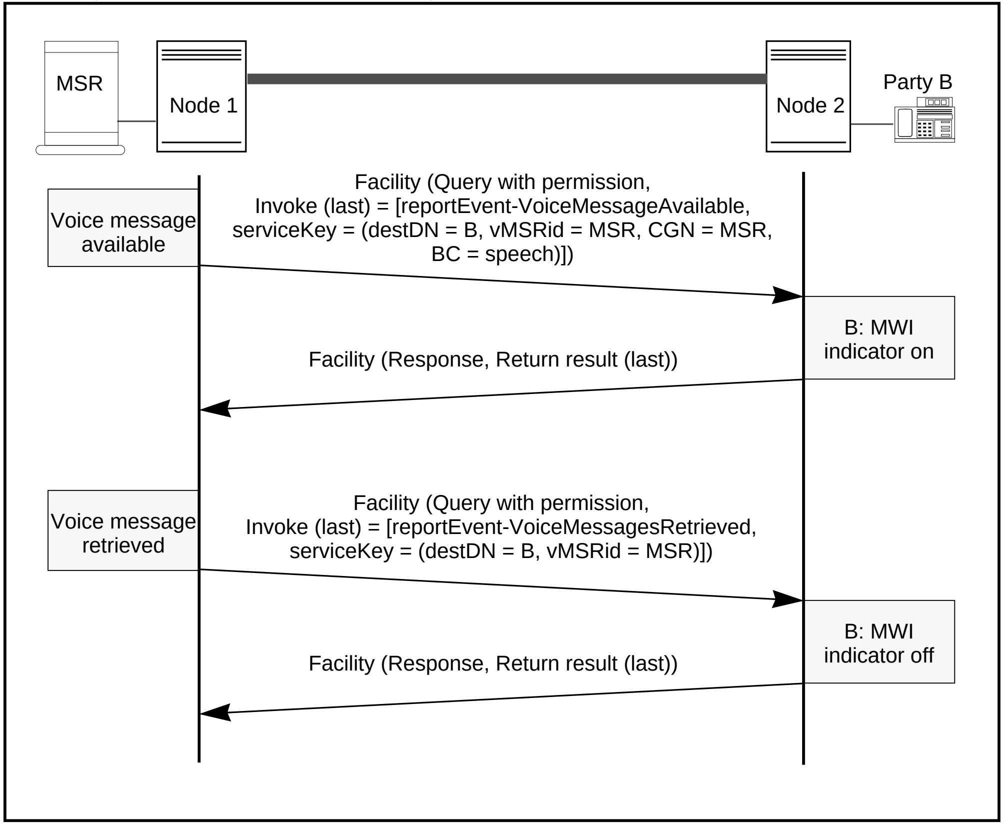
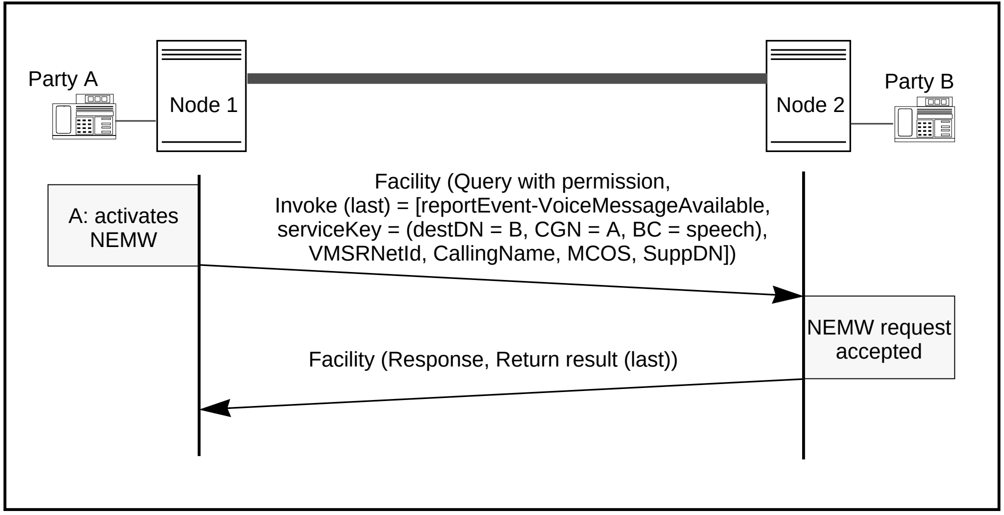


Figure 5-37
Message flow for Network Message Service - NEMW activation



11.2 Protocol

NMS protocol consists of the following elements, each of which is described in detail in the following sections

- *FACILITY* and *FACILITY REJECT* messages for connectionless signaling procedures
- the following information elements, all of which are in codeset 6
    - Facility
    - Origination
    - Destination
    - Options
    - Reason for return
- TCAP protocol
- timers

The detailed structure and coding of the *FACILITY* and *FACILITY REJECT* messages, the above list of information elements and TCAP protocol are described in Section 4 of this specification. Only their specific application to NMS is described in this section.

11.2.1 *FACILITY* and *FACILITY REJECT* messages

FACILITY and *FACILITY REJECT* are the only messages used to carry the NMS protocol. These messages are described in Section 4 of this specification.

11.2.2 Information elements

The *Facility* information element in the *FACILITY* and *FACILITY REJECT* messages is coded as follows

- Service discriminator is “TCAP”
- Service identifier is “Network Message Service (NMS)”
- User data contains a TCAP message pertaining to NMS

The *Origination* and *Destination* information elements are coded as required to identify the calling and called party’s nodes, respectively.

The *Options* information element may be included in the *FACILITY* message if the originating node wants to be notified if an error occurs in the routing of the *FACILITY* message. Otherwise, the originating node receives no notification if the *FACILITY* message is not routed successfully. The options value field is coded as “Return message on error”.

The *Reason for return* information element is included in a *FACILITY REJECT* message if a *FACILITY* message could not be successfully routed and the originator of the *FACILITY* message included an *Options* information element, as described above. The diagnostic field in the *Reason for return* information element indicates the problem encountered.

11.2.3 TCAP protocol

This section discusses the operations, error codes and parameters that NMS uses in TCAP messages between the originating and terminating nodes. The general TCAP message structure is described in Section Chapter 4-4: 4.5.15.2 on page 4-85.

11.2.3.1 Operations

The operations associated with NMS are described in this section. The operation codes for these operations are all defined in private TCAP, using the private TCAP operation code.

The detailed definition of the operations is described using macros. An operation macro consists of the following

- A parameter list to be included in the component, as indicated by the keyword PARAMETERSET followed by the parameter list. The list may be empty or contain default or optional parameters.
- The RESULT keyword indicates that a Return result component is sent in response to the operation when it is successfully invoked. The result may have parameters. Absence of RESULT indicates that a successful outcome is not reported.
- The ERRORS keyword indicates that a Return error component is sent in response to the operation if it is not successfully invoked. ERRORS is followed by a list of the possible error codes. Absence of ERRORS indicates that an unsuccessful outcome is not reported.
- The RESPONSEOPERATIONS keyword indicates other operations that are allowed in response to this operation. RESPONSEOPERATIONS is followed by the list of allowed operations. Absence of RESPONSEOPERATIONS indicates that no other operations are linked to this one.
- The numerical operation value is shown following the “::=” symbol.

reportEvent-VoiceMessageAvailable

The originating node uses this operation when a Message Service needs to inform a subscriber that there are messages waiting, or when a calling party has invoked NEMW for a busy or alerting called party. A Message Service may use this operation for an incoming message, even if the subscriber's message waiting indicator is already on, since additional calling party information can be provided to the subscriber.

```
reportEvent-VoiceMessageAvailable          OPERATION

PARAMETERSET      {   serviceKey [10] IMPLICIT SET {
                           destinationNumber Digits,
                           vMSRIdentifier    Digits   OPTIONAL,
                           callingNumber     Digits   OPTIONAL,
                           BCrequested                OPTIONAL },
                      VMSRNetworkId                   OPTIONAL,
                      CallingName                     OPTIONAL,
                      MessageClassOfService           OPTIONAL,
                      SuppressedDN                    OPTIONAL }

RESULT            { }

ERRORS            {   taskRefused,
                      notificationUnavailableToDestinationDN,
                      destinationDNunassigned,
                      vMSRIDdidNotMatchUserProfile }

:: =        8A01 -- (hex)
```

The value of the Invoke ID in the Invoke component is used to unambiguously identify the specific service associated with this operation. It is coded as follows:

- For NMWI the Invoke ID is set to 0.
- For NEMW the Invoke ID is set to 2.

reportEvent-VoiceMessagesRetrieved

The originating node uses this operation when a Message Service needs to inform a subscriber that there are no more messages waiting. This operation is not used for NEMW.

```
 reportEvent-VoiceMessagesRetrieved        OPERATION

PARAMETERSET       {   destinationNumber   Digits,
                       vMSRIdentifier   Digits        OPTIONAL }

RESULT             { }

ERRORS             { taskRefused,
                      notificationUnavailableToDestinationDN,
                      destinationDNunassigned,
                      vMSRIDdidNotMatchUserProfile }

:: =        8A02 -- (hex)
```

The value of the Invoke ID in the Invoke component is set to 1.

11.2.3.2 Errors

The errors associated with NMS operations are described in this section. The Return error component contains an error code to identify the reason for unsuccessful completion of an invoked operation. The error codes are defined in both national and private TCAP. National TCAP error codes are defined in ANSI T1.114. Private TCAP error codes are described in this section.

The detailed definitions of the errors are described using macros. An error macro consists of the following

- the PARAMETERSET keyword indicates whether there are any parameters associated with the error
- the numerical error value is shown following the “::=” symbol

notificationUnavailableToDestinationDN

This error code is used when the notification can not be provided to the destination for some short term reason. For example, the line is temporarily out of service.

```
notificationUnavailableToDestinationDN              ERROR

PARAMETERSET          { }

:: =        16
```

destinationDNunassigned

This error code is used when the destination number is not assigned to an active interface.

```
destinationDNunassigned                    ERROR

PARAMETERSET        { }

:: =       14
```

vMSRIDdidNotMatchUserProfile

This error code is used when the destination number is not a customer of the identified Message Service.

```
vMSRIDdidNotMatchUserProfile               ERROR

PARAMETERSET        { }

:: =       17
```

11.2.3.3 Parameters

This section describes all the parameters used by the operations defined for NMS. Private TCAP parameters are defined in this section. National TCAP parameters are defined in ANSI T1.114, but their usage for NMS is shown in this section.

Digits

The digits parameter is defined in National TCAP. It consists of the following fields:

- Type of digits - coded as follows for each indicated parameter
    - destinationNumber - “destination number”
    - vMSRIdentifier - “vMSRId” (coded as “0000 1100”)
    - callingNumber - “calling number”
- Nature of number - “National, no presentation restriction”
- Encoding scheme - “BCD”
- Numbering plan - “E.164”
- Number of digits present
- Digits

The destination number is used to identify the party at the terminating node whose message waiting indicator is to be affected. Typically, this number is the number dialed by the calling party.

The VMSR Identifier is used to identify the Message Service associated with NMWI.

The calling number contains the same information as the VMSR Identifier.

BCrequested

The BCrequested parameter indicates the bearer capability associated with a message. The parameter contains the contents of the *Bearer capability* information element as described in Section 4 of this specification.

The BCrequested parameter is defined in private TCAP.

```
BCrequested      :: =      [ PRIVATE 18 ] IMPLICIT OCTET STRING
```

CallingName

The CallingName parameter is used to indicate the name of the calling user who is invoking NEMW. It is not included for NMWI. Octets 1, which must be present, is coded “0000 0000”. The calling name characters are coded starting in octet 2, to a maximum length of 15 characters, with one IA5 character per octet.

The CallingName parameter is defined in private TCAP.

```
CallingName      :: =      [ PRIVATE 1 ] IMPLICIT OCTET STRING
```

MessageClassOfService

The MessageClassOfService parameter (MCOS) is associated with the party invoking NEMW. MCOS is not used for NMWI. Each user can have up to four MCOSs assigned to it, of class “A” through to class “P”.

The MessageClassOfService parameter is defined in private TCAP.

```
MessageClassOfService      :: =   [PRIVATE 10] OCTET STRING

--   MCOS “x”is assigned if the associated bit is set to “1”
--
--   Octet 1:  8 7 6 5   4 3 2 1     Octet 2:  8 7 6 5   4 3 2 1
--             H G F E   D C B A               P O N M   L K J I
```

VMSRNetworkId

The VMSRNetworkId parameter is used to provide the network identification associated with the party invoking NEMW. It is not used for NMWI. The terminating node uses this parameter to determine a dialable number which could be used to set up a call to the invoking party.

The VMSRNetworkId parameter is defined in private TCAP.

```
VMSRNetworkId        :: =     [ PRIVATE 11 ]
                               IMPLICIT OCTET STRING

--  The content of this parameter is a one octet long unsigned
--  integer which ranges in value from 0 to 255.
```

SuppressedDN

The SuppressedDN parameter is used to determine whether or not the calling number can be displayed by the terminating party.

The SuppressedDN parameter is defined in private TCAP.

```
SuppressedDN         :: =     [ PRIVATE 12 ] BOOLEAN
```

11.2.4 Timers

The following timer is defined for use with NMS:

T1 Length of time that the originating node waits after sending out a TCAP Query package before abandoning the request. T1 can range from 0 to 100 seconds, in steps of 1 second, and with a default value of 3 seconds.

11.3 Procedures

The protocol details for coding the TCAP messages mentioned in the following procedures are described in section 6.2 on page 5-62.

11.3.1 Actions at the originating node

When a Message Service needs to notify a served party of an incoming message, and the served used is located at a remote node which is connected with PRI, the originating node invokes NMWI by sending a TCAP Query with permission package to the terminating node with the following content

- a new Transaction ID
- Invoke (last) component with the following content
  - — operation reportEvent-VoiceMessageAvailable
  - — Invoke ID of 0
- destinationDN parameter with the 10-digit public number of the served party.
- vMSRIdentifier parameter with the 10-digit public number of the Message Service.
- callingNumber parameter coded identically to the vMSRIdentifier parameter

- BCrequested parameter coded as “speech”, as described in Chapter 4-4: 4.5.5.1 on page 4-52

The originating node starts timer T1. If timer T1 expires, the originating node releases the Transaction ID and may provide a failure indication to the Message Service.

When the originating node receives a TCAP Response package, for the above operation, with a Return result (last) component, the originating node

- releases the Transaction ID
- stops timer T1
- optionally, informs the Message Service

When a calling party invokes NEMW (the called party is either busy or is alerting as the result of a call attempt), the procedures at the originating node are the same as above for NMWI, with the following exceptions

- Invoke ID of 2
- destinationDN parameter with the 10-digit public number of the called party
- vMSRIdentifier parameter is not included
- callingNumber parameter with the 10-digit public number of the calling party
- VMSRNetworkId of the calling party
- CallingName parameter with the calling party’s name, if available, otherwise this parameter is filled with blank characters
- MessageClassOfService parameter with the MCOS associated with the calling party
- SuppressedDN parameter with the calling party’s number privacy indication

When a Message Service needs to notify a served party that there are no more messages waiting, and the served user is located at a remote node which is connected with PRI, the originating node sends a TCAP Query with permission package to the terminating node with the following content

- a new Transaction ID
- Invoke (last) component with the following content
    - — operation of reportEvent-VoiceMessagesRetrieved
- Invoke ID of 1

- destinationDN parameter with the 10-digit public number of the served party.
- vMSRIdentifier parameter with the 10-digit public number of the Message Service.

Other procedures are as above for the voice message activation operation.

Unlike for NMWI, the calling party who has previously invoked NEMW to a called party is not able to deactivate the called party's message waiting indicator.

11.3.2 Actions at the terminating node

When the terminating node receives a TCAP Query with permission package with an Invoke (last) component containing the operation "reportEvent-VoiceMessageAvailable" or "reportEvent-VoiceMessagesRetrieved", the terminating node

- validates the requested service operation and parameters
- performs the requested NMWI or NEMW service
- sends a TCAP Response package to the originating node with a Return result (last) component

Sending of the TCAP Response package as described above indicates that the requested NMWI or NEMW service was successfully performed.

11.3.3 Error procedures

Errors are reported with either a TCAP Response or a Unidirectional package. Since a message containing the TCAP Unidirectional package does not require a transaction ID, this package is used when

- a protocol error makes the Transaction ID impossible to determine
- the error occurred in a TCAP Response package; since this package ends the TCAP transaction, the other node has already released the Transaction ID

In all other cases, a TCAP Response package is used to report the error.

Two types of errors can occur during a TCAP transaction

- protocol errors
- application errors

11.3.3.1 Protocol errors

Protocol errors are caused by incorrectly coded TCAP packages. These include errors in the format of a component, invalid or duplicate component IDs or an invalid parameter format. Protocol errors are reported with a Reject component. The Reject component contains a problem code to describe the protocol error. Problem code definitions can be found in Section 4 of this specification.

11.3.3.2 Application errors

Application errors are those errors which are specific to NMS operations. Application errors are only detected if the TCAP package, and the included component, do not contain protocol errors. Application errors are reported in a TCAP package (as described above), containing a Return error component with one of the error codes described in section 6.2.3.2 on page 5-65. The Transaction ID, if allocated, is released.

Chapter 5-12:
Release Link Trunk (RLT)

This section describes the functionality and messaging protocols of the Release Link Trunk (RLT) Network Side for DMS-100 on NTNA PRI.

12.1 Introduction

RLT provides for the optimization of NTNA PRI Trunks. If a call between two parties subscribing to the same DMS-100 occurs as a result of a network redirection (for example, a call transfer invoked by a party subscribing to a PBX), RLT bridges the call across the switch. RLT thereby releases B channels which would otherwise be dedicated unnecessarily.

In all cases, RLT involves exactly two B channels which run between the network side (at the DMS-100) and the user side (at the PBX). These can be on the same PRI trunk group or on different PRI trunk groups. If the B channels are on different PRI trunk groups, they must connect to the same DMS-100 and PBX. One B channel carries a call that originates from the network side and terminates on the user side. This channel will be referred to as channel 1. The other B channel, which originates from the user side and terminates on the network side, will be referred to as channel 2. The calls which are carried over channel 1 and channel 2 will be referred to as call 1 and call 2 respectively. Also, for the purposes of the examples, Node1 and Node 2 always refer to the user side and network side respectively.

12.2 Functional Overview

There are several ways in which RLT can be invoked. Three typical usages are for Call Forwarding Universal/Busy (see Figure 5-38 on page 5-117), Call Forward No Reply (see Figure 5-39 on page 5-118), and Call Transfer (see Figure 5-40 on page 5-119). Described below are the requirements and messaging specific to RLT. Call forward universal/busy and call forward no reply are described in section 5.4.1 on page 5-41 and section 5.4.2 on page 5-47 respectively. Call transfer is described in section 5.4.4 on page 5-55.

Figures 5-38, 5-39 and 5-40 detail messaging sequences which describe ways in which RLT is typically used. In these diagrams, a dashed line indicates a message associated with call 1. A solid line indicates a message associated with call 2. The messages that are bold face have FACILITY Information Elements relating to RLT included in them. The function of these FACILITY Information Elements is described later in this chapter.

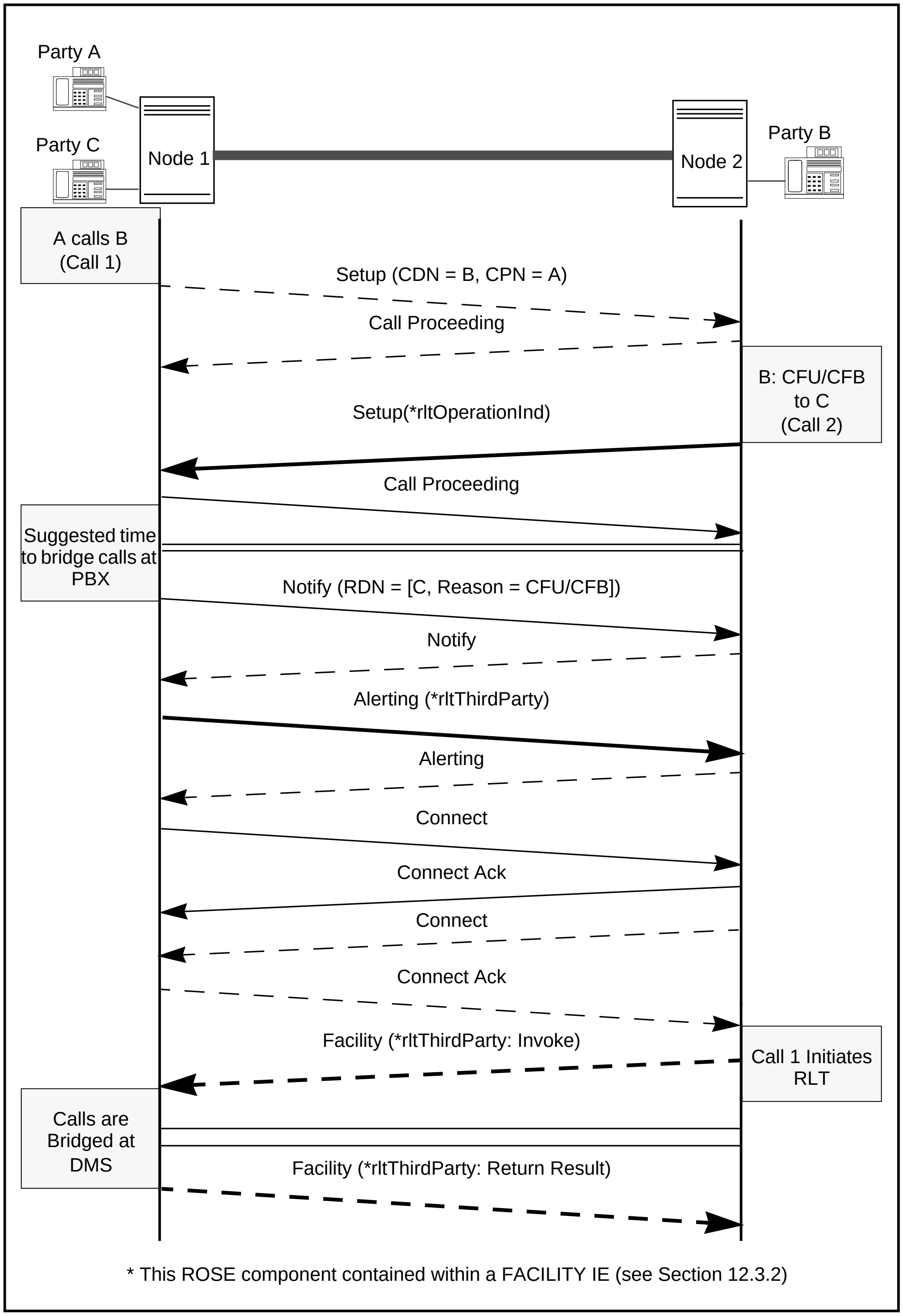
Note that there are many other ways in which RLT could be invoked. These three examples merely describe common ways that a PBX would use RLT. Apart from the RLT specific messaging, which is in bold face, the messaging sequence is the same as it would be if RLT were not invoked. Also, please note that these scenarios are dependant upon the PBX. These examples are given for illustration only.

Figure 5-38 shows the messaging sequence for RLT with Call Forward Universal/Busy. In this example, user A calls user B. This call is automatically forward to user C. The phone for user B never rings. Instead, the phone for user C rings, and the signalling for the call is propagated through the PBX to user A. When user C answers the phone, the PBX invokes RLT and the call is bridged at the DMS-100. The PRI lines to the PBX are taken down and user B is no longer involved with the call.

Figure 5-39 shows the messaging sequence for RLT with Call Forward, No Reply. When user A calls user B, the phone on user B rings. After a certain period of time (provided that user B does not answer the phone), the call is forwarded to user C. The PBX does not propagate the ALERTING message to user A, since it was already informed that the call was alerting. Apart from the above, there is no difference between this scenario and Call Forward.

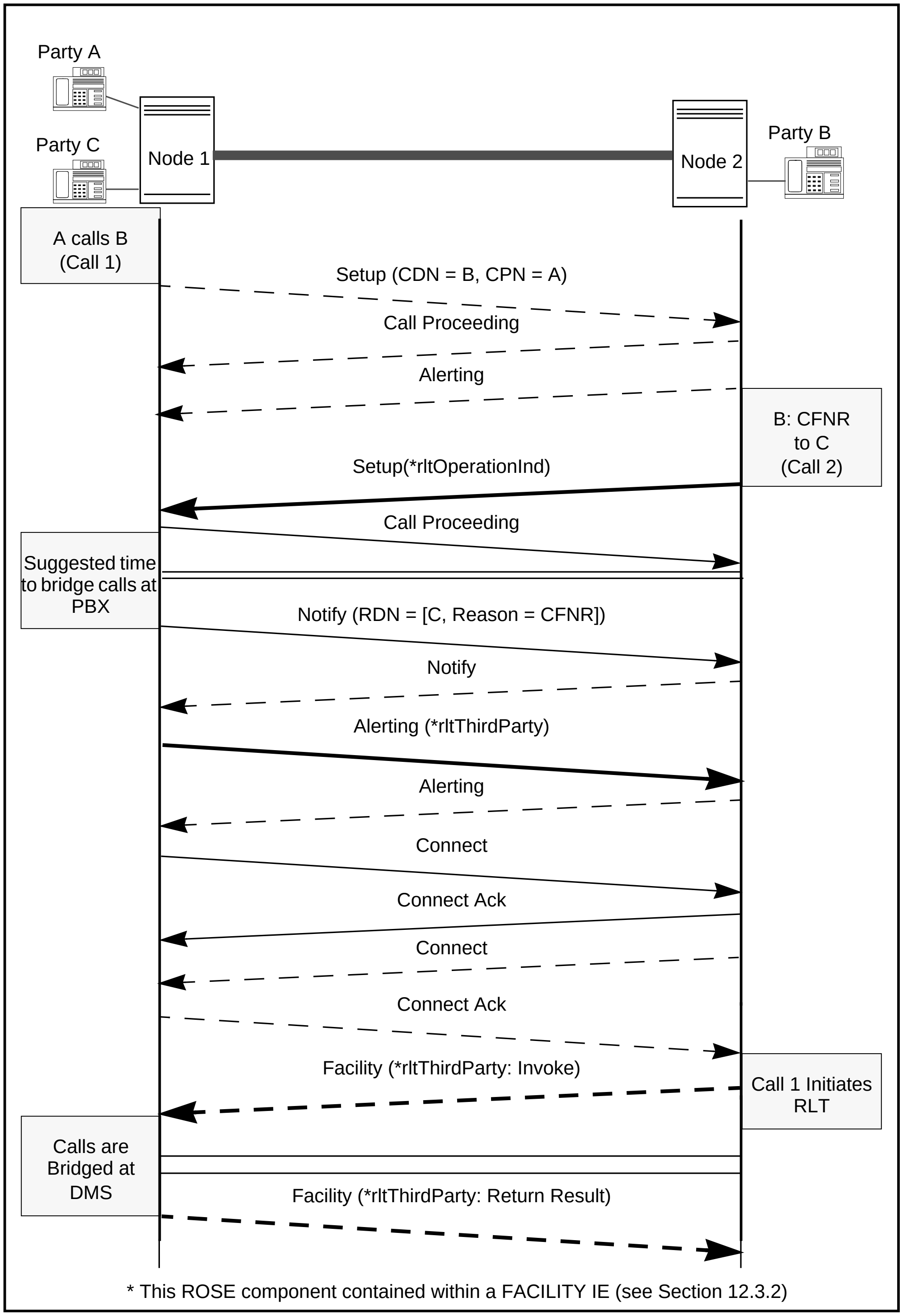
Figure 5-40 shows the messaging sequence for RLT with Call transfer. In this example user A calls user B. User B answers the phone and then transfers the call to user C. Because user A and user B are already connected, no messages are propagated from user B to user A. Sometime after user C answers the phone, user B drops out of the call and the PBX invokes RLT. The call is bridged at the DMS-100 and the PRI lines to the PBX are taken down. User B is no longer involved with the call.

Figure 5-38
RLT with CFU/CFB



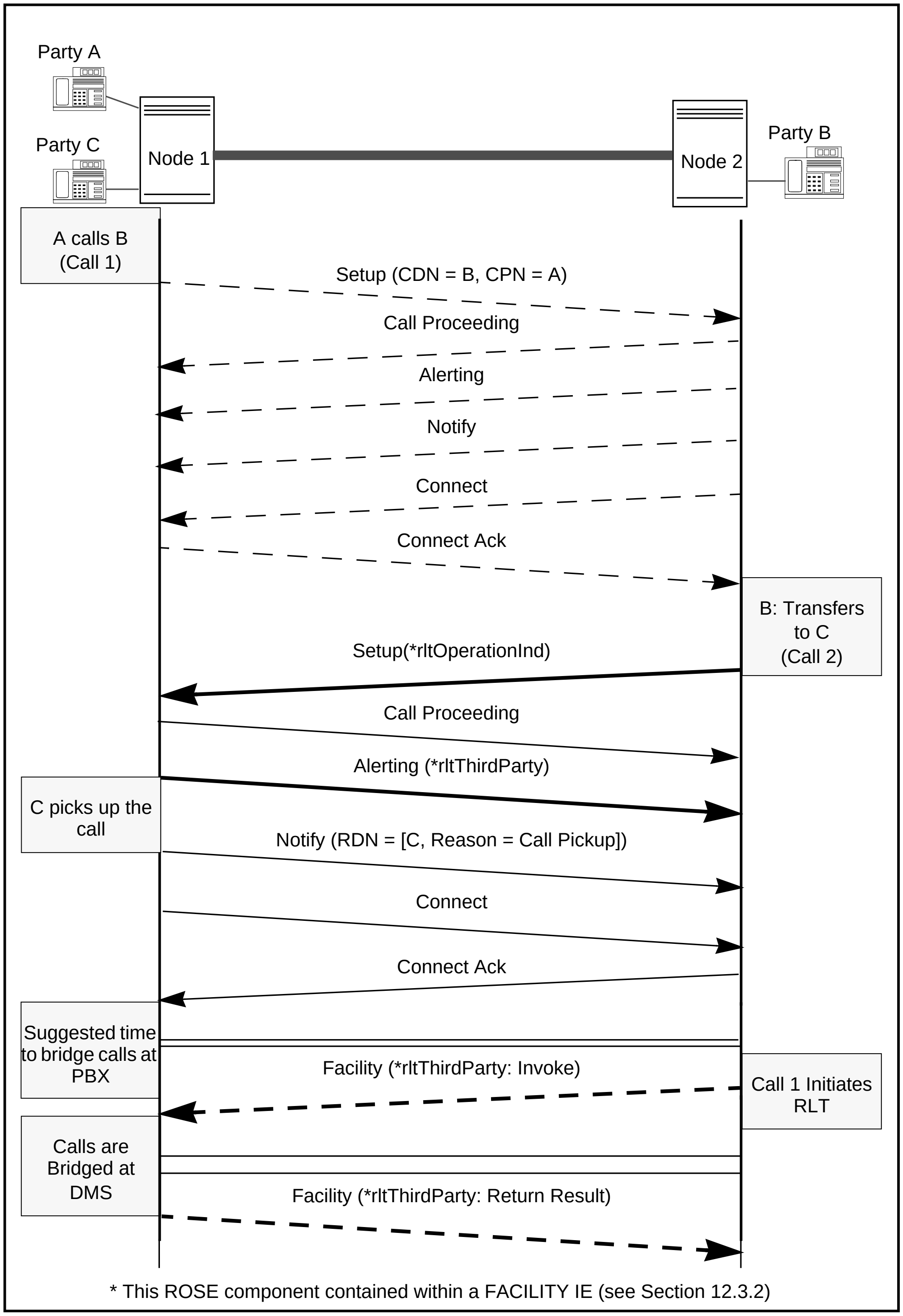
* This ROSE component contained within a FACILITY IE (see Section 12.3.2)

Figure 5-39
RLT with CFNR



* This ROSE component contained within a FACILITY IE (see Section 12.3.2)

Figure 5-40
RLT with Call Transfer



* This ROSE component contained within a FACILITY IE (see Section 12.3.2)

Despite the previous examples, it is important to note that it doesn't matter whether call 1 is originated before or after call 2. It is possible for call 2 to be set up for RLT before call 1 arrives, if the PBX predicts a need for a future transfer.

When RLT is invoked, calls 1 and 2 must both be connected. They must also be bridged at the PBX. This is to ensure that User A receives the appropriate tones and announcements from Call 2. Additionally, no user may be associated with the call at the PBX. Otherwise, they would be disconnected from the call when the two PRI trunks are taken down.

There are two separate phases of messaging required to invoke RLT. The first phase occurs when call 2 is originated. If the PBX wants to involve channel 2 in RLT, it must include a FACILITY IE (Information Element) in the SETUP message when originating call 2. The format of the FACILITY IE is described in section 12.3 on page 5-123.

When the network side receives a SETUP message with a FACILITY IE requesting RLT, it will respond by adding its own FACILITY IE to the ALERTING or PROGRESS message associated with call 2. This FACILITY IE will contain the call ID of call 2. Full details of the FACILITY IE contents are described in section 12.3 on page 5-123.

The user side must remember the call ID that was sent, as it will be used to invoke RLT later.

Any time after call 2 is originated and before RLT is invoked, the user side must bridge calls 1 and 2. It must also disconnect any of the users at the user side who are involved in either call.

When the above criteria have been met, and provided that call 2 is connected, the user side may invoke RLT. The user side may send a FACILITY message associated with call 1 to the network side. This FACILITY message must contain a FACILITY IE with the call ID that was sent back from the network side previously. The exact contents of the FACILITY message are described in section 3.3.1 on page 4-35 while the contents of the FACILITY IE are described in section 12.3 on page 5-123.
Upon receiving this FACILITY message, the network side will bridge the two calls. It will then send DISCONNECT messages, associated with each call, to the user side. The user and network sides will then proceed to release the two channels in the usual way.

The end result of this action is that the two calls are bridged at the network side. No B or D channels between the network side and the user side are involved in either call. The user side is not involved in either call at this point.

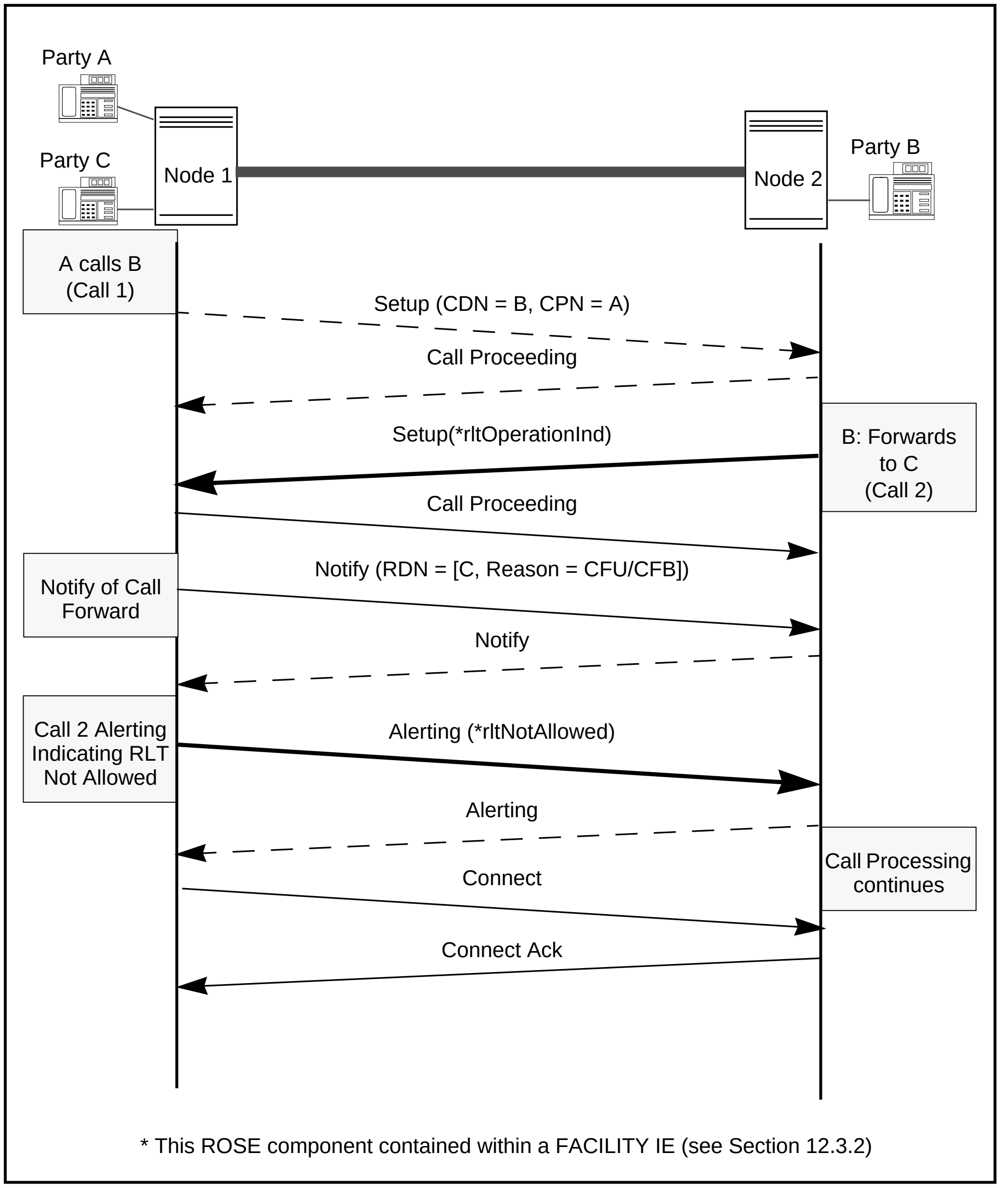
Billing of the calls will occur as if RLT had never been invoked.

Error conditions can occur and are described in section 12.3 on page 5-123. They will not, however, interfere with call processing. RLT will merely be disallowed. Since the calls are already bridged at the PBX, the call will stay up. In general, there are two places where an error condition can occur. The DMS can disallow RLT after receiving the SETUP message. Alternatively, the DMS can fail to bridge the call after receiving the FACILITY message.

Typical scenarios for error handling are shown in Figure 5-41 and Figure 5-42. For convenience, both of these scenarios are based on a Call Forward Universal/Busy scenario. Similar activity would occur for other scenarios. In Figure 5-41, the PBX requests that call 2 be involved in RLT. The DMS-100 determines that RLT is not allowed for the trunk group on which call 2 is situated. This could be because the trunk group was not datafilled for RLT, or because the feature is not enabled on the DMS-100. The PBX returns a FACILITY IE in the ALERTING message indicating that RLT is not allowed. The call continues as if RLT had never been invoked.

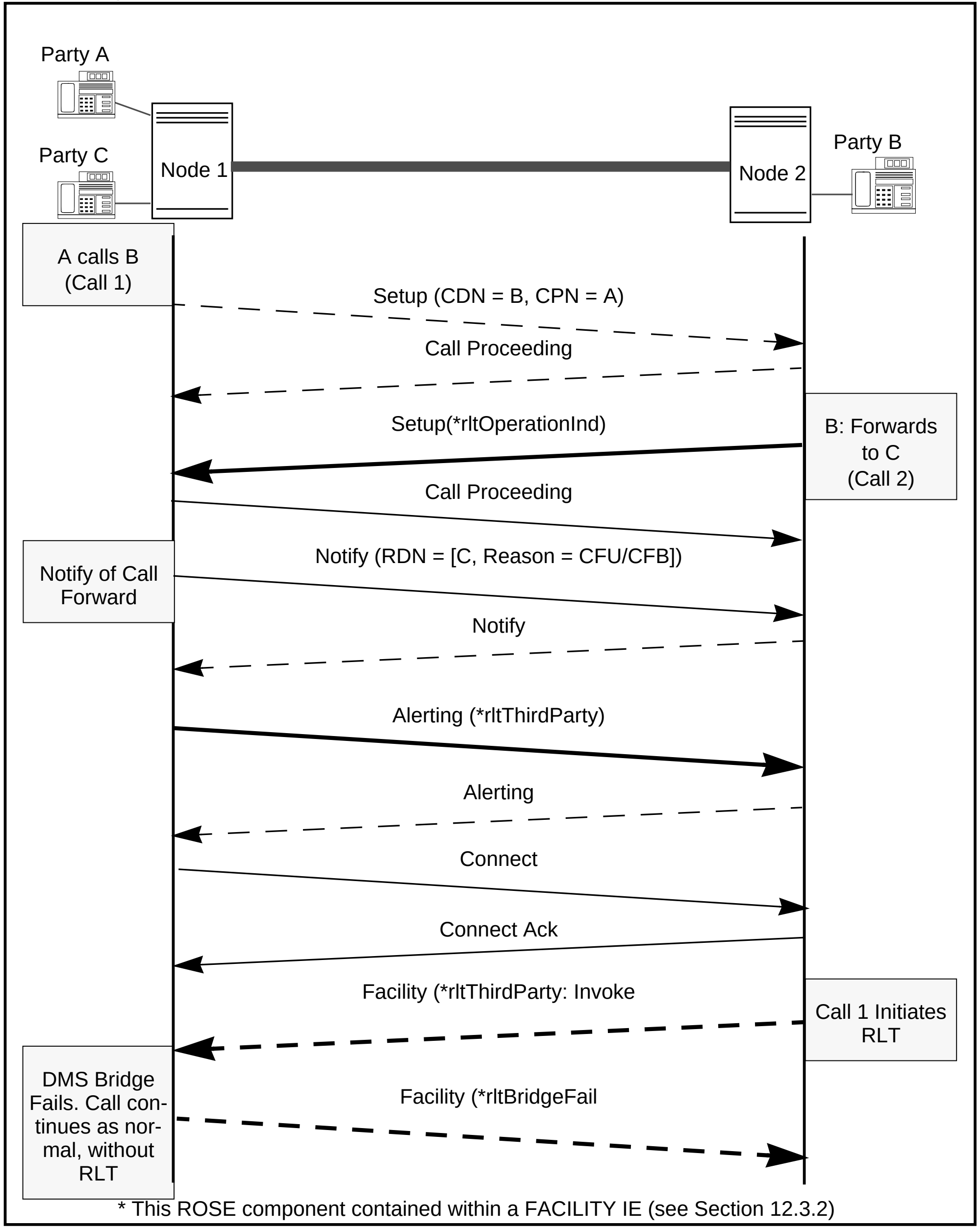
Figure 5-42 depicts a situation in which the call could not be bridged at the DMS-100. RLT is successfully set up for call 2, but when the PBX tries to invoke RLT, the call bridging fails. This can be due to many reasons. The trunk group for call 1 may not be datafilled for RLT. RLT may have been disabled on the DMS-100 between the time that call 2 was set up and the time that RLT was invoked. Whatever the reason, the DMS-100 returns a FACILITY IE in a FACILITY message indicating that bridging failed. The call continues as if RLT was never invoked.

Figure 5-41
RLT Not Allowed Scenario



* This ROSE component contained within a FACILITY IE (see Section 12.3.2)

Figure 5-42
RLT Bridge Failure Scenario



* This ROSE component contained within a FACILITY IE (see Section 12.3.2)

12.3 RLT and PRI Layer 3 Messages

The purpose of this section is to outline the PRI layer 3 messaging which will occur when RLT functionality is introduced by this feature. This section describes the actual messages that will be sent..

12.3.1 FACILITY Messages and FACILITY Information Elements

This feature uses the FACILITY message and FACILITY Information Element (IE) to provide RLT capability. For the purposes of this feature, the FACILITY IE will also be used as part of the ALERTING, PROGRESS and SETUP messages.

For the standard format of the Facility IE please refer to section 4.5.15 on page 4-76 . The Service Identifier specifies to which service this IE will relate. For this feature, it will contain the identifier for RLT. A FACILITY IE which contains this service identifier will contain information pertinent to an RLT service.

FACILITY IEs which contain RLT information must be encoded using a subset of the ROSE protocol. Please see section 4.5.15 on page 4-76 for more information on the Service Discriminator, which is used to specify the ROSE protocol.

12.3.2 ROSE Components

The User Data in octets 4 and beyond of the FACILITY IE are contained in a ROSE component. Please refer to section 4.5.15 on page 4-76 for the format of ROSE components.

There are four different ROSE components used by this feature. These are Invoke, Return Result, Return Error and Reject. Each RLT related FACILITY IE will have a single ROSE component in its User Data octets.

Octet 4 (the first of the User Data octets) contains the Componentt Tag. This tag identifies the kind of component in the FACILITY IE. Please refer to section 4.5.15 on page 4-76 for more information on the format of the Component Tag.

Following the Component Tag is the Component Length. This octet (octet 5) contains the length of the IE past octet five. In other words, it contains the number of octets in the component (not counting octets 4 and 5).

The next three octets (octets 6-8) contain the Invoke Identifier. Octet 6 contains 2_{10} which indicates that this is an Invoke Identifier. Octet 7 contains the length of the Invoke Identifier. In all cases this will be 1_{10}. The last mandatory octet (octet 8) contains the Invoke Identifier. This contains the Operation Value of the RLT Invoke component that caused this IE to be generated. Please refer to “12.3.3 Invoke Component” on page 125 for more information on the Operation Value. In the case where the IE is not sent in response to anything, the Invoke ID will be set to the Operation Value. The description of each component, given below, will indicate the value to which the Invoke Identifier will be set.

12.3.3 Invoke Component

The invoke component is used to indicate that an RLT action is desired. The user side will send a FACILITY IE containing an invoke component in order to setup and invoke RLT. There are two kinds of invoke components. These are the RLT Operation Indication and the RLT Third Party invoke components. The first is used in a SETUP message to indicate that the call will eventually be involved in RLT. The second is used in a FACILITY message to actually invoke RLT.

Mandatory Information for Invoke Component

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
Operation Value Tag								9
Operation Value Length								10
Operation Value								11

Both types of invoke components have an Operation Value. Octet 9 contains the Operation Value Tag, 2_{10},Which indicates that the following octets contain an Operation Value. Octet 10 contains the length of the Operation Value. In all cases this will be 1_{10}. Octet 11 contains the Operation value.

Operation Values (octet 11)

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	1	RLT Operation Indication
0	0	0	0	0	0	1	0	RLT Third Party

Octet 11 is the last octet in an RLT Operation Indication invoke component.

The RLT Third Party invoke component must contain the Call ID. This takes the form of a parameter. In this case, the Call ID parameter is part of a sequence of parameters.

Additional RLT Third Party Invoke Information

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
Sequence Tag								12
Sequence Length								13
Call ID Tag								14
Call ID Length								15
Call ID								16
								17
								18
Reason For Redirect Tag								19
Reason For Redirect Length								20
Reason For Redirect								21

Octet 12 contains the Sequence Tag of 48_{10}. This indicates that there is a parameter to follow. The next octet is the Sequence Length. This holds the length of the parameter. In the case of an RLT Third Party Invoke Component, this will always be 8_{10} (octets 14-21 are part of the parameter).

Octets 14-18 contain the information for the Call ID. Octet 14 contains 128_{10}, the Call ID Tag. This indicates that this parameter holds a call ID. The next octet (octet 15) holds the length of the Call ID. This can be 3_{10} or 4_{10}, indicating that the Call ID is 3 or 4 bytes long. Finally octets 16-18 hold the call ID.

Octets 19-21 hold the Reason for Redirect. This information is not used in this feature, but must be present in the IE. Octet 19 contains 129_{10},The Reason for Redirect Tag. The next octet (octet 20) holds the length of the Reason for

Redirect. In all cases this will be 1_{10}. The final octet (octet 21) contains the Reason for Redirect. As this value is not used, it can be set to anything.

Octet 21 is the last octet in an RLT Third Party invoke component.

12.3.4 Return Result Component

A return result component is returned upon the successful completion of the requested operation. It will be sent by the network side after it has completed the operation requested by a preceding FACILITY IE with an invoke component.

There are two types of return result component created by this feature. The simplest is sent upon successful completion of processing an RLT Third Party invoke component (that is, after the network side has successfully bridged the two calls). In this case there is no additional information added to the IE. The Invoke ID is set to 2_{10} (RLT Third Party) to indicate that this is a response to an RLT Third Party invoke component.

The other type of return result component created by this feature is sent upon successful completion of processing an RLT Operation Indication invoke component (The invoke component is sent in the SETUP message indicating that RLT is desired. The return result is sent back in the PROGRESS or ALERTING message and contains the Call ID of that call). The Invoke ID is set to 1_{10} (RLT Operation Indication) to indicate that this is a response to an RLT Operation Indication invoke component. This component also contains some additional information.

Additional Return Result Component(rltOperationInd) Information

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
Sequence Tag								9
Sequence Length								10
Operation Value Tag								11
Operation Value Length								12
Operation Value								13
Call ID Tag								14
Call ID Length								15
Call ID								16
								17
								18

Octet 9 contains the Sequence Tag of 48. This tag indicates that there is more information to follow. The next octet (octet 10) contains the sequence length. This holds the length of the rest of the component (octets 11-18). The value will always be 8_{10}.

The Operation Value Tag in octet 11 will be set to 2_{10}, to indicate that the next octets are part of an Operation Value. The Operation Value Length is next (octet 12) and will always have a value of 1_{10}. Octet 13 holds the Operation Value. The Operation Value for this component is 1_{10} (RLT Operation Indication).

Finally, Octets 14-18 hold the Call ID information. The Call ID Tag in octet 14 is set to 128_{10}, to indicate that the following octets hold a Call ID. Octet 15 holds the Call ID Length. This will be 3_{10}. Octets 16 through 18 hold the actual

Call ID. This value must be saved by the PBX so that it may be sent the RLT Third Party Component, when invoking RLT.

12.3.5 Return Error Component

A return error component is generated when the network side is unable to complete the request of the previous invoke component. This component is only used in response to a properly formatted request. Please refer to “12.3.6 Reject Component” on page 130 for information on handling badly formed requests.

The Invoke ID of this component is set to the value of the Operation Value in the invoke component that initiated this message. This indicates which operation could not be completed. All return error components in this feature have the same additional information. Please refer to section 4.5.15 on page 4-76 for the format of the Return Error Component.

Octet 9 contains 2_{10}, the Error Value Tag. This indicates that the following two octets are part of the Error Value. The next octet (octet 10) contains the Error Value Length. This will always be 1_{10} for this feature. The final octet (octet 11) is the Error Value. This value depends on the actual error encountered.

Error Values (octet 11)

8	7	6	5	4	3	2	1	
0	0	0	1	0	0	0	0	RLT Bridge Fail
0	0	0	1	0	0	0	1	RLT Call ID Not Found
0	0	0	1	0	0	1	0	RLT Not Allowed
0	0	0	1	0	0	1	1	RLT Switch Equip Congs (not used)

The only value that will be returned after an RLT Operation Indication invoke component is 18_{10}(RLT Not Allowed). This means that RLT was not datafilled on the particular trunkgroup, or that the feature has not been activated on the switch.

After an RLT Third Party invoke component, value 16_{10} (RLT Bridge Fail) will be returned if the switch was unable to bridge the two calls. RLT Call ID Not Found (value 17_{10}) will be returned after an RLT Third Party invoke component if the switch was unable to identify the Call ID sent in the invoke component. Finally, RLT Not Allowed (value 18_{10}) may also be returned after an RLT Third Party invoke component if RLT was not datafilled on the particular trunkgroup or if RLT was not activated on the switch. RLT Switch Equip Congs (value 19_{10}) is not used by this feature.

12.3.6 Reject Component

The Reject component will be sent when a protocol error occurs. For the purposes of this feature, this will be returned if the DMS-100 is unable to parse the data in an RLT FACILITY IE. Because it may not be possible to determine the Operation Value of the invoke component that initiated this response, the Invoke ID will be set to 0_{10}. Please refer to section 4.5.15 on page 4-76 for the format of the Reject Component.

The Problem Tag in octet 9 contains 130_{10}, to indicate that the following octets are part of the Problem Value. The next octet (octet 10) contains the Problem Length. This will always be 1_{10}. The final octet (octet 11) contains the Problem Value. The only value used by this feature is 2_{10} (Mistyped Result).

12.4 Message Protocols

This section discusses the actual messaging protocol for RLT in detail. Please refer to “12.2 Functional Overview” on page 115 for a high level overview of this information.

There are two phases of messaging. The first phase, RLT setup, occurs when the user side is attempting to originate call 2. The second phase of messaging occurs when the user side actually invokes RLT. This phase will be called RLT invocation.

12.4.1 RLT Setup

When the user side attempts to originate call 2, it must announce its intention to involve this B channel in RLT. It does this by adding a FACILITY IE with an RLT Operation Indication invoke component to the outgoing SETUP message.

Upon receipt of this SETUP message, the network side will try to originate the call. If it is unsuccessful, the network side will take down the call as usual and no further RLT specific messaging will be associated with this call.

If, however, the network side is successful in originating the call, it will send the appropriate messages, as usual. Eventually, the network side will indicate to the user side that the call is alerting. It does this by sending either an ALERTING message or, in the case of a call which is not end to end ISDN, a PROGRESS message (which contains a FACILITY IE if RLT is invoked).

Before sending the ALERTING or PROGRESS message, the network side will check to make sure that the trunk to which B channel 2 belongs is subscribed to RLT. It does this by checking the datafill in table TRKGRP. If that trunk belongs to a subscribed trunk group, the network side will check to make sure that the RLT feature is activated. If RLT is activated, the network side will add a FACILITY IE with a return result component. This component will contain the CALL ID of call 2.

If the trunk group in question is not datafilled for RLT, or the RLT feature has not been activated, the ALERTING or PROGRESS message will contain a FACILITY IE with a return error component. This error will indicate that RLT is not available. No further RLT messaging will be done involving this call.

Note that it is possible for a PROGRESS message to be sent by the DMS-100 before the CALL PROCEEDING message. This message will not be related to RLT and will not contain an RLT FACILITY IE.

12.4.2 RLT Invocation

In order to invoke RLT, the following criteria must have been reached:

- Call 1 must have been originated and connected.
- Call 2 must have been originated, sending an RLT FACILITY IE in the SETUP message.
- The user side must have received and recorded the Call ID of call 2 from the return result component in the RLT FACILITY IE of the ALERTING or PROGRESS message of call2.
- Call 2 must be connected.
- Calls 1 and 2 must be bridged at the user side.
- There must be no users connected to either call 1 or call 2 at the user side.

The conditions that calls 1 and 2 must be connected and bridged at the user side before invoking RLT insures that announcements and tones are properly sent to the initiator of call 1.

When these criteria are true, the user side may send a FACILITY message, containing a FACILITY IE with an RLT Third Party invoke component, to the network side. This message associates call 1 (call reference IE) and call 2 (call ID in the invoke component of FACILITY IE).

When the network side receives a FACILITY IE with an RLT Third Party invoke component, it will check the trunk group of the B channel on which it has received the message (B channel 1). It does this by ensuring that the trunk group is datafilled for RLT in table TRKGRP. It then makes sure that the RLT feature is activated on the switch. If these conditions are satisfied, it will attempt to bridge the call. Please refer to “12.4.4 Call Bridging” on page 132 for more information on the conditions necessary to bridge the call.

12.4.3 RLT FACILITY IE Parsing Failure

If, at any time, the network side receives a FACILITY IE with a ROSE component which it can not decipher, it will return a FACILITY message containing a FACILITY IE with a reject component.

12.4.4 Call Bridging

In this stage, the DMS-100 will attempt to bridge the calls. If the call is bridged successfully, the network side will send a FACILITY message containing a FACILITY IE with a return result component.

If the call is not bridged successfully, or if RLT is not allowed, the DMS-100 will return a FACILITY message containing a FACILITY IE with a return error component. The error component will have an error value of 1 (RLT Call ID Not Found) if the bridging failed due to the fact the network side did not recognize the call ID in the invoke component. The error value will be 2 (RLT Not Allowed) if the trunk group was not datafilled for RLT, or the RLT feature was not activated. Finally, the error value will be 0 (RLT Bridge Fail), if the bridging failed for any other reason. Error value 3 (RLT Switch Equip Cong) is not used by this feature.

12.4.5 B Channel Release

After the call is bridged at the network side and the FACILITY message containing the FACILITY IE with the return result component has been sent to user side, the network side will take down both calls 1 and 2. It will do this by sending DISCONNECT messages to the user side. The calls will then be taken down in the normal fashion.

12.5 Interactions

There are no feature interactions which will cause bridging to fail.

If the PBX sends NOTIFY messages after it has invoked RLT, these may not be propagated to their intended recipients. The PBX must send all notify messages before invoking RLT.

RLT feature interactions with both AIN 0.1 and AIN 0.2 are not supported. However, RLT feature interactions with Local Number Portability (LNP) are supported.

Appendix A: List of terms

ACD

Automatic Call Distribution

Alarm indication signal (AIS)

A signal transmitted in lieu of the normal signal to maintain transmission continuity, and to indicate to the receiving terminal that there is a transmission fault which is located either at the transmitting terminal or upstream of the transmitting terminal. AIS is commonly called the Blue Alarm signal.

ANSI

American National Standards Institute

B-channel

A 64 kbit/s channel that carries customer information such as voice calls, circuit switched data, or packet switched data. A distinguishing characteristic is that a B-channel does not carry signaling information for control of circuit switching by the ISDN.

BC

Bearer capability

BCD

Binary coded decimal

BCS

Batch Change Supplement

BFCV

Binary Facility Coding Value

Bipolar (alternate mark inversion) signal

A pseudo-ternary signal, conveying binary digits, in which successive “ones” (marks, pulses) are of alternating positive (+) and negative (-) polarity, equal in amplitude, and in which a “zero” (space, no pulse) is of zero amplitude.

Bipolar violation

In a bipolar signal, a one (mark, pulse) which has the same polarity as its predecessor.

bit/s

bits per second

BRI

ISDN Basic Rate Interface

B8ZS (bipolar with 8-zero substitution)

A code where eight consecutive “zeros” are replaced with the sequence if the preceding pulse was +1, and with the sequence if the preceding pulse was -1, where +1 represents a positive pulse, -1 represents a negative pulse and 0 represents no pulse.

C/R

Command/Response field bit (Layer 2)

Carrier

An organization that provides telecommunications services to the public.

CCITT

International Telephone and Telegraph Consultative Committee

CCS7

Common channel signaling system no. 7

CDN

Called party number

CEI

Connection endpoint identifier

CES

Connection endpoint suffix

CFB

Call Forward - Busy

CFNR

Call Forward - No Reply

CFU

Call Forward - Universal

CGN

Calling party number

CLASS

Custom Local Area Signaling Services

Clear channel capability

A characteristic of a transmission path in which the bit positions allocated for customer data may represent any combination of zeros and ones. For the DS-1 rate, the bits allocated for customer data are the last 192 bits of each frame.

CN

Connected number

CND

Calling Number Delivery

CO

Central office

CPN

Calling party number information element

CTX

Centrex

Customer installation (CI)

Equipment and facilities at the customer’s location on the customer side of the network interface.

Cyclical redundancy check (CRC)

A method of checking the integrity of received data, where the check uses a polynomial algorithm based on the content of the data.

D-channel

A channel that is primarily intended to carry signaling information for ISDN switching. For the primary rate interface, the D-channel transmission rate is 64 kbit/s.

DID	Direct inward dialing
DISC	Disconnect frame (Layer 2)
DL	Prefix for communication primitives between Layer 3 and Layer 2.
DLCI	Data link connection identifier
DM	Disconnect mode frame (Layer 2)
DN	Directory number
DOD	Direct outward dialing
DS-1 ()	Digital signal level 1 - digital signal transmitted at the nominal transmission rate of 1.544 Mbit/s.
E.164	CCITT Recommendation for the ISDN/telephony numbering plan.
EA	Extended address field bit (Layer 2)
ECSA	Exchange Carriers Standards Association
Embedded operation channel (EOC)	An embedded operation channel (EOC) is provided on telecommunications facilities to support administration and maintenance. For the primary rate interface, the EOC is the extended superframe data link at Layer 1.
EMW	Executive Message Waiting
ET	Exchange termination

Extended superframe (ESF) terminal

The extended superframe (ESF) terminal is the source and sink of ESF framing, cyclical redundancy check (CRC 6) bits, and performance report messages (PRMs). The extended superframe terminal may be in a network terminal 2 (NT2) or terminal equipment (TE) functional group, or in equipment located within the network.

FCS

Frame check sequence

FRMR

Frame reject frame (Layer 2)

FX

Foreign Exchange line

I

Information frame (Layer 2)

Ia

Ia is the 4 wire (2 pair) bi-directional primary rate interface point on the network side of the termination equipment (that is, NT1, NT2, TA, and TE) including the equipment connecting cord or equivalent on the user side of the interface cable.

IA5

International alphabet No. 5

Ib

Ib is the 4 wire (2 pair) bi-directional primary rate interface point on the user side of the termination equipment (that is, NT and NT2) including the equipment connecting cord or equivalent on the network side of the interface cable.

ID

Identification or identifier

IE

Information element

IEC

Inter-exchange carrier

ISA

Integrated Services Access

INWATS

Inward Wide Area Telephone Service (800 service)

IRQ

Information request information element

ISA

Integrated Services Access

ISDN

Integrated services digital network

ISO

International organization for standardization

Isolated pulse

An isolated pulse is a pulse that is free from the effects of the other pulses in the same signal. A suitable testing signal is a repetitive pattern of a single "one" pulse followed by seven "zero" pulses {10000000100000010000000...}.

ISUP

CCS7 ISDN user part

ITA

Integrated Trunk Access

Jitter

Jitter is a measurement of the short term variation of the significant instants of a digital signal from their ideal positions with respect to time. Short term implies that these variations are high frequency (greater than 10 Hz).

Keep alive signal

A keep-alive signal is a signal that is transmitted instead of the normal signal to maintain transmission continuity on a particular channel.

L1

Layer 1

L2

Layer 2

L3	Layer 3
LATA	Local Access and Transport Area
LAPB	Link access procedure - balanced
LAPD	Link access procedure on the D-channel
LDN	Listed directory number
Loopback	A loopback is a state of the transmission facility in which the received signal is returned towards the sender.
LSI	Load status information (NACD)
M	Modifier function bit (Layer 2)
MCOS	Message class of service
MDL	Prefix for communication primitives between the management entity and Layer 2.
MF	Multiple frequency (analog) signaling
MSN	Meridian Switched Network (formerly ESN)
MSR	Message storage and retrieval system
Multiplexer	A multiplexer is a piece of equipment that is used for combining (multiplexing) two or more tributary signals into a single composite signal. In

general, the multiplexer is also used to de-multiplex the composite signal. That is, to separate the composite signal into its component tributary signals.

MWI

Message Waiting Indicator

N(R)

Receive sequence number (Layer 2)

N(S)

Send sequence number (Layer 2)

NACD

Network Automatic Call Distribution

NEMW

Network Executive Message Waiting

Network channel terminating equipment (NCTE)

Network channel terminating equipment (NCTE) is a device that connects to the network on one interface and to terminal equipment on another interface.

NI

The network interface (NI) is the point of demarcation between the network and the customer interface (CI).

NMWI

Network Message Waiting Indicator

NMS

Network Message Service

NPI

Numbering plan identification

NRAG

Network Ring Again

NSF

Network specific facilities information element

NT1

A functional group that provides the physical layer functions for access line termination.

NT2

A functional group that provides protocols above layer 1 for DS-1 path termination. For example, a private branch exchange (PBX) has an NT2.

OCN

Original called number information element

OUTWATS

Outward Wide Area Telephone Service

P/F

Poll/Final bit (Layer 2)

Payload

Payload is a term that is used to indicate the information data in a frame. For instance, the payload of a DS-1 frame consists of the 192 information data bits.

PBX

Private branch exchange

Performance report messages (PRM)

An autonomous report initiated by an ISDN primary rate interface terminal (ET or NT/TE) that provides an objective measurement of the quality of transmission incoming to the terminal.

Phase transient

An event which causes movement of the phase of the signal with respect to absolute time (for example, clock rearrangement).

Physical interface

An interface at the Layer 1 level of the open system interface (OSI) reference model.

PI

Presentation indicator

Primary rate interface (PRI)

A term used to describe a DS-1 rate access to an ISDN network that supports standard combinations of channels with a 1536 kbit/s payload.

PTS

Per trunk signaling

Pulse density

A measure of the number of “ones” (marks, pulses) as a percentage of the total number of digital time slots transmitted.

RDN

Redirection number information element

Receive signal

The signal received across an interface Ia or Ib by the associated equipment.

Receiver

The sink or terminator of any signal in a transmission medium.

Reference point

A conceptual point at the conjunction of two non-overlapping functional groups. In a specific access arrangement, a reference point may correspond to a physical interface between pieces of equipment, although this is not always necessary. In some arrangements, there may be more than one physical interface associated with a reference point.

Regenerator

Equipment that reconstructs and retransmits a received pulse train.

REJ

REJect

Remote alarm indication (RAI)

A remote alarm indication (RAI) signal is transmitted in the outgoing direction when a terminal determines that it has lost the incoming signal. The RAI is commonly called the Yellow Alarm signal.

Ri

Reference number

RLT

Release Link Trunk

RNR

Receive not ready frame (Layer 2)

RR

Receive ready frame (Layer 2)

S	Supervisory (Layer 2)
S1	Supervisory function bit (Layer 2)
SABME	Set asynchronous balanced mode extended frame (Layer 2)
SAP	Service access point (Layer 2)
SAPI	Service access point identifier (Layer 2)
SI	Screening indicator
T1 line	A full duplex digital transmission facility that is composed of two twisted metallic pairs and regenerators that carry one DS-1 signal.
TCAP	CCS7 Transaction Capabilities Application Part
TE	Terminal equipment
TEI	Terminal endpoint identifier
TIE	Tie trunk
TNS	Transit network selection information element
TON	Type of number
Transmit signal	The signal sent across an interface Ia or Ib from the associated equipment.

Transmitter

The source or generator of any signal in a transmission medium.

U

Unnumbered frame (Layer 2)

UA

Unnumbered acknowledgment frame (Layer 2)

UI

Unnumbered information (Layer 2)

Unit interval (UI)

The nominal difference in time between consecutive significant instants of an isochronous signal. In wave theory, this is referred to as the period of a wave.

V(A)

Acknowledged state variable (Layer 2)

V(M)

Recovery state variable (Layer 2)

V(R)

Receive state variable (Layer 2)

V(S)

Send state variable (Layer 2)

VMSR

Voice Message Storage and Retrieval service

Wander

Wander is a measurement of the long term variations of the significant instants of a digital signal from their ideal positions with respect to time. Long term implies that these variations are low frequency (less than 10 Hz).

Appendix B: Index

Digital Switching System

ISDN Primary Rate User-Network Interface Specification

The information disclosed herein is proprietary to Northern Telecom or others and is not to be used by or disclosed to unauthorized persons without the written consent of Northern Telecom. The recipient of this document shall respect the security status of the information.

Document number: NIS-A211-1
Product Release: NA011
Document Release: 08.01
Date: August 1998

Printed in the United States and Canada

NORTEL
NORTHERN TELECOM