INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.965

(03/2001)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Digital sections and digital line system – Digital section and digital transmission systems for customer access to ISDN

V-interfaces at the digital local exchange (LE) – V5.2 interface (based on 2048 kbit/s) for the support of access network (AN)

ITU-T Recommendation G.965

(Formerly CCITT Recommendation)

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TESTING EQUIPMENTS	G.500–G.599
TRANSMISSION MEDIA CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
General	G.900–G.909
Parameters for optical fibre cable systems	G.910–G.919
Digital sections at hierarchical bit rates based on a bit rate of 2048 kbit/s	G.920–G.929
Digital line transmission systems on cable at non-hierarchical bit rates	G.930–G.939
Digital line systems provided by FDM transmission bearers	G.940–G.949
Digital line systems	G.950–G.959
Digital section and digital transmission systems for customer access to ISDN	**G.960–G.969**
Optical fibre submarine cable systems	G.970–G.979
Optical line systems for local and access networks	G.980–G.989
Access networks	G.990–G.999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation G.965

V-interfaces at the digital local exchange (LE) – V5.2 interface (based on 2048 kbit/s) for the support of access network (AN)

Summary

This Recommendation defines a V-interface (V5.2) for the connection of an Access Network (AN) and the Local Exchange (LE) for the support of the following access types

– analogue telephone access;

– ISDN basic access with an NT1 separate from the AN, or integrated in the AN, based on ITU-T G.960 and I.430;

– ISDN primary rate access with an NT1 separate from the AN, or integrated in the AN, based on ITU-T G.962 and I.431;

– other analogue or digital accesses for semi-permanent connections without associated outband signalling information,

with flexible information channel (bearer channel) allocation by use of a bearer channel connection protocol providing concentration capability within the AN.

This Recommendation is based on ITU-T G.964 and refers to it for those parts which are common in both Recommendations.

The electrical and functional interface specification for the interface links uses the 2048 kbit/s parts of ITU-T G.703, G.704 and G.706. Up to 16 interface links may be operated in parallel forming the V5.2 interface.

The signalling from the PSTN user port is converted into a stimulus protocol with a functional part for the signalling path using layer 3 multiplexing for the information from the different user ports.

The information from the ISDN D-channels is frame relayed in the Access Network using the mechanisms defined in ITU-T Q.933.

A control protocol defined in this Recommendation is used for the exchange of the individual port status and control functions required for the coordination with the call control procedures in the Local Exchange.

A bearer channel connection protocol establishes and de-establishes bearer connections required on demand, identified by the signalling information, under the control of the Local Exchange.

A link control protocol is defined for the mult-link management to control link identification, link blocking and link failure conditions.

In order to coordinate the traffic demands in the various protocols, up to three communication channels can be provisioned per interface link to transport the various protocols and frame relayed information. The data link layer for the protocols is defined on the bases of ITU-T Q.920 and Q.921.

A protection protocol, operated on two separate data links for security reasons, is defined to manage the protection switching of communication channels in case of link failures.

Source

ITU-T Recommendation G.965 was revised by ITU-T Study Group 15 (2001-2004) and approved under the WTSA Resolution 1 procedure on 1 March 2001.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

Page

Page

Page

Page

Introduction

Major differences between the V5.1 interface and the V5.2 interface

The V5.1 Recommendation (ITU-T G.964) is a complete Recommendation in itself whereas this V5.2 Recommendation references parts of ITU-T G.964.

V5.1 uses only one 2048 kbit/s link whereas V5.2 may use up to sixteen (16) 2048 kbit/s links on one interface.

V5.1 does not support concentration whereas V5.2 is inherently designed to support it using a dedicated protocol known as the Bearer Channel Connection (BCC) protocol.

V5.1 does not support ISDN primary rate access user ports whereas V5.2 does.

V5.1 has no concept of communication channel protection whereas this function is available for V5.2 when that particular V5.2 interface uses more than one 2048 kbit/s link. A specific protocol, known as the protection protocol, is provided for this function.

The control protocol for V5.2 is slightly modified to that used for V5.1.

A link control protocol is specified for V5.2 as multiple links have to be managed.

The following major changes have improved this version of ITU-T G.965, as compared against the previous version (dated 1995).

- [clause 4]: Generalizing the electrical and physical requirements;
- [5.1.1]: Link-ID verification not required for a single-link V5.2 interface;
- [5.1.2]: Enhancements of the link blocking in case of AN internal failures;
- [8.7.4]: Added reference to V5.1 about the need for a flow control mechanism on layer 2;
- [10.3]: Added pointers to V5.1 for control-field and frame type;
- [15.4]: Accelerated port alignment is an additional function that reduces the messages over the V5 interface during startup procedures;
- [16.2.1]: Clarification of link blocking and unblocking procedures;
- [16.2.4.3.1]: Immediate link blocking (and protection) on AN internal failure;
- [16.2.4.3.4]: Enhancements of the coordinated unblocking procedures;
- [16.2.4.3.5]: Simultaneous (AN+LE) link identification, but with priority for LE if on the same link;
- [17.3]: General for the message types with optional information elements: optional (O) has changed to conditional (C);
- [Figure 22]: Octet-1 changed from 0 × 40 to 0 × 44;
- [17.4.2.5/6]: Length of diagnostics in Reject/Protocol-error Cause IE;
- [Figure 24]: Note added on the use of the "extension" domain;
- [17.5.8.1a]: Added clause on BCC Reference Number coding error;
- [17.5.8.4/5/6]: Added Note on mandatory and optional IEs;
- [18.1.1]: Enhanced introduction for the Protection protocol;
- [18.1.5]: Improved text on monitoring of link failures;
- [Table 62]: Added coding for Logical C-Channel identification error;
- [18.6.6.1a]: Added clause on Logical C-Channel identification error;
- [Annex A]: Added A.7 "Possible AN/LE configuration using the V5 standard";

- [Annex C]: This annex is rewritten, to be in line with ITU-T G.964. When an item is the same, it only references V5.1. Procedures that have been modified are mostly related to startup, restart of the interface and also link blocking/unblocking. Supervision of the processing of startup sometimes has been added;
- [Annex E/Table E.2]: Three added IEs on PSTN (metering and attenuation);
- [Annex K.6]: Rewrite of AN internal failure rules;
- [Annex K.10]: Added clause on Link failure rules;
- [Annex L]: Added annex on Interoperability.

ITU-T Recommendation G.965

V-interfaces at the Digital Local Exchange (LE) – V5.2 interface (based on 2048 kbit/s) for the support of access network (AN)

1 Scope

This Recommendation specifies the electrical, physical, procedural and protocol requirements for the V5.2 interface between an Access Network (AN) and the Local Exchange (LE) for the support of the following access types:

– analogue telephone access;

– ISDN basic access with a line transmission system conforming to ITU-T G.960 [4] for the case with a NT1 separate from the AN;

– ISDN basic access with a user network interface according to ITU-T I.430 [3] at the user side of the AN (i.e. the interface at the T reference point);

– ISDN primary rate access with a line transmission system conforming to ITU-T G.962 [10] for the case with a NT1 separate from the AN;

– ISDN primary rate access with a user network interface according to ITU-T I.431 [9] at the user side of the AN (i.e. the interface at the T-reference point);

– other analogue or digital accesses for semi-permanent connections without associated out-band signalling information,

with flexible information channel (bearer channel) allocation on a call by call basis which provides concentration capability within the AN and over the V5.2 interface. This Recommendation does not specify the implementation of the requirements within the AN and does not constrain any implementation alternative as long as the functionality at the V5.2 interface as specified in this Recommendation is met.

This Recommendation should be used in conjunction with ITU-T G.964 [8]. The two Recommendations share a common format and clauses within ITU-T G.964 [8] are referenced in this Recommendation.

A link control capability is provided in order to manage the possible multi-link arrangements within a V5.2 interface. See clause 16.

A protection capability is provided in order to allow the interface to continue functioning in the event of 2048 kbit/s link failures.

Annex A provides an overview of the service scenarios and architecture taken as the conceptual basis for the specification of the V5.2 interface.

Annex B defines the use of the protocol information elements for the definition of the national PSTN protocols and information flow diagrams to the PSTN protocol specification. Annex H provides the definition of the Layer 3 PSTN protocol error detection.

Annex C specifies the basic assumptions of the management function in the LE and the AN to support correct operation and control of the configuration.

Annex D describes the protocol architecture for the ISDN and PSTN user port status control information transfer.

Annex E provides an overview of frame formats used in the V5.2 interface and also the message types allocated to the V5.2 interface.

Annexes F, G and H refer to Annexes F, H and K of ITU-T G.964.

Annex J presents explanatory notes and information flow for the Protection protocol.

Annex K gives information on principles for the BCC protocol application.

Annex L gives examples for an implementation with high interoperability.

2 Normative references

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of currently valid ITU-T Recommendations is regularly published.

[1] ITU-T G.703 (1998), *Physical/electrical characteristics of hierarchical digital interfaces*.

[2] ITU-T G.704 (1998), *Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels*.

[3] ITU-T I.430 (1995), *Basic user-network interface – Layer 1 specification*.

[4] ITU-T G.960 (1993), *Access digital section for ISDN basic rate access*.

[5] ITU-T Q.920 (1993), *ISDN user-network interface data link layer – General aspects*; and ITU-T Q.921 (1998), *ISDN user-network interface – Data link layer specification*.

[6] ITU-T Q.931 (1998), *ISDN User-network interface layer 3 specification for basic call control*.

[7] ITU-T G.823 (2000), *The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy*.

[8] ITU-T G.964 (2001), *V-interfaces at the digital local exchange (LE) – V5.1 interface (based on 2048 kbit/s) for the support of access network (AN)*.

[9] ITU-T I.431 (1993), *Primary rate user-network interface – Layer 1 specification*.

[10] ITU-T G.962 (1993), *Access digital section for ISDN primary rate at 2048 kbit/s*.

[11] ITU-T G.706 (1991), *Frame alignment and cyclic redundancy check (CRC) procedures relating to basic frame structures defined in Recommendation G.704*.

[12] ITU-T Q.824.5 (1997), *Stage 2 and stage 3 description for the Q3 interface – Customer administration: Configuration management of V5 interface environments and associated customer profiles*.

[13] ITU-T Q.831 (1997), *Fault and performance management of V5 interface environments and associated customer profiles*.

3 Definitions, symbols and abbreviations

3.1 Definitions

This Recommendation defines the following terms, in addition to those given in ITU-T G.964 [8] and in the normative references:

3.1.1 active C-channel: A physical C-channel which is currently carrying a logical C-channel. An active C-channel becomes a standby C-channel when it is not carrying a logical C-channel.

3.1.2 bearer channels: Bearer channels are used to provide the bidirectional transmission capability for allocated B-channels from basic access user ports, primary rate access user ports, or A-law PCM encoded 64 kbit/s channels from PSTN user ports. They may be used in multiples of 64 kbit/s channels in order to facilitate certain ISDN services.

3.1.3 bearer channel connection (BCC) protocol: A protocol which allows the LE to instruct the AN to allocate bearer channels, either singly or in multiples, on demand.

3.1.4 communication channel (C-channel): A 64 kbit/s time slot on a V5.2 interface provisioned to carry communication paths.

3.1.5 communication path (C-path): Any one of the following information types (see also 8.4.1):

- the layer 2 data link carrying the Control protocol;
- the layer 2 data link carrying the Link control protocol;
- the layer 2 data link carrying the PSTN signalling;
- each of the layer 2 data links carrying the Protection protocol;
- the layer 2 data link carrying the BCC protocol;
- all the ISDN Ds-type data from one or more user ports;
- all the ISDN p-type data from one or more user ports;
- all the ISDN f-type data from one or more user ports.

It should be noted that this definition includes the possibility that there is more than one C-path of the same information type, each allocated to a different logical C-channel.

3.1.6 ISDN D-channel information: ISDN D-channel information is defined as that D-channel information from basic or primary rate access user ports (including Ds-, p- and f-type data).

3.1.7 logical communication channel (logical C-channel): A group of one or more C-paths, all of different types, but excluding the C-path for the protection protocol.

3.1.8 multi-link: A collection of more than one 2048 kbit/s link which together make up a V5.2 interface (although a V5.2 interface need not have more than one 2048 kbit/s link).

3.1.9 multi-slot: A group of more than one 64 kbit/s channels providing 8 kHz and time slot sequence integrity, generally used together within an ISDN Primary Rate Access (ISDN-PRA) user port, in order to supply a higher bit-rate service.

3.1.10 physical communication channel (physical C-channel): A 64 kbit/s time slot on a V5.2 interface which has been assigned for carrying logical C-channels. A physical C-channel may not be used for carrying bearer channels.

Time slots 16 in the primary link and the secondary link (only in a V5.2 interface with more than one 2048 kbit/s link) are always physical C-channels.

3.1.11 pre-connected bearer channels: Any bearer channel or multiples thereof, set up using the BCC protocol in order to provide switched services within the AN over bandwidth reserved on the V5.2 interface reserved for it.

3.1.12 primary link: The 2048 kbit/s link in a multi-link V5.2 interface whose physical C-channel in time slot 16 carries a C-path for the protection protocol and, on V5.2 initialization, also the C-path for the control protocol, link control protocol, and the BCC protocol. Other C-paths may also be carried in the time slot 16.

3.1.13 protected group: A group of N logical C-channels.

3.1.14 protection group: A group of (N + K) physical C-channels, where K is the number of physical C-channels which act as standby C-channels for the N logical C-channels.

3.1.15 secondary link: The 2048 kbit/s link in a multi-link V5.2 interface whose time slot 16 carries a C-path for the protection protocol and, on V5.2 initialization, acts as the standby C-channel for the control protocol, link control protocol, and BCC protocol and any other C-paths initially carried in time slot 16 of the primary link.

3.1.16 standby C-channel: A physical C-channel which is not carrying a logical C-channel, but is used for the protection of logical C-channels. Once it is used to carry a logical C-channel, a standby C-channel becomes an active C-channel.

3.1.17 T-reference point: The term T-reference point is used in a general sense. If an ISDN terminal or terminal adapter is connected to the interface at the T-reference point then, according to the ISDN reference configuration, the S- and T-reference points coincide or, if a network termination type 2 is connected to the interface at the T-reference point, then this is the explicit T-reference point.

3.2 Symbols and abbreviations

This Recommendation uses the following abbreviations, in addition to those given in ITU-T G.964 [8]:

BCC	Bearer Channel Connection
dB	Decibel
ISDN-PRA	ISDN Primary Rate Access
H0	Channel with 384 kbit/s accompanied by timing
H12	Channel with 1920 kbit/s accompanied by timing
LFA	Loss of Frame Alignment
M	Mandatory protocol element
NOF	Normal Operational Frame
O	Optional protocol element
REQ	Request
SN	Sequence Number
TSSI	Time Slot Sequence Integrity
VP(R)	Receive state Variable for Protection protocol
VP(S)	Send state Variable for Protection protocol

4 Electrical and physical interface requirements

The V5.2 interface may have between one and sixteen 2048 kbit/s links, as required.

The interface may use any standard transmission system [1] and [2] that is designed to transport 2048 kbit/s signals. The interface shall conform to the electrical (optical) and format requirements appropriate for the selected structure.

NOTE – The remainder of this Recommendation is based on 2048 kbit/s electrical interface specifications.

For those cases when multiple (1-16) 2048 kbit/s electrical interfaces are used, the electrical and physical characteristics of each of the 2048 kbit/s interfaces shall conform to ITU-T G.703 [1], 2048 kbit/s case.

Two interface presentation alternatives are defined in ITU-T G.703 [1], the balanced interface pair type and the coaxial type. According to the two alternatives of interface applications shown in Figure 1, it is left to the network operator to request the interface presentation required.

The jitter requirements for each of the 2048 kbit/s links shall be the same as for ITU-T G.964 [8].

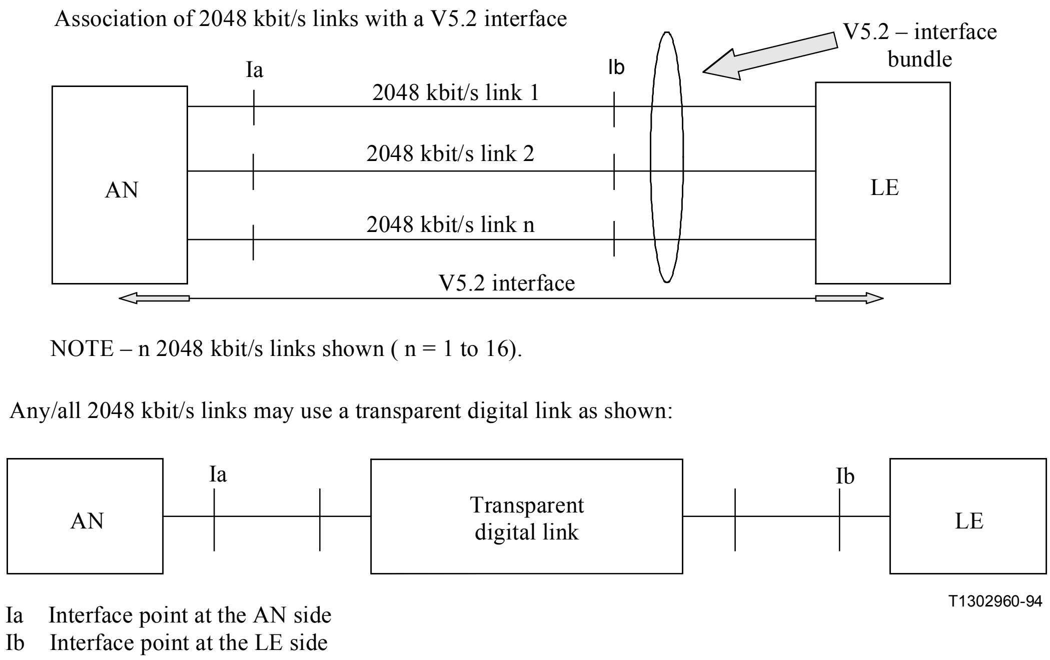


Figure 1/G.965 – V5.2 application with and without transparent digital link

5 Procedural interface requirements

The functional and procedural requirements of each of the 2048 kbit/s links shall be the same as for ITU-T G.964 [8].

5.1 Link control requirements and procedures

Since the V5.2 interface may consist of multiple 2048 kbit/s links, there is a need for link ID-verification and for blocking of a specific link. Two procedures have been defined for these functions in 16.2 and are performed through the link control protocol.

5.1.1 Link-ID verification

The link-ID verification is a symmetrical procedure that shall be applied from both ends of the V5.2-interface links, when the interface Layer 1 Finite State Machine (L1-FSM) enters the normal state. If the procedure fails, the FSM shall return to the non-operational state.

This procedure shall apply to all links, including the primary and secondary links. It may also be performed when permanently in the normal state, e.g. on a timed basis, or on a request from the Q-interface (AN/LE).

5.1.2 Link blocking

For link-maintenance additional functionality is required for blocking a single 2048 kbit/s link of a V5.2 interface. Link blocking is an asymmetrical procedure, where the AN may request the blocking of a link, but the LE decides, as master of the service. The LE releases any switched connection on the requested link as appropriate to the service and, in due time, re-establishes semi-permanent and pre-connected connections onto other links within the same V5.2 interface. The LE shall use the protection protocol to move affected logical C-channels, if at all possible.

In case of AN internal failures which result in the link not being available any longer the AN may apply immediate blocking of the link. In parallel, protection of any affected C-channels shall be initiated if available.

These procedures may be applied even in the case of the single 2048 kbit/s V5.2 interface.

NOTE – In this case, blocking takes the complete interface out of service.

6 Services and architecture aspects and requirements

The services to be supported by the V5.2 interface shall include all those supported by V5.1 (as defined in ITU-T G.964 [8]) with the addition of ISDN-PRA. However, it is not the intention of this Recommendation to restrict any implementation of ANs or LEs to support the full set or a subset of the services listed in this Recommendation.

The architecture of V5.2 from a service point of view is shown in Figure 2.

6.1 On-demand services

On-demand services pass through the V5.2 interface. The following three types of accesses are supported.

6.1.1 PSTN

The contents of this clause are identical to 6.1.1/G.964 [8].

6.1.2 ISDN Basic Access (ISDN-BA)

The contents of this clause are identical to 6.1.2/G.964 [8].

In addition, the 2 × 64 kbit/s multi-slot bearer service may be supported through the bearer channel capability defined in this Recommendation.

6.1.3 ISDN Primary Rate Access (ISDN-PRA)

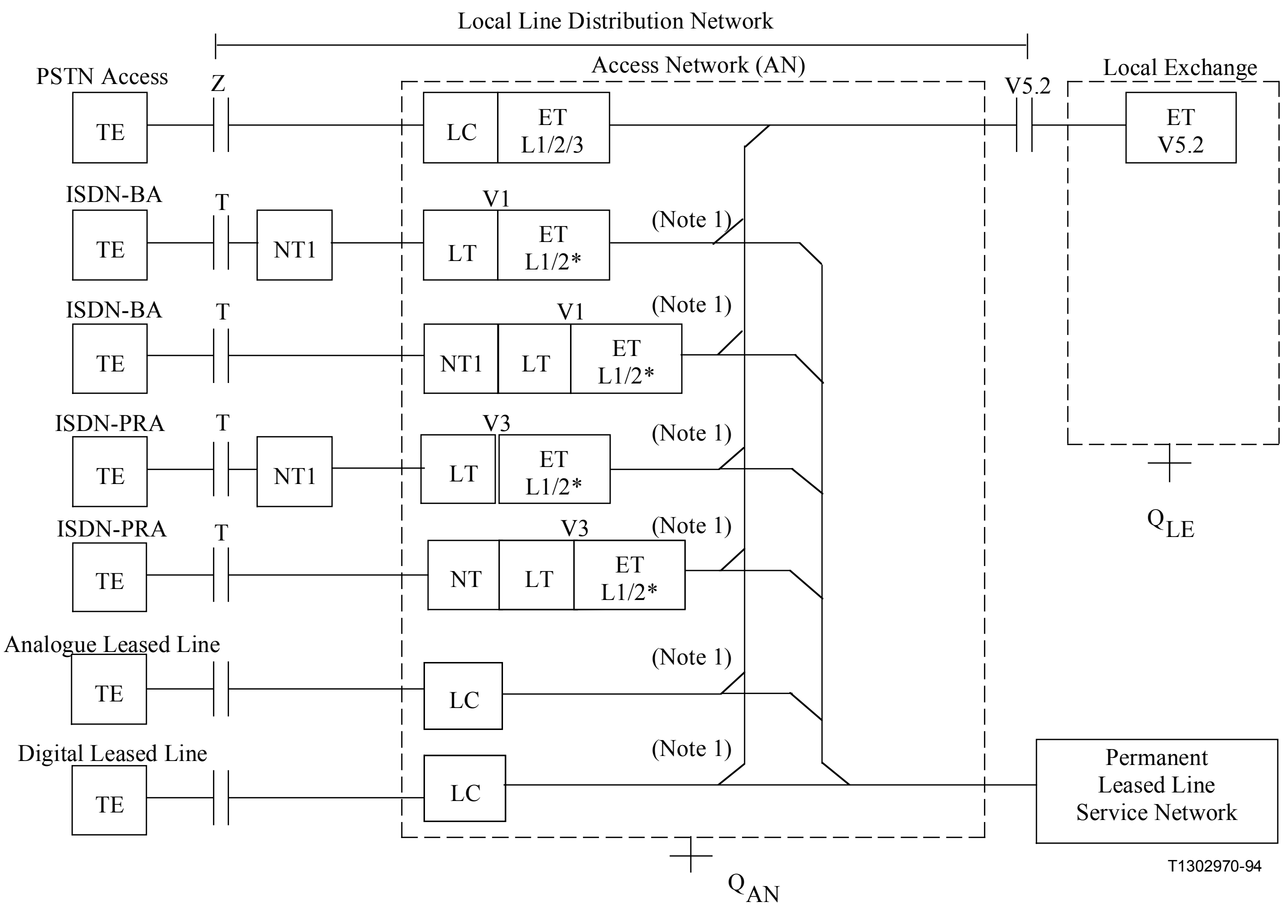
ISDN-PRA is supported either with an NT1 as an integral part of the AN, or as a separate equipment supporting transmission systems conforming to ITU-T G.962 [10] for the support of NT2 (e.g. ISDN PABX), connected at the T-reference point.

Bit rates lower than 64 kbit/s are not supported directly. They are seen as user applications within a 64 kbit/s B-channel in the PRA.

One or more B-channels in the PRA may be used for the optional permanent line capability or semi-permanent leased line service.

Multi-rate bearer services, which may use H0, H12 or other multi-slot channels between userport and LE are also supported by any V5.2 interface supporting ISDN-PRA using the appropriate ISDN signalling systems.

NOTE – Without support for these services from the LE or AN, they will be unavailable to users.



NOTE 1 – The selection of channels and the service allocation are part of the provisioning.
NOTE 2 – The asterisk indicates that layer 2 is only partially terminated in the AN.

Figure 2/G.965 – Architecture of V5.2 interface from a service point of view

6.2 Permanent Line (PL) capability

The contents of this clause are identical to 6.2/G.964 [8]. However, the PL capability shall be provided for the ISDN-PRA service as specified in 15.3.

6.3 Semi-permanent leased line

The contents of this clause are identical to 6.3/G.964 [8]. However, the semi-permanent leased line requirement shall be applicable for the ISDN-PRA as well.

6.4 Permanent leased line service

The contents of this clause are identical to 6.4/G.964 [8].

7 Control and provisioning

7.1 Control principles

7.1.1 General requirements and assumptions

Based on Figure 3, the following general requirements have been defined for both the ISDN-BA port and the ISDN-PRA port. They shall be relevant for the PSTN ports as well if not stated otherwise:

1) The responsibility for call control resides in the LE (i.e. the AN may have no knowledge of the call state during normal operation of the V5.2 interface).

2) The access management in the AN and the service management in the LE each maintain their FSMs and protocol entities and communicate over the V5.2 interface.

   FSMs are required for each user port and for the 2048 kbit/s interfaces as well as protocol entities for the layer 2 links, in both the AN and the LE (see Figure 4 for clarification and clause 15 for the definition of the FSMs, protocol entities and the layer 3 protocol). The information provided from the individual FSM or protocol entity to the management shall be used to decide on the appropriate action towards other FSMs and protocol entities, the call control function and the operating system. Further information on some basic assumptions is provided in Annex C.

3) Port blocking request, for non-urgent port maintenance via the Q-interface of the AN, can only be granted by the LE, (i.e. blocking request should not interfere with on-going calls, calls being set up or cleared down or semi-permanent connections).

4) Urgent port maintenance requested via the Q-interface of the AN shall be indicated to the LE irrespective of the state in the LE (i.e. "immediate blocking" effective immediately, but new state to be synchronized with the LE).

5) Detected layer 1 failures related to bearer channels within the failed 2048 kbit/s links shall result in the calls being cleared. Detected layer 1 failures relating to physical C-channels within a failed 2048 kbit/s link shall result in the protection protocol reassigning these C-channels if it has sufficient resources to do so. Pre-emption of physical C-channels autonomously by the protection protocol is not permitted. Detected layer 1 failures relating to semi-permanent leased lines within a failed 2048 kbit/s link shall result in the resource manager within the LE attempting to set up another bearer connection on which the service is to be provided. There may be anomalies and defects which may degrade the service but do not result in a total loss of service and thus do not result in the generation of the above re-configurations. Such anomalies or defects affecting PSTN service may impact the PSTN protocol, for instance through the negative acknowledgement of a request message, but shall not affect the port FSM.

6) It is required that detected anomalies and other events are reported to the associated management within the AN or LE and logged.

7) When a port is blocked, originating calls are not possible and terminating calls should be treated by the LE as if the port is out of service according to the national protocol.

8) The LE shall know the transmission quality level relating to user ports via "grading" messages from the AN to the LE which do not affect the port status FSMs. These messages contain grading information to be registered in the LE. The LE may use this information to decide whether a requested service should be delivered or not.

   This requirement is only relevant to an ISDN port with an NT1 which lies outside the AN. The performance between user port and V5.2 interface shall not be impacted unduly by a reduced performance due to bit errors occurring on AN internal links. This shall be excluded by in-service monitoring and blocking of AN internal links from service in the case of reduced error performance.

9) Loop-backs shall only be applied when the port is in the blocked state. This function is under the control of the AN.

   The execution of failure localization within the AN and the user port is the responsibility of the AN. Active testing which interferes with the service under the responsibility of the LE, shall not be carried out until the port is blocked (FSM in blocked condition) by the LE.

10) There shall be a mechanism to identify individual V5 interfaces, and the labels of their current and new provisioning variants. The provisioning variant is a unique label of a complete provisioning data set applied via the Q-interfaces (see 15.7).

11) It shall be possible to identify each individual 2048 kbit/s link on a V5.2 interface. A (symmetrical) procedure for checking the identity of 2048 kbit/s links shall be applied on any restoration of frame alignment and after reprovisioning (which may or may not affect V5.2 links).

12) It shall be possible to block an individual 2048 kbit/s link for a V5.2 interface. The AN may issue a request, but the LE decides: for switched connections it will wait for calls to terminate, semi-permanent and AN reserved connections will be re-established onto other links. LE system management will use the protection protocol to move affected logical C-channels before a 2048 kbit/s link is blocked. Using a slightly different mechanism, the AN may perform an immediate block of a designated 2048 kbit/s link.

13) 2048 kbit/s links may be removed from service within a V5.2 interface for maintenance purposes via Q_{LE} and Q_{AN} with the support of the V5.2-interface link control protocol. They will be brought back into service, also using the V5.2-link control protocol.

14) Individual bearer channels within a V5.2 interface may be barred from use via Q_{LE}.

7.1.2 Control of ISDN-BA user port for the PL capability

The control of ISDN-BA user ports when the PL capability is provided shall be the same as that provided by 7.1.2/G.964 [8].

7.1.3 Control of ISDN-PRA user ports when the PL capability is provided

The provision of a PL capability shall not affect the operation of an ISDN-PRA user port.

7.1.3.1 Statements and assumptions

1) The PL capability supported by an AN in the V5.2 configuration is an additional feature at an ISDN user network interface, which cannot be supported by an access connected directly to an LE.

2) The PL capability may, as an option, use one or more (or possibly all) of the B-channels on a user port that are not provisioned in the AN or LE to carry on-demand services. Only Normal Operational Frames (NOF) may be sent to the V-reference point as shown in Figure 3.

3) The LE is responsible for on-demand services.

4) When the LE blocks the user port, which puts the user port into a non-operational state for all types of services, the AN may regain control in order to allow ports with a PL capability to continue operating.

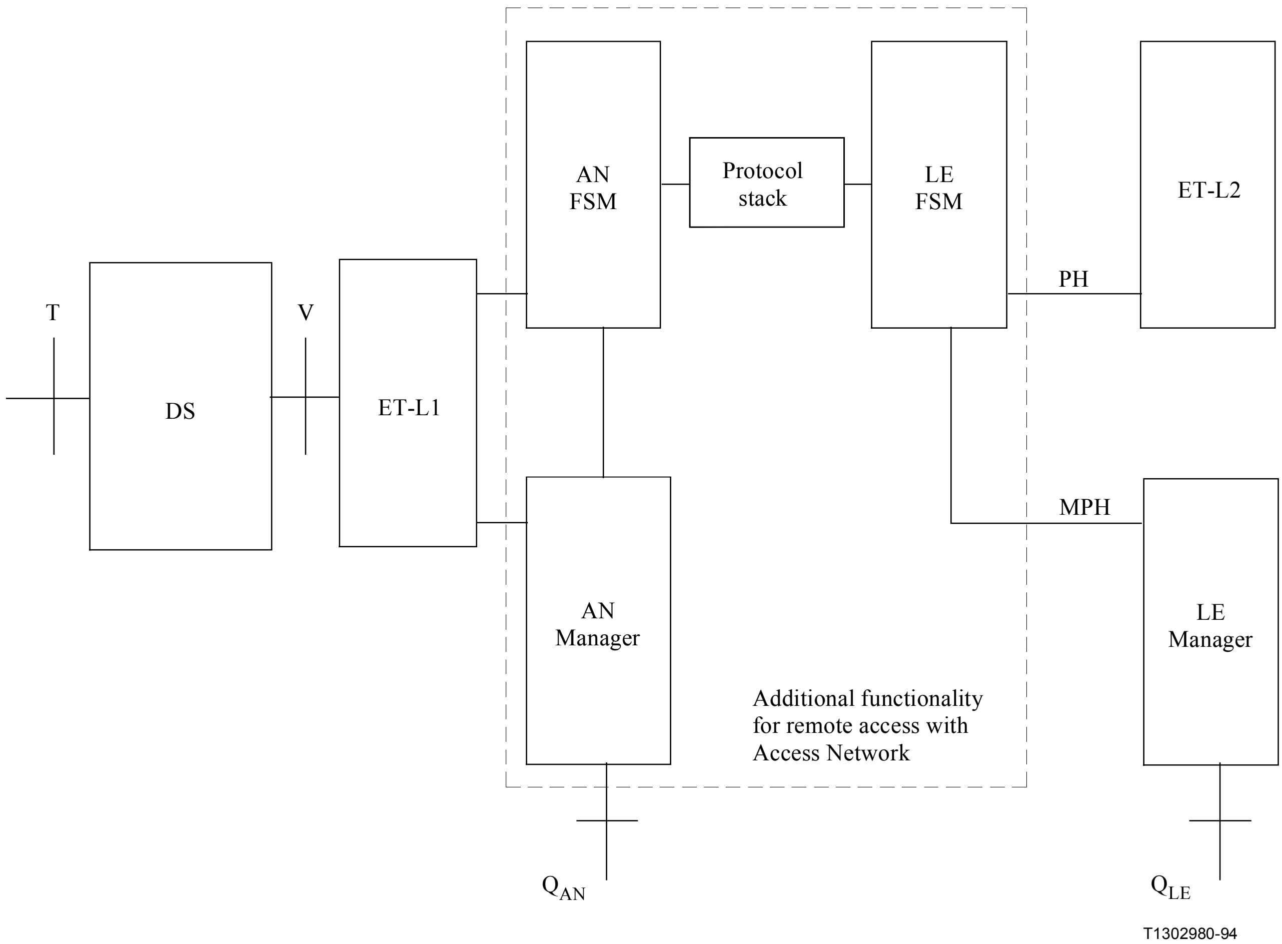
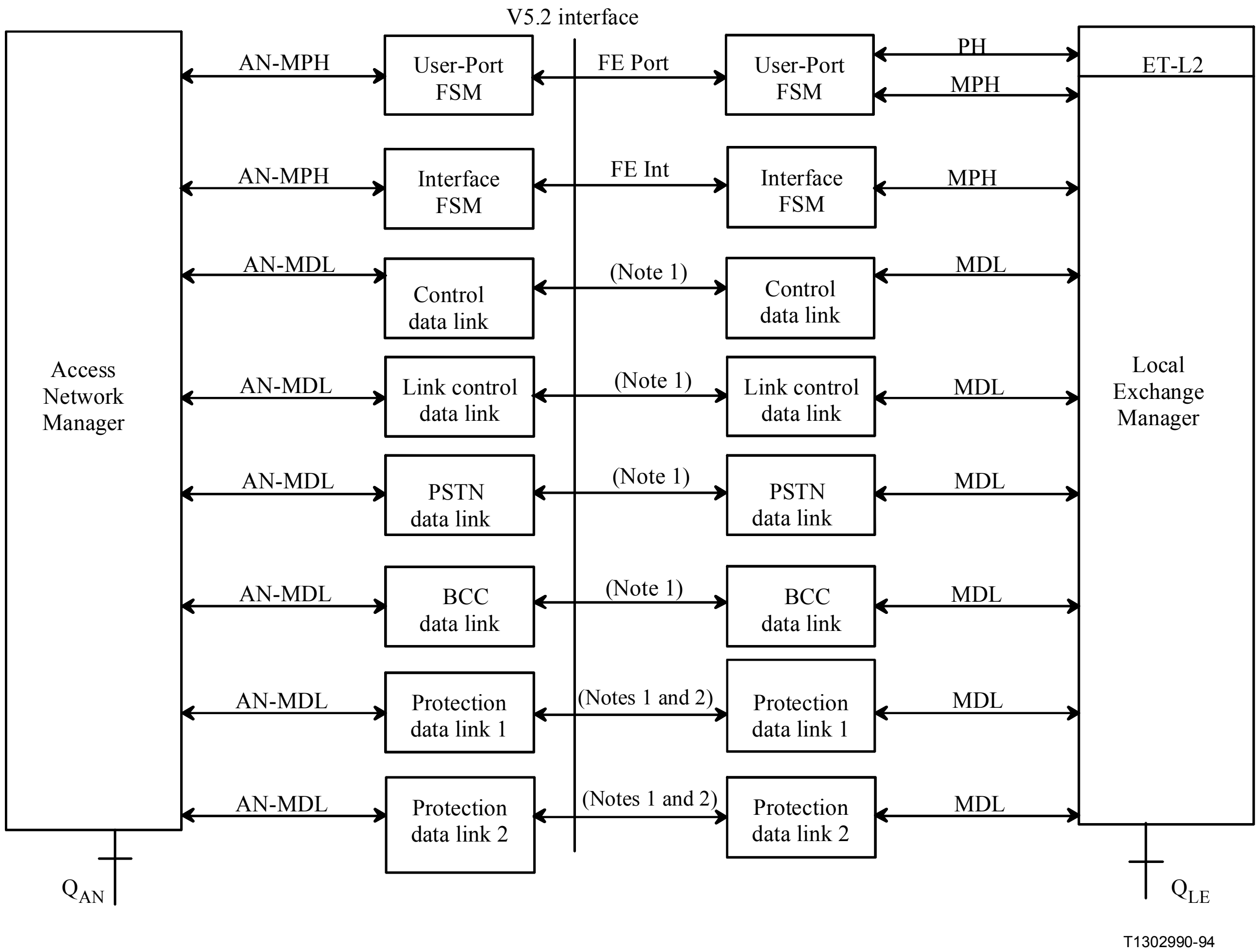


Figure 3/G.965 – ISDN user port functional model



NOTE 1 – Refer to 10.4.

NOTE 2 – The protection link protocol entities shall only be used in the case of a V5.2 interface with more than one 2048 kbit/s link.

Figure 4/G.965 – Layer 1 and layer 2 FSM functional model

7.1.3.2 ISDN and PL capability

The PL service shall not use the D-channel for messages to the LE. The currently defined ISDN-PRA service, ITU-T G.962 [10], delivered to an ISDN user port at an AN shall be the same as for direct access connections to the LE.

For an AN, no impact on an ISDN on-demand service can be accepted from any service (e.g. the PL service) that uses one or more of the B-channels for other than on-demand service.

7.2 Provisioning strategy and requirements

7.2.1 General

Provisioning is one of many aspects to control functions. It has been separated from the other control requirements because provisioning shall be performed through the Q-interfaces of the AN and the LE and is therefore not directly relevant to the V5.2-interface specification. Only those provisioning aspects having at least conceptual or indirect implication to the interface definition are defined.

7.2.2 Provisioning requirements

See 7.2.2/G.964 [8] for a list of items to be provisioned in addition to those below. The first item of the referenced list however is not valid for the V5.2 interface because the association of bearer channels is under the control of the BCC protocol and not statically associated through provisioning.

Provisioning requirements

1) The number of 2048 kbit/s links used on a V5.2 interface and their identification are assigned by provisioning.
2) Physical C-channels are assigned to time slots/links by provisioning.
3) The physical C-channels of time slots 16 of primary and secondary link form the protection group 1, including the protection protocol. (This assumes more than one 2048 kbit/s links on that V5.2 interface). Otherwise, this provisioning is invalid.
4) One of the physical C-channels of protection group 1 acts as the active C-channel. The other physical C-channel of protection group 1 acts as the standby C-channel of this group.
5) Logical C-channels are assigned to physical C-channels by provisioning as a default assignment.
6) A physical C-channel without assigned logical C-channel acts as a standby C-channel. (Assignment of C-paths to logical C-channels shall be through provisioning.)
7) The assignment of C-paths for Ds-type data (also for p-type and f-type data) or PSTN signalling is a provisioned option.
8) The active physical C-channel of protection group 1 shall carry at least the C-paths of the protection protocol, the BCC protocol, the control protocol, and the link control protocol.
9) Q_{LE} may be used to remove a logical C-channel's assignment from a physical C-channel.
10) Q_{LE} may be used to assign a particular logical C-channel to a physical C-channel. Protection may change it later.
11) When provisioning physical C-channels for an installation, care has to be taken if the LE and/or the AN consists of modules which share the software termination functions for the V5.2 interface. The effect of which physical C-channel is served by which module on load distribution has to be taken into account. Care has to be taken when provisioning physical C-channels for standby use in order that future protection switching onto these physical C-channels will not cause undue unevenness in the load on these modules.

    Similarly, if an LE and/or AN is modularized for the purpose of safeguarding performance in the presence of failures, care has to be taken that physical C-channels (both used and provided for standby) are provisioned in such a way that performance can be safeguarded through protection switching, not only in the presence of failures of 2048 kbit/s links but also in the presence of module failures within the LE and the AN.

7.3 Bearer Channel Connection (BCC)

The BCC protocol is used to allocate bearer channels on a specific 2048 kbit/s link to user ports, generally on a call by call basis. It is assumed that bearer channel resource management systems are provided within the LE and the AN but this Recommendation only defines the functions which directly impact the V5.2 interface.

The bearer channels allocated by means of the BCC protocol but not on a call by call basis are given below:

– *The semi-permanent leased line connection* – These use one or more bearer channels which are assigned to user ports using Q_{LE} and are set up using the BCC protocol;

– *The pre-connected bearer channels* – These use one or more bearer channels which are assigned to user ports using Q_{LE} and are set up using the BCC protocol.

An audit function is provided via the BCC protocol in order that V5.2-bearer channel allocation and connections within the AN may be checked.

An AN internal failure function is also provided in the BCC protocol in order that the AN may notify the LE about internal failures affecting bearer channel connections.

7.4 Protection

The protection protocol is used in the case of interfaces with more than one 2048 kbit/s link. It is required that the link control, the control, and the BCC protocols have a communication path over the V5.2 interface, even in the event of one 2048 kbit/s link failure (i.e. primary or secondary link).

The protection protocol has the responsibility to ensure that there is a method by which entities in the LE and AN can communicate for the purpose of protecting logical C-channels in the case of a single link failure, if standby physical C-channels are provisioned.

In the event of protection switching being required for logical C-channels, it is the responsibility of the protection management function to initiate the switch-over in a controlled manner using the protection protocol.

8 Protocol architecture and multiplexing structure

8.1 Functional description

The functional description is illustrated in Figure 5. Items in ITU-T G.964 [8] related to ISDN basic access shall also apply to ISDN primary rate access. The following functional requirements are defined in addition to those given in ITU-T G.964 [8]:

– a BCC protocol is used to assign bearer channels under the control of the LE;

– service requiring multi-slot connections, shall be provided over one 2048 kbit/s link within a V5.2 interface. In this case, 8 kHz and time slot sequence integrity shall always be provided;

– a link control protocol is defined which will support the management functions of the 2048 kbit/s links of the V5.2 interface;

– a protection protocol is defined which will support switching of logical C-channels between physical C-channels as appropriate.

8.2 Protocol requirements for PSTN and ISDN

Figure 6 shows the protocol architecture in a simplified form. The functions specified in this Recommendation are shaded.

The functions are defined in the following clauses:

– envelope function sublayer of LAPV5 (LAPV5-EF): clause 9;

– data link sublayer of LAPV5 (LAPV5-DL): clause 10;

– frame relaying sublayer of the AN (AN-FR): clause 11;
– sublayer-to-sublayer communication and mapping function: clause 12;
– general layer 3 protocol structures: clause 13;
– PSTN signalling protocol specification: clause 14;
– control protocol: clause 15;
– link control protocol: clause 16;
– BCC protocol: clause 17;
– protection protocol: clause 18.

The ISDN D-channel information from ISDN-BA and ISDN-PRA ports shall be multiplexed at layer 2 and frame relayed over the V5.2 interface. The capability to separate p-type and f-type data from Ds-type signalling data onto different communication channels shall be supported by the AN and the LE, but it shall be possible to carry them on a single communication channel as a provisioning option (see also 8.4).

Annex E gives an overview of message codepoints and frame formats used in the V5.2 interface.

The protocol specification for PSTN ports is specified in ITU-T G.964 [8].

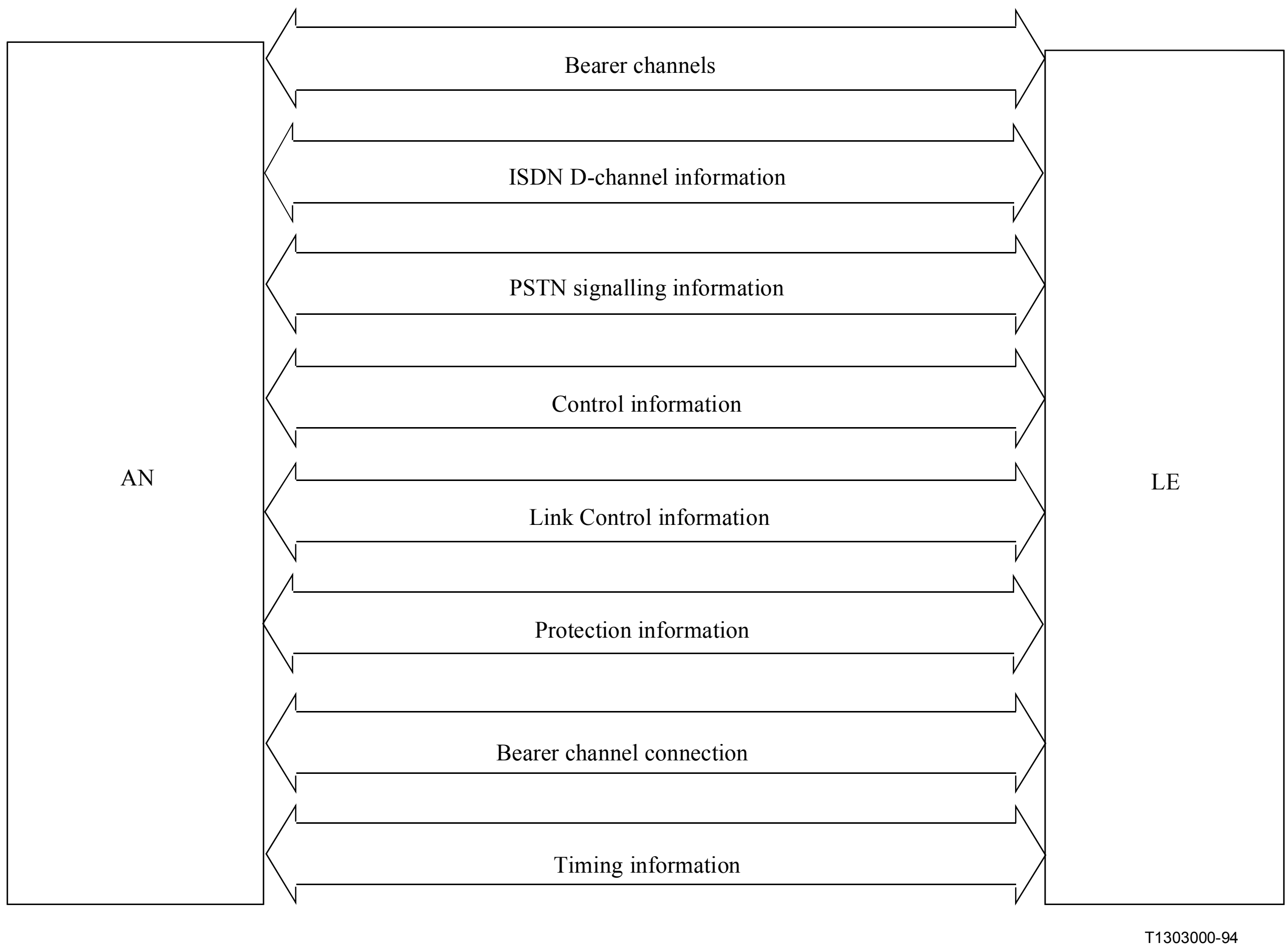


Figure 5/G.965 – Functional description of the V5.2 interface

8.3 Time slots

There shall be a minimum of one and a maximum of sixteen 2048 kbit/s links on a V5.2 interface. Each of these shall have a layer 1 structured according to clauses 4 and 5.

Time slots 16, 15 and 31 of each 2048 kbit/s link may be used as physical communication channels and shall be allocated as required by provisioning.

Time slots not provisioned as physical communications channels are available to be used as bearer channels under the control of the BCC protocol.

8.4 Time slot allocation for physical communication channels

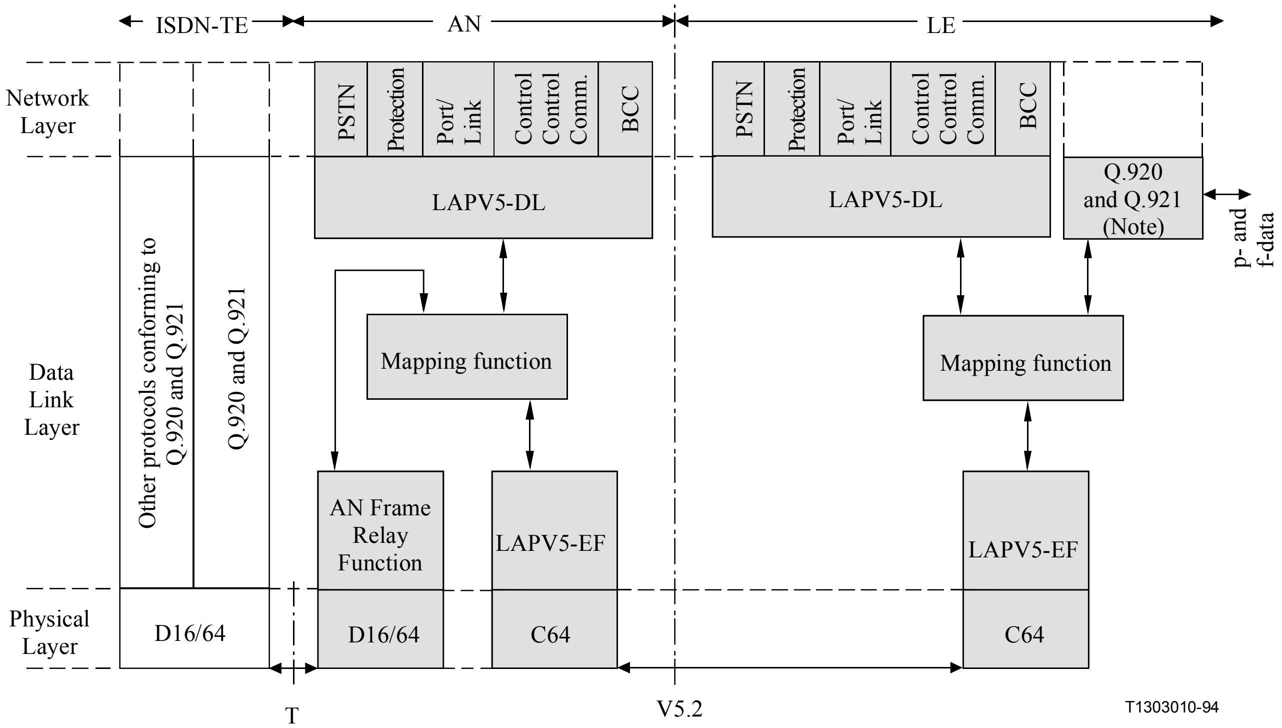
In the case of only one 2048 kbit/s link, the time slot allocation for the physical C-channels shall be the same as that for the physical C-channels in ITU-T G.964 [8]. This is to ensure full compatibility with V5.1.

In the case of more than one 2048 kbit/s links forming a V5.2 interface, then the protection protocol shall be used. In this case, time slot 16 of the primary link will contain the protection protocol and any C-path which has been provisioned to be within the same C-channel. Time slot 16 of the secondary link will also contain the protection protocol.

Further physical C-channels should preferably be allocated in the following sequence:

– Time slots 16 of the remaining 2048 kbit/s links as required. If more are required, then:
– Time slot 15 of a 2048 kbit/s link. If still more are required, then:
– Time slot 31 of the same 2048 kbit/s link shall be allocated. If still more are required, then:
– Continue the allocation by allocating time slot 15 and then 31 of the next 2048 kbit/s link as indicated in the previous subclause. This process may be repeated until all time slots 15 and 31 on all 2048 kbit/s links have been allocated.

The above guidelines have been created to allow for maximum flexibility when allocating time slots as physical C-channels whilst not constraining future service additions such as the ISDN H-channels. The allocation indicated above need not be followed, in particular when either upgrading from V5.1 to V5.2, or when increasing the capacity of a V5.2 interface, as to follow these guidelines explicitly may result in a total rearrangement of the physical C-channels on a V5.2 interface being required.



NOTE – Except those functions terminated in the AN Frame Relay function in the AN.

Figure 6/G.965 – Protocol architecture

8.4.1 Data types for V5.2 C-paths

The following types of data have been defined which are conveyed over the V5.2 interface as communication paths:

a) p-type data – This is ISDN D-channel data with SAPI 16.

b) f-type data – This is ISDN D-channel data with SAPI = 32 to 62.

c) Ds-type – This is ISDN D-channel signalling type data with SAPI not equal to any of those above.

NOTE – It has been identified that services using previously reserved SAPIs may be provided in the future. Giving a default allocation at least allows earlier implementations of V5.2 to transport these D-channel signalling types across the AN although their future data type allocation may be changed.

d) PSTN – This is PSTN signalling information.

e) Control – This is control information data.

f) Link control – This is link control information data.

g) BCC – This is a protocol which allocates bearer channels on demand.

h) Protection – This is a protocol which assigns logical C-channels to different physical C-channels when there are link failures within a V5.2 interface.

The control, BCC, link control and the protection communication paths shall always be allocated to time slot 16 of the primary link on initialization. The other communication paths shall be allocated to any logical C-channel excluding time slot 16 of the secondary link or those provided for protection purposes.

8.4.2 Communication paths when PSTN is provided on a V5.2 interface

Only one logical C-channel shall contain the PSTN protocol.

8.4.3 Communication paths when ISDN is provided on a V5.2 interface

p-type data from ISDN user ports may be placed in one or more logical C-channels.

f-type data from ISDN user ports may be placed in one or more logical C-channels.

Ds-type data from ISDN user ports may be placed in one or more logical C-channels.

The communication paths carrying p-type, f-type or Ds-type data from an ISDN user port may be placed in the same logical C-channel or split over different logical C-channels.

p-type data from any single user port shall not be split into different logical C-channels.

f-type data from any single user port shall not be split into different logical C-channels.

Ds-type data from any single user port shall not be split into different logical C-channels.

NOTE – p-type or f-type data may also be routed by an AN through the leased line service network by provisioning. There is no impact on this Recommendation.

8.5 Layer 2 sublayering and multiplexing on communication channels

The protocol specification and procedures for V5.2 follow directly from those provided in 8.5/G.964 [8].

8.6 Layer 3 multiplexing

In general, layer 3 multiplexing is the same as for 8.6/G.964 [8] with the following V5.2-relevant additions:

The link control protocol multiplexes information at layer 3 which is carried via the link control layer 2 data link over the V5.2 interface. The link control protocol is defined in clause 16.

The BCC protocol multiplexes information at layer 3 which is carried via the BCC layer 2 data link over the V5.2 interface. The BCC protocol is defined in clause 17.

The protection protocol multiplexes information at layer 3 which is carried via two protection layer 2 data links, one over the primary and the other over the secondary 2048 kbit/s links. The protection protocol is defined in clause 18.

8.7 Congestion control

The contents of this clause are identical to those of 8.7/G.964 [8].

8.7.1 Flow control end to end

The contents of this clause are identical to those of 8.7.1/G.964 [8].

8.7.2 Congestion control on the V5.2 interface

The contents of this clause are identical to those of 8.7.2/G.964 [8].

8.7.3 Blocking of ISDN user ports at layer 2

The contents of this clause are identical to those of 8.7.3/G.964 [8] and will also cover ISDN-PRA ports as well.

8.7.4 Flow control using LAPV5-DL mechanisms

The contents of this clause are identical to clause 8.7.4/G.964 [8].

9 Envelope Function sublayer of LAPV5 (LAPV5-EF)

The contents of this clause are identical to those of clause 9/G.964 [8].

10 Data Link sublayer of LAPV5 (LAPV5-DL)

10.1 Frame structure for peer-to-peer communication

The contents of this clause are identical to those of 10.1/G.964 [8].

10.2 Invalid frames

The contents of this clause are identical to those of 10.2/G.964 [8].

10.3 Elements of procedures and formats of fields for data link sublayer peer-to-peer communication

10.3.1 Link address field format

The contents of this clause are identical to those of 10.3.1/G.964 [8].

10.3.2 Link address field variables

10.3.2.1 Address field extension bit (EA)

The contents of this clause are identical to those of 10.3.2.1/G.964 [8].

10.3.2.2 Command/response field bit

The contents of this clause are identical to those of 10.3.2.2/G.964 [8].

10.3.2.3 V5DLaddr

The V5DLaddr shall be a 13-bit number. Values in the range of 0 up to 8175 shall not be used to identify a layer 3 protocol entity, because that range is used for identifying ISDN user ports.

Defined values of the V5DLaddr are given in Table 1.

10.3.3 Control field formats

The contents of this clause are identical to subclause 10.3.3/G.964 [8].

10.3.4 Control field parameters and associated state variables

The contents of this clause are identical to subclause 10.3.4/G.964 [8].

10.3.5 Frame types

The contents of this clause are identical to subclause 10.3.5/G.964 [8].

10.4 Definition of the peer-to-peer procedures of the data link sublayer

The contents of this clause are identical to those of 10.4/G.964 [8].

11 AN frame relay sublayer

The contents of this clause are identical to those of clause 11/G.964 [8].

12 Sublayer-to-sublayer communication and mapping function

The contents of this clause are identical to those of clause 12/G.964 [8].

Table 1/G.965 – Coding of V5DL address values

Bits								V5DLaddr
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
1	1	1	1	1	1	C/R	EA	Octet 1
								Octet 2
1	1	1	0	0	0	0	EA	PSTN signalling (8176 decimal)
1	1	1	0	0	0	1	EA	Control protocol (8177 decimal)
1	1	1	0	0	1	0	EA	BCC protocol (8178 decimal)
1	1	1	0	0	1	1	EA	Protection protocol (8179 decimal)
1	1	1	0	1	0	0	EA	Link control protocol (8180 decimal)

13 General layer 3 protocol structures

13.1 General

Within the V5.2 interfaces, different layer 3 protocols are supported, all of them using the same "protocol discriminator". Hence, the full set of protocols can be seen as a unique "V5.2" protocol composed by different sub-protocols:

– PSTN protocol;

– control protocol (common control and userport control);

– link control protocol;

– BCC protocol; and

– protection protocol.

All of these layer 3 protocols are defined as message-oriented protocols. Every message shall consist of the following parts (information elements). For each of them is indicated its number of octets (between brackets):

a) protocol discriminator (1 octet);

b) layer 3 address (2 octets);

c) message type (1 octet); and

d) other information elements, as required (the number of octets is information element dependent).

Information elements a), b) and c) shall be present in all messages, acting as a "header" for each of the messages; while information elements d) are specific to each message type.

This organization is illustrated in the example shown in Figure 7.

8	7	6	5	4	3	2	1	Octets
Protocol discriminator								1
Layer 3 address								2
Layer 3 address (lower)								3
0	Message type							4
Other information element								etc.

Figure 7/G.965 – General message organization example

For all the V5.2 protocols, every particular information element can be present only once in a particular message.

For each of the octets composing each of the information elements, the bit designated "bit 1" is transmitted first, followed by bits 2, 3, 4, etc. Similarly, for each of the information elements, the octet designated "octet 1" is transmitted first, followed by octets 2, 3, 4, etc.

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 the field.

The possible bits not used within the octet structure of a particular information element are considered as "reserved" and shall be coded as binary "all 0". However, the reception of a reserved field coded as something different than "all 0" will not cause a protocol error.

13.2 Information elements that appear in every message (header)

Within this clause, the information elements that appear in every message (acting as a message header) are described.

These information elements do not include an explicit information element identifier field. Hence each of them will be identified from the position of the octets in every message.

13.2.1 Protocol Discriminator information element

The purpose of the Protocol Discriminator information element is to distinguish messages corresponding to one of the V5 protocols (PSTN protocol, Control protocol, Link control protocol, BCC protocol or Protection protocol) defined in ITU-T G.964 [8] and this Recommendation, from other messages corresponding to other protocols (not defined within these Recommendations) making use of the same V5 (in this case V5.2) data link connections.

NOTE – The Protocol Discriminator information element has been included within the V5 protocols for structure compatibility with other protocols (e.g. with ITU-T Q.931 [6]). It provides a mechanism for future compatibility, allowing the use of the same V5-data link connection for other Layer 3 protocols not yet identified.

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

The length of the Protocol Discriminator information element shall be 1 octet.

The structure and coding of the Protocol Discriminator information element shall be as indicated by Figure 8.

8	7	6	5	4	3	2	1	Octet
0	1	0	0	1	0	0	0	1

NOTE – All other values are reserved.

Figure 8/G.965 – Protocol Discriminator information element

13.2.2 Layer 3 Address information element

The purpose of the Layer 3 Address information element is to identify the layer 3 entity, within the V5.2 interface, to which the transmitted or received message applies.

The Layer 3 Address information element shall be the second part of every message (located after the Protocol Discriminator information element).

The length of the Layer 3 Address information element shall be 2 octets.

The structure of the Layer 3 Address information element is protocol dependent, for the PSTN protocol (see 13.4.3/G.964 [8]) and for the Control protocol (see 14.4.2.3/G.964 [8]). For the link control protocol, this information element retains the name layer 3 address although it is used to refer to 2048 kbit/s links (it is defined in 16.3.2.1). For the BCC protocol this information element has been named the "BCC Reference Number" information element and is defined in 17.4.1. For the Protection protocol this information element has been named the "Logical C-channel identification" information element and is defined in 18.5.1.

13.2.3 Message Type information element

The purpose of the Message Type information element is to identify the function of the message being sent or received.

The Message Type information element shall be the third part of every message (located after the Layer 3 address information element).

The length of the Message Type information element shall be 1 octet.

The structure of the Message Type information element shall be as indicated by Figure 9.

8	7	6	5	4	3	2	1	Octet
0	Message Type							1

Figure 9/G.965 – Message Type information element

The coding of the Message Type information element shall be as specified within this Recommendation. See Annex E for a full listing of message codepoints.

The general layout of the coding of the Message Type field shall be as indicated in Table 2.

Table 2/G.965 – Message type coding structures for the V5.2 protocols

Bits							Message types
7	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	–	–	–	–	PSTN protocol message types
0	0	1	0	–	–	–	Control protocol message types
0	0	1	1	–	–	–	Protection protocol message types
0	1	0	–	–	–	–	BCC protocol message types
0	1	1	0	–	–	–	Link control protocol message types
NOTE – All other values are reserved.							

13.3 Other information elements

These information elements may appear in the different messages, being optional or mandatory depending on the message semantics and/or the protocol application of the message.

These information elements are specific for each of the protocols. For the PSTN protocol specific information elements see 13.4/G.964 [8], for the control protocol specific information elements see 14.4.4.2/G.964 [8], for the link control protocol specific information elements see 16.3.2, for the BCC protocol specific information elements see 17.4 and for the protection protocol specific information elements see 18.5.

See Annex E for a complete list of V5.2-information elements.

13.4 Protocol message functional definition and information content

In the protocol definitions of this Recommendation the different messages are specified highlighting the functional definition and information content (i.e. semantics) of each message. Each definition includes:

a) A brief description of the message, direction and use.

b) A table listing the information elements in the order of their appearance in the message (same relative order for all message types). For each information element the table indicates:

   1) the clause of this Recommendation describing the information element;

   2) the direction in which it may be sent: i.e. AN to LE, LE to AN, or both;

   3) whether inclusion is mandatory ("M") or optional ("O");

   4) the length of the information element in octets.

13.5 Codesets

For the coding of the information elements the same rules apply as defined in 4.5.1/Q.931 [6], without the functionality of the Shift information element, i.e. there shall be only one codeset.

14 PSTN signalling protocol specification and layer 3 multiplexing

The contents of this clause are identical to those of clause 13/G.964 [8].

15 Control requirements and protocol

This clause defines the port control and common control requirements, protocols and procedures in the form of normative FSM specifications and supporting prose description of the procedures.

15.1 ISDN-BA user port status indication and control

The contents of this clause are identical to those of 14.1/G.964 [8].

15.2 PSTN user port status indication and control

The contents of this clause are identical to those of 14.2/G.964 [8].

15.3 ISDN primary rate user port status indication and control

15.3.1 General aspects

The ISDN primary rate user port status indication is based on the defined split of responsibilities between AN and LE. Only that status information of the user port having call control relevance shall influence the state machine in the LE via the V5.2 interface.

Port tests, e.g. loop back operation, shall be the responsibility of the AN. However, those tests which interfere with the service shall only be performed when the port is "Blocked", either due to failure or on request to and permission by the LE. This requires two groups of states, relevant to the V5.2-interface protocol, at both sides:

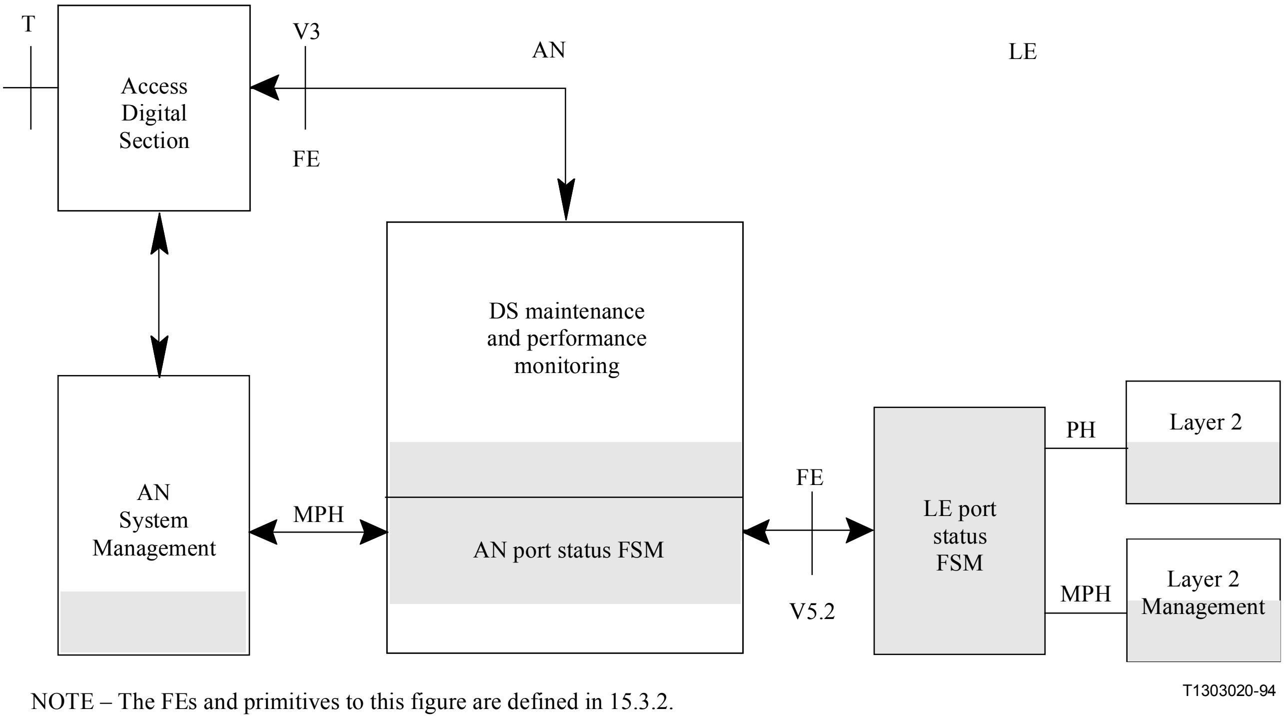
– operational state; and

– non-operational state.

Additional states are required in the AN for maintenance of the DS and the user port. ISDN primary rate access is permanently active at layer 1. If the DS detects a loss of layer 1 capability at its user side, the access shall be considered as non-operational from the LE point of view, while from the AN point of view, the DS is still in normal condition. This distinction is made by the AN system management and reported to the LE using additional Function Elements (FEs) and management primitives.

Figure 10 shows the functional model for control of the ISDN primary rate user port. The shading indicates the area defined in this Recommendation. The definition of the other functions and capabilities are outside the scope of this Recommendation. Reference is made to Annex C for further information about assumptions for the system management functions in the AN and LE.

In the following, only those functions and procedures are specified having relevance to the V5.2 interface.



NOTE – The FEs and primitives to this figure are defined in 15.3.2.

Figure 10/G.965 – Primary rate port control functional model

15.3.2 Events and function elements relevant for the control of the state machines

Tables 3, 4, 5 and 6 give the set of FEs relevant for the V5.2 interface, the FEs defined in ITU-T G.962 [10] and the primitives (PH and MPH) towards layer 2 and the system management function in AN or LE (see also Figures 3/G.964 and 4/G.964 [8]. Figure 10 gives the definitions and the procedures for the FEs and the events used in Tables 3 to 6.

Table 3/G.965 – ITU-T G.962 [10] set of function elements with relevance to interface V5.2

FE	Name	DS ⇔ ET	Meaning at ET in LE
FE-A	Normal operation of DS	→	Not directly relevant
FE-B	Normal operation of ET	←	Not directly relevant
FE-C	Unintentional loopback	AN maintenance	Not directly relevant
FE-D	LOS/LFA at TE (FC2)	AN maintenance	Not directly relevant
FE-E	LOS at line side of NT1 (FC3)	AN maintenance	Not directly relevant
FE-F	LOS/LFA at V3 reference point of ET (FCL)	AN maintenance	Not directly relevant
FE-G	LOS/LFA at T reference point of NT1 (FC4)	AN maintenance	Not directly relevant
FE-H	FC3 and FC4 simultaneously	AN maintenance	Not directly relevant
FE-I	Loss of power at NT1	AN maintenance	Not directly relevant

Table 3/G.965 – ITU-T G.962 [10] set of function elements with relevance to interface V5.2

FE	Name	DS ⇔ ET	Meaning at ET in LE
FE-K	FE-I and FE-D simultaneously	AN maintenance	Not directly relevant
FE-L	LOS at line side of LT (FC1)	AN maintenance	Not directly relevant
NOTE – FE-M to FE-P of ITU-T G.962 [10] refer to failures in a separate digital link and are not relevant. FE-Q to FE-T refer to loopback operation and are outside the scope of interface V5.2. FE-U to FE-Y are related to CRC-4 error detection and relevant to performance monitoring only (see 15.3.4).			

Table 4/G.965 – Set of function elements of interface V5.2

FE	Name	AN ⇔ LE	Description
FE201	Unblock	←	Request or acknowledgement
FE202	Unblock	→	Request or acknowledgement
FE203	Block	←	Command
FE204	Block	→	Command
FE205	Block request	→	Request
FE206	Grading	→	Performance information (Note 1)
FE207	D-channel block	←	Command (Note 2)
FE208	D-channel unblock	←	Command (Note 2)
FE209	TE out of service	→	Indication of user failure
FE210	Failure inside network	→	Indication of network failure
NOTE 1 – The grading information may be sent from the AN system management when being in state AN/LE2.0, see also 15.3.4. NOTE 2 – The commands "D-channel block" and "D-channel unblock" shall be used to interrupt or resume the operation of the upstream D-channel of an individual ISDN user port according to the requirement in 8.7.3/G.964 [8]. These commands may appear when being in state AN/LE2.0 without change of state.			

The function elements are reported by the DS immediately after detection of an event. The effect on the port control, which has relevance to the call control procedures, shall be delayed by an appropriate persistence check procedure. This is outside the scope of this Recommendation and not reflected in the AN (ISDN primary port) FSM. Reference is made to ITU-T I.431 [9] which gives an example of an appropriate persistence check procedure.

Table 5/G.965 – Set of primitives in the LE

Primitive	FSM ⇔ L2/Management	Description
MPH-UBR	←	Unblock request
MPH-UBR	→	Unblock request
MPH-UBI	→	Unblock indication
MPH-BI	←	Block command
MPH-BI	→	Block command
MPH-BR	→	Incoming block request
PH/MPH-AI	→	Access activated (operational)
PH/MPH-DI	→	Access deactivated (not operational)
MPH-UF	→	User failure indication
MPH-NF	→	Network failure indication
MPH-GI	→	Grading information with parameter (Note 1)
MPH-DB	←	Block D-channel from user port (Note 2)
MPH-DU	←	Unblock D-channel from user port (Note 2)
NOTE 1 – The grading information may be sent from the AN system management when in state LE2.0, see also 15.3.4. NOTE 2 – The commands "MPH-DB" and "MPH-DU" shall be used to interrupt or resume the operation of the upstream D-channel of an individual ISDN user port according to the requirement in 8.7.3/G.964 [8]. These commands may appear when in state LE2.0 without change of state.		

15.3.3 ISDN-PRA user port FSMs, AN (ISDN port) and LE (ISDN port)

The primitives, FEs and the state tables are given for the definition of the functional behaviour and cooperation between the various functional blocks. There is no restriction for the implementation of these functions as long as the implementation is in conformance with the functionality defined in this Recommendation over the interface V5.2 and with the primary rate access digital section.

Table 6/G.965 – Set of management primitives in the AN relevant to interface V5.2

Primitive	Management ⇔ FSM	Description
MPH-UBR	→	Unblock request
MPH-UBR	←	Unblock request
MPH-UBI	←	Unblock indication
MPH-BI	→	Block command
MPH-BI	←	Block command
MPH-BR	→	Block request
MPH-NOF	←	User and DS normal
MPH-Eic	←	AN maintenance
MPH-Eid	←	AN maintenance

Table 6/G.965 – Set of management primitives in the AN relevant to interface V5.2

Primitive	Management ⇔ FSM	Description
MPH-Eie	←	AN maintenance
MPH-Eig	←	AN maintenance
MPH-Eih	←	AN maintenance
MPH-Eii	←	AN maintenance
MPH-Eik	←	AN maintenance
MPH-Eil	←	AN maintenance
MPH-EIlos	←	AN maintenance
MPH-UF	→	User failure indication
MPH-NF	→	Network failure indication
MPH-GI	→	Grading information with parameter (Note 1)
MPH-DB	←	Block D-channel from user port (Note 2)
MPH-DU	←	Unblock D-channel from user port (Note 2)
MPH-PAR	→	Request for port operation for PL capability (Note 3)
MPH-PAI	←	Port operation for PL capability indication (Note 3)
MPH-PDR	→	Request port non-operation for PL capability (Note 3)
MPH-PDI	←	Port non-operation for PL capability indication (Note 3)
MPH-LxAR	→	Activate loopback (Note 3)
MPH-AI	←	Loopback activation indication (Note 3)
MPH-DR	→	Loopback release request (Note 3)
NOTE 1 – The grading information may be sent from the AN system management when being in state AN2.0, see also 15.3.4. NOTE 2 – The commands "MPH-DB" and "MPH-DU" are used to interrupt or resume the operation of the upstream D-channel of an individual ISDN user port according to the requirement in 8.7.3/G.964 [8]. These commands may appear when being in state AN2.0 without change of state. NOTE 3 – The last seven primitives are not directly relevant for the interface V5.2 but given for information and complete description of the reaction in the FSM on receipt of those events even in states relevant to interface V5.2.		

15.3.3.1 Description of the states

The procedure for blocking and unblocking of the user port as specified in the port FSMs takes account of the principles given in 7.1/G.964 [8].

Blocking request shall be issued from the AN system management only when being in the operational state. This request does not have any effect on the state unless the LE responds with FE203.

Immediate blocking indication has immediate effect in any relevant state in both FSMs. No specific confirmation of this indication is required.

Unblocking needs to be coordinated on both sides. Therefore, an unblock request requires confirmation from the other side. The Coordination is guaranteed through the two unblock states. If a block indication is received from the other side when in local unblock state this shall only be interpreted as no confirmation and may be relevant only for the management system.

The unblock request may also be used by the management system to confirm the status of the layer 1 state machines.

The AN-FSM defined for the ISDN primary rate port supports the optional PL-capability which requires that the access digital section and the user terminal may become operational under the control of the AN while the LE is non-operational. The procedure uses the states AN1.1 and AN3.0.

Maintenance of the DS and loopback tests (see FE-Q to FE-T of ITU-T G.962 [10]) may use the additional states AN4 which are outside the scope of this Recommendation. These states shall only be entered from the state AN1.0 or AN1.2.

State AN4 can only be entered from states AN1 and shall only return to AN1.0. To align AN and LE FSM FE204 shall be sent to the LE and the unblock procedure may then be applied.

15.3.3.2 Definition of port control states

The user port FSMs reflect the AN and LE view of the layer 1 state of the ISDN port only. Call control is the responsibility of the ISDN protocol.

15.3.3.2.1 ISDN-PRA user port FSM – AN (ISDN port)

Non-operational (AN1 and AN3): D-channel blocking has been applied to the port. Therefore, no layer 2 information shall be frame relayed to the LE, and the port cannot be used to originate or terminate calls.

Blocked (AN1.0): The port is in the non-operational state and neither side has initiated unblocking. Two sub-states are required to satisfy the DS and the user-network interface specification.

Local unblock (AN1.1): The AN has initiated unblocking (by sending FE202) and is awaiting confirmation from the LE. Although the DS is in normal condition the AN-FSM has to signal to the TE that the access is not operational by sending RAI.

Remote unblock (AN1.2): The LE has initiated unblocking (by sending FE201) and is awaiting confirmation from the AN. Two sub-states are required to satisfy the DS and the user-network interface specification. They correspond to the two sub-states of AN1.0.

NOTE – States AN1.1 and AN1.2 provide a mechanism for the synchronized unblocking of ports.

PL operational (AN3): The AN system management has initiated the port operation for PL capability when the LE does not support unblocking of the port (AN1.1). In case of a failure report from the DS or on request from the AN system management the AN port FSM goes back to state AN1.02.

Operational (AN2.0): The port is operational from the AN and LE point of view, layer 2 (and layer 3) links may be established and the port can be used to originate or terminate calls.

15.3.3.2.2 ISDN-PRA user port FSM – LE (ISDN port)

Non-operational (LE1): No layer 2 information is expected at the LE, and the port cannot be used to originate or terminate calls.

Blocked (LE1.0): The port is in the non-operational state and neither side has initiated unblocking.

Local unblock (LE1.1): The LE has initiated unblocking (by sending FE201) and is awaiting confirmation from the AN.

Remote unblock (LE1.2): The AN has initiated unblocking (by sending FE202) and is awaiting confirmation from the LE.

NOTE – States LE1.1 and LE1.2 provide a mechanism for the synchronized unblocking of ports.

Operational (LE2.0): Layer 1 of the primary rate access is operational. Layer 2 (and layer 3) links may be established. The port can be used to originate or terminate calls.

15.3.3.3 Principles and procedures

15.3.3.3.1 General

The next subclauses describe the mechanism implemented in the FSMs in AN and LE for ISDN (primary rate access) ports, which are presented in the relevant state transition tables.

The following mechanisms are described:

- blocking;
- blocking request;
- coordinated unblocking;
- user failure/network failure indication;
- support of the permanent line capability.

15.3.3.3.2 Blocking

A user port, when being in the operational state (AN2/LE2), can be blocked from either sides. However, the AN system management has no knowledge about the call state of the port, and hence shall only apply this procedure under failure and other conditions (when the persistence check procedure has been passed), that allow for affecting the service.

When AN system management issues MPH-BI, the FSM sends FE204 (Block Command) to the LE and goes to the Blocked state AN1.0, sub-state AN1.02 to signal the non-operational condition to the TE.

The AN-FSM may also block the port autonomously when the DS indicates a failure condition. The appropriate sub-state supports the port control through the DS as specified in the relevant Recommendations.

When LE system management issues MPH-BI, the FSM sends FE203 (Block Command) to the AN and goes to the Blocked state LE1.0.

15.3.3.3.3 Blocking request

The blocking request mechanism allows for non-urgent port blocking (e.g. deferrable maintenance). In this case AN system management issues a Blocking Request (MPH-BR) resulting in FE205 to the LE. This request shall be passed by the LE-FSM to LE System management by MPH-BR.

LE System management, knowing the call state, may grant the request by issuing MPH-BI, resulting in FE203 (Block Command) to the AN, then goes to Blocked state.

In case of a semi-permanent connection the LE System management will not grant this request but send MPH-UBR as a negative confirmation.

The AN system management may cancel the blocking request by issuing MPH-UBR. The LE system management may then receive MPH-UBI and cancel the blocking request (i.e. ignore the previously received request) if the port has not yet been blocked. In the latter case, the LE may start the unblock procedure by issuing MPH-UBR.

15.3.3.3.4 Coordinated unblocking

Unblocking a port, needs to be Coordinated at both sides. An unblock request requires confirmation from the other side. To guarantee this Coordination there are two separate Unblock states (Local & Remote Unblock) in both FSMs. This procedure is fully symmetrical between AN and LE. If the LE wants to unblock, it issues MPH-UBR, sends FE201 (Unblock request) and goes to "Local Unblock" (LE1.1). The AN goes to "Remote Unblock" (AN1.2), to the corresponding sub-state as in state AN1.0, and sends MPH-UBR to its system management, which may agree, then responds with MPH-UBR (unblock acknowledge), sends FE202 and goes to "Access Operational" state (AN2.0).

For the LE in "Local unblock" and receiving this acknowledgement, the FSM goes to "Access Operational" (LE2.0) and issues MPH-UBI to its system management. The AN System management may as well take the initiative, for which the same procedure applies.

For AN and LE, when in "Remote unblock" (AN1.2x, LE1.2x) state and receiving FE204 or FE203 respectively, the port state FSM is returned back to "Blocked" (AN1.0, LE1.0), and a MPH-BI sent to system management. This undoes a previous Unblock Request from the other side.

The AN system management may cancel the blocking request by issuing MPH-UBR. The LE system management may then receive MPH-UBI and cancel the blocking request (i.e. ignore the previously received request) if the port has not yet been blocked. In the latter case the LE may start the unblock procedure by issuing MPH-UBR.

See C.5 for basic system management requirements.

15.3.3.3.5 User failure/network failure indication

For the full support of the ISDN service the LE needs to know the reason for the blocking of the port, i.e. the port was blocked due to failure in the user's responsibility or in the network's responsibility. This information can only be provided by the AN system management knowing the location of the failure from the information provided by the access digital section and internal failure detection capabilities. Failure conditions (FC) 2 and 4 (FE-G only, FE-G and FE-K together, under certain conditions) are understood as user failures but the AN may confirm this by applying failure localization prior to the indication to the LE. The identification of "loss of power at NT1" (FE-I) as user failure or network failure depends on the NT1 powering arrangement.

The AN system management shall inform the LE system management by sending the appropriate information (MPH-UF or MPH-NF) to the AN (ISDN primary port) FSM which will send FE209 or FE210 to the LE (ISDN primary port) FSM respectively. The FSM in the LE will then inform the LE system management accordingly.

15.3.3.3.6 Support of the permanent line capability

Since the primary rate user port is permanently active there is no particular requirement for the V5.2 primary rate port control above the procedures already defined. If the LE blocks the user port or, if after restoration from a failure in the DS or TE, the unblock procedure is not supported by the LE, the AN system management may bring the user port into PL operational by issuing MPH-PAR. The AN FSM will go into state AN3.0 and confirm with MPH-PAI. With MPH-PDR the AN system management may disable PL capability which will be responded by the FSM with a change to state AN1.02 and MPH-PDI. This procedure is not relevant to the LE.

15.3.3.4 ISDN port FSM at the AN

The ISDN-PRA user port FSM is defined in Table 7 in accordance with Figure 10.

Table 7/G.965 – AN (ISDN primary port) FSM for ISDN-PRA user ports

State	AN1.01	AN1.02	AN1.1	AN1.21	AN1.22	AN2.0	AN3.0
Event \ State name	Blocked 1	Blocked 2	Local unblock	Remote unblock 1	Remote unblock 2	Access operational	PL operational
Signal to V3	NOF	RAI	RAI	NOF	RAI	NOF	NOF
FE201	MPH-UBR 1.21	MPH-UBR 1.22	MPH-UBI 2.0	MPH-UBR –	MPH-UBR –	FE202; MPH-UBI –	MPH-UBI 2.0
FE203	–	–	MPH-BI 1.02	MPH-BI 1.01	MPH-BI 1.02	MPH-BI 1.02	MPH-BI –
MPH-UBR	MPH-BI –	FE202 1.1	FE202 –	FE204; MPH-BI 1.01	FE202; MPH-UBI 2.0	FE202; MPH-UBI –	MPH-PAI –
MPH-BI	FE204 –	FE204 –	FE204 1.02	FE204 1.01	FE204 1.02	FE204 1.02	FE204 1.02
MPH-BR	–	–	/	/	/	FE205 –	/
NOF	MPH-NOF 1.02	MPH-NOF –	–	MPH-NOF 1.22	MPH-NOF –	–	–
LOS/LFA	MPH-EIlos 1.02	MPH-Eilos –	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02	FE204; MPH-Eilos 1.02
FE-C	MPH-EIc 1.02	MPH-Eic –	FE204; MPH-Eic 1.02	FE204; MPH-Eic 1.02	FE204; MPH-Eic 1.02	FE204; MPH-Eic 1.02	FE204; MPH-EIc 1.02
FE-D	MPH-EId –	MPH-EId 1.01	FE204; MPH-Eid 1.01	FE204; MPH-Eid 1.01	FE204; MPH-Eid 1.01	FE204; MPH-EId 1.01	FE204; MPH-EId 1.01
FE-E	MPH-EIe –	MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01	FE204; MPH-EIe 1.01
FE-G	MPH-EIg 1.02	MPH-EIg –	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02	FE204; MPH-EIg 1.02
FE-H	MPH-EIh 1.02	MPH-EIh –	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02	FE204; MPH-EIh 1.02
FE-I	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –	MPH-EIi –
FE-K	MPH-EIk –	MPH-EIk 1.01	FE204; MPH–EIk 1.01	FE204; MPH-EIk 1.01	FE204; MPH-EIk 1.01	FE204; MPH-EIk 1.01	FE204; MPH-EIk 1.01
FE-L	MPH-EIl 1.02	MPH-EIl –	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02	FE204; MPH-EIl 1.02
MPH-LxAR	FE-Q/R 4.x	FE-Q/R 4.x	/	FE-Q/R 4.x	FE-Q/R 4.x	/	/

Table 7/G.965 – AN (ISDN primary port) FSM for ISDN-PRA user ports

State	AN1.01	AN1.02	AN1.1	AN1.21	AN1.22	AN2.0	AN3.0
State name / Event	**Blocked 1**	**Blocked 2**	**Local unblock**	**Remote unblock 1**	**Remote unblock 2**	**Access operational**	**PL operational**
Signal to V3	**NOF**	**RAI**	**RAI**	**NOF**	**RAI**	**NOF**	**NOF**
MPH-UF	FE209 –	FE209 –	/	FE209 –	FE209 –	/	/
MPH-PAR	/	/	MPH-PAI 3.0	/	/	/	–
MPH-PDR	/	/	/	/	/	/	MPH-PDI 1.02
MPH-NF	FE210 –	FE210 –	/	FE210 –	FE210 –	/	/
MPH-GI	/	/	/	/	/	FE206 –	/
FE207	/	/	/	/	/	MPH-DB –	/
FE208	/	/	/	/	/	MPH-DU –	/

– No state change

/ Unexpected event, no state change

NOF Normal Operational Frames

LOS/LFA Loss of Signal/Loss of Frame Alignment

NOTE 1 – States AN4 are not relevant to interface V5.2 and not defined in this Recommendation.

NOTE 2 – If D-channel blocking has been applied to a user port after receipt of FE207, when in state AN2.0 and if the port FSM leaves state AN2.0, then D-channel blocking shall be removed.

The AN FSM covers single failure events from the DS only except where multiple failures are reported by the DS, i.e. FE-H and FE-K. A new detected event means that a previously reported failure has disappeared.

The AN FSM provides a mechanism which allows the system management of the AN to verify that the FSM is in the Operational state, without having to go through the sequence of blocking and unblocking. This mechanism is internal to the AN. To do so the AN system management issues MPH-UBR and receives the information whether the FSM is in a non-operational state.

15.3.3.5 ISDN port FSM at the LE

Table 8 gives the FSM of the LE.

Table 8/G.965 – LE (ISDN primary port) FSM for ISDN-PRA user ports

State	LE1.0	LE1.1	LE1.2	LE2.0
Event / State name	**Blocked**	**Local unblock**	**Remote unblock**	**Access operational**
MPH-UBR	FE201 1.1	FE201 –	PH/MPH-AI; FE201 2.0	FE201 –
MPH-BI	FE203 –	FE203 1.0	FE203 1.0	FE203 1.0
FE202	MPH-UBR 1.2	PH/MPH-AI 2.0	MPH-UBR –	MPH-UBI
FE204	–	MPH-BI 1.0	MPH-BI 1.0	MPH-BI; PH/MPH-DI 1.0
FE205	–	–	–	MPH-BR –
FE206	/	/	/	MPH-GI –
FE209	MPH-UF –	MPH-UF –	/	/
FE210	MPH-NF –	MPH-NF –	/	/
MPH-DB	/	/	/	FE207 –
MPH-DU	/	/	/	FE208 –

– No state change

/ Unexpected event, no state change

NOTE – If the D-channel blocking has been applied to a user port when in state LE2.0, by issuing the MPH-DB primitive, the system management shall be aware that D-channel blocking in the AN will be removed, after the port FSM in the AN leaves state AN2.0.

The LE FSM provides a mechanism which allows the system management of the LE to verify that the FSM is in the operational state by issuing MPH-UBR, without having to go through the sequence of blocking and unblocking.

Unlike the corresponding situation for the AN, this mechanism is not internal to the LE and requires the cooperation of the AN FSM, and confirms the alignment of both FSMs and the link between them.

The asymmetry here reflects the responsibility of the LE for supporting the service.

15.3.4 Performance monitoring aspects

The performance of the primary rate access digital section, if implemented with the NT1 implemented separately from the AN, shall be monitored by the AN (FE-U for the downstream direction or CRC-4 block in error detected in AN for the upstream direction). The application of the mechanism is to be provisioned at the AN and LE on a per port basis.

As reflected in ITU-T G.964 [8] (7.1.1, item 7), the working concept is that on the V5 interface there is no impact from any implementation of the user-port. The AN is supposed to monitor the performance of the access digital section. Parameters for validation algorithms and specific thresholds shall be pre-defined in the AN. Only passing the threshold will be reported ("Grading" with parameter indicating which grade is now relevant) at a maximum rate of once a minute. The LE may use these reports to decide whether or not a requested service shall be delivered. This concept makes performance monitoring on V5 access-implementation independent, having no effect on the Port-Status FSM.

The persistent excess of a bit error ratio of 10^{-3} shall be considered as a failure requiring maintenance (according to the M-series Recommendations and ITU-T G.921), and therefore immediate blocking of the user port.

The use of FE-W, FE-X and FE-y for remote user maintenance under control of the AN is optional and left to the operator. This does not have any impact on the V5.2 interface.

15.4 Control protocol

15.4.1 Control protocol message definition and content

The contents of this clause are identical to 14.4.1/G.964 [8].

Table 9/G.965 – Coding of Control function element

Bits (octet 3)							Control function element
7	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	1	FE101 (activate access)
0	0	0	0	0	1	0	FE102 (activation initiated by user)
0	0	0	0	0	1	1	FE103 (DS activated)
0	0	0	0	1	0	0	FE104 (access activated)
0	0	0	0	1	0	1	FE105 (deactivate access)
0	0	0	0	1	1	0	FE106 (access deactivated)
0	0	1	0	0	0	1	FE201/202 (unblock)
0	0	1	0	0	1	1	FE203/204 (block)
0	0	1	0	1	0	1	FE205 (block request)
0	0	1	0	1	1	0	FE206 (performance grading)
0	0	1	0	1	1	1	FE207 (D-channel block)
0	0	1	1	0	0	0	FE208 (D-channel unblock)
0	0	1	1	0	0	1	FE209 (TE out of service)
0	0	1	1	0	1	0	FE210 (failure inside network)
NOTE – All other values are reserved.							

15.4.2 General message format and information element coding

The contents of this clause are identical to 14.4.2/G.964 [8] with the exception of Table 54/G.964 [8] which is modified due to two additional Control function elements required for the ISDN primary rate port, and with the exception of Table 55/G.964 [8] which is modified due to 20 additional Control function IDs for the accelerated alignment procedure. Tables 9 and 9a show the modified Tables 54 and 55/G.964 [8], respectively.

Table 9a/G.965 – Coding of Control function ID

Bits (octet 3)							Control function ID	Optional information element considered mandatory
7	**6**	**5**	**4**	**3**	**2**	**1**		
0	0	0	0	0	0	0	Verify re-provisioning	Variant
0	0	0	0	0	0	1	Ready for reprovisioning	Variant
0	0	0	0	0	1	0	Not ready for reprovisioning	Variant, Rejection cause
0	0	0	0	0	1	1	Switch over to new variant	Variant
0	0	0	0	1	0	0	Re-provisioning started	Variant
0	0	0	0	1	0	1	Cannot re-provision	Variant, Rejection cause
0	0	0	0	1	1	0	Request variant and interface ID	–
0	0	0	0	1	1	1	Variant and Interface ID	Variant, Interface ID
0	0	0	1	0	0	0	Blocking started	–
0	0	1	0	0	0	0	Restart	–
0	0	1	0	0	0	1	Restart complete	–
0	0	1	0	0	1	0	UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS REQUEST	Note 1, Note 2
0	0	1	0	0	1	1	UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS ACCEPTED	Note 1, Note 2
0	0	1	0	1	0	0	UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS REJECTED	Note 1, Note 2
0	0	1	0	1	0	1	UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS COMPLETED	Note 1, Note 2
0	0	1	0	1	1	0	UNBLOCK ALL RELEVANT PSTN PORTS REQUEST	–
0	0	1	0	1	1	1	UNBLOCK ALL RELEVANT PSTN PORTS ACCEPTED	–
0	0	1	1	0	0	0	UNBLOCK ALL RELEVANT PSTN PORTS REJECTED	–
0	0	1	1	0	0	1	UNBLOCK ALL RELEVANT PSTN PORTS COMPLETED	–

Table 9a/G.965 – Coding of Control function ID

Bits (octet 3)							Control function ID	Optional information element considered mandatory
7	6	5	4	3	2	1		
0	0	1	1	0	1	0	UNBLOCK ALL RELEVANT ISDN PORTS REQUEST	Note 1
0	0	1	1	0	1	1	UNBLOCK ALL RELEVANT ISDN PORTS ACCEPTED	Note 1
0	0	1	1	1	0	0	UNBLOCK ALL RELEVANT ISDN PORTS REJECTED	Note 1
0	0	1	1	1	0	1	UNBLOCK ALL RELEVANT ISDN PORTS COMPLETED	Note 1
0	0	1	1	1	1	0	BLOCK ALL PSTN PORTS REQUEST	–
0	0	1	1	1	1	1	BLOCK ALL PSTN PORTS ACCEPTED	–
0	1	0	0	0	0	0	BLOCK ALL PSTN PORTS REJECTED	–
0	1	0	0	0	0	1	BLOCK ALL PSTN PORTS COMPLETED	–
0	1	0	0	0	1	0	BLOCK ALL ISDN PORTS REQUEST	Note 1
0	1	0	0	0	1	1	BLOCK ALL ISDN PORTS ACCEPTED	Note 1
0	1	0	0	1	0	0	BLOCK ALL ISDN PORTS REJECTED	Note 1
0	1	0	0	1	0	1	BLOCK ALL ISDN PORTS COMPLETED	Note 1
– All other values reserved. NOTE 1 – "ISDN ports" means ISDN basic access ports and ISDN primary rate access ports. NOTE 2 – See the definition of the relevant port in 3.1.								

15.4.3 State definition of the control protocol

The contents of this clause are identical to 14.4.3/G.964 [8].

15.4.4 Control protocol procedures

The contents of this clause are identical to 14.4.4/G.964 [8].

15.4.5 Accelerated alignment of the port related protocol entities and FSMs

Alternatively it is possible to align port states in AN and LE by the commands:

a) Unblock all relevant PSTN and ISDN ports request (Note 1);

b) Unblock all relevant PSTN ports request;

c) Unblock all relevant ISDN ports request (Note 1);

d) Block all PSTN ports request;

e) Block all ISDN ports request (Note 1);

NOTE 1 – The terminus ISDN includes ISDN basic access and ISDN primary rate access.

NOTE 2 – See the definition of the relevant port in 3.1.

This can be accepted or rejected.

In case of the accelerated alignment procedures "unblock all relevant ports requested" according to a), b) and c):

After acceptance by the peer entity, all relevant ports are brought to the unblocked state on both sides except those considered unsuitable to be unblocked. After completion, the ports considered unsuitable to be unblocked are re-aligned by performing the normal port blocking procedure (using MPH-BI). See Annex C for details.

In case of the accelerated alignment procedures "block all ... ports requested" according to d) and e):

After acceptance by the peer entity, all ports are brought to the blocked state on both sides. After completion, the requesting peer entity may initiate normal port unblocking procedures (using MPH-UBR) for those ports considered unsuitable to be blocked. See Annex C for details.

The peer entity which has blocked the ports is responsible for the unblocking of the affected ports after the blocking cause is no longer valid. Nevertheless both sides are allowed to try unblocking of the ports.

The implementation of the accelerated alignment procedures according to a), b), c), d) or e) is optional (e.g. an implementation may support only the procedures b) and d)). If the implementation does not support one of the accelerated alignment procedures, it shall send the corresponding REJECT cause. If the requested procedure is not implemented, the receiving side of the request shall answer with the appropriate REJECT message as defined in Table 9a.

The procedures UNBLOCK ALL RELEVANT PSTN PORTS and UNBLOCK ALL RELEVANT ISDN PORTS shall be used at the requesting side instead of the procedure UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS.

15.5 V5.2-re-provisioning procedures

The contents of this clause are identical to those of 14.5/G.964 [8].

16 Link control requirements and protocol

This clause defines the link control requirements, protocols and procedures in the form of normative FSM specifications and supporting prose description of the procedures.

In the V5.2-interface there is a need for the following functions and requirements for each individual 2048 kbit/s link:

a) the 2048 kbit/s layer 1 link status and link identification as relevant (see 16.1);

b) the blocking and coordinated unblocking of a layer 1 link by the system management (see 16.2);

c) the verification of the link continuity by the link identification (see 16.2);

d) the coordination of these link control functions (see 16.2); and

e) the link control protocol for the communication between AN and LE on the coordination of these functions at both sides (see 16.3).

All these requirements are defined in this clause.

Figure 11 shows the functional model for control of a single link of a V5.2-interface. Reference is made to Annex C for further information about assumptions for the system management functions in the AN and LE.

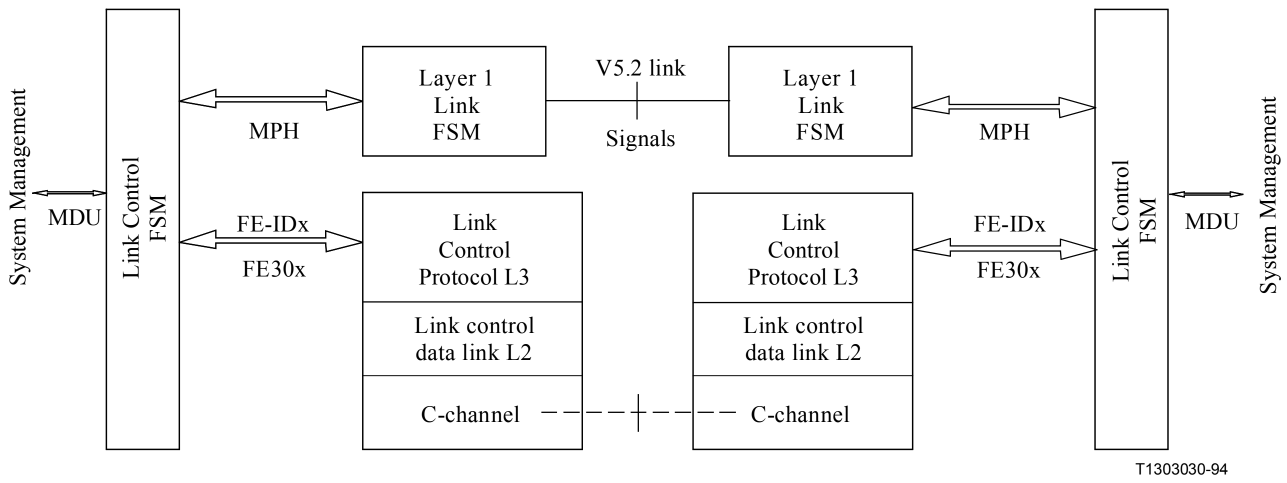


Figure 11/G.965 – Link control functional model

The functional model shows that the layer 1 link FSM, which is directly related to the interface signals, reacts autonomously from the link control functions and procedures. It is the responsibility of the link control to coordinate the layer 1 link and the link control procedures so that the system management is always aware of the status of that link.

Communication of each link control FSM with its layer 1 link FSM is provided through Management Primitives (MPHs), while communication with the system management uses Management Data Units (MDUs). For communication with the remote link control FSM, FEs are conveyed by a layer 3 protocol specified in 16.3. There are as well MDUs sent from the link control protocol entity to the system management for the support of the protocol error handling procedures.

Layer 1 link FSM acts autonomously on layer 1 signals and identifies the layer 1 link status to the link control FSM by MPH-DI and MPH-AI. The layer 1 condition will be detected at both sides of the layer 1 link interface. Due to the fact that the pre-defined persistence check timers may have different values in LE and AN, the indication to the link control FSM may be at different points in time. The possible resulting problems have been taken into account in the definition of the link control FSM.

It is the responsibility of the LE system management to decide whether link operation should be initiated after layer 1 has recovered from a failure condition (link control FSM issues MDU-LAI) without link identification procedure applied or after successful link identification only.

16.1 2048 kbit/s layer 1 link maintenance requirements

16.1.1 Events and failure reports

The requirements and specifications in this subclause are relevant for both the AN and LE because of the symmetry of the interface functions.

The 2048 kbit/s layer 1 link specification is based upon the V5.1-layer 1 interface requirements and procedures. In order to make the upgrade path from V5.1 to V5.2 easier to understand, the parts common to V5.1 and V5.2 are shown first, and the extra parts for V5.2 are then shown. In Table 10, the set of common events are shown first, with the V5.2-specific ones shown below the line within the table. In Table 12, the V5.2-specific states shown as AN/LE5.1 and AN/LE5.2 are shown delineated by double lines.

Table 10 gives the identified events for each 2048 kbit/s layer 1 link of a V5.2-interface.

Table 10/G.965 – Events and primitives for the interface layer 1 link FSM

Event (signal)	AN/LE ⇔ Management	Primitive
Operational signal (normal frames, not RAI)	→	MPH-AI
Non-operational condition	→	MPH-DI
Loss of signal	→	MPH-EIa
Loss of frame alignment	→	MPH-Eia
Reception of remote alarm indication (RAI)	→	MPH-EIb
Reception of AIS (Note 1)	→	MPH-EIc
Internal failure	→	MPH-EId
CRC block received in error	→	MPH-EIe
CRC error information (i.e. E-bit set to ZERO) (Note 2)	→	MPH-EIf
Request to stop with error report (Note 2)	←	MPH-stop
Request to proceed with error report (Note 2)	←	MPH-proceed
Link identification indication	→	MPH-IDI
Send link identification signal	←	MPH-ID
Remove link identification signal	←	MPH-NOR
Link identification request	←	MPH-IDR
Link identification failure	→	MPH-EIg
NOTE 1 – AIS may be generated by the V5.2-interface link in case it has detected an internal failure preventing it from generating the normal output signal. The receiving side of the interface, however, shall detect this event because the application alternative with a transparent digital link between the LE and the AN AIS may be generated by this link according to ITU-T Recommendations (see also clause 4).		
NOTE 2 – These events have relevance for the interface and the relation with the management system but do not have impact on the FSM.		

The FSMs AN (interface) and LE (interface) can both be regarded as being constructed from two fundamental states: operational and non-operational. The transition to these conditions shall be notified by MPH-AI or MPH-DI at the AN and MPH-AI or MPH-DI at the LE respectively.

The report mechanism available to the remote side of the interface is the RAI function and the CRC error report function (E-bit).

16.1.2 Detection algorithm for events and signals

The detection algorithm for events or signals is defined in Table 11.

Table 11/G.965 – Detection algorithm for layer 1 signals

Normal frames	The algorithms shall be in accordance with those given in 4.1.2/G.706 [11] and 4.2/G.706 [11].
Loss of frame alignment	The algorithm shall be in accordance with the one given in 4.1.1/G.706 [11].
RAI	RAI is detected when both of the two following conditions occur: – frame alignment condition; and – reception of one bit A with binary content ONE.
Loss of signal	The equipment shall implement one or both of the following alternatives to detect "loss of signal". The detection of this event shall not inhibit the operation of the frame alignment procedure. a) The incoming signal amplitude is, for a time duration of at least 1 ms, more than 20 dB below the nominal output amplitude defined in ITU-T G.703 [1]. b) The input detects more than 10 consecutive HDB3 ZEROs.
AIS	AIS is detected when both of the two following conditions occur: – loss of frame alignment; and – reception of 512-bit periods containing less than 3-binary ZERO (this is based on 3.3.2/O.162.
CRC error information	Reception of one E-bit set to ZERO.
Link identification signal	Normal frames received with 2 out of 3 Sa7 bits received set to ZERO.

16.1.3 V5.2-interface layer 1 link FSM

Three implementation alternatives have been identified concerning the reporting of detection of events from the FSM to the system management and the decision on the consequent action with regard to service provision:

a) immediate report of the detected event to the system management for logging (MPH-Eie) and processing to evaluate the interface status with regard to consequent actions on the service and the other FSMs. In this case the system management shall perform the necessary persistence check of the reported events to identify the operational or non-operational status of the interface; or

b) immediate report of the detected event to the system management for logging (MPH-EIe). The layer 1 performs the persistence check to evaluate the interface status resulting in a status report to the system management (i.e. MPH-AI, MPH-DI at the AN and LE); or

c) a combination of both alternatives a) and b).

Table 12 gives the interface FSM in the LE and the AN, symmetrical approach. It should be noted that this FSM allows all three approaches concerning the persistence check procedure implementation.

The persistence check timer(s) in AN and LE shall be pre-defined in steps of 100 ms, from 100 ms to 25 s. The persistence check timer(s) shall have a tolerance of ±50 ms for nominal values of 100 ms to 1 s and ±10 % above 1 s.

Layer 1 link FSM does not perform any action towards the link control FSM concerning the link identification procedure. The reason for this is that any possible misinformation has to be avoided if bit errors or coordination problems occur. Any action towards link control FSM required is controlled by an appropriate control function from the link control FSM. If layer 1 link FSM, when being in state 1, detects Sa7 bit set to ZERO (after successful performance of the persistence check procedure specified), the FSM goes to state 5.2, to keep the information available as long as the persistence check procedure result remains unchanged. If the link control FSM requests with MPH-IDR the link identification information, the layer 1 link FSM shall in this case respond with MPH-IDI, otherwise with MPH-EIg, which indicates link identification failure. If layer 1 link FSM is in one of the non-operational states 2 to 4, no link identification is possible and therefore it shall respond with MPH-DI to inform and align the link control FSM about this situation.

Table 12/G.965 – V5.2-interface layer 1 link FSM – AN (interface) and LE (interface)

State number	AN/LE1	AN/LE2	AN/LE3	AN/LE4	AN/LE5.1	AN/LE5.2
Condition	**Normal**	**Locally detected failure**	**Remotely detected failure**	**Internal failure**	**Link ID sending**	**Link ID received**
Signal sent to remote side	**Normal frames Sa7 = ONE**	**RAI Sa7 = ONE**	**Normal frames Sa7 = ONE**	**AIS**	**Normal frames Sa7 = ZERO**	**Normal frames Sa7 = ONE**
Normal frames, Sa7 = ONE	–	Start timer; 1	Start timer; 1	–	–	1
Loss of signal or loss of frame alignment	Start timer; MPH-EIa; 2	MPH-EIa; –	MPH-EIa; MPH-EIbr; 2	MPH-EIa; –	Start timer; MPH-EIa; 2	Start timer; MPH-EIa; 2
RAI	Start timer; MPH-EIb; 3	MPH-EIdr; MPH-EIb; 3	–	–	Start timer; MPH-EIb; 3	Start timer; MPH-EIb; 3
AIS	Start timer; MPH-EIc; 2	MPH-EIc; –	MPH-EIc; MPH-EIbr; 2	MPH-EIc; –	Start timer; MPH-EIc; 2	Start timer; MPH-EIc; 2
Internal failure	MPH-DI; MPH-EId; 4	MPH-DI; MPH-EId; 4	MPH-DI; MPH-EId; 4	–	MPH-DI; MPH-EId; 4	MPH-DI; MPH-EId; 4
Disappearance of internal failure	/	/	/	MPH-EIdr; 3	/	/
Expiry of persistence check timer	MPH-AI; –	MPH-DI; –	MPH-DI; –	–	/	MPH-AI; –
MPH-ID	5.1	MPH-DI; –	MPH-DI; –	MPH-DI; –	–	5.1
MPH-NOR	–	MPH-DI; –	MPH-DI; –	MPH-DI; –	1	/
Normal frames, Sa7 = ZERO	5.2	Start timer; 5.2	Start timer; 5.2	–	–	–
MPH-IDR	MPH-EIg; –	MPH-DI; –	MPH-DI; –	MPH-DI; –	/	MPH-IDI

Table 12/G.965 – V5.2-interface layer 1 link FSM – AN (interface) and LE (interface)

– No state change
/ Unexpected event, no state change
MPH-EI Error indication (the parameter "r" means recovery from a previously reported error condition)
NOTE 1 – The generation of AIS may not be possible in all internal failure conditions.
NOTE 2 – The persistence check timer shall be started upon reception of the appropriate event as indicated by "start timer". If, due to reception of another event another timer is started, a currently running timer is to be stopped and reset.
The values for the timers, which may be specific for each event, shall be pre-defined. The timer values for the AN shall be:
– greater for going into non-operational condition than for the LE; and
– smaller for going into operational condition than for the LE.

When the layer 1 link FSM receives MPH-ID being in state AN/LE1 or AN/LE5.2, it goes to state AN/LE5.1 and sets the Sa7 bit in the sending bitstream to ZERO. When in state AN/LE5.1, on receipt of MPH-NOR, the FSM shall return to state AN/LE1 (i.e. Sa7 bit set to one). It returns to the appropriate state on detection of a failure condition and shall send the relevant signal according to the current layer 1 link interface condition.

16.1.4 Requirements and procedures for the additional functions

The CRC-4 multiframe alignment shall be established in states AN/LE1, AN/LE3 and AN/LE5.x and detected CRC blocks in error shall be reported to both the remote end by setting bit E to ZERO and to the system management by MPH-EIe. The system management may process the CRC error information according to pre-defined thresholds and may react towards the operation system. This is outside the scope of the interface FSM. A persistent error rate or worse than 1 in 10^{-3} shall be considered as non-operational.

CRC-4 error information may be received in states AN/LE1, AN/LE3, AN/LE4 and AN/LE5.x. E-bits set to ZERO, which may be received in state AN/LE1, shall be reported to the system management by MPH-EIf. The system management may process the CRC error information according to pre-defined thresholds and may react towards the operation system. This is outside the scope of the interface FSM. A persistent error rate of worse than 1 in 10^{-3} shall be considered as non-operational.

If the interface FSM receives the primitive MPH-Stop from the system management, the FSM continues to operate but shall not send any MPH-EI to the system management. On receipt of the primitive MPH-Proceed, it shall send the actual status (last generated MPH-EI to the system management and any further one).

16.2 Link control requirements and procedures

16.2.1 The link blocking and unblocking

There are two different types of blocking requests from AN to LE: deferred and non-deferred blocking request.

The AN may request a non-deferred blocking of a link but the LE, as master of the service, decides. If the link carries one or more active C-channels, the LE system management shall use the Protection protocol to switch the logical C-channel(s) onto standby physical C-channels. Then the

LE shall release all switched connections on that link as appropriate to the service but shall re-establish the semi-permanent and AN-reserved connections onto other links within the same V5.2-interface and shall then send "block indication" to the AN. If however protection of logical C-channels is not possible, the LE shall reject the request by sending "unblock indication" to the AN.

The AN may also request a deferred blocking of a link. In this case the LE shall disable all non-assigned bearer channels in this link from future assignment and shall wait until all bearer channels (assigned for on-demand services) become unassigned. After that the LE shall continue with protection of logical C-channels and semi-permanent and AN-reserved connections, if required, and shall send "block indication" to the AN. If however protection of logical C-channels is not possible, the LE shall reject the request by sending "unblock indication" to the AN.

If the non-deferred blocking request was rejected by the LE but the link blocking is urgently necessary from the AN point of view, the AN can block a single link of the V5.2-interface immediately. It should be noted that this forced blocking by AN of a single link can move the whole V5.2-interface into a non-operational state, if it effects the primary or secondary link.

In case of AN internal failures which result in the link not being available any longer the AN may apply immediate blocking of the link. In parallel, protection of any affected C-channels shall be initiated if available.

The link status indication of a single link of a V5.2-interface is based on the defined split of responsibilities between AN and LE.

Tests which interfere with any service via this link, shall only be performed when the link is in one of the non-operational states, either due to failure or on request to and permission by the LE. This requires two main states, relevant to the V5.2-interface protocol, at both sides:

– operational; and
– non-operational.

16.2.2 The link identification

This procedure is used in order to check the link identification for a specific link. If the other end can accept this request (notably, if it is not already performing a similar procedure at that time), then it sends a specific physical signal (bit Sa7 in TS 0 set to zero, while otherwise it shall be set to one) on the link with the address indicated in the message. This allows the requesting end to check that there is no mismatch between the ends of this link.

The procedure is symmetrical and may be applied from either end of the 2048 kbit/s link. Link identification initiated from LE has priority over AN initiated procedure in case of collision of requests from AN and LE.

When the L1 interface FSM indicates to the link control FSM by MPH-AI that it has entered the normal state, the system management may request the link identification procedure to be performed. This procedure is applicable to all links, including the primary and secondary link.

NOTE – The link identification procedure may also be performed by the system management on a timed basis. Link identification may be applied after re-provisioning. At system startup, system management or the OS may decide not to apply the link identification procedure.

The principle of the link identification procedure is provided in Figure 12.

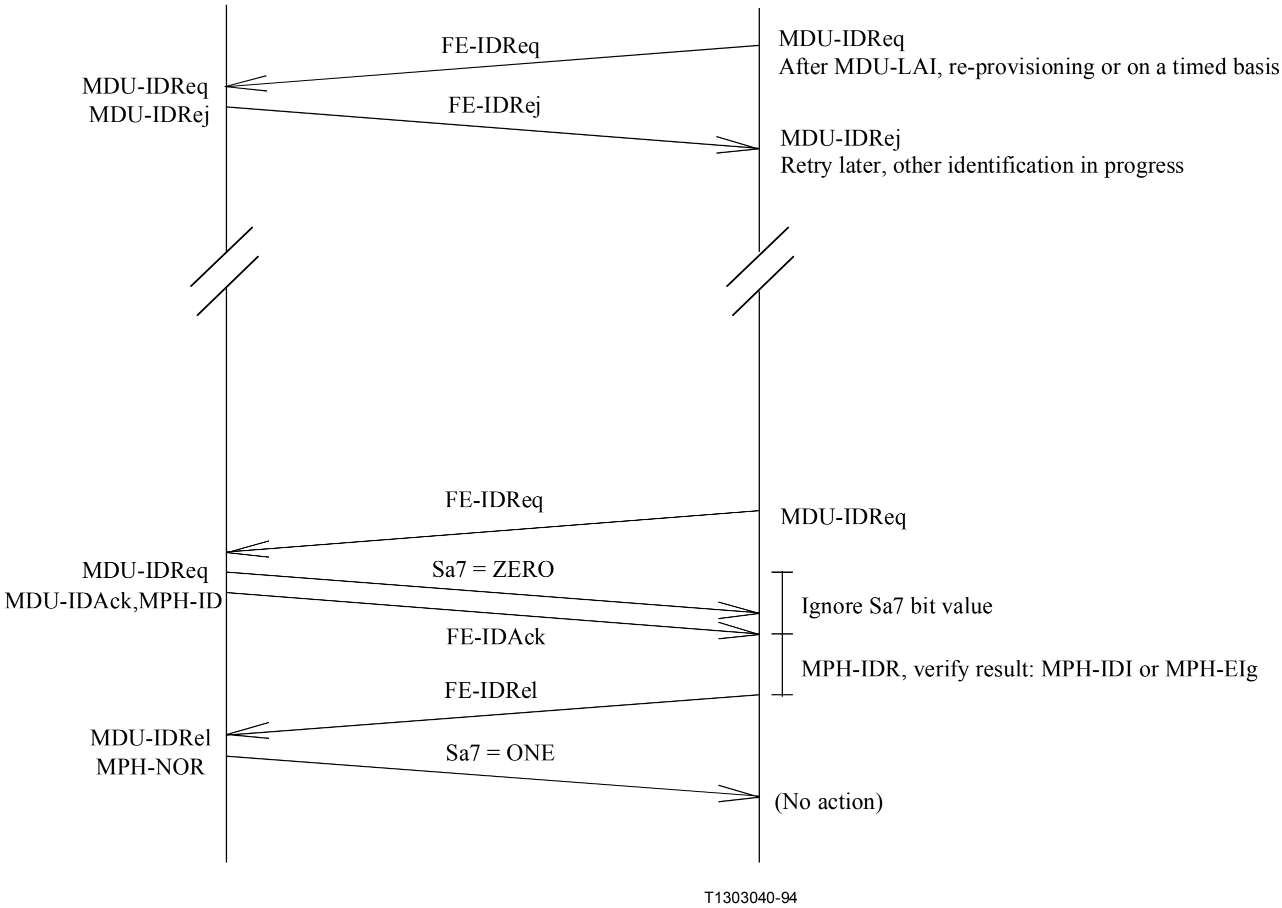


Figure 12/G.965 – Link identification functional procedure, arrow diagram

16.2.3 Events and function elements relevant for the control of the link state machines

Tables 13, 14 and 15 give the set of FEs and management primitives relevant for the link control procedures of the V5.2-interface and the system management as well as the management data units primitives towards the layer 1 link FSM and the system management function in AN or LE.

Table 13/G.965 – Set of link control function elements

FE	Name	AN ⇔ LE	Description
FE-IDReq	Link identification	↔	Request
FE-IDAck	Link identification	↔	Acknowledge
FE-IDRel	Link identification	↔	Release request
FE-IDRej	Link identification	↔	Reject indication
FE301	Link unblock	←	Request or indication
FE302	Link unblock	→	Request or indication
FE303	Link block	←	Indication
FE304	Link block	→	Indication
FE305	Link block	→	Request, deferred
FE306	Link block	→	Request, non-deferred

Table 14/G.965 – Set of primitives and data units for link control in the LE

Primitive	L1 FSM ⇔ Link control	Link control ⇔ System management	Description
MPH-AI	→		Layer 1 link is operational
MDU-AI		→	Link is operational
MPH-DI	→		Layer 1 link is not operational
MDU-DI		→	Link is not operational
MDU-LAI		→	Link identification required
MDU-IDReq		↔	Link identification request
MDU-IDAck		←	Send link identification acknowledge
MPH-ID	←		Send link identification
MPH-IDR	←		Send link identification information
MPH-IDI	→		Link identification indication
MPH-NOR	←		Remove link identification
MDU-IDRel		→	Link identification release indication
MDU-IDRej		↔	Link identification request rejected
MPH-EIg	→		Link identification failure
MDU-EIg		→	Link identification failure indication
MPH-EIa-f			Error indications from layer 1
MDU-LUBR		↔	Link unblock request
MDU-LUBI			Link unblock indication
MDU-LBI		→	Link block indication
MDU-LBR		↔	Link block request, deferred
MDU-LBRN		→	Link block request, non-deferred

16.2.4 Link control FSM, AN (link) and LE (link)

The primitives, data units, FEs and the state tables are given for the definition of the functional behaviour and cooperation between the various functional blocks. There shall be no restriction for the implementation of these functions as long as the implementation is in conformance with the functionality defined in this Recommendation over the V5.2-interface, the layer 1 link FSM and the system management.

16.2.4.1 Description of the states

The link control FSM in the AN and in the LE can both be regarded as being constructed from two fundamental states: operational and non-operational.

The non-operational state is divided into 5 substates:

– layer 1 link failure (0.1);

– layer 1 link failure and link blocked (0.2);

– link blocked (1.0);

– local link unblocked (1.1); and

– remote link unblocked (1.2).

Table 15/G.965 – Set of link control primitives and data units in the AN

Primitive	L1 FSM ⇔ Link control	Link control ⇔ System management	Description
MPH-AI	→		Layer 1 link is operational
MDU-AI		→	Link is operational
MPH-DI	→		Layer 1 link is not operational
MDU-DI		→	Link is not operational
MDU-LAI		→	Link identification required
MDU-IDReq		↔	Link identification request
MDU-IDAck		←	Send link identification acknowledge
MPH-ID	←		Send link identification
MPH-IDR	←		Send link identification information
MPH-IDI	→		Link identification indication
MPH-NOR	←		Remove link identification
MDU-IDRel		→	Link identification release indication
MDU-IDRej		↔	Link identification request rejected
MPH-EIg	→		Link identification failure
MDU-EIg		→	Link identification failure indication
MPH-EIa-f	→		Error indications from layer 1
MDU-LUBR		↔	Link unblock request
MDU-LUBI		→	Link unblock indication
MDU-LBI		↔	Link block indication
MDU-LBR		←	Link block request, deferred
MDU-LBRN		←	Link block request, non-deferred

This subdivision simplifies the coordination of both link control FSMs in the unblocking sequence and ensures that unblocking shall be acknowledged by both sides before going into the operational state.

The data units MDU-LUBI and MDU-LBI shall be used by the both link control FSMs to notify their system management of a transition into and out of the operational state respectively.

The mechanism for link unblocking is acknowledged, as is the mechanism for link blocking request for the AN side. The mechanism for immediate blocking is unacknowledged.

The operational state is divided into three substates:

– link operational (2.0);
– remote link identification (2.1); and
– local link identification (2.2).

All three substates are considered from the link control point of view as operational. It is the responsibility of the relevant system management to initiate any consequent action required according to the system management link status, e.g. to the protection protocol management and the bearer channel resource management.

16.2.4.2 Definition of link control states and general coordination requirements

The link control FSMs reflect the AN and LE view of the functional state of a single link of the V5.2-interface only.

In order to coordinate layer 1 link in failure condition and link blocked condition substate 0.2 has been inserted for the combined link status condition. If during layer 1 link failure a blocking is requested by system management this shall be indicated to the remote entity and the substate 0.2 shall be entered. On recovery of the layer 1, link the link control FSM shall go to the blocked state sending MDU-LBI to trigger system management to coordinate unblocking if desired. This procedure allows as well coordinated recovery from system management misalignment, e.g. loss of control data link due to failure of layer 1 link or loss of system management status data after restart.

A link unblocking request from either side while in layer 1 link failure condition will be considered as a system management misalignment and the link control FSM shall go to substate 0.2 to trigger coordinated unblocking after layer 1 link recovery. The same action is recommended when FE-IDReq is received while the FSM is in layer 1 link failure condition.

16.2.4.2.1 Link control FSM – AN (AN_Link)

Non-operational (AN0.x and AN1.x): The link is forced into the layer 1 link failure or link blocked state. Therefore, physical C-channels on this link shall not be used to carry a logical C-channel or act as a standby. All time slots of this link are not available for call control as bearer channels. A link identification request will be rejected.

Link failure (AN0.1): Layer 1 link FSM has indicated persistent loss of layer 1 capability by MPH-DI.

Link failure and blocked (AN0.2): Layer 1 link FSM has indicated persistent loss of layer 1 capability by MPH-DI while the link was blocked or due to actions requested from system management or the LE side which can be regarded as misalignment of the link control FSMs requiring coordination.

Link blocked (AN1.0): The link is in the non-operational state and neither side has initiated unblocking.

Local link unblock (AN1.1): The AN has initiated unblocking (by sending FE302) and is awaiting confirmation from the LE.

Remote link unblock (AN1.2): The LE has initiated unblocking (by sending FE301) and is awaiting confirmation from the AN.

NOTE – States AN1.1 and AN1.2 provide a mechanism for the synchronized unblocking of links. The AN may remain in these states for an undetermined period of time.

Link Operational (AN2.0): The link shall be considered ready from the layer 1 and link control point of view to support the provisioned capabilities. It may be required to perform the link identification procedure to verify the link continuity.

Remote link identification (AN2.1): The LE has initiated link identification and on confirmation by the system management layer 1 link FSM has been requested to set the link identification bit Sa7 to ZERO. The AN link control is waiting for the link identification release function element.

Local link identification (AN2.2): The AN system management has initiated link identification and is waiting either for the FE-IDAck from the LE or, if already received, for the link identification indication or link identification failure, in response to MPH-IDR, which will then result in the appropriate information to system management and release of link identification.

16.2.4.2.2 Link control FSM – LE (LE_Link)

Non-operational (LE0.x and LE1.x): The link is forced into the layer 1 link failure or link blocked state. Therefore, physical C-channels on this link shall not be used to carry a logical C-channel or act as a standby. All time slots of this link are not available for call control as bearer channels. A link identification request will be rejected.

Link failure (LE0.1): Layer 1 link FSM has indicated persistent loss of layer 1 capability by MPH-DI.

Link failure and blocked (LE0.2): Layer 1 link FSM has indicated persistent loss of layer 1 capability by MPH-DI while the link was blocked or due to actions requested from system management or the AN side which can be regarded as misalignment of the link control FSMs requiring coordination.

Link blocked (LE1.0): The link is in the non-operational state and neither side has initiated unblocking.

Local link unblock (LE1.1): The AN has initiated unblocking (by sending FE301) and is awaiting confirmation from the LE.

Remote link unblock (LE1.2): The AN has initiated unblocking (by sending FE302) and is awaiting confirmation from the LE.

NOTE – States LE1.1 and LE1.2 provide a mechanism for the synchronized unblocking of links. The LE may remain in these states for an undetermined period of time.

Link Operational (LE2.0): The link shall be considered ready from the layer 1 and link control point of view to support the provisioned capabilities. It may be required to perform the link identification procedure to verify the link continuity. This is the responsibility of the system management.

Remote link identification (LE2.1): The AN has initiated link identification and on confirmation by the system management layer 1 link FSM has been requested to set the link identification bit Sa7 to ZERO. The LE link control is waiting for the link identification release function element.

Local link identification (LE2.2): The LE system management has initiated link identification and is waiting either for the FE-IDAck from the AN or, if already received, for the link identification indication or link identification failure, in response to MPH-IDR, which will then result in the appropriate information to system management and release of link identification.

16.2.4.3 Principles and procedures

16.2.4.3.1 General

The AN may request blocking of a specific link: block request (deferred or non-deferred, both with Link ID information element). The LE shall grant this request (once it can do so) and sends a block indication (with Link ID information element). The AN may also request to unblock a specific (blocked) link: unblock request (with Link ID information element). The LE either sends an unblock indication (with Link ID information element) or a block indication (with Link ID information element). The procedure is symmetrical and therefore valid for the LE as well.

If the non-deferred blocking request is not successful but the link blocking is urgently necessary, the AN can block a single link of the V5.2-interface immediately. The immediate blocking of a single link forced by AN can move the whole V5.2-interface into a non-operational state.

In case of AN internal failures which result in the link not being available any longer the AN may apply immediate blocking of the link. In parallel, protection of any affected C-channels shall be initiated if available.

All messages carrying a link control function element of a specific link shall contain the Link ID information element.

The following subclauses describe the mechanism implemented in the FSMs in AN and LE for single links of a V5.2-interface, which are presented in the relevant State Transition Tables.

This procedure shall apply even in the case of the single 2048 kbit/s V5.2 interface.

The following mechanisms are described:

– link blocking;
– link blocking request from the AN (deferred or non-deferred);
– coordinated unblocking;
– link identification procedure.

16.2.4.3.2 Link blocking

A single link of a V5.2-interface can be blocked from both sides. The LE releases any switched connection on this link as appropriate to the service but re-establishes semi-permanent and pre-connected connections onto other links within the same V5.2-interface. LE system management shall use the protection protocol to move logical C-channels, if possible and necessary.

When LE system management issues MDU-LBI, the FSM sends FE303 (link block indication) to the AN and goes to the link blocked state LE1.0.

When AN system management issues MDU-LBI, the FSM sends FE304 (Link block indication) to the LE and goes to the Link Blocked state AN1.0.

16.2.4.3.3 Link blocking request

The AN may request blocking of a specific link: link block request deferred or non-deferred. The LE shall grant this request (once it can do so and after completion of the consequent actions) and shall send a link block indication.

When AN system management issues MDU-LBR or MDU-LBRN and the link is in the operational state, the AN link FSM shall send FE305 or FE306 as relevant. This request shall be passed by the LE link control FSM to the LE system management with MDU-LBR or MDU-LBRN.

16.2.4.3.4 Coordinated link unblocking

Unblocking of a single link of a V5.2-interface needs to be coordinated at both sides. A link unblock request requires confirmation from the other side before the link shall be put into operation. To guarantee this coordination there are two separate link unblock states (Local & Remote Link Unblock) in both link control FSMs. This procedure is fully symmetrical between AN and LE.

If the LE system management wants to unblock the link, it issues MDU-LUBR, the link control FSM sends FE301 (Unblock request) and goes to "Local link unblock" state (LE1.1). The AN on receipt of FE301 goes to "Remote link unblock" (AN1.2) and sends MDU-LUBR to its system management. If the AN system management agrees, it responds with MDU-LUBR (link unblock request), the AN link control FSM shall send FE302 to the LE, send MDU-LUBI (link unblock indication) to system management and goes "Link operational" state (AN2.0). For the LE link control FSM being in "Local link unblock" and receiving this FE302, the link control FSM goes to "Link Operational" (LE2.0) and issues MDU-LUBI to its system management.

The AN system management may as well take the initiative, for which the same procedure applies. If system management does not agree, it shall respond with MDU-LBI.

The AN system management has to execute a Link block/unblock sequence if it does not receive MPH-LBI or MPH-LUBI (link unblock indication) within 5 minutes.

The LE system management has to re-issue MDU-LUBR if it does not receive MPH-LBI or MPH-LUBI within 5 minutes. This is required to resolve a link state mismatch that e.g. may happen if a link is added to the LE provisioning data of an operational interface after the AN has already tried to unblock that link (stays in state AN1.1, local link unblock).

For AN and LE link control FSM, when in "Remote link unblock" state and receiving FE304 or FE303 respectively, the state shall be reset to "Link blocked", and a MDU-LBI sent to system management. This undoes a previous Link Unblock Request from the other side.

In the case of collision of FE301/2 and FE303/4 this may result in an uncoordinated unblocking afterwards. This can be detected by system management by identification of the sequence of primitives. It is recommended that in this case the system management applies the verification procedure after unblocking to ensure coordination of both sides. Uncoordinated unblocking may result in rejections in the BCC allocation procedure or protection switching procedure or the inefficient use of resources within the interface.

16.2.4.3.5 Link identification

Link identification may be required after link layer 1 failure recovery indicated by MPH-AI from the layer 1 link FSM and indicated to the system management by MDU-LAI. It is for the system management to invoke the link identification procedure or not. There may be other triggers within the system management to request this procedure. There shall be only one request for the link identification procedure from the system management at a time for all V5-interfaces of AN or LE. It shall however be possible to perform link identification simultaneously from AN to LE and from LE to AN, as long as no collision occurs on a link as described below.

If the primary or the secondary link was affected by a layer 1 failure, the system management may not invoke this procedure if the link control data link is not (yet) in the operational state indicated by MDL-establish_indication or MDL-establish_confirmation. The establishment of the link control link has, under all circumstances, priority because the link identification procedure is based on the proper functioning of the link control data link.

In order to avoid internal blocking situations, the collision of link identification invoked from both sides at the same point in time for the same link is resolved by priority to the request from the LE which overrides the AN request if not yet acknowledged by the LE. The following description of the procedure is, except for the collision resolution, symmetrical and therefore described as performed from one side only.

Link identification can successfully be started only when the link control FSM is in state 2.0 by MDU-IDReq. In all other cases the response to the system management gives a direct or indirect rejection with the information about the link control status. On receipt of MDU-IDReq, the FSM sends FE-IDReq to the remote side, goes to state 2.2 and waits for the acknowledgement of the request, which is indicated by FE-IDAck. On receipt of FE-IDAck it is implied that the remote link control FSM has requested the relevant layer 1 link FSM to set the Sa7 bit to ZERO (by MPH-ID) which is detected then by the local layer 1 link FSM. This information is not passed directly to the link control FSM to avoid overlapping requests for the link identification.

The remote side receiving FE-IDReq when being in state 2.0 it informs the system management by MDU-IDReq. If the system management can comply to this request it responds with MDU-IDAck and the link control FSM sends FE-IDAck and goes to state 2.1.

On receipt of FE-IDAck the link control FSM requests the link identification information by issuing MPH-IDR to the layer 1 link FSM which then returns the relevant information, either MPH-IDI or MPH-EIg, which is present at that point in time at the layer 1 link FSM. The link control FSM informs the system management by the appropriate MDU, either MDU-AI, which is the successful link identification indication, or by MDU-EIg or MDU-DI, if the layer 1 link FSM is in failure condition at this point in time, which are the unsuccessful link identification indications. Irrespective of the information sent to the system management, the link control FSM will request the release of the link identification at the remote side and goes to state 2.0. This is done by FE-IDRel, which causes the resetting of Sa7 bit to ONE (by MPH-NOR from the remote link control FSM to the layer 1 link FSM).

If the remote system management cannot comply to the request for the link identification it issues MDU-IDRej to the link control FSM, which shall reject the request with FE-IDRej. This causes subsequent information from the local link control FSM to the system management through MDU-IDRej.

It is the responsibility of the system management to take the appropriate action on receipt of any information from the link control FSM, e.g. MDU-IDRej, MDU-IDRel, MDU-AI, MDU-EIg, MDU-DI, as a result of a link identification procedure the system management has requested from the link control FSM.

16.2.4.4 Link control FSM at the AN

Table 16 gives the link control FSM of the AN.

The AN link control FSM provides a mechanism which allows the system management of the AN to verify that the link control FSM is in the link operational state, without having to go through the sequence of blocking and unblocking. This mechanism is internal to the AN. To do so the AN system management issues MDU-LUBR and receives the information whether the link control FSM is in a non-operational state.

16.2.4.5 Link control FSM at the LE

Table 17 gives the link control FSM of the LE.

The LE link control FSM provides a mechanism which allows the system management of the LE to verify that the link control FSM is in the link operational state by issuing MDU-LUBR, without having to go through the sequence of blocking and unblocking.

Unlike the corresponding situation for the AN, this mechanism is not internal to the LE and requires the cooperation of the AN link control FSM, and confirms the alignment of both link control FSMs when receiving MDU-LUBI.

The asymmetry here reflects the responsibility of the LE for supporting the service.

16.3 Link control protocol

16.3.1 Link control protocol message definition and content

The format of the link control protocol messages shall correspond to the generic message structure defined in clause 13.

The complete set of messages for the link control protocol is given in Table 18. The following subclauses give the detailed message structure for each of the messages.

16.3.1.1 LINK CONTROL message

This message is sent by the AN or the LE to convey information required for control functions for each individual 2048 kbit/s link (see Table 19).

Table 16/G.965 – AN link control FSM

State	AN0.1	AN0.2	AN1.0	AN1.1	AN1.2	AN2.0	AN2.1	AN2.2
State name / Event	Link failure	Link failure and blocked	Link blocked	Local link unblock	Remote link unblock	Link opera-tional	Remote link identifi-cation	Local link identifi-cation
MPH-AI	MDU-LAI; 2.0	MDU-LAI; MDU-LBI; 1.0	MDU-LAI; –	–	–	–	–	–
MPH-DI	–	–	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.1	MDU-DI; MPH-NOR; 0.1	MDU-DI; FE-IDRel; 0.1
MDU-IDReq	MDU-DI; –	MDU-DI; –	MDU-LBI; –	MDU-LBI; 1.0	MDU-LUBR; MDU-IDRej: –	FE-IDReq; 2.2	MDU-IDRej; –	–
FE-IDAck	/	/	/	/	/	/	/	MPH-IDR; –
MPH-IDI	/	/	/	/	/	/	/	MDU-AI; FE-IDRel; 2.0
MPH-Eig	/	/	/	/	/	/	/	FE-IDRel; MDU-EIg; 2.0
FE-IDReq	FE304; 0.2	FE304; –	FE304; –	FE-IDRej; –	FE-IDRej; –	MDU-IDReq; –	–	MDU-IDRej; MDU-IDReq; 2.0
MDU-IDAck	/	/	/	/	/	MPH-ID; FE-IDAck; 2.1	–	/
FE-IDRel	–	/	/	–	/	/	MDU-IDRel; MPH-NOR; 2.0	/
MDU-IDRej	/	/	/	/	/	FE-IDRej; –	FE-IDRej; MPH-NOR; 2.0	/
FE-IDRej	–	/	/	–	/	/	MDU-IDRej; –	MDU-IDRej; 2.0
FE301	FE304; 0.2	FE304; –	MDU-LUBR; 1.2	MDU-LUBI; 2.0	MDU-LUBR; –	FE302; MDU-LUBI; –	FE302; MDU-LUBI; MDU-IDRel; MPU-NOR; 2.0	FE302; MDU-IDRej; 2.0
FE303	0.2	–	–	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; MPH-NOR; 1.0	MDU-LBI; 1.0
MDU-LUBR	FE304; MDU-DI; 0.2	FE304; MDU-DI; –	FE302; 1.1	FE302; –	FE302; MDU-LUBI; 2.0	FE302; MDU-LUBI; –	FE-IDRej; MDU-LUBI; MPH-NOR; 2.0	FE-IDRel; MDU-LUBI; 2.0

Table 16/G.965 – AN link control FSM

State	AN0.1	AN0.2	AN1.0	AN1.1	AN1.2	AN2.0	AN2.1	AN2.2
Event \ State name	Link failure	Link failure and blocked	Link blocked	Local link unblock	Remote link unblock	Link opera-tional	Remote link identifi-cation	Local link identifi-cation
MDU-LBI	FE304; 0.2	FE304; –	FE304; –	FE304; 1.0	FE304; 1.0	FE304; 1.0	FE304; MPH-NOR; 1.0	FE304; 1.0
MDU-LBR	FE304; MDU-LBI; 0.2	FE304; MDU-LBI; –	FE304; MDU-LBI; –	FE304; MDU-LBI; 1.0	FE304; MDU-LBI; 1.0	FE305; –	FE305; –	FE305; –
MDU-LBRN	FE304; MDU-LBI; 0.2	FE304; MDU-LBI; –	FE304; MDU-LBI; –	FE304; MDU-LBI; 1.0	FE304; MDU-LBI; 1.0	FE306; –	FE306; –	FE306; –

– No state change

/ Unexpected event, no state change

NOTE 1 – The MPH-EIa-f shall be logged but the report of those events from the interface layer 1 FSM may be suppressed by use of MPH-EIstop and proceeded by use of MPH-EIproceed.

NOTE 2 – The first set of events (MPH-AI/DI) reflects the availability of the link layer 1.

NOTE 3 – The second set (MDU-IREQ ... LE-IDrej) is used for the link identification procedure.

NOTE 4 – The third set is used for the link blocking procedure.

Table 17/G.965 – LE link control FSM

State	LE0.1	LE0.2	LE1.0	LE1.1	LE1.2	LE2.0	LE2.1	LE2.2
Event \ State name	Link failure	Link failure and blocked	Link blocked	Local link unblock	Remote link unblock	Link opera-tional	Remote link identifi-cation	Local link identifica-tion
MPH-AI	MDU-LAI; 2.0	MDU-LAI; MDU-LBI; 1.0	MDU-LAI; –	–	–	–	–	–
MPH-DI	–	–	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.2	MDU-DI; 0.1	MDU-DI; MPH-NOR; 0.1	MDU-DI; FE-IDRel; 0.1
MDU-IDReq	MDU-DI; –	MDU-DI; –	MDU-LBI; –	MDU.LBI; 1.0	MDU-LUBR; MDU-IDRej; –	FE-IDReq; 2.2	MDU-IDRej; –	–
FE-IDAck	/	/	/	/	/	/	/	MPH-IDR; –
MPH-IDI	/	/	/	/	/	/	/	MDU-AI; FE-IDRel; 2.0
MPH-EIg	/	/	/	/	/	/	/	FE-IDRel; MDU-EIg; 2.0
FE-IDReq	FE303; 0.2	FE303; –	FE303; –	FE-IDRej; –	FE-IDRej; –	MDU-IDReq; –	–	FE-IDRej; –

Table 17/G.965 – LE link control FSM

State	LE0.1	LE0.2	LE1.0	LE1.1	LE1.2	LE2.0	LE2.1	LE2.2
State name / Event	**Link failure**	**Link failure and blocked**	**Link blocked**	**Local link unblock**	**Remote link unblock**	**Link opera-tional**	**Remote link identifi-cation**	**Local link identifica-tion**
MDU-IDAck	/	/	/	/	/	MPH-ID; FE-IDAck; 2.1	–	/
FE-IDRel	–	/	–	–	/	/	MDU-IDRel; MPH-NOR; 2.0	/
MDU-IDRej	/	/	/	/	/	FE-IDRej; –	FE-IDRej; MPH-NOR; 2.0	/
FE-IDRej	–	/	–	–	/	/	/	MDU-IDRej; 2.0
MDU-LUBR (Note 5)	MDU-DI; FE303; 0.2	MDU-DI; FE303; –	FE301; 1.1	FE301; –	FE301; MDU-LUBI; 2.0	FE301; –	FE301; MPH-NOR; 2.0	FE301; 2.0
MDU-LBI	FE303; 0.2	FE303; –	FE303; –	FE303; 1.0	FE303; 1.0	FE303; 1.0	FE303; MPH-NOR; 1.0	FE303; 1.0
FE302 (Note 5)	FE303; 0.2	FE303; –	MDU-LUBR; 1.2	MDU-LUBI; 2.0	MDU-LUBR; –	MDU-LUBI; –	MDU-IDRel; MDU-LUBI; MPH-NOR; 2.0	MDU-IDRej; MDU-LUBI; 2.0
FE304 (Note 5)	0.2	–	–	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; 1.0	MDU-LBI; MPH-NOR; 1.0	MDU-LBI; 1.0
FE305	FE303; 0.2	FE303; –	FE303; –	FE303; MDU-LBI; 1.0	FE303; MDU-LBI; 1.0	MDU-LBR; –	MDU-LBR; –	MDU-LBR; –
FE306	FE303; 0.2	FE303; –	FE303; –	FE303; MDU-LBI; 1.0	FE303; MDU-LBI; 1.0	MDU-LBRN; –	MDU-LBRN; –	MDU-LBRN; –

– No state change

/ Unexpected event, no state change

NOTE 1 – The MPH-EIa-f shall be logged but the report of those events from the interface layer 1 FSM may be suppressed by use of MPH-EIstop and proceeded by use of MPH-EIproceed.

NOTE 2 – The first set of event (MPH-AI) reflects the availability of the link layer 1.

NOTE 3 – The second set of event (MDU-IDreq – FE-IDrej) is used for the link identification procedure.

NOTE 4 – The third set of events is used for the link blocking procedure.

NOTE 5 – Notification to system management about L1 fault. Notification sent to system management about layer 1 fault when in state LE0.1.

Table 18/G.965 – Messages for V5.2-link control protocol

Coding within the message type information element							Message types	Reference
7	6	5	4	3	2	1		
0	1	1	0	0	0	0	LINK CONTROL	16.3.1.1
0	1	1	0	0	0	1	LINK CONTROL ACK	16.3.1.2

Table 19/G.965 – LINK CONTROL message content

Message Type: LINK CONTROL

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	Both	M	1
Layer 3 Address	16.3.2.1	Both	M	2
Message Type	13.2.3	Both	M	1
Link Control Function	16.3.2.2	Both	M	3

16.3.1.2 LINK CONTROL ACK message

This message is sent by the AN or the LE as an immediate acknowledgement of the receipt of a LINK CONTROL message (see Table 20).

Table 20/G.965 – LINK CONTROL ACK message content

Message Type: LINK CONTROL ACK

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	Both	M	1
Layer 3 Address	16.3.2.1	Both	M	2
Message Type	13.2.3	Both	M	1
Link Control Function	16.3.2.2	Both	M	3

16.3.2 Link control protocol information element definition, structure and coding

The link control protocol information elements are defined in the following subclauses and summarized in Table 21, which also gives the coding of the information element identifier bits. For each of the information elements the coding of their different fields is provided.

Table 21/G.965 – Information element identifier coding

Bits								Information element	Reference
8	7	6	5	4	3	2	1		
0	–	–	–	–	–	–	–	VARIABLE LENGTH	
0	0	1	1	0	0	0	0	Link control function	16.3.2.2

16.3.2.1 Layer 3 address information element

The purpose of the layer 3 address information element is to identify the 2048 kbit/s link to which the link control message refers.

The L3 address information element is the second part of every message and is coded as shown in Figure 13.

8	7	6	5	4	3	2	1	Octets
0	0	0	0	0	0	0	0	1
L3 address field (low)								2

Figure 13/G.965 – The layer 3 address information element for 2048 kbit/s link identification

The layer 3 address information element is coded in binary.

For a particular V5 2048 kbit/s link, the L3 address field (low) of the L3 address information element shall have the same value as the V5 2048 kbit/s link identifier field of the V5-time slot identification information element which is used for the BCC protocol.

16.3.2.2 Link control function information element

This information element identifies the link control function to be conveyed by the message.

The structure of the link control function information element shall be as indicated by Figure 14.

8	7	6	5	4	3	2	1	Octets
0	0	1	1	0	0	0	0	1
Length of link control function content								2
ext. 1	Link control function							3

Figure 14/G.965 – Link control function information element

The coding of the content of this information element shall be as specified in Table 22.

Table 22/G.965 – Coding of link control function

Bits (octet 3)							Link control function
7	6	5	4	3	2	1	
0	0	0	0	0	0	0	FE-IDReq
0	0	0	0	0	0	1	FE-IDAck
0	0	0	0	0	1	0	FE-IDRel
0	0	0	0	0	1	1	FE-IDRej
0	0	0	0	1	0	0	FE301/302 (link unblock)
0	0	0	0	1	0	1	FE303/304 (link block)
0	0	0	0	1	1	0	FE305 (deffered link block request)
0	0	0	0	1	1	1	FE306 (non-deffered link block request)
NOTE – All other values are reserved.							

16.3.3 Definitions of the link control protocol states

OUT OF SERVICE

This state shall be entered when the system is started or MDU-stop_traffic is received from the system management.

IN SERVICE

This state shall be entered when the control protocol entity is in the OUT OF SERVICE state and receives a MDU-start_traffic from the system management.

AWAIT LINK CONTROL ACK

This state shall be entered when a LINK CONTROL message has been sent to the LINK CONTROL-DL.

16.3.4 Link control protocol procedure

16.3.4.1 General

This clause specifies the procedures for the link control protocol. The link control protocol is symmetrical, i.e. that the procedures apply to both the AN and the LE side of the V5.2-interface.

A link-related link control protocol entity exists for each 2048 kbit/s layer 1 link.

In addition to the above procedures, each message received by a link control protocol entity shall pass the error handling procedures specified in 16.3.5 before being further processed.

The description of the procedure is for a single event (FE or MDU-CTRL) only to be handled at the same point in time. There shall be a memory per link control protocol entity in the AN and LE to store further events to be transmitted in the order received from the FSM. The next event shall be transmitted when the relevant link control protocol FSM has entered state 1.

Each link control protocol message contains a layer 3 address to identify the particular layer 1 link control protocol entity.

Link control protocol messages shall be sent to the data link using a DL-Data-Request primitive; the data link service is specified in clause 10.

16.3.4.2 Start traffic indication

16.3.4.2.1 Normal operation

If a link control layer 3 protocol entity receives in the OUT OF SERVICE state a MDU-start_traffic from the system management entity, the IN SERVICE state shall be entered.

16.3.4.2.2 Exceptional procedures

If a link control layer 3 protocol entity receives in the OUT OF SERVICE state any LINK CONTROL or any FE, a MDU-error-indication shall be generated. No state change occurs.

16.3.4.3 Stop traffic indication

16.3.4.3.1 Normal operation

If a link control layer 3 protocol entity receives in the IN SERVICE or the AWAIT LINK CONTROL ACK state a MDU-stop_traffic from the system management entity, the OUT OF SERVICE state shall be entered.

16.3.4.3.2 Exceptional procedures

None.

16.3.4.4 Link control layer 3 protocol entity procedure

When the link control layer 3 protocol entity is in the "in service" state and receives a LINK CONTROL message, a LINK CONTROL ACK message shall be sent and a FE primitive containing the link control function and the L3 address shall be sent to the system management entity.

When the link control layer 3 protocol entity is in the "in service" state and receives from the link control management entity a FE primitive, a LINK CONTROL message containing the link control function and the L3 address shall be sent, Timer LCT01 shall be started and the state "await link control ack" shall be entered.

If a LINK CONTROL message is received in the "await link control ack" state, a LINK CONTROL ACK message shall be sent and a FE primitive containing the link control function and the layer 3 address shall be sent to the link control management entity.

Upon reception of a LINK CONTROL ACK message in the "await link control ack" state, Timer LCT01 shall be stopped and the "in service" state shall be entered.

If a FE primitive is received from the link control management entity in the "await link control ack" state, the FE primitive shall be saved.

If Timer LCT01 expires the first time in the "await link control ack" state, the LINK CONTROL message shall be retransmitted and Timer LCT01 shall be restarted. If Timer LCT01 expires the second time in the "await link control ack" state, a MDU-link_control (error indication) primitive shall be sent to the system management entity and the "in service" state shall be entered.

16.3.5 Handling of error conditions

Before acting upon a message, the receiving entity, either the AN V5-link control protocol entity or the LE V5-link control protocol entity, shall perform the procedures specified in this clause.

As a general rule, all messages shall contain, at least: the Protocol discriminator, the L3 address and the message type information elements. These information elements, acting as a header for all link control protocol messages, are specified in 13.2. When receiving a message having less than

4 octets, the receiving link control protocol entity in the AN or LE shall issue a MDU-link_control (protocol_error_indication) primitive to the system management and ignore the message.

Each receipt of a link control protocol message shall activate the checks described in clauses 16.3.5.1 to 16.3.5.7 by order of precedence. No state change occurs during these checks.

The error handling procedures in the AN and in the LE are symmetrical.

After the message has been checked using the error handling procedures following and if the message is not to be ignored, then link control protocol procedures (see 16.3.4) shall follow.

NOTE – Within this clause, the term "ignore the message" means to leave the message contents unchanged.

16.3.5.1 Protocol discriminator error

When a message is received in a V5-link control protocol entity with a protocol discriminator coded different to the specification of the protocol discriminator in 13.2.1, the V5-link control protocol entity shall issue a MDU-link_control (protocol_error_indication) primitive to the system management and ignore the message.

16.3.5.2 Layer 3 address error

If the layer 3 address is:

a) not coded as specified in 16.3.2.1; or

b) the value is not recognized or does not correspond to an existing V5 2048 kbit/s link, then:
   - the V5-link control protocol entity shall issue a MDU-link_control (protocol_error_indication) primitive to the system management and ignore the message.

16.3.5.3 Message type error

Whenever an unrecognized message is received, the V5-link control protocol entity shall issue a MDU-link_control (protocol_error_indication) primitive to the system management and ignore the message.

16.3.5.4 Repeated information elements

If a mandatory information element is repeated in a message, the receiving V5-link control protocol entity shall issue a MDU-link_control (protocol_error_indication) primitive to the system management and ignore the message.

16.3.5.5 Mandatory information element missing

When a message is received with a mandatory information element missing, the V5-link control protocol entity shall issue a MDU-link_control (protocol_error_indication) primitive to the system management and ignore the message.

16.3.5.6 Unrecognized information element

When a message is received with one or more information elements unrecognized, the V5-link control protocol entity shall remove all the unrecognized information elements and continue with the processing of the message; it shall also issue a MDU-link_control (protocol_error_indication) primitive to the system management.

For the purpose of the error handling procedures, unrecognized information elements shall be those that are not defined within this Recommendation.

16.3.5.7 Content error of mandatory information elements

When a message is received with a mandatory information element having a content error either:

a) the length does not conform to the length specified in 16.3.1; or

b) the content is not known, then:

   – the V5-link control protocol entity shall issue a MDU-link_control (protocol_error_indication) primitive to the system management and ignore the message.

NOTE – For the purpose of the error handling procedures, information element content errors are codepoints included within a particular information element that are not defined within this Recommendation.

16.3.6 Timers for the link control protocol

The timers for the link control protocol in the AN and the LE are specified in Table 23. The timer tolerances shall be ±10%.

Table 23/G.965 – Timers for the link control protocol

Timer number	Timeout value	State	Cause for start	Normal stop
LCT01	1 s	AN1(CTRL link) LE1(CTRL link)	LINK CONTROL message sent	LINK CONTROL ACK message received

16.3.7 AN and LE side layer 3 protocol entity state tables

Table 24 defines the state transition table of the link control layer 3 protocol entity for the AN side of the V5.2-interface.

Table 25 defines the state transition table of the link control layer 3 protocol entity for the LE side of the V5.2-interface.

17 BCC protocol elements and procedures

17.1 General

The V5.2-BCC protocol provides the means for the LE to request the AN to establish and release connections between specified AN user ports and specified V5.2-interface time slots. It enables V5.2-interface bearer channels to be allocated or de-allocated by independent processes (on a per call, preconnected or semi-permanent basis). There may be more than one process active at any one time for a given user port.

Table 24/G.965 – Link control L3 protocol entity state transition table – AN

State / Event	AN0 OUT OF SERVICE	AN1 IN SERVICE	AN2 AWAIT LINK CONTROL ACK
MDU-start_traffic	AN1	–	–
MDU-stop_traffic	–	Stop LCT01; AN0	Stop LCT01; AN0
FE or saved FE	Send MDU-link_control (error indication); –	Send LINK CONTROL; Start LCT01; AN2	Save new received FE; –
LINK CONTROL	Send MDU-link_control (error indication); –	Send FE; Send LINK CONTROL ACK; –	Send FE; Send LINK CONTROL ACK; –
LINK CONTROL ACK	Send MDU-link_control (error indication); –	/	Stop LCT01; AN1
First expiry LCT01	/	/	Repeat LINK CONTROL; Start LCT01; –
Second expiry LCT01	/	/	Send MDU-link_control (error indication); AN1
UPPER CASE external message or event Lower case internal message or event – No state change / Unexpected message, no state change			

Table 25/G.965 – Link control L3 protocol entity state transition table – LE

State / Event	LE0 OUT OF SERVICE	LE1 IN SERVICE	LE2 AWAIT LINK CONTROL ACK
MDU-start_traffic	LE1	–	–
MDU-stop_traffic	–	Stop LCT01; LE0	Stop LCT01; LE0
FE or saved FE	Send MDU-link_control (error indication); –	Send LINK CONTROL; Start LCT01; LE2	Save new received FE; –
LINK CONTROL	Send MDU-link_control (error indication); –	Send FE; Send LINK CONTROL ACK; –	Send FE; Send LINK CONTROL ACK; –
LINK CONTROL ACK	Send MDU-link_control (error indication); –	/	Stop LCT01; LE1
First expiry LCT01	/	/	Repeat LINK CONTROL; Start LCT01; –
Second expiry LCT01	/	/	Send MDU-link_control (error indication); LE1
UPPER CASE external message or event Lower case internal message or event – No state change / Unexpected message, no state change			

The following processes have been defined to be supported by the BCC protocol:

Allocation process

The procedure used by the BCC protocol which defines the interactions between the AN and the LE in order to allocate a defined number of bearer channels, over the V5.2-interface, to a particular user port. The process has a finite life and shall terminate either when:

a) the BCC protocol reports back to the LE resource manager that it has had confirmation from the AN resource manager that the proposed channels have been allocated; or

b) the allocation has not been successful.

In the second case, all relevant information is returned to the resource manager in the LE.

De-allocation process

The procedure used by the BCC protocol which defines the interactions between the AN and the LE in order to de-allocate a defined number of bearer channels, over the V5.2-interface, from a particular user port. The process has a finite life and shall terminate either when:

a) the BCC protocol reports back to the LE resource manager that it has had confirmation from the AN resource manager that the proposed channels have been de-allocated; or

b) the de-allocation has not been successful.

In the second case, all relevant information is returned to the resource manager in the LE.

Audit process

The procedure used by the BCC protocol which defines the interactions between the AN and the LE in order to check the routing of a bearer channel over the V5.2-interface and its subsequent connection at a user port. Any routing in between cannot be assumed to be fully checked (in general). The process shall be considered terminated when the response to the Audit is sent to the resource manager.

In order to identify a process, a BCC reference number will be allocated to that process.

V5.2-interfaces shall have the capability to support the following three types of bearer connection:

a) connections switched on a per call basis in the LE and on the V5.2-interface, in order to support PSTN and ISDN switched services, with traffic concentration in the AN;

b) connections switched on a per call basis in the LE but pre-connected on the V5.2-interface and the AN, in order to support PSTN and ISDN switched services (without traffic concentration in the AN), for high traffic lines (e.g. PBX lines) and situations where call blocking in the AN or on the V5-interface is unacceptable (e.g. emergency service lines);

c) connections semi-permanently established in the LE and the AN, in order to support semi-permanent leased line services (with no associated logical or physical C-channel signalling).

For connection type a), the BCC procedure shall be applied at the beginning and end of each call, under LE PSTN or ISDN call control.

For connection types b) and c), the BCC procedure shall be applied under LE system management control (e.g. from the Q_{LE} interface), as required for provisioning or ceasing of the switched or leased line service. The LE system management shall not specify a particular V5-interface time slot or 2048 kbit/s link but shall be informed of the time slot and link selected.

For connection types b) and c), the LE system management shall specify the user port and user port time slot.

V5.2-interfaces shall have the capability to establish and release multi-slot connections, n × 64 kbit/s where n equals 1 to 30, in order to support H0, H12 and future multirate services. Such connections can be type a), type b) or type c).

DSS1 channel types shall not be visible to the V5-interface but shall be handled transparently as n × 64 kbit/s connections. Multi-media calls shall not be visible to the V5-interface but shall be handled transparently as several independent connections.

Only connections between AN user ports and the V5.2-interface are supported by the BCC protocol. Intra-switching (i.e. user port to user port connection) is not be supported by the protocol. This does not preclude intra-switching entirely under AN control, e.g. when an AN is isolated from its parent LE due to V5-interface failure.

NOTE – Annex K gives additional information on how the BCC protocol is used by the LE and the AN.

Figure 15 shows the functional model for the BCC protocol.

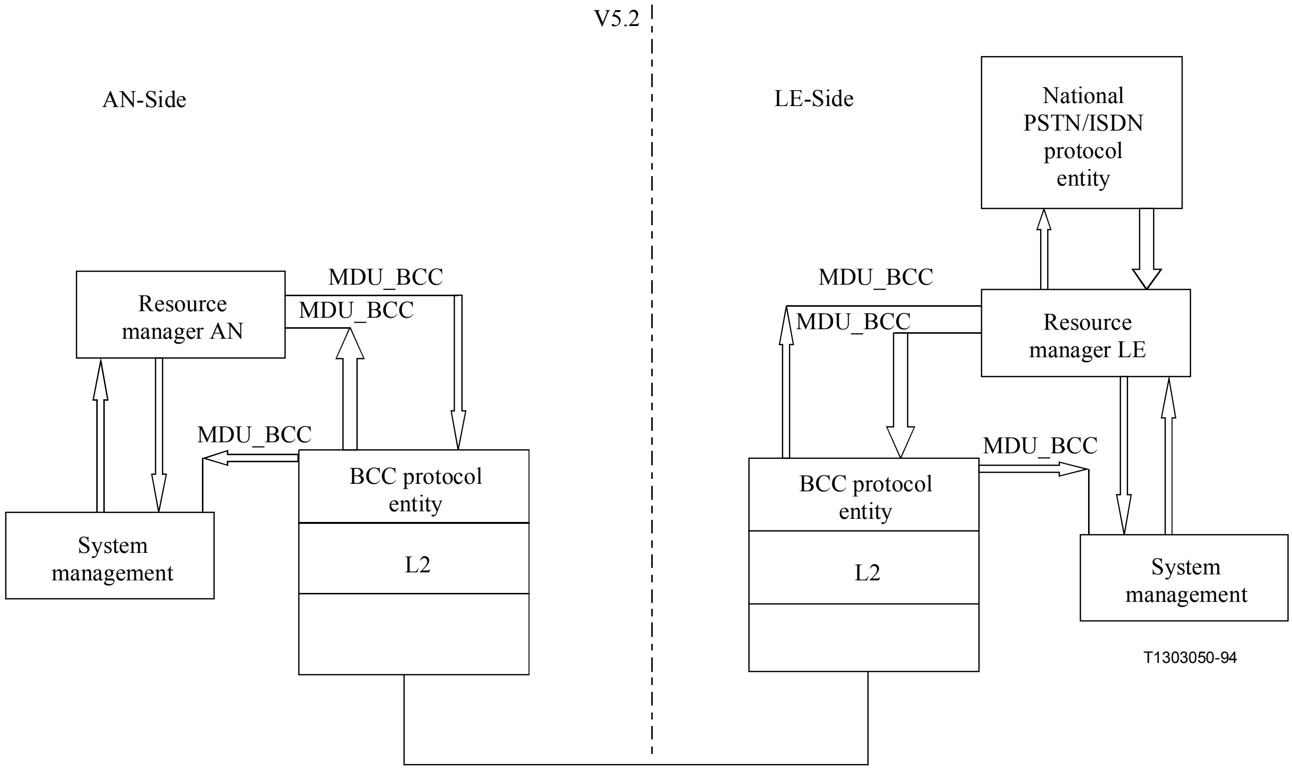


Figure 15/G.965 – The functional model for the BCC protocol

17.2 BCC protocol entity definition

17.2.1 Definition of BCC protocol states

17.2.1.1 BCC states in the AN

BCC OPERATIONAL state (ANBcc0)

The AN BCC protocol entity is a slave of the LE for the purpose of the BCC protocol processes initiated by the LE (allocation, de-allocation and audit processes). For all these processes only one operational state ("Bcc operational" state) is defined within the AN BCC protocol entity.

BCC AN FAULT REPORT state (ANBcc1)

The BCC protocol entity in the AN considers a process in this state when an AN FAULT message has been sent. The AN is now waiting for the reception of an AN FAULT ACKNOWLEDGE message before the expiration of Timer Tbcc5.

17.2.1.2 BCC states in the LE

BCC NULL state (LEBcc0)

The BCC protocol entity in the LE considers a process in this state when it is not yet related to any allocation or de-allocation procedure.

BCC WAITING ALLOCATION state (LEBcc1)

The BCC protocol entity in the LE considers a process in this state when an ALLOCATION message has been sent. The LE is now waiting for the reception of an ALLOCATION COMPLETE message or an ALLOCATION REJECT message before the expiration of Timer Tbcc1.

When being in this state, an internal request for the initiation of a de-allocation (allocation abort) may also occur.

BCC ALLOCATION ABORT state (LEBcc2)

The BCC protocol entity in the LE considers a process in this state when a DE-ALLOCATION message has been sent while being in the BCC waiting allocation state. The LE is now waiting for the reception of a DE-ALLOCATION COMPLETE message or a DE-ALLOCATION REJECT message before the expiration of Timer Tbcc2.

BCC WAITING DE-ALLOCATION state (LEBcc3)

The BCC protocol entity in the LE considers a process in this state when a DE-ALLOCATION message has been sent. The LE is now waiting for the reception of a DE-ALLOCATION COMPLETE message or a DE-ALLOCATION REJECT message before the expiration of Timer Tbcc3.

BCC WAITING AUDIT state (LEBcc4)

The BCC protocol entity in the LE considers a process in this state when an AUDIT message has been sent. The LE is now waiting for the reception of an AUDIT COMPLETE message before the expiration of Timer Tbcc4.

17.2.2 Definition of BCC protocol primitives, messages and timers

Table 26 defines the BCC protocol primitives, messages and timers at the LE side of the V5.2-interface. These protocol events are used in the LE state transition table shown in Table 46.

Table 27 defines the BCC protocol primitives, messages and timers at the AN side of the V5.2-interface. These protocol events are used in the AN state transition table shown in Table 47.

17.3 BCC protocol message definition and content

The format of the BCC protocol messages shall correspond to the generic message structure defined in clause 13.

The complete set of messages for the BCC protocol is given in Table 28. The following subclauses give the detailed message structure for each of these messages.

17.3.1 ALLOCATION message

This message is used by the local exchange to request from the access network the allocation of one or multiple bearer channels to a particular user port by the identification and use of a particular V5-time slot within the V5.2-interface (see Table 29).

Table 26/G.965 – LE side BCC protocol primitives, messages and timers

	Direction	Description
MDU-BCC (Allocation request)	RM → BCC_PE	Initiation of bearer channel allocation process
MDU-BCC (Allocation confirmation)	RM ← BCC_PE	Completion of bearer channel allocation process
MDU-BCC (Allocation reject indication)	RM ← BCC_PE	Completion of bearer channel allocation process is not possible
MDU-BCC (Allocation error indication)	RM ← BCC_PE	After retransmissions of the ALLOCATION message no response is received from the AN side
MDU-BCC (De-allocation request)	RM → BCC_PE	Initiation of bearer channel de-allocation process
MDU-BCC (De-allocation confirmation)	RM ← BCC_PE	Completion of bearer channel de-allocation process
MDU-BCC (De-allocation reject indication)	RM ← BCC_PE	Completion of bearer channel de-allocation process is not possible
MDU-BCC (De-allocation error indication)	RM ← BCC_PE	After retransmissions of the DE-ALLOCATION message no response is received from the AN side
MDU-BCC (Audit request)	RM → BCC_PE	Initiation of audit procedure process
MDU-BCC (Audit confirmation)	RM ←BCC_PE	Completion of audit procedure process
MDU-BCC (Audit error indication)	RM ← BCC_PE	After retransmissions of the AUDIT message no response is received from the AN side
MDU-BCC (AN fault indication)	RM ← BCC_PE	Initiation of AN internal failure procedure process
MDU-BCC (Protocol error indication)	SYS ← BCC_PE	Protocol error detected by the error handling checking
ALLOCATION	LE → AN	Initial message in a bearer channel allocation process
ALLOCATION COMPLETE	LE ← AN	Final message in a bearer channel allocation process successfully completed
ALLOCATION REJECT	LE ← AN	Final message in a bearer channel allocation process unsuccessfully completed
DE-ALLOCATION	LE → AN	Initial message in a bearer channel de-allocation process
DE-ALLOCATION COMPLETE	LE ← AN	Final message in a bearer channel de-allocation process successfully completed
DE-ALLOCATION REJECT	LE ← AN	Final message in a bearer channel de-allocation process unsuccessfully completed

Table 26/G.965 – LE side BCC protocol primitives, messages and timers

	Direction	Description
AUDIT	LE → AN	Initial message in an audit procedure process
AUDIT COMPLETE	LE ← AN	Final message in an audit procedure process successfully completed
AN FAULT	LE ← AN	Initial message in an AN internal failure notification process
AN FAULT ACKNOWLEDGE	LE → AN	Final message in an AN internal failure notification process successfully completed
PROTOCOL ERROR	LE ← AN	Notification of a BCC protocol error
Timeout Tbcc1	LE_BCC internal	When in the Bcc waiting allocation state, no proper message is received
Timeout Tbcc2	LE_BCC internal	When in the Bcc allocation abort state, no proper message is received
Timeout Tbcc3	LE_BCC internal	When in the Bcc waiting de-allocation state, no proper message is received
Timeout Tbcc4	LE_BCC internal	When in the Bcc waiting audit state, no proper message is received
RM LE Resource management entity BCC_PE LE BCC Protocol Entity LE_BCC internal Internal to the LE BCC protocol entity SYS LE System management		

Table 27/G.965 – AN side BCC protocol primitives, messages and timers

	Direction	Description
MDU-BCC (Allocation indication)	RM ← BCC_PE	Initiation of bearer channel allocation process
MDU-BCC [Allocation response (Complete)]	RM → BCC_PE	Completion of bearer channel allocation process
MDU-BCC [Allocation response (Reject)]	RM → BCC_PE	Completion of bearer channel allocation process is not possible
MDU-BCC (De-allocation indication)	RM ← BCC_PE	Initiation of bearer channel de-allocation process
MDU-BCC [De-allocation response (Complete)]	RM → BCC_PE	Completion of bearer channel de-allocation process
MDU-BCC [De-allocation response (Reject)]	RM → BCC_PE	Completion of bearer channel de-allocation process is not possible
MDU-BCC (Audit indication)	RM ← BCC_PE	Initiation of audit procedure process
MDU-BCC (Audit response)	RM → BCC_PE	Completion of audit procedure process

Table 27/G.965 – AN side BCC protocol primitives, messages and timers

	Direction	Description
MDU-BCC (AN fault request)	RM → BCC_PE	Initiation of AN internal failure notification process
MDU-BCC (AN fault confirmation)	RM ← BCC_PE	Completion of AN internal failure notification process
MDU-BCC (AN fault error indication)	RM ← BCC_PE	After retransmissions of the AN FAULT message no response is received from the LE side
MDU-BCC (Protocol error indication)	SYS ← BCC_PE	Protocol error detected by the error handling checking
ALLOCATION	LE → AN	Initial message in a bearer channel allocation process
ALLOCATION COMPLETE	LE ← AN	Final message in a bearer channel allocation process successfully completed
ALLOCATION REJECT	LE ← AN	Final message in a bearer channel allocation process unsuccessfully completed
DE-ALLOCATION	LE → AN	Initial message in a bearer channel de-allocation process
DE-ALLOCATION COMPLETE	LE ← AN	Final message in a bearer channel de-allocation process successfully completed
DE-ALLOCATION REJECT	LE ← AN	Final message in a bearer channel de-allocation process unsuccessfully completed
AUDIT	LE → AN	Initial message in an audit procedure process
AUDIT COMPLETE	LE ← AN	Final message in an audit procedure process successfully completed
AN FAULT	LE ← AN	Initial message in an AN internal failure notification process
AN FAULT ACKNOWLEDGE	LE → AN	Final message in an AN internal failure notification process successfully completed
PROTOCOL ERROR	LE ← AN	Notification of a BCC protocol error
Timeout Tbcc5	AN_BCC internal	When in the Bcc fault report state, no proper message is received
RM	AN Resource Management entity	
BCC_PE	AN BCC Protocol Entity	
AN_BCC internal	Internal to the AN BCC protocol entity	
SYS	System management	

Table 28/G.965 – Set of the BCC protocol messages

Coding within the message type information element							Messages of the BCC protocol	Reference
7	6	5	4	3	2	1		
0	1	0	0	0	0	0	ALLOCATION	17.3.1
0	1	0	0	0	0	1	ALLOCATION COMPLETE	17.3.2
0	1	0	0	0	1	0	ALLOCATION REJECT	17.3.3
0	1	0	0	0	1	1	DE-ALLOCATION	17.3.4
0	1	0	0	1	0	0	DE-ALLOCATION COMPLETE	17.3.5
0	1	0	0	1	0	1	DE-ALLOCATION REJECT	17.3.6
0	1	0	0	1	1	0	AUDIT	17.3.7
0	1	0	0	1	1	1	AUDIT COMPLETE	17.3.8
0	1	0	1	0	0	0	AN FAULT	17.3.9
0	1	0	1	0	0	1	AN FAULT ACKNOWLEDGE	17.3.10
0	1	0	1	0	1	0	PROTOCOL ERROR	17.3.11

Table 29/G.965 – ALLOCATION message content

Message Type: ALLOCATION

Direction: LE to AN

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	LE to AN	M	1
BCC Reference Number	17.4.1	LE to AN	M	2
Message Type	17.3	LE to AN	M	1
User Port Identification	17.4.2.1	LE to AN	M	4
ISDN Port Time Slot Identification	17.4.2.2	LE to AN	C (Note 1)	3
V5-Time Slot Identification	17.4.2.3	LE to AN	C (Note 2)	4
Multi-Slot Map	17.4.2.4	LE to AN	C (Note 3)	11
Information Transfer capability	17.4.2.8	LE to AN	C (Note 4)	3

NOTE 1 – The ISDN Port Channel Identification information element has to be included when allocating a single time slot in order to support a bearer channel related to an ISDN Port and shall be handled as a mandatory information element. This information element shall specify the user port time slot within the ISDN user/network interface (basic or primary) to which the bearer channel has to be through-connected.

NOTE 2 – The Time Slot Identification information element has to be included when allocating a single time slot in order to identify the relevant V5.2 interface time slot and shall be handled as a mandatory information element.

NOTE 3 – The Multi-Slot Map information element has to be included when allocating multiple time slots in order to support multirate (n × 64 kbit/s) ISDN bearer services and shall be handled as a mandatory information element. This information element shall also specify the user port time slots within the ISDN user/network interface (basic or primary) to which the bearer channel has to be through-connected.

NOTE 4 – The Information Transfer Capability shall be included when the User Port Identification information element identifies an ISDN port.

In the case of bearer channel allocations to an ISDN port for the purpose of through-connection, the local exchange shall also indicate the user port time slot in the ISDN interface to be used.

This message also allows the in-block allocation of multirate bearer channels (multiple V5-time slots) to support multirate (n × 64 kbit/s) services.

17.3.2 ALLOCATION COMPLETE message

This message is used by the access network to indicate to the local exchange that the allocation of the requested bearer channel(s) to a particular user port has been successfully completed (see Table 30).

Table 30/G.965 – ALLOCATION COMPLETE message content

Message Type: ALLOCATION COMPLETE

Direction: AN to LE

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	AN to LE	M	1
BCC Reference Number	17.4.1	AN to LE	M	2
Message Type	17.3	AN to LE	M	1

17.3.3 ALLOCATION REJECT message

This message is used by the access network to indicate to the local exchange that the allocation of the requested bearer channel(s) to a particular user port has not been completed (see Table 31).

Table 31/G.965 – ALLOCATION REJECT message content

Message Type: ALLOCATION REJECT

Direction: AN to LE

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	AN to LE	M	1
BCC Reference Number	17.4.1	AN to LE	M	2
Message Type	17.3	AN to LE	M	1
Reject Cause	17.4.2.5	AN to LE	M	3 to 14

17.3.4 DE-ALLOCATION message

This message is used by the local exchange to request from the access network the de-allocation of one or multiple bearer channels from a particular user port. The particular V5-time slot within the V5.2-interface is explicitly identified (see Table 32).

This message also allows the *en bloc* de-allocation of multirate bearer channels (multiple V5-time slots) supporting multirate (n × 64 kbit/s) services.

Table 32/G.965 – DE-ALLOCATION message content

Message Type: DE-ALLOCATION

Direction: LE to AN

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	LE to AN	M	1
BCC Reference Number	17.4.1	LE to AN	M	2
Message Type	17.3	LE to AN	M	1
User Port Identification	17.4.2.1	LE to AN	M	4
ISDN Port Time Slot Identification	17.4.2.2	LE to AN	C (Note 1)	3
V5-Time Slot Identification	17.4.2.3	LE to AN	C (Note 2)	4
Multi-Slot Map	17.4.2.4	LE to AN	C (Note 3)	11
NOTE 1 – The ISDN Port Channel Identification information element has to be included when de-allocating a single time slot in order to support a bearer channel related to an ISDN Port and shall be handled as a mandatory information element. This information element shall specify the user port time slot within the ISDN user/network interface (basic or primary) from which the bearer channel has to be disconnected. NOTE 2 – The Time Slot Identification information element has to be included when de-allocating a single time slot in order to identify the relevant V5.2 interface time slot and shall be handled as a mandatory information element. NOTE 3 – The Multi-Slot Map information element has to be included when de-allocating multiple time slots in order to support multirate (n × 64 kbit/s) ISDN bearer services and shall be handled as a mandatory information element. This information element shall also specify the user port time slot within the ISDN user/network interface (basic or primary) from which the bearer channel has to be disconnected.				

17.3.5 DE-ALLOCATION COMPLETE message

This message is used by the access network to indicate to the local exchange that the de-allocation of the requested bearer channel(s) from a particular user port has been successfully completed (see Table 33).

Table 33/G.965 – DE-ALLOCATION COMPLETE message content

Message Type: DE-ALLOCATION COMPLETE

Direction: AN to LE

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	AN to LE	M	1
BCC Reference Number	17.4.1	AN to LE	M	2
Message Type	17.3	AN to LE	M	1

17.3.6 DE-ALLOCATION REJECT message

This message is used by the access network to indicate to the local exchange that the de-allocation of the requested bearer channel(s) from a particular user port has not been completed (see Table 34).

Table 34/G.965 – DE-ALLOCATION REJECT message content

Message Type: DE-ALLOCATION REJECT

Direction: AN to LE

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	AN to LE	M	1
BCC Reference Number	17.4.1	AN to LE	M	2
Message Type	17.3	AN to LE	M	1
Reject Cause	17.4.2.5	AN to LE	M	3 to 14

17.3.7 AUDIT message

This message is used by the local exchange to request from the access network the provision of the complete information that identifies a 64 kbit/s bearer channel connection (see Table 35).

This message allows the local exchange to request the bearer channel connection information on the basis of the partial information available in certain circumstances such as the user port identification, together with the ISDN port channel identification when applicable or the V5-time slot identification.

Table 35/G.965 – AUDIT message content

Message Type: AUDIT

Direction: LE to AN

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	LE to AN	M	1
BCC Reference Number	17.4.1	LE to AN	M	2
Message Type	17.3	LE to AN	M	1
User Port Identification	17.4.2.1	LE to AN	O (Note 1)	4
ISDN Port Time Slot Identification	17.4.2.2	LE to AN	O (Note 2)	3
V5-Time Slot Identification	17.4.2.3	LE to AN	O (Note 3)	4

NOTE 1 – When auditing on the basis of the user port, this information element identifies the user port terminating the bearer channel connection on which the audit has to be done.

NOTE 2 – When auditing on the basis of the user port, and the port is an ISDN user port, this information element identifies the user port time slot terminating the bearer channel connection on which the audit has to be done. This information element shall appear together with the user port identification information element and shall be handled as a mandatory information element. This information element shall not be included in the message without the User Port Identification IE indicating an ISDN user port.

NOTE 3 – When auditing on the basis of the V5 time slot, this information element identifies the V5 time slot within the V5.2 interface supporting the bearer channel connection on which the audit has to be done.

The AUDIT message shall always include either the User Port Identification IE or the V5 Time Slot Identification IE, but not both. When included, the IE shall be handled as mandatory information element.

17.3.8 AUDIT COMPLETE message

This message is used by the access network to indicate to the local exchange the result of the auditing requested by the provision of the information identifying the bearer channel connection or indicating that no connection is available on the reference provided (see Table 36).

Table 36/G.965 – AUDIT COMPLETE message content

Message Type: AUDIT COMPLETE

Direction: AN to LE

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	AN to LE	M	1
BCC Reference Number	17.4.1	AN to LE	M	2
Message Type	17.3	AN to LE	M	1
User Port Identification	17.4.2.1	AN to LE	O (Note 1)	4
ISDN Port Time Slot Identification	17.4.2.2	AN to LE	O (Note 1)	3
V5-Time Slot Identification	17.4.2.3	AN to LE	O (Note 1)	4
Connection Incomplete	17.4.2.7	AN to LE	O (Note 2)	3
NOTE 1 – The User port identification information element shall be included, together with the ISDN port channel identification information element, when applicable, and the V5 time slot identification information element, if the result of the auditing reflects an existent complete connection. This information element shall be included when the result of an auditing process is not successful because no connection exists associated with the provided reference information of the audit process. NOTE 2 – The AUDIT COMPLETE message shall always include either the User Port Identification IE and the V5 Time Slot Identification IE and the ISDN Port Channel Identification IE (when applicable) or the Connection Incomplete IE. When included, these information elements shall be handled as mandatory information elements.				

17.3.9 AN FAULT message

This message is used by the access network to notify to the local exchange about a single 64 kbit/s bearer channel connection that has been broken in the access network due to an internal failure (see Table 37).

When notifying an internal failure, the AN has to provide the information needed in order to allow the LE to identify all the data related to that connection.

Table 37/G.965 – AN FAULT message content

Message Type: AN FAULT

Direction: AN to LE

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	AN to LE	M	1
BCC Reference Number	17.4.1	AN to LE	M	2
Message Type	17.3	AN to LE	M	1
User Port Identification	17.4.2.1	AN to LE	O (Note 1)	4
ISDN Port Time Slot Identification	17.4.2.2	AN to LE	O (Note 2)	3
V5-Time Slot Identification	17.4.2.3	AN to LE	O (Note 3)	4

Table 37/G.965 – AN FAULT message content

NOTE 1 – When an internal AN connection fails, this information element shall be included, if available, together with the ISDN port channel identification information element, when applicable, in order to notify to the LE the user port affected by the AN failure. NOTE 2 – When an internal AN connection fails, this information element shall be used when the failure notification refers to an ISDN port identified by the User port identification information element. NOTE 3 – When an internal AN connection fails, this information element shall be included, if available, in order to notify to the LE the V5.2 V5-time slot affected by the AN failure.

17.3.10 AN FAULT ACKNOWLEDGE message

This message is used by the local exchange to acknowledge to the access network the reception of an AN FAULT message (see Table 38).

NOTE – The sending of this message is an acknowledgement of the received AN FAULT message and not a notification that the proper actions have been taken.

Table 38/G.965 – AN FAULT ACKNOWLEDGE message content

Message Type: AN FAULT ACKNOWLEDGE

Direction: LE to AN

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	LE to AN	M	1
BCC Reference number	17.4.1	LE to AN	M	2
Message Type	17.3	LE to AN	M	1

17.3.11 PROTOCOL ERROR message

This message is used by the access network to indicate to the local exchange that a protocol error has been identified in a received message (see Table 39).

Table 39/G.965 – PROTOCOL ERROR message content

Message Type: PROTOCOL ERROR

Direction: AN to LE

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	AN to LE	M	1
BCC Reference Number	17.4.1	AN to LE	M	2
Message Type	17.3	AN to LE	M	1
Protocol Error Cause	17.4.2.6	AN to LE	M	3 to 5

17.4 BCC information element definition, structure and coding

This clause defines the coding of the information elements that are specific for the BCC protocol, being used within the BCC protocol specific messages. For each of the information elements, the coding of their different fields is provided.

The BCC protocol specific information elements are listed in Table 40 which also gives the coding of the information element identifier.

Table 40/G.965 – BCC protocol specific information elements

Bits								Information element	Reference
8	7	6	5	4	3	2	1		
0	–	–	–	–	–	–	–	VARIABLE LENGTH INFORMATION ELEMENTS	
0	1	0	0	0	0	0	0	User port identification	17.4.2.1
0	1	0	0	0	0	0	1	ISDN port Time Slot identification	17.4.2.2
0	1	0	0	0	0	1	0	V5-time slot identification	17.4.2.3
0	1	0	0	0	0	1	1	Multi-slot map	17.4.2.4
0	1	0	0	0	1	0	0	Reject cause	17.4.2.5
0	1	0	0	0	1	0	1	Protocol error cause	17.4.2.6
0	1	0	0	0	1	1	0	Connection incomplete	17.4.2.7
0	1	0	0	0	1	1	1	Information Transfer Capability	17.4.2.8
NOTE – All other values are reserved.									

17.4.1 BCC Reference Number information element

This information element is specific for the BCC protocol and uses the location of the Layer 3 address information element within the general message structure as defined in clause 13.

The purpose of the BCC Reference Number information element is to identify the BCC protocol process, within the V5.2 interface, to which the transmitted or received message applies.

The BCC reference number value shall be a random value generated by the entity (AN or LE) creating the new BCC protocol process (this random value may be implemented as a sequential generation of values). It is essential that values are not repeated in messages for which a different BCC process is required (in the same direction), until the old BCC process has been finished and the number deleted. The BCC Reference Number information element, being part of the message header, shall be the second part of every message (located after the Protocol Discriminator information element). In the case of any process generating error indications, the BCC reference number should not be re-used until sufficient time has elapsed for delayed arrival of messages containing the same BCC reference number.

The length of the BCC Reference Number information element shall be 2 octets.

The structure of the BCC Reference Number information element shall be as indicated by Figure 16.

8	7	6	5	4	3	2	1	Octets
Source ID	BCC reference number value							1
0	0	BCC reference number value (low)						2

Figure 16/G.965 – BCC Reference Number information element

The source identification is a field of one bit specifying the entity (LE or AN) that has created the BCC reference number (i.e. the entity that has created the BCC protocol process). The coding of this field shall be ZERO for an LE created process and ONE for an AN created process.

The BCC reference number value field consists of 13 bits and is used for providing the binary coding that identifies the BCC process.

17.4.2 Other information elements

Within this clause the information elements that may appear in the different messages are described.

These information elements may appear in the different messages being optional or mandatory depending on the message semantics and/or the process application of the message.

17.4.2.1 User Port Identification information element

The purpose of the User Port Identification information element is to identify, via the V5.2 interface, the PSTN or ISDN port to which the BCC protocol process related message applies.

The length of the User Port Identification information element shall be 4 octets.

The structure of the User Port Identification information element shall be as indicated by Figures 17 and 18.

The coding of the User Port Identification information element shall be in binary. For the coding of the User Port Identification information element two structures have been defined, one for the PSTN ports application (see Figure 17) and the other for the ISDN ports application (see Figure 18).

8	7	6	5	4	3	2	1	Octets
	Information element identifier							
0	1	0	0	0	0	0	0	1
Length of the information element content								2
User Port Identification Value							1	3
User Port Identification Value (lower)								4

Figure 17/G.965 – User Port Identification information element (PSTN port application)

8	7	6	5	4	3	2	1	Octets
	Information element identifier							
0	1	0	0	0	0	0	0	1
Length of the information element content								2
User Port Identification Value						0	0	3
User Port Identification Value (lower)							1	4

Figure 18/G.965 – User Port Identification information element (ISDN port application)

For the case of the PSTN ports application, the user port identification value (15 bits) shall have the same value as the Layer 3 address information element contained within the PSTN protocol messages related to that PSTN user port for which the process related message applies.

For the case of the ISDN ports application, the user port identification value (13 bits) shall have the same value as the Envelope Address contained within the envelope function frames used for relaying the DSS1 messages related to that ISDN user port for which the process related message applies.

17.4.2.2 ISDN Port Time Slot Identification information element

The purpose of the ISDN Port Time Slot Identification information element is to indicate, only in the case of a single V5-time slot BCC protocol related to an ISDN user port, the user port time slot within the ISDN user/network interface (basic or primary rate access) to which the V5-time slot within the 2048 kbit/s link of the V5.2 interface has to be through-connected, or from which the identified V5-time slot has to be disconnected.

The length of the ISDN Port Time Slot Identification information element shall be 3 octets.

The structure of the ISDN Port Time Slot Identification information element shall be as indicated by Figure 19.

The ISDN user port TS number is a field of five bits used for providing the binary coding that identifies the user port time slot within the ISDN user port. For the case of ISDN-PRA user ports, channels B1 to B31 shall be referred to as ISDN user port time slot number 1 (00001) to 31 (11111). For the case of ISDN basic access user port, channel B1 shall be referred to as ISDN user port time slot number 1 (00001) and channel B2 as ISDN user port time slot number 2 (00010).

8	7	6	5	4	3	2	1	Octets
	Information element identifier							
0	1	0	0	0	0	0	1	1
Length of the information element content								2
1	0	0	ISDN user port time slot number					3

Figure 19/G.965 – ISDN Port Time Slot Identification information element

17.4.2.3 V5-Time Slot Identification information element

The purpose of the V5-Time Slot Identification information element is to identify, in the case of a single V5-time slot BCC protocol process, the V5-time slot within a particular 2048 kbit/s link to which the process applies.

The length of the V5-Time Slot Identification information element shall be 4 octets.

The structure of the BCC Reference Number information element shall be as indicated by Figure 20.

8	7	6	5	4	3	2	1	Octets
0	Information element identifier 1	0	0	0	0	1	0	1
Length of the information element content								2
V5 2048 kbit/s link Identifier								3
0	0	Override	V5-Time Slot Number					4

Figure 20/G.965 – V5-Time Slot Identification information element

The V5 2048 kbit/s Link Identifier is a field of eight bits used for providing the binary coding that identifies a particular 2048 kbit/s link out of those that comprise the V5.2 interface, where the selected V5-time slot to be used as the bearer channel is located. A maximum of 256 (2048 kbit/s links) can be explicitly identified.

The V5-Time Slot Number is a field of five bits used for providing the binary coding that identifies the V5-time slot, or the first V5-time slot of a block of V5-time slots (within the 2048 kbit/s link identified in the previous octet) to be used, or being used, as the bearer channel.

The Override bit specifies the request from the LE for overriding the existing bearer channel connection over the identified V5-time slot when establishing the requested bearer channel connection. The coding of this field shall be a ZERO for "Override not requested" and a ONE for "Override requested".

17.4.2.4 Multi-Slot Map information element

The purpose of the Multi-Slot Map information element is to identify, in the case of *en bloc* allocation or de-allocation of multiple V5-time slots, all the V5-time slots within a particular V5 2048 kbit/s link to which the allocation or de-allocation process applies.

The Multi-Slot Map information element shall also identify the user port time slots within the ISDN user/network interface, to which the identified V5-time slots have to be through-connected, or from which the identified V5-time slots have to be disconnected.

The relationship between the identified V5-time slots and user port time slot shall be one-to-one in the same order of appearance within the respective coding maps.

NOTE – When several V5-time slots have been allocated as one block, these may or may not be de-allocated *en bloc*.

The number of V5-time slots affected by a de-allocation process shall be determined by the resource management system on the basis of the ISDN service being provided.

Under certain circumstances (e.g. ISDN interface restart) a de-allocation process affecting several V5-time slots may be requested by the resource management system, even when those V5-time slots were allocated individually.

The length of the Multi-Slot Map information element shall be 11 octets.

The structure of the Multi-Slot Map information element shall be as indicated in Figure 21.

8	7	6	5	4	3	2	1	Octets
	Information element identifier							
0	1	0	0	0	0	1	1	1
Length of the information element content								2
V5 2048 kbit/s link Identifier								3
V5TS31	V5TS30	V5TS29	V5TS28	V5TS27	V5TS26	V5TS25	V5TS24	4
V5TS23	V5TS22	V5TS21	V5TS20	V5TS19	V5TS18	V5TS17	V5TS16	5
V5TS15	V5TS14	V5TS13	V5TS12	V5TS11	V5TS10	V5TS9	V5TS8	6
V5TS7	V5TS6	V5TS5	V5TS4	V5TS3	V5TS2	V5TS1	0	7
UPTS31	UPTS30	UPTS29	UPTS28	UPTS27	UPTS26	UPTS25	UPTS24	8
UPTS23	UPTS22	UPTS21	UPTS20	UPTS19	UPTS18	UPTS17	UPTS16	9
UPTS15	UPTS14	UPTS13	UPTS12	UPTS11	UPTS10	UPTS9	UPTS8	10
UPTS7	UPTS6	UPTS5	UPTS4	UPTS3	UPTS2	UPTS1	0	11

Figure 21/G.965 – Multi-Slot Identification information element

The V5 2048 kbit/s Link Identifier is a field of eight bits used for providing the binary coding that identifies the 2048 kbit/s link/system (out of those that may compose the V5.2 interface) where the selected V5-time slots to be used as the bearer channels are located. A maximum of 256 (2048 kbit/s) links can be explicitly identified.

Octets 4 to 7 identify multiple V5-time slots within the V5.2 interface being allocated or de-allocated *en bloc*. The bits corresponding to the V5-time slots affected by the process shall be coded as binary "1", the bits corresponding to the V5-time slots non-affected by the process shall be coded as binary "0".

Octets 8 to 11 identify multiple user port time slots within the ISDN user port (basic or primary) to which the specified V5-time slots in octets 4 to 7 have to be through connected or disconnected. The relationship between the V5-time slots and the user port time slots shall be one-to-one in the specified numbering order. The bits corresponding to the user port time slots affected by the process shall be coded as binary "1", the bits corresponding to the user port time slots non-affected by the process shall be coded as binary "0".

For the case of ISDN basic access user port, the two B-channels shall be referred to as user port time slot UPTS1 and user port time slot UPTS2 in the map, UPTS3 to UPTS31 shall never be made active in this case.

17.4.2.5 Reject Cause information element

The purpose of the Reject Cause information element is to indicate from the access network to the local exchange the reason for which the allocation/de-allocation of the requested bearer channel(s) has not been completed.

The Reject Cause information element for some reject cause types shall include a diagnostic field in order to provide additional information related to these reject cause values. This diagnostic field, when present, shall always be a copy of the received information element containing the information that triggered the sending of the reject message. (This is not checked by the LE).

The length of the Reject cause information element may be between 3 and 14 octets. For reject cause types not including a diagnostic information, the length of the information element shall be 3 octets. For reject cause types including a diagnostic information, the length of the information element shall be between 6 and 14 octets (6, 7 and 14 octets are the valid values).

The structure of the Reject Cause information element shall be as indicated in Figure 22.

8	7	6	5	4	3	2	1	Octets
	Information element identifier							
0	1	0	0	0	1	0	0	1
Length of the information element content								2
1	Reject cause type							3
Diagnostic								4 n

Figure 22/G.965 – Reject Cause information element

The coding of the reject cause type field shall be as specified in Table 41.

Table 41/G.965 – Coding of reject cause type

7	6	5	4	3	2	1	Reject cause
0	0	0	0	0	0	0	Unspecified
0	0	0	0	0	0	1	Access network fault
0	0	0	0	0	1	0	Access network blocked (internally)
0	0	0	0	0	1	1	Connection already present at the PSTN user port to a different V5-time slot
0	0	0	0	1	0	0	Connection already present at the V5-time slot(s) to a different port or ISDN user port time slot
0	0	0	0	1	0	1	Connection already present at the ISDN user port time slot(s) to a different V5-time slot(s)
0	0	0	0	1	1	0	User port unavailable (blocked)
0	0	0	0	1	1	1	De-allocation cannot be completed due to incompatible data content
0	0	0	1	0	0	0	De-allocation cannot be completed due to V5-time slot(s) data incompatibility
0	0	0	1	0	0	1	De-allocation cannot be completed due to port data incompatibility
0	0	0	1	0	1	0	De-allocation cannot be completed due to user port time slot(s) data incompatibility
0	0	0	1	0	1	1	User port not provisioned
0	0	0	1	1	0	0	Invalid V5-time slot(s) identification(s)
0	0	0	1	1	0	1	Invalid V5 2048 kbit/s link identification
0	0	0	1	1	1	0	Invalid user port time slot(s) identification(s)
0	0	0	1	1	1	1	V5-time slot(s) being used as physical C-channel(s)
0	0	1	0	0	0	0	V5-link unavailable (blocked)
NOTE – All other values are reserved.							

Table K.1 provides further information on when to use the different reject cause types in the BCC protocol procedures.

The diagnostic field is a field of multiple octets (number of octets dependent of the cause value) providing the relevant diagnostic for each of the reject cause types according to Table 42.

Table 42/G.965 – Diagnostic for the reject cause types

Cause	Diagnostic	Length
Unspecified	Not present	0
Access network fault	Not present	0
Access network blocked (internally)	Not present	0
Connection already present at the PSTN user port to a different V5-time slot	User port identification information element	4
Connection already present at the V5.2 interface V5-time slot(s) to a different port or ISDN user port time slot(s)	V5-time slot identification or Multi-slot map information element	4 or 11
Connection already present at the ISDN user port time slot(s) to a different V5-time slot(s)	ISDN port channel identification or Multi-slot map information element	3 or 11
User port unavailable (blocked)	User port identification information element	4
De-allocation cannot be completed due to incompatible data content	Not present	0
De-allocation cannot be completed due to V5-time slot(s) data incompatibility	V5-time slot identification or Multi-slot map information element	4 or 11
De-allocation cannot be completed due to port data incompatibility	User port identification information element	4
De-allocation cannot be completed due to user port time slot(s) data incompatibility	ISDN port channel identification or Multi-slot map information element	3 or 11
User port not provisioned	User port identification information element	4
Invalid V5-time slot(s) identification(s)	V5-time slot identification or Multi-slot map information element	4 or 11
Invalid V5 2048 kbit/s link identification	V5-time slot identification or Multi-slot map information element	4 or 11
Invalid user port time slot(s) identification(s)	ISDN port channel identification or Multi-slot map information element	3 or 11
V5-time slot(s) being used as physical C-channel(s)	V5-time slot identification or Multi-slot map information element	4 or 11
V5 link unavailable (blocked)	V5-time slot identification or Multi-slot map information element	4 or 11

If the length of the diagnostics in the reject cause information element is not correct (i.e. does not comply with a value given in Table 42), the LE shall react according to 17.5.8.7.

17.4.2.6 Protocol Error Cause information element

The purpose of the Protocol Error Cause information element is to indicate from the access network to the local exchange the type of protocol error detected in a given BCC protocol process.

The Protocol Error Cause information element shall, for some protocol error cause types, include a diagnostic field in order to provide additional information related to these protocol error cause types. This diagnostic field of one or two octets, when present, shall be a copy of the received message type identifier that has triggered the sending of the message containing the Protocol Error

Cause information element, and when needed the relevant information element identifier within that message.

The length of the Protocol Error Cause information element may be between 3 and 5 octets. For Protocol error cause types not including a diagnostic information, the length of the information element shall be 3 octets. For Protocol error cause types including a diagnostic information, the length of the information element shall be 4 or 5 octets.

The structure of the Protocol Error Cause information element shall be as indicated in Figure 23.

8	7	6	5	4	3	2	1	Octets
	Information element identifier							
0	1	0	0	0	1	0	1	1
Length of the information element content								2
1	Protocol error cause type							3
0	Diagnostic (message type identifier)							4
Diagnostic (information element identifier)								5

Figure 23/G.965 – Protocol Error Cause information element

The coding of the protocol error cause type field shall be as specified in Table 43.

Table 43/G.965 – Protocol error cause type

7	6	5	4	3	2	1	Protocol error cause
0	0	0	0	0	0	1	Protocol discriminator error
0	0	0	0	1	0	0	Message type unrecognized
0	0	0	0	1	0	1	Out of sequence information element
0	0	0	0	1	1	0	Repeated optional information element
0	0	0	0	1	1	1	Mandatory information element missing
0	0	0	1	0	0	0	Unrecognized information element
0	0	0	1	0	0	1	Mandatory information element content error
0	0	0	1	0	1	0	Optional information element content error
0	0	0	1	0	1	1	Message not compatible with the BCC protocol state
0	0	0	1	1	0	0	Repeated mandatory information element
0	0	0	1	1	0	1	Too many information elements
0	0	0	1	1	1	1	BCC Reference Number coding error
NOTE – All other values are reserved.							

Clause 17.5.8 specifies when to use the different protocol error cause type values.

The diagnostic field is a field of multiple octets (number of octets dependent of the cause value) providing the relevant diagnostic for each protocol error cause value according to Table 44.

Table 44/G.965 – Diagnostic for the protocol error types

Cause	Diagnostic	Length
Protocol discriminator error	Not present	0
BCC Reference Number coding error	Not present	0
Message type unrecognized	Message type identifier	1
Out of sequence information element	Message type identifier Information element identifier	2
Repeated optional information element	Message type identifier Information element identifier	2
Mandatory information element missing	Message type identifier Information element identifier	2
Unrecognized information element	Message type identifier Information element identifier	2
Mandatory information element content error	Message type identifier Information element identifier	2
Optional information element content error	Message type identifier Information element identifier	2
Message not compatible with the BCC protocol state	Message type identifier	1
Repeated mandatory information element	Message type identifier Information element identifier	2
Too many information elements	Message type identifier	1

If the length of the diagnostics in the Protocol error cause information element is not correct (i.e. does not comply with a value given in Table 44), the LE shall react according to 17.5.8.7.

17.4.2.7 Connection Incomplete information element

The purpose of the Connection Incomplete information element is to indicate from the access network to the local exchange that the result of an auditing process is not successful because no AN connection exists.

Within the reason field, this information element gives information about the reason for that connection being incomplete.

The length of the Connection Incomplete information element shall be 3 octets.

The structure of the Connection Incomplete information element shall be as indicated in Figure 24.

<table>
<tr><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>Octets</td></tr>
<tr><td>0</td><td colspan="7">Information element identifier
1 0 0 0 1 1 0</td><td>1</td></tr>
<tr><td colspan="8">Length of the information element content</td><td>2</td></tr>
<tr><td>ext.
1</td><td colspan="7">Reason</td><td>3</td></tr>
<tr><td colspan="8">NOTE – Bit 8 is marked "ext. 1" as this is the last octet in the extension domain. Additional octets may be defined later ("ext. 1" will change to "ext. 0/1") and equipment shall be prepared to receive such additional octets although the equipment need not be able to interpret or act upon the content of these octets.</td><td></td></tr>
</table>

Figure 24/G.965 – Connection Incomplete information element

The coding of reason field of the connection incomplete information element shall be as specified in Table 45.

Table 45/G.965 – Coding of reason field

7	6	5	4	3	2	1	Reason
0	0	0	0	0	0	0	Incomplete normal
0	0	0	0	0	0	1	Access network fault
0	0	0	0	0	1	0	User port not provisioned
0	0	0	0	0	1	1	Invalid V5-time slot identification
0	0	0	0	1	0	0	Invalid V5 2048 kbit/s link identification
0	0	0	0	1	0	1	Time slot being used as physical C-channel
NOTE – All other values are reserved.							

17.4.2.8 Information Transfer Capability information element

The purpose of the Information Transfer Capability information element is to indicate to the access network the Information Transfer Capability requested for a given ISDN bearer channel on a given ISDN user port.

The Local Exchange shall have the possibility to enable or disable the use of this information element by means of provisioning.

The content of this information element is a subset of the Bearer Capability information element present within DSS1.

The length of the Information Transfer Capability shall be 3 octets.

The structure of the Information Transfer Capability information element shall be as indicated by Figure 24a.

8	7	6	5	4	3	2	1	Octets
0	Information element identifier 1	0	0	0	1	1	1	1
Length of the information element content								2
1	0	0	Information transfer capability					3

Figure 24a/G.965 – Information Transfer Capability information element

The coding of octet 3 is identical to the coding of octet 3 in the Bearer Capability information element in DSS1 messages.

17.5 Description of the BCC protocol and the BCC procedures

Annex K provides further information on the interaction of switched calls with the BCC protocol.

17.5.1 General

Because of the transparency of the AN and the V5.2 interface to the ISDN and PSTN call control protocols, the relevant procedure of this BCC Protocol has to be triggered from the resource management entity in the LE as a consequence of analysis of the ISDN/PSTN call control procedures.

From the BCC point of view, every V5-time slot allocation or de-allocation is considered as an independent process that shall be concluded with the successful completion or abortion of the V5-time slot allocation or de-allocation.

Each of the processes shall be identified by a different BCC reference number. The BCC protocol entity and the resource management entity shall allow multiple BCC processes running in parallel.

NOTE – For the purpose of the BCC Protocol (bearer channel control procedures) it is assumed that an individual FSM has to be implemented for each of the allocation or de-allocation request related to one or more of the V5.2-time slots available to be used as bearer channels.

The procedures composing the BCC protocol, and described in the following subclauses are:

– bearer channel allocation: normal procedure;
– bearer channel allocation: exceptional procedures;
– bearer channel de-allocation: normal procedure;
– bearer channel de-allocation: exceptional procedures;
– audit procedure;
– AN internal failure notification procedure;
– handling of error conditions.

17.5.2 Bearer channel allocation – Normal procedure

The BCC protocol entity in the LE, being in the "Bcc null" state, when receiving the MDU-BCC (Allocation request) primitive shall initiate the bearer channel allocation by sending to the AN an ALLOCATION message indicating the V5-time slot(s) in the V5.2 interface to be used. In the case of the ISDN port related allocations, the LE shall also indicate the ISDN user port time slot(s) in the ISDN user/network interface to be through-connected to the selected V5-time slot.

With the sending of the ALLOCATION message the LE shall start timer Tbcc1 and enter the "Bcc waiting allocation" state.

When the BCC protocol entity in the AN receives the ALLOCATION message, it shall notify the event to the resource management entity by the MDU-BCC (Allocation indication) primitive. When possible, the AN shall allocate the specified V5-time slot(s) to the specified port. After the reception of the MDU-BCC [Allocation response (complete)] primitive, the BCC protocol entity in the AN shall send to the LE the ALLOCATION COMPLETE message.

With the reception of a ALLOCATION COMPLETE message that, by the analysis of the BCC Reference Number information element, the LE considers as the answer to a ALLOCATION message previously sent, the LE shall stop timer Tbcc1, notify the resource management entity by the MDU-BCC (Allocation confirmation) primitive, and enter the "Bcc null" state.

If timer Tbcc1 expires for the first time prior to the reception of the ALLOCATION COMPLETE or ALLOCATION REJECT message, the LE shall retransmit the ALLOCATION message, restart timer Tbcc1 and remain in the "Bcc waiting allocation" state.

If timer Tbcc1 expires for the second time prior to the reception of the ALLOCATION COMPLETE or ALLOCATION REJECT message, the process shall be concluded, entering the "Bcc null" state. The event shall also be notified to the resource management entity by the MDU-BCC (Allocation error indication) primitive, for the proper maintenance action be taken.

17.5.3 Bearer channel allocation – Exceptional procedures

17.5.3.1 Bearer channel allocation

The BCC protocol entity in the LE, being in the NULL state and receiving an ALLOCATION COMPLETE message shall inform the resource management by issuing MDU-BCC (Allocation confirmation) and remain in the NULL state. This situation may occur due to loss of messages and expiry of layer 3 timers but retransmission of the message by layer 2. It is the responsibility of the resource manager to perform any necessary action.

17.5.3.2 Bearer channel allocation reject

When the controlling entity in the AN receives the ALLOCATION message, and the AN resource manager detects that the requested V5-time slot(s) can not be allocated to the identified port (and user port time slot if applicable) in the requested conditions the resource management entity shall generate a MDU-BCC [Allocation response (reject)] primitive, and the AN shall notify the event by the sending to the LE the ALLOCATION REJECT message, specifying within the Reject Cause information element the reason for this rejection.

With the reception of a ALLOCATION REJECT message that, by the analysis of the BCC Reference Number information element, the LE considers as the answer to a ALLOCATION message previously sent, the LE shall conclude the bearer channel allocation process, stop timer Tbcc1, notify the resource management entity by the MDU-BCC (Allocation reject) indication primitive, and enter the "Bcc null" state.

The BCC protocol entity in the LE, being in the NULL state and receiving an ALLOCATION REJECT message shall inform the resource management by issuing MDU-BCC (Allocation reject indication) and remain in the NULL state. This situation may occur due to loss of messages and expiry of layer 3 timers but retransmission of the message by layer 2. It is the responsibility of the resource manager to perform any necessary action.

17.5.3.3 Bearer channel allocation abort

While waiting for the reception of an ALLOCATION COMPLETE or ALLOCATION REJECT message, if the LE BCC protocol entity receives a MDU-BCC (De-allocation request) primitive requesting for the release of the bearer channel being established (for instance as a consequence of a premature call clearing), the LE shall proceed with the bearer channel de-allocation and shall stop timer Tbcc1, send the DE-ALLOCATION message and start timer Tbcc2 and enter the "Bcc allocation abort" state.

When in the "Bcc allocation abort" state, the LE shall discard any ALLOCATION COMPLETE or ALLOCATION REJECT message received.

When the BCC protocol entity in the AN receives the DE-ALLOCATION message, the event is notified to the resource management entity by a MDU-BCC (De-allocation indication) primitive, then the AN shall de-allocate the specified V5-time slot(s) from the relevant port, and send to the LE the DE-ALLOCATION COMPLETE message.

With the reception of a DE-ALLOCATION COMPLETE message that, by the analysis of the BCC Reference Number information element, the BCC controlling entity in the LE considers as the answer to a DE-ALLOCATION message previously sent, the event shall be notified to the resource management entity in the LE by a MDU-BCC (De-allocation confirmation) primitive, then timer Tbcc2 shall be stopped and the "Bcc null" state entered.

If timer Tbcc2 expires for the first time prior to the reception of the DE-ALLOCATION COMPLETE or DE-ALLOCATION REJECT message, the LE shall retransmit the DE-ALLOCATION message, restart timer Tbcc2 and remain in the "Bcc allocation abort" state.

If timer Tbcc2 expires for the second time prior to the reception of the DE-ALLOCATION COMPLETE or DE-ALLOCATION REJECT message, the procedure shall be concluded, entering the "Bcc null" state. The event shall also be notified to the resource management entity by a MDU-BCC (De-allocation error indication) primitive, for the proper maintenance action be taken.

17.5.3.4 Bearer channel allocation request received for existing connection

When the resource management entity at the AN receives an ALLOCATION message requesting a bearer channel allocation already set-up, the AN shall transmit an ALLOCATION COMPLETE message.

17.5.3.5 Bearer channel allocation, connection override requested

Under certain service circumstances (e.g. as a consequence of the DSS1 user port time slot negotiation at the called ISDN user network interface) the LE shall start a BCC bearer channel allocation process over a V5.2 interface V5-time slot already involved in a connection to the same user port. The LE will notify the request by means of the "override" indicator field contained in the V5-time slot identification information element of the transmitted ALLOCATION message.

When receiving an ALLOCATION message, containing an override request, the AN will proceed with the completion of the bearer channel completion overriding the previous connection sending an ALLOCATION COMPLETE message according to the normal procedure for the bearer channel allocation described in 17.5.2. In the event that the LE requests for the overriding of a connection that is not completed over the user port specified in the ALLOCATION message, the AN will reject the allocation procedure sending an ALLOCATION REJECT message according to the bearer channel allocation reject procedure described in 17.5.3.2.

17.5.4 Bearer channel de-allocation – Normal procedure

The resource management entity in the LE shall notify the need for a bearer channel to be de-allocated by a (MDU-BCC (De-allocation request) primitive. Then the BCC protocol entity in the LE, being in the "Bcc null" state, shall initiate the bearer channel de-allocation by sending to the AN a DE-ALLOCATION message indicating the V5-time slot(s) in the V5.2 interface to be released.

With the sending of the DE-ALLOCATION message the LE shall start timer Tbcc3 and enter the "Bcc waiting de-allocation" state.

When the BCC protocol entity in the AN receives the DE-ALLOCATION message, the event shall be notified to the resource management entity by a MDU-BCC (De-allocation indication) primitive. Then, the AN shall de-allocate the specified V5-time slot(s) from the relevant port, and send to the LE the DE-ALLOCATION COMPLETE message.

With the reception of a DE-ALLOCATION COMPLETE message that, by the analysis of the BCC Reference Number information element, the BCC protocol entity in the LE considers as the answer to a DE-ALLOCATION message previously sent, the event shall be notified by a MDU-BCC (De-allocation confirmation) primitive, then the LE shall stop timer Tbcc3 and enter the "Bcc null" state.

If timer Tbcc3 expires for the first time prior to the reception of the DE-ALLOCATION COMPLETE or DE-ALLOCATION REJECT message, the LE shall retransmit the DE-ALLOCATION message, restart timer Tbcc3 and remain in the "Bcc waiting de-allocation" state.

If timer Tbcc3 expires for the second time prior to the reception of the DE-ALLOCATION COMPLETE or DE-ALLOCATION REJECT message, the procedure shall be aborted, entering the "Bcc null" state. The event shall also be notified to the resource management entity by the MDU-BCC (De-allocation error) primitive, for the proper maintenance action be taken.

17.5.5 Bearer channel de-allocation – Exceptional procedures

17.5.5.1 Bearer channel de-allocation

The BCC protocol entity in the LE, being in the NULL state, and receiving a DE-ALLOCATION COMPLETE message shall inform the resource management by issuing MDU-BCC (De-allocation confirmation) and remain in the NULL state. This situation may occur due to loss of messages and expiry of layer 3 timers but retransmission of the message by layer 2. It is the responsibility of the resource manager to perform the necessary action.

17.5.5.2 Bearer channel de-allocation reject

After the reception of a DE-ALLOCATION message, when the resource management entity in the AN detects that the requested V5-time slot(s) can not be de-allocated from the identified port (and user port time slot if applicable), or can not be de-allocated on the conditions requested by the LE, a MDU-BCC [De-allocation response (reject)] primitive shall be generated, and the AN shall notify the event by the sending to the LE the DE-ALLOCATION REJECT message, specifying within the Reject Cause information element the reason for this rejection.

With the reception of a DE-ALLOCATION REJECT message that, by the analysis of the BCC Reference Number information element, the BCC protocol entity in the LE considers as the answer to a DE-ALLOCATION message previously sent, the LE shall conclude the bearer channel de-allocation procedure, stop timer Tbcc3, notify the resource management entity by a MDU-BCC (De-allocation reject indication) primitive, and enter the "Bcc null" state.

The BCC protocol entity in the LE, being in the NULL state, and receiving a DE-ALLOCATION REJECT message shall inform the resource management by issuing MDU-BCC (De-allocation reject indication) and remain in the NULL state. This situation may occur due to loss of messages and expiry of layer 3 timers but retransmission of the message by layer 2. It is the responsibility of the resource manager to perform the necessary action.

17.5.5.3 Bearer channel de-allocation process message missing

When the resource management entity at the AN receives a DE-ALLOCATION message, that refers to V5-time slot and port (and user port time slot when applicable) considered free, the AN shall transmit a DE-ALLOCATION COMPLETE message.

17.5.6 Audit procedure

The BCC protocol entity in the LE, being in the "Bcc null" state, when receiving the MDU-BCC (Audit request) primitive shall initiate the audit procedure by sending to the AN an AUDIT message indicating the single 64 kbit/s V5-time slot or user port and user port time slot, when applicable, on which the audit has to be done.

With the sending of the AUDIT message, the LE shall start timer Tbcc4 and enter the "Bcc waiting audit" state.

When the BCC protocol entity in the AN receives the AUDIT message, it shall notify the event to the resource management entity by the MDU-BCC (Audit indication) primitive. Then, the AN resource manager has to check the received information with its internal information regarding the established bearer channel connections in the AN. After this checking, the AN shall notify to the LE the bearer connection related to the information provided by the LE or the absence of connection matching the information provided by the LE. After the reception of the MDU-BCC (Audit response) primitive, the BCC protocol entity in the AN shall send to the LE the AUDIT COMPLETE message.

With the reception of a AUDIT COMPLETE message that, by the analysis of the BCC Reference Number information element, the LE considers as the answer to an AUDIT message previously sent, the LE shall stop timer Tbcc4, notify the resource management entity by the MDU-BCC (Audit confirmation) primitive, and enter the "Bcc null" state.

If timer Tbcc4 expires for the first time prior to the reception of the AUDIT COMPLETE message, the LE shall retransmit the AUDIT message, restart timer Tbcc4 and remain in the "Bcc waiting audit" state.

If timer Tbcc4 expires for the second time prior to the reception of the AUDIT COMPLETE message, the process shall be concluded, entering the "Bcc null" state. The event shall also be notified to the resource management entity by the MDU-BCC (Audit error indication) primitive, for the proper maintenance action be taken.

17.5.7 AN internal failure notification procedure

The BCC protocol entity in the AN, being in the "Bcc operational" state, when receiving the MDU-BCC (AN fault request) primitive shall initiate the AN internal failure notification procedure by sending to the LE an AN FAULT message indicating the single 64 kbit/s bearer connection affected by the AN internal failure, specifying the V5-time slot or user port and user port time slot, when applicable, or both.

With the sending of the AN FAULT message the AN shall start timer Tbcc5 and enter the "Bcc AN fault report" state.

When the BCC protocol entity in the LE receives the AN FAULT message, it shall notify the event to the resource management entity by the MDU-BCC (AN fault indication) primitive and shall send to the AN the AN FAULT ACKNOWLEDGE message.

With the reception of a AN FAULT ACKNOWLEDGE message that, by the analysis of the BCC Reference Number information element, the AN considers as the answer to an AN FAULT message previously sent, the AN shall stop timer Tbcc5, notify the resource management entity by the MDU-BCC (AN fault confirmation) primitive, and enter the "Bcc operational" state.

If timer Tbcc5 expires for the first time prior to the reception of the AN FAULT ACKNOWLEDGE message, the AN shall retransmit the AN FAULT message, restart timer Tbcc5 and remain in the "Bcc AN fault report" state.

If timer Tbcc5 expires for the second time prior to the reception of the AN FAULT ACKNOWLEDGE message, the process shall be concluded, entering the "Bcc operational" state. The event shall also be notified to the resource management entity by the MDU-BCC (AN fault error indication) primitive, for the proper maintenance action be taken.

17.5.8 Handling of error conditions

Before acting upon a message, the receiving entity, either the AN V5.2-BCC Protocol entity or the LE V5.2-BCC Protocol entity, shall perform the procedures specified in this subclause.

As a general rule, all messages shall contain, at least: the Protocol Discriminator, the BCC Reference Number and the Message Type information elements. These information elements, acting as a header for all BCC messages, are specified in 13.2. When receiving a message having less than 4 octets, the receiving BCC protocol entity in the AN or LE shall generate a MDU-BCC (Protocol error indication) primitive to the management system and ignore the message.

If more than three optional information elements are detected within a message, then the message shall be considered as too long and shall be truncated after the third optional information element. All the truncated information is assumed to be repeated optional information elements. When doing the truncation, the entity shall react according to 17.5.8.4 for repeated information elements.

Each receipt of a message, of the set of messages of the BCC Protocol, shall activate the checks described in 17.5.8.1 through 17.5.8.10 by order of precedence. No state change occurs during these checks.

After the message has been checked using the error handling procedures following, if the message is not to be ignored, then:

– bearer channel allocation procedures (see 17.5.2 and 17.5.3); or
– bearer channel de-allocation procedures (see 17.5.4 and 17.5.5); or
– audit procedure (see 17.5.6); or
– AN internal failure notification procedure (see 17.5.7) shall follow.

NOTE – Within this clause, the term "ignore the message" means to leave the message contents unchanged.

17.5.8.1 Protocol discriminator error

When a message is received by a layer 3 BCC protocol entity with a protocol discriminator coded other than the one specified in 13.2.1 for use in the V5 Protocols:

– the AN BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Protocol discriminator error";
– the LE BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system and ignore the message.

17.5.8.1a BCC Reference Number coding error

When a message is received by a layer 3 BCC protocol entity with a BCC Reference Number which is not coded as specified in clause 17.4.1; then:

– the AN BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "BCC Reference Number coding error";
– the LE BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system and ignore the message.

17.5.8.2 Message type error

Whenever an unrecognized message is received:

– the AN BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Message type unrecognized" including the corresponding diagnostic as specified in 17.4.2.6;

– the LE BCC protocol entity shall generate a MDU-BCC (Protocol error indication primitive) to the management system and ignore the message.

17.5.8.3 Information element out of sequence

An information element which has an information element identifier code value lower than the code value of the preceding information element shall be considered as an out of sequence information element.

Whenever an out of sequence information element is received:

– the AN BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system, remove the out of sequence information element and continue with the processing of the message, it shall also send a PROTOCOL ERROR message indicating the protocol error cause "Out of sequence information element" including the corresponding diagnostic as specified in 17.4.2.6;

– the LE BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system and remove the out of sequence information element and continue with the processing of the message.

If the removed information element is mandatory, this shall be reflected in a mandatory information element missing error situation that shall be treated according to 17.5.8.5.

17.5.8.4 Repeated mandatory information element

Whenever a mandatory information element is repeated in a message, the reaction of the receiving entity shall be as follows:

– the AN BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Repeated mandatory information element" including the corresponding diagnostic as specified in 17.4.2.6;

– the LE BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system and ignore the message.

NOTE – This clause applies also to conditional information elements that shall be handled as mandatory information elements (ALLOCATION and DE-ALLOCATION messages).

17.5.8.4a Repeated optional information element

Whenever an optional information element is repeated in a message the reaction of the receiving entity shall be as follows:

– the AN BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system, remove the repeated optional information element and continue with the processing of the message, it shall also send a PROTOCOL ERROR message indicating the protocol error cause "Repeated optional information element" including the corresponding diagnostic as specified in 17.4.2.6;

– the LE BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system and remove the repeated optional information element and continue with the processing of the message.

17.5.8.5 Mandatory information element missing

Whenever a message is received with a mandatory information element missing, the reaction of the receiving entity shall be as follows:

– the AN BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Mandatory information element missing" including the corresponding diagnostic as specified in 17.4.2.6;

– the LE BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system and ignore the message.

In the event of more than one mandatory information elements missing, the reaction of the receiving entity shall be on the basis of the first mandatory information element identified as missing.

NOTE – This clause applies also to conditional information elements that shall be handled as mandatory information elements (ALLOCATION and DE-ALLOCATION messages).

17.5.8.6 Unrecognized information element

Whenever a message is received with one or more information elements unrecognized, the reaction of the receiving entity shall be as follows:

– the AN BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system, remove all the unrecognized information elements and continue with the processing of the message, it shall also send a PROTOCOL ERROR message indicating the protocol error cause "Unrecognized information element" including the corresponding diagnostic as specified in 17.4.2.6;

– the LE BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system and remove all the unrecognized information elements and continue with the processing of the message.

In the event of more than one unrecognized information elements, the reaction of the receiving entity shall be on the basis of the first unrecognized information element identified.

For the purpose of the BCC protocol error handling procedures unrecognized information elements are those that are not defined within 13.2 and 17.4.

17.5.8.7 Content error of mandatory information element

When a message is received with a mandatory information element having a content error, either:

a) the length does not conform to the length specified in 13.2 and 17.4; or

b) the content is not known; then:

   – the AN BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Mandatory information element content error" including the corresponding diagnostic as specified in 17.4.2.6;

   – the LE BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system and ignore the message.

NOTE – This clause applies also to conditional information elements that shall be handled as mandatory information elements (ALLOCATION and DE-ALLOCATION messages).

17.5.8.8 Content error of optional information element

When a message is received with an optional information element having a content error, either:

a) the length does not conform to the length specified in 17.4; or

b) the content is not known or can not be interpreted; then:

- the AN BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system, remove the information element with a content error and continue with the processing of the message, it shall also send a PROTOCOL ERROR message indicating the protocol error cause "Optional information element content error" including the corresponding diagnostic as specified in 17.4.2.6;
- the LE BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system and remove the information element with a content error and continue with the processing of the message.

17.5.8.9 Unexpected message

A message flow error occurs when an unexpected message is received. The state transition tables give the appropriate action on receipt of any event.

Whenever an unexpected message is received no state change occurs, then:

- the AN BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Message not compatible with BCC protocol state" including the corresponding diagnostic as specified in 17.4.2.6;
- the LE BCC protocol entity shall generate a MDU-BCC (Protocol error indication) primitive to the management system and ignore the message.

17.5.8.10 Optional information element not allowed

When a message is received containing more optional information elements than needed, then:

- the AN BCC protocol entity shall generate a MDU-BCC (protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Too many information elements" including the corresponding diagnostic as specified in 17.4.2.6;
- the LE BCC protocol entity shall generate a MDU-BCC (protocol error indication) primitive to the management system and ignore the message.

17.6 List of system parameters (timers)

The definition of the timers used in the BCC protocol is given in Table 46. The mentioned timers are maintained in the LE or AN BCC protocol entity. The timer tolerances shall be ±10%.

Table 46/G.965 – BCC protocol timers

Timer number	Timeout value	State	Cause for start	Normal stop	At first expiry	At second expiry	Reference
Tbcc1	0.5 to 30 s (Note)	LE Bcc0 LE Bcc1	ALLOCATION sent	After reception of ALLOCATION COMPLETE, ALLOCATION REJECT, or an Allocation Abort Request	Repeat ALLOCATION and restart Tbcc1	Allocation process concluded and notify resource management	17.5.2
Tbcc2	2 s	LE Bcc1 LE Bcc2	DE-ALLOCATION sent	After reception of DE-ALLOCATION COMPLETE, or DE-ALLOCATION REJECT	Repeat DE-ALLOCATION and restart Tbcc2	De-allocation process concluded and notify resource management	17.5.3
Tbcc3	2 s	LE Bcc0 LE Bcc3	DE-ALLOCATION sent	After reception of DE-ALLOCATION COMPLETE, or DE-ALLOCATION REJECT	Repeat DE-ALLOCATION and restart Tbcc3	De-allocation process concluded and notify resource management	17.5.4
Tbcc4	500 to 1500 ms (Note)	LE Bcc0 LE Bcc4	AUDIT sent	After reception of AUDIT COMPLETE	Repeat AUDIT and restart Tbcc4	Audit process concluded and notify resource management	17.5.6
Tbcc5	500 to 1500 ms (Note)	AN Bcc0 AN Bcc1	AN FAULT sent	After reception of AN FAULT ACKNOWLEDGE	Repeat AN FAULT and restart Tbcc5	AN fault process concluded and notify resource management	17.5.7
NOTE – The sum of the values of Tbcc1 and the V5.1 PSTN protocol timer T1 shall not exceed 30 s. The Default value Tbcc1 shall be 1500 ms.							

17.7 LE side and AN side state transition tables

Table 47 defines the state transition table for one process at the LE side of the V5.2-BCC protocol entity.

Table 47/G.965 – LE state transition table

Event \ State	Bcc null (LEBcc0)	Bcc waiting allocation (LEBcc1)	Bcc allocation abort (LEBcc2)	Bcc waiting de-allocation (LEBcc3)	Bcc waiting audit (LEBcc4)
MDU-BCC (Allocation request)	ALLOCATION; Start Tbcc1; LEBcc1;	/	/	/	/
ALLOCATION COMPLETE	MDU-BCC (Allocation confirmation); –	MDU-BCC (Allocation confirmation); Stop Tbcc1; LEBcc0	–	/	/
ALLOCATION REJECT	MDU-BCC (Allocation reject indication); –	MDU-BCC (Allocation reject indication); Stop Tbcc1; LEBcc0	–	/	/

Table 47/G.965 – LE state transition table

State / Event	**Bcc null (LEBcc0)**	**Bcc waiting allocation (LEBcc1)**	**Bcc allocation abort (LEBcc2)**	**Bcc waiting de-allocation (LEBcc3)**	**Bcc waiting audit (LEBcc4)**
MDU-BCC (De-allocation request)	DE-ALLOCATION; Start Tbcc3; LEBcc3	DE-ALLOCATION; Stop Tbcc 1; Start Tbcc2; LEBcc2	/	/	/
DE-ALLOCATION COMPLETE	MDU-BCC (De-allocation confirmation); –	/	MDU-BCC (De-allocation confirmation); Stop Tbcc2; LEBcc0	MDU-BCC (De-allocation confirmation); Stop Tbcc3; LEBcc0	/
DE-ALLOCATION REJECT	MDU-BCC (De-allocation reject indication); –	/	MDU-BCC (De-allocation reject indication); Stop Tbcc2; LEBcc0	MDU-BCC (De-allocation reject indication); Stop Tbcc3; LEBcc0	/
MDU-BCC (Audit request)	AUDIT; Start Tbcc4; LEBcc4	/	/	/	/
AUDIT COMPLETE	/	/	/	/	MDU-BCC (Audit confirmation); Stop Tbcc4; LEBcc0
Expiry Tbcc1 (first)	/	ALLOCATION; Restart Tbcc1; –	/	/	/
Expiry Tbcc1 (second)	/	MDU-BCC (Allocation error indication); LEBcc0	/	/	/
Expiry Tbcc2 (first)	/	/	DE-ALLOCATION; Restart Tbcc2; –	/	/
Expiry Tbcc2 (second)	/	/	MDU-BCC (De-allocation error indication); LEBcc0	/	/
Expiry Tbcc3 (first)	/	/	/	DE-ALLOCATION; Restart Tbcc3; –	/
Expiry Tbcc3 (second)	/	/	/	MDU-BCC (De-allocation error indication); LEBcc0	/
Expiry Tbcc4 (first)	/	/	/	/	AUDIT; Restart Tbcc4; –

Table 47/G.965 – LE state transition table

State / Event	Bcc null (LEBcc0)	Bcc waiting allocation (LEBcc1)	Bcc allocation abort (LEBcc2)	Bcc waiting de-allocation (LEBcc3)	Bcc waiting audit (LEBcc4)
Expiry Tbcc4 (second)	/	/	/	/	MDU-BCC (Audit error indication); LEBcc0
AN FAULT	AN FAULT ACK; MDU-BCC (AN Fault indication); –	/	/	/	/
PROTOCOL ERROR	/	MDU-BCC (Protocol Error indication); stop Tbcc1; LEBcc0	MDU-BCC (Protocol error indication); stop Tbcc2; LEBcc0	MDU-BCC (Protocol error indication); stop Tbcc3; LEBcc0	MDU-BCC (Protocol error indication); stop Tbcc4; LEBcc0
– No state change / Unexpected event, no state change					

Table 48 defines the state transition table for one process at the AN side of the V5.2-BCC protocol entity.

Table 48/G.965 – AN state transition table

State / Event	Bcc operational (ANBcc0)	Bcc AN fault report (ANBcc1)
ALLOCATION	MDU-BCC (Allocation indication); ANBcc0	/
MDU-BCC [Allocation response (complete)]	ALLOCATION COMPLETE; ANBcc0	/
MDU-BCC [Allocation response (reject)]	ALLOCATION REJECT; ANBcc0	/
DE-ALLOCATION	MDU-BCC (De-allocation indication); ANBcc0	/
MDU-BCC [De-allocation response (complete)]	DE-ALLOCATION COMPLETE; ANBcc0	/
MDU-BCC [De-allocation response (reject)]	DE-ALLOCATION REJECT; ANBcc0	/
AUDIT	MDU-BCC (Audit indication); ANBcc0	/
MDU-BCC (audit response)	AUDIT COMPLETE; ANBcc0	/
MDU-BCC (AN fault request)	AN FAULT, Start Tbcc5; ANBcc1	/
AN FAULT ACKNOWLEDGE	/	MDU-BCC (AN fault confirmation), Stop Tbcc5; ANBcc0

Table 48/G.965 – AN state transition table

Event \ State	Bcc operational (ANBcc0)	Bcc AN fault report (ANBcc1)
Expiry Tbcc5 (first)	/	AN FAULT, Restart Tbcc5; ANBcc1
Expiry Tbcc5 (second)	/	MDU-BCC (AN fault error indication); ANBcc0
– No state change / Unexpected event, no state change		

18 Protection protocol specification

18.1 General

18.1.1 Introduction

A single V5.2 interface may consist of up to sixteen (16) 2048 kbit/s links. According to the protocol architecture and multiplexing structure (see clause 8) a communication path may carry information associated to several 2048 kbit/s links (non-associated information transfer). The failure of a communication path could therefore impact the service of a large number of customers in an unacceptable way. This is in particular true for the BCC protocol, the control protocol, and the link control protocol, where all user ports are affected in case of a failure of the relevant communication path.

In order to improve the reliability of the V5.2 interface, protection procedures for the switch-over of communication paths under failure are provided.

The protection mechanisms will be used to protect all active C-channels. The protection mechanism will also protect the protection protocol C-path (itself) which is used to control the protection switch-over procedures.

The protection protocol does not protect bearer channels, or allow the reconfiguration of bearer channels in the event of failure of their associated 2048 kbit/s link. In the event of such failures, customers connections on these bearer channels will fail. This is deemed acceptable, given the low predicted level of such failures. If a Data link failure was derived from 2048 kbit/s link or flag monitoring failure these causes shall have priority. The primary event for which protection is required is failure of 2048 kbit/s links. The protection protocol will also protect against persistent V5-data links failures (i.e. persistent failure of one of the data links for the control, link control, BCC, PSTN, or protection protocol). In addition flags shall be continuously monitored on all physical C-channels (active and standby C-channels) in order to protect against failures which are not already detected by Layer 1 detection mechanisms.

If a failure is detected on a standby C-channel the system management shall be notified and, as a result, shall not switch a logical C-channel to that non-operational standby C-channel. Other equipment failures (at other layers, or inside the AN or LE) will be dealt with separately, in the particular implementation, and are outside the scope of the V5 specification.

No protection for logical C-channels will be available in the single 2048 kbit/s link case. This implies that there will be no protection protocol on time slot 16 or any other physical C-channel, and during system startup the data link for protection will not be established.

As a result of a protection switch-over procedure layer 2 messages and/or layer 3 messages may get lost. It is the responsibility of the relevant layer 3 protocol entities to cover these situations.

This clause provides the principles and the specification of the protection protocol.

18.1.2 Provisioning of physical and logical C-channels

Mappings of C-path to logical C-channels shall be provisioned, in both the LE and the AN.

Initial mappings of logical C-channels to physical C-channels shall be provisioned, in both the LE and the AN.

The two C-paths for the protection protocol shall always be provisioned in time slots 16 of the primary and secondary links, and shall not be switched by the protection mechanism.

The control, link control, and BCC protocol C-paths will start up in time slot 16 of the Primary Link. Time slot 16 of the Secondary Link will be used for protection of the control, link control, and BCC protocol C-paths.

On frame transmission the protection protocol messages shall be given priority over other messages in the same physical C-channel. The contention resolution is based on the Envelope address, which is unique for protection protocol messages, giving priority to EFaddr = 8179.

Each V5.2 interface, consisting of more than one 2048 kbit/s link, shall have protection group 1 and, if provisioned, protection group 2.

Protection group 1 shall always consist of time slot 16 of the Primary and time slot 16 of the Secondary Link. Thus, for protection group 1 the following fixed values are used (refer to definitions):

N1 = 1; and

K1 = 1.

If protection group 2 is provisioned, N2 logical C-channels (and contained C-paths) will be provisioned, and a group of K2 standby C-channels will be provisioned with:

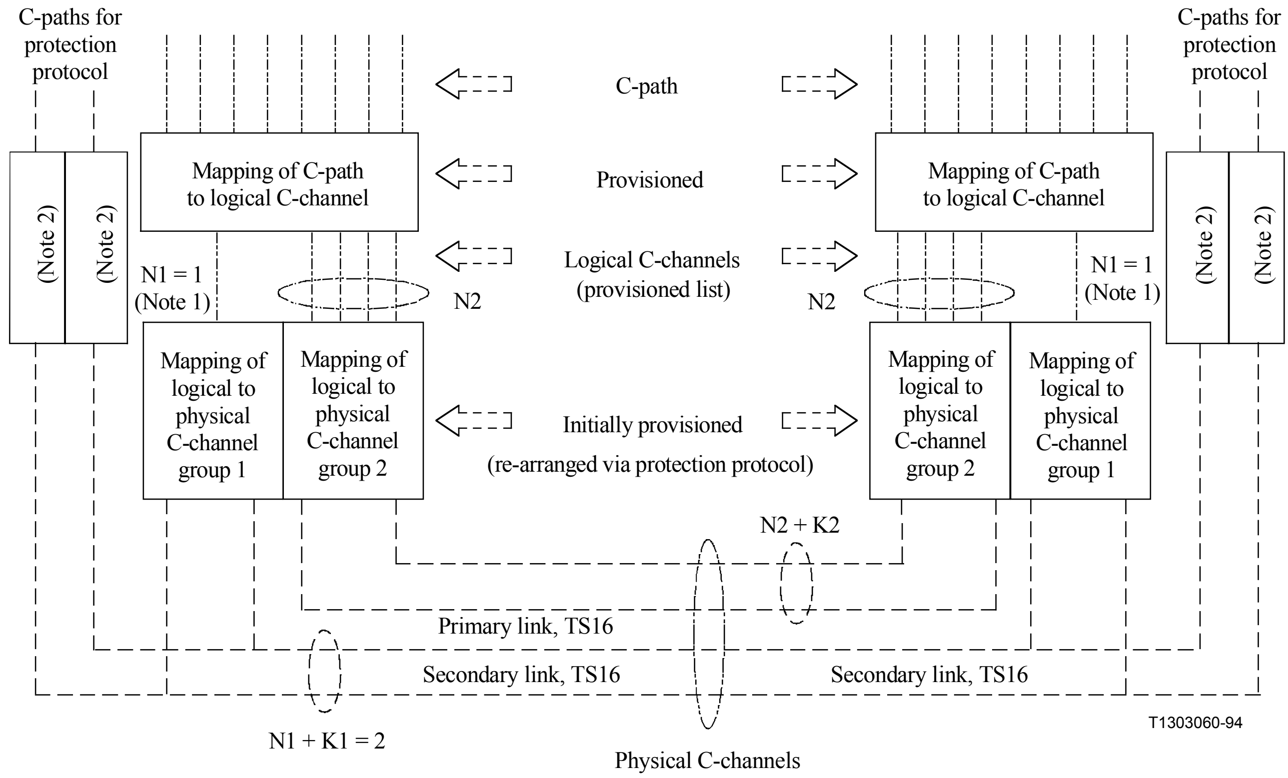
$1 \leq K2 \leq 3$; and

$1 \leq N2 \leq (3 \times L - 2 - K2)$,

where L is the number of 2048 kbit/s links on the V5.2 interface. K2 shall be chosen such, that it is equal to or greater than the maximum number of physical C-channels on any single 2048 kbit/s link of that V5.2 interface. For this rule time slots 16 of the Primary and Secondary links are not considered. This rule ensures that all active C-channels can be protected in case of a single 2048 kbit/s link failure.

NOTE – The network operator may provision no standby C-channel for protection group 2 (K2 = 0), if protection is not required for the logical C-channels of protection group 2. However, in that case some single 2048 kbit/s link failures may have impact on the services related to the failed logical C-channels.

Figure 25 shows the mapping of C-paths to logical C-channel, hence to physical C-channels.



NOTE 1 – Control protocol, link control and BCC protocol C-paths plus optionally other C-paths.

NOTE 2 – Allocation of C-path to physical C-channel.

Figure 25/G.965 – Mapping of C-paths to logical C-channels and hence to physical C-channels

18.1.3 Separation of responsibilities

A protection switch-over may either be triggered autonomously by the system management in the LE or AN as result of a fault detection or link blocking procedure, or by the operator(s) via the Q_{LE} and Q_{AN} interfaces. For protection group 1 the system management shall not allow switch-over initiated by the operator(s) via Q_{AN} or Q_{LE} interfaces.

The LE shall be the master for purposes of protection switching, in that the LE shall assign another physical C-channel to that logical C-channel.

The AN may request a switch-over of any one logical C-channel at any time. If the switch-over was initiated by the operator of the AN via Q_{AN} the operator may request switch-over to a preferred physical C-channel. The LE shall then comply with the request if possible. If no preference is given by the AN-side (this is always the case if failure is detected in AN and autonomous switch-over is initiated by the AN-system management) the LE system management will choose an available standby C-channel.

The AN may reject a protection switch-over command from LE, if for any reason it is unable to comply. If LE or AN cannot comply with the request this shall be notified via the Q_{LE} and Q_{AN} interface with cause.

18.1.4 Management of C-channel resources after failure

The LE system management shall decide which physical C-channel shall be used for protecting a logical C-channel. With respect to the management and control of the available resources the following rules shall be followed.

If protection switch-over is triggered autonomously by the system management in the LE or AN as result of a failure detection, active C-channels shall not be pre-empted in order to protect another logical C-channel. This principle shall also be applied to a switch-over initiated via the Q_{AN} interface.

Only the operator of the LE (via Q_{LE}) may request the allocation of a failed logical C-channel to an active C-channel (physical C-channel that already carries a logical C-channel). In this case a dedicated command shall be sent to the AN and the AN shall not reject switch-over due to the fact that a logical C-channel has already been allocated to this physical C-channel. The AN shall de-allocate the previously assigned logical C-channels and allocate the new logical C-channels, that shall be protected. The de-allocated logical C-channel shall then be protected by the normal protection mechanism as long as resources are available. This mechanism allows the operator of the LE to protect manually protocols with higher priority (e.g. PSTN protocol) in the case of multiple 2048 kbit/s link failures even in situations where the autonomous protection procedure was not successful due to a lack of resources (operational standby C-channels).

When protection is required, an available standby C-channel of the same protection group shall be chosen and used. If more than one standby C-channel is available the resource manager shall follow the following allocation sequence. First all available standby C-channels on time slots 16 shall be used, then time slots 15 shall be used, and finally time slots 31 shall be used. Once the link is restored all physical C-channel provisioned on that link will become standby C-channels (protection switching is not revertive).

In addition, re-provisioning would enable priority to be manually imposed, if necessary due to serious failure conditions (e.g. failure of the Primary and Secondary links). Services supported by the V5 interface are unavailable during reprovisioning of the V5 interface and system startup. Priority, manually imposed during initial provisioning, may change after a protection switch-over, e.g. as a result of a 2048 kbit/s link failure.

In case of a 2048 kbit/s link failure, the resource manager for the protection protocol shall first switch the logical C-channel in TS16, then the one in TS15 and then the one in TS31, as long as resources are still available. If not all logical C-channels can be switched to physical C-channels this shall be notified to the network operator via Q_{LE} and Q_{AN}.

Loss of protection, BCC, control, and link control C-paths, due to failure of both the Primary and Secondary 2048 kbit/s links, can only be overcome by re-provisioning onto another 2048 kbit/s link.

Switch-over actions shall be sequential, i.e. a second switch-over shall only be issued when the first one has been completed.

There shall be only one action invoked by one protection protocol message (e.g. switch logical C-channel X to standby C-channel Y).

A switch-over request from the AN or a switch-over command from the LE may only be either acknowledged or rejected by the peer entity. The reject message shall not include any alternative switch-over proposal. A new switch-over action may be initiated by either side as a result of a switch-over rejection.

18.1.5 Monitoring functions and detection of failures

The primary event for which protection is required is failure of 2048 kbit/s links.

In addition to Layer 1 monitoring, two other monitoring functions shall be used to detect C-channel failures and to trigger an autonomous protection switch-over. These methods are flag monitoring and data link monitoring.

18.1.5.1 Failure of a 2048 kbit/s link

On receipt of a MDU-DI primitive from the link control FSM in the AN or LE (see 16.1) or if the link is blocked in AN or LE (see 16.2), the system management in the AN or LE shall trigger an autonomous switch-over for all active C-channels on that 2048 kbit/s link.

18.1.5.2 Flag monitoring

Flags shall be continuously monitored on both active and standby C-channels.

If no flag is received on a physical C-channel for a time period of 1 second, the physical C-channel shall be regarded as non-operational and an error indication shall be issued to the system management. This condition shall be notified continuously, at a rate of one per second, to the system management as long as the situation persists.

If at least one flag is received on a physical C-channel during a time period of 1 second the physical C-channel shall be regarded as operational.

18.1.5.3 Data link monitoring

Data Link (Layer 2) monitoring will be used in the AN and in the LE on those channels carrying C-paths where there is a full V5-data link terminated in the AN (i.e. protection, control, link control, BCC, and PSTN-protocols).

Data link failure (see C.17), if not already handled by 18.1.5.1 and 18.1.5.2 respectively, shall be a trigger for protection switch-over.

If a MDL-RELEASE-INDICATION is received by the system management as result of a failure in the C-path that has caused the switch-over, no further switch-over shall be initiated by the relevant system management unless a MDL-ESTABLISH-INDICATION or MDL-ESTABLISH-CONFIRM has been received in the meantime. This means that the data link FSM of the failed C-path shall first enter the Multiple-frame-established state (at least once) before a second switch-over shall be performed triggered by the receipt of a MDL-RELEASE indication primitive. Otherwise it is assumed that an internal failure has occurred from which recovery is not possible with the V5-protection mechanism. In this case the system management shall initiate appropriate actions.

18.1.6 Functional model for the protection protocol

One independent data link will be permanently established on each TS16 of the Primary and Secondary Link. The procedures for the data link layer are specified in 10.4.

The EFaddr and the corresponding V5DLaddr for the protection protocol in TS16 of the Primary link and TS16 of the Secondary link shall have the same value and shall be coded according to 9.2 and 10.3.2.3.

The two data links are used to convey information between the protection protocol entities in the AN and LE. Each L3 message shall be broadcast over both data links. The peer Layer 3 entity receiving the messages from both data links shall process the message on its first occurrence and shall then ignore the identical message received via the other data link. Sequence numbers shall be used to distinguish between a message that was received for the first time and a message that has already been received via the other data link.

On detection of a failure, which makes protection switching necessary, the LE or AN-system management shall invoke a switch-over using Management Data Units (MDUs).

The Q_{AN} and Q_{LE} interfaces will be notified in the event of a protection switch-over, giving the current status of the affected logical and physical C-channels.

The operation systems of the LE and the AN may retrieve the current mapping of logical C-channels to physical C-channels on request via Q_{AN} and Q_{LE}.

Figure 26 shows the functional model for the protection protocol.

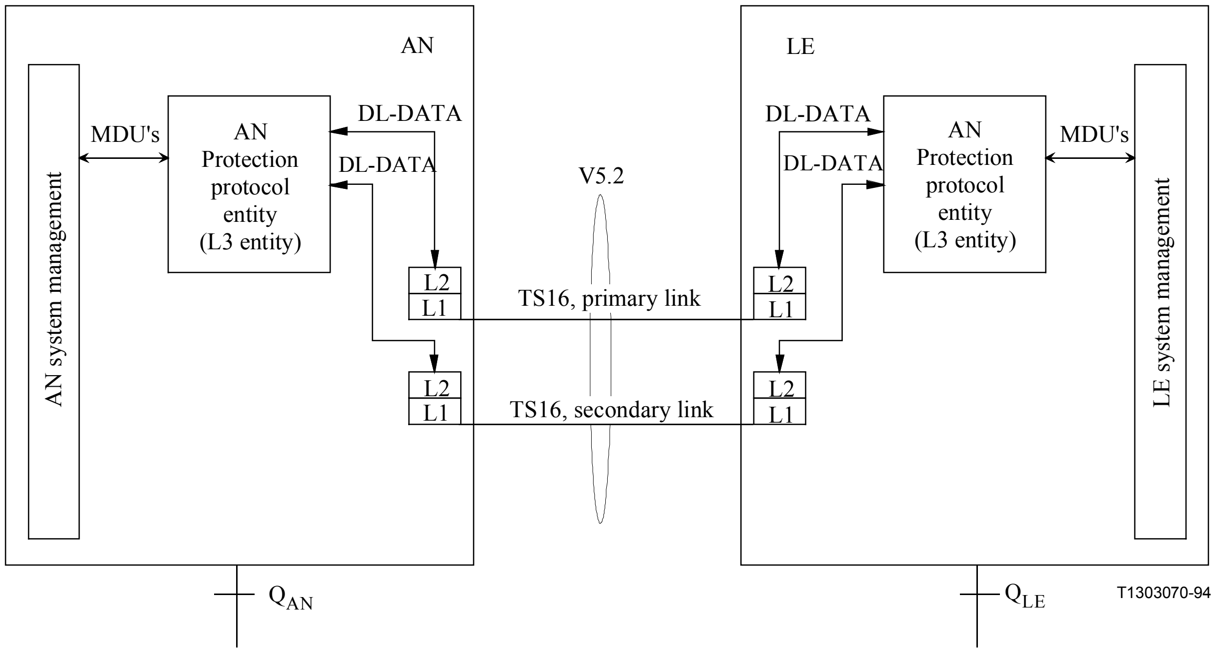


Figure 26/G.965 – Functional model for the protection protocol

18.2 Other principles

Protection switching shall effectively be done on a logical C-channel basis, i.e. no change of the C-path to logical C-channel allocation due to protection switching.

When protecting a logical C-channel, all C-paths of that logical C-channel leave the active C-channel and are switched to a single standby C-channel.

Whether the implementation switches the logical C-channels or the individual C-paths of a logical C-channel is outside the scope of this Recommendation.

After switch-over of a logical C-channel the following LAPV5 data links shall be re-established, if they are carried on that logical C-channel: BCC, link control, control, and PSTN protocol. The protection protocol data links shall not be re-established automatically after switch-over. Re-establishment of a protection protocol data link shall only be attempted in the case of failure of that data link.

18.3 Protection protocol entity definition

18.3.1 Definition of protection protocol states

18.3.1.1 States in the AN

NULL state (SOAN0)

Switch-over has neither been initiated by AN-side nor by LE-side.

SWITCH-OVER REQUESTED BY AN state (SOAN1)

Switch-over has been requested by AN system management through a dedicated Management Data Unit (MDU).

SWITCH-OVER INITIATED BY LE state (SOAN2)

A SWITCH-OVER COM or OS-SWITCH-OVER COM message has been received from the LE-side. The AN system management has now to decide whether switch-over is possible or not.

18.3.1.2 States in the LE

NULL state (SOLE0)

Switch-over has neither been initiated by AN-side nor by LE-side.

SWITCH-OVER INITIATED BY LE state (SOLE1)

Switch-over has been requested by LE system management through a dedicated MDU.

SWITCH-OVER REQUESTED BY AN state (SOLE2)

A SWITCH-OVER REQ message has been received from the AN-side. The LE system management has now to decide whether switch-over is possible or not.

18.3.2 Definition of protection protocol events

Tables 49 and 50 define the MDUs, messages and timers used in the AN and LE protection FSM.

Table 49/G.965 – MDUs, messages and timers used in the AN-protection FSM

	Direction	Description
MDU-Protection (switch-over req)	PROTECT_AN ← SYS	The system management has detected a failure and requests switch-over, a switch-over was initiated by the OS-AN via Q_{AN}.
MDU-Protection (switch-over ack)	PROTECT_AN ← SYS	The system management acknowledges a switch-over in the AN.
MDU-Protection (switch-over reject; cause)	PROTECT_AN ← SYS	The system management rejects a switch-over and indicates the cause.

Table 49/G.965 – MDUs, messages and timers used in the AN-protection FSM

	Direction	Description
MDU-Protection (switch-over com)	PROTECT_AN → SYS	The Protection protocol entity has received a switch-over command from the LE.
MDU-Protection (OS-switch-over com)	PROTECT_AN → SYS	The Protection protocol entity has received a switch-over command from the OS-LE.
MDU-Protection (switch-over reject ind; cause)	PROTECT_AN → SYS	The Protection protocol entity indicates the receipt of a switch-over reject message to the system management and indicates the cause.
MDU-Protection (switch-over error ind)	PROTECT_AN → SYS	The Protection protocol entity indicates the expiry of timer TSO3 to the system management.
MDU-Protection (reset SN com)	PROTECT_AN → SYS	The protection protocol entity indicates to the system management that reset of SN has been initiated.
MDU-Protection (reset SN ind)	PROTECT_AN → SYS	The protection protocol entity indicates the receipt of a RESET SN COM message to the system management.
MDU-Protection (reset SN ack)	PROTECT_AN → SYS	The protection protocol entity indicates to the system management that reset of SN has been acknowledged by the peer entity.
MDU-Protection (reset SN error ind)	PROTECT_AN → SYS	An error with the SN reset procedure is indicated by the protection protocol entity to the system management.
SWITCH-OVER COM	PROTECT_AN←PROTECT_LE	Initiation by LE to switch-over.
OS-SWITCH-OVER COM	PROTECT_AN←PROTECT_LE	Initiation by OS-LE to switch-over.
SWITCH-OVER REQ	PROTECT_AN→PROTECT_LE	Request by AN to switch-over.
SWITCH-OVER ACK	PROTECT_AN→PROTECT_LE	Positive response to a switch-over command.
SWITCH-OVER REJECT (Cause)	PROTECT_AN↔PROTECT_LE	Rejection of a switch-over command with cause.
RESET SN COM	PROTECT_AN↔PROTECT_LE	Reset sequence number command.
RESET SN ACK	PROTECT_AN↔PROTECT_LE	Acknowledgement that state variables have been reset.
PROTOCOL ERROR	PROTECT_AN→PROTECT_LE	Used by AN to indicate to the LE about protocol error.

Table 49/G.965 – MDUs, messages and timers used in the AN-protection FSM

	Direction	Description
MDU-Protection (Protocol error indication)	PROTECT_AN → SYS	Protocol error detected by the error handling procedure.
expiry TSO3	AN internal	Timer TSO3 has expired.
expiry TSO4	AN internal	Timer TSO4 has expired.
expiry TSO5	AN internal	Timer TSO5 has expired.
PROTECT_AN Protection protocol entity in the AN PROTECT_LE Protection protocol entity in the LE SYS System management		

Table 50/G.965 – MDUs, messages and timers used in the LE-protection FSM

	Direction	Description
MDU-Protection (switch-over com)	PROTECT_LE ← SYS	The system management has detected a failure and initiates switch-over, or the switch-over was initiated either by the OS-LE via Q_{LE} or by the AN via V5.2.
MDU-Protection (OS-switch-over com)	PROTECT_LE ← SYS	The OS-LE has initiated a switch-over, this command may cause pre-emption of a Physical C-channel which currently carries a Logical C-channel.
MDU-Protection (switch-over ack)	PROTECT_LE → SYS	The Protection protocol entity indicates the receipt of a positive switch-over response from the AN to the system management.
MDU-Protection (switch-over reject; cause)	PROTECT_LE ← SYS	The system management rejects a switch-over and indicates the cause.
MDU-Protection (switch-over req)	PROTECT_LE → SYS	The Protection protocol entity indicates the receipt of a switch-over request from the AN to the system management.
MDU-Protection (switch-over reject ind)	PROTECT_LE → SYS	The Protection protocol entity indicates the receipt of a switch-over reject message to the system management.
MDU-Protection (switch-over error ind)	PROTECT_LE → SYS	The Protection protocol entity indicates the expiry of timer TSO1 to the system management.
MDU-Protection (reset SN ind)	PROTECT_LE → SYS	The Protection protocol entity indicates the receipt of a RESET SN COM message.
MDU-Protection (reset SN com)	PROTECT_LE → SYS	The Protection protocol entity indicates to the system management that reset of SN has been initiated.

Table 50/G.965 – MDUs, messages and timers used in the LE-protection FSM

	Direction	Description
MDU-Protection (reset SN req)	PROTECT_LE ← SYS	The system management initiates reset of SN during system startup procedure.
MDU-Protection (reset SN ack)	PROTECT_LE → SYS	The Protection protocol entity indicates to the system management that reset of SN has been acknowledged by the peer entity.
MDU-Protection (reset SN error ind)	PROTECT_LE → SYS	An error with the rest procedure is indicated to the system management.
MDU-Protection (Protocol error indication)	PROTECT_LE → SYS	Protocol error detected by the error handling procedure.
SWITCH-OVER COM	PROTECT_LE→ PROTECT_AN	Initiation by LE to switch-over.
OS-SWITCH-OVER COM	PROTECT_LE→ PROTECT_AN	Initiation by OS-LE to switch-over, pre-emption of Active C-channel may be necessary.
SWITCH-OVER REQ	PROTECT_LE← PROTECT_AN	Request by AN to switch-over.
SWITCH-OVER ACK	PROTECT_LE← PROTECT_AN	Positive response to a switch-over command.
SWITCH-OVER REJECT (Cause)	PROTECT_LE↔ PROTECT_AN	Rejection of a switch over command with cause.
PROTOCOL ERROR	PROTECT_LE← PROTECT_AN	Protocol error detected by the error handling procedure in AN, indication is given to LE side.
RESET SN COM	PROTECT_LE↔ PROTECT_AN	Reset sequence number command.
RESET SN ACK	PROTECT_LE↔ PROTECT_AN	Acknowledgement that state variables have been reset.
expiry TSO1	LE internal	Timer TSO1 has expired.
expiry TSO2	LE internal	Timer TSO2 has expired.
expiry TSO4	LE internal	Timer TSO4 has expired.
expiry TSO5	LE internal	Timer TSO5 has expired.
PROTECT_AN Protection protocol entity in the AN PROTECT_LE Protection protocol entity in the LE SYS System management		

18.4 Protection protocol message definition and content

The complete set of messages for the protection protocol is given in Table 51. This clause gives the detailed message structure for each of these messages.

Table 51/G.965 – Set of protection protocol messages

Coding within the message type information element							Messages of the protection protocol	Reference
7	6	5	4	3	2	1		
0	0	1	1	0	0	0	SWITCH-OVER REQ	18.4.1
0	0	1	1	0	0	1	SWITCH-OVER COM	18.4.2
0	0	1	1	0	1	0	OS-SWITCH-OVER COM	18.4.3
0	0	1	1	0	1	1	SWITCH-OVER ACK	18.4.4
0	0	1	1	1	0	0	SWITCH-OVER REJECT	18.4.5
0	0	1	1	1	0	1	PROTOCOL ERROR	18.4.6
0	0	1	1	1	1	0	RESET SN COM	18.4.7
0	0	1	1	1	1	1	RESET SN ACK	18.4.8

18.4.1 SWITCH-OVER REQ message

This message is used by the AN to request a switch-over of a logical C-channel to a particular physical C-channel. The message includes a proposal for the allocation of the failed logical C-channel to a new physical C-channel.

The SWITCH-OVER REQ message content is defined in Table 52.

Table 52/G.965 – SWITCH-OVER REQ message content

Message Type: SWITCH-OVER REQ

Direction: AN to LE

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	AN to LE	M	1
Logical C-channel identification	18.5.1	AN to LE	M	2
Message Type	13.2.3	AN to LE	M	1
Sequence Number	18.5.2	AN to LE	M	3
Physical C-channel identification	18.5.3	AN to LE	M	4

18.4.2 SWITCH-OVER COM message

This message is used by the LE to initiate a switch-over of a logical C-channel to a particular physical C-channel. The message includes the new allocation of the logical C-channel to the particular standby C-channel which shall carry the logical C-channel after successful switch-over.

The SWITCH-OVER COM message content is defined in Table 53.

Table 53/G.965 – SWITCH-OVER COM message content

Message Type: SWITCH-OVER COM

Direction: LE to AN

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	LE to AN	M	1
Logical C-channel identification	18.5.1	LE to AN	M	2
Message Type	13.2.3	LE to AN	M	1
Sequence Number	18.5.2	LE to AN	M	3
Physical C-channel identification	18.5.3	LE to AN	M	4

18.4.3 OS-SWITCH-OVER COM message

This message is used by the LE to initiate a switch-over of a logical C-channel to a particular physical C-channel on request of the operator via Q_{LE}. The message includes the new allocation of the logical C-channel to a particular physical C-channel which shall carry the logical C-channel after successful switch-over.

The OS-SWITCH-OVER COM message content is defined in Table 54.

Table 54/G.965 – OS-SWITCH-OVER COM

Message Type: OS-SWITCH-OVER COM

Direction: LE to AN

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	LE to AN	M	1
Logical C-channel identification	18.5.1	LE to AN	M	2
Message Type	13.2.3	LE to AN	M	1
Sequence Number	18.5.2	LE to AN	M	3
Physical C-channel identification	18.5.3	LE to AN	M	4

18.4.4 SWITCH-OVER ACK message

This message is used by the AN to acknowledge a switch-over of a logical C-channel to a particular physical C-channel as the result of a switch-over command received from the LE.

The SWITCH-OVER ACK message content is defined in Table 55.

Table 55/G.965 – SWITCH-OVER ACK

Message Type: SWITCH-OVER ACK

Direction: AN to LE

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	AN to LE	M	1
Logical C-channel identification	18.5.1	AN to LE	M	2
Message Type	13.2.3	AN to LE	M	1
Sequence Number	18.5.2	AN to LE	M	3
Physical C-channel identification	18.5.3	AN to LE	M	4

18.4.5 SWITCH-OVER REJECT message

This message is used by the AN or the LE to indicate to the peer entity that switch-over cannot be performed.

The SWITCH-OVER REJECT message content is defined in Table 56.

Table 56/G.965 – SWITCH-OVER REJECT

Message Type: SWITCH-OVER REJECT

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	Both	M	1
Logical C-channel identification	18.5.1	Both	M	2
Message Type	13.2.3	Both	M	1
Sequence Number	18.5.2	Both	M	3
Physical C-channel identification	18.5.3	Both	M	4
Rejection Cause	18.5.4	Both	M	3

18.4.6 PROTOCOL ERROR message

This message is used by the AN to indicate to the LE side that a protocol error has been identified in a received message. A protocol error cause is given.

The PROTOCOL ERROR message content is defined in Table 57.

Table 57/G.965 – PROTOCOL ERROR

Message Type: PROTOCOL ERROR

Direction: AN to LE

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	AN to LE	M	1
Logical C-channel identification	18.5.1	AN to LE	M	2
Message Type	13.2.3	AN to LE	M	1
Sequence Number	18.5.2	AN to LE	M	3
Protocol Error Cause	17.5.5	AN to LE	M	3 to 5

18.4.7 RESET SN COM message

This message is used by the LE or AN to indicate to the peer entity that a misalignment of send and receive state variables on the sending and receiving side has occurred and that all state variables shall be set to Zero.

The RESET SN COM message content is defined in Table 58.

Table 58/G.965 – RESET SN COM

Message Type: RESET SN COM

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	Both	M	1
Logical C-channel identification	18.5.1	Both	M	2
Message Type	13.2.3	Both	M	1

18.4.8 RESET SN ACK message

This message is used by the LE or AN to acknowledge to the peer entity that the send and receive state variables have been set to Zero.

The RESET SN ACK message content is defined in Table 59.

Table 59/G.965 – RESET SN ACK

Message Type: RESET SN ACK

Direction: Both

Information element	Reference	Direction	Type	Length
Protocol Discriminator	13.2.1	Both	M	1
Logical C-channel identification	18.5.1	Both	M	2
Message Type	13.2.3	Both	M	1

18.5 Protection protocol information element definition, structure and coding

This clause defines the coding of the information elements that are specific for the protection protocol messages. For each of the information elements, the coding of their different fields is provided.

All protection protocol specific information elements, except the logical C-channel identification information element, are listed in Table 60, which also gives the coding of the information element identifier.

Table 60/G.965 – Protection protocol specific information elements

Information element coding								Messages of the protection protocol	Reference
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**		
0	–	–	–	–	–	–	–	VARIABLE LENGTH	
0	1	0	1	0	0	0	0	Sequence number	18.5.2
0	1	0	1	0	0	0	1	Physical C-channel identification	18.5.3
0	1	0	1	0	0	1	0	Rejection cause	18.5.4
0	1	0	1	0	0	1	1	Protocol error cause	18.5.5
NOTE – All other values are reserved.									

18.5.1 Logical C-channel identification information element

Both the AN and LE side shall maintain a provisioned list of logical C-channels. A logical C-channel is uniquely identified by a dedicated logical C-channel identification number.

The logical C-channel identification number shall have a length of 16 bit and shall be coded in binary. All numbers from 0 to 65535 shall be valid. Up to 44 different logical C-channel identification numbers may be provisioned for a single V5.2 interface.

NOTE – The value 44 corresponds to the maximum number of logical C-channels on a V5.2 interface. It is equal to the maximum number of physical C-channels ($= 3 \times 16 = 48$) minus 1 standby C-channel for protection group 1 and minus 3 standby C-channels for protection group 2 ($48 - 1 - 3 = 44$).

The length of the logical C-channel identification information element shall be 2 octets.

In the RESET SN COM and RESET SN ACK messages the value of the logical C-channel identification shall be 0 (i.e. all bits shall be set to Zero).

The coding of the logical C-channel identification information element shall be according to Figure 27.

8	7	6	5	4	3	2	1	Octets
Logical C-channel identification (upper)								1
Logical C-channel identification (lower)								2

Figure 27/G.965 – Logical C-channel identification information element

18.5.2 Sequence-number information element

The sequence number information element is used by the receiving side to distinguish between a message received for the first time and a message that has already been received via the other data link for the protection protocol.

The length of this information element shall be 3 octets.

The sequence number information element contains a 7-bit sequence number field. The sequence number is coded in binary and may have values from 0 up to 127.

The coding of this information element shall be according to Figure 28.

8	7	6	5	4	3	2	1	Octets
	Information element identifier							
0	1	0	1	0	0	0	0	1
Length of sequence number content								2
ext. 1	Sequence number							3

Figure 28/G.965 – Sequence number information element

18.5.3 Physical C-channel identification information element

This information element identifies the time slot within a V5.2 interface which is assigned to a particular physical C-channel. The system management in the LE shall ensure that only those time slots provisioned as physical C-channels shall be referred to in this information element.

The length of the Physical C-channel identification information element shall be 4 octets.

The structure of the Physical C-channel identification information element shall be as indicated by Figure 29.

8	7	6	5	4	3	2	1	Octets
	Information element identifier							
0	1	0	1	0	0	0	0	1
Length of the information element content								2
V5 2048 kbit/s link Identifier								3
0	0	0	V5-Time Slot Number					4

Figure 29/G.965 – Physical C-channel identification information element

The V5 2048 kbit/s link Identifier is a field of eight bits used for providing the binary coding that identifies a particular 2048 kbit/s link out of those that comprise the V5.2 interface, where the selected V5-time slot to be used as the physical C-channel is located. A maximum of 256 (2048 kbit/s links) can be explicitly identified.

The V5-Time Slot Number is a field of five bits used for providing the binary coding that identifies the V5-time slot (within the 2048 kbit/s link identified in the previous octet) to be used as the physical C-channel.

18.5.4 Rejection Cause information element

The purpose of the Rejection Cause information element is to indicate to the peer entity the reason for which the switch-over of a particular logical C-channel to another physical C-channel has been rejected.

The length of the Rejection Cause information element shall be 3 octets.

The coding of the Rejection Cause information element shall be according to Figure 30.

8	7	6	5	4	3	2	1	Octets
	Information element identifier							
0	1	0	1	0	0	0	0	1
Length of the Rejection Cause information element content								2
ext. 1	Rejection Cause type							3

Figure 30/G.965 – Rejection Cause information element

Table 61 provides the complete list of rejection cause types and the corresponding codings. The table also indicates for which directions the rejection cause type may be used.

Table 61/G.965 – Coding of the rejection cause type field

7	6	5	4	3	2	1	Meaning	Direction
0	0	0	0	0	0	0	No standby C-channel available	LE to AN
0	0	0	0	0	0	1	Target physical C-channel not operational	Both
0	0	0	0	0	1	0	Target physical C-channel not provisioned	Both
0	0	0	0	0	1	1	Protection switching impossible (AN/LE failure)	Both
0	0	0	0	1	0	0	Protection group mismatch	Both
0	0	0	0	1	0	1	Requested allocation exists already	Both
0	0	0	0	1	1	0	Target physical C-channel already has logical C-channel	Both
NOTE – All other values are reserved.								

18.5.5 Protocol Error Cause information element

The purpose of the Protocol Error Cause information element is to indicate from the AN to the LE the type of protocol error detected in a given process.

The Protocol Error Cause information element, for some protocol error cause types shall include a diagnostic field in order to provide additional information related to these protocol error cause types. This diagnostic field of one or two octets, when present, shall be a copy of the received message type identifier that has triggered the sending of the message containing the Protocol Error Cause information element, and when needed, the relevant information element identifier within that message.

The length of the Protocol Error Cause information element may be from 3 through 5 octets. For protocol error cause types not including a diagnostic information, the length of the information element shall be 3 octets. For protocol error types including a diagnostic information, the length of the information element shall be 4 or 5 octets.

The structure of the Protocol Error Cause information element shall be as indicated by Figure 31.

8	7	6	5	4	3	2	1	Octets
0	Information element identifier 1	0	1	0	0	1	1	1
Length of the information element content								2
1	Protocol Error Cause type							3
0	Diagnostic (Message type identifier)							4
Diagnostic (Information element identifier)								5

Figure 31/G.965 – Protocol Error Cause information element

A field of seven bits is used to specify the protocol error cause type as specified in Table 62.

Table 62/G.965 – Coding of the protocol error cause type

7	6	5	4	3	2	1	Protocol error cause type
0	0	0	0	0	0	1	Protocol discriminator error
0	0	0	0	1	0	0	Message type unrecognized
0	0	0	0	1	1	1	Mandatory information element missing
0	0	0	1	0	0	0	Unrecognized information element
0	0	0	1	0	0	1	Mandatory information element content error
0	0	0	1	0	1	1	Message not compatible with protection protocol state
0	0	0	1	1	0	0	Repeated mandatory information element
0	0	0	1	1	0	1	Too many information elements
0	0	0	1	1	1	1	Logical C-Channel identification error
NOTE – All other values are reserved.							

Clause 18.6.6 specifies when to use the different protocol error cause type values.

The diagnostic field is a field of multiple octets (number of octets dependent of the cause value) providing the relevant diagnostic for each protocol error cause value according to Table 63.

Table 63/G.965 – Diagnostic field for the protocol error types

Cause	Diagnostic	Length
Protocol discriminator error	Not present	0
Logical C-Channel identification error	Not present	0
Message type unrecognized	Message type identifier	1
Mandatory information element missing	Message type identifier Information element identifier	2
Unrecognized information element	Message type identifier Information element identifier	2
Mandatory information element content error	Message type identifier Information element identifier	2
Message not compatible with protection protocol state	Message type identifier	1
Repeated mandatory information element	Message type identifier Information element identifier	2
Too many information elements	Message type identifier	1

18.6 Protection protocol procedures

18.6.1 General

The protection protocol is a functional protocol. Both, a switch-over request from the AN-side and a switch-over command from the LE-side are explicitly acknowledged by the peer entities either by SWITCH-OVER COM or by SWITCH-OVER ACK messages, respectively. The receipt of an acknowledgement shall be supervised by timers. On the first expiry of a timer without acknowledgement from the peer entity, the message shall be retransmitted. On the second expiry an error indication shall be given to the system management and the protection protocol entity shall enter the NULL state without retransmitting the message again. The system management has then the responsibility to take the necessary maintenance actions.

It is the responsibility of the LE system management to control to which physical C-channel a logical C-channel shall be allocated to by means of the protection protocol. The LE system management derives this information either autonomously from the protection resource manager in the LE system management in case of a failure detected by the LE, or this information is provided by the operator of the LE via Q_{LE}.

If the switch-over is initiated by the operator via Q_{LE} and if the operator has decided that pre-emption of an active C-channel is required, then LE system management shall indicate this to the protection protocol entity with a dedicated primitive [MDU-Protection (OS-switch-over com)]. Pre-emption shall not be used for protection group 1.

The AN system management may initiate a switch-over due to the detection of an internal failure or triggered by the operator of the OS via Q_{AN}. The operator may indicate a preference for a standby C-channel to be used.

On receipt of a MDU-Protection (switch-over com) or MDU-Protection (OS-switch-over com) primitive the AN system management shall only verify whether the required resources for switch-over are available or not. The result of that verification shall be indicated to the LE by a SWITCH-OVER ACK or SWITCH-OVER REJECT message. This means, that the successful switch-over, itself, will not be acknowledged. If problems with switch-over are identified later by either side a new switch-over action has to be initiated.

18.6.2 Broadcast of protection protocol messages on the two data links of the primary and secondary link

18.6.2.1 Transmission of protection protocol messages

The protection protocol entities in the AN and LE shall pass every protection protocol message via DL-DATA primitives to the corresponding data link layers in time slots 16 of the Primary and Secondary link. Each protection protocol entity shall have a send state variable VP(S). After system start-up, the send state variable VP(S) shall be set to zero. Whenever a protection protocol message, containing a sequence number information element, shall be sent, the Sequence Number (SN) within the sequence number information element shall be set equal to the send state variable on the sending side. The message is then issued to the two data link entities via DL-DATA primitives and the send state variable on the sending side shall be incremented by one modulus 128.

NOTE – SN and VP(S) may have values from 0 through 127 and the modulus is 128.

18.6.2.2 Receipt of protection protocol messages

Each protection protocol entity shall have a receive state variable VP(R). VP(R) denotes the sequence number of the next in-sequence message expected to be received. After system start-up, the receive state variable VP(R) shall be set to zero.

A message received by a layer 3 protection protocol entity shall be checked first by the error handling procedure specified in 18.6.6.

If the protection protocol message contains a sequence number information element, the protection protocol entity of the receiving side shall decide on the basis of SN in conjunction with the receive state variable VP(R) whether this message has already been received via the other data link, whether it is a new valid message received for the first time, or whether there is a misalignment between send and receive state variables on the sending and receiving side, respectively.

NOTE 1 – VP(R) may have values from 0 through 127 and the modulus is 128.

The receiving side shall:

– ignore the message, if SN is in the range $VP(R) - 5 \leq SN \leq VP(R) - 1$, without notification to the system management;
– regard the message as a valid new message, if SN is in the range $VP(R) \leq SN \leq VP(R) + 4$. In this case VP(R) shall first be set equal to SN and shall then be incremented by one modulus 128;
– otherwise, the receiving side shall assume that there is a misalignment between the state variables on the sending and receiving side. The protocol entity shall then start the sequence number reset procedure, which is described in 18.6.2.3.

NOTE 2 – The above inequalities take into account modulus 128.

18.6.2.3 Sequence number reset procedure

18.6.2.3.1 Normal procedure

The sequence number reset procedure is a symmetrical procedure which shall be started from that entity detecting a misalignment of state variables. The procedure will also be started during system startup after at least one of the two data links for protection has been established. In this case the procedure shall be initiated by LE system management, which will issue a MDU-Protection (reset

SN req) primitive to the LE protection protocol entity. This procedure makes use of the messages RESET SN COM and RESET SN ACK, which do not contain a sequence number information element.

The entity, initiating the reset procedure, shall send a RESET SN COM to the peer entity, reset the send state variable VP(S) to Zero and the receive state variable VP(R) to Zero, start timer TSO4, and issue a MDU-Protection (reset SN com) primitive to the system management. If the LE has triggered the SN reset and if the LE protection protocol entity is not in the NULL state (SOLE0) the timers TSO1 and TSO2, if running, shall be stopped and the LE protection protocol entity shall return to the Null state. If the AN has triggered the SN reset and if the AN protection protocol entity is not in the NULL state (SOAN0) the timer TSO3, if running, shall be stopped and the AN protection protocol entity shall return to the NULL state.

The side receiving the RESET SN COM message shall, if timer TSO5 is not running, respond with a RESET SN ACK message, reset the send state variable VP(S) and the receive state variable VP(R) to Zero, start timer TSO5, and issue a MDU-Protection (reset SN ind) primitive to the system management. If the LE has received the RESET SN COM message and if the LE protection protocol entity is not in the NULL state (SOLE0) the timers TSO1 and TSO2, if running, shall be stopped and the LE protection protocol entity shall return to the NULL state. If the AN has received the RESET SN COM message and if the AN protection protocol entity is not in the NULL state (SOAN0) the timer TSO3, if running, shall be stopped and the AN protection protocol entity shall return to the NULL state.

If a RESET SN COM is received while timer TSO5 is running, there shall be no action and no state change.

On receipt of a RESET SN ACK message, while timer TSO4 is running, timer TSO4 shall be stopped and a MDU-Protection (reset SN ack) primitive shall be issued to the system management. On receipt of a RESET SN ACK message, if timer TSO4 is not running, there shall be no action and no state change.

As long as timer TSO4 is running, all received messages, which contain a sequence number information element, shall be discarded without notification to the system management. In this case, the SN check procedures described in 18.6.2.2 are not processed. No state change shall occur.

As long as timer TSO4 in the AN is running, on receipt of a MDU-Protection (switch-over request) primitive in the AN a MDU-Protection (reset SN error ind) primitive shall be issued to the system management. No state change shall occur.

As long as timer TSO4 in the LE is running, on receipt of a MDU-Protection (switch-over com) primitive or a MDU-Protection (OS switch-over com) primitive in the LE a MDU-Protection (reset SN error ind) primitive shall be issued to the system management. No state change shall occur.

On expiry of timer TSO5 there shall be no action and no state change.

18.6.2.3.2 Exceptional procedures

On the first expiry of timer TSO4 a RESET SN COM message shall be sent to the peer entity, the send state variable VP(S) and the receive state variable VP(R) shall be reset to Zero, a MDU-Protection (reset SN com) primitive shall be issued to the system management, and timer TSO4 shall be restarted.

On the second expiry of timer TSO4 a MDU-Protection (reset SN error ind) shall be issued to the system management. It is then the responsibility of the system management to take the proper actions.

In case of an unexpected expiry of timer TSO4 (i.e. when not being in the NULL state) there shall be no action and no state change.

18.6.3 Standard protection switch-over procedure initiated by LE-side

18.6.3.1 Normal procedure

This procedure shall be used if either a failure is detected by the LE-side or if a switch-over is initiated via Q_{LE}. It uses the SWITCH-OVER command which does not allow to pre-empt allocated C-channels.

The protection protocol in the LE, being in the NULL state (SOLE0) or the SWITCH-OVER REQUESTED BY AN state (SOLE2), when receiving a MDU-Protection (switch-over com) primitive shall send a SWITCH-OVER COM message, start timer TSO1, and enter the SWITCH-OVER INITIATED BY LE state (SOLE1). The SWITCH-OVER COM message shall indicate the logical C-channel to be switched and the target standby C-channel.

On receipt of the SWITCH-OVER COM message by the AN protection protocol entity, being in the NULL state (SOAN0), the AN shall enter the SWITCH-OVER INITIATED BY LE state (SOAN2) and issue a MDU-Protection (switch-over com) primitive to the system management of the AN.

The AN system management shall, if it is able to comply with the switch over command, initiate the switch-over action in the AN and shall issue a MDU-Protection (switch-over ack) primitive to the AN protection protocol entity, which shall then send a SWITCH-OVER ACK message to the LE and enter the NULL state (SOAN0).

On receipt of the SWITCH-OVER ACK message from the AN the LE protection protocol entity shall issue a MDU-Protection (switch-over ack) primitive to the LE system management stop timer TSO1, and enter the NULL state (SOLE0).

On receipt of a SWITCH-OVER REQ message from the AN, when being in the SWITCH-OVER INITIATED BY LE state (SOLE1), there shall be no action and no state change.

The LE shall continue to perform the initiated switch-over.

18.6.3.2 Exceptional procedures

The AN system management shall, if it is not able to comply with the switch over command, issue a MDU-Protection (switch-over reject) primitive to the AN protection protocol entity, which shall then send a SWITCH-OVER REJECT message to the LE and enter the NULL state (SOAN0). The message shall indicate to the LE the cause why switch-over was not possible.

On receipt of the SWITCH-OVER REJECT message from the AN the LE protection protocol entity shall issue a MDU-Protection (switch-over reject ind) primitive to the LE system management, stop timer TSO1, and enter the NULL state (SOLE0).

If an unexpected MDU-Protection primitive is received by the AN or LE protection protocol entity there shall be no action and no state change.

18.6.3.3 Procedure on expiry of timer TSO1

If timer TSO1 expires for the first time, while the LE protection protocol entity being in the SWITCH-OVER INITIATED BY LE state (SOLE1), the LE protection protocol entity shall send a SWITCH-OVER COM message to the AN, and restart timer TSO1.

On receipt of a SWITCH-OVER ACK message from the AN in state SOLE0, a MDU-Protection (switch-over ack) primitive shall be issued to the system management. It is the responsibility of the system management to take the proper action according to the sequence of previously received messages (i.e. the system management may trigger switch-over in the LE or may initiate a new switch-over process).

On receipt of a SWITCH-OVER REJECT message from the AN in state SOLE0 a MDU-Protection (switch-over reject ind) primitive shall be issued from the LE protection protocol entity to the system management. It is the responsibility of the system management to take the proper action according to the sequence of previously received messages and according to the content of the Rejection Cause information element (i.e. the system management may initiate a new switch-over process).

If timer TSO1 expires for the second time, while the LE protection protocol entity being in the SWITCH-OVER INITIATED BY LE state (SOLE1), the LE protection protocol entity shall issue a MDU-Protection (switch-over error ind) primitive to the system management and enter the NULL state (SOLE0).

In case of an unexpected expiry of timer TSO1 (i.e. expiry when not being in the SWITCH-OVER INITIATED BY LE state) there shall be no action and no state change.

18.6.4 Dedicated protection switch-over procedure initiated by OS LE

18.6.4.1 Normal procedure

This procedure shall be used only if switch-over is initiated by the operator of the LE via Q_{LE}. If the target physical C-channel is an active C-channel the physical C-channel shall be pre-empted. The procedure is mainly used to rearrange the allocation of logical C-channels in case of multiple 2048 kbit/s failures. This procedure shall only be used for protection group 2.

The protection protocol in the LE, being in the NULL state (SOLE0) or the SWITCH-OVER REQUESTED BY AN state (SOLE2), when receiving a MDU-Protection (OS-switch-over com) primitive shall send an OS-SWITCH-OVER COM message, start timer TSO2, and enter the SWITCH-OVER INITIATED BY LE state (SOLE1). The OS-SWITCH-OVER COM message shall indicate the logical C-channel to be switched and the target physical C-channel.

On receipt of the of the OS-SWITCH-OVER COM message by the AN protection protocol entity, being in the NULL state (SOAN0), the AN shall enter the SWITCH-OVER INITIATED BY LE state (SOAN2) and issue a MDU-Protection (OS-switch-over com) primitive to the system management of the AN.

The AN system management shall, if it is able to comply with the switch over command, initiate the switch-over action in the AN and shall issue a MDU-Protection (switch-over ack) primitive to the AN protection protocol entity, which shall then send a SWITCH-OVER ACK message to the LE and enter the NULL state (SOAN0).

On receipt of the SWITCH-OVER ACK message from the AN the LE protection protocol entity shall issue a MDU-Protection (switch-over ack) primitive to the LE system management stop timer TSO2, and enter the NULL state (SOLE0).

On receipt of a SWITCH-OVER REQ message from the AN, when being in the SWITCH-OVER INITIATED BY LE state (SOLE1), there shall be no action and no state change.

The LE shall continue to perform the initiated switch-over.

18.6.4.2 Exceptional procedures

The AN system management shall, if it is not able to comply with the switch over command, issue a MDU-Protection (switch-over reject) primitive to the AN protection protocol entity, which shall then send a SWITCH-OVER REJECT message to the LE and enter the NULL state (SOAN0). The message shall indicate to the LE the cause why switch-over was not possible. The switch-over command shall not be rejected due to the fact that the target physical C-channel already carried a logical C-channel. Thus the rejection cause "Target physical C-channel already has a logical C-channel" is not allowed as response to an OS-SWITCH-OVER COM message.

On receipt of the SWITCH-OVER REJECT message from the AN the LE protection protocol entity shall issue a MDU-Protection (switch-over reject ind) primitive to the LE system management, stop timer TSO2, and enter the NULL state (SOLE0).

If an unexpected MDU-Protection primitive is received by the AN or LE protection protocol entity there shall be no action and no state change.

18.6.4.3 Procedure on expiry of timer TSO2

If timer TSO2 expires for the first time, while the LE protection protocol entity being in the SWITCH-OVER INITIATED BY LE state (SOLE1), the LE protection protocol entity shall send a OS-SWITCH-OVER COM message to the AN, and restart timer TSO2.

If timer TSO2 expires for the second time, while the LE protection protocol entity being in the SWITCH-OVER INITIATED BY LE state (SOLE1), the LE protection protocol entity shall issue a MDU-Protection (switch-over error ind) primitive to the system management and enter the NULL state (SOLE0).

On receipt of a SWITCH-OVER ACK message from the AN in state SOLE0, a MDU-Protection (switch-over ack) primitive shall be issued to the system management. It is the responsibility of the system management to take the proper action according to the sequence of previously received messages (i.e. the system management may trigger switch-over in the LE or may initiate a new switch-over process).

On receipt of a SWITCH-OVER REJECT message from the AN in state SOLE0 a MDU-Protection (switch-over reject ind) primitive shall be issued from the LE protection protocol entity to the system management. It is the responsibility of the system management to take the proper action according to the sequence of previously received messages and according to the content of the Rejection Cause information element (i.e. the system management may initiate a new switch-over process).

In case of an unexpected expiry of timer TSO2 (i.e. expiry when not being in the SWITCH-OVER INITIATED BY LE state) there shall be no action and no state change.

18.6.5 Protection switch-over procedure requested by AN-side

18.6.5.1 Normal procedure

This procedure shall be used if either a failure is detected by the AN-side or if a switch-over is initiated via Q_{AN}. The LE can only respond by either a SWITCH-OVER COM message (no pre-emption allowed) or a SWITCH-OVER REJECT message.

The protection protocol in the AN, being in the NULL state (SOAN0), when receiving a MDU-Protection (switch-over req) primitive shall send a SWITCH-OVER REQ message, start timer TSO3, and enter the SWITCH-OVER REQUESTED BY AN state (SOAN1). If the switch-over was initiated by the operator of the OS via Q_{AN} the SWITCH-OVER REQ message shall indicate the logical C-channel to be switched and optionally the preferred target physical C-channel (standby C-channel). If the switch-over was autonomously triggered by the AN system management due to detection of a failure the SWITCH-OVER REQ message shall only indicate the logical C-channel to be switched and no preference for a particular standby C-channel shall be given.

In those cases where no preference is given, all bits of both the 2048 kbit/s Link identifier and the Time Slot Number in the physical C-channel information element shall be coded to Zero.

On receipt of the SWITCH-OVER REQ message the LE protection protocol entity, being in the NULL state (SOLE0), the LE shall enter the SWITCH-OVER REQUESTED BY AN state (SOLE2) and issue a MDU-Protection (switch-over req) primitive to the system management of the LE.

On receipt of the SWITCH-OVER REQ message by the LE protection protocol entity, being in the SWITCH-OVER INITIATED BY LE state (SOLE1), the LE shall ignore the message and shall not change the state.

The LE system management shall, if it is able to comply with the switch over request, initiate the switch-over action by issuing a MDU-Protection (switch-over com) primitive to the LE protection protocol entity, which shall then send a SWITCH-OVER COM message to the AN, enter the SWITCH-OVER INITIATED BY LE state (SOLE1), and start timer TSO1.

On receipt of the SWITCH-OVER COM message by the AN protection protocol entity, being in the SWITCH-OVER REQUESTED BY AN state (SOAN1), the AN shall enter the SWITCH-OVER INITIATED BY LE (SOAN2) state, issue a MDU-Protection (switch-over com) primitive to the system management of the AN, and stop timer TSO3.

On receipt of the OS-SWITCH-OVER COM message by the AN protection protocol entity, being in the SWITCH-OVER REQUESTED BY AN state (SOAN1), the AN shall enter the SWITCH-OVER INITIATED BY LE (SOAN2) state, issue a MDU-Protection (OS-switch-over com) primitive to the system management of the AN, and stop timer TSO3.

The AN system management shall, if it is able to comply with the switch over command, initiate the switch-over action in the AN and shall issue a MDU-Protection (switch-over ack) primitive to the AN protection protocol entity, which shall then send a SWITCH-OVER ACK message to the LE and enter the NULL state (SOAN0).

On receipt of the SWITCH-OVER ACK message from the AN the LE protection protocol entity shall issue a MDU-Protection (switch-over ack) primitive to the LE system management, stop timer TSO1, and enter the NULL state (SOLE0).

The LE shall then perform the switch-over. If, for any reason, the LE cannot perform the switch-over, the LE system management has the responsibility to initiate a new switch-over action.

18.6.5.2 Exceptional procedure – AN cannot comply with switch-over command from LE

The AN system management shall, if it is not able to comply with the switch over command, issue a MDU-Protection (switch-over reject) primitive to the AN protection protocol entity, which shall then send a SWITCH-OVER REJECT message to the LE and enter the NULL state (SOAN0). The message shall indicate to the LE the reason why switch-over was not possible.

On receipt of the SWITCH-OVER REJECT message from the AN the LE protection protocol entity shall issue a MDU-Protection (switch-over reject ind) primitive to the LE system management, stop timer TSO1, and enter the NULL state (SOLE0).

If an unexpected MDU-Protection primitive is received by the AN or LE protection protocol entity there shall be no action and no state change.

18.6.5.3 Exceptional procedure – LE cannot comply with switch-over request from AN

The LE system management, being in the SWITCH-OVER REQUESTED BY AN state (SOLE2) shall, if it is not able to comply with the switch over command, issue a MDU-Protection (switch-over reject) primitive to the LE protection protocol entity, which shall then send a SWITCH-OVER REJECT message to the AN and enter the NULL state (SOLE0). The message shall indicate to the AN the cause why switch-over was not possible.

On receipt of the SWITCH-OVER REJECT message from the LE, when being in state SWITCH-OVER REQUESTED BY AN, the AN protection protocol entity shall issue a MDU-Protection (switch-over reject ind) primitive to the AN system management, stop timer TSO3, and enter the NULL state (SOAN0).

If an unexpected MDU-Protection primitive is received by the AN or LE protection protocol entity there shall be no action and no state change.

18.6.5.4 Procedure on expiry of timer TSO3

If timer TSO3 expires for the first time, while the AN protection protocol entity being in the SWITCH-OVER REQUESTED BY AN state (SOAN1), the AN protection protocol entity shall send a SWITCH-OVER REQ message to the LE, and restart timer TSO3.

If timer TSO3 expires for the second time, while the AN protection protocol entity being in the SWITCH-OVER REQUESTED BY AN state (SOAN1), the AN protection protocol entity shall issue a MDU-Protection (switch-over error ind) primitive to the system management and enter the NULL state (SOAN0).

In case of an unexpected expiry of timer TSO3 (i.e. expiry when not being in the SWITCH-OVER REQUESTED BY AN state) there shall be no action and no state change.

18.6.6 Handling of error conditions

Before acting upon a message, the receiving entity, either the AN V5.2 protection Protocol entity or the LE V5.2 protection Protocol entity, shall perform the procedures specified in this clause.

As a general rule, all messages, except the RESET SN COM and RESET SN ACK messages, shall contain, at least the Protocol Discriminator, the Logical C-channel Identification and the Message Type information elements. When receiving a message having less than 4 octets, the receiving protection protocol entity in the AN or LE shall generate a MDU-Protection (Protocol error indication) primitive to the management system and ignore the message.

A message received shall be checked as described in 18.6.6.1 to 18.6.6.7 in order of precedence. No state change occurs during these checks.

If more than two optional information elements are detected within a message, then the message shall be considered as too long and shall be truncated after the second optional information element. All the truncated information is assumed to be repeated optional information elements. When doing the truncation, the entity shall react according to 18.6.6.3 for repeated optional information elements.

If a protocol error is detected in the AN while timer TSO4 is running, no PROTOCOL ERROR message shall be sent to the LE side.

After the message has been checked using the error handling procedures following, if the message is not to be ignored, then the protection protocol procedures as specified in 18.6.2 to 18.6.5 shall follow.

NOTE – Within this subclause, the term "ignore the message" means to leave the message contents unchanged.

18.6.6.1 Protocol discriminator error

When a message is received by a layer 3 protection protocol entity with a protocol discriminator coded other than the one specified in 13.2.1 for the use in the V5 Protocols, then:

– the AN protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Protocol discriminator error";

– the LE protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system and ignore the message.

18.6.6.1a Logical C-Channel identification error

Whenever a message is received by a layer 3 Protection protocol entity with a Logical C-Channel identification, which:

– is not coded as specified in subclause 18.5.1, or

– does not correspond to an existing Logical C-channel, then:

  • the AN protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Logical C-Channel identification error";

  • the LE protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system and ignore the message.

18.6.6.2 Message type error

Whenever an unrecognized message type is received, then:

– the AN protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Message type unrecognized" including the corresponding diagnostic as specified in 18.5.5;

– the LE protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system and ignore the message.

18.6.6.3 Repeated mandatory information element

Whenever a mandatory information element is repeated in a message, the reaction of the receiving entity shall be as follows:

– the AN protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Repeated mandatory information element" including the corresponding diagnostic as specified in 18.5.5;

– the LE protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system and ignore the message.

18.6.6.4 Mandatory information element missing

Whenever a message is received with a mandatory information element missing, the reaction of the receiving entity shall be as follows:

– the AN protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Mandatory information element missing" including the corresponding diagnostic as specified in 18.5.5;

– the LE protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system and ignore the message.

In the event of more than one mandatory information elements missing, the reaction of the receiving entity shall be on the basis of the first mandatory information element identified as missing.

18.6.6.5 Unrecognized information element

Whenever a message is received with one or more information elements unrecognized, the reaction of the receiving entity shall be as follows:

– the AN protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system, remove all the unrecognized information elements and continue with the processing of the message, it shall also send a PROTOCOL ERROR message indicating the protocol error cause "Unrecognized information element" including the corresponding diagnostic as specified in 18.5.5;

– the LE protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system and remove all the unrecognized information elements and continue with the processing of the message.

In the event of more than one unrecognized information elements, the reaction of the receiving entity shall be on the basis of the first unrecognized information element identified.

For the purpose of the protection protocol error handling procedures unrecognized information elements are those that are not defined within 13.2 and 18.5.

18.6.6.6 Content error of mandatory information element

When a message is received with a mandatory information element having a content error, either:

a) the length does not conform to the length specified in 13.2 and 18.5; or

b) the content is not known, then:

  – the AN protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system, ignore the message and send a PROTOCOL ERROR message indicating the protocol error cause "Mandatory information element content error" including the corresponding diagnostic as specified in 18.5.5;

  – the LE protection protocol entity shall generate a MDU-Protection (Protocol error indication) primitive to the management system and ignore the message.

For the purpose of the error handling procedures, information element content errors are codepoints included within a particular information element that are not defined within 13.2 and 18.5.

18.6.6.7 Unexpected message

A message flow error occurs when an unexpected message is received. The unexpected messages are those explicitly qualified as unexpected (/) messages in the state transition tables of the LE and AN side V5.2-protection protocol entities (see Tables 65 and 66). The state transition tables give the appropriate actions on receipt of any event.

Whenever an unexpected message is received, no state change occurs. In addition:

– the AN protection protocol entity shall issue a MDU-Protection (Protocol error indication) primitive to the system management, ignore the message, and send a PROTOCOL ERROR message indicating the protocol error cause "message not compatible with protection protocol state" including the corresponding diagnostic as specified in 18.5.5;

– the LE protection protocol entity shall issue a MDU-Protection (Protocol error indication) primitive to the system management, ignore the message.

18.7 List of system parameters

The definition of the timers used in the protection protocol is given in Table 64. The mentioned timers are maintained in the LE or AN protection protocol entities. The timer tolerances shall be ±10%.

Table 64/G.965 – Protection protocol timers

Timer name	Timeout value	Cause for start	Normal stop	At first expiry	At second expiry	Reference
TSO1	1500 ms	SWITCH-OVER COM sent, SOLE1 state is entered	Receipt of SWITCH-OVER ACK	Retransmissions of SWITCH-OVER COM	Error indication to system management	18.6
TSO2	1500 ms	OS-SWITCH-OVER COM sent, SOLE1 state is entered	Receipt of SWITCH-OVER ACK	Retransmissions of OS-SWITCH-OVER COM	Error indication to system management	18.6
TSO3	1500 ms	SWITCH-OVER REQ sent, SOAN1 state is entered	Receipt of SWITCH-OVER COM	Retransmissions of SWITCH-OVER REQ	Error indication to system management	18.6
TSO4	20 s	RESET SN COM sent, NULL state entered	Receipt of RESET SN ACK	Retransmissions of RESET SN COM	Error indication to system management	18.6
TSO5	10 s	Receipt of RESET SN COM, NULL state entered	TSO5 will always expiry	No action, no state change	Not applicable	18.6

18.8 AN and LE side state tables

18.8.1 Protection protocol FSM in the AN

The state transition table for the FSM of the protection protocol in the AN is given in Table 65.

Table 65/G.965 – AN Protection protocol FSM

State	SOAN0	SOAN1	SOAN2
State name / Event	NULL	SWITCH-OVER REQUESTED BY AN	SWITCH-OVER REQUESTED BY LE
MDU-Prot. (switch-over ack)	/	/	SWITCH-OVER ACK; SOAN0
MDU-Prot. (switch-over req) (Note 1)	SWITCH-OVER REQ; start TSO3; SOAN1	/	/
	MDU-Prot. (reset SN error ind); –		
MDU-Prot. (switch-over reject)	/	/	SWITCH-OVER REJECT; SOAN0
SWITCH-OVER COM (Note 1)	MDU-Prot. (switch-over com); SOAN2	MDU-Prot. (switch-over com); stop TSO3; SOAN2	/
	–		
OS-SWITCH-OVER COM (Note 1)	MDU-Prot. (OS switch-over com); SOAN2	MDU-Prot. (OS switch-over com); stop TSO3; SOAN2	/
	–		
SWITCH-OVER REJECT (Note 1)	/	MDU-Prot. (switch-over reject ind); stop TSO3; SOAN0	/
	–		
Expiry of timer TSO3 (first)	/	SWITCH-OVER REQUEST; start TSO3; –	/
Expiry of timer TSO3 (second)	/	MDU-Prot. (switch-over error ind); SOAN0	/
VP(S), VP(R) misalignment detected	RESET SN COM; start TSO4; MDU-Prot. (reset SN com); set VP(S) = VP(R) = 0; –	RESET SN COM; start TSO4; stop TSO3; MDU-Prot. (reset SN com); set VP(S) = VP(R) = 0; SOAN0	RESET SN COM; start TSO4; MDU-Prot. (reset SN com); set VP(S) = VP(R) = 0; SOAN0
RESET SN COM (Note 2)	RESET SN ACK; set VP(S) = VP(R) = 0; start TSO5; MDU-Prot. (reset SN ind); –	RESET SN ACK; set VP(S) = VP(R) = 0; start TSO5; stop TSO3; MDU-Prot. (reset SN ind); SOAN0	RESET SN ACK; set VP(S) = VP(R) = 0; start TSO5; MDU-Prot. (reset SN ind); SOAN0
	–	–	–

Table 65/G.965 – AN Protection protocol FSM

State	SOAN0	SOAN1	SOAN2
State name / Event	**NULL**	**SWITCH-OVER REQUESTED BY AN**	**SWITCH-OVER REQUESTED BY LE**
RESET SN ACK (Note 1)	–	–	–
	Stop TSO4; MDU-Prot. (reset SN ack); –		
Expiry of timer TSO4 (first)	RESET SN COM; start TSO4; MDU-Prot. (reset SN com); set VP(S) = VP(R) = 0; –	/	/
Expiry of timer TSO4 (second)	MDU-Prot. (reset SN error ind); –	/	/
Expiry of timer TSO5	–	–	–
Detection of protocol error (Note 1)	MDU-Prot. (Protocol error ind); PROTOCOL ERROR; –	MDU-Prot. (Protocol error ind); PROTOCOL ERROR; –	MDU-Prot. (Protocol error ind); PROTOCOL ERROR; –
	MDU-Prot. (Protocol error ind); –		

– No state change, no action

/ Unexpected event, no state change, no action

NOTE 1 – The lower option shall be chosen if timer TSO4 is running.

NOTE 2 – The lower option shall be chosen if timer TSO5 is running.

18.8.2 Protection protocol FSM in the LE

The state transition table for the FSM of the protection protocol in the LE is given in Table 66.

Table 66/G.965 – LE protection protocol FSM

<table>
<tr><th>State</th><th>SOLE0</th><th>SOLE1</th><th>SOLE2</th></tr>
<tr><th>State name
Event</th><th>NULL</th><th>SWITCH-OVER INITIATED BY LE</th><th>SWITCH-OVER REQUESTED BY AN</th></tr>
<tr><td rowspan="2">MDU-Prot.(switch-over com)
(Note 1)</td><td>SWITCH-OVER COM; start TSO1; SOLE1</td><td rowspan="2">/</td><td rowspan="2">SWITCH-OVER COM; start TSO1; SOLE1</td></tr>
<tr><td>MDU-Prot. (reset SN error ind); –</td></tr>
<tr><td rowspan="2">MDU-Prot.(OS switch-over com)
(Note 1)</td><td>OS SWITCH-OVER COM;
start TSO2; SOLE1</td><td rowspan="2">/</td><td rowspan="2">OS SWITCH-OVER COM;
start TSO2; SOLE1</td></tr>
<tr><td>MDU-Prot. (reset SN error ind); –</td></tr>
<tr><td>MDU-Prot.(switch-over reject)</td><td>/</td><td>/</td><td>SWITCH-OVER REJECT; SOLE0</td></tr>
<tr><td rowspan="2">SWITCH-OVER ACK
(Note 1)</td><td>MDU-Prot. (switch-over ack); –</td><td rowspan="2">MDU-Prot.(switch-over ack); stop TSO1; stop TSO2; SOLE0</td><td rowspan="2">/</td></tr>
<tr><td>–</td></tr>
<tr><td rowspan="2">SWITCH-OVER REQ
(Note 1)</td><td>MDU-Prot.(switch-over req); SOLE2</td><td rowspan="2">–</td><td rowspan="2">/</td></tr>
<tr><td>–</td></tr>
<tr><td rowspan="2">SWITCH-OVER REJECT
(Note 1)</td><td>MDU-Prot.(switch-over reject ind); –</td><td rowspan="2">MDU-Prot.(switch-over reject ind); stop TSO1; stop TSO2; SOLE0</td><td rowspan="2">/</td></tr>
<tr><td>–</td></tr>
<tr><td>Expiry of timer TSO1 (first)</td><td>/</td><td>SWITCH-OVER COM; start TSO1; –</td><td>/</td></tr>
<tr><td>Expiry of timer TSO1 (second)</td><td>/</td><td>MDU-Prot.(switch-over error ind); SOLE0</td><td>/</td></tr>
<tr><td>Expiry of timer TSO2 (first)</td><td>/</td><td>OS SWITCH-OVER COM;
start TSO2; –</td><td>/</td></tr>
<tr><td>Expiry of timer TSO2 (second)</td><td>/</td><td>MDU-Prot.(switch-over error ind); SOLE0</td><td>/</td></tr>
<tr><td>VP(S), VP(R) misalignment detected or MDU-Prot. (reset SN req)</td><td>RESET SN COM; start TSO4; MDU-Prot. (reset SN com);
set VP(S) = VP(R) = 0; –</td><td>RESET SN COM;
start TSO4; stop TSO1; stop TSO2;
MDU-Prot. (reset SN com);
set VP(S) = VP(R) = 0; SOLE0</td><td>RESET SN COM;
start TSO4; MDU-Prot. (reset SN com);
set VP(S) = VP(R) = 0; SOLE0</td></tr>
</table>

Table 66/G.965 – LE protection protocol FSM

State	SOLE0	SOLE1	SOLE2
Event \ State name	**NULL**	**SWITCH-OVER INITIATED BY LE**	**SWITCH-OVER REQUESTED BY AN**
RESET SN COM (Note 2)	RESET SN ACK; set VP(S) = VP(R) = 0; start TSO5; MDU-Prot.(reset SN ind); –	RESET SN ACK; set VP(S) = VP(R) = 0; start TSO5; stop TSO1; stop TSO2; MDU-Prot.(reset SN ind.); SOLE0	RESET SN ACK; set VP(S) = VP(R) = 0; start TSO5; MDU-Prot.(reset SN ind); SOLE0
	–	–	–
RESET SN ACK (Note 1)	–	–	–
	Stop TSO4; MDU-Prot. (reset SN ack); –		
Expiry of timer TSO4 (first)	RESET SN COM; start TSO4; MDU-Prot. (reset SN com); set VP(S) = VP(R) = 0; –	/	/
Expiry of timer TSO4 (second)	MDU-Prot. (reset SN error ind); –	/	/
Expiry of timer TSO5	–	–	–
PROTOCOL ERROR (Cause) (Note 1)	MDU-Prot. (Protocol error ind); –	MDU-Prot. (Protocol error ind); –	MDU-Prot. (Protocol error ind); –
	–		

– No state change, no action

/ Unexpected event, no state change, no action

NOTE 1 – The lower option shall be chosen if timer TSO4 is running.

NOTE 2 – The lower option shall be chosen if timer TSO5 is running.

ANNEX A

Service scenarios, architecture and functional definition of access arrangements with AN at the LE

A.1 Conclusions on multiple V5-interface applications

The contents of this clause are identical to A.1/G.964 [8].

A.2 Conclusions on architecture aspects

Any V5.2 interface may have a minimum of one, and a maximum of sixteen physical 2048 kbit/s links.

The number and mix of V5.1 and V5.2 interfaces between any particular AN and LE is unlimited.

The ET layer 1 functions for the ISDN-BA service as defined in ITU-T G.960 [4] are split amongst the AN and the LE (see Figure 3).

The ET layer 1 functions for the ISDN-PRA service as defined in ITU-T G.962 [10] are controlled by the AN.

Additional channel switching between the AN and the LE, e.g. by a separate cross connect, is allowed but without impact on the functionality of the V5.2 interface specified in this Recommendation. Cascading of ANs (i.e. by connecting them with a "V5-type" interface) has no impact on the functions of the V5.2 interface.

The scope of the V5 interface is not limited to ANs exclusively and should be independent of their architecture. Cross connect(s) between an AN and the LE are seen from the V5 interface as being an integral part of the AN.

The coexistence of interfaces V5.1, V5.2 and V3 is possible.

A.3 Implementation of Q_{AN}

The contents of this clause are identical to A.3/G.964 [8].

A.4 Requirements for the support of the PL capability through an ISDN basic access

The contents of this clause are identical to A.4/G.964 [8].

A.5 Requirements for the support of the PL capability through an ISDN primary rate access

Permanent lines bypass the LE and are outside the scope of the V5.2-interface specification. As the ISDN-PRA port is permanently active, an FSM is not required in the LE in order to support the function.

In order for the BCC protocol to function correctly, it shall be controlled via two resource managers, one in the LE and the other in the AN. This Recommendation assumes that these resource managers exist but does not attempt to limit their functionality.

In order for the resource managers to function correctly, the resource manager in the LE shall be informed of demands made on the user port time slots it is controlling. This information shall be passed into the system via Q_{LE}.

A.6 Assumptions and requirements for the support of semi-permanent leased lines

A.6.1 General

Semi-permanent leased lines pass through the V5.2 interface.

For the V5.2 interface, where the connection for all bearer channels is established between the user port of the AN and the LE by the BCC, no additional procedure between the LE and the AN is required for the support of semi-permanent leased lines. These are provisioned via Q_{LE}.

Provisioning of the user port according to the requirements of the user is under the responsibility of the AN and therefore outside the scope of the V5.2-interface specification.

A.6.2 Signalling associated to semi-permanent leased lines

The contents of this clause are identical to A.5.2/G.964 [8].

A.6.3 User ports

The contents of this clause are identical to A.5.3/G.964 [8].

A.6.4 Requirements for non-ISDN user ports for semi-permanent leased lines

The contents of this clause are identical to A.5.4/G.964 [8].

A.7 Example of AN and LE configuration

Figure A.1 shows one case with two LEs and two ANs connected to each other via five V5 interfaces with the following given v5InterfaceID values: 1, 2, 3, 4, up to $2^{24} - 1$, 16777215). LE_1 is connected to AN_1 and AN_2 using V5 interfaces of type both V5.1 and V5.2 to the same AN. Both LE_1 and LE_2 are connected to AN_2 using separate V5 interfaces of different types.

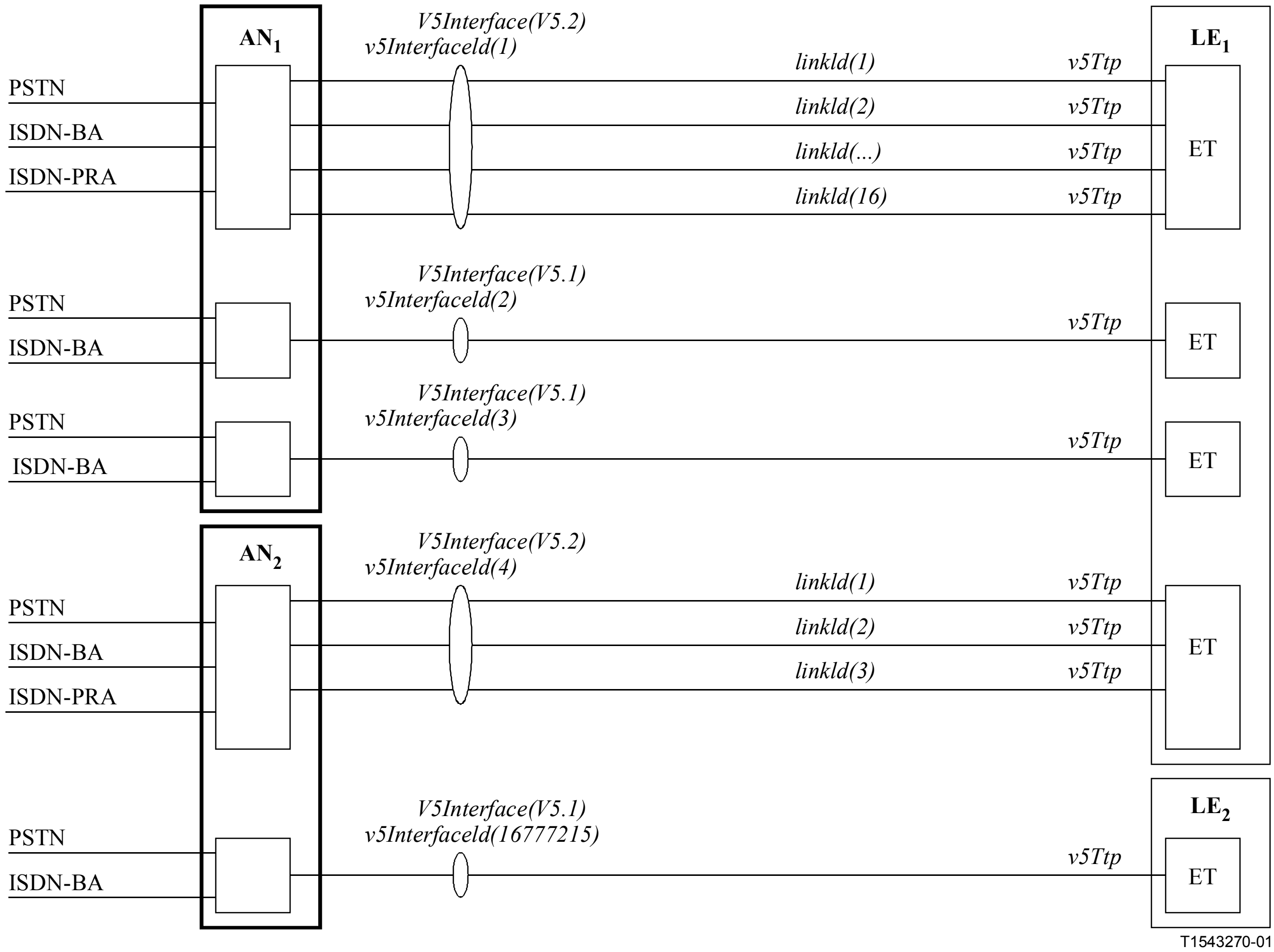


Figure A.1/G.965 – A possible AN/LE configuration using the V5 standard

For V5.1 the interface ID is unique for everything related to this particular interface. The same is true for V5.2 with the difference that the linkID differs for each of the 2048 kbit/s links.

The value of the V5InterfaceId is defined in the LE configuration management standard, ITU-T Q.824.5 [12], and referred to by the AN configuration management standard. The value is set by the Relative Distinguished Name (RDN) of the interface. The v5InterfaceId needs to be identical on the both sides of the V5 interface to succeed with the system start-up procedures defined in Annex C/G.964 [8].

If the network consists of more than two operators, then co-ordination of the interface ID is needed within the network before the configuration activities can start. The interface ID should be unique in the network in some way (which is not defined). It is not sufficient to be unique within the managedElement.

ANNEX B

Use of the protocol information elements for national PSTN protocols

The contents of this annex are identical to that of Annex B/G.964 [8].

ANNEX C

Basic requirements of the system management functions in the AN and the LE

C.1 Procedure for the ISDN basic access continuity test

The contents of this clause are identical to C.1/G.964 [8].

C.2 Port Blocking

The contents of this clause are identical to C.2/G.964 [8].

C.3 Collision between primitives

The contents of this clause are identical to C.3/G.964 [8].

C.4 AN detection of hard failure and unacceptable performance

The contents of this clause are identical to C.4/G.964 [8].

C.5 Port Unblocking

The contents of this clause are identical to C.5/G.964 [8].

C.6 Control and Provisioning

The contents of this clause are identical to C.6/G.964 [8].

C.7 Verification of Port State

Reference is made to 15.3.3.4 and ITU-T G.964 [8] (subclauses 14.1.3.4 and 14.2.3.4) for the AN verification mechanism and to 15.3.3.5 and ITU-T G.964 [8] (subclauses 14.1.3.5. and 14.2.3.5) for the LE verification mechanism using MPH-UBR.

C.8 Permanent Activation of ISDN lines

Reference is made to 15.3.3.3.6 and to Note 1 of Table 36/G.964 [8] concerning permanent activation

C.9 Coordination of FSMs

The contents of this clause are identical to C.9/G.964 [8].

C.10 Error performance of Digital Section

The contents of this clause are identical to C.10/G.964 [8].

C.11 Provisioning verification

The procedure for provisioning verification uses the messages defined in 14.5/G.964 [8] and the protocol elements, coding and procedures are defined in 14.3/G.964 [8] and 14.4/G.964 [8].

Before re-provisioning, it is suggested that the verification mechanism be used to verify that the new provisioning variant is available in both the AN and LE. To do so, the side wishing to do re-provisioning issues the VERIFY RE-PROVISIONING message, and receives either:

– READY FOR RE-PROVISIONING; or

– NOT READY FOR RE-PROVISIONING.

In the latter case it shall be the responsibility of the management to take any necessary action.

C.12 Re-provisioning synchronization

The procedure for provisioning synchronization shall only be applied at the agreed re-provisioning time. The procedure uses the messages defined in 14.3/G.964 [8] and 14.5/G.964 [8].

Re-provisioning initiated from the LE management

The procedure is shown in Figure C.1.

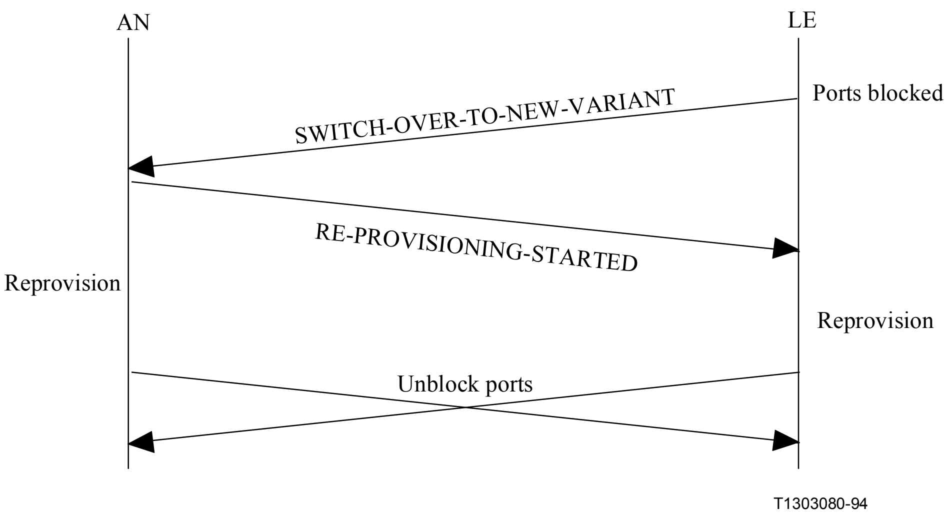


Figure C.1/G.965 – Procedure for re-provisioning initiated from LE

The LE blocks all relevant ports. The LE issues the SWITCH-OVER-TO-NEW-VARIANT message, and receives either:

– RE-PROVISIONING-STARTED; or

– CANNOT RE-PROVISION with cause.

In the former case, the AN then begins re-provisioning upon sending the RE-PROVISIONING-STARTED message and the LE begins re-provisioning upon reception RE-PROVISIONING STARTED message and both ends initiate unblocking of ports when ready using the defined unblocking mechanism. In the latter case, the LE only informs its management and may unblock the ports.

The AN and LE may delay the start of the re-provisioning to ensure the delivery of the RE-PROVISIONING-STARTED ACK message to the AN.

In the latter case it shall be the responsibility of the management to take any necessary action.

Re-provisioning initiated by the AN management

The procedure is shown in Figure C.2.

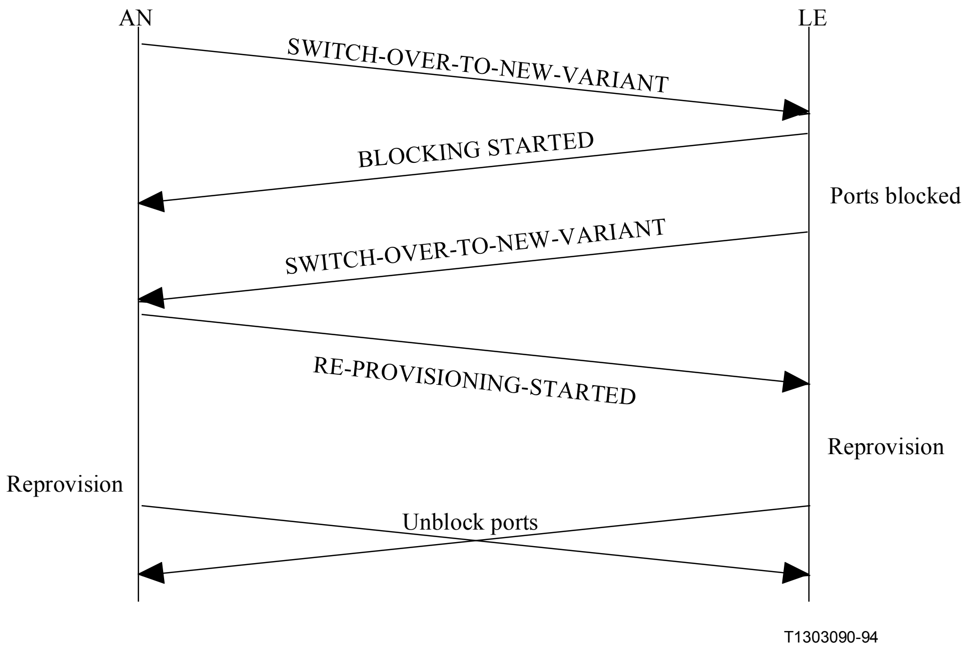


Figure C.2/G.965 – Procedure for re-provisioning initiated from AN

The AN sends the SWITCH-OVER-TO-NEW-VARIANT message. If the LE can support re-provisioning it starts blocking of the relevant ports and responds with BLOCKING STARTED. The procedure is then the same as for LE-initiated re-provisioning. If there are no ports to be blocked or blocked already the LE may proceed immediately with SWITCH-OVER-TO-NEW-VARIANT.

If the LE cannot re-provision, it responds to the SWITCH-OVER-TO-NEW-VARIANT message with the CANNOT RE-PROVISION message. In this case no other action shall be taken at the LE.

Re-provisioning verification

It may be required to request variant and interface ID before starting to unblock the ports. This procedure avoids a situation in which ports are operational while there is a mismatch of variant or interface ID after re-provisioning.

Fallback procedure

It may be possible to "undo" the re-provisioning using the re-provisioning synchronization mechanism if the control protocol link is still active. In this case, the variant used would label a data set corresponding to the old data set.

Application of re-provisioning procedures

Cases where V5-re-provisioning procedures may be applied (affecting both sides of V5: AN and LE):

a) C-channel reconfiguration.

b) Upgrade from V5.1 to V5.2.

Cases where these procedures are not required (as they do not affect service to other ports):

a) Adding, modifying and deleting user ports.

b) Adding and deleting V5.2 links, used for bearer channels only.

C.13 System startup

The default profile contains the initial provisioning data for the mapping of logical to physical C-channels in AN and LE. In both the LE and AN, the default profile will be used for the system startup. During startup and in normal state no changes of the default profile are allowed.

With regards to the remainder of this clause, actions required for any items that are not provisioned shall be ignored.

Pre-conditions

The following shall apply for the entire V5.2 interface:

a) Default profile for the mapping of logical to physical C-channels.

b) BCC: all time slots are de-allocated.

c) At least layer 1 and flag monitoring for the TS16 shall be active for the primary link. Otherwise the exceptional procedure below shall be applied.

d) The states of Link Control FSMs shall be initialized in the following way if not blocked by system management:

   A Links in state Link failure (0.1 AN/LE) shall remain in that state.

   B Links in state Link failure and blocked (0.2 AN/LE) shall enter the state Link failure (0.1 AN/LE).

   C Links in other states shall enter the state Link operational (2.0 AN/LE).

e) The initial states of the various FSMs involved in the start-up of a V5.2 interface are as follows:

– Common Control Protocol FSM	– Out of Service (AN0/LE0)
– Link control protocol FSM	– Out of Service (AN0/LE0)
– Port Control Protocol FSM	– Out of Service (AN0/LE0)
– PSTN Port Status FSMs	– Blocked (AN1.0/LE1.0)

– ISDN BA Port Status FSMs	– Blocked (AN1.0/LE1.0)
– ISDN PRA Port Status FSMs	– Blocked (AN1.0/LE1.0)
– PSTN Signalling FSM	– Port Blocked (AN6/LE6)
– BCC Protocol FSM	– Null (ANBcc0/LEBcc0)
– Protection Protocol FSM	– Null (SOAN0/SOLE0)
– System Management	– Null (ANSYS0/LESYS0)

Normal procedure

a) Activation of LAPV5_DL: MDL-Establish-Request shall be sent to all LAPV5_DLs. MDL-Establish-Request shall be sent to both protection data links. The activation of the LAPV5_DLs can be performed in sequential or parallel order. If sequential order is chosen the following sequence shall apply: PROTECTION_DL, CONTROL_DL, LINK_CONTROL_DL, BCC_DL, and PSTN_DL.

NOTE 1 – MDL-Establish-Request is sent only if the data link is not already established.

b) The sequence number reset procedure as described in 18.6.2.3.1 shall be applied when the appropriate data link has been successfully established.

c) When MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH-INDICATION is received from the first of all of the LAPV5 Data links timer TC10 shall be started. Timer TC10 controls the activation of protection switch-over mechanism for protection group 1 in startup. See C.32 for details on the handling of Timer TC10.

d) When MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH-INDICATION is received from CONTROL_DL, the system management shall send a start-traffic message to the common control protocol FSM.

e) When MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH-INDICATION is received from CONTROL_DL, LINK_CONTROL_DL and BCC_DL, start traffic shall be sent to the port control protocol FSMs and link control protocol FSMs. After that the variant & interface ID shall be checked to be the same as the own variant & interface ID.

f) The system management:

   – shall apply the link block procedure. That means, for those links which are blocked by the system management, MDU_LBI shall be sent to the concerned link control FSMs;

   – may apply the link identification procedure. If applied the link identification procedure shall be actioned for primary and secondary link.

   These two procedures may run sequentially or parallel.

g) Entering the normal state.

h) Post-processing.

NOTE 2 – From now on the following procedures may run in parallel.

A If the link identification procedure is applied, it may be started on the remaining links.

B All relevant user ports shall go through the co-ordinated unblock procedure. PSTN user ports shall only be unblocked if the PSTN_DL is established.

C Pending protection switch-over actions for the protection group 2 shall be performed and the normal protection procedures do apply now.

Exceptional procedures in case of failure in system startup before entering the normal state

Definitions

Re-initiated system startup: When the system startup cannot be continued for some reason, the system startup shall be re-initiated by a system integrity process of the AN or LE. This shall ensure that the system management is put into the SYSTEM STARTUP state repeatedly. Prior to the re-initiation of system startup the appropriate downtimes have to be kept according to the failure conditions that have occurred (see C.29 for details).

a) Protection switch-over in system startup:

During system startup the protection switch-over shall only be used for the logical C-channel of protection group 1. Protection switch-over of a logical C-channel in protection group 2 shall only be allowed in normal state.

b) In case of link control-, control-, PSTN- or BCC-DL failures of protection group 1 in multi-link configuration and if the secondary link is operational, the protection switch-over procedure may be invoked. Protection switch over may also apply in case of flag monitoring failure or 2048 kbit/s link failure of the active link of protection group 1.

c) Data link failure only for protection DLs: If MDL-Release-Indication is received only for a single protection data link or both protection data links, the system management shall send MDL-Establish-Request to the failed protection data link(s). The system startup shall not be influenced through the failure of the protection data link(s) as long as no protection switching is necessary. If it becomes necessary to perform a switch-over when both protection data links are unavailable the startup shall be re-initiated.

d) Failure with variant&interface ID check: In case of an unsuccessful check of the variant&interface ID, a notification shall be given to the management entity and the startup shall be re-initiated. In case of expiry of the timer TV1 the actions described under C.30 shall be taken.

e) PSTN DL failure: If the PSTN DL can not be established, the PSTN user ports remain in the blocked state.

f) Link-ID check failure: If the Link-ID check was applied during system startup and FE-IDRej was received for some link, the state for that link shall not be changed. The Link-ID check shall be repeated later. If Link-ID mismatch occurs indicated by MDU-EIg the link shall be blocked and the system management may trigger an autonomous protection switch-over procedure for the active C-channel of the protection group 1 on that 2048 kbit/s link. System startup may be continued after successful switch over or receipt of FE-IDRej.

g) Error recovery during startup: If the system startup cannot be continued for some reason and error recovery is still possible (e.g. link layer 1 failure recovery, successful protection switch-over, etc), the performance of system startup shall be suspended. On recovery from the error situation startup shall be resumed with the next unfinished step. During error recovery and if error recovery fails system startup may be re-initiated (refer to above definition of re-initiated system startup).

NOTE 3 – If error recovery fails the re-initiation of system startup is guaranteed to be triggered by the expiration of the relevant Data link timers (e.g. TC2).

C.14 PSTN restart procedure

The PSTN restart procedure shall be invoked by the system management in the AN or the LE after PSTN_DL failure as described in C.17.

There is no specific restart procedure defined for the control protocol. The system management shall use port individual blocking and unblocking procedure instead if required.

A PSTN restart procedure shall be initiated:

a) after a PSTN DL failure as described in C.17; or

b) when an MDU-CTRL (restart request) is received from the common control protocol entity.

In case of a), a MDU-CTRL (restart request) shall be sent to the common control protocol entity, a MDU-CTRL (restart request) shall be sent to all PSTN protocol FSMs and the timers TR1 and TR2 shall be started.

In case of b), an MDU-CTRL (restart request) shall be sent to all PSTN protocol FSMs and the timers TR1 and TR2 shall be started.

On being informed of PSTN restart completion by the peer entity via MDU-CTRL (restart complete) from the common control protocol entity and timer TR2 is running, the following actions shall be performed:

– stop timer TR2;
– if restart of all local PSTN protocol FSMs is complete or timer TR1 has expired, then MDU-CTRL (restart complete) is sent to the PSTN protocol FSMs and the procedure ends.

If TR2 is not running, MDU-CTRL (restart complete) shall be ignored.

On being informed of PSTN restart completion by all local PSTN protocol FSMs via MDU-CTRL (restart ack) primitives from the PSTN protocol FSMs and Timer TR1 is running, the following actions shall be performed:

– stop timer TR1;
– send MDU-CTRL (restart complete) to the common control protocol entity;
– if restart of the peer entity is complete, then MDU-CTRL (restart complete) is sent to all PSTN protocol FSMs and the procedure ends.

If TR1 is not running, MDU-CTRL (restart ack) primitives shall be ignored.

On expiry of timer TR1 the following actions shall be performed:

– send an error indication to the maintenance entity;
– send an MDU-CTRL (restart complete) primitive to the common control protocol entity;
– if restart of the peer entity is complete, then MDU-CTRL (restart complete) is sent to all PSTN protocol FSMs and the procedure ends.

On expiry of timer TR2 the following actions shall be performed:

– send an error indication to the maintenance entity;
– send MDU-CTRL (restart complete) to all PSTN protocol FSMs;
– end the procedure.

On being informed of PSTN restart initiated by the peer system management via an MDU-CTRL (restart request) from the common control protocol entity while timers TR1 or TR2 are running, system management shall ignore the primitive.

C.15 Data link activation procedure

The data link activation procedure is described in C.13.

C.16 Data link reset

An MDL-Establish-Indication received from a data link, which the system management considers to be already in the established condition, will be ignored.

C.17 Data link failure

Data link failure shall be detected for any Data link when any of the following events occur:

a) For a Data link which has not yet been established since the initiation of the actual startup:

Expiry or stop of timer TC10 (refer to C.32).

b) For a Data link which is established.

Reception of MDL-Release-Indication.

Failure of the 2048 kbit/s link which carries the C-channel which carries the Data link (refer to 18.1.5.1).

Flag monitoring failure of the C-channel which carries the Data link (refer to 18.1.5.2).

In case of Data link failure of Control, Link Control, BCC and PSTN Data link the relevant timer TC1, TC3, TC4 and TC6 respectively shall be started.

System management shall continuously try to establish any failed Data links even if another MDL-RELEASE-INDICATION primitive is issued from the Data link to system management with the following exceptions:

– Failure of the 2048 kbit/s link which carries the C-channel which carries the Data link (see 18.1.5.1).
– Flag monitoring failure of the C-channel which carries the Data link (see 18.1.5.2).

If the Data link failure was caused by any of these two events the affected Data links shall be stopped immediately by issuing MDL-LAYER_1_FAILURE-INDICATION.

Establishment attempts shall be re-started when the last of these failure conditions has disappeared.

NOTE – This may happen as a consequence of a protection switch-over.

If an MDL-ESTABLISH-INDICATION or MDL-ESTABLISH-CONFIRM following an MDL-RELEASE-INDICATION is received, the relevant TC-timer shall be stopped. If the event is from the CONTROL_DL or LINK_CONTROL_DL and the protocol(s) have been stopped, then MDU-Start-traffic event(s) shall be sent to the relevant protocol(s).

If no MDL-ESTABLISH-INDICATION or MDL-ESTABLISH-CONFIRM is received from the PSTN_DL within 15 seconds (Timer TC3), the blocking of all PSTN ports shall be invoked as described in C.31. The PSTN restart procedure (refer C.14, shall be invoked after the re-establishing of the PSTN_DL. On completion of the PSTN restart, PSTN ports shall be unblocked according to C.31.

If no MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH-INDICATION primitive is received from the CONTROL_DL within 15 seconds (timer TC1), a MDU_stop_traffic shall be sent to all control protocol entities, the blocking of the ISDN ports shall be invoked by the relevant system management and timer TC2 (1 minute) shall be started. Upon expiry of timer TC2, the timer TC8 shall be started. Upon expiry of the timer TC8 the system startup shall be initiated.

If no MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH-INDICATION primitive is received from the LINK_CONTROL_DL within 15 seconds (timer TC4), a MDU_stop_traffic shall be sent to the link control entities (but there is no blocking of the links) and timer TC5 (1 minute) shall be started. Upon expiry of timer TC5, the timer TC8 shall be started. Upon expiry of the timer TC8 the system startup shall be initiated.

If no MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH-INDICATION primitive is received from the BCC_DL within 15 seconds (timer TC6), timer TC7 (1 minute) shall be started. Upon expiry of timer TC7, the timer TC8 shall be started. Upon expiry of the timer TC8 the system startup shall be initiated.

C.18 Control protocol layer 3 protection mechanism error

The contents of this clause are identical to C.18/G.964 [8].

C.19 Timers in the system management entity

The timers in the system management of the AN and the LE are specified in Table C.1. All the timers defined in Table C.1 shall have a tolerance of better than ±5%.

C.20 Application of link identification procedure

Link identification may be required after link layer 1 failure recovery indicated by MPH-AI from the layer 1 link FSM and indicated to the system management by MDU-LAI. It is for the system management to invoke the link identification procedure. There may be other triggers within the system management to request this procedure. There shall be only one request for the link identification procedure from the system management at a time for all V5 interfaces of AN or LE.

C.21 Reaction on result of link identification

It is the responsibility of the system management to take the appropriate action on receipt of any information from the link control FSM, e.g. MDU-IDRej, MDU-AI, MDU-EIg, as a result of a link identification procedure the system management has requested from the link control FSM.

C.22 Link blocking and re-provisioning

There is no need for blocking of 2048 kbit/s links before re-provisioning. After re-provisioning completed the 2048 kbit/s links may go into operational state and may not require link unblocking.

Table C.1/G.965 – Timers in the system management entity

Timer	Timeout value	Cause for start	Normal stop	At expiry	Reference
TR1	100 s	MDU-CTRL(restart request) to all PSTN protocol FSMs	MDU-CTRL(restart ack) from all PSTN protocol FSMs	Abandon PSTN restart process.	C.14
TR2	120 s	MDU-CTRL(restart request) either sent to or received from COMMON CONTROL	MDU-CTRL(restart complete) from COMMON CONTROL	Abandon PSTN restart process	C.14

Table C.1/G.965 – Timers in the system management entity

Timer	Timeout value	Cause for start	Normal stop	At expiry	Reference
TC1	15 s	Data link failure detected for CONTROL_DL	Reception of MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH INDICATION from CONTROL_DL	Start timer TC2	C.17
TC2	60 s	Expiry of TC1	Reception of MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH INDICATION from CONTROL_DL	Initiate system restart by starting timer TC8	C.17
TC3	15 s	Data link failure detected for PSTN_DL	Reception of MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH INDICATION from PSTN_DL	Block all PSTN ports	C.17
TC4	15 s	Data link failure detected for LINK_CONTROL_DL	Reception of MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH INDICATION from LINK_CONTROL_DL	Start timer TC5	C.17
TC5	60 s	Expiry of TC4	Reception of MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH INDICATION from LINK_CONTROL_DL	Start timer TC8	C.17
TC6	15 s	Data link failure detected for BCC_DL	Reception of MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH INDICATION from BCC_DL	Start timer TC7	C.17
TC7	60 s	Expiry of TC6	Reception of MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH INDICATION from BCC_DL	Start timer TC8	C.17
TC8	20 s	Expiry of TC2, TC5 or TC7	This timer always expires	Initiate system start-up.	C.29
TC9	95 s	Stopping or power up (i.e. cold restart) of V5 interface	This timer always expires	Initiate system start-up if required.	C.29
TC10	30 s	Reception of MDL-ESTABLISH-CONFIRM or MDL-ESTABLISH-INDICATION from the first of all LAPV5 Data links in startup	Entering the normal state (according to C.13) or protection switch-over requested by the remote side.	See C.32	C.32

Table C.1/G.965 – Timers in the system management entity

Timer	Timeout value	Cause for start	Normal stop	At expiry	Reference
TV1	15 s	MDU-CTRL(Request variant & interface ID) sent to COMMON CONTROL	MDU-CTRL(Variant & interface id) received from the COMMON CONTROL	Implementation specific. See reference.	C.30
TU1A	100 s	MDU-CTRL(UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS REQUEST) sent	MDU-CTRL(UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS ACCEPTED) received	Abandon process	C.28
TU2A	60 s	MDU-CTRL(UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS REQUEST) received or sent	MDU-CTRL(UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS COMPLETED) received	Unblock relevant PSTN and ISDN ports	C.28
TU1B	100 s	MDU-CTRL(UNBLOCK ALL RELEVANT PSTN PORTS REQUEST) sent	MDU-CTRL(UNBLOCK ALL RELEVANT PSTN PORTS ACCEPTED) received	Abandon process	C.28
TU2B	60 s	MDU-CTRL(UNBLOCK ALL RELEVANT PSTN PORTS REQUEST) received or sent	MDU-CTRL(UNBLOCK ALL RELEVANT PSTN PORTS COMPLETED) received	Unblock relevant PSTN ports	C.28
TU1C	100 s	MDU-CTRL(UNBLOCK ALL RELEVANT ISDN PORTS REQUEST) sent	MDU-CTRL(UNBLOCK ALL RELEVANT ISDN PORTS ACCEPTED) received	Abandon process	C.28
TU2C	60 s	MDU-CTRL(UNBLOCK ALL RELEVANT ISDN PORTS REQUEST) received or sent	MDU-CTRL(UNBLOCK ALL RELEVANT ISDN PORTS COMPLETED) received	Unblock relevant ISDN ports	C.28
TU1D	100 s	MDU-CTRL(BLOCK ALL PSTN PORTS REQUEST) sent	MDU-CTRL(BLOCK ALL PSTN PORTS ACCEPTED) received	Abandon process	C.28
TU2D	60 s	MDU-CTRL(BLOCK ALL PSTN PORTS REQUEST) received or sent	MDU-CTRL(BLOCK ALL PSTN PORTS COMPLETED) received	Block PSTN ports	C.28
TU1E	100 s	MDU-CTRL(BLOCK ALL ISDN PORTS REQUEST) sent	MDU-CTRL(BLOCK ALL ISDN PORTS ACCEPTED) received	Abandon process	C.28
TU2E	60 s	MDU-CTRL(BLOCK ALL ISDN PORTS REQUEST) received or sent	MDU-CTRL(BLOCK ALL ISDN PORTS COMPLETED) received	Block ISDN ports	C.28

C.23 Single link configuration and protection mechanism

In a V5.2 interface with a single link only, the protection protocol will not be implemented. The system management shall not invoke the establishment of the protection data link and shall ignore a MDL-RELEASE-INDICATION from a protection data link, if it occurs.

C.24 Re-establishment of data links after protection switching

In case of protection switching of C-paths for PSTN, port and common control, link control or BCC the LE system management shall request re-establishment of the relevant data link(s) by issuing MDL-ESTABLISH-REQUEST.

C.25 V5.2 initialization and protocol data

During V5.2 initialization, i.e. during or after re-provisioning, all data for the protection, BCC, link control and common control protocol shall be reset to the default. This is not required for the port control part because all the ports shall be blocked before starting re-provisioning and need to be unblocked individually later. For the PSTN protocol, the restart procedure shall be applied as defined in ITU-T G.964 [8].

C.26 The treatment of BCC allocation rejections by system management

System management shall log the information provided by the BCC resource manager which may be retrieved by the operations system for identification of the performance level. Frequent allocation rejections may also cause an autonomous indication to the operation system in order to bring the situation to the service provider's attention. Further action can then be taken at this higher level.

C.27 Link control protocol layer 3 protection mechanism error

On "error indication" from the layer 3 protection mechanism for the link control protocol, the relevant Link Control FSMs in the AN and the LE may be miss-aligned. The following management actions may then be required:

– flush message queue for the link control protocol;
– verify current (operational) state by sending "unblock";
– for those links for which the state could not be clarified, enforce re-alignment through the normal block/unblock sequences.

C.28 Accelerated alignment procedures

The accelerated alignment procedures allow alignment of port states without issuing block and unblock messages for each individual port. The procedures are defined as follows:

a) UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS:

a1) When unblock alignment for all PSTN ports and all ISDN basic access ports and all ISDN primary rate access ports of the interface is necessary a MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS REQUEST) shall be sent to the control protocol entity. Timer TU1A shall be started.

Upon reception of MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS ACCEPTED) from the common control protocol entity, timer TU1A shall be stopped. All relevant PSTN and ISDN ports shall directly enter the unblocked state without any negotiation with the peer entity, except those that are considered unsuitable for the unblocked state (the latter shall be blocked again for mutual re-alignment at the end of the procedure). A MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS COMPLETED) shall be sent to the common control protocol entity, timer TU2A shall be started.

Upon reception of MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS COMPLETED) from the common control protocol entity timer TU2A shall be stopped. MPH-BI shall be sent to those PSTN port status FSMs whose ports are considered unsuitable for the unblocked state. Upon reception of MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS REJECTED) TU1A shall be stopped and the process abandoned. A notification shall be given to the maintenance entity.

Upon expiry of timer TU1A the process shall be abandoned. A notification shall be given to the maintenance entity.

Upon expiry of timer TU2A MPH-BI shall be sent to those PSTN and ISDN port status FSMs whose ports are considered unsuitable for the unblocked state.

a2) Upon reception of a MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS REQUEST) a MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS ACCEPTED) shall be sent to the common control protocol entity. After having unblocked all relevant PSTN and ISDN ports a MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS COMPLETED) shall be sent to the common control protocol entity and timer TU2A shall be started.

a3) If the AN or LE side after having sent MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS REQUEST) receives MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS REQUEST) before MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS ACCEPTED), then it shall proceed with sending a MDU-CTRL (UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS ACCEPTED) to the common control protocol entity.

b) UNBLOCK ALL RELEVANT PSTN PORTS:

The procedure UNBLOCK ALL RELEVANT PSTN PORTS is according to the procedure UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS with the following exceptions:

– the port type to be used is PSTN only;

– the timers TU1B and TU2B shall be used instead of the timers TU1A and TU2A.

c) UNBLOCK ALL RELEVANT ISDN PORTS (ISDN basic access and ISDN primary rate access):

The procedure UNBLOCK ALL RELEVANT ISDN PORTS is according to the procedure UNBLOCK ALL RELEVANT PSTN PORTS with the following exceptions:

– the port type to be used is ISDN basic access and ISDN primary rate access;

– the timers TU1C and TU2C shall be used instead of the timers TU1A and TU2A.

d) BLOCK ALL PSTN PORTS:

d1) When block alignment for all PSTN ports of the interface is necessary a MDU-CTRL (BLOCK ALL PSTN PORTS REQUEST) shall be sent to the control protocol entity. Timer TU1D shall be started.

Upon reception of MDU-CTRL (BLOCK ALL PSTN PORTS ACCEPTED) from the common control protocol entity, timer TU1D shall be stopped. All PSTN ports shall directly enter the blocked state without any negotiation with the peer entity, including those that are considered unsuitable (the latter shall be unblocked again on initiative of the requesting side at the end of the procedure). A MDU-CTRL (BLOCK ALL PSTN PORTS COMPLETED) shall be sent to the common control protocol entity, timer TU2D shall be started.

Upon reception of MDU-CTRL (BLOCK ALL PSTN PORTS COMPLETED) from the common control protocol entity timer TU2D shall be stopped. MPH-UBR shall be sent to those PSTN port status FSMs whose ports are considered unsuitable for the blocked state. Upon reception of MDU-CTRL (BLOCK ALL PSTN PORTS REJECTED) TU1D shall be stopped and the process abandoned. A notification shall be given to the maintenance entity.

Upon expiry of timer TU1D the process shall be abandoned. A notification shall be given to the maintenance entity.

Upon expiry of timer TU2D MPH-UBR shall be sent to those PSTN port status FSMs whose ports are considered unsuitable for the blocked state.

d2) Upon reception of a MDU-CTRL (BLOCK ALL PSTN PORTS REQUEST) a MDU-CTRL (BLOCK ALL PSTN PORTS ACCEPTED) shall be sent to the common control protocol entity. After having blocked all PSTN ports a MDU-CTRL (BLOCK ALL PSTN PORTS COMPLETED) shall be sent to the common control protocol entity and timer TU2D shall be started.

d3) If the AN or LE side after having sent MDU-CTRL (BLOCK ALL PSTN PORTS REQUEST) receives MDU-CTRL (BLOCK ALL PSTN PORTS REQUEST) before MDU-CTRL (BLOCK ALL PSTN PORTS ACCEPTED), then it shall proceed with sending a MDU-CTRL (BLOCK ALL PSTN PORTS ACCEPTED) to the common control protocol entity.

e) BLOCK ALL ISDN PORTS:

The procedure BLOCK ALL ISDN PORTS is according to the procedure BLOCK ALL PSTN PORTS with the following exceptions:

– the port type to be used is ISDN basic access and ISDN primary rate access instead of the port type PSTN;
– the timers TU1E and TU2E shall be used instead of the timers TU1D and TU2D.

f) Performing the accelerated alignment procedures at the same time:

The accelerated alignment procedures are symmetrical and may be applied from either side of the V5.2 interface. Accelerated alignment initiated from LE has priority over AN initiated procedure in case of collision of request from AN and LE. This priority applies only when the alignments request from the LE and the AN are of different natures (i.e. if these requests are incompatible or contradictory). The procedure stays symmetrical if AN and LE requests are identical.

The procedure UNBLOCK ALL RELEVANT PSTN AND ISDN PORTS shall not be performed in parallel to any other accelerated alignment procedure as described above.

The procedure UNBLOCK ALL RELEVANT PSTN PORTS and the procedure UNBLOCK ALL RELEVANT ISDN PORTS can be performed in parallel.

The procedure BLOCK ALL PSTN PORTS and the procedure BLOCK ALL ISDN PORTS can be performed in parallel.

The procedure BLOCK ALL PSTN PORTS shall not be performed in parallel to the procedure UNBLOCK ALL RELEVANT PSTN PORTS.

The procedure BLOCK ALL ISDN PORTS shall not be performed in parallel to the procedure UNBLOCK ALL RELEVANT ISDN PORTS.

The procedure BLOCK ALL PSTN PORTS and the procedure UNBLOCK ALL RELEVANT ISDN PORTS can be performed in parallel.

The procedure BLOCK ALL ISDN PORTS and the procedure UNBLOCK ALL RELEVANT PSTN PORTS can be performed in parallel.

C.29 Handling of timers TC8 and TC9

These timers are used to control the re-initiation of a system startup.

The timer TC8 triggers system startup in case of DL-failures. It is needed to guarantee that after unsuccessful DL-establishment both sides have fallen back to the default profile. Timer TC9 is the minimum time a system must be stopped before it can be returned to service. It is started when the system has been stopped for any reason during the system startup or normal operation. It shall also be run prior invoking the system restart when performing a cold start.

On expiry of timer TC2, TC5 or TC7 the following applies:

– The interface shall be brought into a state in which no established LAPV5-DL exists.
– Start of timer TC8.
– On expiry of TC8 system startup shall be performed.

If the system is stopped by OS request the following applies:

– Start of timer TC9.
– Only after expiry of TC9 system startup may be performed on operator request.

If for any other reason one side (AN or LE) recognizes a necessity to reinitiate a system startup the following applies:

– The interface shall be brought into a state in which no established LAPV5-DL exists.
– Start of timer TC9.
– On expiry of TC9 system startup shall be performed.

C.30 Handling of timer TV1

This timer is used to control the variant and interface ID check.

Upon sending the message MDU(Request variant and interface ID) timer TV1 shall be started. At first expiry of the timer TV1 the message MDU(Request variant and interface ID) shall be repeated and the timer TV1 shall be restarted. If the timer TV1 expires for the second time, a notification shall be given to the management entity and either the system shall be restarted or the variant&interface ID check shall be repeated periodically. The timer TV1 shall be stopped when the variant and interface ID is received from the peer entity.

C.31 Alignment of blocking/unblocking between PSTN and Control protocols

The contents of this clause are identical to C.23/G.964 [8].

C.32 Handling of timer TC10

This timer is used to control activation of protection switch-over mechanism for protection group 1 in startup and to define Data link failure for a Data link that has not yet been established during the actual startup.

TC10 shall be started upon reception of MDL-Establish Confirm or MDL-Establish-Indication from the first of all of the V5.2 Data links in startup, and during TC10 it is not allowed to request the protection switch-over procedure for protection group 1. It shall be stopped either when entering the normal state (according to C.13) or upon reception of a requested protection switch-over procedure from the remote side.

On Expiry of timer TC10 the following shall be applied:

– Activation of the Protection switch-over mechanism for protection group 1.
– Evaluation of Data link states, detection of any Data link failures (refer to C.17/G.964 [8]).
– Check for any existing Protection switch-over reasons for protection group 1 followed by the actions described in clause 18.

If TC10 is stopped upon reception of a requested protection switch-over procedure from the remote side the following shall be applied:

– Activation of the Protection switch-over mechanism for protection group 1, i.e. perform the requested procedure.
– Evaluation of Data link states, detection of any Data link failures (refer to C.17/G.964 [8]).

If TC10 is stopped upon entering the normal state the following shall be applied:

– Activation of the Protection switch-over mechanism for protection group 1.
– Evaluation of Data link states, detection of any Data link failures (refer to C.17/G.964 [8]).
– Check for any existing Protection switch-over reasons for protection group 1 followed by the actions described in clause 18.

ANNEX D

Protocol architecture for PSTN and ISDN (BA and PRA) user port control

D.1 Scope

This annex describes the protocol architecture for the ISDN-BA and ISDN-PRA user port and PSTN user port status control information transfer.

D.2 ISDN-BA port status control

The contents of this clause are identical to D.2/G.964 [8].

D.3 ISDN-PRA user port status control

D.3.1 Functional split between LE and AN

For those ISDN-PRAs which are not directly connected to the LE but remotely accessed via an AN, the ET layer 1 functionality is split between the LE and the AN.

In principle, the LE will only be informed about the layer 1 availability of the user port (operational/non-operational).

Since maintenance of the Access Digital Section and customer lines is the responsibility of the AN the operation of loopbacks or other tests of the digital section only will be controlled by the AN. Thus, no information related to these functions shall be transmitted to the LE (FE-A-FE-Y). The correct identification of the port status is the responsibility of the AN port FSM which shall indicate this status to the LE.

D.3.2 Information transfer between LE and AN

Figure D.1 shows the protocol architecture model for ISDN-PRA user port control functions.

For the bidirectional information transfer between the two user port FSMs, AN (ISDN-PRA) and LE (ISDN-PRA), function elements (FE20x) are used. They are carried on a layer 3 control protocol. This protocol includes an acknowledgement procedure to protect against loss of individual frames.

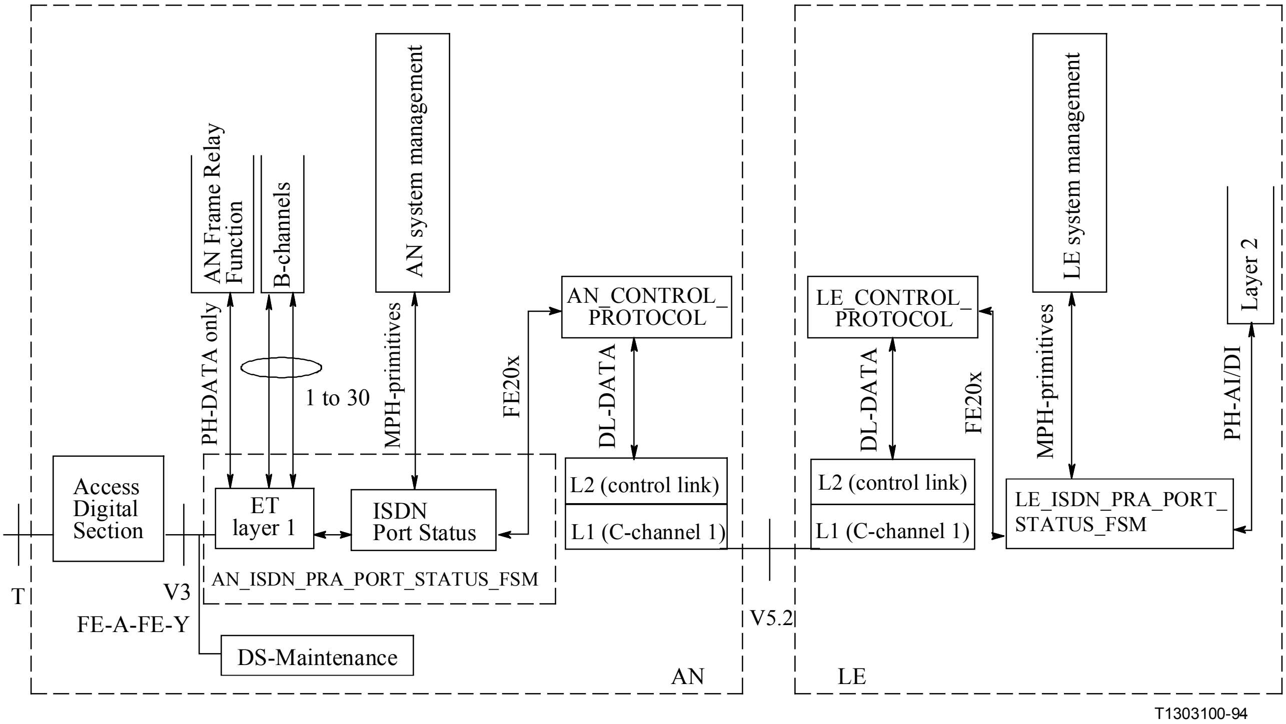


Figure D.1/G.965 – Protocol architecture for ISDN-PRA port control functions

D.3.3 Activation/deactivation

Since ISDN-PRAs are permanently activated there is no activation/deactivation procedure, i.e. the function elements related to activation/deactivation (FE10x) are not used in the V5.2 interface for ISDN primary rate user ports.

Layer 2 in the LE and the LE system management are only informed about operational status of the ISDN-PRA user port by PH-AI/DI and MPH-AI/DI primitives, respectively.

D.4 PSTN user port control

The contents of this clause are identical to D.3/G.964 [8].

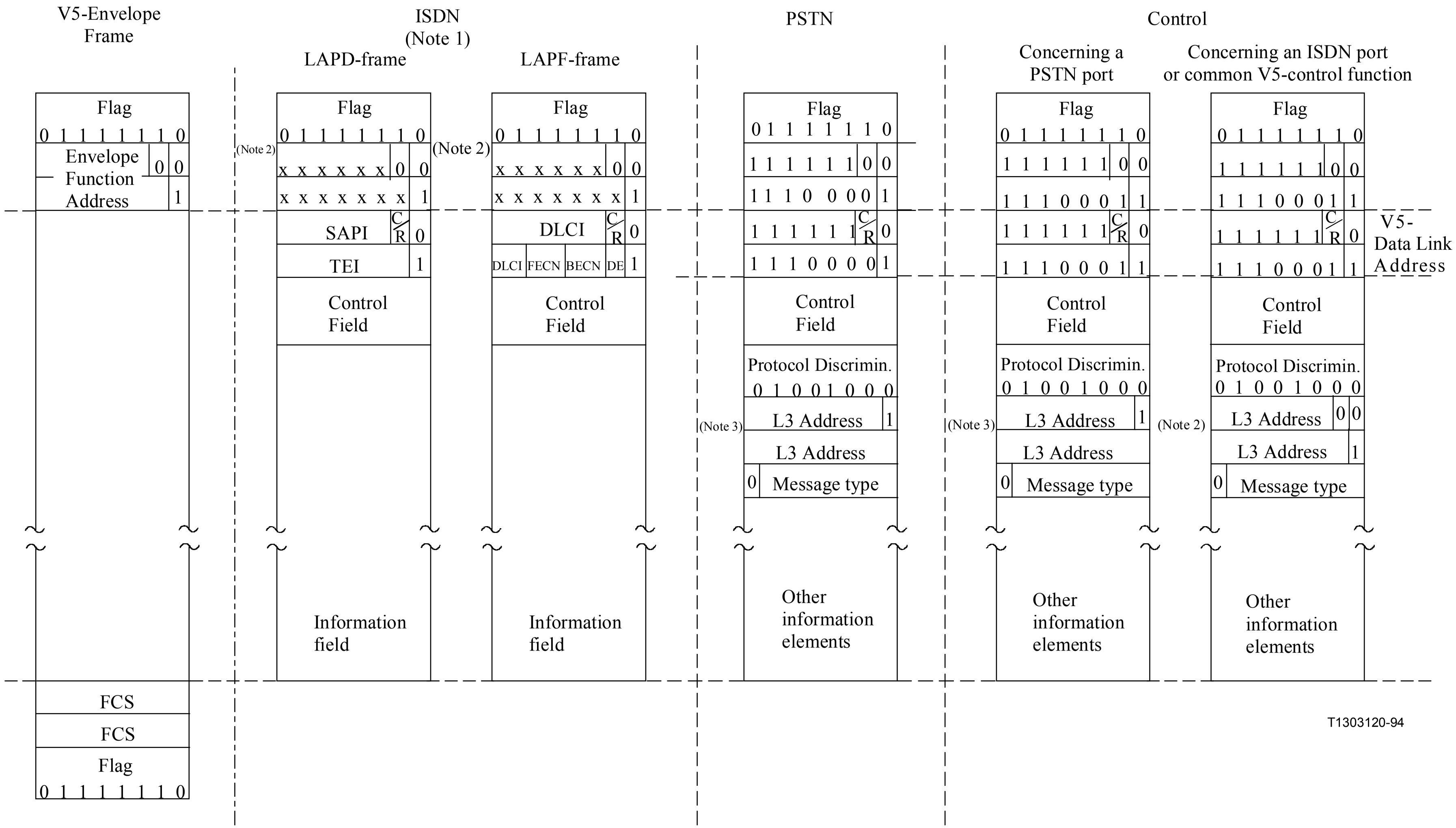
ANNEX E

Frame structures, message codepoints and addressing scheme for V5.2

Figures E.1 and E.2 show the possible structures of frames carried in the various communication channels and protocols.

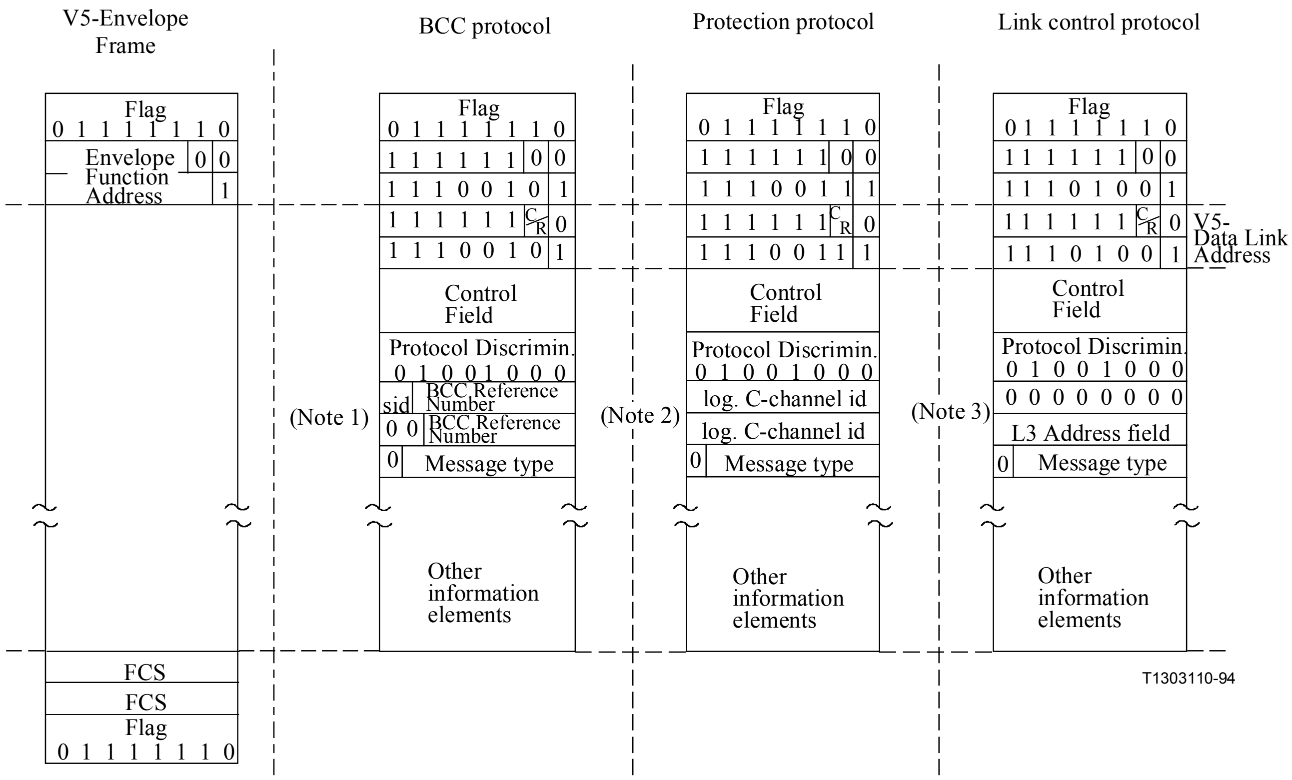
Table E.1 shows the message types allocated to the V5.2 interface.

Table E.2 shows the information elements allocated to the V5.2 interface.



NOTE 1 – For the ISDN case the address, control and information fields of the ISDN Layer 2 frames are not changed at the V5.2 interface.
NOTE 2 – For a given ISDN port these address fields have the same value.
NOTE 3 – For a given PSTN port these address fields have the same value.

Figure E.1/G.965 – Frame formats used in the V5.2 interface



sid Source ID

NOTE 1 – The BCC reference number identifies an individual BCC protocol process.
NOTE 2 – The logical C-channel id identifies an individual logical communications channel.
NOTE 3 – The L3 address field identifies an individual layer 1 link.

Figure E.2/G.965 – Additional frame formats used in the V5.2 interface

Table E.1/G.965 – Message codepoints used within the V5.2 interface

Bits							Message types
7	6	5	4	3	2	1	
0	0	0	–	–	–	–	PSTN protocol message types
0	0	0	0	0	0	0	ESTABLISH
0	0	0	0	0	0	1	ESTABLISH ACKNOWLEDGE
0	0	0	0	0	1	0	SIGNAL
0	0	0	0	0	1	1	SIGNAL ACKNOWLEDGE
0	0	0	1	0	0	0	DISCONNECT
0	0	0	1	0	0	1	DISCONNECT COMPLETE
0	0	0	1	1	0	0	STATUS ENQUIRY
0	0	0	1	1	0	1	STATUS
0	0	0	1	1	1	0	PROTOCOL PARAMETER

Table E.1/G.965 – Message codepoints used within the V5.2 interface

Bits							Message types
7	6	5	4	3	2	1	
0	0	1	0	–	–	–	Control protocol message types
0	0	1	0	0	0	0	PORT CONTROL
0	0	1	0	0	0	1	PORT CONTROL ACKNOWLEDGE
0	0	1	0	0	1	0	COMMON CONTROL
0	0	1	0	0	1	1	COMMON CONTROL ACKNOWLEDGE
0	0	1	1	–	–	–	Protection protocol message types
0	0	1	1	0	0	0	SWITCH-OVER REQUEST
0	0	1	1	0	0	1	SWITCH-OVER COMMAND
0	0	1	1	0	1	0	OS SWITCH-OVER COMMAND
0	0	1	1	0	1	1	SWITCH-OVER ACKNOWLEDGE
0	0	1	1	1	0	0	SWITCH-OVER REJECT
0	0	1	1	1	0	1	PROTOCOL ERROR
0	0	1	1	1	1	0	RESET SN COMMAND
0	0	1	1	1	1	1	RESET SN ACKNOWLEDGE
0	1	0	–	–	–	–	BCC protocol message types
0	1	0	0	0	0	0	ALLOCATION
0	1	0	0	0	0	1	ALLOCATION COMPLETE
0	1	0	0	0	1	0	ALLOCATION REJECT
0	1	0	0	0	1	1	DE-ALLOCATION
0	1	0	0	1	0	0	DE-ALLOCATION COMPLETE
0	1	0	0	1	0	1	DE-ALLOCATION REJECT
0	1	0	0	1	1	0	AUDIT
0	1	0	0	1	1	1	AUDIT COMPLETE
0	1	0	1	0	0	0	AN FAULT
0	1	0	1	0	0	1	AN FAULT ACKNOWLEDGE
0	1	0	1	0	1	0	PROTOCOL ERROR
0	1	1	0	–	–	–	Link control protocol message types
0	1	1	0	0	0	0	LINK CONTROL
0	1	1	0	0	0	1	LINK CONTROL ACK
NOTE – All other values are reserved.							

Table E.2/G.965 – Information elements allocated to the V5.2 interface

Bits (Note 1)								**Protocol**	**Information element**	**Reference** (Note 2)
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**			
0	–	–	–	–	–	–	–		VARIABLE LENGTH INFORMATION ELEMENTS	
0	0	0	0	0	0	0	0	PSTN	Sequence-number	14 (13.4.7.1)
0	0	0	0	0	0	0	1	PSTN	Cadenced-ringing	14 (13.4.7.2)
0	0	0	0	0	0	1	0	PSTN	Pulsed-signal	14 (13.4.7.3)
0	0	0	0	0	0	1	1	PSTN	Steady-signal	14 (13.4.7.4)
0	0	0	0	0	1	0	0	PSTN	Digit-signal	14 (13.4.7.5)
0	0	0	1	0	0	0	0	PSTN	Recognition-time	14 (13.4.7.6)
0	0	0	1	0	0	0	1	PSTN	Enable-autonomous-acknowledge	14 (13.4.7.7)
0	0	0	1	0	0	1	0	PSTN	Disable-autonomous-acknowledge	14 (13.4.7.8)
0	0	0	1	0	0	1	1	PSTN	Cause	14 (13.4.7.9)
0	0	0	1	0	1	0	0	PSTN	Resource-unavailable	14 (13.4.7.10)
0	0	1	0	0	0	1	0	PSTN	Enable-metering	14 (13.4.7.11)
0	0	1	0	0	0	1	1	PSTN	Metering-report	14 (13.4.7.12)
0	0	1	0	0	1	0	0	PSTN	Attenuation	14(13.4.7.13)
0	0	1	0	0	0	0	0	Control	Control-function-element	15.4 (14.4.2.5.4)
0	0	1	0	0	0	0	1	Control	Control-function-D	15.4 (14.4.2.5.5)
0	0	1	0	0	0	1	0	Control	Variant	15.4 (14.4.2.5.6)
0	0	1	0	0	0	1	1	Control	Interface-ID	15.4 (14.4.2.5.7)
0	0	1	1	0	0	0	0	Link control	Link control function	16.3.2.2
0	1	0	0	0	0	0	0	BCC	User port identification	17.4.2.1
0	1	0	0	0	0	0	1	BCC	ISDN port Time Slot identification	17.4.2.2
0	1	0	0	0	0	1	0	BCC	V5 time slot identification	17.4.2.3
0	1	0	0	0	0	1	1	BCC	Multi-slot map	17.4.2.4
0	1	0	0	0	1	0	0	BCC	Reject cause	17.4.2.5
0	1	0	0	0	1	0	1	BCC	Protocol error cause	17.4.2.6
0	1	0	0	0	1	1	0	BCC	Connection incomplete	17.4.2.7
0	1	0	1	0	0	0	0	Protection	Sequence number	18.5.2
0	1	0	1	0	0	0	1	Protection	Physical C-channel identification	18.5.3
0	1	0	1	0	0	1	0	Protection	Rejection cause	18.5.4
0	1	0	1	0	0	1	1	Protection	Protocol error cause	18.5.5
1	–	–	–	–	–	–	–		SINGLE OCTET INFORMATION ELEMENTS	
1	0	0	0	X	X	X	X	PSTN	Line information	14 (13.4.6.2)
1	0	0	1	X	X	X	X	PSTN	State	14 (13.4.6.3)
1	0	1	0	X	X	X	X	PSTN	Autonomous signalling sequence	14 (13.4.6.4)
1	0	1	1	X	X	X	X	PSTN	Sequence response	14 (13.4.6.5)
1	1	0	0	0	0	0	0	PSTN	Pulse-notification	14 (13.4.6.1)
1	1	1	0	X	X	X	X	Control	Performance grading	15.4 (14.4.2.5.2)
1	1	1	1	X	X	X	X	Control	Rejection cause	15.4 (14.4.2.5.1)

NOTE 1 – All other values are reserved.
NOTE 2 – References within parentheses are references to relevant clause in ITU-T G.964 [8].

ANNEX F

The concept and requirements for the upgrade of a V5.1 interface to a V5.2

The contents of this annex are identical to that of Annex F/G.964 [8].

ANNEX G

AN requirements for pulse dialling

The contents of this annex are identical to that of Annex H/G.964 [8].

ANNEX H

Layer 3 error detection procedures

The contents of this annex are identical to that of Annex K/G.964 [8].

ANNEX J

Protection protocol – Explanatory notes and information flow

J.1 Additional information on the principles of the protection protocol

The AN may only request a switch-over, but the switch-over command (SWITCH-OVER COM or OS-SWITCH-OVER COM message) will always come from the LE side. On receipt of the switch-over command, the AN system management will only verify whether resources for a successful switch-over are available or not. The result will be notified to the LE by either a SWITCH-OVER ACK or a SWITCH-OVER REJECT message. The AN cannot check whether switch-over will be successful. If, for any reason, problems related to the switch-over procedure are identified later on, the AN may indicate this to the LE by issuing a new request to the LE.

Before a SWITCH-OVER command is sent from the LE to the AN, the LE system management/resource manager shall verify whether switch-over is, in principle, possible. If, for any reason, problems related to the switch-over procedure are identified later on, the LE may initiate a new switch-over by sending a new SWITCH-OVER command to the AN.

If a SWITCH-OVER ACK message, sent from the AN side, gets lost timer TSO1 or TSO2 will expire and the LE side will retransmit the SWITCH-OVER COM or OS-SWITCH-OVER COM message. Since switch-over in the AN has already been performed, the AN will respond with a SWITCH-OVER REJECT message with the cause "requested allocation exists already". The LE system management shall regard this message as an acknowledgement of the switch-over in the AN and shall as a result perform switch-over in the LE.

Switch-over processes shall not be processed simultaneously. Thus, if a switch-over command is sent from the LE to the AN, the LE side has to wait for a response before a new SWITCH-OVER command may be sent, even if problems are identified in the meantime by the LE-side related to the previous SWITCH-OVER command.

If a failure is detected almost simultaneously, both LE and AN side may request a switch-over procedure at the same time. In this case contention is resolved in the LE since the LE is the master for the protection switch-over (see Figure J.7).

J.2 Information flow

Figures J.1 to J.7 show some examples for the information flow of the Protection protocol.

LE-initiated switch-over triggered autonomously by detected failure or by intervention of the operator is shown in Figure J.1.

AN-initiated switch-over triggered autonomously by detected failure or by intervention of operator is shown in Figure J.2.

Rejection of LE-initiated switch-over by AN is shown in Figure J.3.

Rejection of AN-initiated switch-over by LE is shown in Figure J.4.

LE initiated switch-over, retransmissions due to loss of a message, is shown in Figure J.5.

LE initiated switch-over, retransmissions due to loss of message is shown in Figure J.6.

Switch-over initiated simultaneously by LE and AN side is shown in Figure J.7.

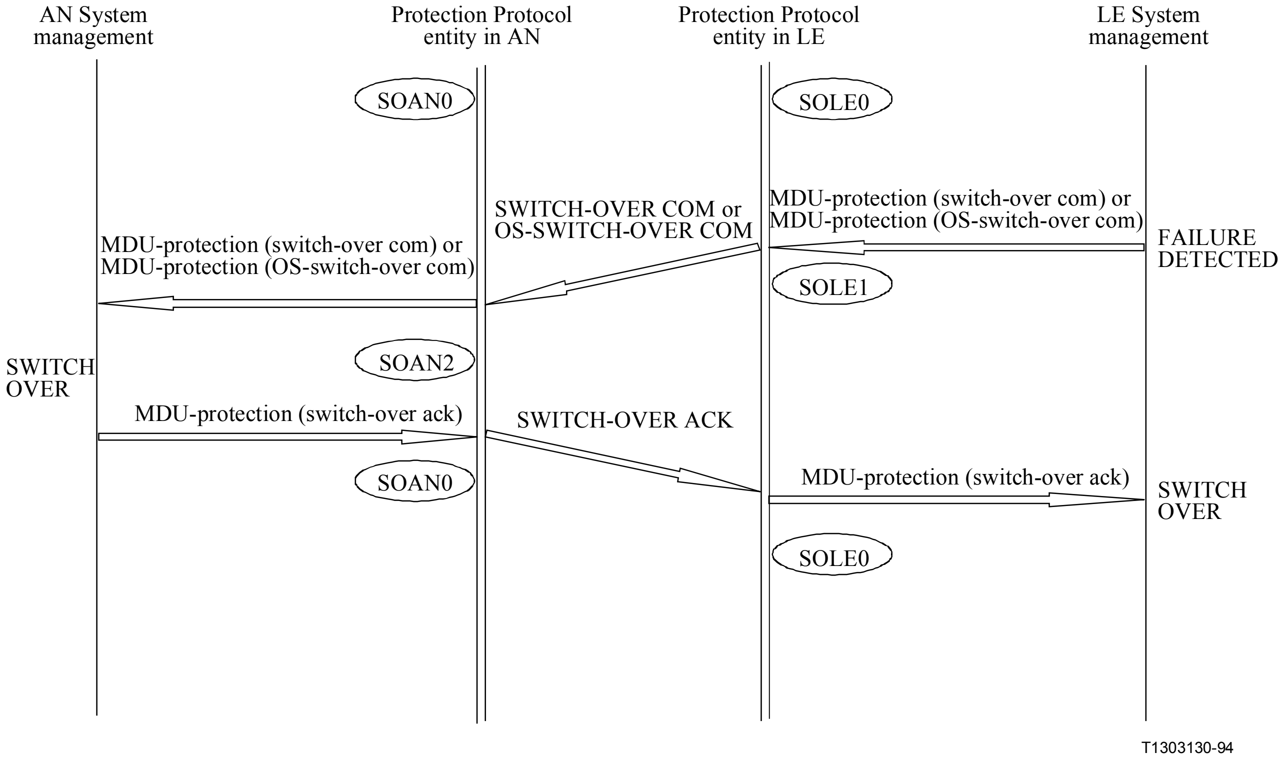


Figure J.1/G.965 – LE initiated autonomous switch-over between physical C-channels

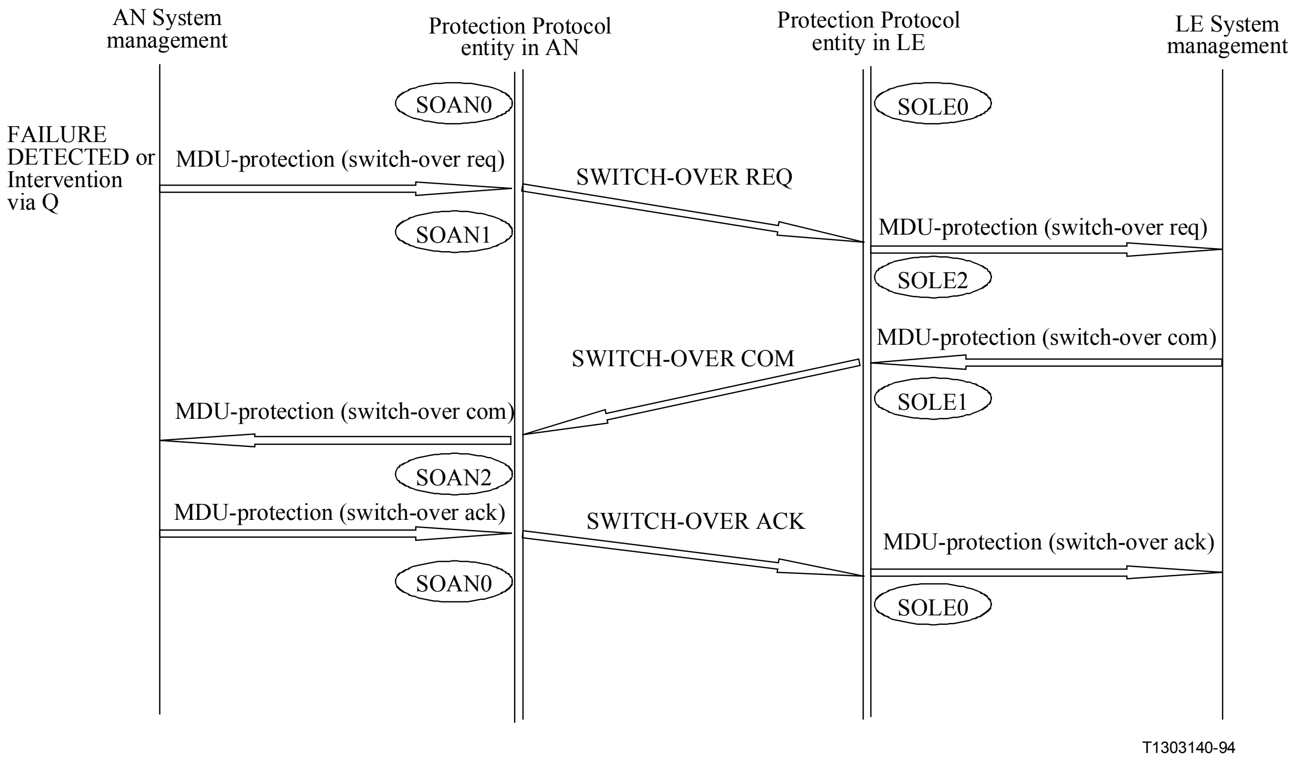


Figure J.2/G.965 – AN-initiated autonomous switch-over

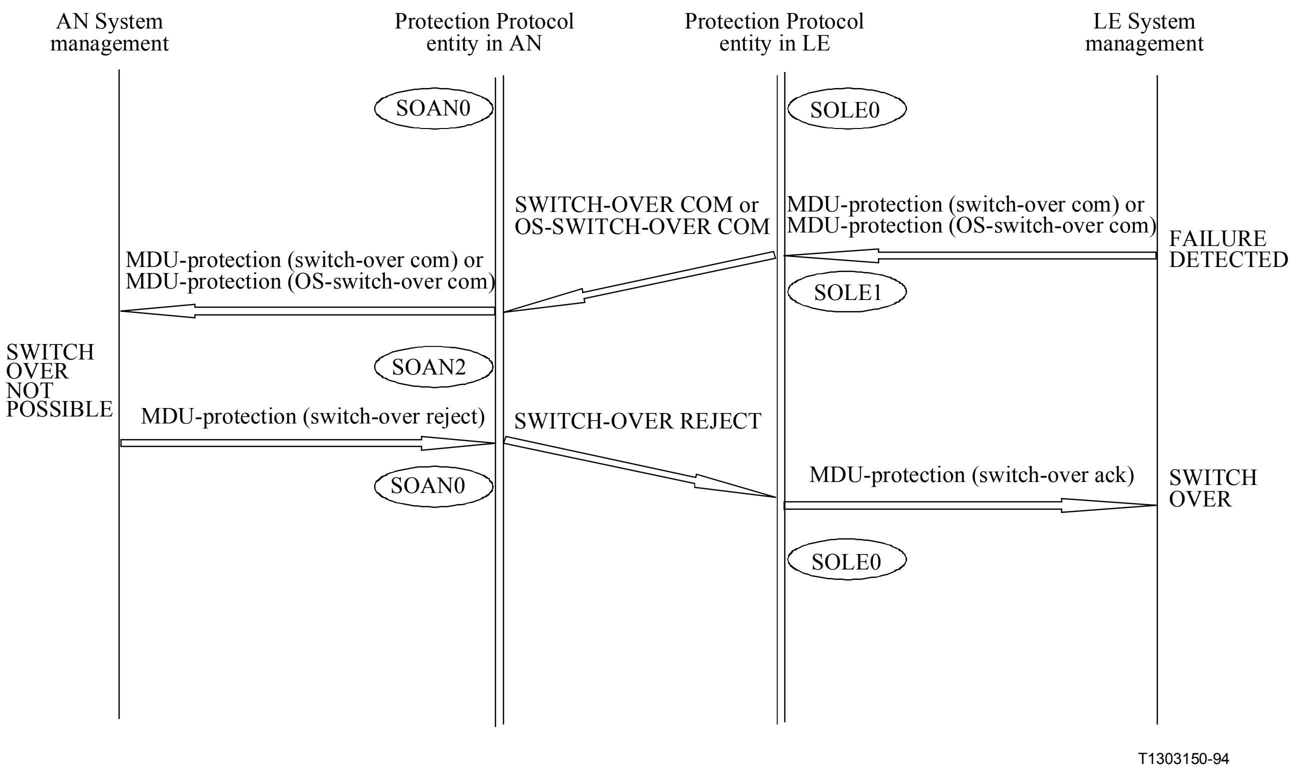


Figure J.3/G.965 – Rejection of LE-initiated switch-over by AN

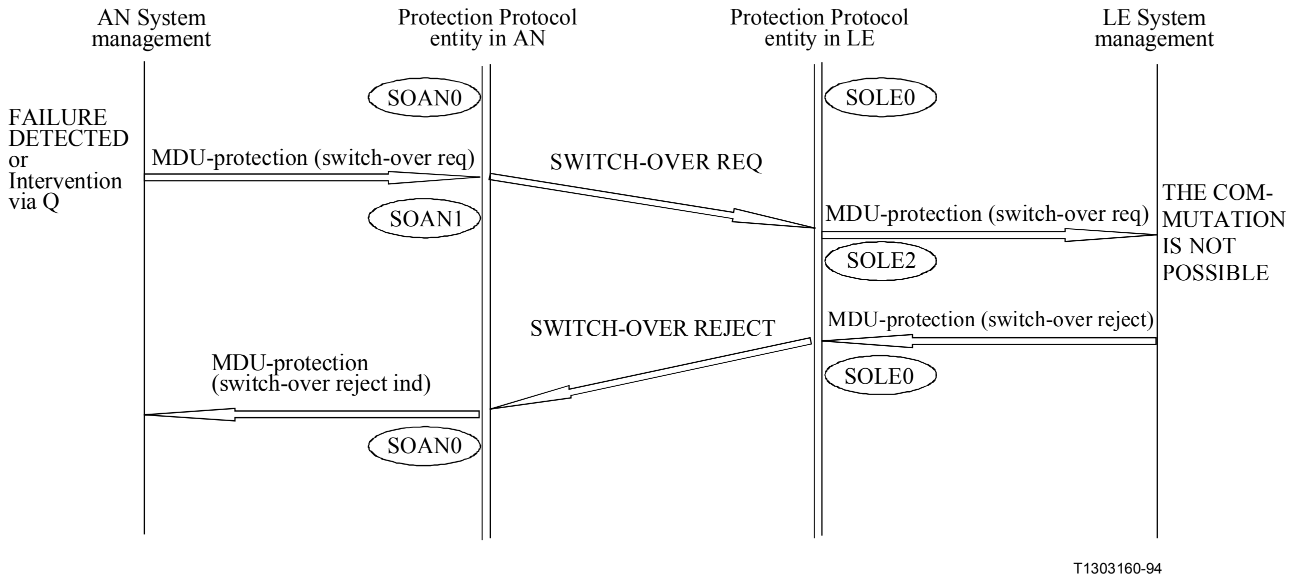
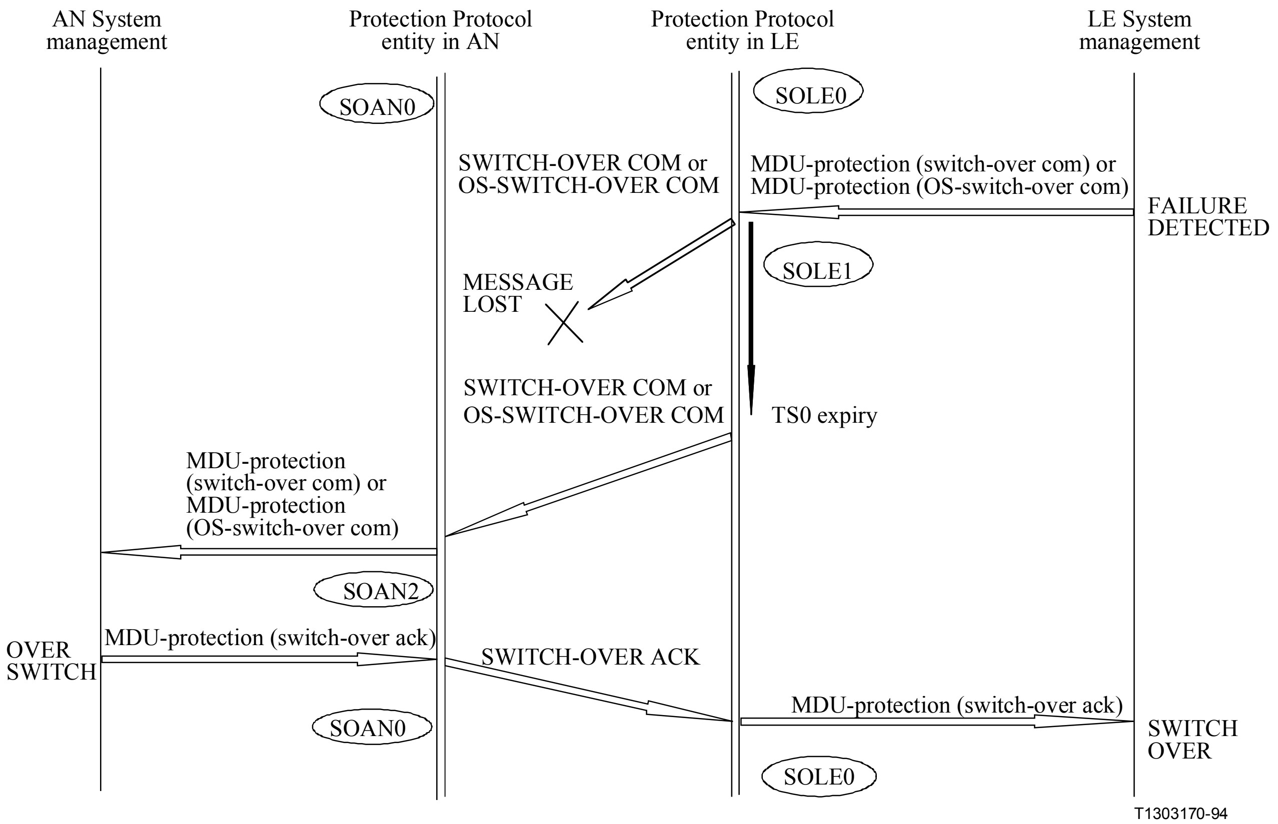
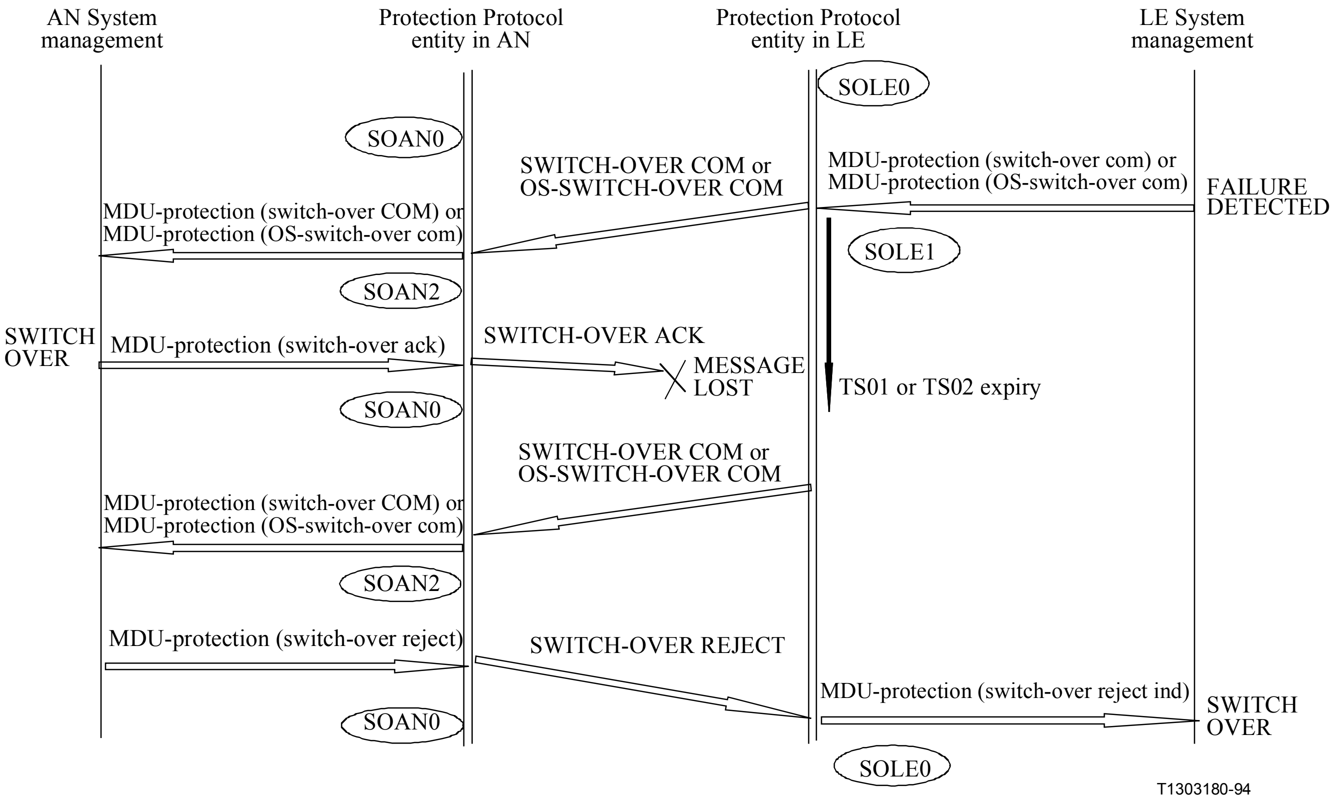


Figure J.4/G.965 – Rejection of AN-initiated switch-over by LE



NOTE – The figure shows an example, where no re-transmission in L2 occurs due to the nature of the failure condition.

Figure J.5/G.965 – LE-initiated switch-over with retransmissions (message loss)



NOTE – The figure shows an example, where no re-transmission in L2 occurs due to the nature of the failure condition.

Figure J.6/G.965 – LE-initiated switch-over (retransmissions due to message loss)

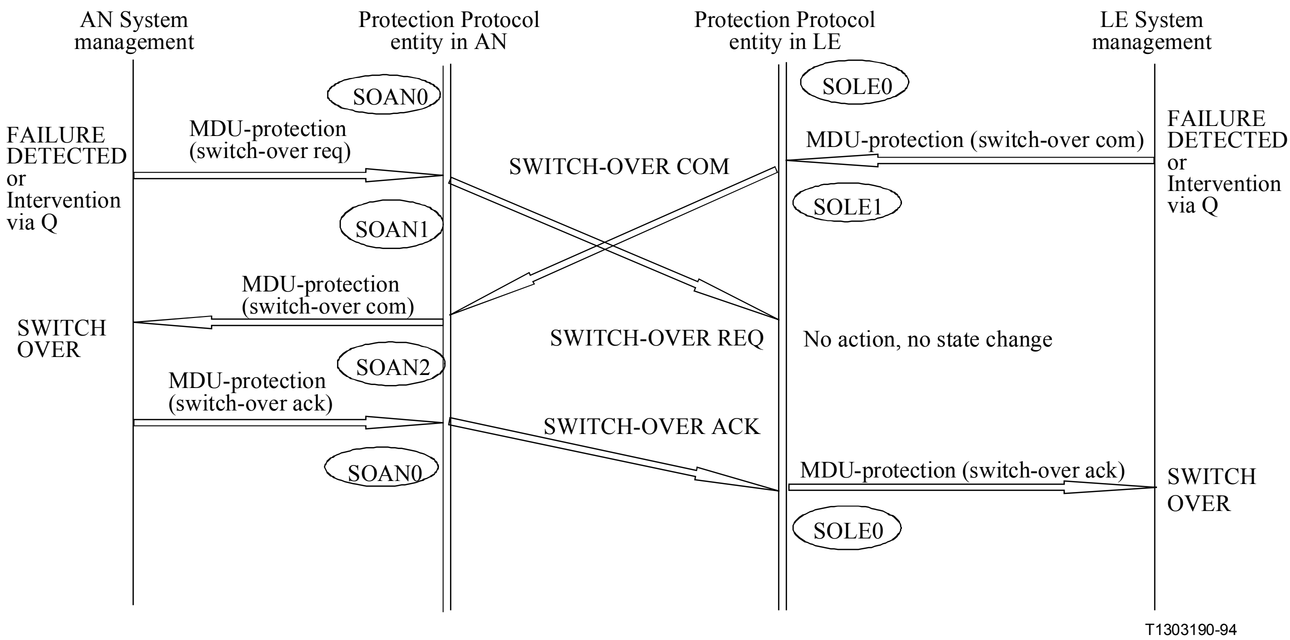


Figure J.7/G.965 – Switch-over initiated simultaneously by LE and AN

ANNEX K

BCC protocol application principles

K.1 Introduction

This annex gives normative information on how the BCC protocol shall be used by the LE and the AN, in order to meet the service demands on the V5.2 interface.

The resource management entities manage the resources involved in the support of bearer channel connections (time slots, user ports and ISDN user port channels) by means of the BCC protocol. The functionality is shared among different entities as follows:

– the LE and AN resource management entities are responsible for the maintenance of the resources available for supporting bearer channel connections and their status (e.g. allocated or de-allocated);

– the control of the BCC protocol (message interchange between the LE and the AN) is under the responsibility of the BCC protocol entity;

– the resource management entities will receive service requests from different entities in the LE (e.g. PSTN national protocol, DSS1 national protocol, management system), however the relationship between the resource management entities and the entities requesting BCC services is outside the scope of this Recommendation.

The BCC protocol provides the means in order to support different types of user services:

a) Switched service, where the resource management entity shall allocate switched connections for the support of the user calls, these connections will be available for the lifetime of the call. The allocation and de-allocation processes under the control of the resource management entity shall be triggered from the national PSTN or DSS1 entities.

b) Semi-permanent leased line service, where the resource management entity shall allocate switched connections for the support of these long period user connections. The allocation and de-allocation processes under the control of the resource management entity shall be triggered from the management system entity due to a request via the Q_{LE} interface.

   The use of the BCC protocol for the establishment of this type of connections guarantees that the resource management entity is fully informed as to the status of these bearer channel connections. In the event of the 2048 kbit/s link on which the semi-permanent line is provided becoming faulty, the resource management entity shall establish another path.

c) Pre-connected bearer channel service, where the resource management entity shall allocate switched connections in order to provide to the user bandwidth in the form of 64 kbit/s bearer channels or their multiples. The allocation and de-allocation processes under the control of the resource management entity shall be triggered from the management system entity due to a request via the Q_{LE} interface.

   This service provides to user permanent connections between the LE and the user port via the V5.2 interface. This service should be used when it is important that the concentration factor provided by the V5.2 interface may not lead to the blocking of crucial services (e.g. the telephony service for a fire station).

   The use of the BCC protocol for the establishment of this type of connections guarantees that the resource management entity is fully informed as to the status of these bearer channel connections. In the event of the 2048 kbit/s link on which the pre-connected bearer channel is provided becoming faulty, the resource management entity shall establish another path and report what it has done via Q_{LE}.

K.2 Time slot usability

Time slots 1 to 14 and 17 to 30 of all 2048 kbit/s links of a V5.2 interface shall be available for allocation as bearer channels.

Where time slots 15, 16 or 31 of any 2048 kbit/s link are not provisioned for use as a physical C-channel, they shall be available for use as a bearer channel.

Bearer channels on a V5.2 interface shall be available for use for any service (e.g. PSTN bearer, ISDN B-channel, ISDN H-channel). There shall be no dedication of bearer channels, bearer channel groups or 2048 kbit/s links to service/channel types.

K.3 Time slot allocation and de-allocation rules

K.3.1 General

The following rules shall be applied by the LE and, where appropriate, the AN, in allocating V5.2-interface time slots to bearer connections:

a) The LE shall have sole responsibility for time slot allocation.

b) The AN may reject a connection request due to a fault or error or due to AN internal blocking.

c) The LE national PSTN protocol entity or the national ISDN protocol entity may request a new time slot allocation.

d) It is not possible to proceed with a de-allocation process of a bearer channel connection for which all the data required within the DE-ALLOCATION message is not included.

   When the LE does not know all the relevant data identifying a bearer channel connection, before starting the de-allocation process, it shall request for the remaining information from the AN by using the audit procedure.

   If the result of the audit procedure is a notification that such a connection does not exist, the LE shall clear internally the BCC bearer channel connection record.

e) ISDN-BA or ISDN-PRA user port B-channel(s), required for a call, shall have been internally reserved by the DSS1 protocol entity, before the V5-interface time slot(s) is set up using the BCC protocol. Then, using the DSS1 procedures, the B-channel(s) will be allocated and notified to the ISDN subscriber within the appropriate DSS1 message. A further rearrangement of B-channels may be necessary under subscriber control.

   This maintains DSS1 service capability and enables the BCC connection request to convey the full identity of both ends of the AN connection.

f) In allocating time slots, the LE shall apply connection packing, i.e. allocate connections to the 2048 kbit/s links of a V5.2 interface in a preferential order. 2048 kbit/s links having more than one physical C-channel shall be given appropriate preference. These rules shall be applied to all connections, in order to minimize congestion probability for multi-slot connections.

   Connection packing increases the service impact of undetected faults, particularly at times of low traffic. This can be ameliorated by not having a single fixed preference. The effect is generally a trade-off between failure performance and multi-slot connection congestion performance. LE implementation for support of V5.2 interfaces should take this trade-off into account.

g) AN semi-permanent connections and pre-connected bearer channels shall be re-allocated by LE management on other 2048 kbit/s links (if available), in the event of failure of the 2048 kbit/s link carrying them, or in the event of AN internal failure reported by the BCC protocol.

Switched bearer connections shall not be reallocated to other V5.2-time slots, in the event of failure.

h) In the case of terminating ISDN calls (calls offered by the LE to the AN), the LE has to indicate in the DSS1 SETUP message to be sent to the ISDN access, the identification of the B or H-channel to be used for the call.

Hence, before sending the SETUP message, the LE has to ensure the availability of the necessary time slots in the interface to be used as bearer channels, and that these time slots are properly allocated to the ISDN port. This represents a need for protocol synchronization in such a way that the allocation process has to be completed before sending the DSS1 SETUP message.

In the case of the reception of an ALLOCATION REJECT message, the BCC protocol entity in the LE shall notify the event to the resource management entity by the MDU-BCC (allocation reject indication) primitive, which shall also send the proper notification to the ISDN protocol entity. Upon reception of this indication, the ISDN protocol entity may request another bearer channel allocation before sending the RELEASE COMPLETE to the ISDN subscriber. The number of these re-attempts, if any, will depend upon implementation decisions and DSS1 timing constraints controlled by the ISDN protocol entity.

i) In the case of originating ISDN calls (calls offered by the AN to the LE), the LE has to indicate in the DSS1 message sent as the answer to the received SETUP message (i.e. ALERTING, CALL PROCEEDING, CONNECT) the identification of the B- or H-channel to be used for the call.

Hence, before sending the proper answer to the received SETUP message the LE has to ensure the availability of the necessary time slots in the interface to be used as bearer channels, and that these time slots are properly allocated to the ISDN port. This represents a need for protocol synchronization in such a way that the allocation process has to be completed before sending the DSS1 message in response to the received SETUP message.

j) In the case of terminating PSTN calls (calls offered by the LE to the AN), in general the LE before sending the "initial ring signal", has to ensure the availability of a bearer channel for the call. However there are some cases in which a PSTN signalling path is established and no allocation of a bearer channel is required.

k) In the case of originating PSTN calls (calls offered by the AN to the LE), in general the LE before sending the "dialling tone", has to ensure the availability of a bearer channel for the call. However there are some cases in which a PSTN signalling path is established and no allocation of a bearer channel is required.

l) When clearing ISDN or PSTN calls (either initiated by the user or the network), the LE shall initiate the proper action towards the AN in order to clear the V5.2 resources allocated to that particular call.

When initiating an ISDN port related de-allocation process, the LE may disconnect the bearer channel (V5-time slot) from the call connection and proceed with the ISDN call clearing before the completion of the de-allocation process (i.e. synchronization between the DSS1 protocol and the BCC de-allocation process is not required).

m) Table K.1 gives information on when to use the different reject cause types in the BCC protocol procedures.

n) Other than the possible allocation/de-allocation of bearer channels, the provision of DSS1 supplementary services shall not require any other functions from the BCC protocol.

Table K.1/G.965 – Use of the reject cause types

Cause	Description
Unspecified	A fault not otherwise covered by this table has been found.
Access network fault	The allocation or de-allocation process cannot be completed because an internal AN fault has been identified.
Access network blocked (internally)	The allocation process cannot be completed because an internal AN blocking has been discovered.
Connection already present at the PSTN user port to a different V5-time slot	The allocation process cannot be completed because a connection already exists on the selected PSTN port to a different time slot.
Connection already present at the time slot(s) to a different port or ISDN user port time slot	The allocation process cannot be completed because a connection already exists on the selected V5.2 time slot(s) to a different user port or user port time slot.
Connection already present at the ISDN user port time slot(s) to a different time slot(s)	The allocation process cannot be completed because a connection already exists on a selected user port time slot(s) to a different time slot(s).
User port unavailable (blocked)	The allocation process cannot be completed because the selected user port is not available for service.
De-allocation can not be completed due to incompatible data content	The de-allocation process cannot be completed because the provided data regarding the time slot, user port and user port time slot does not match any user port connection.
De-allocation can not be completed due to V5-time slot(s) data incompatibility	The de-allocation process cannot be completed because the provided data regarding the V5-time slot(s) does not match the AN data.
De-allocation can not be completed due to port data incompatibility	The de-allocation process cannot be completed because the provided data regarding the user port does not match an AN user port.
De-allocation can not be completed due to user port time slot(s) data incompatibility	The de-allocation process cannot be completed because the provided data regarding the user port time slot(s) does not match the AN user port(s).
User port not provisioned	The allocation process cannot be completed because the identified user port has not been provisioned.
Invalid V5-time slot(s) identification(s)	The identification of the V5-time slot(s) does not match the one(s) available for use as bearer channels.
Invalid 2048 kbit/s link identification	The identification of the 2048 kbit/s link at the V5.2 interface does not match any available link.
Invalid user port time slot(s) identification(s)	The identification of the User port time slot(s) does not match the one(s) available at the selected ISDN user port.
V5-time slot(s) being used as physical C-channel(s)	The process cannot be completed because the identified V5-time slot is being used as a physical C-channel.
NOTE – No other value is applicable.	

K.3.2 Multi-slot connections

The following rules shall be applied by the LE and, where appropriate, the AN, in allocating V5.2-interface time slots to multi-slot (i.e. n × 64 kbit/s) bearer connections:

a) At the beginning of a call (or semi-permanent or pre-connected bearer channel allocation), all time slots for a multi-slot connection shall be allocated simultaneously by one single BCC allocation process.

b) During a call (or semi-permanent or pre-connected allocation), it shall be possible for time slots constituting a multi-slot connection to be released individually or for any proportion of the time slots to be released simultaneously. This capability enables the bandwidth allocation to be reduced for the remaining part of a call (or semi-permanent or pre-connected allocation).

c) At the end of a call (or semi-permanent or pre-connected allocation), all time slots constituting a multi-slot connection shall be released simultaneously.

d) The multiple time slots required for a multi-slot connection shall be selected from any free time slots (within a single 2048 kbit/s link) and need not be in a block of contiguous time slots.

e) The structural attribute of time slot sequence integrity (TSSI) shall apply to the connection element between the user-network interface and the V5 interface. Thus:
   – at the user-network interface and the V5 interface, time slots are implicitly or explicitly demarcated for each channel of an aggregate of channels;
   – the information parts delivered from the time slots at the receiving end are in the same order as submitted at the transmitted end;
   – all time slots used at the user side shall be in the same ISDN-BA or ISDN-PRA interface;
   – all time slots used at the V5 interface shall be in the same 2048 kbit/s link.

f) The structural attribute of 8 kHz integrity shall apply to the connection element between the user-network interface and the V5 interface. Thus:
   – at the user-network interface and the V5 interface, intervals of 125 μs are implicitly or explicitly demarcated (e.g. by frame boundaries); and
   – all bits submitted within a single demarcated 125 μs interval are delivered within a corresponding single demarcated 125 μs interval.

g) If a pre-connected bearer channel is required to support multi-rate switched services (e.g. H0 or H12), as opposed to 64 kbit/s services alone, it shall be set up as an n × 64 kbit/s connection, to ensure TSSI and 8 kHz integrity for such services.

K.3.3 Override capability

In order to better support some user service capabilities, the LE, when allocating bearer channel connections, may use the override capability. This allows the bearer channel that was connected to one B-channel of an ISDN user port to be connected to another B-channel on the same ISDN user port.

The override capability can only be used on single 64 kbit/s bearer channel allocation processes.

K.4 Audit procedure rules

The BCC protocol includes the necessary means in order to allow the LE to obtain from the AN information regarding certain connection for which the information is partially unknown for the LE. This procedure shall comply with certain rules such as:

a) the LE shall start an auditing only when no other process (allocation or de-allocation) is pending of completion;

b) when an auditing process has been started, no other allocation or de-allocation process shall be started by the LE;

c) several auditing processes may be running simultaneously, using different BCC reference numbers;

d) auditing processes shall be started by the resource management entity in the LE, or by the request from the system management entity;

e) Table K.2 gives information on when to use the different reason values given in the BCC protocol.

Table K.2/G.965 – Use of the reason values

Reason	Use
Incomplete normal	The audit process cannot be completed because the connection does not exist.
User port not provisioned	The audit process cannot be completed because the identified user port has not been provisioned.
Invalid V5-time slot identification	The identification of the bearer channel does not match the one available for the bearer channel under audit.
Invalid 2048 kbit/s link	The identification of the 2048 kbit/s link at the V5.2 interface does not match the one supporting the bearer channel under audit.
Time slot used as physical C-channel	The process cannot be completed because the identified time slot is being used as a physical C-channel.

K.5 AN internal failure notification rules

The BCC protocol includes the necessary means in order to allow the AN to notify to the LE internal failures affecting internal connections supporting bearer channels. For the use of this procedure the following rules apply:

a) The AN shall notify all the internal connections supporting bearer channel connection when an internal failure happens.

   Internal failures not affecting allocated bearer channels will not be notified via the BCC protocol.

b) The AN internal failure notification shall be done on single 64 kbit/s connection basis starting an individual process for each of them.

c) When notifying an internal failure, the AN shall provide as much information as possible in order to allow the LE to identify the bearer connection. However, if the AN is not able to provide all the required information, the LE will obtain the complete information from its internal data on the basis of the partial information received.

K.6 AN internal failure rules

When an AN internal failure is notified by the AN to the LE by an AN FAULT message containing the User Port Identification IE and in case of ISDN the ISDN Port Channel Identification IE as well as the V5 Time Slot Identification IE, all resources in the AN related to the connection affected are freed internally. The resource management entity in the LE shall initiate internal de-allocation for the notified bearer channel connection and shall notify the event to the PSTN/ISDN protocol entities for proper service actions to be taken.

When an AN internal failure is notified by the AN to the LE by an AN FAULT message containing either the User Port Identification IE and in case of ISDN the ISDN Port Channel Identification IE or the V5 Time Slot Identification IE but not all the IEs mentioned, the resource management entity in the LE shall initiate de-allocation for the notified bearer channel connection send a DE-ALLOCATION message to the AN and shall notify the event to the PSTN/ISDN protocol entities for proper service actions to be taken.

In the case that the LE resource management entity identifies that the affected bearer channel connection is part of a multi-slot arrangement, no action shall be taken by the resource management entity on the rest of the bearer channel connections. The triggering of the proper action to be taken (for example: de-allocating the rest of the bearer channel connections) is an ISDN protocol entity responsibility on the basis of the service requirements.

K.7 BCC protocol errors

The BCC protocol entities shall be able to detect three different categories of protocol errors:

a) Errors referring to an alive BCC process (e.g. due to the absence of response to a retransmitted ALLOCATION message). These errors shall be notified to the resource management entity.

b) Errors referring to a non existent BCC process (e.g. due to the reception of an ALLOCATION COMPLETE message when the LE is in the Bcc0 state). These errors shall be notified to the system management entity.

c) Errors referring to the protocol error handling procedures (see 17.5.8) shall be notified to the system management.

K.8 Arrow diagrams – Examples of BCC protocol and DSS1 coordination

K.8.1 ISDN call initiated by the subscriber

K.8.1.1 Normal procedure

The arrow diagram showing the interaction of the BCC protocol with DSS1 for the case: Call initiated by the subscriber (normal procedure) is given in Figure K.1.

In the case of an ISDN call set-up and bearer channel allocation, the need for protocol synchronization is shown; the allocation process has to be completed before sending the DSS1 message in response to the received SETUP message.

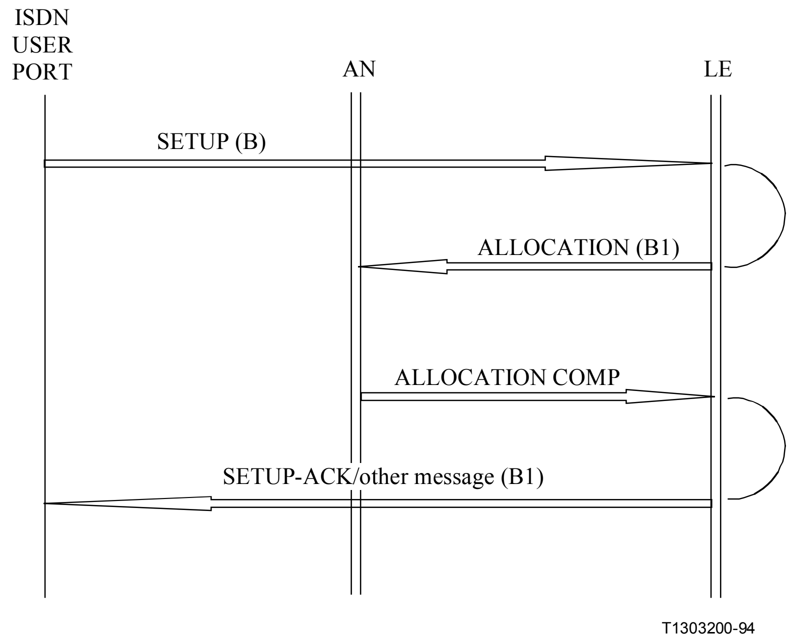


Figure K.1/G.965 – ISDN call initiated by subscriber – Normal procedure

K.8.1.2 Exceptional procedure

The arrow diagram showing the interaction of the BCC protocol with DSS1 for the case: Call initiated by the subscriber (exceptional procedure) is given in Figure K.2.

K.8.1.3 Simultaneous ISDN call set-up (from the same ISDN port)

The arrow diagram showing the interaction of the BCC protocol with DSS1 for the case: Simultaneous ISDN call set-up from one user port is given in Figure K.3.

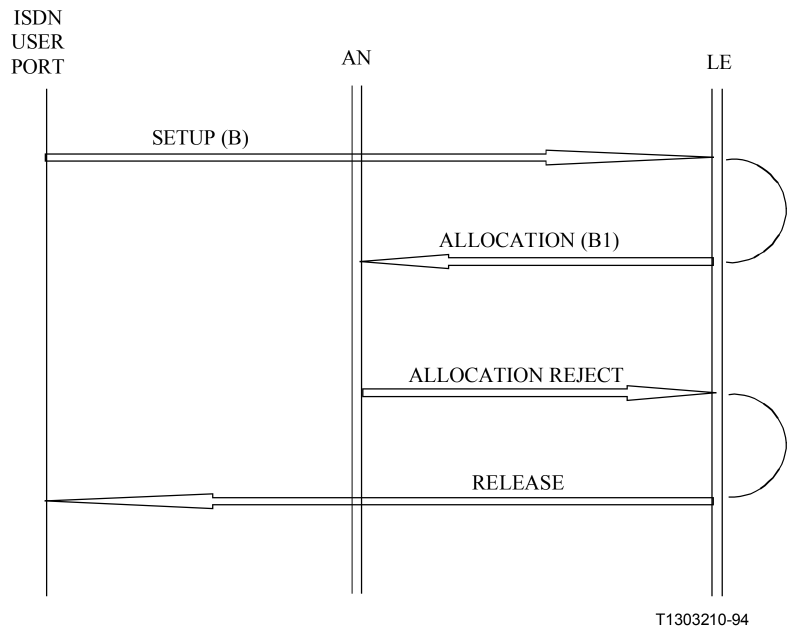


Figure K.2/G.965 – ISDN call initiated by subscriber – Exceptional procedure

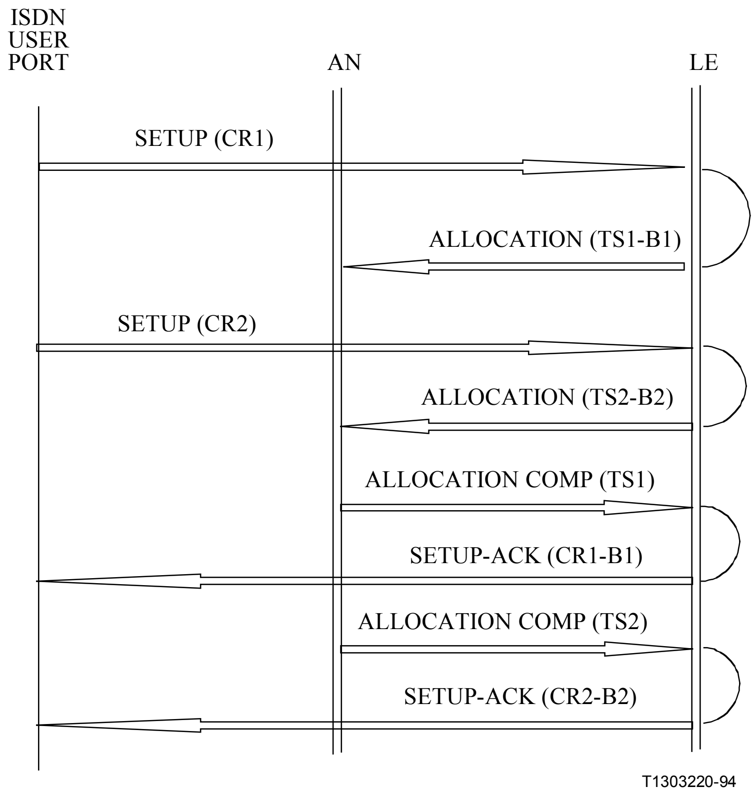


Figure K.3/G.965 – Simultaneous ISDN call set-up from one ISDN user port

K.8.2 ISDN call initiated by the network

K.8.2.1 B-channel negotiation not allowed (e.g. passive bus configuration)

The arrow diagram showing the interaction of the BCC protocol with DSS1 for the case: ISDN call initiated by the network (B-channel negotiation not allowed) is given in Figure K.4.

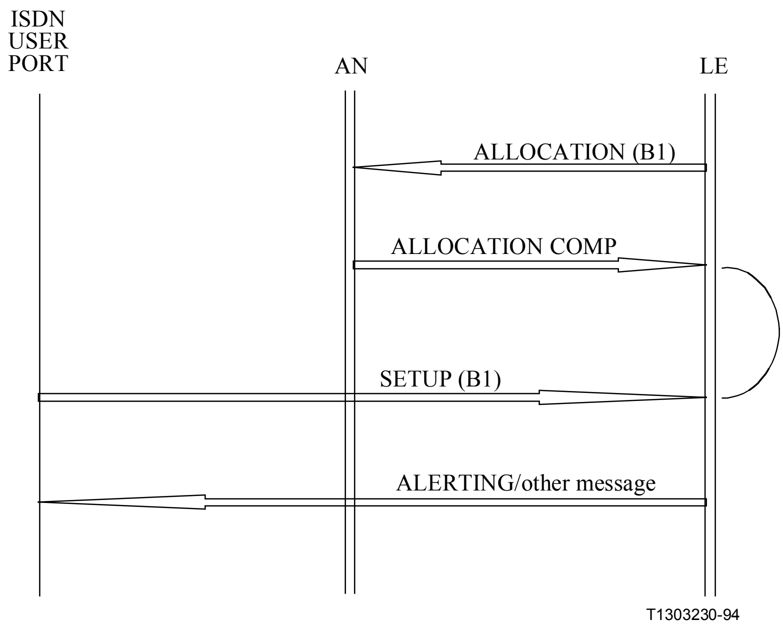


Figure K.4/G.965 – ISDN call initiated by the network – B-channel negotiation not allowed

K.8.2.2 B-channel negotiation allowed (e.g. point-to-point configuration)

The arrow diagram showing the interaction of the BCC protocol with DSS1 for the case: ISDN call initiated by the network (B-channel negotiation allowed) is given in Figure K.5.

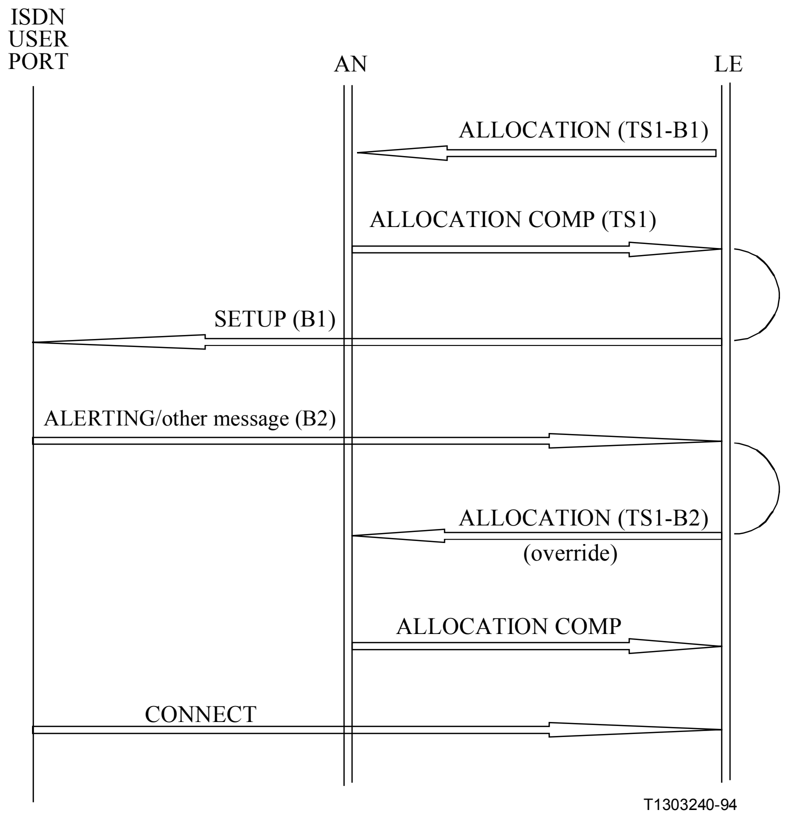


Figure K.5/G.965 – ISDN call initiated by the network – B-channel negotiation allowed

K.8.2.3 ISDN call waiting supplementary service support

The arrow diagram showing the interaction of the BCC protocol with DSS1 for the case where no B-channel is available on the UNI: is given in Figure K.6.

At the point indicated in Figure K.6 by an X), an internal reallocation takes place in the LE, the resources (time slot and B-channel) being used by a port for a call are reallocated to a new call that has to be terminated at the very same end-point. The support of this ISDN supplementary service is an internal function of the LE (BCC resource management entity) involved, without any implication in the BCC protocol entity.

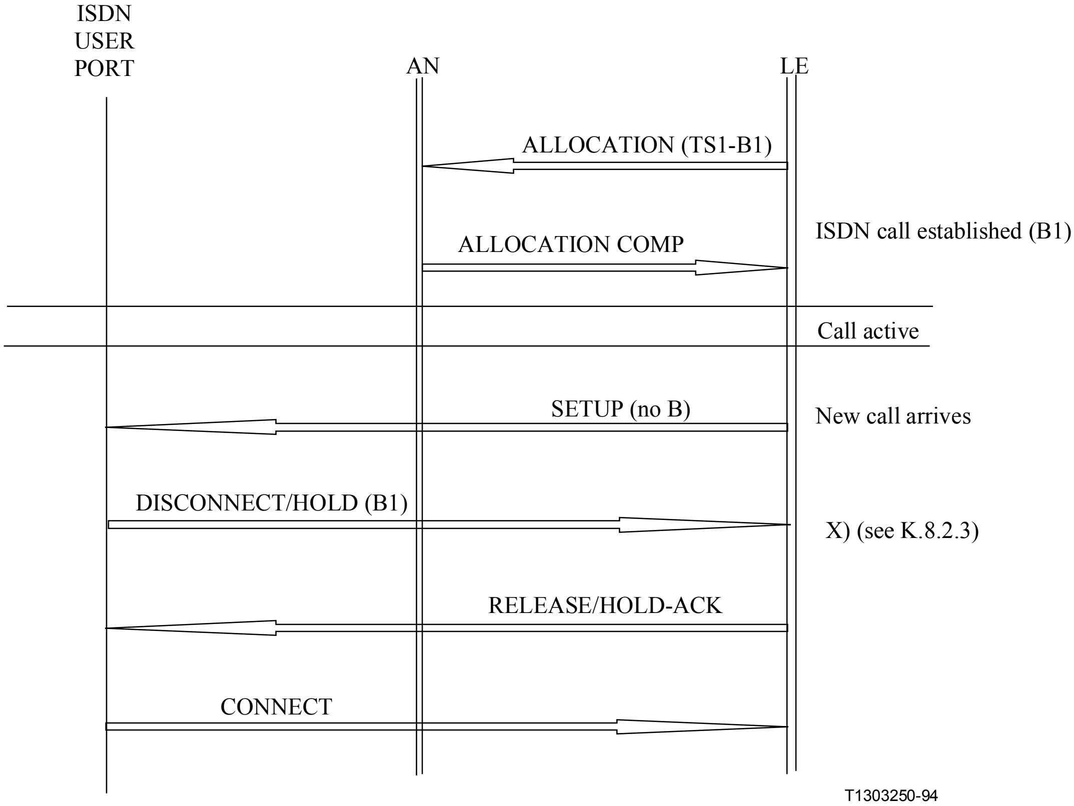


Figure K.6/G.965 – ISDN call initiated by the network, call waiting supplementary service support

K.8.3 ISDN call release initiated by the subscriber

The arrow diagram showing the interaction of the BCC protocol with DSS1 for the case: Call release initiated by the subscriber is given in Figure K.7.

In the case of ISDN call clearing and bearer channel de-allocation, the protocols synchronization is not needed, therefore the sending of the DSS1 response to the DISCONNECT message is decoupled from the sending of the DE-ALLOCATION message.

K.8.4 ISDN call release initiated by the network

The arrow diagram showing the interaction of the BCC protocol with DSS1 for the case: Call release initiated by the network is given in Figure K.8.

In the case of ISDN call clearing and bearer channel de-allocation, the protocol synchronization is not needed, therefore the sending of the DE-ALLOCATION message is decoupled from the receipt of the DSS1 RELEASE message.

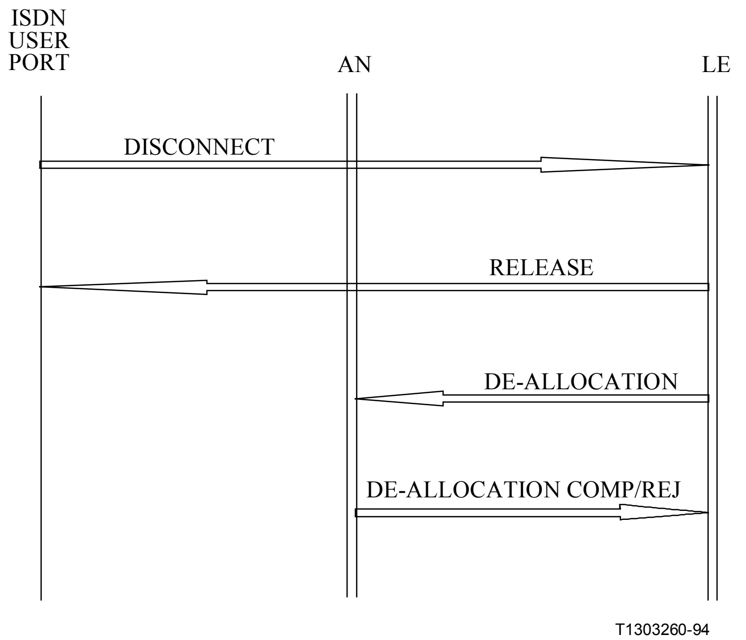


Figure K.7/G.965 – ISDN call release initiated by the subscriber

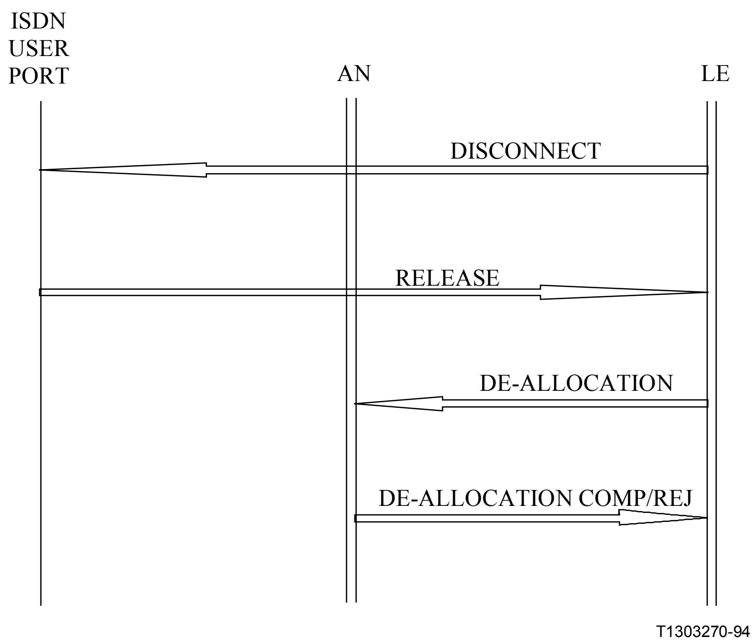


Figure K.8/G.965 – ISDN call release initiated by the network

K.8.5 Terminal portability supplementary service support

The arrow diagram showing how the DSS1 messages SUSPEND and RESUME should be supported is given in Figure K.9.

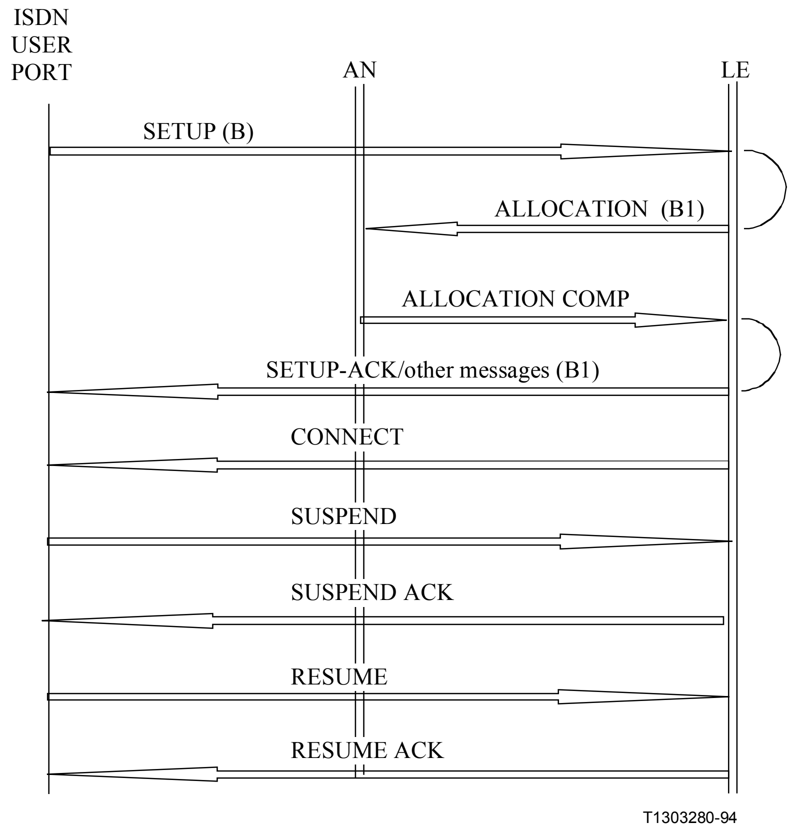


Figure K.9/G.965 – Terminal portability supplementary service

K.9 Arrow diagrams – Examples of BCC and PSTN protocol coordination

This clause demonstrates the expected coordination between the BCC and the national PSTN entities. It does not give a complete list of the possibilities and is informative only.

K.9.1 PSTN call initiated by the subscriber

K.9.1.1 Normal procedure

The arrow diagram showing an example for the interaction of the BCC protocol with the PSTN protocol for the case: Call initiated by the subscriber (normal procedure) is given in Figure K.10.

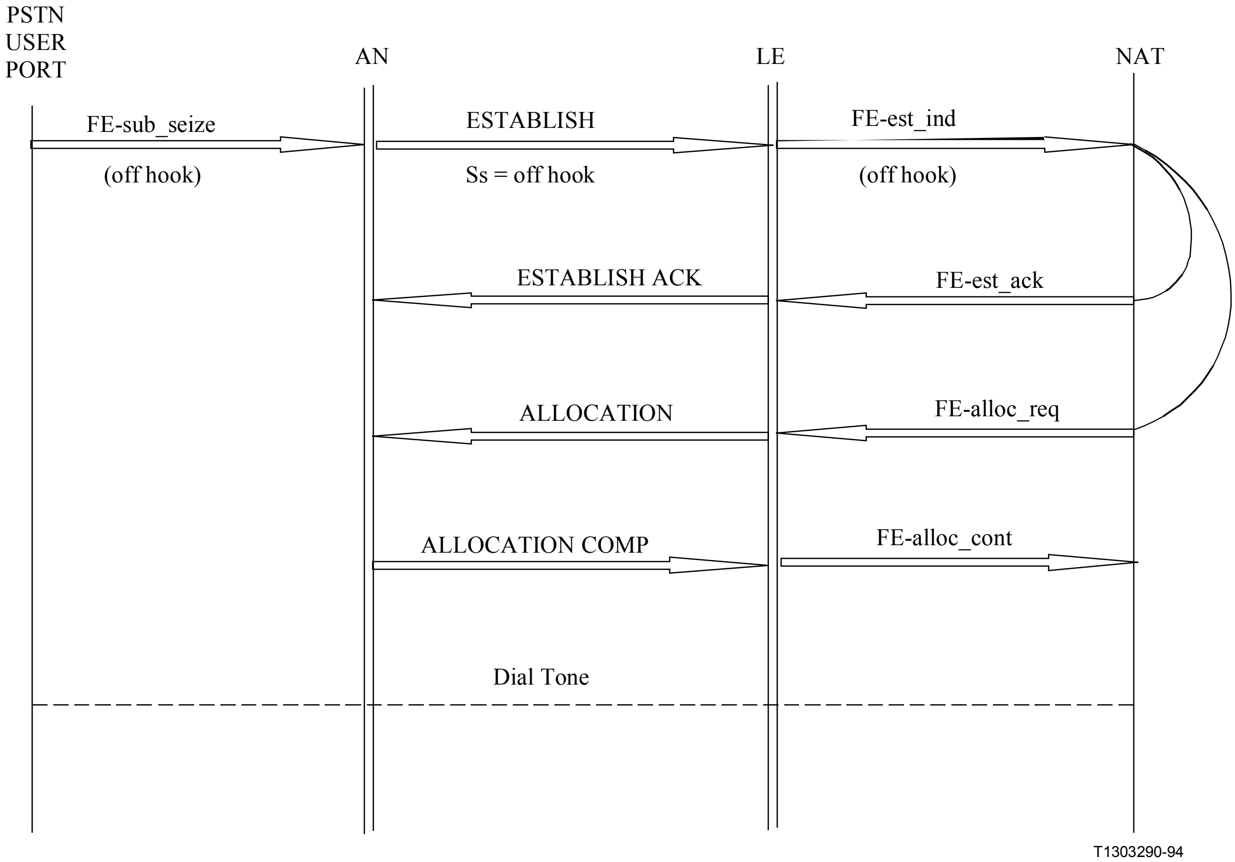


Figure K.10/G.965 – PSTN call initiated by the subscriber – Normal procedure

K.9.1.2 Exceptional procedure

The arrow diagram showing an example for the interaction of the BCC protocol with the PSTN protocol for the case: Call initiated by the subscriber (exceptional procedure) is given in Figure K.11. After a ALLOCATE REJECT message from the AN, there can be subsequent attempts to allocate a bearer channel (e.g. controlled by a timer in the national protocol).

K.9.2 PSTN call initiated by the network

The arrow diagram showing an example for the interaction of the BCC protocol with the PSTN protocol for the case: Call initiated by the network is given in Figure K.12.

K.9.3 Call collision

K.9.3.1 Call Collision – Originating call has priority

The arrow diagram showing an example for the interaction of the BCC protocol with the PSTN protocol for the case: Call collision (originating call has priority) is given in Figure K.13.

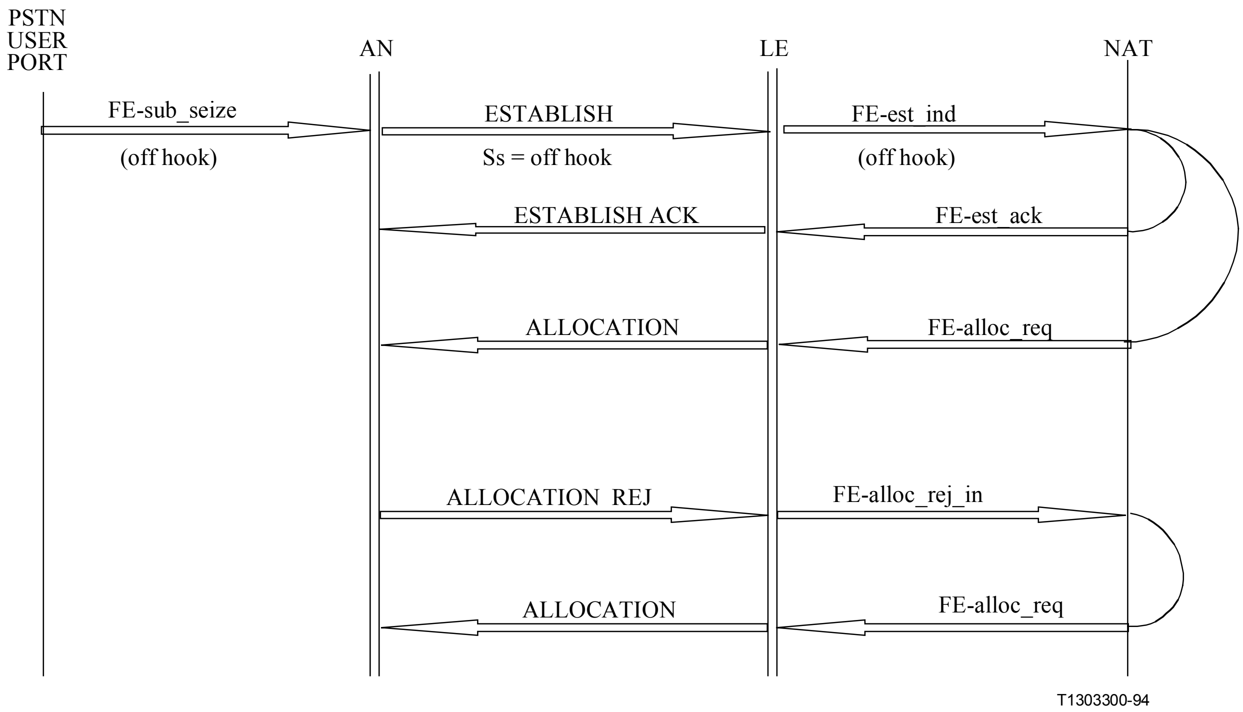


Figure K.11/G.965 – PSTN call initiated by the subscriber – Exceptional procedure

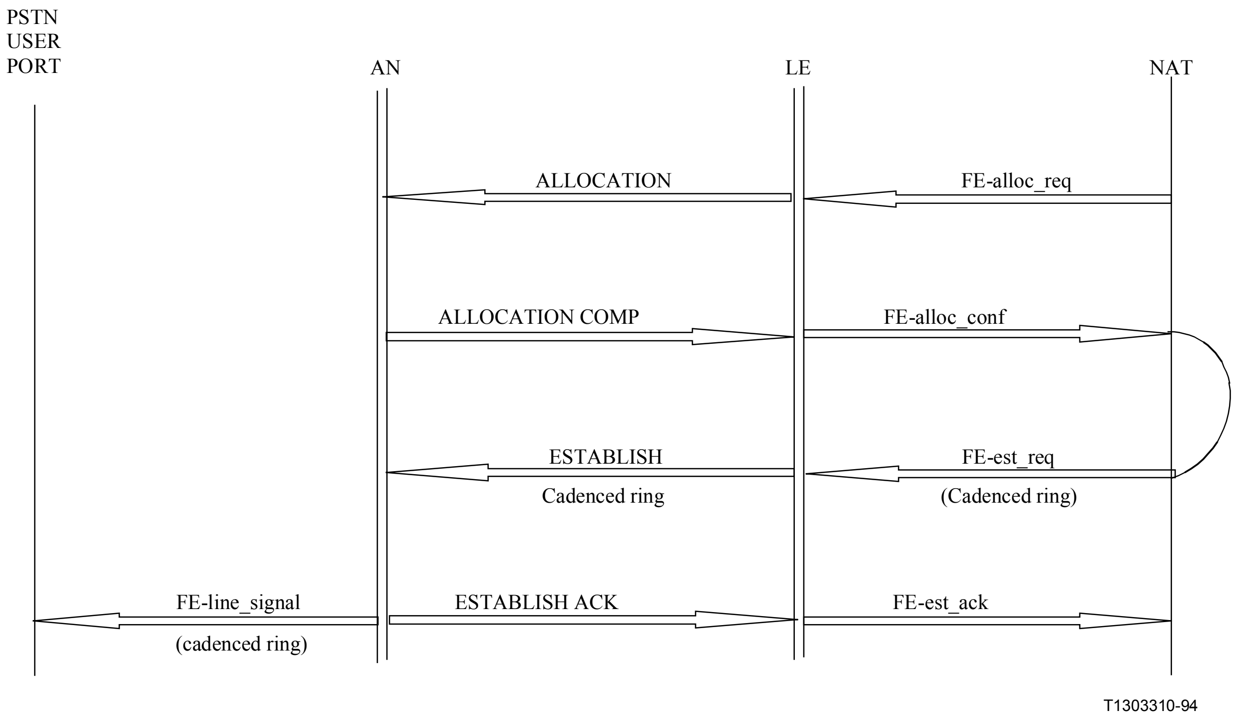


Figure K.12/G.965 – PSTN call initiated by the network

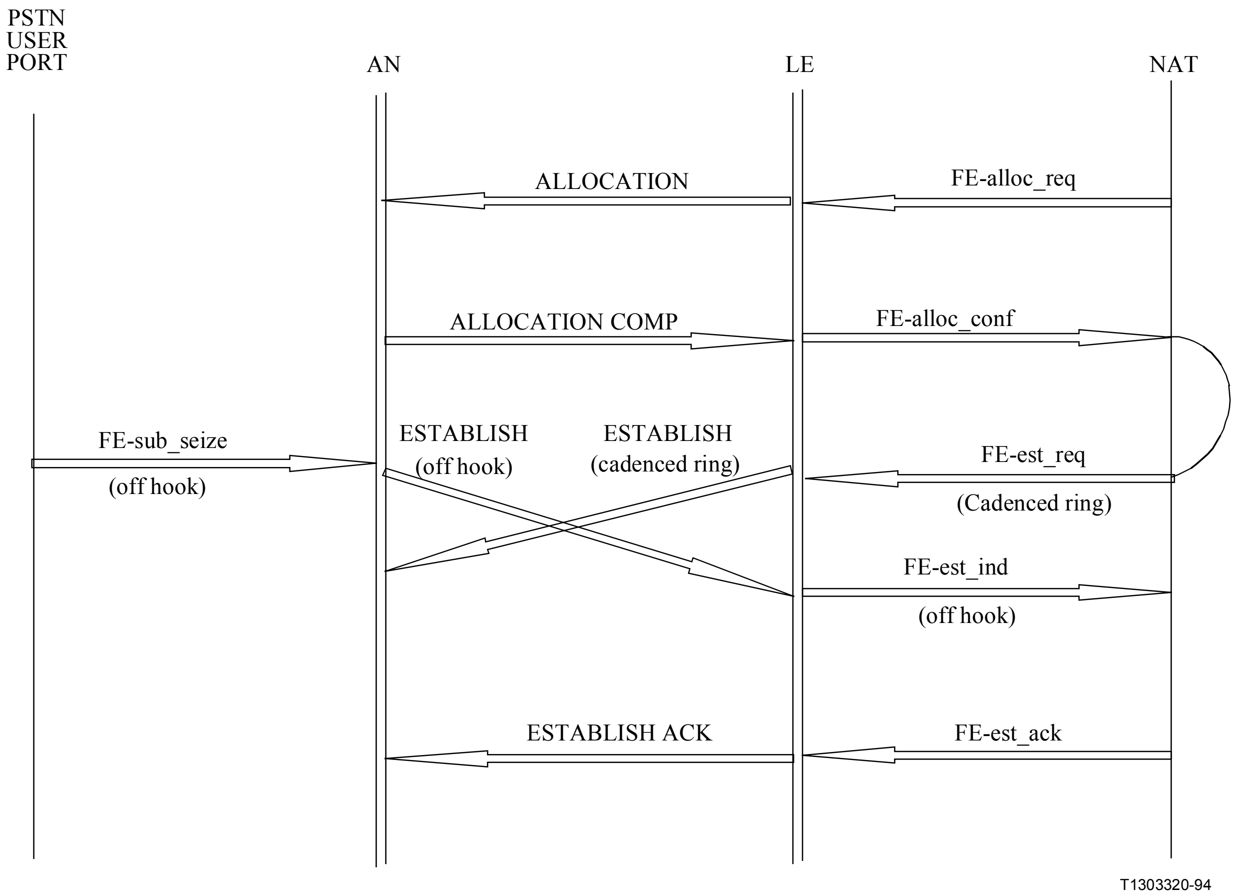


Figure K.13/G.965 – PSTN call collision – Originating call has priority

K.9.3.2 Terminating call has priority

The arrow diagram showing an example for the interaction of the BCC protocol with the PSTN protocol for the case: Call collision (terminating call has priority) is given in Figure K.14.

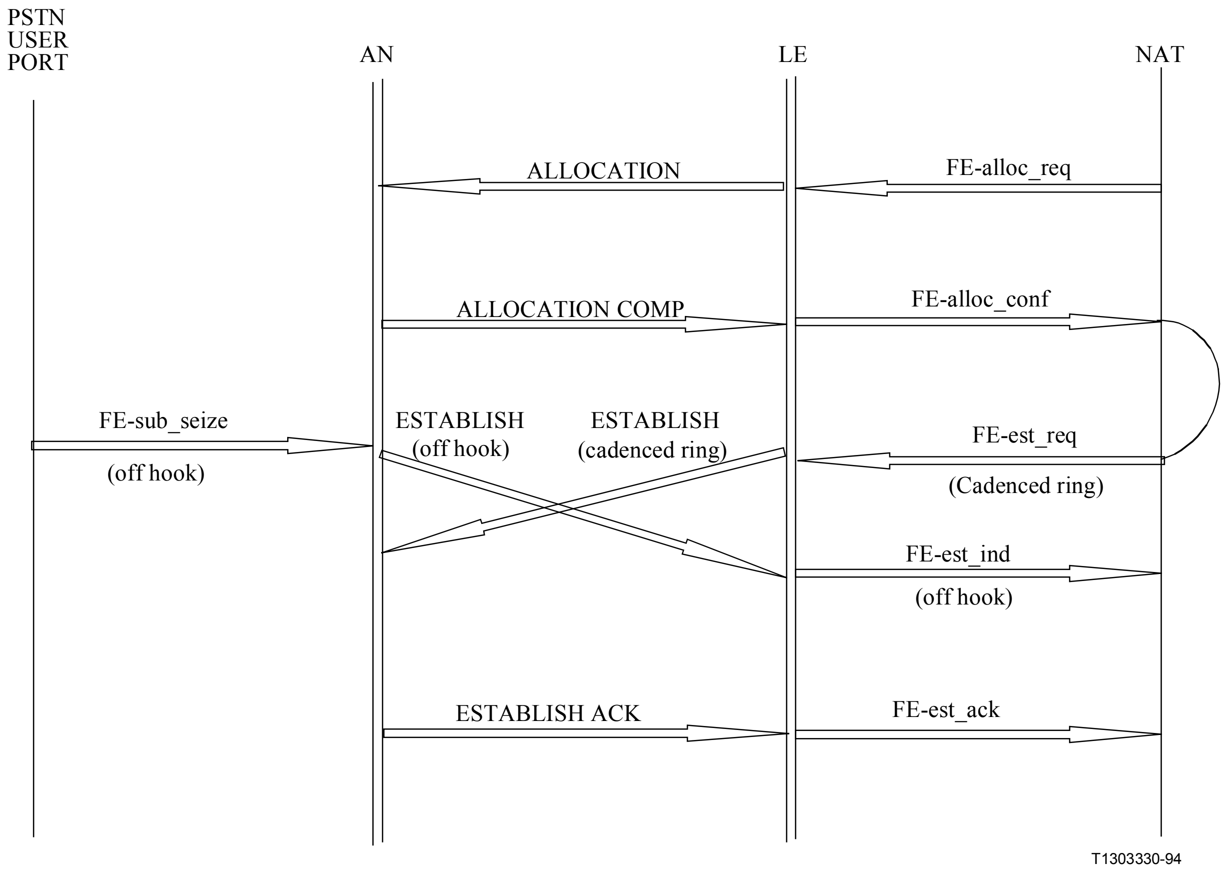


Figure K.14/G.965 – PSTN call collision – Terminating call has priority

K.9.4 Call release

K.9.4.1 Call release initiated by the subscriber

The arrow diagram showing an example for the interaction of the BCC protocol with the PSTN protocol for the case: Call release initiated by the subscriber is given in Figure K.15.

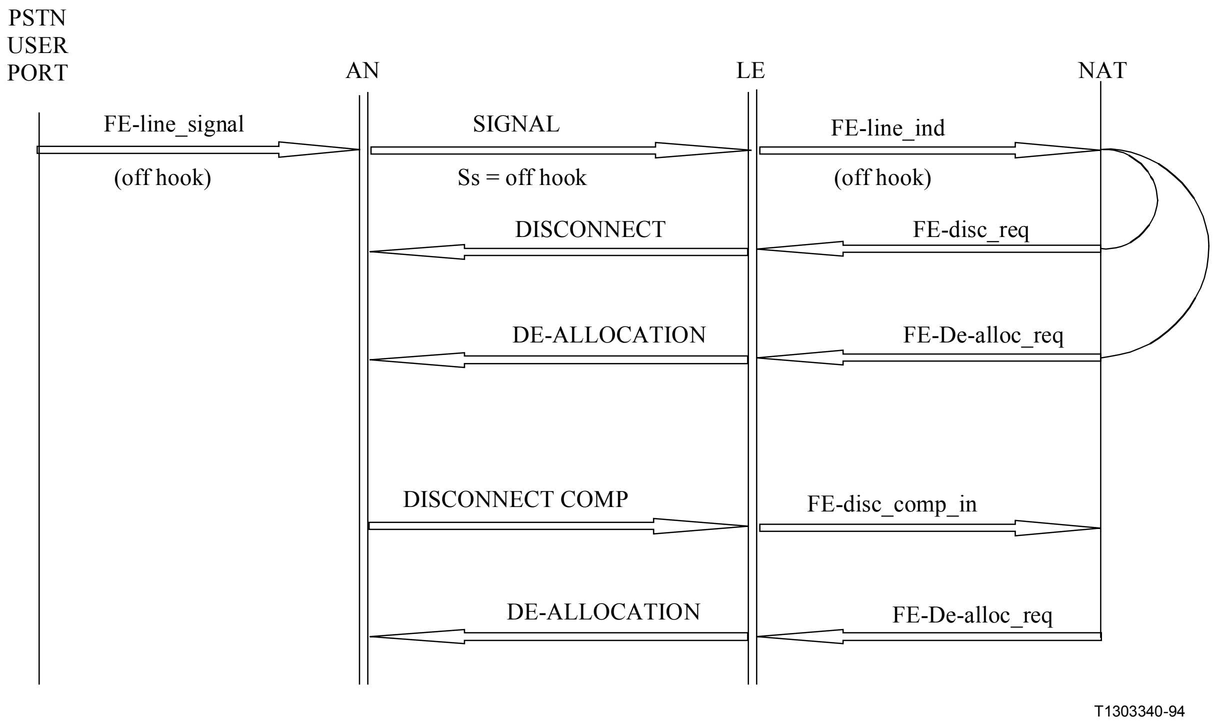


Figure K.15/G.965 – PSTN call release initiated by the subscriber

K.9.4.2 Call release initiated by the network

The arrow diagram showing an example for the interaction of the BCC protocol with the PSTN protocol for the case: Call release initiated by the network is given in Figure K.16.

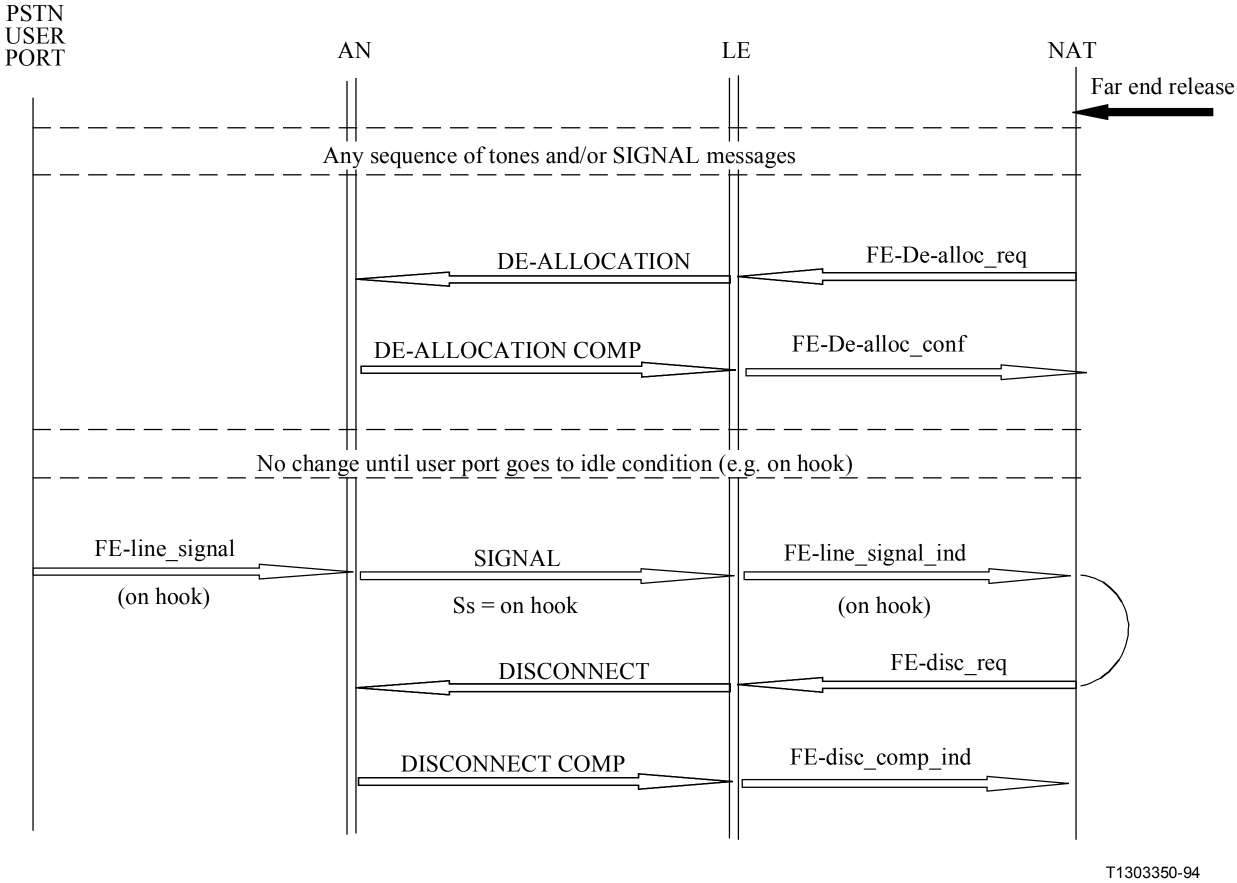


Figure K.16/G.965 – PSTN call release initiated by the network

K.10 Link failure rules

Persistent link failures, which will be recognized generally by both sides, shall not be notified by the AN as internal failure.

If the LE sends a link block command in a LINK CONTROL message for a link containing time slots allocated to ports (e.g. in case of a link failure recognized), all resources in the AN related to the connections affected are freed internally. The resource management entity in the LE shall initiate internal de-allocation for the notified bearer channel connection and shall notify the event to the PSTN/ISDN protocol entities for proper service actions to be taken.

ANNEX L

Examples for an implementation with high interoperability

This annex gives examples of typical problems that occur in the interaction of systems, which support international standards such as V5. Precautions are shown that may help to achieve a high degree of compatibility and interoperability. The approach chosen is on the basis of procedures, which are to be performed in cooperation. It is well known that not all systems support the full set of procedures defined. This may be caused by different versions of standards or simply by the choice of the manufacturers. How this may be handled in a way to guarantee the highest degree of compatibility possible is described as well.

L.1 Locally unsupported procedures

Most optional procedures offer the opportunity to be rejected by the side that receives the request. If a system does not support a specific requested procedure it should at least implement the appropriate reject message. This is to inform the remote side on the rejection properly and as soon as possible. That way, delays resulting from timer supervisions at the initiating side can be avoided.

L.2 Remotely unsupported procedures

a) *Rejection received*

The initiating side should always be ready to receive a reject message for a requested procedure. It should immediately take the appropriate actions to perform the task in an alternative way if possible. Rejections should never result in malfunctions of the receiving side i.e. unnecessary affection of services supported.

b) *Local timeout*

If the initiating side does not receive any response on the request, but there is a local timeout that ends the procedure, the same behaviour as for a rejection should be applied.

L.3 Cooperative design in general

a) *Passive support of procedures*

The support of procedures should not be limited unnecessarily. A system should support a procedure to the maximum extent possible. This applies even if, in case of symmetrical procedures, it is not yet ready to apply it as active part, i.e. as requesting side.

EXAMPLE 1: Link Id Check, Variant and Interface Id Check, etc.

This is especially useful when systems with implementations according to different versions of the V5 specifications have to cooperate, e.g. during interface startup.

Requests for procedures that cannot be rejected but are not yet ready to perform should be saved and responded to as soon as conditions change and the procedure may be applied.

EXAMPLE 2: PSTN restart procedure after PSTN DL failure, when the Establish message for the PSTN DL has not yet been received locally but the remote side already requests the procedure.

b) *Master only implementations of symmetrical procedures*

Master only implementations should be avoided. Any system that supports such a procedure (e.g. accelerated alignment procedures) should be ready to be the active and also the passive part.

APPENDIX I

Bibliography

– ITU-T G.921 (1988), *Digital sections based on the 2048 kbit/s hierarchy*.

– ITU-T G.961 (1993), *Digital transmission system on metallic local lines for ISDN basic rate access*.

– ITU-T M.3602 (1992), *Application of maintenance principles to ISDN subscriber installations*.

– ITU-T M.3603 (1992), *Application of maintenance principles to ISDN basic rate access*.

– ITU-T M.3604 (1992), *Application of maintenance principles to ISDN primary rate access*.

–	ITU-T O.162 (1992), *Equipment to perform in-service monitoring on 2048, 8448, 34 368 and 139 264 kbit/s signals*.
–	ITU-T Q.922 (1992), *ISDN data link layer specification for frame mode bearer services*.
–	ITU-T Q.933 (1995), *Digital Subscriber Signalling System No. 1 (DSS1) – Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2002