



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

I.313

(09/97)

SERIES I: INTEGRATED SERVICES DIGITAL
NETWORK

Overall network aspects and functions – Network
functional principles

B-ISDN network requirements

ITU-T Recommendation I.313

(Previously CCITT Recommendation)

ITU-T I-SERIES RECOMMENDATIONS
INTEGRATED SERVICES DIGITAL NETWORK

GENERAL STRUCTURE	I.100–I.199
Terminology	I.110–I.119
Description of ISDNs	I.120–I.129
General modelling methods	I.130–I.139
Telecommunication network and service attributes	I.140–I.149
General description of asynchronous transfer mode	I.150–I.199
SERVICE CAPABILITIES	I.200–I.299
Scope	I.200–I.209
General aspects of services in ISDN	I.210–I.219
Common aspects of services in the ISDN	I.220–I.229
Bearer services supported by an ISDN	I.230–I.239
Teleservices supported by an ISDN	I.240–I.249
Supplementary services in ISDN	I.250–I.299
OVERALL NETWORK ASPECTS AND FUNCTIONS	I.300–I.399
Network functional principles	I.310–I.319
Reference models	I.320–I.329
Numbering, addressing and routing	I.330–I.339
Connection types	I.340–I.349
Performance objectives	I.350–I.359
Protocol layer requirements	I.360–I.369
General network requirements and functions	I.370–I.399
ISDN USER-NETWORK INTERFACES	I.400–I.499
Application of I-series Recommendations to ISDN user-network interfaces	I.420–I.429
Layer 1 Recommendations	I.430–I.439
Layer 2 Recommendations	I.440–I.449
Layer 3 Recommendations	I.450–I.459
Multiplexing, rate adaption and support of existing interfaces	I.460–I.469
Aspects of ISDN affecting terminal requirements	I.470–I.499
INTERNETWORK INTERFACES	I.500–I.599
MAINTENANCE PRINCIPLES	I.600–I.699
B-ISDN EQUIPMENT ASPECTS	I.700–I.799
ATM equipment	I.730–I.749
Management of ATM equipment	I.750–I.799

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

ITU-T RECOMMENDATION I.313

B-ISDN NETWORK REQUIREMENTS

Summary

This Recommendation presents the B-ISDN network architecture needed to support broadband services and service features. The B-ISDN communication configurations and the B-ISDN addressing necessary to support the broadband services are also included in this Recommendation.

Source

ITU-T Recommendation I.313 was prepared by ITU-T Study Group 13 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 19th of September 1997.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The 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 Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 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

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The 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, the 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.

© ITU 1998

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

CONTENTS

	<i>Page</i>
1 Scope.....	1
2 Normative references	1
3 Terms and definitions.....	1
3.1 Definitions	1
3.2 Abbreviations	1
4 B-ISDN communication configurations.....	2
4.1 Point-to-point communication configuration.....	2
4.2 Unidirectional point-to-multipoint communication configuration.....	2
4.3 Multipoint-to-point communication configuration	4
4.4 Multipoint-to-multipoint communication configurations.....	5
4.5 Bidirectional point-to-multipoint communication configuration	6
5 Network control requirements.....	6
6 B-ISDN numbering and addressing.....	7
6.1 Public B-ISDN networks	7
6.2 Private networks	8
6.3 Interworking requirements between the public and private B-ISDN	9
7 B-ISDN management functions.....	10
7.1 Configuration management.....	10
7.2 Fault management.....	11
7.3 Performance management.....	12
7.4 Accounting management.....	12
7.5 Security management.....	12
Annex A – B-ISDN service requirements template.....	13
A.1 B-ISDN service	13
A.2 Service description	13
A.3 Communication configuration(s).....	14
A.4 Connection type(s).....	14
A.5 B-ISDN network capability requirements.....	14
A.6 Specific B-ISDN signalling requirements.....	14
A.7 Interworking	14
Appendix I – Examples of communication configurations.....	14
I.1 Example of multipoint-to-point communication configurations.....	14
I.2 Example of multipoint-to-multipoint communication configurations.....	16
I.3 Example of bidirectional point-to-multipoint communication configuration.....	18
Appendix II – B-ISDN service requirements template for database backup/alignment	20
II.1 B-ISDN service name	20
II.2 Service description	20
II.3 Communication configurations.....	22
II.4 Connection type(s).....	22
II.5 B-ISDN network capability requirements.....	22
II.6 Specific B-ISDN signalling requirements.....	23
II.7 Interworking	24

	<i>Page</i>
Appendix III – B-ISDN service requirements template for video on demand.....	24
III.1 B-ISDN service name.....	24
III.2 Service description	24
III.3 Communication configuration(s).....	24
III.4 Connection type(s).....	24
III.5 B-ISDN network capability requirements.....	25
III.6 Specific B-ISDN signalling requirements.....	26
III.7 Interworking	27
Appendix IV – B-ISDN service requirements template for CDH services.....	27
IV.1 B-ISDN service name.....	27
IV.2 Service description	27
IV.3 Communication configuration(s).....	28
IV.4 Connection type(s).....	28
IV.5 B-ISDN network capabilities.....	28
IV.6 Specific B-ISDN signalling requirements.....	30
IV.7 Interworking	30
Appendix V – Use of NSAP address formats for private ATM network addressing.....	30
V.1 NSAP structures	30
V.2 ATM address formats	31
V.3 ATM address structures.....	32

B-ISDN NETWORK REQUIREMENTS

(Geneva, 1997)

1 Scope

This Recommendation specifies the Broadband ISDN Network requirements in support of B-ISDN services and service features. This Recommendation provides an overview of B-ISDN architecture, including communication configurations, network control requirements, numbering and addressing issues for both public and private networks.

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 the currently valid ITU-T Recommendations is regularly published.

- ITU-T Recommendation E.164 (1997), *The international public telecommunication numbering plan*.
- ITU-T Recommendation E.191 (1996), *B-ISDN numbering and addressing*.
- ITU-T Recommendation I.311 (1996), *B-ISDN general network aspects*.
- ITU-T Recommendation I.610 (1995), *B-ISDN operation and maintenance principles and functions*.
- ITU-T Recommendation X.213 (1995), *Information technology – Open Systems Interconnection – Network service definition*.

3 Terms and definitions

This Recommendation defines the following terms.

3.1 Definitions

- 3.1.1 look ahead:** Describes a procedure used to determine connection and termination compatibility prior to any call/connection establishment.
- 3.1.2 leaf:** Part of the connection between a branching point and the party which is added to a point-to-multipoint call.
- 3.1.3 root:** Initiator of the call.
- 3.1.4 data volume:** The traffic generated by a party.
- 3.1.5 service feature:** Is a reusable part of one or more service capabilities forming all or part of a service.

3.2 Abbreviations

This Recommendation uses the following abbreviations.

AAL	ATM Adaptation Layer
AESA	ATM End System Address
B-ISDN	Broadband Integrated Services Digital Network
CDH	Cooperative Document Handling

CDV	Cell Delay Variation
CLR	Cell Loss Ratio
CTD	Cell Transfer Delay
CPCS	Common Part Convergence Sublayer
DCC	Data Country Code
DNI	Destination Network Identifier
DSP	Domain Specific Part
ICD	International Code Designator
IDI	Initial Domain Identifier
IN	Intelligent Network
MID	Message Identifier
MMD	Multimedia Document
NSAP	Network Service Access Point
PDU	Protocol Data Unit
PM	Performance Management
QOS	Quality of Service
SDH	Synchronous Digital Hierarchy
TMN	Telecommunications Management Network
UNI	User Network Interface
UPC	Usage Parameter Control
VC	Virtual Channel
VCI	Virtual Channel Identifier
VP	Virtual Path
VPI	Virtual Path Identifier

4 B-ISDN communication configurations

Communication configuration specifies who talks to whom (users' point of view) and does not say how the U-plane information is supported in terms of connections. Given communication configurations may be supported by means of more than one possible connection configuration. This is illustrated in Appendix I.

4.1 Point-to-point communication configuration

4.1.1 Type 1 – Point-to-point connection

A point-to-point connection may provide unidirectional or bidirectional symmetric and asymmetric communications between parties "A" and "B". See Figure 1.

This connection can be established, modified, or released by Party "A", "B" requests. Third party (C or D) may also request the action.

4.2 Unidirectional point-to-multipoint communication configuration

4.2.1 Type 2 – Point-to-multipoint (Multicast) connection

A Type 2 connection provides unidirectional communications from the "root" party "A" to "leaf" parties "B" and "C". See Figure 2.

This connection may be established, modified, or released in one of the following ways:

- the root party "A" may request the action; or
- either leaf ("B" or "C") may request the action and individually define the full configurations;

- each leaf ("B" or "C") may individually request to be added to (or deleted from) the configuration independent of the other leaves (e.g. in case of public multicast);
- an external entity ("D") may request the action.

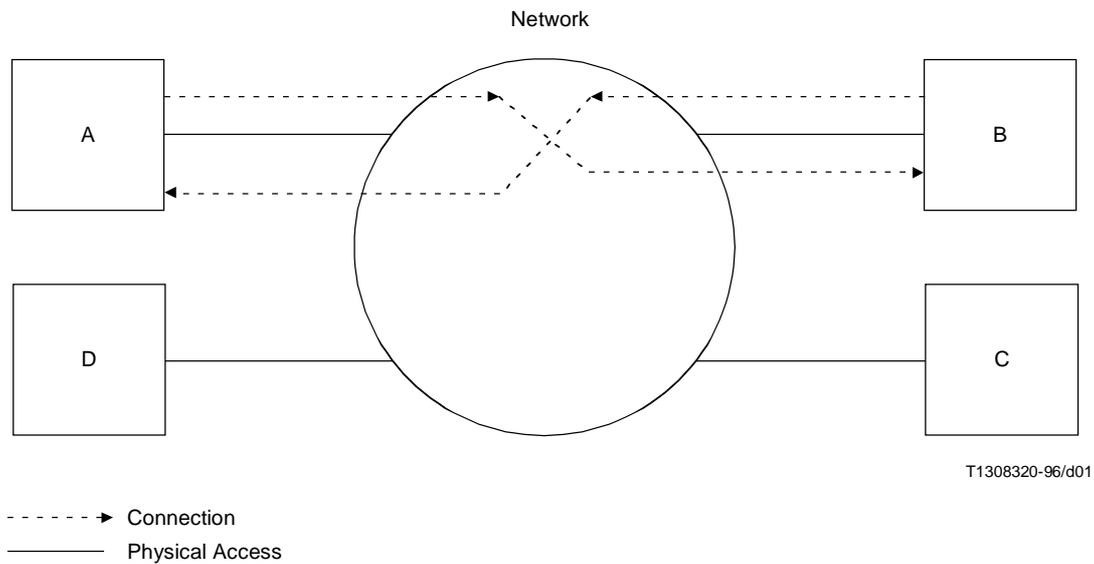


Figure 1/I.313 – Bidirectional point-to-point connection

The initiator of the call may be able to specify which called parties must be mandatory and which are optional before the execution of the call.

NOTE – Type 2 connections may be used to support multicast and/or broadcast services.

A multicast connection is a unidirectional multipoint connection from a single endpoint to a specified number of specified distribution endpoints. In a multicast connection, the "leaf" parties are specified before the connection is established, or by subsequent operations. The "root" party at the connection will always be aware of all the "leaf" parties of the connection.

A broadcast connection is a unidirectional multipoint connection from a root (source) to a number of leaves (sink) which are not always known to the root.

In order to establish a point-to-multipoint connection, a Replication Function "R" in the network is required (see 4.2.1.1).

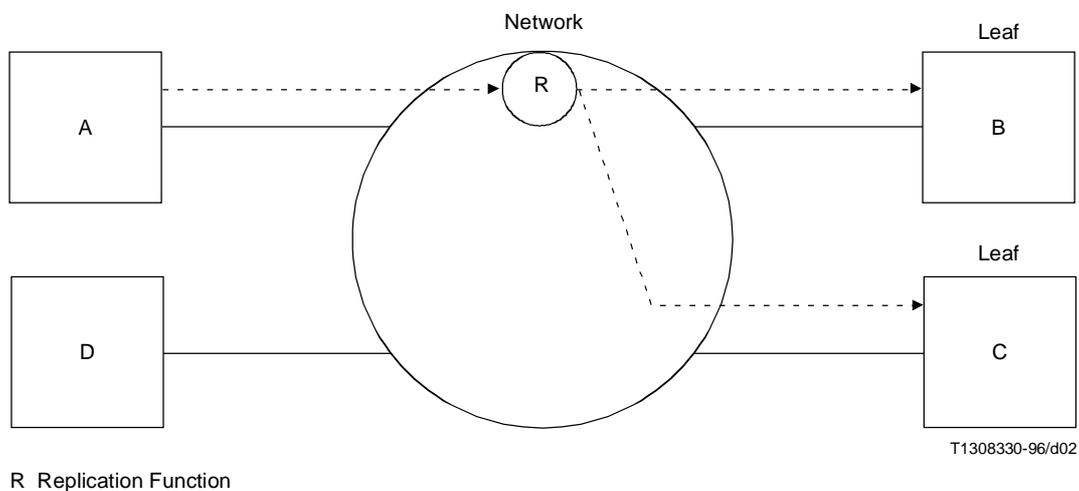


Figure 2/I.313 – Unidirectional point-to-multipoint

4.2.1.1 Replication Function

A Replication Function point in the ATM network is a point in a Type 2 connection where U-plane data received from one incoming data flow is replicated on two or more outgoing data flows. A replication is possible in the ATM layer, within the AAL or in higher layers.

The initial signalling requirements support ATM layer replication point. In this case replication may occur in any node (ATM switch) of the network in order to provide multiple routes.

The ATM layer Replication Function is based on the VPI: VCI fields in the ATM cell header. At the replication point each cell arriving is copied onto two or more outgoing ATM cell streams and within each cell stream onto one or more ATM virtual paths or virtual channels.

NOTE – ATM cell payload content is not altered by the copying process.

4.3 Multipoint-to-point communication configuration

4.3.1 Type 3 – Multipoint-to-point connection

A multipoint-to-point connection provides unidirectional communications from the "leaf" parties "B" and "C" to the "root" party "A". The bandwidth transmitted by the leaf parties may be different. In some cases, multipoint-to-point may be provided using Type 1 connections (see Figure I.1-2). In certain cases when processing is performed in the merging point, the bandwidth received by the "root" party may be different from the sum of the transmitter's bandwidth.

This connection may be established, modified, and released in one of the following ways:

- the root "A" may request the action;
- either leaf ("B" or "C") may request the action and individually define the full configuration;
- each leaf ("B" or "C") may individually request to be added to (or deleted from) the configuration independent of other leaves;
- an external entity ("D") may request the action.

The initiator of the call may be able to specify which called parties must be mandatory and which are optional before the execution of the call.

Note that "M" denotes a Merging Function as shown in Figure 3 and described in 4.3.2.

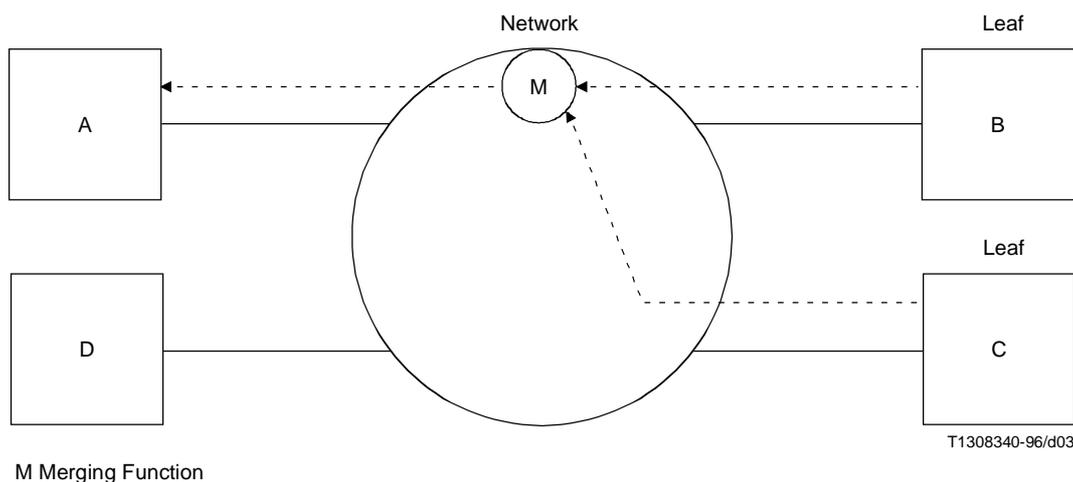


Figure 3/I.313 – Unidirectional multipoint-to-point

4.3.2 Merging Function

A Merging Function point in the ATM network is a point in a connection where user plane data received from two or more incoming data flows are combined in a single data flow. Merging functions may exist in one or more network nodes. Merging is possible in the ATM layer, within the AAL or in higher layers.

In an ATM layer, merging point cells from two different incoming cell streams are interleaved onto a single ATM virtual channel of a single outgoing cell stream. Cell information field contents are not altered by this interleaving process. This function does not work where the user information packets are more than a single cell, unless some form of multiplexing field is present in the SAR sublayer of the AAL (i.e. in each cell). Where user information can be carried within a single cell, some form of identification of the point of origin is needed.

If the AAL Type 3/4 is used in a Merging Function, it will be used for all incoming VCs and outgoing VC belonging to the same multipoint-to-point ATM connection. In this case, the following functionality will apply:

- a one-to-one mapping between incoming and outgoing CPCS-PDUs;
- the sum of the number of MID values concurrently used on all incoming VCs shall be allowed on the outgoing VC;
- mutually exclusive sets of MID values are used on all incoming VCs.

This makes the mapping function simple, whereby cells can be handled "on-the-fly" without any AAL processing.

Merging may also involve processing of the user information as performed in a voice bridge.

Merging could take place in higher layers when a special server function is used (see Figure I.1-3). Merging can also be performed in the sink, which means that the network could establish a multipoint-to-point communication configuration by using Type 1 connections. (See Appendix I.)

4.4 Multipoint-to-multipoint communication configurations

4.4.1 Type 4 – Multipoint-to-multipoint connection

The multipoint-to-multipoint connection provides the capability that all parties can communicate with each other (see Figure 4). In some cases, a multipoint-to-multipoint may be provided using Type 2 connections (see Figure I.2-2). In certain cases when processing is performed in the merging point, the receiver bandwidth of each party may be different from the sum of the bandwidths transmitted and may be different for each party. The bandwidth transmitted by each party may be different from each other and different from the bandwidth received.

The connection may be established, modified or released in one of three ways:

- any party associated with the connection may request the action and individually define the full configuration;
- any external party "D" may request the action;
- any party may request to be added to the configuration.

The initiator of the call may be able to specify which called parties must be mandatory and which are optional before the execution of the call.

A server function may also be used as described in I.2.3, and shown in Figure I.2-3.

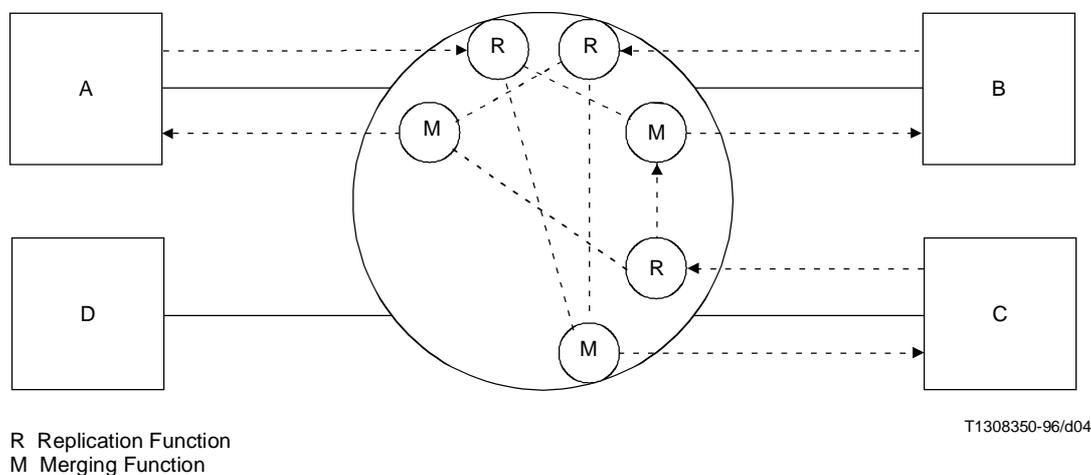


Figure 4/I.313 – Multipoint-to-multipoint connection

4.5 Bidirectional point-to-multipoint communication configuration

4.5.1 Type 5 – Bidirectional point-to-multipoint connection

This type of connection provides communication between root party A and leaf parties B and C as shown in Figure 5. This type of connection allows the root party to generate data to the leaf parties using a Replication Function in the network, while the leaf parties send data only to the root party.

This type of connection is formed when a Type 2 connection is superimposed on a Type 3 connection, such that the source of the Type 2 connection is the same as the sink for the Type 3, and the sinks for the Type 2 are the source for the Type 3.

This type of connection may also be formed using a combination of connection Types 1 and 2 (see Figure I.3-2).

The connections may be established, modified and released in one of the following ways:

- the root "A" may request the action;
- either leaf ("B" or "C") may request the action and individually define the full configuration;
- each leaf ("B" or "C") may individually request to be added (or deleted) to (from) the configuration independent of other leaves;
- an external entity ("D") may request the action.

The initiator of the call may be able to specify which called parties must be mandatory and which are optional before the execution of the call.

A server function may also be used as described in I.3.3, and shown in Figure I.3-3.

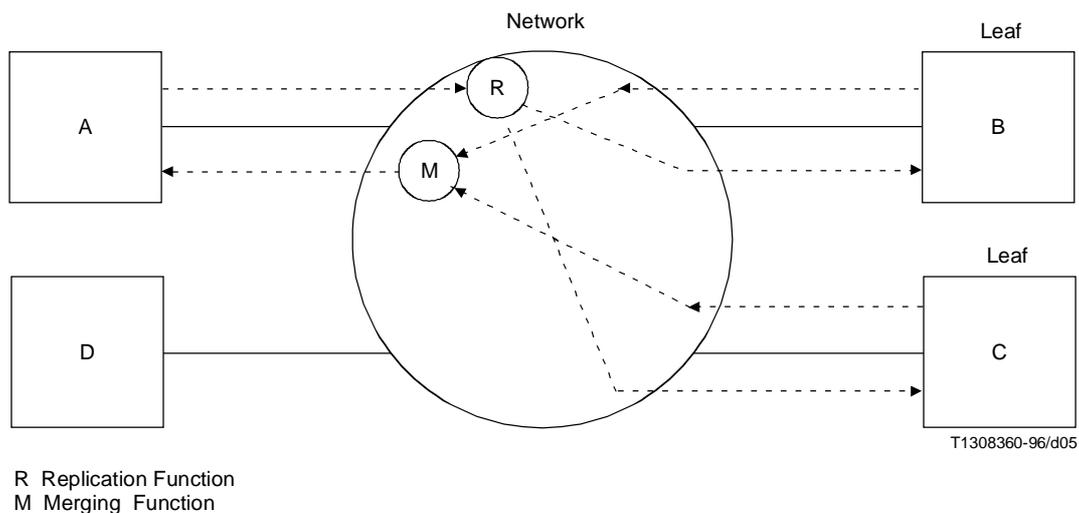


Figure 5/I.313 – Bidirectional point-to-multipoint connection

5 Network control requirements

When defining and verifying network capabilities and signalling requirements for B-ISDN services or service feature applications, a B-ISDN service requirements template is used as shown in Annex A. Examples of how the service template is used are shown in Appendices II and III.

The following list of B-ISDN network control requirements are necessary to support future B-ISDN communication configurations and service features:

- establishment of switched B-ISDN connections;
- support of connections configurations on a point-to-point and point-to-multipoint basis;
- support of point-to-multipoint connections;

- support of look-ahead mechanisms;
- support of point-to-point multi-connections;
- support of point-to-multipoint mono-connections;
- support of multipoint multi-connections;
- support of symmetric and asymmetric connections (e.g. low or zero bandwidth in one direction and high bandwidths in the other);
- to be able to establish a call without connections;
- to be able to add connections to an existing call;
- support specification of quality of service (QOS) classes;
- support negotiation of ATM traffic descriptors during call establishment;
- support of bandwidth renegotiation during active phase for point-to-point connections;
- grouping of bearer connections keeping timing relation;
- support of signalling procedures for interworking with 64 kbit/s based ISDN for circuit mode, packet mode, and frame mode bearer service;
- support of multipoint-to-multipoint connections and multipoint-to-point connections;
- QOS attribute value negotiation during call set-up;
- support of call offering to multiple terminals on a single UNI access;
- support of user-to-user information during call set-up;
- support of end-to-end transit delay information element;
- interworking with IN;
- interworking with TMN;
- support of B-ISDN teleservices, including multimedia, and distributive services;
- support of mobility services.

6 B-ISDN numbering and addressing

6.1 Public B-ISDN networks

6.1.1 B-ISDN numbering requirements

The requirements for B-ISDN numbering are:

- a) support of switched, permanent, semi-permanent, point-to-point and point-to-multipoint connections;
- b) support of both single and group addressing;
- c) does not identify the type of service requested;
- d) uniquely identifies the originating and destination endpoints;
- e) B-ISDN number assignments for users may be made at the S_B and T_B reference points;
- f) a B-ISDN destination network identifier code to be included in the number for countries having multiple B-ISDN networks;
- g) to a particular interface or multiple interfaces at the UNI, there may be assigned more than one B-ISDN number at the T_B reference point.

6.1.2 B-ISDN numbering

The public B-ISDN network shall be numbered according to the E.164 numbering plan. Additional numbering and addressing requirements not covered in Recommendation E.164 are described in Recommendation E.191.

6.1.3 B-ISDN addressing

The B-ISDN address is based upon the format and structure defined in Recommendation E.164 with additional extensions (possibly carried in appropriate protocol fields) as deemed necessary to support the deployment of the broadband services.

Where required (for example, to identify within a subscriber installation a point beyond the public network boundary), additional address information (a subaddress) shall be transported transparently across the ATM network. The subaddress field may be used, for example, to address terminals on private ATM networks.

Two options are available for specifying a B-ISDN address. The B-ISDN address structures are shown in Figure 6.

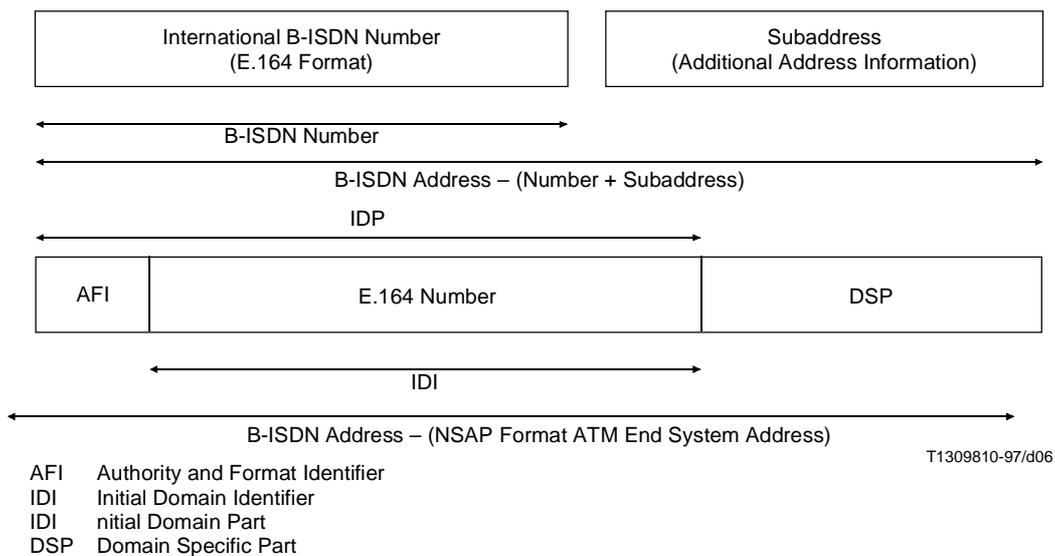


Figure 6/I.313 – B-ISDN address structures

The first structure is based on the use of a subaddress to provide additional addressing information to that provided by the E.164 number in order to identify the entity involved in the specific B-ISDN communication. The subaddress may be a simple string of digits or it may be a structured address; for example an NSAP address as defined in Annex A of ITU-T Rec. X.213 | ISO/IEC 8348.

The second structure is based on the structure of the E.164 format of an NSAP address as defined in Annex A of ITU-T Rec. X.213 | ISO/IEC 8348. The E.164 number contained in the IDI identifies the user-to-network interface associated to the entity identified by the B-ISDN address. This structure is known as an ATM End System Address (AESAs). Details on the coding and use of NSAP address formats are given in Appendix V.

6.2 Private networks

This subclause provides guidance on numbering and addressing used in private networks in order that terminals on such private networks can be numbered in harmony with the public network numbering plan and can interwork with terminals on the public network.

The point of attachment of a private network to a public network (the public UNI) is identified by one or more E.164 numbers. An ATM private network address (assigned at the private UNI) is one which uniquely identifies an ATM endpoint or terminal on the private network. A reference model specifying the public UNI and the private UNI is shown in Figure 7.

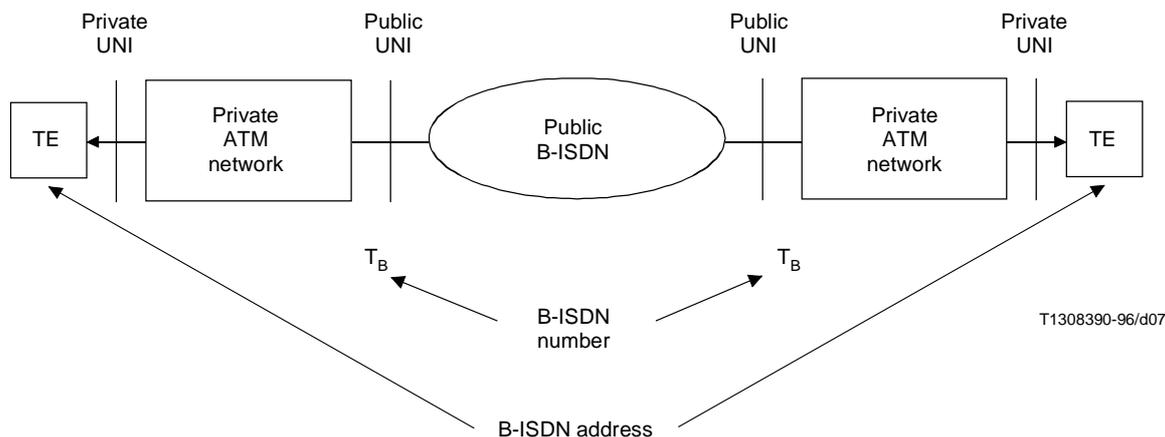


Figure 7/I.313 – Reference model for private and public UNI

NOTE – The TE may be connected directly to the public network at S_B/T_B reference points.

The numbering/addressing mechanism used within a private network will be implementation-dependent. However, private networks wishing to interwork with the public networks will require a numbering scheme that:

- a) identifies the private network point of attachment;
- b) enables an individual ATM endpoint (terminal) to be addressed.

The private network address structure should be such that:

- a) an endpoint has the ability to originate a call to any other endpoint on the private network independent of the type of addressing scheme used;
- b) all private networks will be able to accept call set-up messages containing ATM addresses and progress the call towards its final destination;
- c) the endpoint address should be globally unique.

The above requirements may be met by in-dialling capabilities. However, to meet the above requirements and simultaneously identify a large number of terminals on the private network, it will be generally necessary to utilize a subaddressing mechanism. The subaddresses in conjunction with the E.164 number specifying the point of attachment will define a globally unique address. A recommended method is the use of the OSI Network Service Access Point (NSAP) address structure (format) defined in Annex A of ITU-T Rec. X.213 | ISO/IEC 8348. All three ATM address structures of the NSAP formats, i.e. DCC, ICD, and E.164, may be used at the private UNI. The NSAP address structure ensures a globally unique address which can be used to identify a terminal or a process. Guidance on the use of the NSAP format addresses for private ATM network addressing is given in Appendix V. Other types of ATM private address structures are for further study.

6.3 Interworking requirements between the public and private B-ISDN

In order to route calls to terminals on private networks, it is necessary to identify both the point of attachment of the private network and the terminal address in the call set-up message.

If a terminal on a private network is identified only by its private network address (which may have an NSAP address format), it is necessary that in order to route the call across the public B-ISDN the private ATM address must be mapped to the E.164 number specifying the point of attachment of the private network. The called party E.164 address can be directly determined from the NSAP format address only in the case when the E.164 IDI format of the NSAP is used. The determination of the E.164 called party number resulting from analysis of the NSAP format address requires additional functionality in the network. Only the E.164 number will be used for routing a call within the public B-ISDN to the point of attachment.

Any subaddress must be transparently transferred across the public B-ISDN. Such subaddresses may uniquely identify a private ATM endpoint.

7 B-ISDN management functions

This clause presents the B-ISDN management requirements for the B-ISDN network. Five management functional areas are identified and described.

7.1 Configuration management

Configuration management identifies, exercises control over, collects data from, and provides data to open systems for the purpose of preparing for initializing, starting, providing for the continuous operation of, and terminating interconnection services. Configuration management includes functions to:

- a) set the parameters that control the routine operation for the open system;
- b) associate names with managed objects and sets of managed objects;
- c) initialize and close down managed objects;
- d) collect information on demand about the current condition of the open system;
- e) obtain announcements of significant changes in the condition of the open system; and
- f) change the configuration of the open system.

Configuration management functions also relate to the management of information required to provision connections in the ATM Network Element (NE) and between NEs to support any specific services provided by a network operator. The configuration management function enables the Operation Support Function (OSF) to interconnect/provision and manage the connections appearing at any interface of the NE and provide information to update the state of any interface.

The following are requirements which should be included in configuration management.

7.1.1 Maintain location/information

The ability of the network to maintain site information required to keep accurate records of site (node) data relative to country, city, address, building, floor location. Logical descriptions of site (node) type, category, function, etc., are also required to maintain location information. Other information, such as owner/provider and/or responsible parties for maintaining the operation of the site (node) may also be required.

7.1.2 Equipment

For further study.

7.1.3 Maintain facility

The facility is defined as the physical component which connects network elements together. In this case, the optical or the electrical media could serve as the physical components.

7.1.4 Provide network element and facility view

The configuration and connectivity of network elements via facilities comprise the physical and logical network topology required to support the management of a telecommunications network.

7.1.5 Maintain bandwidth hierarchical structure (synchronous/asynchronous)

An SDH and asynchronous compliant bandwidth definition for transmission paths must be independent of terminating vendor or equipment.

One major capability of this new technology is the mid-span meet between equipment from different vendors. The SDH-defined rates and levels allow communications across a path using terminating equipment from two different vendors. Manufacturers do not have to use the same multiplexing procedure, a comparable physical equipment arrangement, a common bay/shelf/slot/port identification method, or an equivalent card port to bandwidth location mapping scheme. The data representation of the transmission path bandwidth should be based on the SDH defined rates/levels rather than the specific equipment configuration of the vendor.

Several management views of the bandwidth must be presented to support installation and maintenance of bandwidth. The network element level viewpoint includes the relationship between the bandwidth and the connection and termination points.

7.1.6 Maintain signal mapping formats

SDH technology will allow for transport of any bit rate that the customer requires. This bit rate will range from fractional 64 kbit/s to the maximum available rate, including rates that are considered non-standard.

7.2 Fault management

The initial standard should cover the following functions:

Fault management functions enable the detection, reporting and localization of anomalies, defects and failures that may occur in any connection. The occurrence of a defect may trigger alarm indications either in-band or out-of-band (alarm surveillance). Localization of faults may be based upon in-band procedures (e.g. loopbacks) or out-of-band test procedures:

- alarm surveillance;
- testing.

7.2.1 Fault

7.2.1.1 Fault presentation

The fault presentation capabilities must provide the operator with fault information collected from the B-ISDN network as well as automated interfaces to related fault management activities. The operator must have real-time access to all active and historical alarm events in the network or subsets based on priority, geographical regions, subnetworks, etc.

7.2.1.2 Control capabilities

Fault management activities include requests for network configuration or state changes. An integrated capability to use configuration services to accomplish these tasks through automated interfaces and ergonomic selection of available control options is required.

7.2.1.3 Fault localization – Perform root cause analysis

Fault management must support the ability to determine the probable cause of network conditions. If necessary, diagnostics and test routines may be requested to assist in fault localization.

7.2.1.4 Alarm surveillance

This is an element management layer function that notifies the network management layer of alarm objects and their relationships to equipment or functions (configuration). This function also notifies the NML of all applicable alarm object status changes. This element management layer function eliminates unnecessary or duplicate alarms received from the network elements.

7.2.1.5 Network element states

In addition to the managed object states in-service and disabled, fault management needs additional state definitions that will affect the way operators and their applications utilize fault information. Prior to network elements being in-service, a network state of "under construction" needs to be supported during the period of time when a managed object is installed and being tested/verified but prior to traffic being placed on the systems. Personnel conducting acceptance testing of these managed objects need to be notified of abnormal conditions. Similarly, systems that are no longer carrying traffic but have not been decommissioned yet should be identified as "out-of-service". Finally, a "maintenance" state indicating that maintenance activities are in progress should be supported.

7.2.1.6 Faults mapped to configuration (equipment/functions/trails/services)

One of the most critical functions that a network management system must perform in order to automate fault activities is the association of alarm and status information with network configuration including both physical and logical relationships in the network.

7.3 Performance management

7.3.1 Performance management functions

Function set that reports on and evaluates network behaviour and effectiveness; monitors, modifies and controls resources utilization (e.g. throughput, average response time and data flow).

- Performance management functions enable the monitoring of the performance/QOS parameters such as CLR, CTD and CDV etc. The general B-ISDN performance parameters are specified in Recommendation I.356. Procedures may be in-service (e.g. PM cells), or out-of-band service by test procedures.
- Performance anomalies that meet threshold or trend definitions will result in alarm objects that will alert the fault management system of the problem, but performance management must provide flexible real-time presentation and reporting capabilities for all current and historical network performance data. Performance enquiries must be supported at the service, network and element management levels. Performance problems determined by threshold violations or trends must be reported to fault management for localization and corrective action.
- Performance management must have the ability to determine if the performance of any network resource is degrading over time as an early network problem indication.
- Performance management must include the ability to determine if performance parameter data received from the network have exceeded user specified values or thresholds.
- This element management layer function manages the interface to the managed object including session management if applicable.

7.4 Accounting management

This function performs usage measurements and provides data for billing and reporting purposes.

7.4.1 Billing measurement functions

- Collecting and storing network usage data. The collection of measurements data that indicates the network usage interval is automatically generated, collected and stored by the network elements.
- Distributing the collected data.
- Reporting the large amounts of billing measurement data in an appropriate billing format.

7.4.2 Traffic measurements functions

- Collecting sets of measurements data from a given network. The collection of data could be scheduled at regular, prespecified intervals or on demand.
- Storing and distribution of collected measurement data for later use.

7.5 Security management

7.5.1 Security management function

Function set that manages the integrity of the network's data. Security is an important link in a network management architecture. The following functions apply:

- enforce unique user ID;
- maintain all currently active users;
- ability to authenticate users;
- prevent bypassing the deployed authenticate mechanism;
- maintain access control;
- prevent access to any user unless identified and authenticated;

- prevent access if information is invalid;
- record overall log-in activities;
- provide time-out feature;
- secure log-off;
- provide additional security checks for remote access mechanism;
- provide a security log;
- provide security log to support after-the-fact investigation;
- provide security log entry that include user ID;
- monitor and report in real-time any security violation;
- provide status reports.

7.5.2 Mechanisms for security management

A partial list of mechanisms for security management in B-ISDN environment could be defined as follows:

a) *Authentication*

A procedure to verify the identity of the served user. Different authentication procedures may be used.

b) *Authorization*

The permission for the user to use the service.

c) *Access control*

The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

d) *Integrity*

The provision of the complete data and the guarantee that it has not been altered or destroyed in an unauthorized manner.

e) *Confidentiality*

The protection of data for making information unavailable or for disclosing it to unauthorized access.

7.5.3 Provision of security management

Security management mechanisms will be provided to the user after arrangement with the service provider whenever the provision of such mechanisms (security services) is part of the (supplementary) service. The service provider will inform the user of the user's confidential code. Security mechanisms are automatically activated at subscription of the related (supplementary) service and are automatically deactivated if all supplementary (services) related to this have been withdrawn.

Annex A

B-ISDN service requirements template

A.1 B-ISDN service

This subclause identifies the name of the service or service feature.

A.2 Service description

This subclause provides a high level description of the service from the user point of view. A further description of the service features may also be necessary.

A.3 Communication configuration(s)

This subclause specifies the communication configuration(s) needed from the network side, including bandwidth restrictions, etc. to support the B-ISDN service requested.

A.4 Connection type(s)

This subclause identifies the broadband network connection types as defined in this Recommendation.

A.5 B-ISDN network capability requirements

This subclause identifies the network interconnection steps required to implement the service. Supporting figures are needed.

A.6 Specific B-ISDN signalling requirements

A list of the B-ISDN signalling requirements are identified to support the step-by-step implementation of the service.

A.7 Interworking

This subclause identifies any interworking requirements with prior B-ISDN capability sets or release(s).

Appendix I

Examples of communication configurations

This Appendix describes a number of configuration alternatives to support:

- multipoint-to-point communication configuration;
- multipoint-to-multipoint communication configuration;
- bidirectional point-to-multipoint communication configuration.

The alternatives are relevant when defining a signalling requirement. The different alternatives also represent different requirements on layer management and on network design.

I.1 Example of multipoint-to-point communication configurations

I.1.1 Cell interleaving at the ATM layer

The data from leaves "B" and "C" are interleaved on the same VCI at point "I" and transferred towards the root "A". See Figure I.1-1.

The data volume generated by each leaf "B" and "C" may be different. The data volume received by the root "A" is the sum of the data volume generated by the leaves "B" and "C" unless there is congestion in the network. When reserving resources (bandwidth) in the network it should be considered that the sources are independent. Layer management problems with this configuration exist and are for further study.

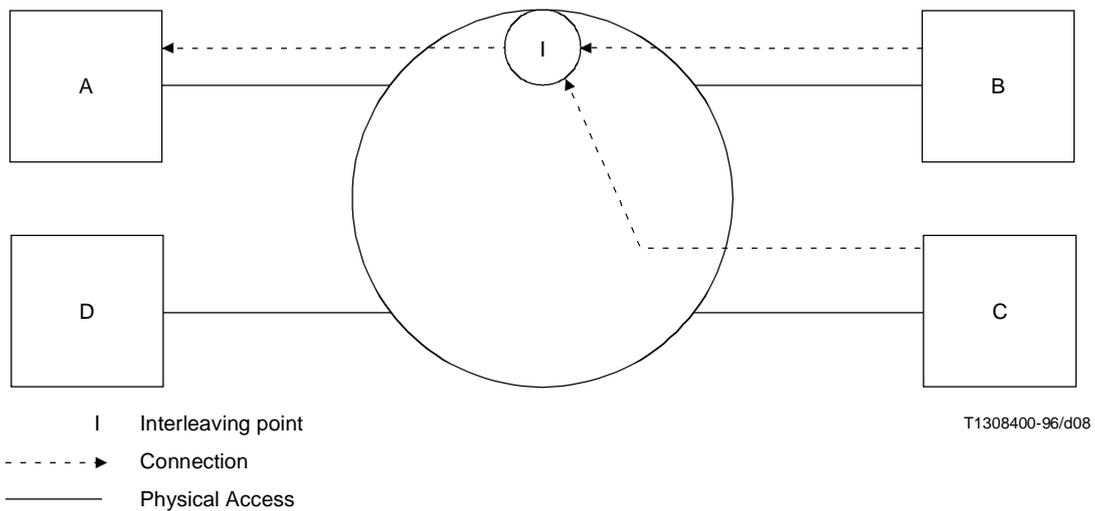


Figure I.1-1/I.313 – Interleaving connection

I.1.2 Multiple Type 1 point-to-point connections

Different point-to-point Type 1 connections are established from the "leaves" "B" and "C" to the "root" "A". See Figure I.1-2.

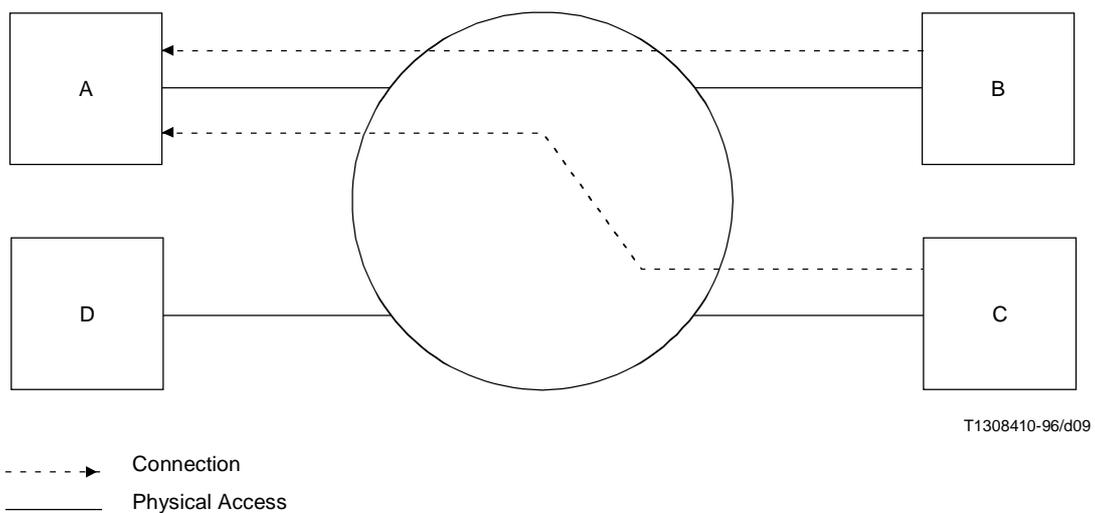


Figure I.1-2/I.313 – Multiple point-to-point connections

The data volume generated by each leaf "B" and "C" may be different. The data volume received by the root "A" is the sum of the data volume generated by the leaves "B" and "C" unless there is congestion in the network. When reserving resources (bandwidth) in the network it should be considered that the sources are independent.

The application and the protocols are completely transparent to the ATM network.

The layer management is not a problem and identical to the one defined for point-to-point connections.

I.1.3 Using a server

This configuration is established by using three separate Type 1 point-to-point connections at the ATM layer between the users and the server. A server "S" is receiving data from the leaves "B" and "C" and the server may process the information before it is relayed to the root "A". The server "S" may either be integrated with the network as in Figure I.1-3 or external to the network.

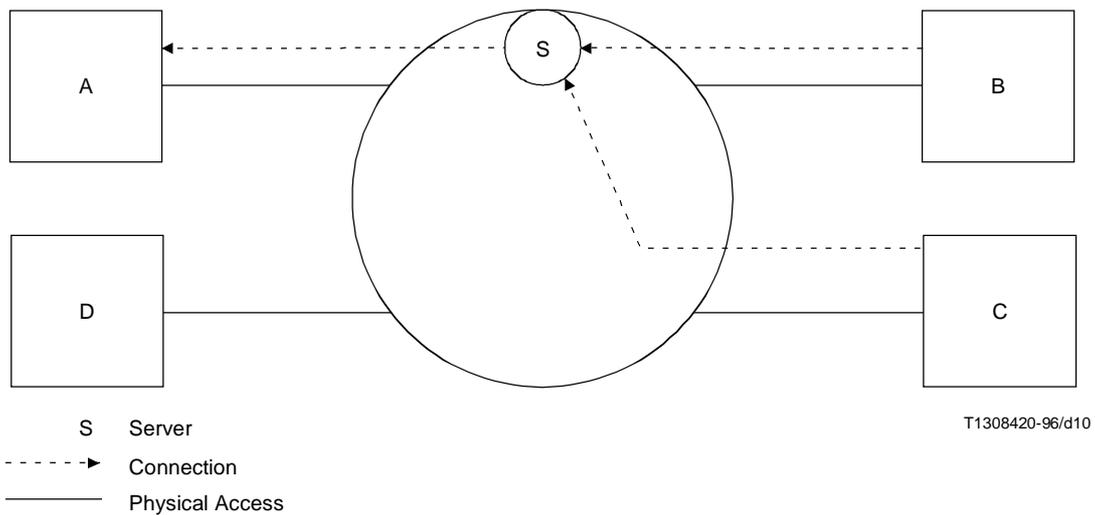


Figure I.1-3/I.313 – Server application

The data volume generated by each leaf "B" and "C" may be different. The data volume received by the root "A" may be different from the sum of the data volume generated by the leaves "B" and "C" since the service dependent server "S" may process the information before relaying it to the root "A". When reserving resources (bandwidth) in the network it should be considered that the sources are independent.

Management is not a problem in this case. The three connections at the ATM layer are managed as separate point-to-point connections. The server "S" terminating higher layer protocols is also managed and maintained separately.

I.2 Example of multipoint-to-multipoint communication configurations

I.2.1 Combining Type 2 point-to-multipoint connections with cell interleaving

The data from each port "A", "B" and "C" is replicated "R" and interleaved "I" before it is transferred back to ports "A", "B" and "C". This is done so that everybody can listen in to anybody else (but not to himself). Each port will represent the root to a generated as well as interleaved data stream. See Figure I.2-1.

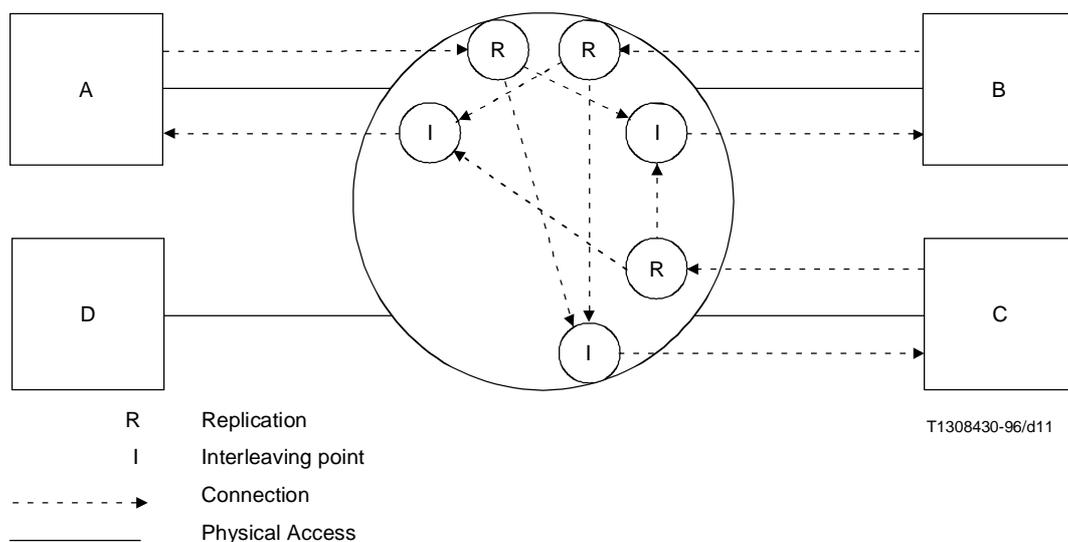


Figure I.2-1/I.313 – Point-to-multipoint interleaved connection

The data volume generated by each of the terminals may be different. The data volume received by a terminal is the sum of the data volume generated by the other terminals unless there is congestion in the network. The bandwidth reservation in the network may be different at different segments due to burstiness, etc.

Most of the conference functionality for a higher layer (in a voice conference, for example) have still to be implemented in the terminals. Observe also the problem we have with identifying the source when interleaving "I" is ATM cell based as in this case.

In this case, the user application can provide feedback from a master (A, B or C), adding some discipline into the conference in order to avoid that terminals generate data independent of each other, thereby improving the resource utilization in the network.

Layer management problems exist with this configuration and are for further study.

I.2.2 Multiple Type 2 point-to-multipoint connections

To support the conference between N users as many (N) point-to-multipoint connections as terminals (ports) involved in the conference are established. Each terminal represents a root to one such connection. See Figure I.2-2.

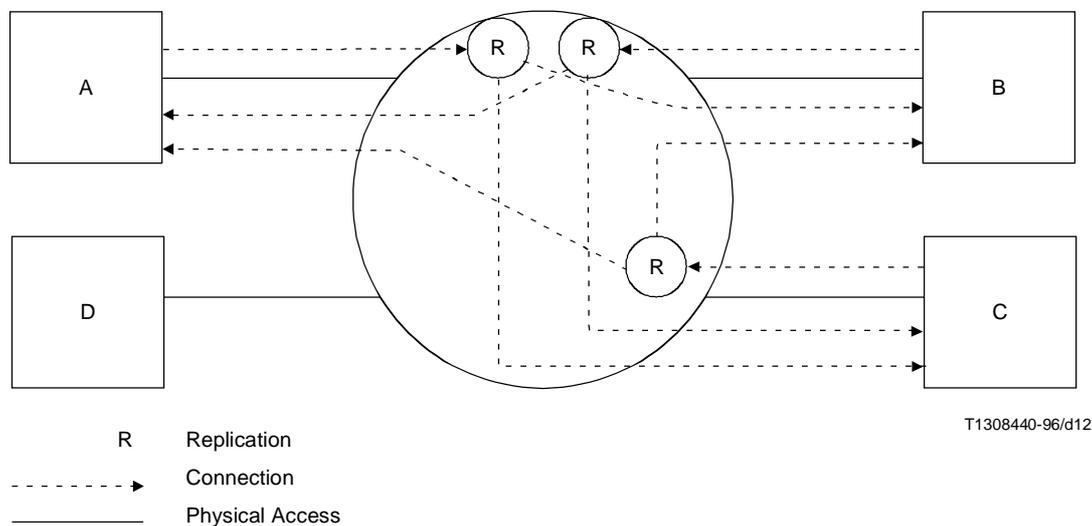


Figure I.2-2/I.313 – Multiple Type 2 connections

The data volume generated by each of the terminals may be different. The data volume received by a terminal is the sum of the data volume generated by the other terminals unless there is congestion in the network. The bandwidth reservation in the network may be different at different segments due to burstiness, etc.

Most of the conference functionality for a higher layer (in a voice conference, for example) have still to be implemented in the terminals. In this case we will not have the problem to identify the source.

In this case, the user application can provide feedback from a master (A, B or C), adding some discipline into the conference in order to avoid that terminals generate data independent of each other, thereby improving the resource utilization in the network.

The layer management functionality is limited to connection Type 2. Each Type 2 connection will use a different VCI.

I.2.3 Using a server

This configuration is established by using three separate Type 1 point-to-point connections at the ATM layer between the users and the server.

An application dependent server "S" is introduced to provide the conference service. The server "S" may process the information before it is returned to all users in the conference. The server "S" may either be integrated with the network as in Figure I.2-3 or external to the network.

All connections are Type 1 (bidirectional).

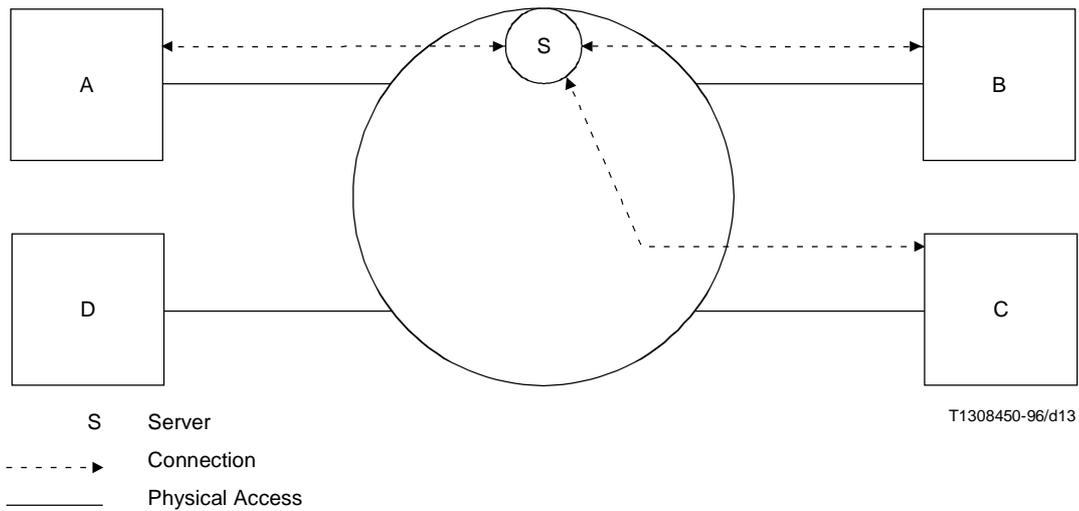


Figure I.2-3/I.313 – Server application

The data volume generated by each of the terminals may be different. In addition, the data volume received by a terminal may be different from the sum of the data volume generated by the other terminals since the service dependent server "S" may process the information before relaying it. The bandwidth reservation in the network may also be different at different segments.

The management is not a problem in this case. The three connections at the ATM layer are managed as separate point-to-point connections. The server "S" terminating higher layer protocols are also managed and maintained separately.

I.3 Example of bidirectional point-to-multipoint communication configuration

I.3.1 Type 5 connection with cell interleaving

For the communication from the root "A" to the leaves "B" and "C" a point-to-multipoint connection with replication function "R" is used. In the backward direction the cell interleaving "I" is used, as shown in Figure I.3-1.

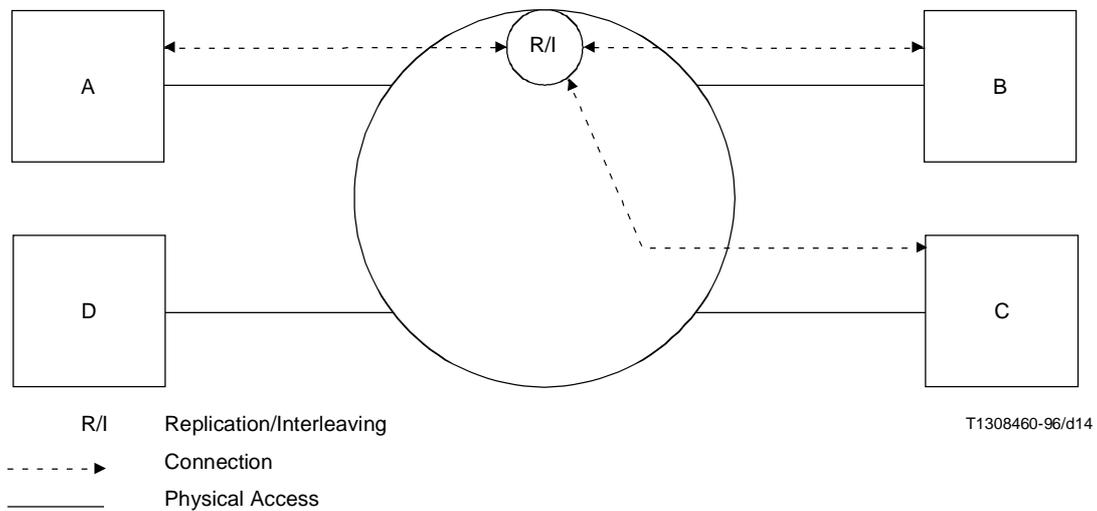


Figure I.3-1/I.313 – Type 5 connection with cell interleaving

The data volume received by leaves "B" and "C" is the same as the data volume transmitted from the root "A". The bandwidth reservation in the network is also assumed to be the same. The data volume received by the root "A" will be the sum of the data volume generated by the leaves "B" and "C" unless there is congestion in the network. The bandwidth reservation for the backward direction at the root "A" may, however, be different from the sum of the bandwidth allocated from the leaves "B" and "C", assuming that "B" and "C" are never transmitting at the same time (solved by a higher layer protocol) or assuming statistical gain in the network.

If the cell interleaving is made at the ATM layer, the root "A" can handle only single cell messages.

Layer management problems exist with this configuration and are for further study.

I.3.2 Combining Type 1 and Type 2 connections

Different Type 1 connections are established from the "leaves" "B" and "C" to the "root" "A" for the backward information (see Figure I.3-2).

For the forward direction from the "root" "A" a Type 2 connection is established.

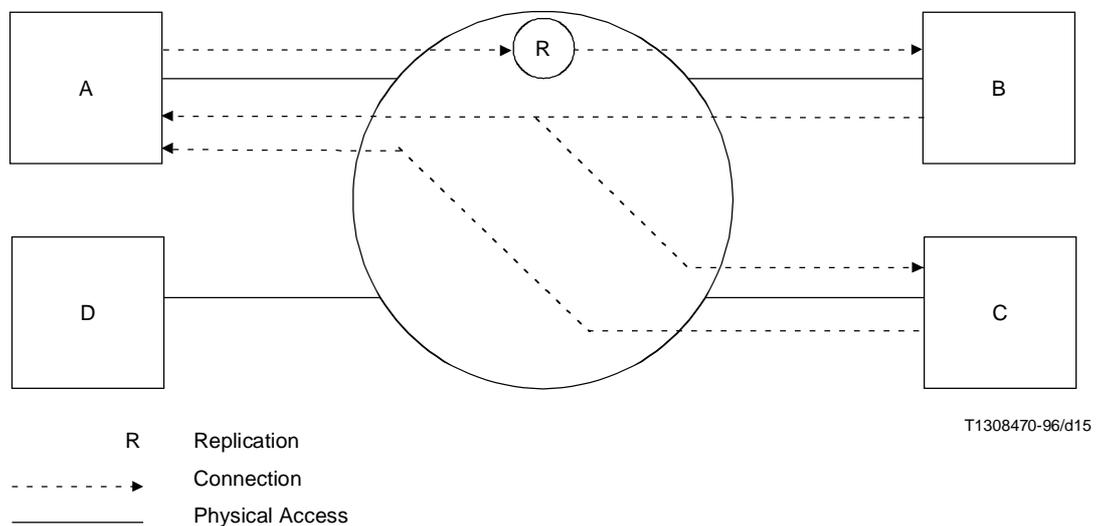


Figure I.3-2/I.313 – Combining Type 2 and Type 1 connections

The data volume received by leaves "B" and "C" is expected to be the same as the data volume transmitted from the root "A". The bandwidth reservation in the network is also assumed to be the same. The data volume received by the root "A" will be the sum of the data volume generated by the leaves "B" and "C" unless there is congestion in the network. The bandwidth reservation for the backward direction may, however, be different for different segments of the backward connections, assuming that "B" and "C" are never transmitting at the same time (solved by a higher layer protocol).

The application and the protocols are here completely transparent to the ATM network.

The layer management functionality is limited to the one for Type 1 and Type 2. Each connection will use a different VCI value.

I.3.3 Using a server

This configuration is established by using three separate Type 1 point-to-point connections at the ATM layer between the users and the server.

An application dependent server "S" is introduced to provide the service. The server "S" may process the information from the leaves "B" and "C" before it is passed to the root "A". The server "S" may either be integrated with the network as in Figure I.3-3 or external to the network.

All connections are Type 1 (bidirectional).

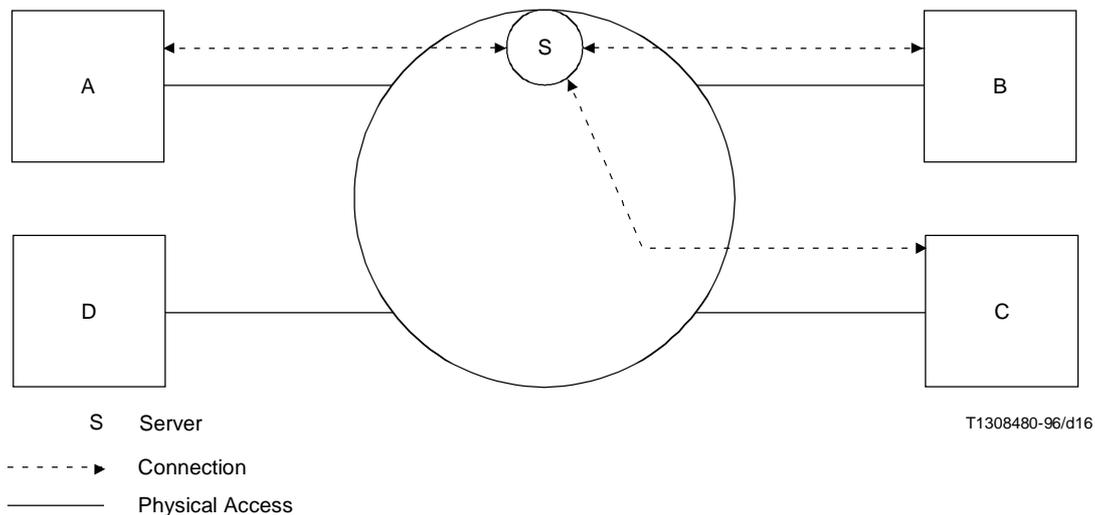


Figure I.3-3/I.313 – Server application

Since processing may be involved in the server, the bandwidth on the different point-to-point connections may be different and asymmetric.

The management is not a problem in this case. The three connections at the ATM layer are managed as separate point-to-point connections. The server "S" terminating higher layer protocols is also managed and maintained separately.

Appendix II

B-ISDN service requirements template for database backup/alignment

II.1 B-ISDN service name

Database backup/alignment.

II.2 Service description

The database backup/alignment scenario describes a company's telecommunications activity requiring the transfer of portions and/or complete client/server databases on a regular basis. This database would include not only traditional accounting and inventory information, but also graphical images of receipts required to substantiate customer transactions.

II.2.1 Service feature description

Typically, client-server applications use real-time systems which track business operations as the transactions occur. These transactions are applied to fresh copies of local, regional and corporate databases on a daily basis. At the close of the daily business cycle, information on these databases is transferred to regional and corporate offices to reflect business activity for that cycle. This activity provides even the largest business with an up-to-date picture of corporate position.

Figure II.1 describes a company model outlining a transaction function of the type outlined above. Specific application examples might be:

- point of sale accounting;
- teller activities in local, regional corporate offices;
- intermediate transfer agencies (transportation agents);
- image data for credit card vouchers.

The common entity for all these activities is the need to track tens or hundreds of thousands of transactions per field location and "batch copies of these transactions" electronically to complete various levels of account tracking.

For example, look at an inventory application. This application would track real-time database transactions occurring locally in each field location. Nightly, complete images of the database would be transferred to regional sites. Regional sites would analyse inventory changes including orders for out-of-stock items. The regional application would determine whether the requested items could be satisfied by another location within that region or, if not, forward the requests on to the corporate offices. A similar stock comparison would be made by the headquarters location among regional sites. Those requests would be provided either by another region or ordered from an outside vendor.

It should be noted that a similar technique would be used for accounting for credit card purchases where the individual merchants provide credit card vouchers to the card issuing companies for billing verification of purchases. Credit card companies are required to have copies of vouchers in hand prior to billing a charge. By providing image data from the merchant, the float time is reduced for both the merchant and the card issuer.

The signalling requirements for the uploading of transaction data/images are shown in Figure II.1.

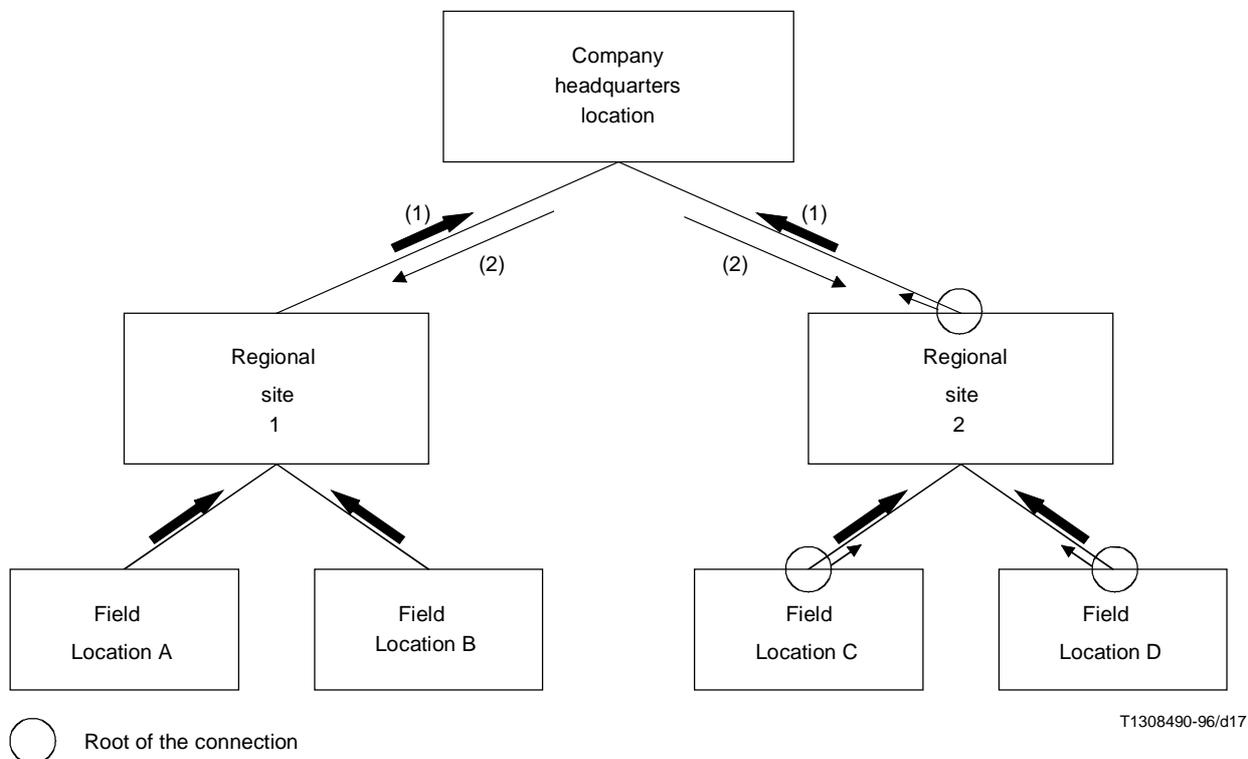


Figure II.1/I.313 – Database backup application

Point-to-point connection

Upload function transaction summaries are forwarded up to each region on to headquarters.

- Arrow (1) in Figure II.1 illustrates transfer of transaction data to corporate facilities. B-ISDN signalling requirements would correspond to (1) in Figure II.3 for the Type 1 connection.
- Arrow (2) in Figure II.1 is the response and is shown as item (2) of the Type 1 connection in Figure II.3.

Specific signalling interactions are shown as follows in Figure II.2.

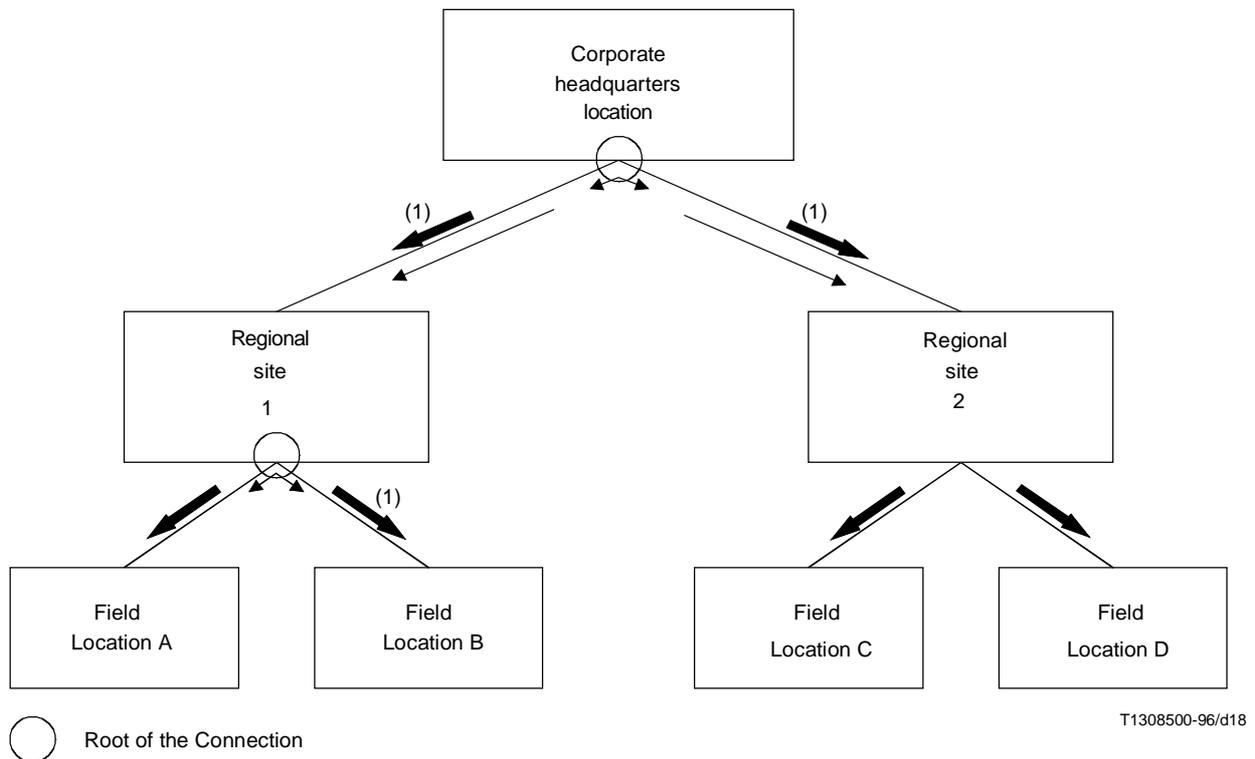


Figure II.2/I.313 – Database backup application

Point-to-multipoint connection

The download function takes complete copies of the updated databases and transfers them to regional and field offices nightly. This not only provides for daily synchronization of data, but also offsite security.

Figure II.2 provides the database download function. Item (1) represents the transfer of data from corporate facilities to regional/field sites using point-to-multipoint connections. These correspond to the connections pictured in Figure II.4. The database information is replicated to all regional sites.

II.3 Communication configurations

- Point-to-point requiring asymmetric bandwidth.
- Point-to-multipoint.

II.4 Connection type(s)

- Connection Type 1.
- Connection Type 2.

II.5 B-ISDN network capability requirements

See Figures II.3 and II.4.

(1) Connection illustrates the point-to-point connection which is required to support the database transfer function.

(2) Connection illustrates the response confirmation in nightly response to nightly transfer control/management information.

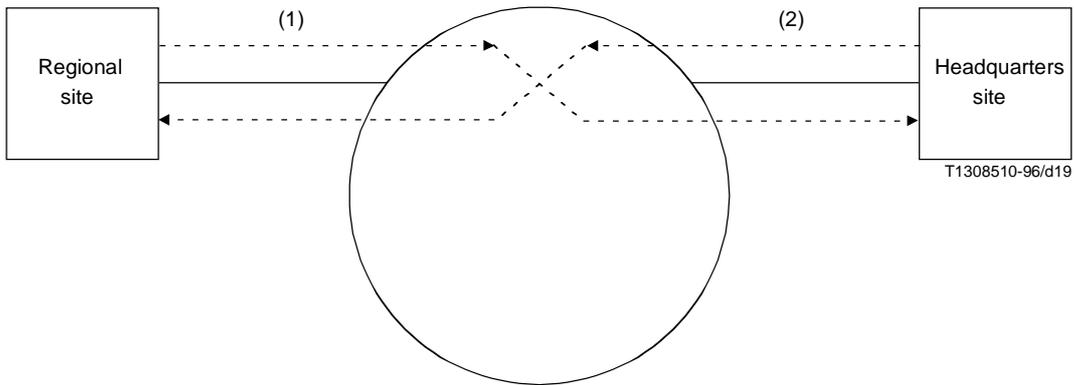


Figure II.3/I.313 – Point-to-point connection Type 1 for field to regional site, regional site to field

(1) Connection illustrates the point-to-multipoint connection which is required to support the database transfer from Corporate site to Regional sites. The replication function (R) creates duplicate copies to regional locations

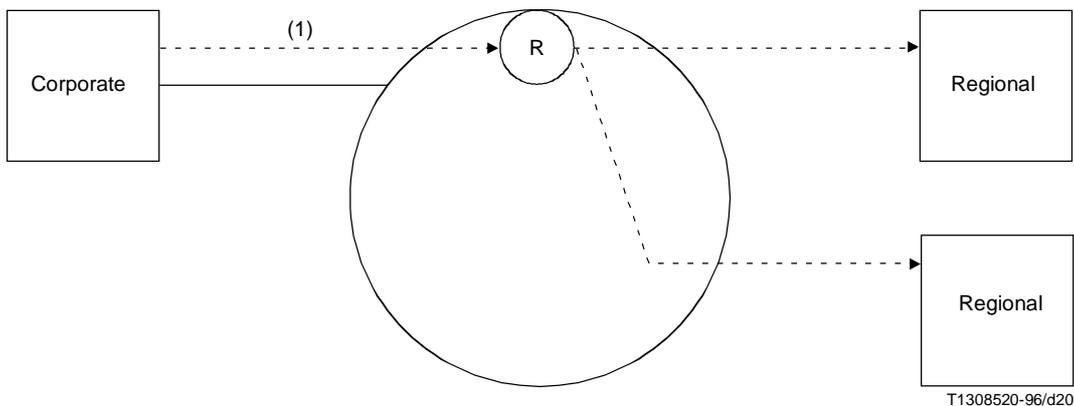


Figure II.4/I.313 – Point-to-multipoint connection Type 2 for corporate to regional locations

II.6 Specific B-ISDN signalling requirements

The signalling requirements fall into two categories:

- requirements for uploading the databases from individual field locations and regional operations following daily business; and
- requirements for downloading the updated databases from the corporate headquarters following nightly backroom processing. The following illustrates some of the signalling requirements necessary for this application.

Call and network connection establishment – Type 1 connection

Establishment of a call containing a point-to-point network connection requested by a party that will be a connection endpoint (Items 1 and 2 in Figures II.1 and II.3, respectively).

Call and network connection establishment – Type 2 connection

- Establishment of a call containing a point-to-multipoint network connection group requested by a party who is the root of the network connection group. (Item 1 in Figures II.2 and II.4.)
- Release/detach connections:
 - Detach a party from an existing network connection when requested by the party itself.
 - Release a network connection from an existing call requested by the call owner.
 - Release a party from an existing call when requested by the call owner.
 - Release an existing call requested by the call owner party.
 - Release a party from several existing connections requested by a party that is also an endpoint of the connection associated with the party to be released.

II.7 Interworking

For further study.

Appendix III

B-ISDN service requirements template for video on demand

III.1 B-ISDN service name

Video on demand.

III.2 Service description

The video on demand application would provide for multiplexing of original sources into a common multiplexed signal. Included in this application is a video on demand capability which would be accessed via selections from the consumer CPE and which would result in the transmission of selected video information back to the consumer.

Service feature description

The video application would merge video signals from various sources into a multiplexed signal transmitted typically to households. The sources for these signals would come into the video service provider from a variety of means including satellite feeds, network feeds from local stations, local videodisk/videotape and on-demand video server. Also included in the signal sent to customer CPE is a variety of management messages which include individual units authorizations, operational information and customer requests (for the video on demand). Due to the variable nature of a portion of the signal, the ability to adjust bandwidth to end users is a critical requirement. The topology for this application could be described as in Figure III.1.

This application combines various sources of video signals into a multiplexed signal which can be transmitted to subscribers. This application would provide for video on demand.

III.3 Communication configuration(s)

Point-to-multipoint asymmetric bandwidth.

III.4 Connection type(s)

Connection Types 1 and 2.

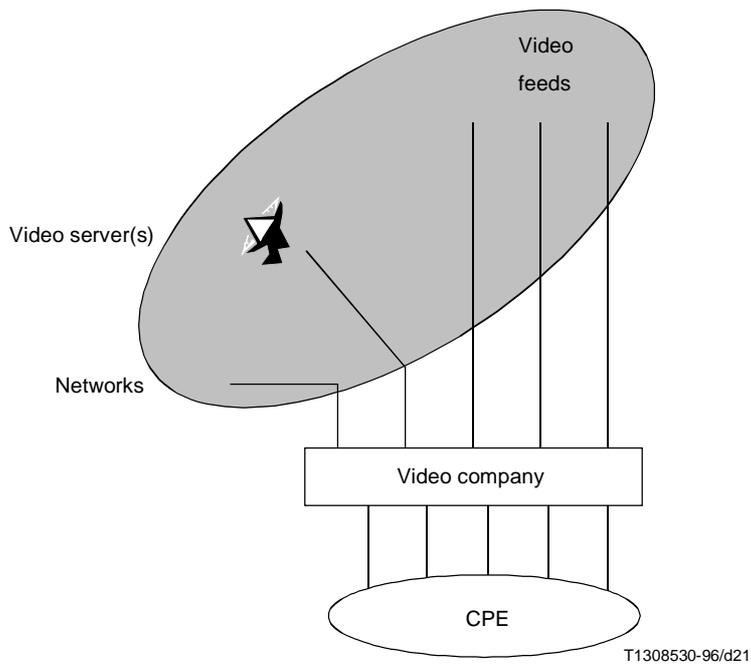


Figure III.1/I.313 – Point-to-multipoint

III.5 B-ISDN network capability requirements

See Figures III.2 and III.3.

Video on Demand
Step 1

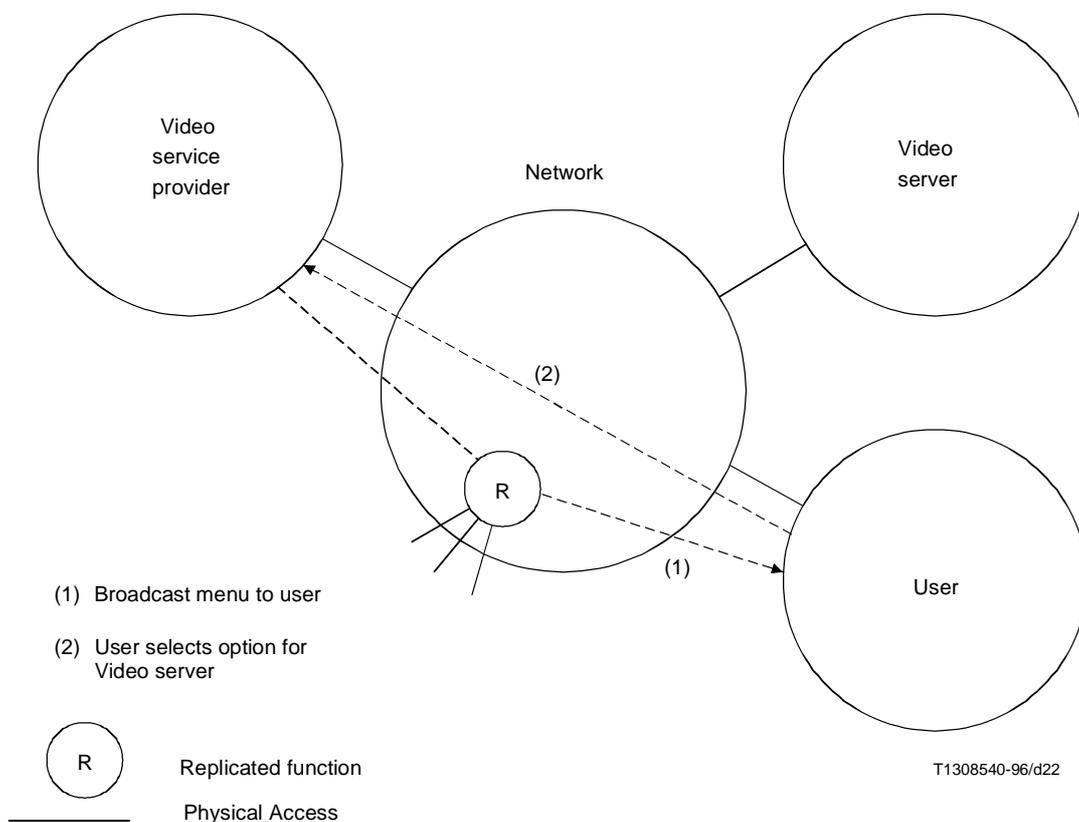


Figure III.2/I.313 – User selection of video service

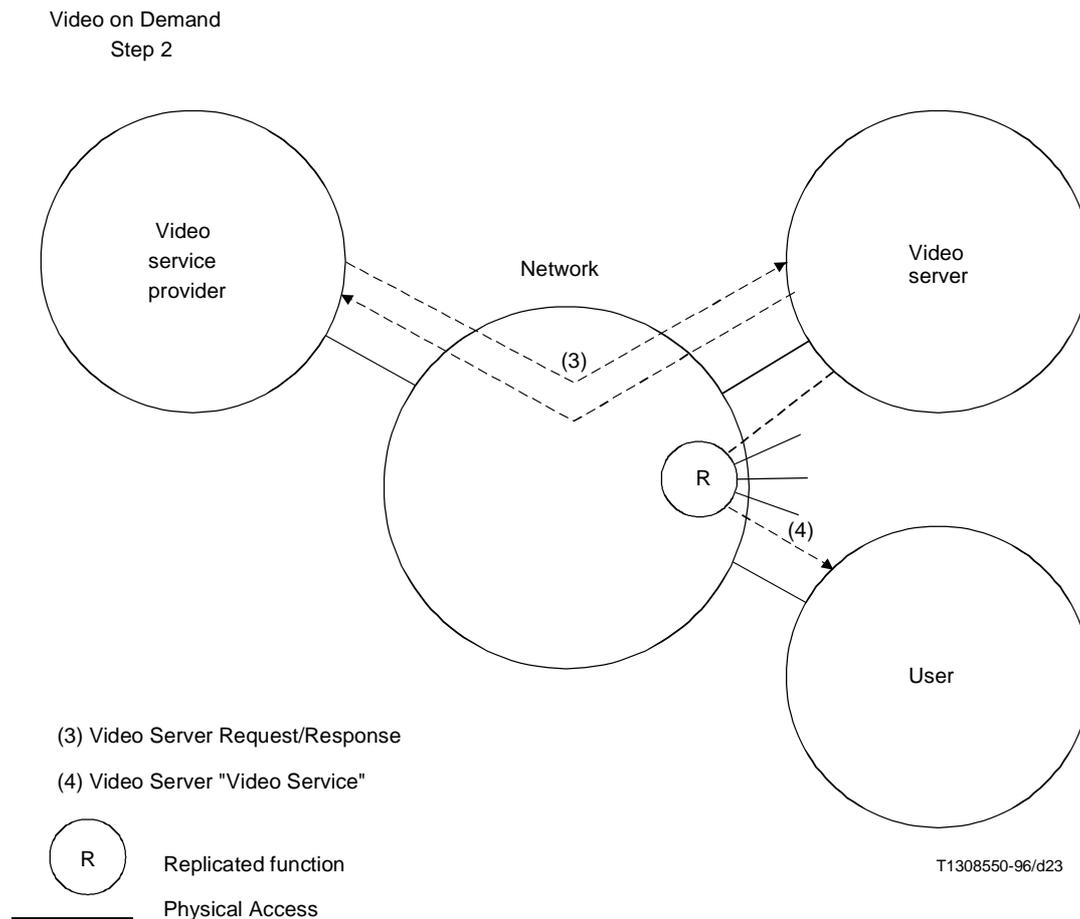


Figure III.3/I.313 – Video server provides service

III.6 Specific B-ISDN signalling requirements

A large bandwidth is required to support this type of service application. As in other applications, the information flow is bidirectional but asymmetric in bandwidth. Small bandwidth capability from the CPE to video company and from the CPE to the source is required, large bandwidth from video company to CPE and from the source to video company.

The following are examples of the signalling requirements necessary to accomplish the video on demand company. Note that many applications would be necessary to accommodate specific business needs including provision of the video service, billing, etc. These interactions therefore are only an example of the signalling requirements to provide this service.

Call and network connection establishment – Type 2 connection

- Establishment of a call containing a point-to-multipoint network connection group requested by a party who is the root of the network connection group. (Item 1 in Figure III.2.)

Call and network connection establishment – Type 1 connection

- Establishment of a call containing a point-to-point network connection requested by a party that will be the sink of the connection. (Item 2 in Figure III.2.)

Call and network connection establishment – Type 1 connection

- Establishment of a call containing a point-to-point network connection requested by a party that will not be a connection endpoint. (Item 3 in Figure III.3.)

Call and network connection establishment – Type 2 connection

- Establishment of a call containing a point-to-multipoint network connection group requested by a party who is the root of the network connection group. (Item 4 in Figure III.3.)
- Release/detach connections.
- Detach a party from an existing network connection when requested by the party itself.
- Release a network connection from an existing call requested by the call owner.
- Release a party from an existing call when requested by the call owner.
- Release an existing call requested by the call owner party.
- Release a party from several existing connections requested by a party that is also an endpoint of the connection associated with the party to be released.
- Negotiation and renegotiation of the traffic characteristics.
- Addition and release of connections within a call.

III.7 Interworking

For further study.

Appendix IV

B-ISDN service requirements template for CDH services

IV.1 B-ISDN service name

Multimedia document handling services.

IV.2 Service description

IV.2.1 CDH service

Multimedia Cooperative Document Handling (CDH) services allow for audiovisual communication between one editor and several participants and provide them with the facilities needed to handle Multimedia Documents (MMDs). This service allows for serial editing through one editor only.

IV.2.2 Service feature description

Audiovisual conferencing facilities will provide audio communication from the beginning of the call. Video communication may be added immediately at the beginning of the call, or later on request.

Document handling functionalities provide for the following Service Features (SFs):

- retrieving of the MMD to be discussed from a remote store/server. This may take place at the beginning of the call and will usually be done by the editor;
- distribution of the MMD from the editor to (all) other participants in the call/conference. This will usually happen at the beginning of the call;

- distribution of the editor's screen to the other participants so that everybody can see that part of the MMD which is currently discussed. This will happen during the main part of the call;
- moving a pointer on the editor's screen by sending control information from an appropriate control device (e.g. a mouse). This is provided on request to an end user wishing to comment on the MMD and may be deactivated after the comment has been made;
- sending of comments or modifications from one participant to the editor. This allows (only) one participant to comment on the MMD at the time. When the comment is expressed orally, this functionality is not needed because conferencing is active and such comments will be made during the discussion together with using the pointer. But when the comment contains a modification, e.g. the insertion of a new section into the MMD, this functionality will be needed;
- sending the edited document to a remote store/server after the session. This will usually be done by the editor and may take place after having already deactivated the conferencing, i.e. at the end of the call.

Concerning the use of CDH services, it is assumed that the conferencing facilities will be active during most of the call. Additionally, those document handling functionalities which are necessary for the specific application will be activated.

IV.3 Communication configuration(s)

- Multipoint-to-multipoint – symmetric.
- Point-to-multipoint – unidirectional.
- Point-to-point – unidirectional.

IV.4 Connection type(s)

- Connection Type 1.
- Connection Type 2.
- Connection Type 4.

Existing multimedia communication applications are presently running on Local Area Networks. Their main features are the following:

- The video conference service is based on a multiwindow concept, in which each participant screen is displaying one picture per correspondent in a small window. Thus, the input scheme supports point-to-point channels – one per video image; and no picture processing in a server is required.
- There is not one single editor for the document. The participants are actually sharing the same document and are informally allowed to modify it when needed in the meeting.

This kind of telemeeting application, already used on LANs, is generally well-suited for informal working meetings or Drafting Groups with a reasonable number of participants.

As far as the network requirements are concerned, since the applications have originally been designed for TCP/IP base exchanges, their existing ATM implementation is built up with a full multiple point-to-point linkage between end points. Thus, only Type 1 connection is required.

IV.5 B-ISDN network capabilities

Connection Type 1 – Point-to-point connections

Type 1 connections provide the users with the unidirectional communication capabilities for the sending of comments or modifications to the editor and for moving the pointer on the editor's screen. See Figure IV.1.

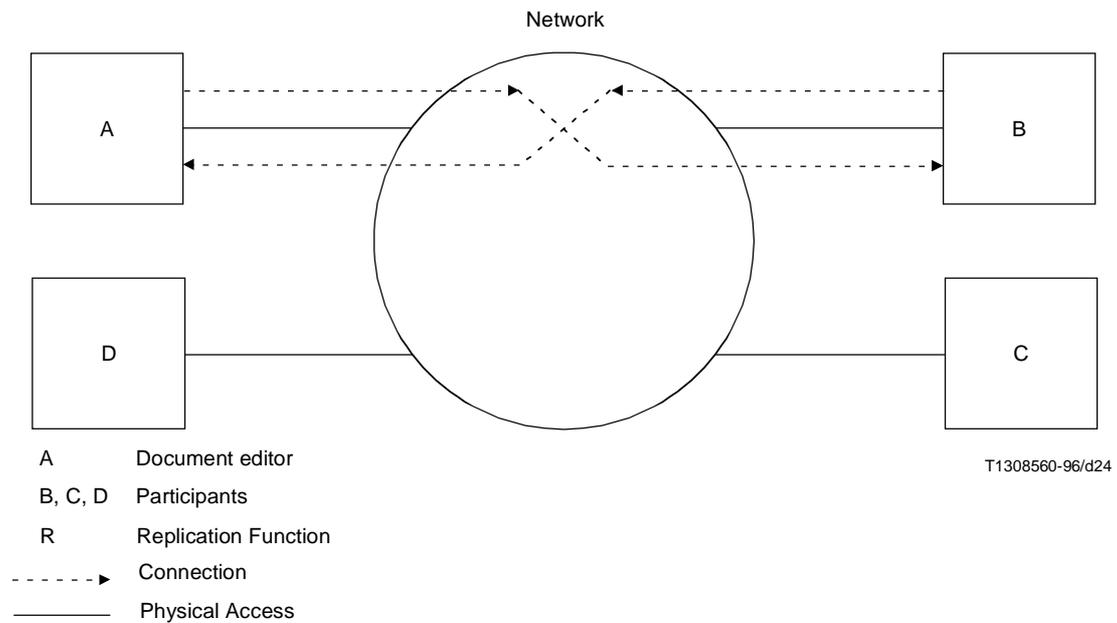


Figure IV.1/I.313 – Bidirectional point-to-point

Connection Type 2 – Point-to-multipoint connections

Type 2 connections provide the editor with the unidirectional communications for the distribution of the MMD and of his screen to the other users. See Figure IV.2.

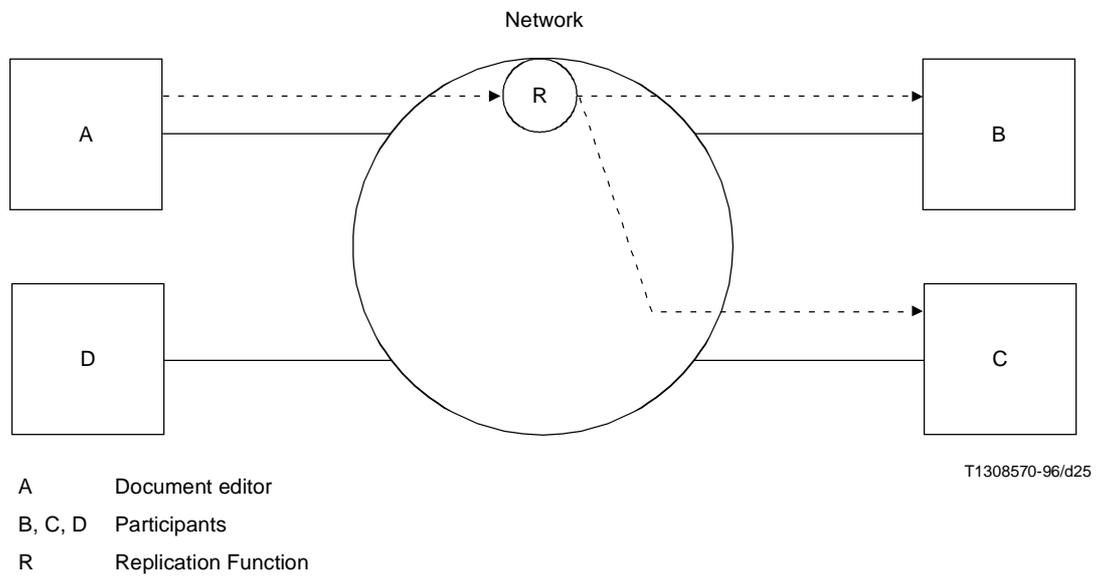


Figure IV.2/I.313 – Unidirectional point-to-multipoint connection

Connection Type 4 – Multipoint-to-multipoint connection

The multipoint-to-multipoint connection provides the communication capability for the audiovisual conferencing. See Figure IV.3.

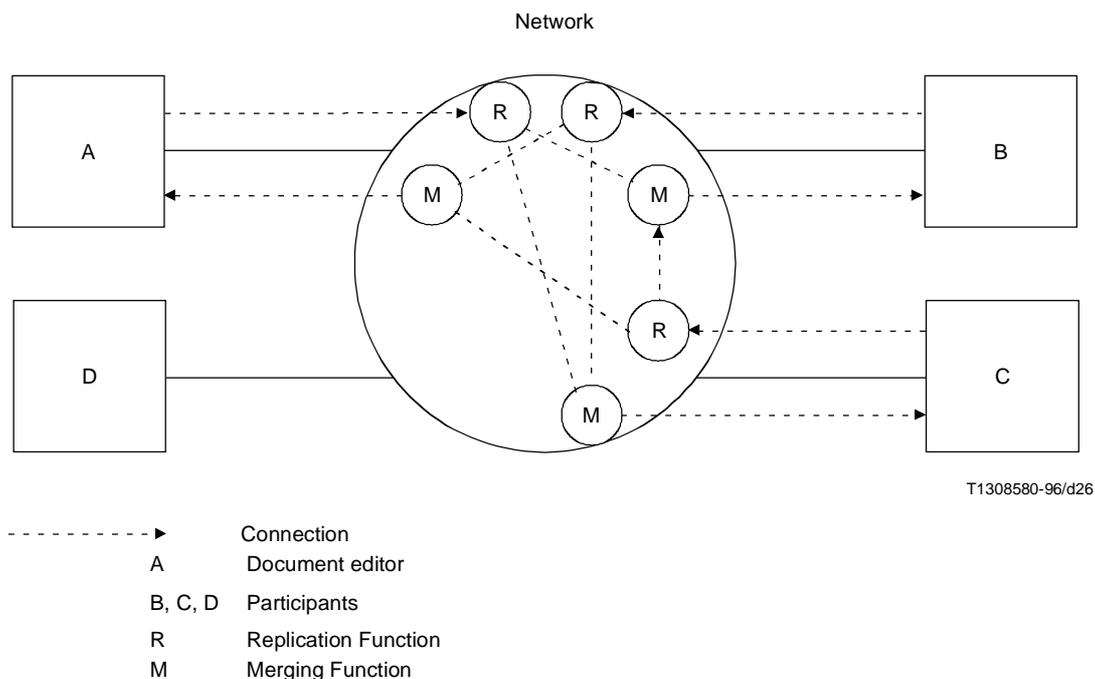


Figure IV.3/I.313 – Multipoint-to-multipoint connection

IV.6 Specific B-ISDN signalling requirements

To be developed.

IV.7 Interworking

For further study.

Appendix V

Use of NSAP address formats for private ATM network addressing

This Appendix provides guidance on the use of the NSAP address formats in defining a private ATM network address. ATM private network addresses may be modelled on the OSI Network Service Access Point (NSAP) address structure defined in Annex A of ITU-T Rec. X.213 | ISO/IEC 8348. The NSAP format address will be carried transparently across the network.

V.1 NSAP structures

This subclause provides an overview of the NSAP address structure. Annex A of ITU-T Rec. X.213 | ISO/IEC 8348 is the definitive text for the OSI Network Service Access Point (NSAP) address structure.

An NSAP address consists of two basic semantic parts. The first part is the **Initial Domain Part (IDP)** and the second part is the **Domain Specific Part (DSP)** as illustrated by Figure V.1.

The **Initial Domain Part IDP** consists of two fields – The Authority and Format Identifier (AFI) and the Initial Domain Identifier (IDI). The abstract syntax of the IDP is decimal digits.

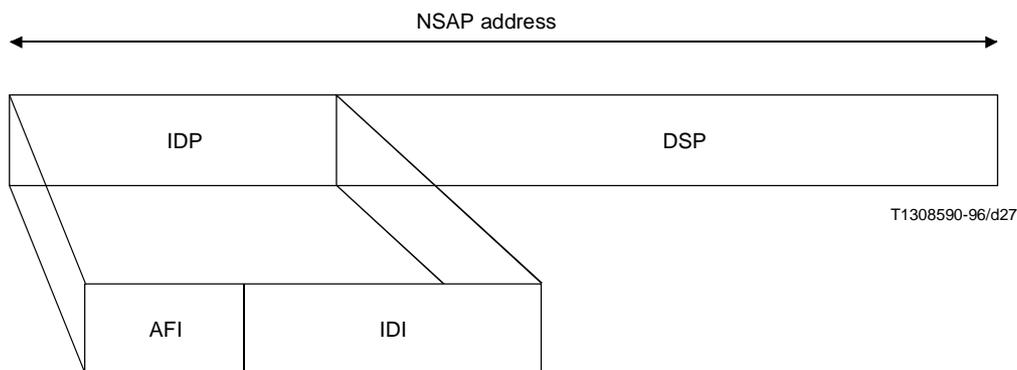


Figure V.1/I.313 – NSAP address structure

The **Authority and Format Identifier (AFI)** specifies:

- a) the format of the IDI;
- b) the network addressing authority responsible for allocating values of the IDI;
- c) whether or not leading zero digits in the IDI are significant; and
- d) the abstract syntax of the DSP.

The **Initial Domain Identifier (IDI)** specifies:

- a) the network addressing domain from which the values of the DSP are allocated; and
- b) the network addressing authority responsible for allocating values of the DSP from that authority.

The **Domain Specific Part (DSP)** identifies a specific network address within the addressing domain.

V.2 ATM address formats

Three possible NSAP address formats are suitable for structuring an ATM address for use in private B-ISDN networks. These formats are identified by the AFI value as allocated in the following table.

AFI value	Format
45, 59 (Note 1)	Rec. E.164
47	ISO 6523 ICD (Note 2)
39	ISO DCC (Note 2)

NOTE 1 – The numerically greater AFI value is used when the first significant digit in the IDI is zero. The called party E.164 address can be determined from the NSAP format address when this format is used. The determination of the E.164 called party number resulting from analysis of the NSAP format address requires additional functionality in the network. Only the E.164 number can be used for routing a call within the B-ISDN.

NOTE 2 – The ISO ICD and ISO DCC formats are the so-called "network independent" formats and contain no information on the point of attachment (i.e. the E.164 number) of the private network or terminal to the public network. When establishing a call across the public B-ISDN, the use of these formats implies that an "alternative address" (to the default E.164 address) is being used to identify the called party. If these formats are used to identify the called party address (within the public network), additional functionality is required within the private network gateway (or the public network) to resolve the called party E.164 address. The use and support of these formats within the public B-ISDN network is for further study.

V.2.1 E.164 IDI format

The IDI consists of an ISDN number of up to 15 digits allocated according to Recommendation E.164. The international format of the E.164 number will be used. The full ISDN number identifies the authority responsible for allocating and assigning values of the DSP; i.e. the owner of the E.164 number. The semantics of the IDI is 15 digits and thus the length of the IDP is 17 digits. The leading pad digits are zero (0) if the AFI value specifies that the leading significant digit in the IDI is non-zero. If the leading significant digit of the IDI is zero, the pad digits are one (1) digit.

V.2.2 ISO DCC IDI format

The IDI consists of a three-digit numeric code allocated according to ISO 3166. The Data Country Code specifies the country in which the DSP of the NSAP address is registered. The semantics of the IDI is 3 digits and thus the length of the IDP is 5 digits.

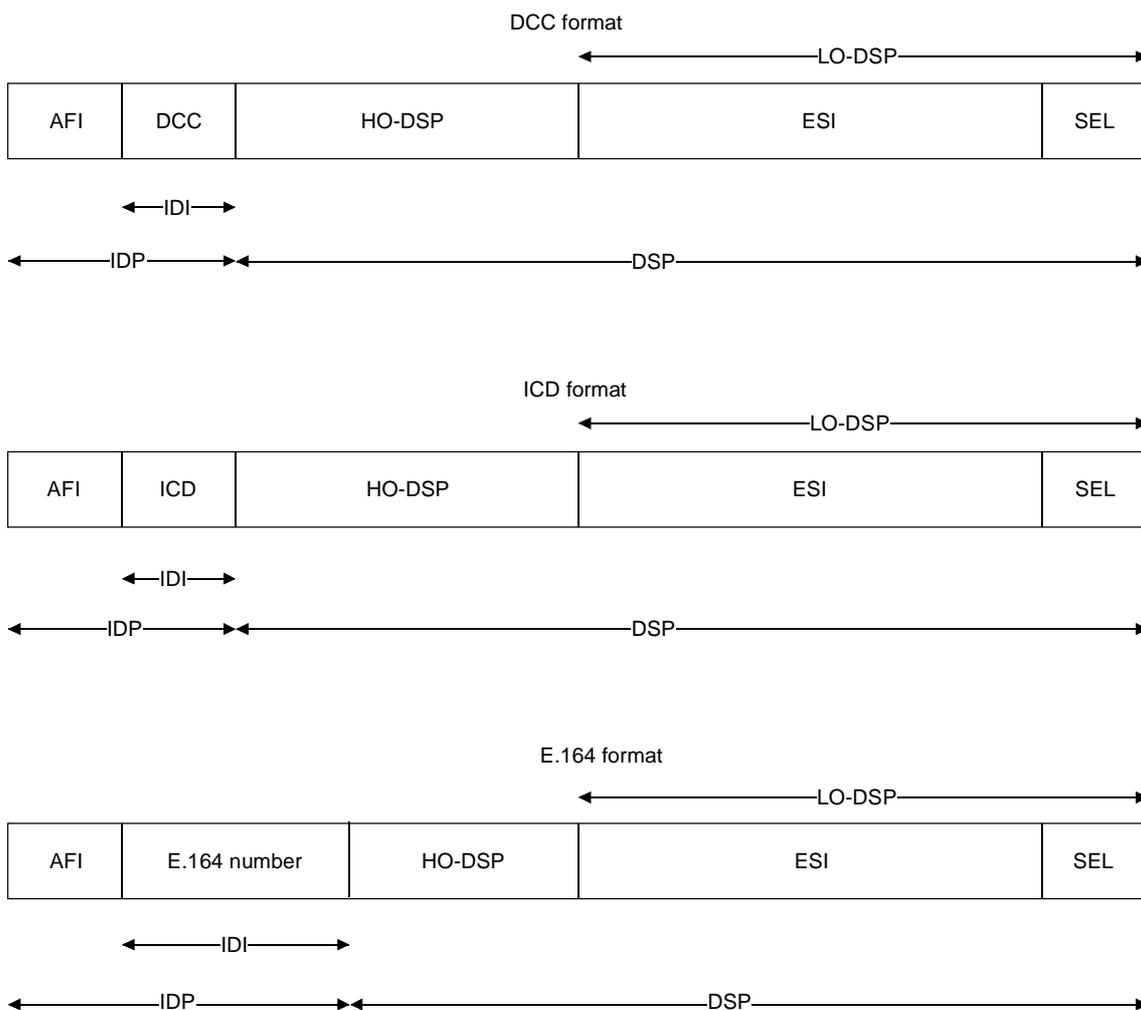
V.2.3 ISO 6523 ICD IDI format

The IDI consists of a four-digit International Code Designator allocated according to ISO 6523. The ICD identifies a particular organizational coding scheme which is responsible for allocating and assigning values of the DSP. The semantics of the IDI is 4 digits and thus the length of the IDP is 6 digits.

V.3 ATM address structures

Additional guidance on the structure of the Domain Specific Part of an NSAP address is given in ISO/IEC 10589:1992 – Intermediate system to intermediate system intra-domain-routing information exchange protocol.

A possible structure for the three formats (DCC, ICD and E.164) of the NSAP format addresses is shown in Figure V.2. The specific number of octets allocated to the fields within the DSP of a particular format is implementation dependent and is thus not shown.



T1308600-96/d28

Figure V.2/I.313 – ATM "NSAP format" address structures

The Domain Specific Part (DSP) may be subdivided into a High Order DSP (HO-DSP) and a Low Order part which may (optionally) consist of an End System Identifier (ESI) and a selector (SEL).

The coding of the HO-DSP is specified by the authority identified by the IDP. The authority determines how identifiers will be assigned and interpreted within the DSP. The authority can create further subdomains. That is, the authority may define a number of subfields within the HO-DSP and use these to identify a lower authority which may be responsible for defining the balance of the HO-DSP.

The ESI identifies an end system. This identifier must be unique within a particular value of IDP + HO-DSP. The selector (SEL) is not used for ATM routing but may be used by end systems. The length of this field is 1 octet.

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the 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	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 communication
Series Z	Programming languages