INTERNATIONAL TELECOMMUNICATION UNION

CCITT

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

M.3600

(10/92)

MAINTENANCE: ISDN

PRINCIPLES FOR THE MANAGEMENT OF ISDNs

Recommendation M.3600

FOREWORD

The CCITT (the International Telegraph and Telephone Consultative Committee) is a permanent organ of the International Telecommunication Union (ITU). CCITT 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 Plenary Assembly of CCITT which meets every four years, establishes the topics for study and approves Recommendations prepared by its Study Groups. The approval of Recommendations by the members of CCITT between Plenary Assemblies is covered by the procedure laid down in CCITT Resolution No. 2 (Melbourne, 1988).

Recommendation M.3600 was revised by Study Group IV and was approved under the Resolution No. 2 procedure on the 5th of October 1992.

CCITT NOTE

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

© ITU 1993

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.

Recommendation M.3600

PRINCIPLES FOR THE MANAGEMENT OF ISDNs

(Melbourne 1988 as Rec. M.36; revised and renumbered in 1992)

Abstract

This recommendation provides the management principles and architecture of the ISDN. Management functions and their relationships are defined in detail.

Keywords:

- ISDN management architecture;
- ISDN management principles;
- ISDN management;
- management service provider;
- OAM-centre;
- subscriber access;
- subscriber installation.

1 General

The purpose of this Recommendation is to provide management principles and architecture to be adopted by administrations, RPOAs and other Management Service Providers (MSP) in order to manage ISDNs.

1.1 *Scope of application*

In providing this guidance, due consideration has been given to the principles identified in the following Recommendations:

- Recommendation M.20 [1] defines the maintenance philosophy for telecommunications networks;
- Recommendation M.3010 [2] defines the principles for the telecommunications management network;
- Recommendation M.32 [3] defines the principles for using alarm information for maintenance of international transmission systems and equipment;
- Recommendation M.34 [4] defines the performance monitoring on international transmission systems and equipment;
- Recommendations Q.940 and Q.941 [6] describe the model, service elements and protocols to be provided at the ISDN user/network interfaces for management;
- Recommendation M.2100 [9] provides the maintenance limits for digital paths and sections to achieve the performance objectives given in Recommendation G.821 [10].

This Recommendation defines the ISDN management concepts with respect to areas of fault, performance and configuration management of subscriber installations, networks, including the transit network, and interworking between ISDNs, and other networks, including both existing and future public and private networks[1)].

---

1) Other aspects of management are for further study.

This Recommendation takes into consideration basic ISDN features such as:

– open communication via the S/T reference points;

– portability of terminals between S/T reference points, from subscriber installation to subscriber installation, and from ISDN-to-ISDN.

For information on ISDN channels, terminations and interfaces, see Recommendations I.411 and I.142 [8].

1.2 *Relation to other Recommendations*

This Recommendation is the overview Recommendation in a Series of Recommendations on ISDN management. The other Recommendations are the following:

a) Other M.3600-Series Recommendations describe reference configuration and general architecture for maintenance of ISDN subscriber access and subscriber installation as follows:

   – Recommendation M.3602 [11] is concerned with the maintenance of the ISDN subscriber installation. The maintenance principles are given in a general way for functions which are dependent on the design of NT2 and TE and more precisely where it impacts on the S or T interface (i.e. in relation to Recommendations I.430 and I.431 [8]). These functions are supervised and/or controlled by the subscriber installation.

   – Recommendation M.3603 [12] describes maintenance for the network portion of the ISDN basic rate access (144 kbit/s). A common format with other similar Recommendations, in conformance with Recommendation M.20 [1], is used. The functions performed by the digital transmission section and the exchange termination (ET) are identified. These functions are supervised and/or controlled by the network or administration.

   – Recommendation M.3604 [13] describes maintenance of the network portion of the ISDN primary rate access (2048 and 1544 kbit/s) following the same principles as given in Recommendation M.3603 [12]. The functions provided by the digital transmission section and the exchange termination (ET) are identified. The functions are supervised and/or controlled by the network or administration.

   – Recommendation M.3605 [14] describes the maintenance of a multiplexed basic rate system. Reference is made to Recommendations M.3603 [12] and M.3604 [13] when common mechanisms are applied. The functions performed by the digital section of the ISDN basic rate access, the basic access multiplexer, the digital link, and the exchange termination (ET) are identified. These functions are supervised and/or controlled by the network or administration.

b) Recommendation M.3620 [15] describes ISDN test calls originating from a test system and terminated by a test call responder. It also describes their application as part of end-to-end ISDN maintenance.

c) Recommendation M.3640 [16] describes management of layers 2 and 3 of the D-channel communications.

d) Recommendation M.3660 [17] describes ISDN interface management services and their use in maintaining ISDN.

   The ISDN management protocols which provide this activity are contained in Recommendation Q.941 [6] on ISDN user-network management protocols.

2 Definitions

2.1 *Reference definitions*

2.1.1 *Organizational component definitions*

2.1.1.1 **Subscriber Installation (SI)**

An SI is an organization located in the subscriber side, that contains people, TEs, NEs and, if needed, operations systems, which together have the responsibility for and capability of maintaining subscriber installation facilities.

2.1.1.2 **Local Exchange Centre (LEC)**

An LEC is an organization that is in charge of operating and maintaining local exchanges and subscriber accesses. It may contain people, local exchanges and local exchange operation systems, which together have the responsibility for and capability of maintaining local exchanges and ISDN subscriber accesses.

2.1.1.3 **Operation Administration Maintenance Centre (OAME)**

An OAMC is an organization that is in charge of operating and maintaining networks and services. It is located somewhere within the network and contains people and operations systems, which together have the responsibility for and capability of maintaining ISDNs.

2.1.1.4 **Management Service Provider (MSP)**

MSP is an organization which provides management services to subscribers. An MSP contains people and operation systems, which together have the responsibility for and capability of providing a limited management service for ISDNs.

- Agreement on responsibility for management between subscriber and the MSP for each part or parts of the subscriber installation should be made at the time of subscription (this may take the form of a commercial contract). In any case, provision to allow a customer to change the management service provider(s) is recommended. The subscriber may choose not to make such an agreement with an MSP.
- Management service providers can be:
  - private providers; or
  - the administration; or
  - the subscriber.
- It is the responsibility of a subscriber installation and not of the network to ensure that an unauthorized MSP cannot access management functions in the subscriber installation.

2.1.2 *System definitions*

2.1.2.1 **SI Operation System (SI-OS)**

SI-OS is a system that performs operation functions within SI and communicates with other OSs within other organizations in order to facilitate the management of subscriber access and ISDN services. This OS may be realized as part of the equipment located within the subscriber installation.

2.1.2.2 **Local Exchange Operation System (LE-OS)**

LE-OS is a system that is located in a local exchange centre and performs local exchange operation functions to maintain local exchanges and subscriber access. This OS may be realized as part of the local exchanges. This OS communicates with other OSs within other organizations in order to facilitate the management of subscriber access and ISDN services.

2.1.2.3 **OAMC Operation System (OAMC-OS)**

OAMC-OS is a system that is located in OAMC and performs network operation functions to maintain ISDN facilities and services. This OS communicates with other OSs in other organizations in order to facilitate the management of ISDN facilities and services.

2.1.2.4 **MSP Operation System (MSP-OS)**

MSP-OS is a system that is located in MSP and performs part of management functions in SI. This OS communicates with other OSs in other organizations in order to increase its management functions.

2.1.3 *Management function definitions*

2.1.3.1 **Subscriber Installation Management Function (SIMF)**

A SIMF represents a group of dedicated functions contained within the functional groups (as specified in Recommendation I.411 [8]) of the subscriber installation which may have one or more of the following purposes:

– interaction with the (human) user;

– handling of management protocol from the SAMF and /or an MSP-MF;

– control of internal testing and maintenance mechanism.

It is considered that the functions may be distributed throughout the protocol layers implemented in the subscriber equipment, SI-OS, and MSP-OSs, including NT1 functions in some applications, but the precise architecture and protocol of the SIMF implementation is not a subject of this Recommendation.

Examples of SIMFs are:

– control TE loopbacks;

– identification of TE service capability;

– control generation of test signals for maintenance of subscriber installation wiring;

– provide access to performance data within subscriber installation, e.g. layer two and three protocol performance;

– security screening of requests from MSP-MF.

2.1.3.2 **Subscriber Access Management Function (SAMF)**

A SAMF represents a group of functions for managing the subscriber access and communication with other management functions in other OS. The SAMF may be distributed throughout a local exchange OS and OAMC-OS but precise architecture of the SAMF implementation is not a subject of this Recommendation.

Examples of SAMFs are:

– control loopbacks in an NT1 or LT;

– supervise the service state of the subscriber access;

– provide access to subscriber access performance information.

2.1.3.3 **OAMC Management Function (OAMC-MF)**

An OAMC-MF represents a group of functions for managing the network including facilities and services. The OAMC-MF may be distributed to several OAMC-OSs but the precise architecture of the OAMC-MF implementation is not a subject of this Recommendation.

Examples of OAMC-MF functions are:

– request SAMF to control loopback activation;

– supervise the bringing into service of a subscriber access;

– obtain performance information on the subscriber access from the SAMF;

– manage teleservices provided to a subscriber;

– screen requests from MSPs for authorization.

2.1.3.4 **MSP Management Function (MSP-MF)**

An MSP-MF represents a group of functions for managing the subscriber installation or a part of the subscriber installation. An MSP-MF cannot control the management functions of the subscriber access. If authorized, it can request information from the OAMC-MF about the subscriber access.

Examples of MSP-MF functions are:

– Request SIMF maintenance activity;

– request OAMC-MF management information that is allowed;

– provide test responders function.

2.2 *Other definitions*

2.2.1 **Network**

A network is the public part of the ISDN which is managed under the responsibility of the administration or a RPOA.

2.2.2 **Operation, Administration and Maintenance (OAM)**

These three aspects form the base for the necessary management functions for ISDN.

2.2.3 **ISDN Interface Management Services**

These services are defined on the User Network Interface UNI and provide a customer with management capabilities.

3 Management principles for ISDN

3.1 *General maintenance principles for ISDN*

The fundamental maintenance strategy is to rely on performance monitoring wherever possible in order to apply the controlled maintenance principles of Recommendation M.20 [1].

The maintenance capabilities provided must allow for the clear differentiation of troubles between subscriber and network equipment.

The maintenance capabilities provided must allow for clear differentiation between failures and legitimate subscriber activities.

An MSP should be able to localize the fault in its domain without disturbing the network or other domains. This should be possible locally and remotely, i.e. across networks and between any allowed management entities.

Testing will be needed both to supplement the performance monitoring for trouble detection and to provide additional trouble localization ability.

The subscriber installation should be able to receive failure or performance information if sent from the network side. The network should be able to receive failure or performance information from the subscriber side.

A capability should be provided to control the status of the subscriber access and of the subscriber equipment during maintenance operations.

The subscriber installation (or its MSP) should be able to receive information about the maintenance status of its access, if sent from the network .

Only the Administration may initiate maintenance action within the subscriber access.

The subscriber installation (or its MSP, either private or administration) may initiate maintenance action within the subscriber installation.

In order to try and meet overall objectives, a number of points have been identified for administrations and MSPs:

- to detect fault conditions, identify the failed maintenance entity, take system protection actions, inform the maintenance staff of administrations;
- to incorporate the capability to enable the failure to be located by the maintenance staff, so that the failure correction is achieved by a single visit to the failure location;
- to provide an appropriate maintenance organization and levels of staffing, so as to achieve goals for out-of-service repair times;
- to incorporate the capability to differentiate between failures in the subscriber installation and failures in the network;
- to incorporate the capability to differentiate between failures and normal subscriber activities.

3.2 *Supervision of the subscriber access and end-to-end performance monitoring*

For maintenance purposes, each Maintenance Entity (ME) and Maintenance Entity Assembly (MEA) provides its own performance measuring according to Recommendation M.20 [1]. The generated anomaly and defect information allows detection and identification of an ME or MEA in a degraded or unacceptable state, and reporting that state to the associated management entity.

The network can only measure the performance of MEs and MEAs. The problem of how to combine the performance of the MEs and MEAs of the transit network with that of the subscriber accesses to determine the end-to-end performance as seen by the subscriber, is for further study.

3.3 *Management functions*

This section lists the functions which could be provided by a system to other systems according to the management function relationship. The list below is not exhaustive.

A system may provide the following management functions:

1) *Reporting mechanism control* – For reporting occurrences of events in its domain including alarm detection and creation, deletion and modification of management information. The control allows creation, deletion and modification of the reporting mechanism.

2) *Logging mechanism control* – For recording events in its domain including alarm detection, creation, deletion and modification of management information and performance parameters. The control allows creation, deletion and modification of the logging mechanism and retrieve and deletion of logged records.

3) *Protection mechanism control* – If supported, in order to swap faulty elements in its domain for stand-by (redundant) elements. The control allows retrieval of protection mechanism state information, modification of protection activation conditions and initiation of protection functions.

4) *B-channel state transition control* – For maintaining consistency of B-channel state in both ends. The control includes retrieval of state information and state change control.

5) *Internal test performer control* – In order to initiate and perform test functions. The control includes modification of test conditions, initiation and termination of tests and test result retrieval and deletion.

6) *Loopback mechanism control* – Located in the subscriber installation for the purpose of fault localizing testing. The control includes loop-back, loop-down and loop status retrieval.

7) *Terminal profile information control* – Of ISDN terminals in the subscriber installation. The control includes retrieval and modification of information.

8) *Subscriber installation configuration information control* – Which consists of terminal location, connections, and cabling data.

9) *End-to-end traffic information control* – Obtained by ISDN terminals.

10) *Service profile information control* – Of ISDN terminals which are maintained by the system. The control includes retrieval and modification of information.

11) *Subscriber access configuration information control* – Which consists of equipment locations, connections, and cabling data.

12) *Local traffic information control* – Within the subscriber access.

13) *Local path tracing information control* – Regarding connections within the subscriber access which consists of component elements' management information.

14) *Network configuration information control* – Maintained by the system, which consists of equipment locations, connections, etc.

15) *Overall traffic information control* – Within the transit network.

16) *Overall path tracing information control* – Regarding connections within the network which consists of a component elements' management information.

17) *Trouble ticketing information control* – Which contains status of fault localization activity and history. The control includes creation, deletion, modification and retrieval of trouble ticketing information.

18) *Fault statistics information control* – Including alarm and performance statistics.

19) *Subscriber information control* – For other systems.

20) *Contract information control* – For other systems.

21) *Other useful information control* – For the other systems.

Table 1/M.3600 indicates possible management functions allocations to each ISDN management functions defined in § 3.3.

3.4 *Management strategies*

Management of ISDN is based upon the principles of OSI management and TMN. The management strategy chosen affects the information model used. Changing management strategy may therefore require changing the information model.

For example all kinds of performance information concerning the layers 2 and 3 of the D-channel may be forwarded to a network element management system. When the number of D-channels within a single ISDN local exchange becomes large, it is convenient to use a log object (see Recommendation X.735 [5] on Log Control Function) in the managed system's information model to hold the performance information for a certain period of time. Restrictions on the capacity of an exchange limits the set of performance information which can be held.

TABLE 1/M.3600

Management functions allocation to SIMF, SAMF, OAMC-MF and MSP-MF

Management functions	SIMF	SAMF	OAMC-MF	MSP-MF
Reporting mechanism control	X	X	X	X
Logging mechanism control	X	X	X	X
Protection mechanism control	X	X		
B-channel state transition control	X	X		
Internal test performer control	X	X	X	X
Loopback mechanism control	X	X		
Terminal profile information control	X			X
Subscriber installation configuration information				X
End-to-end traffic information	X			
Service profile information control		X	X	
Subscriber access configuration information		X		
Local traffic information		X		
Local path tracing information		X		
Fault statistics		X		
Network configuration information			X	X
Subscriber information			X	
Overall traffic information		X	X	
Overall path tracing information			X	
Trouble ticketing information control			X	X
Contract information				X

3.5 *Security provision*

To facilitate maintenance and management activities on ISDN, operation systems responsible for different management domains may need to communicate. However, since management and maintenance information is of critical importance to system integrity, access to management functions and information is subject to prior authorization and security restrictions.

The security restrictions are enforced by the recipient of the maintenance request and may include requirements for user authentication, the use of passwords and/or limited access based on the originating call.

The use of adequate security mechanism is especially important in the case of the OAMC since maintenance function for many users may be affected by unauthorized access.

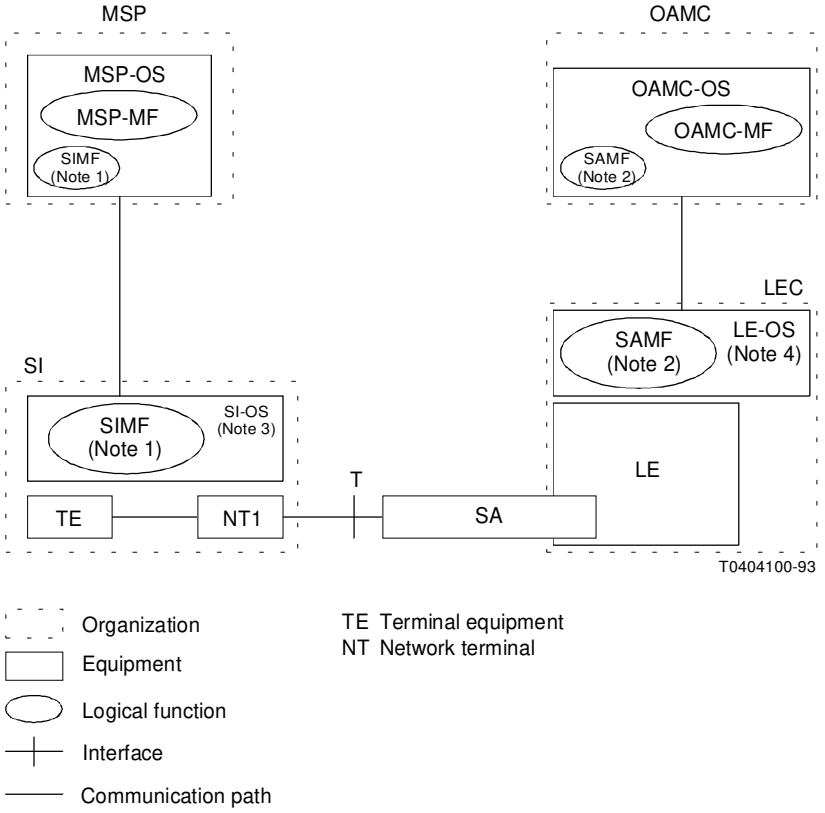
4 Management reference models

4.1 *Reference management configurations*

Shown in Figure 1/M.3600 is the reference management configuration, which gives the relationship between subscriber installation and subscriber access to be maintained and the various maintenance organizations, operation systems, management functions and ISDN.

The lines between physical devices containing each functional entity represent physical communications paths over which the management information may flow.

In this reference configuration, subscriber access is maintained by an OAMC-OS. Local or remote user or MSP-OSs may communicate with the OAMC-OS to request certain maintenance functions under its control. The SAMF provides the communication functions for network local management functions and contains the control functions for such local activities. The SAMF may either be entirely part of a local exchange including LE-OS or may be distributed between the LE/LE-OS and OAMC-OS.



Note 1 – SIMF can reside in MSP-OS and SI-OS or in SI-OS.

Note 2 – SAMF can reside in LE-OS and OAMC-OS or in LE-OS.

Note 3 – SI-OS may be entirely part of TE and NT1.

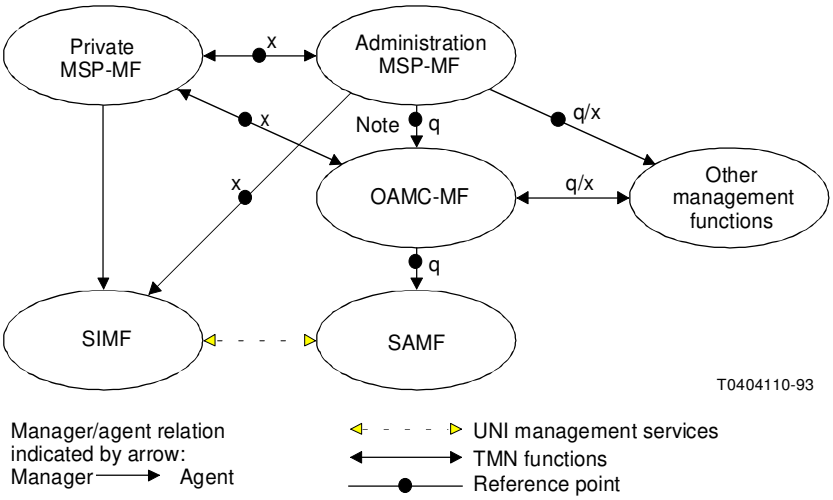
Note 4 – LE-OS may be entirely part of LE.

FIGURE 1/M.3600

Reference configuration for ISDN management

Management functions relevant to ISDN management and maintenance are SIMF, SAMF, OAMC-MF and MSP-MF. Figure 2/M.3600 depicts Manager/Agent relationship of ISDN management functions.

A relationship does not imply any lower layer communication functions between systems. A unidirectional arrow indicates that a manager/agent role can change based on applications. For example, an SIMF always takes the agent's role for management functions except when controlling an SAMF. Figure 2/M.3600 also indicates the type of management services or functions used in each relationship. When an SIMF controls management services offered to a customer controlled by an SAMF, UNI management services may be applied. In other cases TMN functions may be used.



Note – Functionality provided by OAMC-MF to a private MSP-MF and an administration MSP-MF shall be the same except security aspects.

FIGURE 2/M.3600

Manager/Agent relationship of ISDN management function

4.2 *End-to-end models*

This section provides two examples of end-to-end ISDN connections. Figure 3/M.3600 shows connection examples where a call from one subscriber access (primary or basic rate) is switched through the public network to another subscriber access.

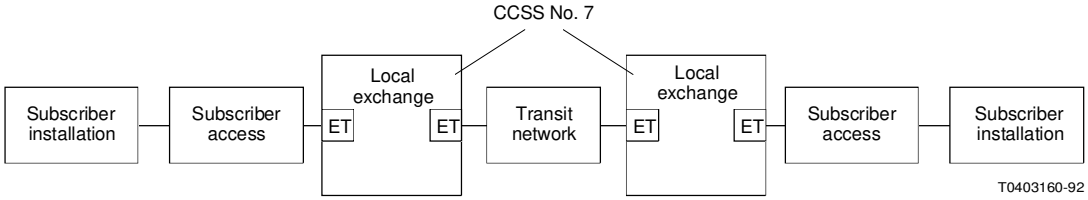


FIGURE 3/M.3600

End-to-end public switched ISDN connection

Figure 4/M.3600 shows an end-to-end leased circuit arrangement example where at each end a subscriber primary rate access is connected to a Digital Cross-connect System (DCS). From the DCSs, B-channels may be connected to the switches or may be used to provide an end-to-end connection between the subscriber locations.

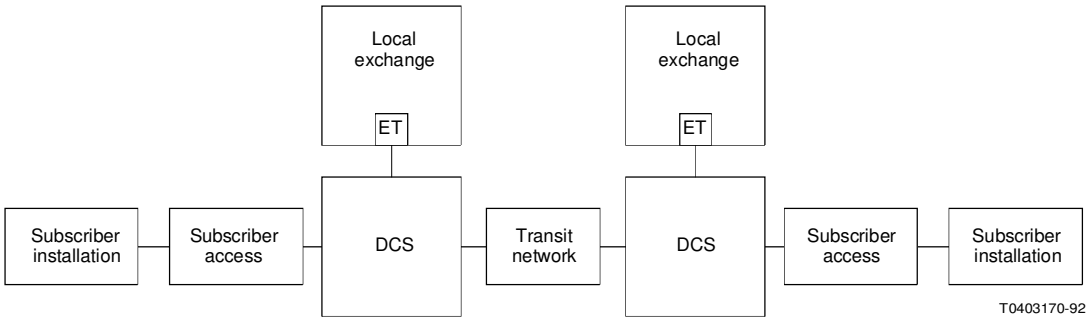


FIGURE 4/M.3600

End-to-end leased circuit connection

A variation on this example would have a second primary rate access, without a D-channel, connected end-to-end via a DCS. In this case there is a possibility of a hidden fault between the DCSs that is not reported to either end and is not detected via the loss of the D-channel. Thus, this is a configuration where a continuity check is required to detect the fault.

4.3 *ISDN interworking model*

Primary or basic rate subscribers via their ISDN access may wish to interwork with other networks, such as the Public Switched Telephone Network (PSTN), a Packet Switched Data Network (PSDN) or with another public or private ISDN. A model for this interworking is shown in Figure 5/M.3600.

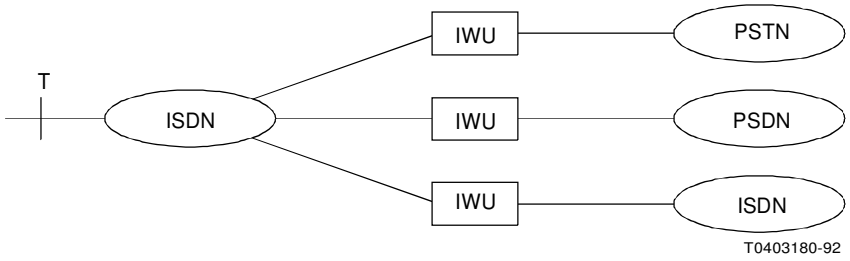


FIGURE 5/M.3600

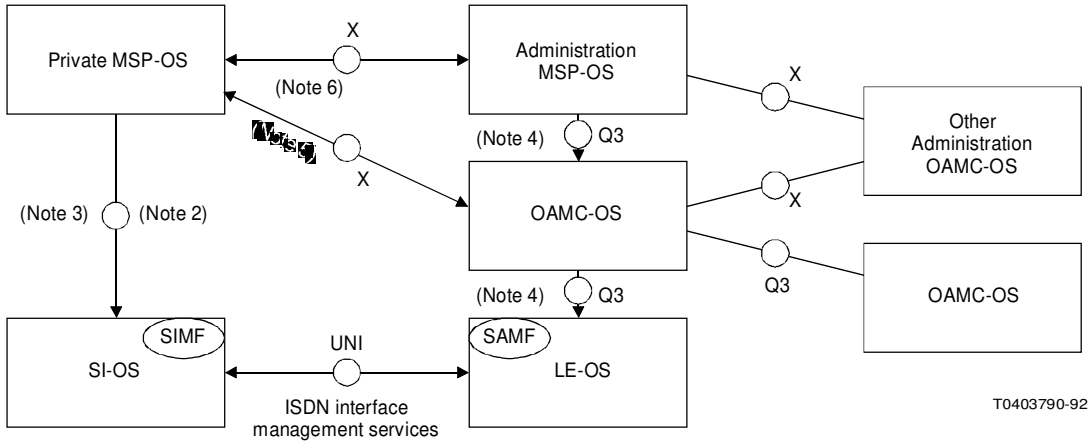
ISDN interworking model

An example of the Interworking Unit (IWU) would be a modem pool used in the PSTN case.

Maintenance of interworking is for further study.

4.4 *ISDN management related systems and relationship*

Figure 6/M.3600 depicts ISDN management related systems and their relationship.



Note 1 – Q3 and X are TMN interfaces, described in Recommendation M.3010 [2].

Note 2 – Not subject to standardization, this interface can be Q3 or proprietary; the Data Communication Network (DCN) may be ISDN.

Note 3 – Remote management; remote invocation of Interface Management Service (IMS) is part of remote management.

Note 4 – Remote management in which TMN principle are implied; remote invocation of IMS is part of remote mnagement.

Note 5 – Functionality provided by OAMC-OS to a private MSP-OS and an administration MSP-OS shall be the same except security aspects.

Note 6 – Supplementary definitions may be required.

FIGURE 6/M.3600

ISDN interface management and relation to TMN

4.4.1 *Remote management*

Remote management refers to the management operations in which communication of management information is required between two systems (e.g. between the private MSP-OS and SI-OS). One example is requesting the status of the performance of layer 2 protocol with entities within the SI.

Remote management includes the invocation of ISDN interface management services, e.g. a private MSP-OS requesting the SI-OS to invoke the Service Profile Verification (SPV) service on the UNI.

4.4.2 *TMN interfaces*

The TMN is intended to provide an Administration an independent communications network to carry its management (operations, administration and maintenance) messages to and from its operations systems (OSs) to the telecommunications network it manages, including ISDN and associated network elements.

In Figure 6/M.3600, the TMN would carry management messages between the OAMC-OS (including an administration MSP-MF, if provided) and the ISDN over a Q type TMN interface (see Recommendation M.3010 [2] for a description of the TMN interfaces). The TMN would also provide the communications for an administration's externally provided MSP-OS using the TMN PQ-DCN protocol suite (as defined in Recommendation M.3010 [2]) over a T type physical ISDN interface. A private MSP-OS may be connected directly to the ISDN via a T type interface. It may also be connected to the TMN by interworking via other network interworking interfaces that are under study. While supporting the ISDN, the TMN is also supporting other management functions for the administration, including the maintenance of transmission system equipment.

An interface defined between OSs has management information aspects and protocol aspects. Regarding interfaces between MSP-OS and OAMC-OS, functionalities provided by OAMC-OS to both private and administration MSP-OSs shall be the same except security aspects.

4.5 *ISDN management information model*

The scope of management information covers several broad areas:

– physical equipment;

– circuit switched connections;

– protocol and softwares;

– ISDN services;

– and maintenance operations.

These areas serve as the basis for the focus of ISDN management activities. This overview information is shown in Figure 7/M.3600.

Figure 7/M.3600 shows five different aspects of an ISDN:

1) physical configuration;

2) communications;

3) protocol layers;

4) loopbacks; and

5) management domains and ownership.

The physical configuration of an ISDN is illustrated using the following physical entities:

– TEs;

– NT2s;

– NT1s;

– LTs;

– ETs; and

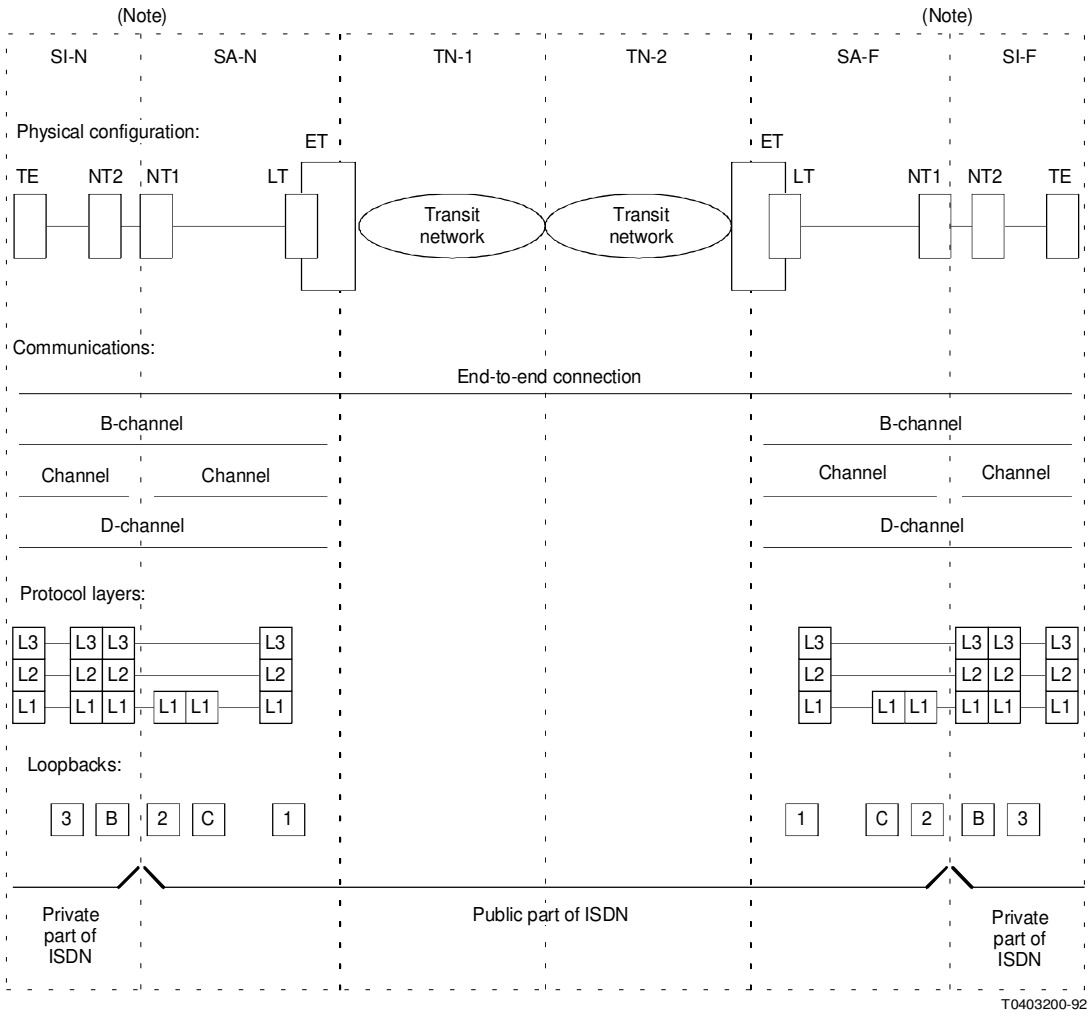
– transit networks.

The communications function of an ISDN is illustrated by an end-to-end connection between TEs. This uses B-channels in the subscriber access signalled for by Digital Signalling System No. 1 on the D-channel.

Also shown are the several layers of the DSS1 protocol and where these layers terminate, information of concern for maintenance of the protocol implementations.

Loopbacks are shown with the naming used in the M.3600-Series Recommendations.

Management domains are divided into subscriber installations, or the private part of ISDNs, and subscriber access and transit networks, or the public part of ISDNs.



SI-N Near end subscriber installation
SA-N Near end subscriber access
TN-1 Transit network 1
TN-2 Transit network 2
SA-F Far end subscriber access
SI-F Far end subscriber installation

Note – In some Administrations or RPOAs, NT1 belongs to the subscriber installation.

FIGURE 7/M.3600

Entities considered within ISDN management

The overview information, management functions, and requirements for management services presented in the M.3600-Series Recommendations will be used to derive managed object class definitions. Instances of those managed object classes represent resources to be managed on management interfaces, i.e. the ISDN UNI or TMN interfaces. The definition of those managed object classes is out of the scope of this Recommendation.

5 Management of public part of ISDN

5.1 *TMN for public part of ISDN*

This section presents a reference configuration for management of the network, the public part of the ISDN. The operation, administration and maintenance functions (OAMC-MF) are described.

Management of the ISDN shall be structured in accordance with the Principles for a Telecommunication Management Network which are defined in Recommendation M.3010. The public part of the ISDN consists of the local exchanges and the transit networks between them. Public networks can be interconnected to enable communication to users on other public networks. In Figure 8/M.3600, the OAMC-OS management function consists of several management functions:

- service management functions;
- network management functions; and
- network element management functions.

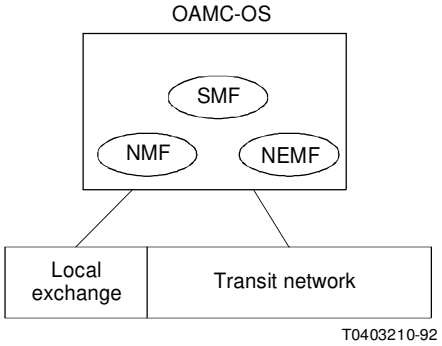


FIGURE 8/M.3600

Management of ISDN public network

The service management functions manage the public network in terms of the services provided over the network. The service management functions may communicate with the network management functions for this purpose.

The network management functions manage the local exchanges and the transit network[2]. Combined together these enable public network wide network management.

The network element management functions manage the local exchanges and the network elements of the transit network.

The local exchange provides the user access as can be seen in Figure 9/M.3600. The OAMC-OS sends operations to the local exchange or LE-OS. The local exchange including LE-OS sends notifications to the OAMC-OS upon the occurrence of events. The operations and notifications which can be exchanged are determined by the managed objects in the local exchange which are visible to the OAMC-OS. The managed objects are an abstraction of the physical and functional resources that constitute the local exchange.

---

2) The transit network might incorporate a separate signalling network (e.g. CCSS No. 7).

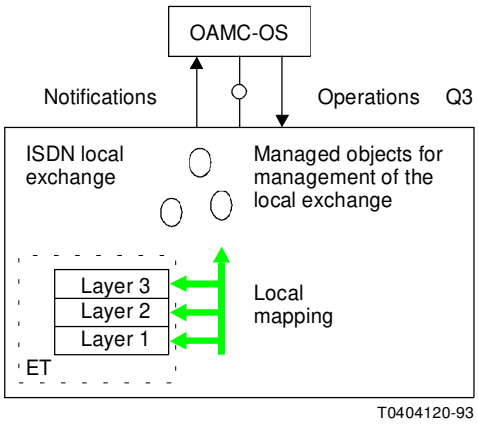


FIGURE 9/M.3600

Example of TMN for management of ISDN

5.2 *Management scenarios*

For further study.

6 Management of the private part of ISDN

6.1 *TMN for private part of ISDN*

Management of customer equipment may be performed via a private interface or TMN Q interface from a private MSP-OS or an administration MSP-OS as shown in Figure 10/M.3600.

6.2 *Management scenarios*

For further study.

7 End-to-end ISDN management

7.1 *Cooperation with other TMNs*

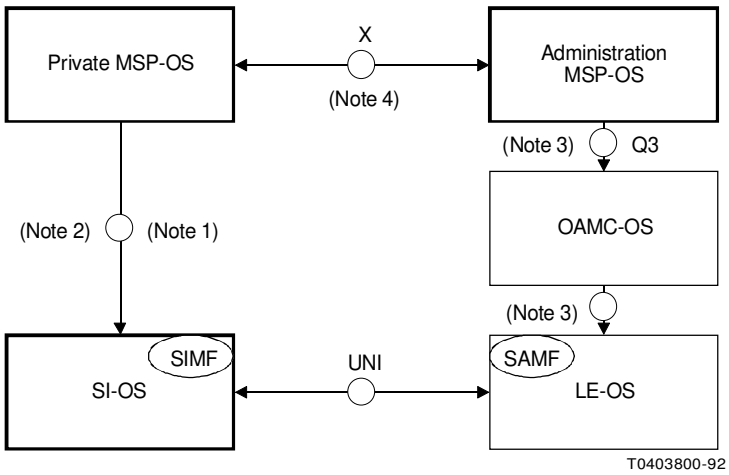
ISDN in general is a unique network which provides an integrated network. Although this ideally may be true, in the near term, interworking may be needed with dedicated networks like the public switched data networks.

Cooperation of management functions between management of foreign ISDNs; and CCSS No. 7-networks is required in order to apply the management (maintenance) principles.

Recommendations for cooperating management functions between management of ISDN; and

– management of CCSS No. 7[3];
– management of PSPDN;
– management of another ISDN
– management service provider,

are for further study.



Note 1 – Not subject to standardization, this interface can be Q3 or proprietary; the DCN may be ISDN.

Note 2 – Remote management; remote invocation of IMS is part of remote management.

Note 3 – Remote management in which TMN principles, are implied; remote invocation of IMS is part of remote management.

Note 4 – Supplementary definitions may be required.

FIGURE 10/M.3600

Management of the private part of ISDN

7.2 *Management scenarios*

For further study.

---

[3] In Recommendations Q.750 and Q.751 [7] a number of management functions are described which are related to management of an ISDN. To enable Administrations to localize faults in either the ISDN or the CCSS No. 7, network cooperation is required. Also for performance monitoring correlation of information from both networks would be necessary.

8 ISDN interface management services

8.1 *Potential capabilities*

Considering that:

- multiple ISDN terminals may be connected to a single interface;
- there exists only limited capability for the Network Element (NE) MSP to maintain and administer terminals in an ISDN environment over the physical layer;
- ISDN protocols allow the implementation of value added management services,

a set of services is required for the purposes of maintaining and administering ISDN terminal equipment (TEs, and TAs and NT2s). These services are called ISDN Interface Management Services (IMS).

ISDN Interface Management Services are defined as services for which the communication of management information take place across one ISDN interface between two peer protocol entities. The following are potential ISDN interface management services. The list is not exhaustive.

- service profile verification-basic;
- local loopback management;
- service profile management-basic,
- service profile verification-primary;
- service profile management-primary; and
- state change management.

Stage 1 descriptions of interface management are provided in Recommendation M.3660 [17].

8.2 *Use of IMSs*

For further study.

ANNEX A

(to Recommendation M.3600)

Management functions in TMN and ISDN

A.1 *Network element*

Management of ISDN can gradually be derived from management of a PSTN.

The network element functions for the ISDN represent the management capabilities within the ISDN-exchange and transmission equipment. One of the characteristic features in this function group will be management of: supplementary services, physical equipment and associated protocols, measurements, etc.

A.2 *Network element management*

The network element management functions enable management of network elements individually. Each network element can be characterized by certain properties, like being of the same supplier or performing the same telecommunication functions. Management functions which use individual network element information belong to the network element management functions.

If network element management functions are implemented in real systems, the following properties are distinguished:

1) *Supplier* – Systems of the same supplier are the responsibility of one network element management system.

2) *Location* – For example, maintenance purposes network elements in the same location are couple with the same network element management system.

3) *Data* – Certain specific data from different network elements are centralized within one system. This does not mean that data can be combined or correlated.

The network element management functions manage each network element individually.

A.3 *Network management*

Each network management function only presents management information concerning individual network elements. The network management functions perform end-to-end management, including end-to-end performance measurements.

Only those management functions requiring an overview of the network are present in the network management functions.

A.4 *Service management*

The service management functions manage services, like bearer services or supplementary services. They also handle customer requests.

References

[1] CCITT Recommendation M.20 *Maintenance philosophy for telecommunications network*.

[2] CCITT Recommendation M.3010 *Principles for a telecommunications management network*.

[3] CCITT Recommendation M.32 *Principles for using alarm information for maintenance of international transmission systems and equipment*.

[4] CCITT Recommendation M.34 *Performance monitoring on international transmission systems and equipment*.

[5] CCITT Recommendation X.700-Series *OSI systems management Recommendations*.

[6] CCITT Recommendations Q.940 and Q.941 *ISDN user/network interface protocol for management general aspects and protocol profile*.

[7] CCITT Recommendations Q.750 and Q.751 *Overview of CCSS No. 7 management and managed object definitions*.

[8] CCITT Recommendations I.400-Series *ISDN user/network interface Recommendations*.

[9] CCITT Recommendation M.2100 *Performance limits for bringing-into-service and maintenance of international digital paths, sections and transmission systems*.

[10] CCITT Recommendation G.821 *Error performance of an international digital connection forming part of an integrated services digital network*.

[11] CCITT Recommendation M.3602 *Application of maintenance principles to ISDN subscriber installations*.

[12] CCITT Recommendation M.3603 *Application of maintenance principles to ISDN basic rate accesses*.

[13] CCITT Recommendation M.3604 *Application of maintenance principles to ISDN primary rate accesses*.

[14] CCITT Recommendation M.3605 *Application of maintenance principles to static multiplexed ISDN basic accesses*.

[15] CCITT Recommendation M.3620 *Principles for the use of ISDN test calls, systems and responders*.

[16] CCITT Recommendation M.3640 *Management of D-channel, data link and network layer*.

[17] CCITT Recommendation M.3660 *ISDN interface management services*.