

SECTION 2

USER-NETWORK MANAGEMENT

Recommendation Q.940

ISDN USER-NETWORK INTERFACE PROTOCOL
FOR MANAGEMENT – GENERAL ASPECTS

1 General

This Recommendation is one of a proposed series of Recommendations describing the management model, service elements and protocol to be provided at the ISDN user-network interface. These Recommendations also specify the management functions required to support the ISDN subscriber installation. This Recommendation describes the Management Architecture and provides a general overview of the management services and functions.

Other Recommendations in this series will specify the System Management Service Elements and Protocol and the procedures associated with management functions.

The management functions provided at the user-network interface have, as an objective, full alignment with the network management functions being addressed by the Telecommunications Management Network (TMN) and the Management Framework for Open System Interconnection (OSI). While the TMN defines management functions from a network perspective, this Recommendation describes the management functions from the subscriber perspective and provides for remote user management functions.

1.1 Scope

This series of Recommendations will provide for a common approach for management communications to support procedures used by a remote maintenance centre, internal or external to the network and those initiated locally.

These Recommendations deal with the specification of the following items:

- a) the specification of a Management Architecture and identification of communications paths;
- b) the specification of management functionality to be provided at the ISDN user-network interface;
- c) the specification of an information exchange protocol for the exchange of management information between two peer system management application entities (SMAE);
- d) the specification of primitives between the Management Application process (user) and the SMAE (i.e., the primitives at the systems management service interface (SMSI));
- e) the specification of service primitives between the SMAE service element and the next lower layer service elements (i.e., primitives at the presentation layer service access point (PSAP));
- f) the specification of a convergence function that may be required to permit the direct access of the SMAE service elements to services provided by layer 3 (i.e., the primitives at the network layer service access point (NSAP)).

1.2 Field of application

The protocols and procedures described in these Recommendations provide the means to support management functions at the ISDN user-network interface. Management activities that manage network services, operations such as network resource configuration, routing information and maintenance activities shall be

supported by the functions and protocols defined in these Recommendations. In particular these management functions should be able to support specific requirements such as those defined in the I.60-Series of Recommendations (Subscriber Access and Installation Maintenance). These protocols make it possible to control loopbacks and diagnostic tests, initiate and terminate event reporting and to exchange management information across the ISDN user-network interface, i.e., between equipment connected to the S/T reference points.

The physical layer signals in the digital transmission section which are used to control maintenance functions are outside the scope of this Recommendation.

The protocols can be used on the D Channel of both the basic and primary rate interface structures and across both reference points S and T. The higher layer protocols can also be used on other ISDN channels and services.

The protocols and procedures described in these Recommendations take into account that interactions with the TMN will occur. It is, therefore, desirable that the services and protocols to be used to support access management are aligned, wherever possible, with those to be defined for the TMN and OSI management.

2 Categories of management information exchange

Management information exchanges may be categorized into the following three categories:

- a) Event notification: information transfer initiated by one system reporting instantaneously the occurrence of an event (e.g., a fault occurrence) to another system.
- b) Data transfer: information exchange initiated by one system in order to get management-related information from another system. These exchanges follow the "request followed by response" paradigm.
- c) Control information: information exchanges which are of an executive nature, where one system requests that an action be performed by another system (e.g., for test access and downloading of parameters).

3 Management functions

Management functions may be classified in accordance with fields of application. The following major functions have been identified:

- a) Fault management
 - Maintenance functions
 - Fault tracing
 - Spontaneous error reporting
 - Error threshold alarm reporting
 - Continuous monitoring
 - Diagnostic testing
 - Resource (re)initialization
 - Confidence testing
 - Resource identification
 - Trouble isolation.
- b) Configuration management
 - Routing changes
 - Data base changes
 - Equipment identification
 - Network/equipment reconfiguration.
- c) Accounting management
 - Reporting of billing data.
- d) Performance management
 - Collecting and reporting of traffic data
 - Performance monitoring
 - Applying controls.
- e) Security management.

4 Management reference models

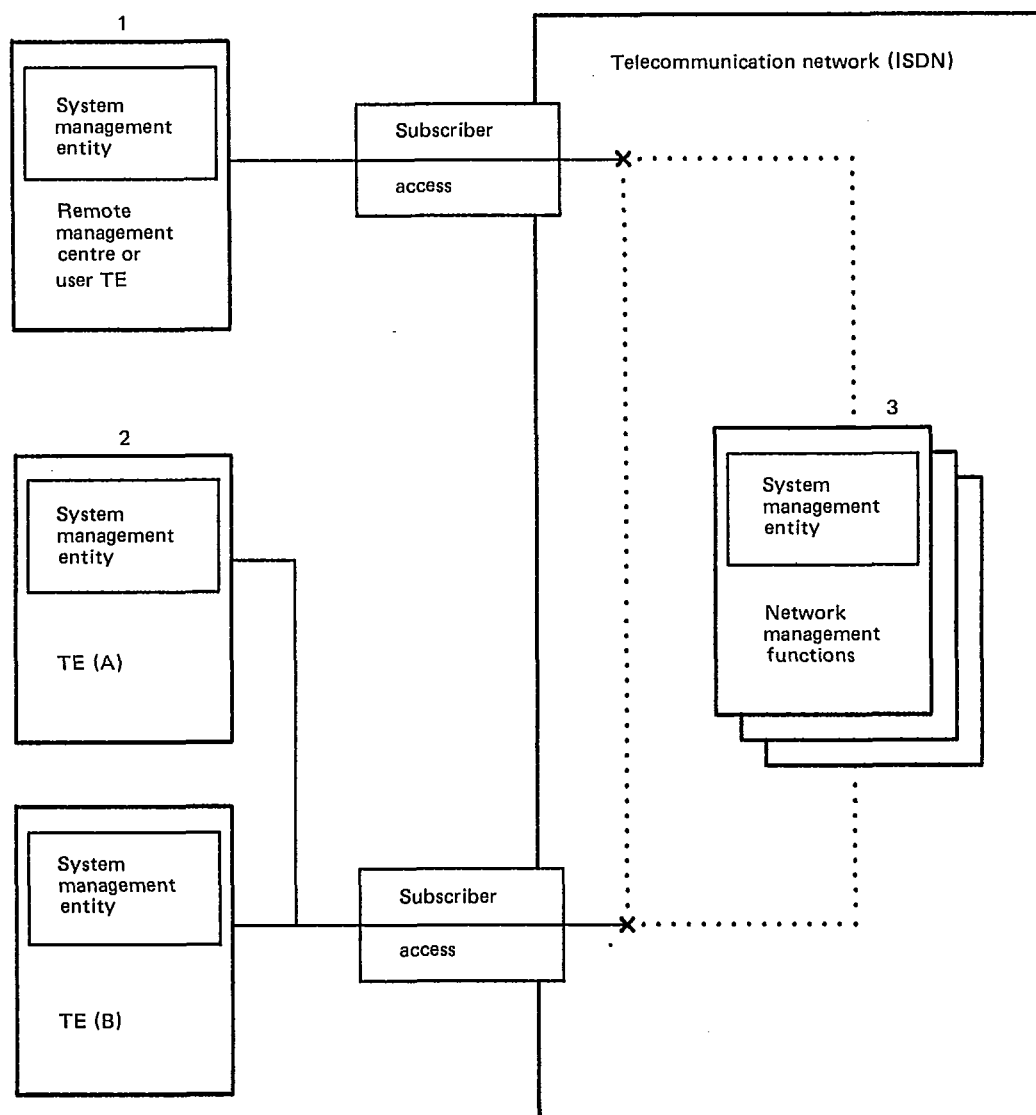
4.1 Communications path model

Figure 1/Q.940 shows the entities which may contain System Management Entities (SME) which may require capability to communicate. System Management Entities may be located in the local exchanges, subscriber installations, remote management centres or network management centres.

The management functions supported by the various systems may differ depending on system requirements and may vary between different networks. However, the communications facilities provided by the systems management entities should be as common as possible.

The scope of this Recommendation covers those functions and protocols that have immediate impact on the user-network interface.

The system management entities may be in a TE, NT2 or management service provider. Although communication between any two management entities may be possible in the model, it does not imply that information held at a particular management entity is available to all other management entities. Security mechanisms may be used to restrict access to the information.



T1115740-88

..... Optional communication paths in the network

FIGURE 1/Q.940
Management communication model

Figure 1/Q.940 shows that three types of management communications can be accommodated:

- a) TE (or Remote Management Centre) $\longleftrightarrow$ TE (1 $\longleftrightarrow$ 2);
- b) TE $\longleftrightarrow$ Network Management Function (1 $\longleftrightarrow$ 3);
- c) TE $\longleftrightarrow$ Network Management Function $\longleftrightarrow$ TE (1 $\longleftrightarrow$ 3 $\longleftrightarrow$ 2);

Types a) and b) are direct peer communication. In type c), the TE requests the Network Management Entity to act as an agent which then, on behalf of the requesting TE, communicates with another TE.

4.1.1 *Secure access to management and maintenance functions*

To facilitate maintenance procedures and fault sectionalization, maintenance entities located in different management domains may 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 upon access.

The security restrictions are normally enforced by the recipient of the management information but may be enforced by the originator independently of any security imposed by the recipient. The security measures may include requirements for peer-entity authentication.

The use of adequate security mechanisms is especially important in the case of a network since many users may be affected by unauthorized access.

Whenever system management communication crosses an S or T reference point, the requirement for access authorization must be presumed.

Note – This does not preclude implicit actions on layer management parameters as specified within the relevant signalling protocols, e.g., Recommendations Q.921 and Q.931. These actions are, however, beyond the scope of this Recommendation.

4.2 *System management entity*

Figure 2/Q.940 shows the internal structure of the SME.

4.2.1 *System management application entity (SMAE)*

The SMAE is an application layer entity that supports system management functions. The SMAE is responsible for communication with peer systems.

The function of the SMAE is to provide the communications necessary to make a system management accessible to another SMAP. It is not necessary for the SMAE to be provided if only local system management is required.

4.2.2 *system management application process (SMAP)*

An SMAP is an application process of a system performing management functions. The SMAP controls the SMAE, and includes the Management Information Base (MIB) and may include one or more managers providing various functionalities.

4.2.3 *management information base (MIB)*

The MIB is the repository of all information relevant to the operation of a system. Both the SMAP and Layer Management Entities (LME) have access to the MIB.

4.2.4 *layer management entity (LME)*

The LME is that part of a Layer Entity which manages resources and parameters residing in its layer protocol entity.

4.2.5 *protocol entity (PE)*

The PE is that part of a layer entity which is dedicated to peer-to-peer communications. A layer PE provides services to the next upper layer and uses services of the next lower layer.