SECTION 3 - USER-NETWORK MANAGEMENT

Contents of Recommendation Q.940

SECTION 3 - USER-NETWORK MANAGEMENT

Draft 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:

- 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.
- Configuration management

    - Routing changes
    - Data base changes
    - Equipment identification
    - Network/equipment reconfiguration.

- Accounting management

    - Reporting of billing data.

- Performance management

    - Collecting and reporting of traffic data
    - Performance monitoring
    - Applying controls.

- 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.

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

a) TE (or Remote Management Centre) <-> TE (1 <-> 2);

b) TE <-> Network Management Function (1 <-> 3);

c) TE <-> Network Management Function <-> TE (1 <-> 3 <-> 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.

It should be noted that this model presently permits communication between peer management processes either by attaching to a Presentation Layer Access Point (PSAP) or by attaching directly to the Network Layer Service Access Point (NSAP). A convergence function may be provided as an alternative to the full seven layer OSI Reference Model (as specified in Recommendation X.200) to accommodate simple terminals that may be used in the ISDN environment. If provided, the functions will be kept to a minimum, i.e., the OSI layer services lost by elimination of layers 4-6 will not be recovered by the convergence function. Therefore, the use of all seven layers is to be preferred. This has the consequence that "convergence functions" may need to be specified.

4.2.6 Management Information Protocol (MIP)

The Management Information Protocol provides the support for information exchange between peer SMAEs.

4.3 Managed objects: a hierarchical object model

4.3.1 Definitions

4.3.1.1 Managed object

A managed object is a collection of data objects and telecommunications or information processing resources that may be managed by means of the management protocol specified in this Recommendation.

4.3.1.2 A data object is an object that is the direct recipient of an action or generator of an event report.

4.3.2 The hierarchical object model

The maintenance functions are described as asymmetric functions using symmetrical communications paths. A maintenance activity is always started by an Invoker who is asking an Executor to manipulate event reports or data objects. These can be classified as belonging to individual managed objects. Each elementary operation that will have to access or refer to data objects will identify these by specifying first the managed object to which they belong and then identifying them within the managed object.

A hierarchical object model is defined that allows access to any individual data object in a simple way. When a given managed object may be duplicated, an instance identifier will help to resolve the ambiguity.

As an example, the model for user-network ISDN access interface is represented by the hierarchical tree of Figure 3/Q.940.

FIGURE 3/Q.940

Example hierarchical object tree

The parameters and event reports pertaining to a particular managed object can then be defined implicitly within the managed object. Some managed objects may be empty when no data object is identified within them. In this case they are only present as an indication of a hierarchical level.

It has to be noted that the ISDN user-network access interface model only contains managed objects that belong to the network access functions, i.e., that are involved in the provision of the required bearer service (signalling and lower layer protocols on the bearer channels). The protocols that are not involved in the provision of the bearer service are excluded from this model as they belong to the application part.

Note - The identity of an object at the executing end may not be known to the Invoker when it requests a maintenance action at the remote end of a connection. In this case the Executor will be able to identify the object by the context of the connection path used to convey the maintenance request.

As an example, remote maintenance may be required on an existing B Channel connection. The channel identity is only locally significant at each end. The maintenance request must be transmitted over the signalling connection that is used to control the B Channel associated with the existing call. The identity of the B Channel will be implied by the signalling connection used to convey the maintenance request.

5. Management structure and activities

This section considers the specific structure and activities of management in terms of system management, layer management and protocol processing for management purposes.

5.1 System management

This section introduces the concept of system management, its boundaries and other structures and activities related to management.

5.1.1 Introduction

The scope of system management is described in terms of the bounds of the SMAP. The boundaries show where the SMAP ends and other objects (either inside or outside the system) begin. The boundaries provide a sense of the relationship of the SMAP to other objects and therefore a sense of the SMAP scope.

5.1.2 System management boundaries

The boundaries of the SMAP are shown in Figure 4/Q.940.

FIGURE 4/Q.940

SMAP Boundaries

This figure shows the relationship between the SMAP and two other major components. The Communications component contains the seven layers of the reference model. The people and software component contains the people/software in the local environment that use the local systems manager.

The SMAE is the system management application entity, and (N)-LME represents the layer managers in the system.

5.1.2.1 Local interface

The local interface is located between the SMAP and the people and software that request services from the SMAP. Service request/responses pass through this boundary to invoke one or more system management functions. Local interfaces, when present, are beyond the scope of this Recommendation.

5.1.2.2 LMSI

The Layer Management Service Interface is the boundary between the SMAP and the individual layer management ((N)-LMEs). Data and control information pass through this boundary. The boundary provides a way for each layer manager to gain access to parameters within the scope of that layer. This service interface is not subject to standardization.

5.1.2.2.1 From system management to layer management

The boundary between system management and (N)-layer management supports the flow from system management to layer management of:

1) requests to read, set, and perform actions with respect to various values, counters, statuses, etc., within a

given layer;

2) response to inquiries made by an (N)-layer management entity upon the system management function;

3) data from the (N)-layer management of other systems.

5.1.2.2.2 From layer management to system management

The boundaries between system management and (N)-layer management supports the flow from (N)-layer management to system management of:

1) responses to read, set and request for action that came from system management;

2) request to send data to (N)-layer management in another system;

3) requests to place data into the Management Information Base;

4) requests to obtain information from the Management Information Base.

5.1.2.3 SMSI

The System Management Service Interface is the boundary between the SMAP and the SMAE. The SMAE is a type of application entity which communicates system management messages to its peer SMAE in another system. Data and control information to and from the SMAE pass through this boundary. A service definition defines this boundary, and this service boundary defines system management.

5.1.3 System management functions

The responsibilities of system management are considered from two points of view:

a) Local system responsibilities (included for completeness of description):

- to initiate the (N)-layer manager for each layer, upon system activation;

- to serve as the manager of information that is common to several layers or that is supplied externally.

b) Communications responsibilities:

- to provide support for the exchange of information between the (N)-LMEs of a single layer so that the (N)-LMEs do not need to provide separate protocols for such exchanges;

- to coordinate the activities of the various SMAPs within telecommunication networks and subscriber installations.

5.1.4 Relationship to (N)-layer management

System management provides the only vehicle for the exchange of information between layers. Direct communication of management information between layers is deliberately precluded in the reference model to prevent inter-layer dependencies from occurring.

Since inter-layer exchanges of information will have to occur (i.e., error statistics), system management has been

designated as the vehicle through which this exchange will occur. Each layer will have defined sets of information it may make known or will need to acquire.

System management implements the means of acquiring and disseminating this information. This may require activities on the part of system management that span several systems.

System management maintains the MIB and provides the support of (N)-LME access to the MIB.

5.1.5 Relationship to the Management Information Base

The SMAP is responsible for the MIB and provides authorized access to the MIB across the system boundaries.

5.2 Layer management

This section introduces the concept of layer management and its relationships to other entities.

5.2.1 Scope

In keeping with the general principle that each layer is independent of all others, each layer has its own management functions. These layer management functions are described in this Recommendation as the (N)-LME.

The role of the (N)-LME is threefold. Firstly, it serves to coordinate the activities of the (N)-entities within the layer. Secondly, it serves as the "window" to system management for the entities within the layer. Thirdly, in conjunction with both system management and its peer LMEs it manages the layer.

The (N)-LMEs are restricted to activities within an (N)-layer. The (N)-LME must not interact directly with a layer manager of any other layer.

5.2.2 Relationship to (N)-entities which operate protocols

The (N)-LME is charged with coordinating the activities and relationships of various (N)-entities which operate the protocols within the layer.

The (N)-LME is responsible for accessing the MIB on behalf of the (N)-entities. It will access the MIB to retrieve external parameters that the (N)-entity will need to operate, and to store and retrieve operating data that is in external storage contained within the scope of the peer management entity. The (N)-LME is also the focus for control of the (N)-entities by system management.

5.2.3 Relationship between peer (N)-LMEs

The (N)-LMEs will frequently need to exchange information. This exchange ordinarily will be accomplished through the peer SMAPs. However, in some cases, layer management protocols are necessary. These cases are limited to the following:

1) where the exchange of information, or the circumstances under which such information might be exchanged would necessarily interfere with the support of the SMAE by the lower layers: for example, loop testing at layer 1 might be supported by a layer 1 management protocol, and exchange of routing information might be supported by a layer 3 management protocol;

2) where layer management protocols already exist; for example, see Recommendation Q.921.

In no event may a layer management protocol interact directly with any other layer. System management provides the only means for data transfer.

5.2.4 Relationship to system management

The (N)-LMEs rely upon services from system management for three purposes. These are to provide communication for intra-layer management activities, to coordinate inter-layer management activities and to serve as a general repository for management information.

As system management is the supervisor for any action on layer management, the service request/response for external action (e.g., parameter manipulation, statistic gathering, etc.,) will use the SMAP as defined in § 6.1.

5.3 Protocol processing for management purposes

5.3.1 Scope

On occasion, the (N)-entities do participate in the management process. This occurs when the protocol has embedded within itself information that must be made known to other entities and when events occur that must be made known to other entities.

5.3.2 Relationship of (N)-entities to (N)-LMEs

The (N)-entities rely upon the (N)-LME to provide coordination between the various (N)-entities in the (N)-layer, and access to data and services that come from outside the (N)-layer. There is, therefore, a flow of control information between the (N)-entities and the (N)-LME.

Since the (N)-entities exist independently of the other (N)-entities within the (N)-layer, they are dependent upon the (N)-LME to coordinate activities between the various (N)-entities within the sub-system. As an example the (N)-entities rely upon the (N)-LME to determine when requests for connection are being made to establish the association between the connection request at a connection endpoint and the (N)-entity. The (N)-LME also controls the instantiation of (N)-entities at the time of connection requests.

6. Overview of services required by the SMAP

6.1 High layer context management

When the two SMAPs are involved in a management dialogue, they may want to establish a context that will be maintained during the life of the dialogue. In this sense two SMAPs typically work in a connection-oriented mode. The SMAE will provide services that will allow it to work in connection-oriented mode by providing the capability to establish and release associations between peer applications.

These services are to be described further in future Recommendations.

The use of a connectionless service is for further study.

6.2 Definition of a set of generic functions

As presented in § 5, management covers a large spectrum of applications. These applications may be implemented by dedicated SMAPs that can make use of a reduced set of generic functions. The generic functions are listed hereafter with examples for their use:

- trigger an action (e.g., activate or deactivate loopbacks or internal tests);
- event report (e.g., error reporting, alarm reporting);
- get attributes (e.g., cumulative error counters, get parameter values);

- set attributes (e.g., set or modify parameters, thresholds, etc.);

- create and delete managed objects (e.g., create a routing table).

The SMAE provides facilities to allow the generic functions to be communicated between SMAPs.

7. Addressing for information exchange

The information flow takes place between two SMAPs and the originator must be able to address the destination SMAP.

Depending upon the location of the communicating SMAPs different addressing schemes may apply:

1) Explicit Addressing. In this case the remote entity is explicitly addressed by its ISDN address.

2) Implicit Addressing. Implicit addressing relies on mechanisms other than an explicit address in the maintenance message to identify the recipient of the information.

For system management two cases of implicit addressing may be identified:

a) permanent connections;

b) hot line service.

8. Terminal selection

In addition to the normal ISDN addressing mechanisms the maintenance procedures which require actions to perform to particular user equipment require the existence of an identification method that allows access to the unique piece of user equipment to be maintained.

Selection of a unique terminal is based on compatibility checking of various parameters. Compatibility is determined first on the basis of the ISDN address and then on the basis of service information (bearer capability, high layer compatibility, etc.). The service information alone is adequate to provide unique identification if a single unit of equipment satisfies this requirement.

When several TEs connected to the same access, sharing one ISDN address, provide the same functionality, and neither the NSAP nor service information are sufficient, then a unique equipment identifier must be used.

9. Access control

In many cases information accessible through the management function may be private or a management action may result in taking the equipment out of service. Access security to management and maintenance functions must, therefore, be provided.

Access controls may be applied both to the call establishment phase of the maintenance call and also within individual maintenance transactions.

The use of Calling Line Identity provides one method by which maintenance calls can be screened. Further access right discrimination can be performed on the basis of message type in which the management information is carried. Each

message type may have its own implied access rights.

Additionally, specific access control can be performed on the basis of an explicit access control parameter. This parameter has the following characteristics:

1) access control mechanisms are defined as parameters of the primitives passed between system management and the service provider;

2) use of access control parameters is optional;

3) in addition to meeting compatibility requirements, management calls must also satisfy the access control requirements;

4) access control information may be encrypted.
