5i’

SECTION 4

OPERATIONS, MAINTENANCE AND ADMINISTRATION PART (OMAP)

Recommendation Q.795

OPERATIONS, MAINTENANCE AND ADMINISTRATION PART (OMAP)

1 Introduction

The purpose of this Recommendation is to provide procedures and protocols related to operations and maintenance information. These procedures and protocols are associated with the application layer of the Open Systems Interconnection model, as well as the System Management Application Process (SMAP) residing above the application layer. In addition, the procedures and protocols related to operations and maintenance information use other procedures and protocols specified by CCITT in the framework of the OSI model.

The operations and maintenance procedures described are generally associated with two types of signalling points. The controlled signalling point(s) are the signalling point(s) to which controls are applied and about which information is collected. The controlling signalling point(s) are the signalling point(s) which are initiating the controls and to which information from the controlled signalling point(s) are directed.

This Recommendation is divided into eight sections. The first, is the introduction. The second describes those procedures in OMAP which are currently defined for the signalling network. The third describes those operations and maintenance procedures associated with the exchanges. The fourth describes those common operations and maintenance procedures that are associated with the signalling network and exchanges and the fifth section describes those capabilities required by OMAP from other layers of the OSI and gives examples of why the capabilities are required. The sixth section defines timers, timer values and performance timers. The seventh section provides state transition diagrams for the currently defined OMAP procedures. The eighth section defines the OMAP ASEs.

1.1 *Description of management model*

The Signalling System No. 7 Management model is concerned with the control, coordination, and monitoring of the resources which allow SS No. 7 based communication to take place. More specifically, activities relate to the way various SS No. 7 entities obtain data and cooperate in relation to maintaining these resources. Figure 1/Q.795 presents a graphical description of the SS No. 7 Management model in relation to the OSI Management model.

The compatibility of OMAP with OSI management protocols [i.e.Common Management Information Protocol (CMIP)] is for further study.

Figure 1/Q.795, p.

1.1.1 *Management categories*

In order to achieve the functionality described above, three categories of management are identified: Systems Management, (N)-Layer Management, and (N)-Protocol Management. As previously described, Systems management monitors, controls, and coordinates resources through the application layer protocols. The collection of these functions is known as the Systems Management Application Process (SMAP). (N)-Layer Management functions are performed within the corresponding (N)-Layer by a local system. Examples of (N)-Layer functions are measurements and the maintenance of network routing tables. (N)-Protocol Management is concerned with a single instance of communication within the (N)-Layer. It is the responsibility of the (N)-protocol to distinguish between management information carried within the (N)-protocol and other information. OMAP is generally concerned with Systems Management and (N)-Layer Management functions each of which may be considered a sub-set of Systems Management.

1.1.2 *Management information base*

All management information which exists in an open system and which may be transferred or affected through the use of management protocols comprises the Management Information Base (MIB). This information may be provided or accessed by remote systems using OMAP. The exchange of data may be in the form of either monitoring information or exercise of control. The internal structure of the MIB is not specified.

1.2 *Application layer model*

The set of functions above the application layer which collectively encompass systems management is termed Systems Management Application Process (SMAP). The aspect of the SMAP which is then involved with communications is the Systems Management Application Entity (SMAE). The SMAE is also known as the OMAP AE. The OMAP AE consists of a set of one or more Application Service Elements (ASEs). Currently, two ASEs are defined in the OMAP AE, the Transaction Capabilities Application Part (TCAP Recommendations Q.771-775), and the MTP Routing

Verification Test (MRVT) (§ 8). The MRVT ASE uses the services of the TCAP ASE.

The SMAP communicates with the OMAP AE via a set of OM-Primitives at the Systems Management Service Interface (SMSI). Currently, two primitives are defined for OMAP: OM-Confirmed-Action, and OM-Event-Report. These Primitives are defined in § 8. These OM-Primitives are based on the M-Primitives used in the Common Management Information Protocol (CMIP) defined in IS0 9595/6.

1.2.1 *Transfer categories*

There are two categories of data transfer which are of concern to SMAP and management. These are connectionless service and a connection-oriented service.

1.2.1.1 *Connectionless service*

OMAP as currently defined in this Recommendation uses the services of connectionless TCAP as currently specified in Recommendations Q.771-774. This service is generally used for those functions which require only a few messages, e.g. MRVT (see § 2.1) see Figure 2/Q.795.

Figure 2/Q.795, p.

1.2.1.2 *Connection-oriented service*

OMAP as currently defined does not offer a connection-oriented service, however this is an item for further study. This service would generally be used for those functions which require a number of messages. See Figure 3/Q.795.

2 Operations, maintenance and administration procedures for the signalling network

2.1 *Management of routing data*

These procedures deal with the creation, modification, deletion, interrogation, activation and deactivation of routing data. This capability is provided in two basic modes: *multiple* and *single* . *Multiple mode* provides the capability of dealing with many routing relations, while *single mode* deals with a single routing relation.

2.1.1 *Functions*

2.1.1.1 *Creation*

This function provides a means of adding new routing data associated with routing relations to a node in the network. It could cause additional information to be added to an existing table or it may involve adding a completely new table.

Figure 3/Q.795, p.2b

2.1.1.2 *Modification*

This function allows for the modification of existing routing data associated with routing relations within a particular node.

2.1.1.3 *Deletion*

This function is the inverse of creation, in that routing data associated with routing relations will be deleted from the routing tables.

2.1.1.4 *Interrogation*

This function provides a means for requesting the routing data in a specified signalling point.

For example the user can query a signalling point and the signalling point will respond with the respective data. This data can then be compared with the set of data which is expected to be in the signalling point.

2.1.1.5 *Activation*

Activation initiates the use of specified routing data.

The activation of routing relations implies that the new data is actually being used for routing purposes. It may be instantaneous or scheduled for a later time. Activation is accomplished via the activation procedure alone or may be a part of the creation, modification and deletion procedures.

2.1.1.6 *Deactivation*

Deactivation discontinues the use of specified routing data.

If a routing table is erroneously changed, another modification must be made to correct the data in order to continue routing in a sane manner. If a previous version of the table has been retained, the deactivation function may cause this table to be used. Deactivation can be either automatic or may require manual intervention.

2.1.1.7 *Rearrangement*

Rearrangement deals with the coordinated change of a set of routing relations within the signalling network (e.g. when an application is moved from one signalling point to another). This may be handled by requiring that the activation of routing relations in the various signalling points be made (e.g. by an operations and maintenance centre) in a particular order.

2.1.2 *Information elements*

The specification of information elements is left for further study.

2.2 *Circuit validation test (CVT)*

Note — The encoding of the CVT messages is for further study.

2.2.1 *General procedures*

The purpose of a CVT is to ensure that the two exchanges have sufficient and consistent translation data for placing a call on a specific circuit of an interexchange circuit group. A CVT may be initiated by either exchange on demand by maintenance or operations personnel. The test is to be performed before a continuity test while turning up a circuit, so that if a continuity failure is experienced it may be uniquely attributed to a circuit hardware trouble. Before a test is performed, it is necessary to ensure that messages are capable of being routed to that exchange.

2.2.2 *Translations tested*

Both the near end and far end checks are required to perform a complete CVT. The initiating end starts the test by accessing the circuit to be tested when stimulated by a local implementation dependent request. The circuit is identified by an identification code agreed upon by the two exchanges at either end of the circuit.

The translation check at the initiating end must perform adequate tests to ensure that translation data exists for:

1) deriving a physical appearance for the circuit so that a transceiver may be connected to it, and

2) deriving a circuit identification code (CIC) and routing label so that a CCS circuit-related message may be generated.

If the near end test fails, the local maintenance personnel is notified with the reason for the near end failure (e.g. failure reason — circuit unequipped). The test is terminated and a CVT request message is not generated for the circuit under test.

The far end receiving the CVT request message will check to see if the CIC indicated in the message is assigned. If the CIC is unassigned, a failure indication is explicitly returned to the near end via a CVT response message (rather than via an unequipped CIC message). If the CIC is assigned, the far end must perform adequate tests to ensure that translation data exists for deriving a physical circuit appearance from the received routing lable and the CIC so that a loop or transceiver may be connected to the physical circuit appearance. Additionally, the far end must also check that an identification

code for the circuit exists for the physical circuit appearance. If the far end checks fail, the CVT response message will contain the reason for failure and will include an identification code of the failing exchange as agreed upon by the two exchanges. If the far end checks pass, the CVT response message will contain the far end derived identification code for the circuit. At the near end, a comparison of the near end and the far end circuit identification codes are made. If they match, an identification of a successful CVT is given to the maintenance personnel at the initiating end. If the comparison fails, a CVT failure indication with all the relevant data is given to the maintenance personnel for the purpose of isolating the problem.

The CVT response message will also contain data about the circuit with respect to the characteristics of the interexchange circuit group that it is part of. The interexchange circuit group characteristics will include whether:

— odd or even CICs are in control in the case of double seizing;

— the blocked circuit group is classified as ‘‘Block, immediately release the call’’ or ‘‘Block, as soon as the call is normally released’’;

— whether the interexchange circuit group contains analogue, digital or a mix of analogue and digital circuits in order to determine if continuity checks should be performed.

If the group characteristics are unavailable, the CVT response must explicitly indicate this with an unavailable indication. Inconsistencies between the interexchange circuit group characteristics between the two exchanges must be reported to the initiating end maintenance personnel for corrective action.

2.3 *MTP routing verification test (MRVT)*

The MTP routing verification test requirements are as follows:

a) Independence of MTP routing policy.

b) Independence of link set failures.

c) Use the existing MTP without modifications.

d) Response at all tests (positive or negative).

e) Independence of the network structure.

f) The procedure must:

— detect loops in the signalling network;

— detect excessive length routes;

— detect unknown destinations;

— check the bidirectionality of the signalling relations (i.e. if SP A can reach SP B, can SP B reach SP A?).

2.3.1 *General procedure considerations*

The object of the MTP routing verification test is to determine if the data of the MTP routing tables in the network are consistent. It is based on a decentralized test procedure using test messages. It will follow all possible routes to reach the test destination, while tracking the identities of STPs crossed. The procedure is independent of signalling link set availability status. The test is started in any point (SP or STP) for any destination which is in the MTP routing tables and is stopped at the test destination or any intermediate SP at which an error is detected. The test will check the complete routing tables in the network only if all intermediate signalling points know the initiator.

When an inconsistency or failure is detected, local actions are to be specified. The initiator of the test is alerted. The MRVT procedure is applied to individual MTP routing tables. If the MTP is to use structured routing tables (e.g. some or all of the entries in the routing tables may refer to sets of point codes) then the procedure (and/or its initiation) is for further study.

If an MRVA, MRVR, or MRVT message received in an SP contains information extra to that defined in § 2.3, the extra information is ignored unless it is contained as spare subfields within defined fields, and then it will be sent onwards.

2.3.2 *The MRVT messages*

The MTP routing verification test procedure uses three Operations, Maintenance, and Administration Part (OMAP) messages.

2.3.2.1 *The MTP Routing Verification Test (MRVT) message*

The routing verification test message (MRVT) is sent from an SP to an adjacent SP. The MRVT message may use any available signalling route to reach its destination. It contains:

a) information indicating MRVT;

b) the point code of the test destination;

c) the initiator point code;

d) the threshold N of the maximum allowed number of STPs crossed (including the initiator if it is an STP);

e) the information indicating that a trace is requested; the possible values are:

i) for all routes which may be used to reach the test destination the MRVR messages are returned regardless of the result of the test;

ii) no detailed information requested (the MRVR messages sent only if a failure or inconsistency is detected);

f) the list of STPs crossed together with the initiator point code if this point has the STP function.

2.3.2.2 *The MTP Routing Verification Acknowledgment (MRVA) message*

The routing verification acknowledgment (MRVA) message is sent from the SP receiving an MRVT message to the SP which has sent the MRVT message. The MRVA message may use any available signalling routes to reach its destination. It contains:

a) information indicating MRVA;

b) information indicating that an MRVR has been sent;

c) the reason for any failure (partial or complete). If any failure has occurred, one or more of the following indications is present:

i) detected loop;

ii) detected excessive length route;

iii) unknown destination point code;

iv) MRTV not sent due to inaccessibility (e.g. network blockage or network congestion);

v) timer expired (MRVA not received);

vi) unknown initiator point code (this result means that the test destination or an intermediate point does not know the initiator of the test);

vii) test cannot be run due to local conditions (e.g. unavailability of processing resources).

Note that in the case of success, only a) will be present; in the cases of partial success and failure, a), b) and c) will be present.

2.3.2.3 *The MTP Routing Verification Result (MRVR) message*

The MRVR message is sent from an SP to the initiator of the MTP routing verification test. It contains:

a) information indicating MRVR;

b) the test destination point code;

c) the result of the test;

d) the information field.

The content of this information field depends on the result of the test. It contains:

Determined by System Management Application Process (SMAP)

i) if the result of the test is ‘‘success’’:

the point codes of the STPs crossed contained in the MRVT message;

ii) if the result of the test is ‘‘detected loop’’:

the point codes of the STPs which are in the loop;

iii) if the result of the test is ‘‘detected excessive length route’’:

the point codes of STPs crossed contained in the MRVT message;

iv) if the result of the test is ‘‘unknown destination point code’’:

no additional information;

v) if the result of the test is ‘‘MRVT not sent due to inaccessibility’’:

the point code of the inaccessible SP;

vi) if the result of the test is ‘‘MRVA not received’’:

the identity of the SP(s) from which an MRVA was not received when expected;

vii) if the result of the test is ‘‘unknown initiator point code’’:

the point code of the SP returning an MRVA to cause the MRVR to be sent;

viii) if the result of the test is ‘‘test cannot be run due to local conditions’’:

no additional information.

2.3.3 *Initiation of the MRVT procedure at a Signalling Point*

The procedure is started when:

a) New MTP routing data is introduced. It is mandatory that each signalling relation should pass the MRVT procedure successfully before being opened to traffic.

b) MTP routing data is changed.

c) On reception of an unexpected MRVR (due to unknown Signalling Point).

d) On receipt of an MRVT message.

e) On demand from local maintenance staff or an operations and maintenance centre.

f) Periodically at a Signalling Point (having the STP function) to detect cases of mutilation of routing data. (The period is network dependent and should be such that the load on the network is not seriously increased.)

In cases c) and f) above, the ‘‘expected result type’’ field of the MRVT message should be set to indicate no trace is requested. See § 2.3.2.1.

2.3.4 *The MRVT procedure*

2.3.4.1 *At the point initiating the procedure*

2.3.4.1.1 *Initial actions*

When a signalling point initiates an MRVT procedure, it sends an MRVT message for each signalling route which is contained in the MTP routing table to reach the test destination. The destination (DPC) of each of these messages is the adjacent signalling point within the particular route under test. If the test destination is an adjacent signalling point, operated in the associated mode, an MRVT message is not sent to the tested destination itself.

When the MRVT procedure is initiated, a timer T1 (see § 6) is started. An SP cannot initiate an MRVT procedure for a test destination until any previous MRVT procedure for that destination has completed.

2.3.4.1.2 *Subsequent actions*

2.3.4.1.2.1 *Reception of an MRVA message*

An MRVA message acknowledges an MRVT message previously sent.

The reception of the last expected MRVA message stops T1. When an MRVA message is received after T1, it is ignored. When all MRVA messages expected have been received or when T1 expires, the test is complete and results are given to SMAP.

The possible test results at this point in the procedure are listed in § 2.3.2.2 c).

The result ‘‘unknown initiator point code’’ could be a positive result (e.g. when installing a new SP). A test is positive when all expected MRVA messages have been received inside T1 without fault indications.

2.3.4.1.2.2 *Reception of an MRVR message*

The reception of an MRVR message regardless of whether the receiving SP was the initiator causes the information contained in the message to be given to SMAP (see § 2.3.2.3).

2.3.4.2 *In an intermediate point*

2.3.4.2.1 *Initial actions (on reception of an MRVT message)*

If the test cannot be run due to local conditions, an MRVR message is sent to the initiating point, if the initiating point is known to the intermediate SP, and an MRVA message is sent to the sender of the MRVT. The MRVR message contents are as described in § 2.3.2.3. The MRVA message contains the indication ‘‘test cannot be run due to local conditions’’. The test is stopped after informing SMAP.

If the test can be run, looking at the contained fields in the received MRVT message, the point determines if the initiating SP is known, and if the test destination is known in the MTP routing tables. Then:

a) If the initiating SP is unknown, an MRVA message is returned with result ‘‘unknown initiating SP’’ and the value of the ‘‘MRVR sent’’ indicator denotes that the MRVR message was not sent. The test is then stopped, after informing SMAP.

b) If the destination is unknown, the point acknowledges the received MRVT message by an MRVA message with indication ‘‘unknown destination point code’’, and MRVR message is sent to the initiating point. An indication is given to SMAP and the test stopped.

c) If the initiating SP of the test as well as the test destination exist within the SPs routing tables, the SP makes a list ‘‘A’’ of the following adjacent SPs:

i) STPs used to route to the destination (according to the MTP routing tables), excluding the SP from which the MRVT message was received,

ii) the tested destination, if this is adjacent.

The SP then compares the list of STPs crossed contained in the MRVT message with its own list ‘‘A’’ for the following conditions:

i) If the point code of an SP is already in the list of STPs crossed contained in the MRVT message, a loop is detected. An MRVR message is sent to the initiator of the test with the indications described in § 2.3.2.3, then an MRVA message is sent to the point which has sent the MRVT message with the indication ‘‘detected loop’’. The test is stopped (MRVT messages are not regenerated), after SMAP is informed.

ii) If the point code of an SP is not in the list of STPs crossed contained in the MRVT message and if the size of the list is equal to a threshold N in the MRVT message, an excessive length route is detected. An MRVR message is sent to the initiator of the test with the indications described in § 2.3.2.3, then an MRVA message is sent to the point which has sent the MRVT message with the indication ‘‘detected excessive length route’’. The test is stopped (MRVT messages are not regenerated), after SMAP is informed.

iii) If it is impossible to route an MRVT message, an MRVR message is sent to the initiator of the test with the indications described in § 2.3.2.3, then an MRVA message containing the indication ‘‘MRVT not sent due to inaccessibility’’ is sent to the point which has sent the MRVT message. The test is stopped (no MRVT messages are regenerated), after SMAP is informed.

iv) In other cases a timer T1 is started, and MRVT messages are sent to all the SPs in list ‘‘A’’. When an MRVT message is sent by an STP, the STP adds its identity in the MRVT message sent.

2.3.4.2.2 *Subsequent actions (on reception of an MRVA message)*

The reception of an MRVA message acknowledges the corresponding MRVT message previously sent. The timer is stopped when all the expected MRVA messages have been received.

MRVA message is sent when all expected MRVA messages have been received. The result of the test contains the different results from the MRVAs received.

If any MRVA message contained both the result ‘‘unknown initiating SP’’ and the value of the ‘‘MRVR sent’’ indicator denotes that the MRVR was not sent, an MRVR is returned to the initiator.

If one (or several) MRVA message is not received before T1 expires, an MRVA message is sent and an MRVR message is sent to the initiator of the test with the indications described in § 2.3.2.3.

If an MRVA message cannot be sent, no action is taken.

If an MRVA message is received after T1 expires, it is ignored.

2.3.4.3 *At the test destination receiving an MRVT message*

On reception of an MRVT message, the test destination checks that the initiator of the test is known.

If the initiator is unknown, an MRVA message is sent to the point which had sent the MRVT message. This MRVA message contains the result ‘‘unknown initiator point code’’ and the ‘‘MRVR sent’’ indicator set to denote that the MRVR was not sent.

If the initiator of the test is known, the test is finished with success and the following actions are taken:

a) If the MRVT message received contains the indication that a trace is expected, (see § 2.3.2.1) an MRVR message is sent to the initiator of the test with the indications described in § 2.3.2.3. An MRVA message is then sent to the point which had sent the MRVT message.

b) If the MRVT message received contains the indication that a trace is not expected, (see § 2.3.2.1), an MRVA message is sent to the point which had sent the MRVT message. No MRVR message is sent.

If an MRVA message cannot be sent, no action is taken.

2.4 *Reception of a message for an unknown destination*

When an indication is received from the MTP due to the reception of a message for an unknown destination, an MRVR message is sent to the point which has sent the messages with the indications described in § 2.3.2.3.

When a point receives such an unexpected MRVR message, an indication is given to SMAP and an MRVT is started.

2.5 *SCCP routing verification test (SRVT)*

The SCCP routing verification test requirements are as follows:

a) No modification should be needed to the SCCP protocol specification.

b) The SRVT should be independent of the SCCP routing policy.

c) The SRVT should be independent from the network structure, considering the SCCP routing points.

d) The SRVT is not required to verify MTP routing correctness (the MRVT is expected to do this).

e) A response (either positive or negative) is to be given to all tests.

f) The procedure should:

— Be able to check all possible SCCP routes, including:

i) parallel SCCP routing points (this is understood to mean multiple translation points);

ii) serial SCCP routing points (this is understood to mean multiple translation points);

iii) multiple destinations corresponding to the tested Global title (this is understood to be multiple signalling points/subsystem numbers where SCCP permits a maximum of two destinations to be derived from a Global title).

— Detect loops in the SCCP routing.

— Detect unknown destination (a destination corresponds to the tested Global title).

— Verify Global Title Translation data for accuracy, completeness, and inconsistency.

2.5.1 *General procedure considerations*

The general procedure considerations of the SRVT are left for further study.

2.5.2 *The SRVT messages*

The SRVT mesages are left for further study.

2.5.3 *Initiation of the SRVT procedure*

Initiation of the SRVT procedure is left for further study.

2.5.4 *The SRVT procedure*

The specification of the SRVT procedure is left for further study.

2.6 *Long-term measurement collection*

The measurements to be taken are given in Recommendation Q.791.

Periodically, at the same time, every signalling point collects the required data. The data collected may be transferred toward the appropriate signalling point(s) (e.g. an operations and maintenance centre) either on demand or on a scheduled basis.

The procedures and means used for transfer of data are for further study.

2.6.1 *Functions*

2.6.1.1 *Parameter intialization*

This function initializes, in a signalling point, the destination address(es) to which measurements will be transferred, sets up default parameters describing which indications should be reported and, if scheduled, when the measurements should be transferred.

2.6.1.2 *Parameter modification*

This function allows modifications to the default measurements which are collected in a signalling point. It may not be used to modify the measurements duration nor to remove those measurements described as being obligatory in Recommendation Q.791. The following list represents the set of modifications currently available and the information elements that must be provided at the controlled signalling point. Other modifications have been left for further study.

a) *Allow measurement collection* is used to indicate that a particular measurement(s) should be collected for a particular controlling signalling point.

Command, controlling address, measurement 1, measurement 2, etc.

b) *Inhibit measurement collection* is used to indicate that a particular measurement(s) should not be collected for a particular controlling signalling point.

Command, controlling address, measurement 1, measurement 2, etc.

2.6.2 *Information elements*

2.6.2.1 *Command indicates the function to be performed*

2.6.2.2 *Controlling address* is the address of the signalling point from which commands are sent and to which the measurements are transferred.

2.6.2.3 *Measurement* is the name of a particular measurement which should (not) be collected.

2.7 *On-occurrence measurement reporting*

These procedures deal with the transfer and control of the measurements described in Recommendation Q.791 (Monitoring and measurements for Signalling System No. 7 networks) as being reported on occurrence. The record of an on-occurrence measurement is referred to as an *event indicator* or *indicator* .

2.7.1 *Functions*

2.7.1.1 *Parameter initialization*

This function initializes, in a signalling point, the destination address(es) to which reporting should be made (e.g. an OMC), sets up default parameters describing which indicators should be reported, what thresholds are associated with the indicators and which indicators should be logged along with the establishment of logging files (see § 2.7.1.4).

2.7.1.2 *Parameter modification*

Parameter modification allows modifications to be made to the default indicators which are to be logged and transmitted. In addition, it allows the modification of the destination addresses that are associated with particular indicators. The following list represents the set of modifications available and the information elements that must be provided at the controlled signalling point. Other modificaitons have been left for further study.

a) *Create a logging file* | is used to create a logging file and set the number of event indicators to be logged before overwriting old indicators:

command, controlling address, file name, size.

b) *Change a controlling address* | is used to modify a controlling address (e.g. of an OMC) to which reports should be made:

command, old controlling address, new controlling address.

c) *Allow event logging* | is used to indicate that a particular indicator(s) should be logged and optionally assign a threshold to the indicator:

command, controlling address, event indicator 1, threshold 1, etc.

d) *Inhibit event logging* | is used to indicate that a particular indicator(s) should not be logged:

command, controlling address, event indicator 1, event indicator 2, etc.

e) *Change event logging threshold* | is used to modify a threshold associated with a particular indicator(s) to be logged:

command, controlling address, event indicator 1, threshold 1, etc.

f) *Allow event reporting* | is used to indicate that a particular indicator(s) should be reported to a controlling address and optionally assign a threshold to the indicator:

command, controlling address, event indicator 1, threshold 1, etc.

g) *Inhibit event reporting* | is used to indicate that a particular indicator(s) should not be reported:

command, controlling address, event indicator 1, event indicator 2, etc.

h) *Change event reporting threshold* | is used to modify a threshold associated with a particular indicator(s) to be reported:

command, controlling address, event indicator 1, threshold 1, etc.

2.7.1.3 *Event indicator reporting*

This function notifies a specified controlling address of on-occurrence measurements by the transfer of an event indicator. The following information elements are included in each message that is sent for reporting purposes:

event type, controlled address, affected address, time stamp, additional information.

2.7.1.4 *Recovery of recent on-occurrence measurement history*

In the event of failure of a controlling signalling point (e.g. an operations maintenance centre) or a signalling relation to that controlling signalling point, a recovery procedure is required to allow the controlling signalling point to recover a recent history of on-occurrence measurements in the signalling network. This is accomplished by maintaining a log of the last N event indicators, at the signalling point, which may be requested by the controlling signalling point after recovery.

The logging file may also be used to store event indicators which have not been requested for reporting by the controlling signalling point, for example, measurements with lower thresholds for logging than for reporting.

The maximum number of event indicators logged (N) is for further study.

2.7.2 *Information elements*

2.7.2.1 *Controlling address* | is the address of the signalling point from which commands are sent and to which the event indicators are reported.

2.7.2.2 *Controlled address* | is the address of the signalling point which is being controlled and from which measurements are being reported.

2.7.2.3 *Affected address* | is the address of the signalling point about which an event indicator pertains.

2.7.2.4 *Command* | indicates a function to be performed.

2.7.2.5 *File name* | is the name of a file at the signalling point where logging is to be performed.

2.7.2.6 *Size (N)* | is the maximum number of event indicators that may be recorded in an event log.

2.7.2.7 *Event type* | describes the on-occurrence measurement associated with an event indicator.

2.7.2.8 *Threshold* | represents some threshold associated with an on-occurrence measurement before its associated event indicator is reported or logged.

2.7.2.9 *Time stamp* | represents the unique network time when the event indicator was generated.

2.7.2.10 *Additional information* | is any additional information associated with the on-occurrence measurement being indicated (e.g. the link ID of a signalling link experiencing a failure).

2.8 *Delay measurements*

These procedures deal with measuring delays across the signalling network, whether these delays are measured point-to-point or round trip.

2.8.1 *Functions*

The specifications of functions is left for further study.

2.8.2 *Information elements*

The specification of information elements is left for further study.

2.9 *Clock initialization*

The clock initialization procedures provide a means for setting clocks in a signalling point for operations and maintenance and for other purposes. Its main function allows clocks in the network to be set up to a unique network time.

2.9.1 *Functions*

The specification of specific functions has been left for further study.

2.9.2 *Information elements*

The specification of information elements is left for further study.

2.10 *Real-time control*

These procedures allow for automatic or manual controls to be taken in a controlled signalling point based on input from a controlling signalling point. The controlling signalling point may initiate these procedures based on input from procedures like the *on-occurrence measurement reporting* procedures.

2.10.1 *Functions*

The specification of functions is left for further study.

2.10.2 *Information elements*

The specification of information elements is left for further study.

2.11 *Operations*

These procedures provide a capability to perform operations, such as activation of links, within the signalling network.

2.11.1 *Functions*

The specification of functions is left for further study.

2.11.2 *Information elements*

The specification of information elements is left for further study.

3 Operations and maintenance procedures for the exchanges

This paragraph deals with those procedures associated with the operations and maintenance of exchanges and remains as a topic for further study. A basis for the definition of this paragraph will be Recommendations Q.511, Q.512, Q.542 and Q.544, Supplement 6 of Fascicle II.3 and Recommendation Z.318.

4 Operations and maintenance procedures for both the Signalling Network and Exchanges

This section deals with those procedures associated with operations and maintenance that are found in common with both the Signalling Network and the Exchanges. See OMAP procedures and protocols in this document and also Recommendations Q.541, Q.543, Q.544 and M.30. The contents of this paragraph remains as a topic for further study.

5 Requirements on the protocols used to support the operations and maintenance procedures

It is assumed that the procedures defined in the previous paragraphs will make use of the protocols defined by CCITT in the various functional layers of the OSI model. This paragraph describes the capabilities required from these layers. No attempt is made to allocate the requirements to specific functional layers of the OSI model. See OMAP procedures and protocols in this document and also Recommendations Q.541, Q.543, Q.544 and M.30.

5.1 *Addressing capability*

This capability allows the user of the OMAP to address applications in nodes in the signalling network or to applications in nodes that may exist in any interconnected network.

5.2 *Distribution capability*

This capability is responsible for delivering information to the appropriate operations and maintenance application within the destination node.

5.3 *Connection-oriented communication capability*

This capability establishes a connection, whether physical or logical, for the purposes of transporting operations and maintenance information between two signalling points. This is required, for example, for the interactions between a controlling signalling point where MML commands are entered and a controlled signalling point where the functions controlled by the MML commands exist.

5.4 *Connectionless communication capability*

The capability allows the transfer of operations and maintenance information between two signalling points without the establishment of a connection. This is required, for example, to transfer event indicators used in the *on-occurrence measurement reporting* .

5.5 *File transfer capability*

This capability provides the means for communications between operations and maintenance applications which require file transfers. This is required, for example, to transport files generated by *long-term measurement collection* .

5.6 *Other capabilities*

Other capabilities which may be required are for further study.

6 Timer definitions and values, and performance time definitions and values

6.1 *Timer definitions and values*

T1 at a signalling point (Near End Signalling Point) initiating an MRVT is the guard time waiting for all MRVA messages in response to the MRVT messages sent from the Near End SP.

$$T1 \text{ (Near End SP)} = D(N+1)$$

where N is defined in § 2.3.2.1 d), and D is defined in § 6.2 below.

T1 at an intermediate signalling point is the guard time associated with a received MRVT message, waiting for all MRVA messages in response to all MRVT messages sent.

T1 (Intermediate SP) = T1 deduced from the received MRVT message — D

6.2 *Performance time definitions and values*

$$D = Max(d1) + Max(d2) + Max(d3) + Max(d4)$$

where

d1: time to transfer an MRVT message.

d2: time to take into account an MRVT message received.

— In an Intermediate SP, performance time d2 is the time between the reception of an MRVT message and the sending of the MRVT messages to the concerned SPs (or the sending of the MRVA message to the point which has sent the MRVT message when a problem is detected).

— In the tested destination, performance time d2 is the time between the reception of an MRVT message and the sending of the MRVA message to the point which has sent the MRVT message.

d3: time to transfer an MRVA message.

d4: time to take into account an MRVA received.

— In an Intermediate SP, performance time d4 is the time between the reception of the last MRVA message and the sending of the MRVA message to the point which has sent the MRVT message.

H.T. [T1.795]

Performance time	Estimated maximum value
d1	2 seconds (provisional)
d2	3 seconds (provisional)
d3	2 seconds (provisional)
d4	1 second (provisional)
D	8 seconds (provisional)

Table [T1.795], p.

7 State transition diagrams

7.1 *General*

Paragraph 7 contains the description of the test functions described in §§ 2.2 and 2.3 in the form of state transition diagrams according to the CCITT Specification and Description Language (SDL).

A set of diagrams is provided for each of the following tests:

a) Circuit Validation Test (CVT), described in § 2.2;

b) MTP Routing Verification Test (MRVT), described in § 2.3.

7.2 *Abbreviations used in Figures 4/Q.795 to 5/Q.795*

CVT Circuit validation test;

CKT Circuit;

MRVT MTP Routing verification test;

MRVA MTP Routing verification acknowledgement;

MRVR MTP Routing verification result;

PC Point code;

REQ Request;

RESP Response;

SMAP System management application process.

Figure 4/Q.795, p.

Figure 5/Q.795 Sheet 1 of 3, p.

Figure 5/Q.795 Sheet 2 of 3, p.

Figure 5/Q.795 Sheet 3 of 3, p.

8 ASEs

In the event of a conflict between § 2 and § 8, then § 2 will take precedence.

8. *MRVT ASE* |

The MRVT ASE provides the services accessed via the two OM-primitives OM-CONFIRMED-ACTION and OM-EVENT-REPORT. These are described in Figure 6/Q.795 of the OM-CONFIRMED-ACTION primitive, while routeTrace is the EventType of the OM-EVENT-REPORT primitive. Each is described below with the appopriate arguments (ActionArg for testRoute and EventInfo for routeTrace) and, for testRoute, the appropriate ActionResults and ActionErrors. For both OM-primitives in Figure 6/Q.795, the InvokeID in the respective primitives is the InvokeID passed to TCAP, the ResourceClass indicates MTP Routing Tables, and the ResourceInstance contains the point code of the test destination. In addition, the accessControl argument in OM-CONFIRMED-ACTION is absent. The testRoute Action makes use of the BEGIN message with result (MRVA) returning in an END. The routeTrace Event (MRVR) uses a BEGIN message with pre-arranged end.

8.1.1 *testRoute Action*

The testRoute Action is invoked to initiate an MTP routing verification test. At the initiator node, this invocation is requested by the local SMAP. At subsequent nodes, the Action is requested implicitly by the receipt of a testRoute Action invocation. A successful reply indicates successful completion of the test at the point it was invoked and, implicitly, at all subsequent points where the test was invoked. A failure indication is returned to indicate that the test failed in this or a subsequent node.

H.T. [T2.795]

testRoute CNF-ACTION	*Timer* = T1	*Class* = 1	*Code* = 00000001
ActionArg	*Opt/Man*	*Reference*	
initiating SP	M	8.1.1.1.1	
traceRequested	M	8.1.1.1.2	
threshold	M	8.1.1.1.3	
pointCodesTraversed	M	8.1.1.1.4	

Table [T2.795], p.

See X.208 and X.209 for description of formal notation.
Derived from ISO 9596.

H.T. [T3.795]

testRoute CNF-ACTION
ACTIONARG SEQUENCE {
 {
initiating SP [0] IMPLICIT PointCode,
traceRequested [1] IMPLICIT BOOLEAN,
threshold [2] IMPLICIT INTEGER,
pointCodesTraversed [3] IMPLICIT PointCodeList
 }
   }
 {
ACTIONRESULT
empty
SPECIFICERRORS
{ ailure, partialSucces }
 }
::=1

Table [T3.795], p.

8.1.1.1 *testRoute Action Arguments*

8.1.1.1.1 *initiating SP*

The initiating SP identifies the original requestor of the test. It is of type PointCode, defined as an octet string.

H.T. [T4.795]

Parameter	*Code*
initiating SP	10000000
Contents	

{
Bit 0 contains the first bit of the point code,
}
{
Bit 1 contains the second bit of the point code, etc.
}	

PointCode ::= OCTET STRING	

Table [T4.795], p.

8.1.1.1.2 *traceRequested*

traceRequested indicates that a trace of all routes used to reach the destination should be reported to the originator (the routeTrace Event is described in § 8.1.2). It is of type BOOLEAN.

H.T. [T5.795]

Parameter	*Code*
traceRequested	10000001
Contents	*Meaning*
TRUE (=1) trace was requested, return trace information on success and failure. }	{
FALSE (=0) trace not requested, return trace information only on failure. }	{

Table [T5.795], p.

8.1.1.1.3 *threshold*

The originator sets a maximum threshold level of signalling points (SP) which are allowed to be crossed in the course of the test (including the initiator if it is an STP). This aids in detecting overly long routes. This threshold is an integral number of SPs, thus it is of type INTEGER.

H.T. [T6.795]

Parameter	*Code*
threshold	10000010
Contents	

{
Integer number represented in binary.
 }	

Table [T6.795], p.

8.1.1.1.4 *pointCodesTraversed*

As each SP is crossed, it adds its own point code to the list of point codes traversed. This aids in detecting loops and is also useful information in case of a failure or if a route trace is requested. It is a list of point codes thus of type PointCodeList. This PointCodeList could be empty.

H.T. [T7.795]

Parameter	*Code*
pointCodesTraversed	10100011
Contents	

{
Sequence of PointCodes, tagged as 'PointCode' with the contents indicating the exact point code.
 }	

{
PointCodeList ::= SEQUENCE OF PointCode
 }	

Table [T7.795], p.

8.1.1.2 *Action Results*

There are no contents in a successful return indication.

8.1.1.3 *Action Errors*

SpecificErrors are possible errors which can occur during this test which are unique to this test. These specific errors are in addition to the errors already identified in the OM-ACTION service and appear as parameters to the Processing Failure Error.

8.1.1.3.1 *failure*

failure indicates a condition of total failure, where no route worked correctly. Most often this will be used as a failure indication from the point which detects the error and does not invoke any further testRoute Actions. The failure SpecificError has with it a parameter to indicate the error condition causing the failure. This parameter failureType is represented as a big string. In addition, the second parameter is to be used when failureType indicates the error Unknown initiating SP. traceSent indicates whether or not a routeTrace Event has been invoked to report trace information. It is necessary to indicate this for this error since the node detecting the error cannot send the routeTrace, thus the previous node must. traceSent is a type of BOOLEAN.

H.T. [T8.795]

Specific Error	*Code*
failure	00000001
Parameters	*References*
failureType traceSent	8.1.1.3.1 8.1.1.3.1

Table [T8.795], p.

H.T. [T9.795]

Parameter	*Code*
failureType	10000000
Bit	*Meaning*
0 1 2 3 4 5 6	detectedLoop excessiveLengthRoute unknownResourceInstance routeInaccessible processingFailure unknown Initiating SP timerExpired

Table [T9.795], p.

H.T. [T10.795]

Parameter	*Code*
traceSent	10000001
Contents	*Meaning*
TRUE the trace information was sent } FALSE the trace information was not sent }	{ {

Table [T10.795], p.

H.T. [T11.795]

{
failure SPECIFICERROR
failure
PARAMETER SEQUENCE
{ ailureType [0] IMPLICIT FailureString,
traceSent [1] IMPLICIT BOOLEA }
failure
::=1
}

Table [T11.795], p.

H.T. [T12.795]

{
FailureString ::= BITSTRING
detectedLoop [0],
excessiveLengthRoute [1],
unknownResourceInstance [2],
routeInaccessible [3],
processingFailure [4],
unknown Initiating SP [5],
timerExpired [6]
}

Table [T12.795], p.

8.1.1.3.2 *Partial Success*

This indication is given when at least one routeTest Action invocation failed and at least one succeeded (at least partially). In this case, each type of error that occurred will be noted and sent in the final reply. The format and contents of partial success are the same as failure.

H.T. [T13.795]

Specific Error	*Code*
partialSuccess	00000010
Parameters	*References*
failureType traceSent	8.1.1.3.1 8.1.1.3.1

{
partialSuccess SPECIFICERROR
PARAMETER SEQUENCE { ailureType [0] IMPLICIT FailureString,
PARAMETER SEQUENCE
traceSent [1] IMPLICIT BOOLEA }
::=2
}	

Table [T13.795], p.

8.1.2 *routeTrace Event*

The routeTrace Event reports trace information. Trace information consists of zero, one or more point codes, such as the point code detecting an error or the entire list of point codes traversed along a route. This event is invoked either at the explicit request of the originating node (indicated by traceRequested, see § 8.1.1.1.2) or by failure at any point along the route. This event is not confirmed, therefore no replies to this invocation are expected (no error or succes indications are expected).

H.T. [T14.795]

routeTrace Event	*Timer* = 0	*Class* = 4	*Code* = 00000010
EventInfo	*Opt/Man* (see Note)	*Reference*	
success	O	8.1.2.1.1	
detectedLoop	O	8.1.2.1.2	
excessiveLengthRoute	O	8.1.2.1.3	
unknownResource Instance	O	8.1.2.1.4	
routeInaccessible	O	8.1.2.1.5	
processingFailure	O	8.1.2.1.6	
unknown Initiating SP	O	8.1.2.1.7	
timerExpired	O	8.1.2.1.8	

Note — One and only one of these parameters must be present.

Table [T14.795], p.

H.T. [T15.795]

{
routeTrace EVENT
EVENTINFO CHOICE [
success [0] IMPLICIT PointCodeList,
detectedLoop [1] IMPLICIT PointCodeList,
excessiveLengthRoute [2] IMPLICIT PointCodeList,
unknownResourceInstance [3] IMPLICIT NULL,
routeInaccessible [4] IMPLICIT PointCode,
processingFailure [5] IMPLICIT NULL,
unknown Initiating SP [6] IMPLICIT PointCode,
timerExpired [7] IMPLICIT PointCodeList]
::=2
}

Table [T15.795], p.

8.1.2.1 *Event Information*

8.1.2.1.1 *success*

On successful completion, the trace of the point codes (one or more) of the crossed SPs are included.

H.T. [T16.795]

Parameter	*Code*
success	10100000
Contents	*References*

{
Sequence of Point Codes, Tagged as ‘‘Point Code’’, with contents indicating the exact point code.
}
	8.1.1.1.4

Table [T16.795], p.

8.1.2.1.2 *detectedLoop*

When a loop is detected, the point codes (three or more) contained in the loop are included.

H.T. [T17.795]

Parameter	*Code*
detectedLoop	10100001
Contents	*References*

{
Sequence of Point Codes, Tagged as ‘‘Point Code’’, with contents indicating the exact point code.
}
	8.1.1.1.4

Table [T17.795], p.

8.1.2.1.3 *excesiveLengthRoute*

When an excessively long route is found (threshold exceeded), the entire route is included.

H.T. [T18.795]

Parameter	*Code*
excessiveLengthRoute	10100010
Contents	*References*

{
Sequence of Point Codes, Tagged as ‘‘Point Code’’, with contents indicating the exact point code.
}
	8.1.1.1.4

Table [T18.795], p.

8.1.2.1.4 *unknownResource*

If the resource instance is unknown, no additional information is required.

H.T. [T19.795]

Parameter	*Code*
unknownResourceInstance	10000011
Contents	*References*
empty	—

Table [T19.795], p.

8.1.2.1.5 *routeInaccessible*

The point code of the node where the route was inaccessible is included.

H.T. [T20.795]

Parameter	*Code*
routeInaccessible	10000100
Contents	*References*

{
Bit 0 contains the first bit of the Point Code,
}
{
Bit 1 contains the second bit of the Point Code, etc.
}
	8.1.1.1.1

Table [T20.795], p.

8.1.2.1.6 *processingFailure*

If a processing failure occurs, no additional information is required.

H.T. [T21.795]

Parameter	*Code*
processingFailure	10000101
Contents	*References*
empty	—

Table [T21.795], p.

8.1.2.1.7 *unknownInitiating SP*

The point code of the node detecting the unknown Initiating SP is included.

H.T. [T22.795]

Parameter	*Code*
unknown Initiating SP	10000110
Contents	*References*

{
Bit 0 contains the first bit of the Point Code,
}
{
Bit 1 contains the second bit of the Point Code, etc.
}
	8.1.1.1.1

Table [T22.795], p.

8.1.2.1.8 *timerExpired*

The point code(s) of the node(s) from where no result for the testRoute Action was received is included.

H.T. [T23.795]

Parameter	*Code*
timerExpired	10100111
Contents	*References*

{
Sequence of one or more Point Codes tagged as ‘‘Point Code’’, with contents indicating the exact point code.
}
	—

Table [T23.795], p.

OMAP runs tests on resources such as the MTP and SCCP routing tables. These resources are here described as ‘‘Resource Classes’’ and are identified by an object identifier which specifies the CCITT, the study period Q.795, and the type of resource. This structure is shown below for the OMAP object identifiers mtp-Routing-Tables and sccp-Routing-Tables.

omap OBJECT IDENTIFIER ::= { CCITT, Q.795 } mtp-Routing-Tables-1988 OBJECT IDENTIFIER ::= { omap 0 }
sccp-Routing-Tables-1988 OBJECT IDENTIFIER ::= { omap 1 } [unused]

The Resource Class of MTP Routing Tables is 0011861B00 (hexadecimal), and for SCCP Routing Tables is 0011631B01 (hexadecimal). See Recommendation X.208, Annex C.

Figure 6/Q.795 Sheet 1 of 8 [T24.795], p. (a traiter comme tableau MEP)

OM-EVENT-REPORT

The OM-EVENT-REPORT service as given in Table 1/Q.795 provides a user with the capability to report the occurrence of an event concerning a management resource to a user in another open system. The specific event that occurred is interpreted in the context of the resource class specified.

H.T. [T25.795]

TABLE 1/Q.795

OM-EVENT-REPORT Parameters

Parameter Name	Req/Ind
InvokeID	M
ResourceClass	M
ResourceInstance	M
EventValue	M
EventTime	O
EventInfo	O

{
Parameters Definitions:
}
{
InvokeID:
as defined in Recommendation Q.772.
}
{
ResourceClass:
identifies the class of resources for which this event is defined.
}
{
ResourceInstance:
identifies the resource instance on which the event is to be performed.
}
{
EventValue:
specifies the particular event that is being reported by the resource instance.
}
{
EventTime:
specifies the time at which the event was generated.
}
{
EventInfo:
provides additional event specific information.
}	

Table 1/Q.795 [T25.795], p.

The eventReport operation is defined, using the TCAP OPERATION MACRO, as in Figure 6/Q.795, Sheet 2.

–v’6p’

Figure 6/Q.795 Sheet 2 of 8 [T26.795], p. (a traiter comme tableau MEP)

Specific event reports are categorized by resource class. The protocol uses may be described by the EVENT Macro in Figure 6/Q.795, Sheet 3.

–v'6p'

Figure 6/Q.795 Sheet 3 of 8 [T27.795], p. (a traiter comme tableau MEP)

OM-CONFIRMED-ACTION

The OM-CONFIRMED-ACTION service as shown in Table 2/Q.795 provides a user with the capability to request that a management action be performed on a resource instance by a user in another open system. The specific action to be performed is interpreted in the context of the resource class specified. This service is a confirmed service (a report of success or failure is always sent).

–v'6p'

H.T. [T28.795]
TABLE 2/Q.795
OM-CONFIRMED-ACTION Service

Parameter Name	Req/Ind	Res/Con
InvokeID	M	M=
AccessControl	O	—
ResourceClass	M	—
ResourceInstance	M	—
CnfAction Value	M	—
ActionArg	O	—
ActionResult	—	M | ua)
ActionError	—	M | ub)

a) Mandatory in Return Result component (may be empty).

b) Mandatory in Return Error component.

{ *Parameter Definitions:* }
{ InvokeID: as defined in Recommendation Q.772. }
{ AccessControl: information to be used as input to access control functions. }
{ ResourceClass: identifies the class of resources for which this action is defined. }
{ ResourceInstance: identifies the resource instance on which the action is to be performed. }
{ ActionValue: specifies a particular action that is to be performed on the resource instance. }
{ ActionArg: contains the argument for the particular action being invoked. }
{ ActionResult: this field contains the result of the successful action performed, as appropriate. }
{ ActionError: this field indicates error or problem status information if the action did not successfully complete. }

Table 2/Q.795 [T28.795], p.

The confirmedAction operation is defined, using the TCAP OPERATION MACRO, as shown in Figure 6/Q.795, Sheet 4.

–v’6p’

Figure 6/Q.795 Sheet 4 of 8 [T29.795], p. (a traiter comme tableau MEP)

Specific Actions are categorized by resource class. The protocol uses may be described by the ACTION Macro as shown in Figure 6/Q.795, Sheet 5.

Figure 6/Q.795 Sheet 5 of 8 [T30.795], p. (a traiter comme tableau MEP)

ERROR DEFINITIONS

A number of error codes have been referred to in the definition of the two OM-Services. These error situations are defined in this section.

Definitions:

noSuchResourceClass: the resource class in the Invoke APDU is not recognized by the receiving end.

noSuchResource: while the resource class in the Invoke APDU is recognized, there is no corresponding resource instance of that class at the receiving end.

accessDenied: access to the resource is denied.

processingFailure: a failure occurred while processing a specific action or event. The failure indicators and parameters are action or event specific.

noSuchEvent: the event type specified is not supported by or known to the receiving end.

noSuchAction: the action type specified is not supported by or known to the receiving end.

noSuchAttribute: the attribute specified is not supported by or known to the receiving end.

invalidAttributeValue: the attribute value is out of range.

BLANC

Figure 6/Q.795 (page 6 sur 8) [T31.795], p. (a traiter comme tableau MEP)

Figure 6/Q.795 (page 7 sur 8) [T32.795], p. (a traiter comme tableau MEP)

OTHER TYPE DEFINITIONS

Figure 6/Q.795 Sheet 8 of 8 [T33.795], p. (a traiter comme tableau MEP)

ANNEX A
(to the Recommendation Q.795)

Example MRVT message as delivered to the SCCP

Figure A-1/Q.795, p.

Figure A-2/Q.795, p.

Figure A-3/Q.795 [T34.795], p. (à traiter comme tableau MEP)

Figure A-4/Q.795 [T35.795], p. (a traiter comme tableau MEP)

Figure A-5/Q.795 [T36.795], p. (a traiter comme tableau MEP)

ANNEX B
(to Recommendation Q.795)

SCCP Routing Verification Test (SRVT)

B.1 *Introduction*

This annex describes an SCCP Routing Verification Test (SRVT). The procedure described covers the case of a single MTP network. Enhancements of this procedure are required to ensure that:

— the procedure works for multiple MTP networks;

— the procedure tests the change of Gobal Title at an SCCP relay node;

— the procedure is signalling network structure independent.

B.2 *SRVT*

B.2.1 *General*

The SCCP Routing Verification Test (SRVT) is the means of testing the global title translation service of the Signalling Connection Control Part (SCCP). The test is designed to verify the accuracy and completeness of the global title translation data in global title translation service points. This test is only meant for the case of a single MTP network. An SRVT for multiple MTP networks is for further study. The test will be used after a recent translation data change, when a translation problem is suspected, or on a periodic basis to detect cases of mutilation of translation data.

When an inconsistency or failure is detected, local actions are to be specified. The initiator of the test is alerted.

B.2.2 *Messages*

The SCCP Routing Verification Test uses three OMAP messages which are specified by the OMAP Application Service Element.

B.2.2.1 *SCCP Routing Verification Test (SRVT) message*

The SRVT message is sent from a Signalling Point (SP) initiating the appropriate part of the SRVT procedure based on the function of the respective SP. The message serves three different functions, depending upon the nature of the SP sending it. In coding, both Verify and Request are delineated by the No Compare setting of the From Indicator parameter.

The request form of the SRVT message is sent by a Signalling Point (SP) to request an SRVT global title translation within the SRVT procedure. The originating SP may be the Near End Signalling Point (NESP), or an Intermediate Translation Signalling Point (ITSP). The destination of the message is a Translation Signalling Point (TSP) which is to perform a global title translation on the Global Title contained in the message. Hence, the Translation Point Code (TPC) is the Destination Point Code (DPC) in the routing label.

The Verify form of the SRVT message is sent by a Final Translation Signalling Point (FTSP), i.e. the last SP that performs the global title translation service, to both the Primary Point Code (PPC) and the Secondary

Point Code (SCP, if any) derived from the global title translation. Hence, the PPC and SPC are used as the Destination Point Codes (DPC) in the routing labels.

The Compare form of the SRVT message is sent by a Translation Signalling Point (TSP) to a point performing the duplex global title translation. The message is sent so the results of both tanslations can be compared. This message is mandatory only in networks that have duplex global title translation service (i.e. the identical translation is duplicated at a mate signalling point). The point code of the Duplex Translation Signalling Point (DTSP) is the Destination Point Code (DPC) in the routing label.

The message contains:

a) Information Indicating SRVT;

b) Form Indicator (Compare or No Compare);

c) GTI + GT — Global Title Indicator + Global Title (Destination);

d) MTP Backward Routing Required Indicator for SRVA and SRVR;

e) NEPC — Near End Point Code from which test was initiated;

f) GTI + NEGT — Global Title Indicator + Near End Global Title;

g) DPC — Destination Point Code (Translation PC or Primary PC);

h) Destination SSN — Optional Subsystem Number based on DPC;

i) Backup DPC — Backup Destination Point Code (Translation PC or Secondary PC);

j) Backup SSN — Optional Subsystem Number based on Backup DPC;

k) Threshold N of maximum allowed number of crossed translation points;

l) Additional Trace Information Requested Indicator (SRVR Requested);

m) List of Translation Points — used to check for translation loops and whether or not the threshold number of translations is exceeded.

B.2.2.2 *SCCP Routing Verification Acknowledgement (SRVA) Message*

The SRVA message is the standard message sent in response to an associated SRVT message. It carries the results of the test and is sent back using either direct routing on the Originating Point Code (OPC) or by global title translation on the Near End Global Title. Both addresses are found from the original message to which the SRVA is responding. The Destination Point Code (DPC) in the routing label may be dependent upon a global title translation if the MTP Backward Routing Indicator in the SRVT message is not set.

The message contains:

a) Information Indicating SRVA;

b) SRVR sent indicator;

c) Result of test.

This last field contains the following information:

— Success (no error indication);

— Partial Success (at least one SRVA indicating success or partial success); or

— Failure.

In the case of partial success or failure, some or all of the following failure reasons are provided:

i) No translation data exists for the GTI + GT at Translation Signalling Point.

ii) Incorrect translation for PPC + SSN at Translation Signalling Point.

iii) Incorrect translation for SPC + SSN at Translation Signalling Point.

iv) Incorrect intermediate translation for next translation point at Translation Signalling Point.

v) SRVT message arrived at wrong Signalling Point (Not duplicate or mated).

vi) The primary destination of the GT address does not serve GTI + GT as the primary destination.

vii) The secondary destination of the GT address does not serve GTI + GT as the secondary destination.

viii) The primary destination of the GT address does not recognize the SPC + SSN as the secondary destination for the GTI + GT.

ix) The secondary destination of the GT address does not recognize the PPC + SSN as the primary destination for the GTI + GT.

x) Timeout waiting for SRVA message.

xi) Inability to send message due to inaccessibility (network congestion or blockage).

xii) Detected loop at signalling point.

xiii) Exceeded threshold of N translations at signalling point.

xiv) Routing problem — Run MRVT.

xv) Unknown Initiator — NEGT (reverse routing to be done using OPC).

xvi) Test cannot be run due to local conditions.

B.2.2.3 *SCCP Routing Verification result (SRVR) message*

The SRVR message is sent from a terminating SP to the initiator of the test when ‘‘Additional Trace Information Requested’’ indicator is set. It carries the results of the test with additional information on a failure. It is sent back using either direct routing on the Near End Point Code (NEPC) or by global title translation on the Near End Global Title (NEGT).

The message contains:

a) Information Indicating SRVR;

b) Result of test;

c) Information field.

The content of this information field depends on the result of the test. It contains:

i) If the result of the test is ‘‘success’’:

— the point codes of the crossed SCCP Relay Nodes contained in the SRVT message.

ii) If the result of the test is ‘‘detected loop’’:

— the point codes of the SCCP Relay Nodes which are in the loop.

iii) If the result of the test is ‘‘detected excessive length route’’:

— the point codes of crossed SCCP Relay Nodes contained in the SRVT message.

iv) If the result of the test is ‘‘unknown destination point code’’:

— no additional information.

v) If the result of the test is ‘‘SRVT not sent due to inaccessibility’’:

— the point code of the inaccessible SP.

vi) If the result of the test is ‘‘SRVA not received’’:

— the identity of the SP(s) from which an SRVA was not received when expected.

vii) If the result of the test is ‘‘unknown initiator point code’’:

— the point code of the SP returning an SRVA to cause the MRVR to be sent.

viii) If the result of the test is ‘‘test cannot be run due to local conditions’’:

— no additional information.

ix) If any other failure result:

— the point codes of the crossed SCCP Relay Nodes contained in the SRVT message.

B.2.3 *Test initiation*

The procedure is started when there is an input from OA&M (SMAP) resulting in the sending of an SRVT message. The test is initiated:

a) When new SCCP routing data is introduced. Each global title translation should pass the SRVT before being opened to traffic.

b) When SCCP translation data is changed.

c) On receipt of an SRVT message.

d) On demand from local maintenance staff or an operations and maintenance centre.

e) Periodically at a Signalling Point to detect cases of mutilation of translation data. The period is network dependent and should be such that the load on the network is not seriously increased.

B.2.4 *Procedures*

The capability to execute a complete SCCP Routing Verification Test (SRVT) is found in three procedures. These procedures are organized by the function of the Signalling Point in which they reside for a given test instance. The procedures are partitioned into functions at the initiating point, functions at a translation point, and functions at the tested destination. The duplex translation procedures are found in the translation points.

B.2.4.1 *Initiating point*

The procedure is started when there is an input from OA&M as defined under the conditions of § B.2.3. It is initiated at an SP with SCCP capabilities in the network, and is triggered by an SRVT request. The SRVT request must include the Global Title of the tested destination. An SCCP Node cannot initiate an SRVT procedure for a test destination until any previous SRVT procedures for that destination have completed.

B.2.4.1.1 *Initial actions*

Upon receipt of an SRVT request on a given Global Title, the Near End Signalling Point (NESP) determines the location(s) of the initial translation from its tables. The NESP then begins a guard timing period, T2, and sends SRVT messages to the Translation Point Codes (TPCs) previously determined. The NESP then waits for SRVA messages corresponding to each SRVT sent.

If the NESP was identified as a Translation Signalling Point (TSP) for the respective Global Title, it performs the Global Title Translation, and follows the procedures defined at a translation point (§ B.2.4.2), depending upon the nature of the translation (i.e. intermediate or final).

B.2.4.1.2 *Subsequent actions*

Upon receipt of all SRVA messages, the guard timer, T2, is stopped and the test is complete. The results are reported to system management (SMAP) in accordance to the structure of the Result of Test parameters (§ B.2.2.2) and proper actions are taken to fix any problems. If the timer expires before receipt of an SRVA message, the result, Time out waiting for SRVA message (§ B.2.2.2. c.x), is reported to management (SMAP) along with the Point Code of the SP. There is no penalty for not receiving an SRVR. However, it is assumed, analogous to the MRVTs MRVR message, that the SRVR will return before the final SRVA.

B.2.4.2 *Translation point*

For the SRVT, two types of Translation Points exist: intermediate and final. The procedure at the Translation point differs only in the content of the SRVT messages which emerge. An intermediate translation point is an SP with SCCP functionality that has been specified at the NESP for the translation of the Global Title originally given. However, due to the nature of the Global Title, further translation at another SP is needed to determine the PC of the tested destination.

A final translation point is an SP with SCCP functionality that has been specified at the NESP or an ITSP for the translation of the Global Title. It performs the final translation which results in a Primary Point Code + Subsystem Number (PPC + SSN) and a Secondary Point Code + Subsystem Number (SPC + SSN) (optional). Note that the NESP does not know if it sends an SRVT message to an Intermediate or Final Translation Signalling Point.

B.2.4.2.1 *Upon Receipt of an SRVT message*

When a Translation Signalling Point (TSP) receives an SRVT message, it:

a) Attempts to translate the GTI + GT to the PPC + SSN and SPC + SSN (optional):

i) If the SP is unable to perform the translation, the Result of Test is equal to ‘‘No translation data exists’’. The SP sends an SRVR to the NESP, an SRVA message with SRVR sent indication and corresponding result parameter (§ B.2.2.2 c.i) to the OPC, and an indication to SMAP.

ii) If it recognizes that further translation is needed, a Translation Point Code (TPC) and a backup Translation Point Code (optional) are derived.

iii) If the translation is final and successful, the PPC + SSN and SPC + SSN (optional) are derived and retained for the SRVA message.

b) Checks for mated SCCP relay node:

i) If a mated SCCP relay node exists for the current TSP, a SRVT is sent to the mate so that it may perform duplicate translation for comparison purposes.

ii) If no mated SCCP Relay Node exists, the test proceeds with step c) below.

c) Examines the list of translation points (§ B.2.2.1 m):

i) If the point code of the next TSP or the point code of the mated SCCP Relay Node (optional) appears in the SRVT’s list of translation points, then the SP sends an SRVR to the NESP, an SRVA message with SRVR sent indication and an SCCP loop detected indication (§ B.2.2.2 c.xii) to the OPC, and an indication to SMAP. The test is stopped.

ii) If the number of point codes in the SRVT's list of translation points exceeds a predefined threshold number of translations, then the SP sends an SRVR to the NESP, the SP an SRVA message with SRVR sent indication and the threshold exceeded indication (§ B.2.2.2 c.xiii) to the OPC, and an indication to SMAP. The test is stopped.

iii) If any point code(s) of the next TSP or the mated SCCP Relay Node (Optional) does not appear in the SRVT's list of translation points, then the TSP will add both its own point code and the point code of the mated SCCP Relay Node (if any) to the list of translation points.

d) Attempts to send an SRVT message to the next TPC or tested destination (from a) above):

i) If the TSP is unable to send the SRVT due to inaccessability (network congestion or blockage), the TSP sends an SRVR to the NESP, an SRVA with SRVR sent indication and corresponding result parameter (§ B.2.2.2 c.xi) to the OPC and an indication to SMAP. The test is stopped.

ii) If the TSP is unable to send the SRVT due to an MTP routing problem, the TSP sends an SRVR to the NESP, an SRVA with SRVR sent indication and the corresponding result parameter (§ B.2.2.2 c.xiv) to the OPC and an indication to SMAP. The test is stopped.

iii) If the TSP is unable to send the SRVT due to local conditions, the TSP sends an SRVR to the NESP, an SRVA with SRVR sent indication and the corresponding result parameter (§ B.2.2.2 c.xvi) to the OCP and an indication to SMAP. The test is stopped.

iv) If an SRVT may be sent, a guard timer, T2, is started and SRVT message(s) are sent to either the next TPC(s) or the PPC — SSN and SPC + SSN (optional) resulting from attempted translation. This timer is the guard for SRVA(s) received in response to both the Compare and No Compare SRVT messages.

B.2.4.2.2 *Subsequent actions*

Upon receipt of an SRVA message, the following actions are taken:

a) If all of the SRVA(s) in response to the SRVT(s) have not yet been received, the results are stored, waiting for pending SRVA(s).

b) If all other expected SRVA(s) have been received, the following actions are taken:

i) The guard timer, T2, is stopped.

ii) The reverse Global Title Translation is performed on the NEGT to determine the Originating Point Code (OPC). This may be considered optional in networks which perform reverse routing on OPC (known from e.g. Network Identifier) instead of Global Title Translation. If the NEGT is not recognized, an SRVA is retured to the previous PC with the ‘‘Unknown Initiator’’ indication (§ B.2.2.2 c.xv).

iii) Results of the duplicate translation comparison are incorporated into the Result of Test parameters (§ B.2.2.2). This is optional in networks not subscribing to the concept of mated SCCP Relay Nodes and duplicate translations. If the SRVA in response to the SRVT has not yet been received, the ITSP will wait for it up to the expiration of the timer.

iv) If the SRVR send indication is not set and an SRVR has been requested, the SP sends an SRVR message with appropriate indications from the SRVA.

v) The SP sends an SRVA message in response to the original SRVT message. The complete result of test parameter list is retained and the SRVR sent indication is set appropriately.

c) If the timer has already expired, the message is discarded.

If the guard timer expires before receipt of the SRVA(s) responding to the SRVT(s), results of the duplicate translation comparison are incorporated into the Result of Test parameters (if available) and an SRVA is sent back with the ‘‘Timeout waiting for SRVA message’’ response (§ B.2.2.2 c.x). Any SRVAs received after the timer expires will be discarded. If an SRVA cannot be sent, no further action is taken.

B.2.4.2.3 *Duplex translation (optional)*

When a TSP receives an SRVT message, it:

a) Checks to determine if the originating SP is a mated SCCP Relay Node to the receiving SP. If not, an SRVA is returned with ‘‘SRVT arrived at wrong SP’’ (§ B.2.2.2 c.v).

b) Attempts to translate GTI + GT and compares the results with the point code information contained in the SRVT message:

i) If the results of the duplicate translation match the data in the SRVT message from the previous translation, an SRVA message is returned with Result of Test equal to success (§ B.2.2.2 c).

ii) If no translation data exists for the Global Title, then an SRVA message is returned with the result ‘‘No translation data exists for the GTI + GT’’ (§ B.2.2.2 c.i).

iii) If the results of the duplicate translation do not match the data in the SRVT message from the previous translation, an SRVA message is returned with Result of Test equal to either ‘‘Incorrect intermediate translation’’ (§ B.2.2.2 c.iv), ‘‘Incorrect translation for PPC + SSN’’ (§ B.2.2.2 c.ii) or ‘‘Incorrect translation for SPC + SSN’’ (§ B.2.2.2 c.iii).

B.2.4.3 *Tested destination*

The tested destination is an SP with SCCP functionality that has been specified at the FTSP by use of Global Title Translation. The address is referred to as either the Primary Point Code (PPC) or Secondary Point Code (SPC).

B.2.4.3.1 *Primary point*

This procedure is performed at the primary destination signalling point derived from the global title translation. When the destination receives an SRVT message, it verifies the PPC + SSN serves as the primary destination for the GTI + GT. The following action should result:

a) If the test is successful, the SP sends an SRVR (if requested) with success indication to the NESP, an SRVA with SRVR sent indication and success indication to the OPC, and an indication to SMAP.

b) If the Signalling Point does not serve GTI + GT as the primary destination, the test is unsuccessful and the SP sends an SRVR to the NEPC, an SRVA with the SRVR sent indication set appropriately and the corresponding Result of Test parameter (§ B.2.2.2 c.vi) to the OPC, and an indication to SMAP.

c) If the Signalling Point does not recognize SPC + SSN as the secondary destination for GTI + GT, then the test is unsuccessful and the SP sends an SRVR to the NEPC, an SRVA with the SRVR sent indication set appropriately and the corresponding Result of Test parameter (§ B.2.2.2 c.viii) to the OPC, and an indication to SMAP.

If an SRVA cannot be sent, no further action is taken.

B.2.4.3.2 *Secondary point*

This procedure is performed at the secondary destination signalling point (optional) derived from the global title translation. When the destination receives an SRVT message, it verifies the SPC + SSN serves as the secondary destination for the GTI + GT. The following action should result:

a) If the test is successful, the SP sends an SRVR (if requested) with success indication to the NESP, an SRVA with SRVR sent indication and success indication to the OPC, and an indication to SMAP.

b) If the Signalling Point does not serve GTI + GT as the secondary destination, the test is unsuccessful and the SP sends an SRVR to the NESP, an SRVA with the SRVR sent indication set appropriately and the corresponding Result of Test parameter (§ B.2.2.2 c.vii) to the OPC, and an indication to SMAP.

c) If the Signalling Point does not recognize SPC + SSN as the primary destination for GTI + GT, then the test is unsuccessful and the SP sends an SRVR to the NESP, an SRVA with the SRVR sent indication set appropriately and the corresponding Result of Test parameter (§ B.2.2.2 c.ix) to the OPC, and an indication to SMAP.

If an SRVA cannot be sent, no further action is taken.

B.3 *State transition diagram*

Figure B-1/Q.795 shows the state transition diagram for the SRVT using SDL.

Figure B-1/Q.795 (sheet 1 of 4), p.

Figure B-1/Q.795 (sheet 2 of 4), p.

Figure B-1/Q.795 (sheet 3 of 4), p.

Figure B-1/Q.795 (sheet 4 of 4), p.

B.4 *Example*

Figure B-2/Q.795 demonstrates the SRVT. It should be noted that the Signalling Points shown are assumed to be SCCP adjacent and NOT physically adjacent. Furthermore, all examples show both a primary and secondary destination. The secondary result may be considered optional.

Figure B-2/Q.795, p.

MONTAGE: PAGE 542 = BLANCHE