Superseded by a more recent version

INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

E.411

(10/96)

SERIES E: TELEPHONE NETWORK AND ISDN

Quality of service, network management and traffic engineering – Network management – International network management

---

International network management – Operational guidance

ITU-T Recommendation E.411

Superseded by a more recent version

(Previously CCITT Recommendation)

Superseded by a more recent version

ITU-T E-SERIES RECOMMENDATIONS

TELEPHONE NETWORK AND ISDN

OPERATION, NUMBERING, ROUTING AND MOBILE SERVICES	
INTERNATIONAL OPERATION	E.100–E.229
OPERATIONAL PROVISIONS RELATING TO CHARGING AND ACCOUNTING IN THE INTERNATIONAL TELEPHONE SERVICE	E.230–E.299
UTILIZATION OF THE INTERNATIONAL TELEPHONE NETWORK FOR NON-TELEPHONY APPLICATIONS	E.300–E.329
ISDN PROVISIONS CONCERNING USERS	E.330–E.399
QUALITY OF SERVICE, NETWORK MANAGEMENT AND TRAFFIC ENGINEERING	
NETWORK MANAGEMENT	E.400–E.489
International service statistics	E.400–E.409
International network management	**E.410–E.419**
Checking the quality of the international telephone service	E.420–E.489
TRAFFIC ENGINEERING	E.490–E.799
Measurement and recording of traffic	E.490–E.505
Forecasting of traffic	E.506–E.509
Determination of the number of circuits in manual operation	E.510–E.519
Determination of the number of circuits in automatic and semi-automatic operation	E.520–E.539
Grade of service	E.540–E.599
Definitions	E.600–E.699
ISDN traffic engineering	E.700–E.749
Mobile network traffic engineering	E.750–E.799
QUALITY OF TELECOMMUNICATION SERVICES: CONCEPTS, MODELS, OBJECTIVES AND DEPENDABILITY PLANNING	E.800–E.899
Terms and definitions related to the quality of telecommunication services	E.800–E.809
Models for telecommunication services	E.810–E.844
Objectives for quality of service and related concepts of telecommunication services	E.845–E.859
Use of quality of service objectives for planning of telecommunication networks	E.860–E.879
Field data collection and evaluation on the performance of equipment, networks and services	E.880–E.899

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

Superseded by a more recent version

ITU-T RECOMMENDATION E.411

INTERNATIONAL NETWORK MANAGEMENT – OPERATIONAL GUIDANCE

Summary

Network management requires real-time monitoring of current network status and performance and the ability to take prompt action to control the flow of traffic when necessary (see Recommendation E.410). Operational guidance to meet these requirements, including a description of status and performance parameters, traffic controls and the criteria for their application are included in this Recommendation. It should be noted that the complete range of parameters and traffic controls are not necessary for the introduction of a limited network management capability, however a comprehensive selection will bring substantial benefit (see clause 5/E.410). In addition, some guidance on beginning network management is provided, along with information on developing a network management centre and the use of common channel signalling for network management purposes.

Source

ITU-T Recommendation E.411 was revised by ITU-T Study Group 2 (1993-1996) and was approved under the WTSC Resolution No. 1 procedure on the 8th of October 1996.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1 (Helsinki, March 1-12, 1993).

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

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

CONTENTS

Recommendation E.411

INTERNATIONAL NETWORK MANAGEMENT – OPERATIONAL GUIDANCE

(revised in 1996)

1 Introduction

Network management requires real-time monitoring of current network status and performance and the ability to take prompt action to control the flow of traffic when necessary (see Recommendation E.410). Operational guidance to meet these requirements, including a description of status and performance parameters, traffic controls and the criteria for their application are included in this Recommendation. It should be noted that the complete range of parameters and traffic controls are not necessary for the introduction of a limited network management capability, however a comprehensive selection will bring substantial benefit (see clause 5/E.410). In addition, some guidance on beginning network management is provided, along with information on developing a network management centre and the use of common channel signalling for network management purposes.

2 Information requirements

2.1 Network management requires information of where and why difficulties are occurring or are likely to occur in the network. This information is essential to identify the source and effect of a difficulty at the earliest possible time, and will form the basis for any network management action which is taken.

2.2 The information relating to current difficulties can be obtained from:

a) real-time surveillance of the status and performance of the network;

b) information from telephone operators as to where they are experiencing difficulties; or where they are receiving customer complaints of difficulties;

c) transmission system failure indicators and planned outage reports (these reports need not relate only to the network local to one Administration, but should reflect the whole international network);

d) international or national exchange failures and planned outage reports;

e) news media reports detailing unforeseen events which stimulate traffic (for example, natural disasters).

2.3 The information relating to difficulties which are likely to occur in the future will be obtained from:

a) reports of future planned outages of transmission systems;

b) reports of future planned outages of international or national exchanges;

c) knowledge of special events (for example, international sporting events, political elections);

d) knowledge of national holidays and festivals (e.g. Christmas Day, New Year's Day);

e) an analysis of past network performance.

2.4 The system availability information point, defined in Recommendation M.721, will provide a ready source for much of the information indicated above.

3 Network status and performance data

3.1 In order to identify where and when difficulties are occurring in the network, or are likely to occur, data will be required which will indicate the status and measure the performance of the network. Such data will require real-time collection and processing, and may require the use of thresholds (see 5.1).

3.2 Data may be collected in various ways which include counters in electromechanical exchanges which can be read manually when required (e.g. during periods of heavy traffic or special events), data output reports from SPC exchanges, or computerized network management operations systems which can collect and process data from a large number of exchanges.

3.3 Network status/performance information includes information on the status of exchanges, circuit groups, common channel signalling systems and transmission equipment. This status/performance information can be provided by one or more types of displays. These may include printers, video displays, and/or indicators/graphical representation on a display board or network management console. To be useful, network status indicators should be available as rapidly as possible.

3.3.1 Exchange status information includes the following:

– *Load measurements* – These are provided by attempt counts, usage or occupancy data, data on the percent of real-time capacity available (or in use), blocking rates, percentage of equipment in use, counts of second trials, etc.

– *Congestion measurements* – These are provided by measurements of the delay in serving incoming calls, holding times of equipment, average call processing and set-up time, queue lengths for common control equipment (or software queues), and counts of equipment time-outs, etc.

– *Service availability of exchange equipment* – This information will show when major items of equipment are made busy to traffic. This could highlight a cause of difficulty or give advance warning that difficulties could arise if demand increases.

– *Congestion indicators* – In addition to the above, indicators can be provided by SPC exchanges which show the degree of congestion. These indicators can show:

  - moderate congestion: level 1;
  - serious congestion: level 2;
  - unable to process calls: level 3.

  NOTE – While this is desirable, SPC exchanges may not be able to provide a level 3 indicator during catastrophic failures.

– *Network management control status indicators* – Indicators can be provided to show controls that are active throughout a time interval, such as 30 seconds, or on occurrence to show controls that are added or deleted.

The availability of specific exchange status information will depend on the switching technology employed by each Administration. Details of exchange measurements are found in Recommendations E.502 and Q.544.

3.3.2 Circuit group status information relates to the following:

– status of all circuit groups available to a destination;

– status of individual circuit sub-groups in a circuit group;

– status of circuits on each circuit group.

Status indicators can be provided to show when the available network is fully utilized by indicating:

– when all circuits in a circuit group are busy;

– when all circuits in a circuit sub-group are busy;

– when all circuit groups available to a destination are busy.

This would indicate that congestion is present or imminent. Status information can be provided to show the availability of the network for service, by reporting the number or percentage of circuits on each circuit group that are made busy or are available for traffic.

This information could identify the cause of difficulty or give advance warning that difficulties may arise as the demand increases.

An indicator should be provided to alert network managers, when the configuration or routing data is changed, for example, when a circuit group is deleted.

3.3.3 Common channel signalling system status provides information that will indicate failure or signalling congestion within the system. It includes such items as:

– receipt of a transfer prohibited signal (Signalling Systems Nos. 6 and 7);

– initiation of an emergency restart procedure (Signalling System No. 6);

– presence of a signalling terminal buffer overflow condition (Signalling System No. 6);

– signal link unavailability (Signalling System No. 7);

– signal route unavailability (Signalling System No. 7);

– destination inaccessible (Signalling System No. 7).

This information may identify the cause of difficulty or give advance warning that difficulties may arise as the demand increases. Details are shown in Recommendations E.415 and E.505.

3.3.3.1 Network management actions may help to reduce congestion in common channel signalling systems by reducing traffic being offered to common channel signalling circuit groups, or by diverting traffic to conventional signalling circuit groups.

3.4 Network performance data should relate to the following:

– traffic performance on each circuit group;

– traffic performance to each destination;

– effectiveness of network management actions.

It may also be desirable to assemble performance data in terms of circuit group and destination combinations and/or traffic class (for example, operator-dialled, subscriber-dialled, transit). (See 2.1/E.412.)

3.5 Data collection should be based on a system of measurement which is either continuous or of a sufficiently rapid sampling rate to give the required information. For example, for common control switching equipment, the sampling rate may need to be as frequent as every second.

Reports on network status and performance should be provided periodically, for example, on a 3-minute, 5-minute, 15-minute, 30-minute or hourly basis, with the more frequent reports usually being more useful. However, the more frequent reports may produce erratic data due to the peakedness of traffic, especially on small circuit groups. Data reports compiled by a network management operations system take on added value in that a more global view of network performance is provided.

3.5.1 Information of critical status or alert such as common channel signalling failures, exchange congestion, etc. should be made available to network managers at a relatively fast frequency, for example, on a 30-second basis, or on an occurrence basis. Such information is typically true/false indication, rather than quantitative measurement. The indication can be classified into two categories: status and alert. Status indication shows a condition that holds throughout a time interval, such as 30 seconds, whereas alert indication shows a change of condition that occurs at a moment within a time interval. For example, a Temporary Alternative Routing (TAR) control being active is a status indication; a TAR control being added or deleted is an alert indication.

Distinct true/false indications and their correlations can be shown all together in a simple display, which helps network managers quickly identify the causes of network problems.

A very powerful means to obtain real-time status and performance information at destination level is that based on call record data, which allow to analyse and possibly correlate call attempts which were successful or failed. This information can be useful, for example, in HTR determination.

A subpart of the call records is the call failure records, i.e. any call not receiving an answer back (B-answer signal). Call failure records are provided in "real-time" by switches as they occur, with data on status and performance of individual traffic streams that is essential for:

- the correct determination of location and nature of traffic failures or abnormalities;
- the choice of the optimal NM control to apply in the network;
- the monitoring of the effectiveness of NM controls.

Main information in the call failure records to be reported to the network manager is:

- recording switch;
- date and time of failure;
- failure reason (as perceived by switch's call processing logic and/or as a result of a received signalling message) along with POTS and in particular for ISDN these five:
  1) failed due to transmission medium requirements;
  2) failed due to ISUP preference indicator;
  3) failed due to external congestion;
  4) failed due to internal congestion;
  5) failed due to subscriber faults.
- digits received/transmitted;
- incoming and/or outgoing circuit group;
- incoming and/or outgoing circuit;
- type of signalling being used at time of failure, and other relevant data dependent on the used type of signalling;
- service type (see 2.1/E.412);
- A-subscriber number (if available);
- other common equipment components (based on vendor-specific architectural components).

Details of the call records analysis can be found in Recommendations E.502, E.503 and E.491.

3.6 The network performance data is generally expressed in parameters which help to identify difficulties in the network. Among these parameters are:

3.6.1 percentage overflow (% OFL): % OFL indicates the relationship between the total bids offered to a circuit group or destination, in a specified period of time, and the quantity of bids not finding a free circuit. It will, therefore, give an indication of the overflow from one circuit group to another, or the bids which fail because all circuit groups to a destination are busy.

% OFL =
Error! × 100

3.6.2 bids per circuit per hour (BCH)[1]: BCH is an indication of the average number of bids per circuit, in a specified time interval. It will therefore identify the demand and, when measured at each end of a both-way operated circuit group, will identify the direction of greater demand.

BCH = **Error!**

It is not necessary to accumulate data for an hour to calculate BCH. However, the calculated BCH must be adjusted when data accumulation is less than hourly. For example, the bids should be doubled if 1/2 hour data is used. The result would be BCH for the data collection period.

3.6.3 answer seizure ratio (ASR): ASR gives the relationship between the number of seizures that result in an answer signal and the total number of seizures. This is a direct measure of the effectiveness of the service being offered onward from the point of measurement and is usually expressed as a percentage as follows:

ASR = **Error!** × 100

Measurement of ASR may be made on a circuit group or on a destination basis.

3.6.4 answer bid ratio (ABR): ABR gives the relationship between the number of bids that result in an answer signal and the total number of bids. ABR may be made on a circuit group or on a destination basis.

ABR = **Error!** × 100

ABR is expressed as a percentage and is a direct measure of the effectiveness of traffic onward from the point of measurement. It is similar to ASR except that it includes bids that do not result in a seizure.

3.6.5 seizures per circuit per hour (SCH)[1]: SCH is an indication of the average number of times, in a specified time interval, that each circuit group is seized. When related to the expected values of average call holding times and effective call/seizure rate for the circuit group, it will give an indication of the effectiveness of the service being offered.

SCH = **Error!**

It is not necessary to accumulate data for an hour to compute SCH. (See 3.6.2 – BCH.)

3.6.6 occupancy: Occupancy can be represented in units, for example: erlangs, hundred-call-seconds or as a percentage. It can be measured as a total for a destination or for a circuit group and as an average per circuit on a circuit group. Its use for network management purposes is to show usage and to identify unusual traffic levels.

---

[1] International networks contain one-way and both-way operated circuits, and their traffic flow characteristics are inherently different. This difference needs to be taken into account when calculating BCH and SCH by either:

i) multiplying the number of one-way circuits by 2 to derive an equivalent number of both-way circuits; or

ii) dividing the number of both-way circuits by 2 to derive an equivalent number of one-way circuits.

When analyzing BCH and SCH data, and when BCH and SCH data are exchanged between Administrations, it is essential that the method used is understood so that erroneous conclusions may be avoided.

3.6.7 mean holding time per seizure: This is the total holding time divided by the total number of seizures and can be calculated on a circuit group basis or for switching equipment.

3.6.8 busy-flash seizure ratio (BFSR): BFSR gives the relationship between the number of seizures that result in a "busy-flash" signal (or its equivalent) and the total number of seizures. Measurement of BFSR is usually made on a circuit group basis.

BFSR = **Error!** × 100

NOTE – The source of "busy-flash" signals, or their equivalent, will vary with the signalling system used. Therefore, the calculated BFSR on individual circuit groups may naturally be different, and as a result, caution should be used when comparing BFSR among circuit groups.

3.7 The number of parameters possible or necessary for particular Administration purposes will depend upon a variety of factors. These will include:

a) the data available at an exchange;

b) the particular routing arrangements employed (for example, SCH and BCH relate to circuit group performance only; ABR, ASR, and % OFL can relate to circuit group or destination performance);

c) the interrelationships which exist between the parameters (for example, SCH can give similar indications to ASR – see 3.6.5 above).

3.8 The correlation between transmission and switching alarms (e.g. failure, congestion) can assist Network Management and Restoration control activities (see Recommendation E.413).

The provision of transmission network supervision information will guide the application of network management controls and may also be useful to the restoration control point (see Recommendation M.725) in setting priorities for restoration. The provision of such timely information will enable the network manager to be in a position to understand and control/reconfigure the network and traffic flows immediately rather than react to traffic congestion or poor performance after it occurs. This function can be assisted by the development of knowledge-based systems capable of using a model of the network, the present network status and a history of previous network incidents, to suggest possible control/reconfigure options.

3.8.1 Transmission equipment status and performance information should separately identify network element and network element managers, where possible/applicable, and include the following:

– network element identity;

– error performance/Quality of Service indicators (BER: see Recommendation G.821, Availability: see Recommendation G.106, Bit Utilization, Dynamic Load control, etc.);

– network element load (e.g. processor load);

– network element status (includes Mode of Operation, Failed, Degraded Service, Systems affected);

– Restoration Mode (identity of network element used for restoration).

Such parameters can also provide information for the resource management of Digital Transmission Equipment (DTE) facilities. Standardization of the indicators from DTE such as Digital Circuit Multiplication Equipment (DCME) and Digital Cross Connect (DCC) systems is a recognized requirement.

3.8.2 Within a modern network, network surveillance is necessary for integrated service management. Accordingly, a transmission monitoring system is required to provide centralized alarm collection and performance monitoring to enable the network manager to react immediately and identify the network element likely to affect traffic.

Such a system should be capable of interfacing to a network management system, via a standard interface, (see Recommendation M.3010). It should interface to network elements to enable:

– the capture of network alarms and performance information and the relaying of such information, in an intelligent form, to a centralized network management centre;

– the association of transmission alarms on a site basis (if applicable);

– processing to provide alarms and alarm reports to the duty responsible;

– filtering out of lower level alarms in favour of higher order ones;

– the association of circuits/routes/systems with network elements, such as DCME and DCC systems, and an indication of the effect of element failure on performance.

4 Interpretation of parameters

The interpretation of parameters on which network management actions are based can most conveniently be made by considering the originating international exchange as the reference point (see Figure 1).

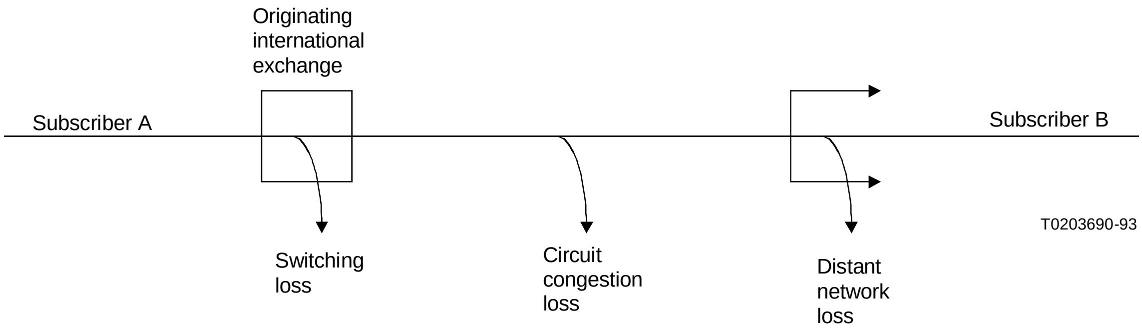

FIGURE 1/E.411

From this reference point, the factors which affect call completion can broadly be divided into three main components:

a) switching loss (near-end loss);

b) circuit congestion loss (near-end loss);

c) distant network loss (far-end loss).

4.1 Switching loss

Switching loss may be due to:

1) common equipment or switchblock congestion, or queue overflows or processor overloads;

2) failures in incoming signalling;

3) subscriber/operator dependent errors, such as insufficient or invalid digits, premature call abandonment, etc.;

4) routing errors, such as barred transit access;

5) other technical failures.

Guidance to the identification of switching loss can be obtained from 3.3.

4.2 Circuit congestion loss

This loss will depend on:

1) the number of circuits available for a destination;

2) the level of demand for that destination; and

3) the traffic performance on the circuit groups to that destination.

Indication that circuit congestion loss may occur can be obtained from the status information detailed in 3.3.2 above.

Circuit congestion loss can be identified by any of the following:

– percentage overflow (see 3.6.1);

– a difference between the "bids per circuit per hour" and "seizures per circuit per hour" measurements on the final circuit group (see 3.6.2 and 3.6.5);

– a difference between the "answer bid ratio" and the "answer seizure ratio" (see 3.6.4 and 3.6.3).

It should be noted that for both-way operated circuit groups, excessive demand in the incoming direction may also cause circuit congestion loss. This can be identified by comparing incoming and outgoing bids, seizures or occupancy.

4.3 Distant network loss

Distant network loss may be divided into:

1) *technical loss:* due to distant exchange and national circuit faults;

2) *subscriber dependent loss:* due to subscriber B busy, no answer, invalid distant number, number unavailable, etc.;

3) *traffic dependent loss:* these losses are due to lack of distant network capacity to meet traffic demand.

Under normal conditions, and for a large sample measured over a long period, distant network loss can be said to have a fixed or ambient overhead loss (this value depends on destination with some hour-by-hour and day-by-day variations).

Under abnormal situations (heavy demand, failures, etc.) distant network losses can be significantly affected. Variations in distant network loss can be identified by any of the following:

– answer seizure ratio (see 3.6.3) (this is a direct measurement);

– seizures per circuit per hour (see 3.6.5) (this is an indirect measurement);

– mean holding time per seizure (see 3.6.7) (this is an indirect measurement);

– busy-flash seizure ratio (see 3.6.8) (this is a direct measurement).

5 Criteria for action

5.1 The basis for the decision on whether any network management action should be taken will depend upon real-time information on the status and performance of the network. It is advantageous if the output of this information can be initially restricted to that which is required to identify possible difficulties in the network. This can be achieved by setting threshold values for performance parameters, and for the number or the percentage of circuits and common control equipment which are in service, such that when these threshold values are crossed, network management action can be considered. These threshold values will represent some of the criteria by which decisions are reached.

5.2 Indications that a threshold has been crossed and "all circuits on a circuit group are busy" and "all circuit groups to a destination are busy" may be used to direct attention to the particular area of the network for which detailed performance information will then be required.

5.3 The decision on whether or not to take network management action, and what action will be taken, is the responsibility of the network management personnel. In addition to the criteria mentioned above, this decision will be based on a number of factors, which could include:

– a knowledge of the source of the difficulty;

– detailed performance and status information;

– any predetermined plans that exist (see Recommendation E.413);

– experience with and knowledge of the network;

– routing plan employed;

– local traffic patterns;

– ability to control the flow of traffic (see Recommendation E.412).

This personnel is responsible for ensuring that conventional network management controls, once activated, are not left unsupervised.

6 Network management actions

6.1 General

Network management actions fall into two broad categories:

a) "expansive" actions, which are designed to make available lightly loaded parts of the network to traffic experiencing congestion;

b) "protective" actions, which are designed to remove traffic from the network during congestion which has a low probability of resulting in successful calls.

Normally, the first choice response to a network problem would be an expansive action. Protective actions would be used if expansive actions were not available or not effective.

Network management actions may be taken:

– according to plans which have been mutually agreed to between Administrations prior to the event (see Recommendation E.413);

– according to ad hoc arrangements agreed to at the time of an event (see Recommendation E.413);

– by an individual Administration wishing to reduce its traffic entering the international network, or to protect its own network.

6.2 Expansive actions

Expansive actions involve the rerouting of traffic from circuit groups experiencing congestion to other parts of the network which are lightly loaded with traffic, for example, due to differences in busy hours.

Examples of expansive actions are:

a) establishing temporary alternative routing arrangements in addition to those normally available;

b) in a country where there is more than one international exchange, temporarily reorganizing the distribution of outgoing (or incoming) international traffic;

c) establishing alternative routings into the national network for incoming international traffic;

d) establishing alternative routings to an international exchange in the national network for originating international traffic.

The protective action of inhibiting one direction of operation of both-way circuits [see 6.3 a)] can have an expansive effect in the other direction of operation.

6.3 Protective actions

Protective actions involve removing traffic from the network during congestion which has a low probability of resulting in successful calls. Such traffic should be removed as close as possible to its origin, thus making more of the network available to traffic which has a higher probability of success.

Examples of protective actions are:

a) *Temporary removal of circuits from service (circuit busying)* – This action may be taken when a distant part of the network is experiencing serious congestion.

NOTE – In the case of both-way circuits, it may only be necessary to inhibit one direction of operation. This is called directionalization.

b) *Special instructions to operators* – For example, such instructions may require that only a limited number of attempts (or none at all) be made to set up a call via a congested circuit group or exchange, or to a particular destination experiencing congestion.

c) *Special recorded announcements* – Such announcements may be connected at an international or national exchange and, when there is serious congestion within part of the network, would advise customers (and/or operators) to take appropriate action.

d) *Inhibiting overflow traffic* – This action prevents traffic from overflowing onto circuit groups or into distant exchanges which are already experiencing congestion.

e) *Inhibiting direct traffic* – This action reduces the traffic accessing a circuit group in order to reduce the loading on the distant network.

f) *Inhibiting traffic to a particular destination (code blocking or call gapping)* – This action may be taken when it is known that a distant part of the network is experiencing congestion.

g) *Circuit reservation* – This action reserves the last few idle circuits in a circuit group for a particular type of traffic.

6.4 Information on the network management controls (and their method of activation) which can be used for expansive and protective actions is found in Recommendation E.412.

6.5 Actions during disasters

6.5.1 Disasters whether man-made or natural can result in damage to the telephone network, they can give rise to heavy calling, or both.

6.5.2 A single point of contact for network-related information should be established to prevent confusion, duplication of effort, and to ensure an orderly process of returning communications to normal. It is recommended that the single point of contact be the network management implementation and control point (see clause 4/E.414) within the Administration affected by the disaster.

6.5.3 The role of the network management implementation and control point may vary depending on the size or impact of a disaster. However, the following are functions which may be required:

– assess the impact of the disaster on the network (transmission systems, exchanges, circuit groups, destination codes, isolated destinations);

– provide status information, as appropriate, to:
  i) operator services;
  ii) public relations and media;
  iii) government agencies;
  iv) other network management implementation and control points.
– develop and implement control strategies (expansive and protective);
– assist in determining the need for, and locating, technical equipment to restore communications.

7 Exchange of information

7.1 Effective network management requires good communications and cooperation between the various network management elements within an Administration and with similar elements in other Administrations (see Recommendation E.414). This includes the exchange of real-time information as to the status and performance of circuit groups, exchanges and traffic flow in distant locations.

7.2 Such information can be exchanged in a variety of ways, depending on the requirements of the Administrations. Voice communications can be established between or among network management centres using dedicated service circuits or the public telephone network. Certain signals may be related to the exchange status (as for the switching congestion indicators), to the status of the destination (as for Hard-to-Reach information) and to information concerning the previous routing of the call, which may imply a particular handling when specific NM controls are activated (as for TAR and rerouted calls indicators), see also Recommendation E.412. These may be transported directly by the common channel signalling system. (See Recommendation Q.297 for Signalling System No. 6 and Recommendations Q.722, Q.723, Q.724, Q.762, Q.763 and Q.764 for Signalling System No. 7.) Larger data exchange requirements on a regular basis may be supported by the Telecommunications Management Network (TMN) (see Recommendation M.3010) or by use of a packet switched network capability. The transfer of smaller amounts of data on an infrequent basis may be supported by telex or similar media, or by facsimile.

7.3 Guidance on the use of common channel signalling for network management

7.3.1 Common channel signalling systems provide a fast and reliable means of transferring network management operational signals between exchanges. An example is the transfer of exchange congestion status signals for the Automatic Congestion Control (ACC) system (see 3.1/E.412). These signals should be given a high priority in common channel signalling flow control. Specific details on the application of network management operational signals in Signalling System No. 6 are found in Recommendation Q.297. In the case of Signalling System No. 7, the details for the Telephone User Part (TUP) are found in Recommendations Q.722, Q.723 and Q.724, and the ISDN User Part (ISUP) are found in Recommendations Q.762, Q.763 and Q.764.

7.3.2 Signalling System No. 7 may also be used to transfer network management data and status information between an exchange and its network management operations system, and between network management operations systems. It should be noted that in these applications, the volume of data to be transferred can be quite large and its frequency of transmission can be as high as every three minutes. When this data is transferred over signalling links which also handle user signalling traffic, stringent safeguards must be adopted to minimize the risk of signalling system overloads during busy periods when both user signalling traffic and network management data transmissions are at their highest levels. These safeguards include the following:

- limiting the amount of network management information to be transferred on signalling links which also carry user signalling messages;
- using dedicated signalling links for network management purposes;
- using the Telecommunications Management Network (TMN), or the Operations and Maintenance Application Part (OMAP) in Signalling System No. 7 (for further study);
- developing appropriate flow control priorities for network management information (for further study);
- equipping the network management operations system in such a way that it can respond to signalling system flow control messages.

8 Beginning network management

The introduction of network management into an existing network should be viewed as a long-term project. This long period is required:

- to gain knowledge and experience of network management;
- to carry out studies on the requirements of an individual network;
- to write specifications for network management requirements in present and future telephone exchanges and to hold discussions with manufacturers;
- to oversee the introduction of facilities and to organize and train suitable network management staff;
- to introduce limited facilities in existing older technology exchanges.

A rational approach would consist in first using existing limited facilities to manage the network, while at the same time developing full network management facilities with the introduction of modern Stored Program Control (SPC) exchanges.

8.1 Utilizing existing resources and capabilities

8.1.1 Responsibility

As an important first step, the responsibility for network management should be identified and assigned within an organization. This initial organization can then be expanded, as required, in accordance with Recommendation E.414.

8.1.2 Telephone operators

Operators are usually aware of problems as they occur in the network, and this information can reveal the need to control traffic. The operators can then be directed to modify their procedures to reduce repeated attempts, or to use alternative routings to a destination. They can also provide special information and/or instructions to customers and distant operators during unusual situations.

8.1.3 Exchange capabilities

Exchanges may have been provided with certain features which can be adapted for network management purposes. Data already available for maintenance or traffic engineering purposes could be used for network management, or could be made available through the addition of an interface unit. In addition, manually operated switches or keys can be provided in electromechanical exchanges to block certain destination codes or to change alternate routing. They can be provided separately for each item of common control equipment, thereby allowing flexible control of traffic to a destination.

The scope for network management in a telecommunications network may depend on the technology of the exchanges in that network. However, close examination of the manufacturers' specifications for SPC exchanges may reveal that certain network management functions may be available, for example, via a maintenance terminal.

8.1.4 Circuits

Both-way circuits can be made busy to one direction of operation to improve the flow of traffic in the other direction. In addition, both-way and one-way circuits can be removed from service, when necessary. Both of these actions may be taken by verbal direction to the responsible maintenance organization.

8.2 Improving capabilities

From the experience gained through the use of these simple tools, more sophisticated network management facilities can be specified. In the interest of cost reduction, these upgraded network management capabilities should be planned for introduction as a part of a planned addition or modification to an exchange, and should be specified as a part of the initial installation of new systems. Before purchasing a new exchange, attention should be paid to the ability of the exchange to provide network management requirements as specified in Recommendations Q.542 and Q.544.

In some cases, certain off-line network management information storing and processing needs may be accommodated by the use of personal computers.

9 Considerations for the development of network management

9.1 Network management can be provided on a distributed basis, where network management functions are provided "on-site" at the exchange, or on a centralized basis, where network management functions for a number of exchanges are provided at a single location. Each approach provides certain advantages which should be recognized when deciding which one would be appropriate for an Administration's situation. In general, the decentralized distributed approach may be more appropriate where activity levels are relatively low. It may also be an appropriate way to get started in network management. The centralized approach may be more appropriate in networks where activity levels are high. In some networks, a combination of these approaches may be most effective.

9.2 Advantages of the decentralized (distributed) approach

The decentralized (distributed) approach provides certain advantages, which include the following:

- locally available features and capabilities can be developed and used (see 8.1.3);
- a more detailed analysis and assessment of localized problems are possible;
- survivability of network management functions is improved, since a problem or outage at one location will not usually result in the loss of all network management capabilities;
- network management functions may be assigned to existing staff, eliminating the need to develop a dedicated, specialized staff;
- it may provide an interim capability while a long-term plan is being developed and deployed.

9.3 Advantages of the centralized approach

A centralized network management centre provides a number of operational benefits when compared with a distributed approach, where network management functions are provided "on-site" at the exchange. These include:

– More effective network management operations. A centralized approach is inherently more effective in dealing with complex, interrelated network problems in the SPC common channel signalling environment, and will become more so during the transition to ISDN. In many cases, the most effective response to a problem in the international network might be to take action in the national network, and vice versa. A centralized approach simplifies the problem of coordination of activities in these cases.

– A more "global" view of network performance. This, in turn, will permit faster and more accurate problem identification, and the development of more effective control strategies which can be implemented with less delay.

– A central point of contact for network management, both internally and with other Administrations (see Recommendation E.414).

– More efficient network management operations. The cost of staffing and training is reduced, and staff expertise is enhanced through specialization.

9.4 Network management operations systems

A computer-based network management operations system can provide considerable benefits to a network management centre due to its ability to process large volumes of information and to present that information in a common format. The functions of a network management operations system include the following:

– collecting alarms, status information and network management traffic data from exchanges (see clause 3 and Recommendation E.502);

– processing the collected data and calculating network management parameters (see clause 3 and Recommendation E.502);

– providing performance reports (see 9.4.1);

– comparing network management parameters with thresholds to identify unusual conditions;

– applying controls in exchanges based on input commands;

– calculating hard-to-reach status of destinations and providing this information to exchanges;

– interfacing with network management centre visual displays, and work station terminals and printers;

– preparing administrative reports;

– maintaining a database of network statistics and information.

NOTE – Many of these functions can also be provided to the Network Management Centre by each SPC exchange; however, the provision of these functions in a network management operations system may reduce the requirements placed on the exchanges.

9.4.1 Performance reports

Performance reports can be provided in the following ways:

i) *Automatic data* – This data is provided automatically as specified in the operations system software, and cannot be readily changed by the network manager.

ii) *Scheduled data* – This data is provided according to a schedule established by the network manager.

iii) *Demand data* – This data is provided only in response to a specific request by the network manager. In addition to performance data, demand data includes reference data, such as the number of circuits provided or available for service, routing information, assigned threshold values, numbers of installed switching system components, etc.

iv) *Exception data* – This data is provided when a data count or calculation crosses a threshold established by the network manager.

Data reports can be provided on a regular basis, for example, every 3 minutes, 5 minutes, 15 minutes, 30 minutes, or every hour. The specific interval for any data report will be determined by the network manager. Historic data relating to at least the previous two or three periods should also be available.

9.4.2 Other considerations

It should be noted that shorter collection intervals increase the usefulness of the data to the network manager, but also increase the size and cost of the operations system and may increase the volatility of the data.

It should also be noted that it is important that network management controls should not become completely unavailable due to the failure or malfunction of the network management operations system or of its communications links with exchanges. Therefore, network management operations systems should be planned with a high degree of reliability, survivability and security. This could be achieved through the provision of certain essential capabilities (such as controls and automatic routing protection mechanisms) on-site in the exchange, or by redundancy in computers and data links, or through the provision of alternative stand-by centres.

The failure of a network management operations system should not have an adverse impact on normal traffic flow in the network.

10 Intelligent network

Network management for a Service Control Function (SCF) (of Recommendation Q.1204) depends on communication between the SCF and a Service Switching Function (SSF) /Call Control Function (CCF) (of Recommendation Q.1204). If an SCF communicates with an SSF/CCF via a signalling network, network management can be performed via the signalling network. If an SCF communicates with an SSF/CCF via circuit groups that support, for example, ISDN interface, network management can be performed via the circuit groups.

10.1 Surveillance for an SCF via a signalling network

Surveillance for an SCF can be performed based on Recommendation E.505 which covers performance measurements for ITU-T Signalling System No. 7. Performance measurements for SCFs are application instances of performance measurements described in Recommendation E.505.

10.2 Surveillance for an SCF via circuit groups

An SCF can be implemented in an Adjunct (AD), Intelligent Peripheral (IP) or Service Node (SN) (of Recommendation Q.1205) that connects to a Service Switching Point (SSP) (of Recommendation Q.1205) via circuit groups with, for example, ISDN interface. Surveillance of such an SCF can be performed based on status information and traffic performance data of the circuit groups. Circuit group status information can indicate that congestion is present or imminent. Circuit group traffic performance data is generally expressed in parameters. For example, percentage overflow (% OFL) can indicate the congestion of traffic between an SSF/CCF and an SCF.

Annex A

Terminology for intelligent network

The following glossary is quoted collectively from Recommendations Q.1204 and Q.1205. It includes only the terms that are referred to in 10.1, 10.2 and clause 7/E.412. In addition to this glossary, more terminology in IN are available in Recommendations Q.1204 and Q.1205.

A.1 Adjunct (AD)

The adjunct Physical Entity (PE) is functionally equivalent to an SCP (i.e. it contains the same functional entities) but it is directly connected to an SSP. Communication between an adjunct and an SSP is supported by a high speed interface. This arrangement may result in differing performance characteristics for an adjunct and an SCP. The application layer messages are identical in content to those carried by the signalling network to an SCP.

An adjunct may be connected to more than one SSP, and an SSP may be connected to more than one adjunct.

A.2 Call Control Function (CCF)

The CCF is the Call Control (CC) function in the network that provides call/connection processing and control. It:

a) establishes, manipulates and releases call/connection instances as "requested" by the Call Control Agent Function (CCAF);

b) provides the capability to associate and relate CCAF functional entities that are involved in a particular call and/or connection instance (that may be on SSF requests);

c) manages the relationship between CCAF functional entities involved in a call (e.g. supervises the overall perspective of the call and/or connection instance);

d) provides trigger mechanisms to access IN functionality (e.g. passes events to SSF);

e) is managed, updated and/or otherwise administered for its IN-related functions (i.e. trigger mechanisms) by a Service Management Function (SMF).

A.3 Intelligent Peripheral (IP)

The IP provides special resources for customization of services, and supports flexible information interactions between a user and the network. Optionally, the switching matrix used to connect users to these resources may be accessible to external SLPs. Examples of possible resources are (this list is not meant to be exhaustive):

- customized and concatenated voice announcements;
- synthesized voice/speech recognition devices;
- DTMF digit collection;
- audio conference bridge;
- information distribution bridge;
- tone generator;
- text to speech synthesis;
- protocol converters.

The IP contains the Specialized Resources Function (SRF), and optionally a service switching function/call control function (SSF/CCF). This optional SSF/CCF is used to provide external access to the connections to the resources within the IP. The IP connects to one or more SSPs, and/or to the signalling network.

An SCP can request to an SSP to connect a user to a resource located in an IP that is connected to the SSP from which the service request is detected. An SCP can also request the SSP to connect a user to a resource located in an IP that is connected to another SSP.

A.4 Service Control Function (SCF)

The SCF is a function that commands call control functions in the processing of IN-provided and/or custom service request. The SCF may interact with other functional entities to access additional logic or to obtain information (service or user data) required to process a call/service instance. It:

a) interfaces and interacts with service switching function/call control function, Specialized Resource Function (SRF) and Service Data Function (SDF) functional entities;

b) contains the logic and processing capability required to handle IN provided service attempts;

c) interfaces and interacts with other SCFs, if necessary;

d) is managed, updated and/or otherwise administered by an SMF.

A.5 Service Node (SN)

The SN can control IN services and engage in flexible information interactions with users. The SN communicates directly with one or more SSPs, each with a point-to-point signalling and transport connection. Functionally, the SN contains an SCF, SDF, SRF, and SSF/CCF. This SSF/CCF is closely coupled to the SCF within the SN, and is not accessible by external SCFs.

In a manner similar to an adjunct, the SCF in an SN receives messages from the SSP, executes SLPs, and sends messages to the SSP. SLPs in an SN may be developed by the same service creation environment used to develop SLPs for SCPs and adjuncts. The SDF in an SN enables the SN to interact with users in a manner similar to an IP. An SCF can request the SSF to connect a user to a resource located in an SN that is connected to the SSP from which the service request is detected. An SCF can also request the SSP to connect a user to a resource located in an SN that is connected to another SSP.

A.6 Service Switching Function (SSF)

The SSF is the Service Switching (SS) function which, associated with the CCF, provides the set of functions required for interaction between the CCF and a Service Control Function (SCF). It:

a) extends the logic of the CCF to include recognition of service control triggers and to interact with the SCF;

b) manages signalling between the CCF and the SCF;

c) modifies call/connection processing function (in the CCF) as required to process requests for IN-provided service usage under the control of the SCF;

d) is managed, updated and/or otherwise administered by an SMF.

A.7 Service Switching Point (SSP)

In addition to providing users with access to the network (if the SSP is a local exchange) and performing any necessary switching functionality, the SSP allows access to the set of IN capabilities. The SSP contains detection capability to detect request for IN services. It also contains capabilities to communicate with other PE(s) containing a Service Control Function (SCF), such as a Service Control Point (SCP), and to respond to instructions from the other PE. Functionally, an SSP contains a Call Control Function (CCF), a Service Switching Function (SSF), and if the SSP is a local exchange, a Call Control Agent Function (CCAF). It also may optionally contain a Service Control Function (SCF), and/or a Specialized Resource Function (SRF), and/or a Service Data Function (SDF).

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	**Telephone network and ISDN**
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media
Series H	Transmission of non-telephone signals
Series I	Integrated services digital network
Series J	Transmission of sound-programme and television signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound-programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminal equipment and protocols for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communication
Series Z	Programming languages