All drawings appearing in this Recommendation have been done in Autocad.

Recommendation E.411

xe ""§INTERNATIONAL NETWORK MANAGEMENT – OPERATIONAL GUIDANCE

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 Recommendation E.410, § 5). 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 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 xe ""§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 information includes information on the status of exchanges, circuit groups and common channel signalling systems. This status information can be provided by one or more types of displays. These may include printers, video displays, and/or indicators 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 measurementsxe "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 measurementsxe "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 equipmentxe "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 indicatorsxe "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

– serious congestion
Level 2;

– unable to process calls

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

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 informationxe "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.

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.

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 Recommendation E.412, § 2.1.)

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.

3.6 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.

$$\% \text{ OFL} = \times 100$$

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 =

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 = × 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 = × 100

---

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 either by:

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.

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)**[2])

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 =

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 (CCS) 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.

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”

---

2)

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 either by:

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.

signal (or its equivalent) and the total number of seizures. Measurement of BFSR is usually made on a circuit group basis.

BFSR = × 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).

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/E.411).
Figure 1/E.411 - CCITT 48150

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, and:
2) the level of demand for that destination,
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 §§ 3.6.3 and 3.6.4).

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 xe ""§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 xe ""§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 *xe ""§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 *xe ""§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 directionalizationxe " 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 *xe ""§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 Recommendation E.414, § 4) 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)
  - ii)
  - iii)
  - iv)

– develop and implement control strategies (expansive and protective);

– assist in determining the need for, and locating, technical equipment to restore communications.

7 xe ""§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 operational signals, such as switching congestion indicators, 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.30) 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 thexe ""§ use of common channel signalling for network management*

7.3.1 Common channel signalling systems provide a fast and reliable means of transfering network management operational signals between exchanges. An example is the transfer of exchange congestion status signals for the Automatic Congestion Control (ACC) system (see Recommendation E.412, § 3.1). 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 electro–mechanical 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 up–graded 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 *xe ""§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 § 3 and Recommendation E.502);
- processing the collected data and calculating network management parameters (see § 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 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.

ANNEX A
(to Recommendation E.411)

xe ""§Terminology for network management

A.1 **circuit**

A circuit connects two exchanges. A national circuit connects two exchanges in the same country. An international circuit connects two international exchanges situated in different countries. (Based on Recommendation D.150 and Recommendation F.68.)

A.2 **circuit group**

The set of all switched circuits which directly interconnect one exchange with another.

A.3 **circuit sub–group**

A set of circuits within a circuit group which are uniquely identifiable for operational or technical reasons. A circuit group may consist of one or more circuit sub–groups.

A.4 **destination**

A country in which the called subscriber is located or an area or other location that may be specified within that country. A destination can be identified by the digits used for routing the call.

A.5 **bid**

An attempt to obtain a circuit in a circuit group or to a destination. A bid may be successful or unsuccessful in seizing a circuit in that circuit group or to that destination.

A.6 **seizure**

A seizure is a bid for a circuit in a circuit group which succeeds in obtaining a circuit in that circuit group.

A.7 **answer signal**

A signal sent in the backward direction indicating that the call is answered. (Based on Recommendation Q.254.)

A.8 **holding time**

The time interval between seizure and release of a circuit or switching equipment.

A.9 **busy–flash signal (sent in the backward direction)**

This signal is sent to the outgoing international exchange to show that either the circuit group, or the called subscriber, is busy (Signalling Systems No. 4 and No. 5, see Recommendations Q.120 and Q.140).

Note – In Signalling Systems No. 6 and No. 7, there is no busy–flash signal. However, the equivalent of busy–flash can be roughly approximated through the aggregation of specific backward failure signals such as circuit group congestion, national network congestion and subscriber busy.