INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Q.542

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/93)

DIGITAL EXCHANGES

DIGITAL EXCHANGE DESIGN OBJECTIVES – OPERATIONS AND MAINTENANCE

ITU-T Recommendation Q.542

(Previously "CCITT Recommendation")

FOREWORD

The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the International Telecommunication Union. 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, established the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

ITU-T Recommendation Q.542 was revised by the ITU-T Study Group XI (1988-1993) and was approved by the WTSC (Helsinki, March 1-12, 1993).

NOTES

1 As a consequence of a reform process within the International Telecommunication Union (ITU), the CCITT ceased to exist as of 28 February 1993. In its place, the ITU Telecommunication Standardization Sector (ITU-T) was created as of 1 March 1993. Similarly, in this reform process, the CCIR and the IFRB have been replaced by the Radiocommunication Sector.

In order not to delay publication of this Recommendation, no change has been made in the text to references containing the acronyms "CCITT, CCIR or IFRB" or their associated entities such as Plenary Assembly, Secretariat, etc. Future editions of this Recommendation will contain the proper terminology related to the new ITU structure.

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

© ITU 1994

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

CONTENTS

			Page
1	General		1
2	Maintenance design objectives		1
	2.1	Status and other information	1
	2.2	Inputs and outputs	1
	2.3	Routine testing	1
	2.4	Trouble localization	1
	2.5	Fault and alarm detection and actions at interfaces A, B, V_2, V_3 and V_4	2
	2.6	Fault and alarm signal detection and actions at interface V_1	4
	2.7	Fault and alarm signal detection and actions at interface Z	4
	2.8	Fault and alarm signal detection and actions for transmission systems	5
	2.9	Fault and alarm signal detection and actions for channel associated signalling (2048 and 8448 kbit/s)	5
	2.10	Fault and alarm signal detection and actions for channel associated channel signalling (1544 kbit/s)	6
	2.11	Fault and alarm signal detection and actions for common channel signalling	6
	2.12	Fault and alarm detection and consequent actions – Other functions of the exchange	6
	2.13	Supervision or testing of interface function	7
	2.14	Supervision or testing of signalling functions	7
	2.15	Supervision or testing of exchange connections	7
	2.16	Supervision or testing of digital link performance	8
	2.17	Supervision or testing of analogue link performance	8
3	Subscriber line maintenance and testing design objectives		8
	3.1	Analogue subscriber lines	8
	3.2	Digital subscriber lines	9
4	Operations design objectives		9
	4.1	General	9
	4.2	Operations features	9
	4.3	Exchange functions related to the TMN	10
5	Network management design objectives		10
	5.1	General	10
	5.2	Network management elements	11
	5.3	Information provided by an exchange for network management purposes	11
	5.4	Exchange controls for network management	13
	5.5	Automatic controls for network management	15
	5.6	Order of application of controls	21

DIGITAL EXCHANGE DESIGN OBJECTIVES – OPERATIONS AND MAINTENANCE

(Melbourne, 1988; modified at Helsinki, 1993)

1 General

This Recommendation applies to digital local, combined, transit and international exchanges for telephony in Integrated Digital Networks (IDN) and mixed (analogue/digital) networks, and also to local, combined, transit and international exchanges in an Integrated Services Digital Network (ISDN).

The field of application of this Recommendation is more fully defined in Recommendation Q.500. Some objectives only apply to a certain type (or types) of exchange. Where this occurs, the application is defined in the text. Where no such qualification is made, the objective applies to all exchange applications.

2 Maintenance design objectives

The exchange shall be arranged so that normal maintenance activities can be easily performed by maintenance personnel. It should be capable of providing all information necessary for the identification of trouble conditions and the direction of repair activities.

2.1 Status and other information

The exchange shall provide information to maintenance personnel so that they can quickly ascertain:

- equipment/system status;
- critical load levels;
- trouble conditions;
- network management controls in effect.

2.2 Inputs and outputs

The exchange shall be able to transmit and receive maintenance information and respond to commands from on-site and if appropriate, from remote maintenance centre(s) or systems over the recommended interface(s) (see Recommendation Q.513).

Depending on the degree of processing desired by the Administration, the human/machine terminal could offer the following features:

- operational data processing and analysis;
- maintenance data processing and analysis;
- exchange status observation.

In performing operations and maintenance functions, the exchange shall use CCITT MML at its input/output terminals as covered in the Z.300-Series Recommendations.

2.3 Routine testing

The exchange shall have facilities for performing or directing routine test activities on its component parts and possibly with interfacing equipment or systems.

2.4 Trouble localization

The exchange shall have adequate facilities for diagnosing and locating faults within the exchange.

2.5 Fault and alarm detection and actions at interfaces A, B, V_2, V_3 and V_4

The exchange shall interact with transmission systems as required to detect fault and alarms and take appropriate actions.

2.5.1 Fault detection

The following fault conditions should be detected:

- failure of local power supply (if practicable);
- loss of incoming signal;

  NOTE – The detection of this fault condition is required only when the fault does not result in an indication of loss of frame alignment.

- loss of frame alignment (see Recommendation G.706; the loss of frame alignment will also be assumed if no CRC multiframe alignment can be achieved or if the proportion of corrupted CRC checks exceeds a certain value);
- excessive error ratio (without CRC procedure). The criteria for activating and deactivating the indication of the fault condition are given in Recommendation G.707. Consequent actions are given in 2.5.3;
- CRC error reporting, if applicable:

  a) every time a received CRC block is detected errored by the exchange termination:

     – a report will be transmitted to the error monitoring function;

     – the information "one multiframe errored" is transmitted in the outgoing signal at the interface using an E bit (see 2.3.3.4/G.704);

  b) every time that an E bit in the binary state 0 is received, a report will be transmitted to the error monitoring functions.

     (On a provisional basis the considerations related to the E bit may only apply to V interfaces – for further study.)

2.5.2 Alarm signal detection

The following alarm indications should be detected:

- Alarm indication (remote alarm) received from the remote end.
- AIS (alarm indication signal). The equivalent binary content of the alarm indication signal (AIS) is a continuous stream of "1"s at 2048 or 8448 kbit/s.

The strategy for detecting the presence of the AIS should be such that the AIS is detectable even in the presence of an error ratio of 1 in 10^3. However, a signal with all bits except the frame alignment bit in the 1 state should not be mistaken as an AIS.

2.5.3 Consequent actions

2.5.3.1 Generation of alarm signals for action within the exchange

- The service alarm indication should be generated to signify that the service is no longer available (see Table 1).
- The prompt maintenance alarm indication should be generated to signify that performance is below acceptable standards and that immediate maintenance attention is required locally (see Table 1).

2.5.3.2 Generation of alarm signals transmitted by the exchange

- Alarm signals sent in the outgoing direction at the exchange interface. The relevant alarm bits for the remote alarm indication, as recommended in Recommendation G.704 should be effected as soon as possible (see Table 1).
- Alarm signals sent towards the switching function. Alarm indication signal applied in all received time-slots containing speech, data and/or signalling should be applied as soon as possible and not later than 2 ms after the detection of the fault condition (see Table 1).

TABLE 1/Q.542

Fault conditions and alarms detected by exchange termination functions and consequent actions (excluding interface V_1)

Fault conditions and alarm signals detected	Consequent actions (see 2.5.3)			
	Service alarm indication generated	Prompt maintenance alarm indication generated	Alarm indication to remote end generated	AIS towards the switching stages
Failure of power supply	Yes	Yes	Yes, if practicable	Yes, if practicable
Loss of incoming signal	Yes	Yes	Yes	Yes
Loss of frame alignment	Yes	Yes	Yes	Yes
Excessive error ratio	Yes	Yes	Yes	Yes
Alarm indication received from remote end	2048 + 8448 kbit/s: Yes 1544 + 6312 kbit/s: optional	1544 + 6312 kbit/s: Yes		
AIS received	Yes		Yes	Yes

NOTE – A *Yes* in the table signifies that an action should be taken. An open space in the table signifies that the relevant action should *not* be taken if this condition is the only one present. If more than one fault condition or alarm is simultaneously present, action should be taken if for at least one of the conditions a *Yes* is shown, except in the case of AIS received for which 2.5.3.4 applies. The use of error performance monitoring in this table is for further study.

2.5.3.3 Removal of alarm indications

When all fault conditions have been cleared and alarm indication signal is no longer received, the alarm indication signal and remote alarm indication should be removed within the same respective time limits as specified in 2.5.3.4 after the conditions have cleared.

2.5.3.4 Alarm processing

The following items are required to ensure that equipment is not removed from service due to short breaks in transmission (e.g. due to noise or transient fault) and to ensure that maintenance action does not result where no direct maintenance action is required.

- The persistence of service alarm and of the prompt maintenance alarm indications may be verified for 100 ms before action is taken.
- When the AIS is detected, the prompt maintenance alarm indication, associated with loss of frame alignment and excessive error rate in the frame alignment pattern, should be inhibited.
- When the fault conditions cease, the service alarm and prompt maintenance alarm indications, if given, should be removed. Again, the persistence of this change in condition may be verified for 100 ms before action is taken.
- It is possible that some systems could suffer from frequent transient faults resulting in an unacceptable quality of service. For this reason, if a persistence check is provided, fault rate monitoring should also be provided for each digital transmission system. This monitoring will result in permanent removal from service of digital transmission system which are frequently removed from the service or frequently produce transient alarm conditions. The threshold for removal from service needs study. When this action is taken, the service alarm indication and the prompt maintenance alarm indication shall be given.

2.5.4 Error performance monitoring using CRC

2.5.4.1 General

When the CRC procedure is implemented at the interface, the exchange should monitor the error performance of the interface to report on the performance (see Recommendation G.821).

2.5.4.2 Error performance parameters

The exchange should derive the following information from CRC checks in the incoming signal and received E bits:

- degraded minutes (DM);
- severely errored seconds (SES);
- error-free seconds (EFS).

NOTES

1 These parameters are defined in Recommendation G.821.

2 The definition of a value for the suitable time interval during which the parameters should be assessed needs further study.

3 The choice has to be made between the association of one type of parameter to each direction of transmission and the integration of the two directions in one type of parameter. This needs further study.

4 The correlation between the results of CRC checks and the parameters quoted above requires further study.

2.5.4.3 Error performance evaluation

Each of the performance parameters will be processed separately in order to evaluate the performance of the interface.

The following classification of the interface maintenance conditions has to be made by the exchange (see I.600-Series Recommendations):

- correct functioning interface;
- degraded transmission interface;
- unacceptable transmission interface.

NOTES

1 This subclause may only apply to V interfaces (for study).

2 The level at which an interface for ISDN access enters the degraded transmission condition may be dependent on the quality of service provided to the customer.

3 The levels at which an interface enters the degraded or unacceptable transmission conditions are for further study and are outside the scope of this Recommendation.

2.5.4.4 Consequent actions

For further study.

2.6 Fault and alarm signal detection and actions at interface V_1

The exchange shall interact with transmission systems as required to detect fault and alarm signals and take appropriate actions.

a) Fault detection
b) Alarm detection
c) Consequent actions

} To be specified

2.7 Fault and alarm signal detection and actions at interface Z

a) Fault detection
b) Alarm detection
c) Consequent actions

} To be specified

2.8 Fault and alarm signal detection and actions for transmission systems

Faults and alarms which cannot be directly detected by the exchange termination function but which are detected by transmission equipment (e.g. group pilot failure) should be accepted by the exchange as needed to take appropriate action.

2.9 Fault and alarm signal detection and actions for channel associated signalling (2048 and 8448 kbit/s)

2.9.1 Fault detection

The exchange signalling function should detect the following fault conditions for each multiplex carrying a 64 kbit/s signalling channel:

– failure of local power supply (if practicable);

– loss of 64 kbit/s incoming signal;

NOTE – The detection of this fault condition is required only when the fault does not result in an indication of loss of multiframe alignment.

– loss of multiframe alignment.

The criteria for activating and deactivating the indication of the fault condition are given in Recommendations G.732 and G.744.

2.9.2 Alarm detection

The exchange signalling function should detect the alarm indication (remote alarm) received from the remote end.

2.9.3 Consequent actions

2.9.3.1 Generation of alarm signals for action within the exchange

– The service alarm indication should be generated by the exchange signalling function to signify that the service is no longer available (see Table 2).

– The prompt maintenance alarm indication should be generated to signify that performance is below acceptable standards and that immediate maintenance attention is required locally (see Table 2).

2.9.3.2 Alarm transmitted by the exchange

An alarm indication (remote alarm) should be applied in the outgoing direction at the transmission/switching interface as soon as possible (see Table 2). The relevant alarm bit for the remote alarm indication is given in Recommendation G.732.

2.9.3.3 Removal of alarm indication

When all fault conditions have been cleared and AIS is no longer received, the remote alarm indication should be removed as soon as possible.

2.9.3.4 Alarm processing

Same as in 2.5.3.4.

TABLE 2/Q.542

Fault conditions and alarms detected by the exchange signalling function and consequent actions

Fault conditions and alarm detected	Consequent actions (see 2.9.3)		
	Service alarm indication generated	Prompt maintenance alarm indication generated	Alarm indication to remote end generated
Failure of power supply	Yes	Yes	Yes, if practicable
Loss of 64 kbit/s incoming signal	Yes	Yes	Yes
Loss of multiframe alignment	Yes	Yes	Yes
Alarm indication received from remote end	Yes		
NOTE – A *Yes* in the table signifies that an action should be taken. An open space in the table signifies that the relevant action should *not* be taken if this condition is the only one present. If more than one fault condition or alarm is simultaneously present, action should be taken if for at least one of the conditions a *Yes* is shown.			

2.10 Fault and alarm signal detection and actions for channel associated channel signalling (1544 kbit/s)

Requires further study.

2.11 Fault and alarm signal detection and actions for common channel signalling

Requirements specified in relevant Recommendations apply.

2.12 Fault and alarm detection and consequent actions – Other functions of the exchange

2.12.1 Faulty circuits

The exchange should not switch any new calls to a detected faulty circuit.

The exchange should remove from service all circuits found to be permanently faulty as detailed in 2.5, 2.8, 2.9, 2.10 and 2.11.

2.12.2 Master clock distribution

The absence of timing information distributed from a master clock located at the exchange or received from an external master clock shall be recognized and a prompt maintenance alarm shall be given.

Changeover to an alternate timing source shall be operated so as to fulfil the requirements of 2.7.2/Q.543 and 2.7.3/Q.543.

2.12.3 Internal timing distribution

The distribution of timing information to the major elements of the exchange shall be supervised as required. A service alarm shall be given when a failure is detected. A maintenance alarm shall be given if it is appropriate.

NOTE – Remote elements may have to be taken into consideration.

2.13 Supervision or testing of interface function

The exchange shall have the capability of verifying the proper operation of the interface functions, including the fault detection and supervision functions.

Routine tests, statistical tests, manual activities and/or other means may be used to verify proper operation of these functions.

Information shall be given to the far end exchange when new calls cannot be established on the circuits on which routine tests are being initiated. Established calls, including semi-permanent connections, must not be interrupted. During the tests, the generation of alarms at the far end exchange due to the removal of circuits from service should be avoided, if possible.

2.13.1 ET functions – Interfaces A, B, V_2, V_3 and V_4

The verification of the proper operation of exchange termination functions can be performed by the means of statistical observations or by testing. Testing may be manual or automatic.

2.13.2 ET functions – Interfaces C and Z

i) Failures of codecs [except those covered in ii) below] should be recognized by the exchange using the criteria defined in Recommendation G.732.

ii) Supervision or testing of codecs of one or a small number of channels may be accomplished according to i) above or by inter-office transmission measurement and testing on circuits between exchanges or by statistical measurements.

2.13.3 ET functions – Interface V_1

To be specified.

2.14 Supervision or testing of signalling functions

In addition to fault detection required in 2.7, the following applies.

2.14.1 Channel associated signalling

The exchange should be able to verify the proper operation of the signalling functions by generating and responding to test calls or by a statistical observation.

2.14.2 Common channel signalling

The exchange should be able to verify the proper operation of the signalling functions as required by common channel signalling Recommendations.

2.15 Supervision or testing of exchange connections

Checking the different portions of the path individually in a digital exchange network helps to ensure the continuity of the connections overall. In this respect, the exchange has to verify:

– the continuity across the exchange, as covered in this subclause;

– the continuity in the transmission links terminating on the exchange as covered in 2.16 and 2.17.

2.15.1 Continuity across the exchange

A means should be provided to determine that the operational error performance requirement (i.e. on bit error ratio) is being met. (The design objective for error performance can be found in Recommendation Q.554.)

The exchange should provide adequate provision of the cross office path continuity and verify the transmission performance. (The design objective for transmission performance can be found in Recommendation Q.543.) This will guarantee, in particular, an acceptable transmission quality to its connections.

2.15.2 Verification depending on the type of connection

The verifications to be performed by the exchange should depend also on the type of connection. In particular:

- for 64 kbit/s switched connections, the transmission performance requirements of Q.543 may be considered to be sufficient in order to guarantee the cross office path continuity;
- semi-permanent connections may require special supervision procedures which need further study;
- supervision of n × 64 kbit/s requires further study for both switched and semi-permanent connections.

2.16 Supervision or testing of digital link performance

The exchange shall have the capability of monitoring digital link performance to detect when bit error ratio and loss of framing thresholds exceed operational objectives. The exchange will then take subsequent action to give appropriate trouble indications or alarms and perform other appropriate actions, such as removing circuits from service.

2.17 Supervision or testing of analogue link performance

2.17.1 Interexchange circuit continuity check

The exchange should be capable of performing circuit continuity checks in accordance with appropriate signalling system Recommendations. Circuits failing circuit continuity checks should be removed from service and repair procedures initiated as required.

2.17.2 Interexchange transmission measurement and testing on circuits between exchanges

The exchange may also be equipped within itself or give access to external equipment to perform other transmission tests on circuits. Faulty circuits should be removed from service and repair procedures initiated as required.

3 Subscriber line maintenance and testing design objectives

3.1 Analogue subscriber lines

3.1.1 Testing arrangements for wire-pair lines terminated at the exchange

The exchange shall be capable of providing for automatic testing of subscriber lines and/or for providing test access to subscriber lines for testing systems not integrated into the exchange. The objective is to have capability to:

- automatically select and test analogue subscriber lines in a given sequence;
- test a percentage of the lines, directed by a maintenance system operator;
- provide automated testing of a line as directed by a repair-man at the location of the telephone set.

3.1.2 Test parameters

The analogue subscriber line testing arrangement shall have the capability to detect and/or measure parameters specified by the Administration, such as the following:

- the presence of extraneous voltages (AC or DC) on either side of the subscriber line pair;
- the insulation resistance between the two wires of the pair, between each wire and ground and between each wire and the negative side of the exchange battery;
- the integrity of the loop and telephone set signalling circuit;
- a check of two states of the loop:
  a) with the telephone instrument connected; and
  b) with the pair shorted at the instrument;

– a check of the operation of the dial, either DTMF or decadic pulses;

– the connection of two or more telephone sets to the line.

3.1.3 Test values

The network provider or the Administration shall specify tests and limits. Use of parameters and limits shown in applicable CCITT Recommendations, such as Recommendation Q.23, covering frequencies produced by dialing devices, is recommended.

3.2 Digital subscriber lines

For further study.

4 Operations design objectives

4.1 General

The exchange and/or any associated Operations and Maintenance Systems/Centres shall have the capabilities necessary to permit it to be operated, administered and maintained efficiently while providing service in accordance with an Administration's performance requirements.

The Telecommunications Management Network (TMN) architecture, as described in Recommendation M.30, considers the exchange to be a Network Element (NE) which can interact with Operations Systems (OS) within a TMN. Operations systems may be used at the discretion of Administrations to improve operating efficiencies and service by centralizing and mechanizing operations, administrative and maintenance functions. The number and variety of operations systems will depend on the operating practices of the Administration.

The decision to implement TMN principles rests with the Administration.

4.2 Operations features

4.2.1 Service provisioning and records

There should be efficient means of establishing service, testing, discontinuing service and maintaining accurate records for:

– subscriber lines and services (in local exchanges);

– interexchange circuits.

4.2.2 Translation and routing information

There should be efficient means of establishing, testing and changing call processing information, such as translation and routing information.

4.2.3 Resource utilization

There should be efficient means of measuring performance and traffic flows and to arrange equipment configurations as required to insure efficient use of system resources and to provide a good grade of service to all subscribers (e.g. load balancing).

4.2.4 Exchange observation and measurements

The exchange should provide means for making observations and measurements on quality of service and network performance, to satisfy, for example, grade of service objectives as covered in Recommendation E.500, or for provisioning purposes. Details of measurements for digital exchanges are given in Recommendation Q.544.

4.3 Exchange functions related to the TMN

Detailed descriptions, definitions and classifications of TMN functions to which the exchange will contribute is for further study.

A partial list of TMN functions is given below. A more complete list is given in Recommendation M.30.

Exchanges may have requirements for Operations, Administration and Maintenance functions which are not related to TMN. This is for further study.

4.3.1 Functions potentially related to TMN

- subscriber administration;
- tariff and charging administration;
- routing administration;
- network management;
- maintenance of subscriber lines;
- maintenance of circuits between exchanges;
- exchange maintenance;
- signalling network maintenance;
- administration of hardware configuration;
- administration of software configuration;
- external alarms and indications;
- O&M staff procedures;
- traffic measurements;
- quality of service and network performance observation.

4.3.2 Information flows

Generally, information flows will consist of requests/demands to the exchange and responses from the exchange. There will also be autonomous information flows from the exchange (e.g. alarms, programmed response, etc.). Refer to Recommendation Q.513 for information on interfaces to the TMN.

This subject is for further study.

5 Network management design objectives

5.1 General

Network management is the function of supervising the performance of a network and taking action to control the flow of traffic, when necessary, to promote the maximum utilization of network capacity.

These functions have application in exchanges within the IDN, and may or may not have application in national networks during the transition period to IDN.

The implementation of network management features and functions in national networks and in specific exchanges will be at the option of Administrations. Likewise the choice of which controls and features to use will be the option of each Administration.

5.1.1 Network management objectives

Information on network management objectives can be obtained from Recommendation E.410, and from the CCITT "Handbook on Service Quality, Network Maintenance and Management", ITU, Geneva 1984.

5.1.2 The application of network management in exchanges

In addition to the normal engineering and economic factors, the decision whether or not to provide network management capabilities in a digital exchange will be based on the following considerations:

- the size of the exchange, the size of circuit groups it serves and the network architecture;
- the role and importance of the exchange in its own network, or as an access exchange interfacing other exchanges and networks (e.g. international or other exchange networks);
- the requirement for the exchange to interact for network management purposes with other exchanges and/or network management centres;
- the features necessary to provide essential services in emergency situations, where other means are not available;
- alternative approaches such as providing redundancy and special routing methods;
- the need for managing network resources effectively when overload conditions occur in its own or interworking networks.

Other factors to be considered are:

- the network management organization, its equipment and selected functions;
- the possible interactions of both the circuit switched and signalling networks when network management actions are applied under various traffic conditions or network configurations;
- the potential impact of network management functions on the engineering design and administration of the network and the exchange;
- the evolution towards IDN and interworking of SPC with non-SPC exchanges in the interim period;
- the proportion of automatic and manual features to be implemented and the rate of introduction of various network management features;
- the reduction of exchange processing capacity due to the additional load imposed by network management (if appropriate);
- possible additional holding time of equipment in some switching and signalling systems where open numbering is used, if and when certain network management controls are applied.

5.2 Network management elements

The basic elements of a network management system to be provided by an exchange or by network management centres are:

- collection of information about network status and performance;
- processing of information for network management decisions;
- delivery to exchanges of network status information and/or commands for control activities;
- activation/deactivation of controls resulting from decisions made in the exchange or a network management centre;
- feedback of status in response to control actions.

Descriptions of the functions required in the exchanges to support these elements are given in 5.3 and 5.4.

5.3 Information provided by an exchange for network management purposes

5.3.1 General

The term “information” is used here as meaning all messages, signals or data in any form, used or provided by the exchange or by a network management centre.

5.3.2 Sources of information

The information provided by an exchange for network management will be based on the status, availability and performance and configuration of:

- circuit groups;
- exchange processes;
- common channel signalling link sets;
- other exchanges with direct links to this exchange;
- destination exchanges.

Status information is generated by comparing the current value of load indicators with appropriate threshold values and/or detecting abnormal conditions. Such type of information assumes discrete values and it can be used, without other processing, to activate traffic control routines.

This information should be sent spontaneously in a real-time basis to other exchanges or to a network management centre.

Performance information is obtained by means of traffic measurements and can be used for centralized processing or for network supervision in a network management centre. Such type of information can be sent in a near-real-time basis.

Configuration information is used for a network management data base at exchange level. This information could include:

- threshold values actually used;
- list of supervised circuit groups;
- list of supervised signalling circuits;
- list of supervised processors;
- list of supervised destination codes;
- list of primary and alternate routes for specified destinations.

Details of network measurements are given in Recommendation Q.544.

5.3.3 Processing of network management information in an exchange

Information collected at an exchange for network management purposes may or may not require some form of sorting and assembly (processing) before being used for network management.

Where processing is required, this may be done by the exchange processor, or by a data processing system serving one or more exchanges, or by a network management centre.

5.3.4 Transmittal of information

Network management information may be sent on a scheduled near-real-time basis when triggered by abnormal situations (e.g. overload conditions, alarms, etc.): alternatively, information may be sent on demand, i.e. in response to an external request. Table 3 shows the correspondence between sources of information and their transmission mode.

TABLE 3/Q.542

Source of information	Data transmission mode		
	Real-time	On demand	Scheduled
Status information	X	X	
Performance and availability information		X	X
Configuration information		X	

The destinations of network management information may be:

- within the originating exchange;
- to distant exchanges;
- to a network management centre.

Information may be carried by the TMN over a dedicated telemetry or data facility, over a common channel signalling network, or over other telephony network facilities as appropriate.

For each mode of transmittal the appropriate interface and protocol requirements, where covered by CCITT Recommendations, should be satisfied.

5.3.5 Presentation of information

Indications of network management controls in effect in an exchange shall be presented on visual indicators and/or printing-type or video display terminals for purposes of advising on-site personnel.

Similar displays and/or indicators may also be provided in a co-located and/or distant network management centre.

5.4 Exchange controls for network management

5.4.1 General

Network management controls provide the means to alter the flow of traffic in the network, in support of network objectives. Most network management controls are applied by, or in the exchange; however, certain actions may be taken external to the exchange. Recommendation E.412 provides specific information on network management controls and gives guidance on their application. Additional information is provided in the CCITT "Handbook on Service Quality, Network Management and Maintenance".

5.4.2 Activation and deactivation of controls

Controls in an exchange can be activated, or deactivated, by input from a network management operations system or by direct input from an exchange man-machine interface terminal. In addition, some controls can be activated automatically either by external or internal stimulus, or by a threshold being crossed.

When automatic control operation is provided, means for human override should also be provided.

Controls will usually be activated or deactivated in steps (stages) that are intended to avoid surge effects in the network that could be caused by too much control being added or removed too quickly.

A low level threshold may be required to remove controls as appropriate, when traffic conditions have been stabilized.

5.4.3 Traffic to be controlled

Exchanges should be capable of applying a range of network management controls (see Recommendation E.412).

The operational parameters of a control can be defined by a set of traffic attributes. As shown in Figure 1, these parameters include distinctions based on the origin of traffic, for example, customer-dialed, operator-dialed, transit or other classification as may be specified by the Administration. These can be further defined by type of service, particularly by ISDN.

Additional attributes can be specified, for example, incoming/outgoing circuit group class, or hard-to-reach status of destinations can be used. Further distinctions can be based on the outgoing traffic type, for example, direct-routed, alternate-routed or transit.

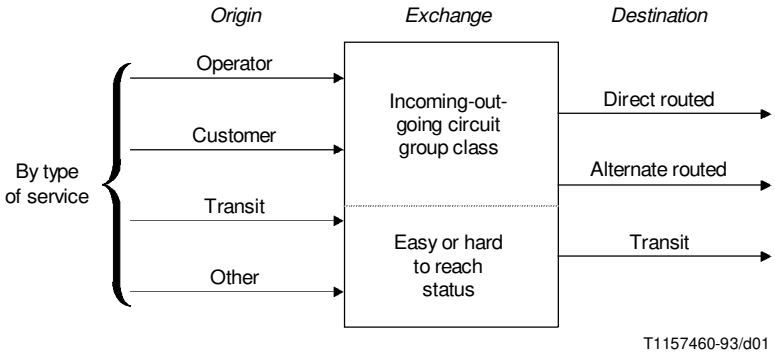

FIGURE 1/Q.542

Traffic attributes affecting network management controls

5.4.4 Network management controls

The following is a list of typical network management controls to be considered for implementation in a given exchange.

It is desirable that these controls be activated to affect a variable percentage of traffic (for example, 25%, 50%, 75% or 100%). Alternatively the number of call attempts routed in a particular period may be controlled (for example, one call per minute). It may also be desirable to apply controls on a destination code basis.

These controls are normally activated/deactivated manually from a man-machine interface in the exchange, or from an operations system. The automatic operation of these controls and the need for new controls is for further study.

It is preferable that these controls be provided in international transit exchanges and large transit exchanges in national applications. However, the decision whether or not to provide these controls in local and combined local/transit exchanges is at the discretion of the Administration.

5.4.4.1 Code blocking control

This control bars or restricts routing to a specific destination code. Code blocking can be done on a country code, an area code, an exchange identifying code and, in some cases, on an individual line number.

5.4.4.2 Cancellation of alternative routing

There are two types of cancellation of alternative routing control. One version prevents traffic from overflowing from the controlled route [Alternate Routed From (ARF)]. The other version prevents overflow traffic from all sources from having access to the controlled route [Alternate Routed To (ART)]. When cancellation of alternative routing is to be provided, both types are recommended.

5.4.4.3 Call gapping

This control sets an upper limit on the number of call attempts allowed to be routed towards the specified destination in a particular period of time (for example, one call per minute).

5.4.4.4 Restriction of direct routing

This control limits the amount of direct routed traffic accessing a route.

5.4.4.5 Skip route

This control allows traffic to bypass a specific route and advance instead to the next route in its normal routing pattern.

5.4.4.6 Temporary alternative routing

This control redirects traffic from congested routes to routes not normally available which have idle capacity at the time. This can be done for subscriber, and/or operator-originated traffic.

5.4.4.7 Circuit directionalization

This control changes both-way operated circuits to one-way operated circuits.

5.4.4.8 Circuit turndown/busying

This control removes one-way and/or both-way operated circuits from service.

5.4.4.9 Recorded announcements

These are announcements which give special instructions to operators and subscribers, such as to defer their call to a later time.

5.5 Automatic controls for network management

5.5.1 General

This subclause provides descriptions of some automatic traffic control methods that can be provided in digital exchanges for network management purposes.

Automatic, and/or dynamic network management controls represent a significant improvement over static manual controls. These controls, which are pre-assigned, can respond automatically to conditions internally detected by the exchange, or to status signals from other exchanges and can be promptly removed when no longer required.

The following are a basic set of automatic methods for use in the telephone network:

- Automatic Congestion Control system (ACC);
- Selective Circuit Reservation control (SCR);
- Hard-To-Reach process (HTR);
- Temporary Trunk Blocking (TTB).

The above list of methods is not exhaustive, but will provide a framework for more advanced controls which may be required in the ISDN.

In the following four subclauses the typical operation of each control is described, and guidance on the application of the controls is given in 5.5.6.

5.5.2 Automatic Congestion Control system

The Automatic Congestion Control (ACC) system allows a congested exchange to send a congestion indicator in a backward direction to the preceding exchange. The exchange receiving the congestion indication should respond by reducing the amount of traffic offered to the congested exchange.

The preferred method of conveying the congestion indication is via the relevant common channel signalling system.

a) *Detection and transmission of congestion status*

An exchange should establish a critical operating system benchmark, e.g. the time required to perform a complete basic cycle of operations. The exchange should continuously monitor this benchmark and, when continued levels of nominal performance are not achieved, a state of congestion is declared. Thresholds should be established so that two levels of congestion can be identified, with congestion level 2 (C2) indicating a more severe performance degradation than congestion level 1 (C1). When either level of congestion is detected, the exchange should have the capability to

1) code an ACC indication in the appropriate signalling messages, and

2) notify its network management support system of its current congestion status.

The system can offer benefit, however, by recognizing a single level of congestion. Where this situation exists, it should be regarded as congestion level 2.

b) *ACC control operation*

Exchanges receiving an ACC indication from an affected exchange or network operations centre should have the capability to institute the appropriate ACC controls and to notify its network management support system of the receipt of an ACC indication.

An exchange receiving an ACC indicator from a congested exchange should activate the assigned ACC controls and start a timer. (The provisional value of the timer is five seconds and is for further study.) Subsequent received ACC indicators restart the timer, when the timer expires, the ACC controls in the exchange are removed. One or more different response categories should be available from which to choose.

To avoid the incorrect application of controls, it is important that an exchange receiving an ACC indication should not re-transmit that indication to a preceding exchange.

c) *ACC response*

An exchange should have the capability of assigning an ACC response category to individual circuit groups. There should be several categories available from which to choose. Each category would specify how much traffic should be controlled in response to each of the received ACC indicators. The categories should be structured so as to present a wide range of response options to received ACC indicators.

The control options for further processing of calls denied access to the circuit group may be SKIP or CANCEL. The SKIP response allows a call to alternate route to the next circuit group in the routing pattern (if any) while the CANCEL response blocks the call.

NOTE – ACC response categories can be set locally in the exchange or by input from a network management center.

Table 4 is an example of the flexibility that could be achieved in a control's response to an exchange that is experiencing congestion.

In this example, different control actions would be taken based upon the distinction between Alternate Routed To (ART) and Direct Routed (DR) traffic types. In the future, other distinctions between traffic could be identified that would expand the number of traffic types in Table 4. These additional traffic types could be assigned different control percentages (or excluded from ACC control, as in the case of priority calls), to give them different treatment during periods of congestion. An example would be to control hard-to-reach traffic as indicated in 5.5.4.

Methods used to achieve the percentages are implementation specific. Additional response categories could also be added to Table 4 to give greater flexibility and more response options to the ACC control.

TABLE 4/Q.542

An example of 2-congestion level ACC percentage control response table

Congestion level	Traffic type	Response category		
		A	B	C
CL1	ART DR	0 0	0 0	100 0
CL2	ART DR	100 0	100 75	100 75

5.5.3 Selective Circuit Reservation control

The Selective Circuit Reservation (SCR) Network Management control enables a digital exchange to automatically give preference to a specific type (or types) of traffic over others (e.g. direct routed calls over alternate routed calls) when circuit congestion is present or imminent. A digital exchange should provide either the single threshold of multithreshold version of the control, with the latter being preferred due to its greater selectivity.

5.5.3.1 General characteristics

A Selective Circuit Reservation control may be defined, for a given circuit group, by the following parameters:

- a reservation threshold(s); and
- a control response.

The reservation threshold defines how many circuits should be reserved for those traffic types to be given preferred access to the circuit group. The control response defines which traffic types should be given a lesser preference in accessing the circuit group, the quantity of each type of traffic to control, and how those calls denied access to the circuit group should be handled. Examples of possible traffic types are Direct Routed (DR), Alternate Routed To (ART), Hard-To-Reach (HTR), and various combinations thereof. The quantity of each type of traffic to be controlled when the threshold is exceeded may be represented by a percentage of the total traffic of that type. The control action options for further processing of calls denied access to the circuit group may be SKIP or CANCEL.

When the number of idle circuits in the given circuit group is less than or equal to the reservation threshold the exchange would, for that call, check the specified control response to determine if the call should be controlled. The SKIP response allows a call to alternate route to the next circuit group in the routing pattern (if any) while the CANCEL response blocks the call.

These parameters should be able to set locally in the exchange or by input from a network management centre. In addition, the network manager should have the capability to enable and disable the control, and to enable the control but place it in a state where the control does not activate (e.g. by setting the reservation threshold to zero).

5.5.3.2 Single-threshold Selective Circuit Reservation control

In this version of the control, only a single reservation threshold would be available for the specified circuit group.

Table 5 is an example of the flexibility that could be achieved in the control's response to circuit group congestion. Consider, for example, a case in which a network manager assigns response category "B", a reservation threshold of five circuits (RT1 = 5), and a control action of SKIP to a circuit group. Then, when the control is enabled, every time the number of idle circuits in the circuit group is less than or equal to 5, the exchange SKIPs 50 percent of the alternate routed traffic attempting to access the circuit group. Direct routed traffic has full access to the circuit group because the quantity of direct routed traffic to be controlled is zero percent. Note that the reservation threshold (in this example RT1 = 5) is the same for any of the response categories (A, B and C) that can be assigned to a circuit group. One or more response categories should be available from which to choose.

In the future, other distinctions between traffic could be identified that would expand the number of traffic types in Table 5. An example would be to control Hard-To-Reach traffic, as indicated in 5.5.4, or to give preference to priority calls.

5.5.3.3 Multi-threshold Selective Circuit Reservation control

The multi-threshold control would support two reservation thresholds for the specified circuit group. The purpose of multiple reservation thresholds would be to allow a gradual increase in the severity of the control response as the number of idle circuits in the circuit group decreased. The only restriction on the reservation thresholds would be that a reservation threshold associated with a more stringent control must always be less than or equal to the reservation threshold of any less stringent control, in terms of the number of reserved circuits (RT2 ≤ RT1 in Table 6).

Table 6 is an example of the flexibility that could be achieved in the control's response to circuit group congestion with two reservation threshold control. In the future, other distinctions between traffic could be identified that would expand the number of traffic types in Table 6, or to give preference to priority calls.

TABLE 5/Q.542

An example of a single threshold selective circuit reservation percentage control response table

Circuit group reservation threshold	Traffic type	Response category assigned to circuit group		
		A	B	C
RT1	ART	25	50	100
	DR	0	0	25

TABLE 6/Q.542

An example of a two threshold selective circuit reservation percentage control response table with HTR capability

Circuit group reservation threshold	Traffic type	Response category assigned to circuit group				
		A	B	C	D	E
RT1	ART-HTR	50	75	100	100	100
	DR-HTR	0	0	0	0	0
	ART-ETR	0	25	50	75	100
	DR-ETR	0	0	0	0	0
RT2	ART-HTR	100	100	100	100	100
	DR-HTR	0	25	50	75	100
	ART-ETR	50	50	75	100	100
	DR-ETR	0	0	25	50	75

5.5.4 Hard-to-reach (HTR) process

The hard-to-reach process for network management allows exchanges to automatically make more efficient use of network resources during periods of network congestion.

Part of the improved performance of automatic controls can be derived from the ability to distinguish between destinations that are easy-to-reach (ETR) and destinations that are hard-to-reach (HTR), i.e. destinations with a low answer bid ratio, and applying heavier controls to HTR destinations. This distinction can be based on:

i) internal performance measurements within the exchange/Network Management Operations System (OS) (for example, low Answer Bid Ratio (ABR) to a destination);

ii) similar information gathered by other exchanges;

iii) historical observations of network performance by network managers.

The network manager should have the ability to set the threshold for HTR determination and to assign manually a destination code as HTR.

5.5.4.1 Simplified HTR process components

To provide the fundamental elements of a simplified HTR process, the following capabilities must exist:

a) HTR administration;

b) HTR determination;

c) manually controlling calls as if hard-to-reach.

Items a) and b) may be entirely provided by the exchange or by a Network Management (OS) in cooperation with the exchange(s). Item c) can only be provided in the exchange.

a) *HTR administration*

Network managers will administer the HTR process to optimize the information obtained about current network performance. In order to properly administer the HTR system, network managers need four capabilities. These capabilities are listed below.

1) *Codes to be observed*

An exchange should automatically collect ABR data for some destination areas, e.g. countries, area codes, etc. In addition, network managers should have the capability to designate/change destinations an exchange should monitor in greater detail. An exchange should accept at least three network management designated sets of digits that identify a specific destination area and automatically begin surveillance of the specified destination areas. The specific number of digits to be analyzed is left to the discretion of the Administration and may be exchange dependent.

2) *Administration of HTR thresholds*

There should be a set of thresholds used to monitor destination areas and another set for use when monitoring destinations in greater detail. Network managers should be able to specify/change the values of "B" and "T" for the pre-established threshold sets and the HTR hysteresis modifiers [see b), sub-item 3), below].

3) *Administration of HTR determination exclusion*

A network manager should have the capability to exclude destination codes from being determined as HTR. This should prevent these destination codes from automatically being calculated as HTR and prevent these destination codes from being automatically placed on the "HTR Control" list. A network manager should also have the ability to restore destination codes to the fully automatic HTR determination function.

4) *Administrative review of HTR list*

Network managers should have the capability to view the contents of the "HTR Control" list, either via a terminal at the exchange or remotely through a Network Management OS. The list should indicate which destination codes have been manually designated as HTR [see c) below]. In addition, network managers should have access to a list of those destination codes which have been manually excluded from automatic HTR determination.

b) *HTR determination*

The capability should exist to determine automatically which destination codes are HTR. This is based on three capabilities.

1) *Code measurements*

The HTR/ETR status of a destination is based on analyzing the data for groupings of routing digits. An exchange should take measurements based on a sufficient number of routing digits to identify a destination. The exchange should take those measurements necessary to calculate the ABR for each such destination.

2) *HTR calculations*

Periodically, the ABR for these destination codes under surveillance should be calculated. A recommended time interval is every 5 minutes.

3) *Determining destination code HTR/ETR status*

For each destination code, the capacity should be provided to compare the number of bids and the calculated ABR to a set of pre-established thresholds. There should be a set of thresholds applicable to determining HTR destination areas and another set for destinations being monitored in greater detail.

A set of pre-established threshold consists of:

– B: Bids; the number of calls received by an exchange for a given destination code. This count includes calls that are successfully forwarded to the succeeding exchange as well as calls that fail within the current exchange.

– T: ETR threshold; the threshold above which a destination code's ABR should be considered ETR.

A destination code would be considered HTR if, based on the 5-minute calculations, the measured number of bids to the code is greater than or equal to threshold "B" and the ABR is less than or equal to threshold "T".

A destination code that is determined to be HTR should be placed on a "HTR Control" list in the exchange.

To avoid having destination codes oscillate on and off the "HTR Control" list, hysteresis modifiers should be applied to determine when destination codes should be removed from the "HTR Control" list. In succeeding 5-minute periods, these hysteresis modifiers should be applied to both values "B" and "T" when it is time to recalculate the HTR/ETR status of the destination code.

At the beginning of each 5-minute period, the "HTR Control" list should be reviewed. If a destination code that was calculated to be HTR is determined to be no longer than HTR, then it should be removed from the "HTR Control" list.

c) *Manually controlling calls as if HTR*

A network manager should have the capability of specifying any destination code as HTR so as to cause automatic network management control actions to take place within the exchange as indicated in 5.5.4.2. The manually specified destination code(s) may go on the "HTR Control" list. They should not, however, be subject to the 5-minute review and removal procedure described above. They should be removed upon request of a network manager. To this end, a network manager should have the capability of ending this stimulus to identifying a destination code as HTR.

Whenever a network manager adjusts the HTR status of a destination code, that manual action should take precedence over any automatic actions for that destination code.

5.5.4.2 Controlling calls based on HTR status

When a call to a destination code that is on the "HTR Control" list is being routed and a manual or automatic network management control is encountered during the processing of the call, the control should take into account the fact that the destination code is HTR. If a destination code is on the "HTR Control" list, then the call should be considered HTR for all outgoing circuit groups.

As an example of an automatic network management control incorporating HTR, the Automatic Congestion Control (ACC) response percentage table (Table 4) could be expanded to apply more stringent controls to HTR traffic, as shown in Table 7. A similar application of the Selective Circuit Reservation control is possible (see 5.5.3).

TABLE 7/Q.542

Example of automatic congestion control response percentages with HTR

Congestion level	Traffic type	Response category				
		A	B	C	D	E
CL1	ART-HTR	0	0	100	100	100
	DR-HTR	0	0	0	100	100
	ART-ETR	0	0	0	0	0
	DR-ETR	0	0	0	0	0
CL2	ART-HTR	100	100	100	100	100
	DR-HTR	0	100	100	100	100
	ART-ETR	0	0	0	100	100
	DR-ETR	0	0	0	0	75

5.5.5 Temporary Trunk Blocking

Temporary Trunk Blocking (TTB) is an alternative method of exchange congestion control for application in national networks.

When an exchange is in a low level overload condition, a Temporary Trunk Blocking signal may be sent to a preceding exchange to indicate that the release or re-occupation of a trunk should be delayed for a short (e.g. 100 s) period of time. This may permit an overall level of up to the maximum possible load in the overloaded exchange without need to generate ACC signals. The preferred method of conveying the TTB signal is via the relevant common channel signalling system.

The exchange receiving the Temporary Trunk Blocking signal will delay the release or the re-occupation of the concerned trunk for a short time. This time should be made changeable by operating personnel command.

The duration of trunk blocking is limited by a timer in the exchange receiving the Temporary Trunk Blocking signal. Therefore, an unlimited blocking of the trunk is avoided.

5.5.6 Application

5.5.6.1 ACC

Generally, where an Administration has introduced or is planning to introduce network management controls, it is considered appropriate for digital transit and large digital combined local/transit exchanges to be provided with full ACC capabilities. Digital local and smaller combined local/transit exchanges should only be provided with ACC receive and control capabilities.

5.5.6.2 SCR

It is considered appropriate for digital transit and large digital combined local/transit exchanges to be provided with a two-threshold Selective Circuit Reservation Network Management Control. Network Management of digital local and smaller combined local/transit exchanges could benefit from having available, ideally, the two threshold or the single threshold Selective Circuit Reservation Network Management Control. The decision whether or not to provide this control in these exchanges is left to the discretion of the various Administrations.

5.5.6.3 HTR

It is considered appropriate for digital transit and large digital combined local/transit exchanges (optionally in conjunction with a Network Management OS) to be provided with full HTR capabilities. Digital local and smaller combined local/transit exchanges should only be provided with the manual HTR and HTR controlling (based on HTR status) capabilities, i.e. those capabilities found in 5.5.4.1 c), and 5.5.4.2. It is also recommended that control modifications, based on HTR status, be added to both the ACC and Selective Circuit Reservation capabilities.

5.5.6.4 TTB

It is considered appropriate for TTB to be provided in digital transit and large digital combined local/transit exchanges in national applications. It may be particularly useful in exchanges that may not be provided with ACC capabilities, such as local exchanges.

5.6 Order of application of controls

The order in which various network management controls shall be applied in an exchange is for further study.