INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

E.412

(01/2003)

SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

Network management – International network management

Network management controls

ITU-T Recommendation E.412

ITU-T E-SERIES RECOMMENDATIONS

OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

INTERNATIONAL OPERATION	
Definitions	E.100–E.103
General provisions concerning Administrations	E.104–E.119
General provisions concerning users	E.120–E.139
Operation of international telephone services	E.140–E.159
Numbering plan of the international telephone service	E.160–E.169
International routing plan	E.170–E.179
Tones in national signalling systems	E.180–E.189
Numbering plan of the international telephone service	E.190–E.199
Maritime mobile service and public land mobile service	E.200–E.229
OPERATIONAL PROVISIONS RELATING TO CHARGING AND ACCOUNTING IN THE INTERNATIONAL TELEPHONE SERVICE	
Charging in the international telephone service	E.230–E.249
Measuring and recording call durations for accounting purposes	E.260–E.269
UTILIZATION OF THE INTERNATIONAL TELEPHONE NETWORK FOR NON-TELEPHONY APPLICATIONS	
General	E.300–E.319
Phototelegraphy	E.320–E.329
ISDN PROVISIONS CONCERNING USERS	E.330–E.349
INTERNATIONAL ROUTING PLAN	E.350–E.399
NETWORK MANAGEMENT	
International service statistics	E.400–E.409
International network management	**E.410–E.419**
Checking the quality of the international telephone service	E.420–E.489
TRAFFIC ENGINEERING	
Measurement and recording of traffic	E.490–E.505
Forecasting of traffic	E.506–E.509
Determination of the number of circuits in manual operation	E.510–E.519
Determination of the number of circuits in automatic and semi-automatic operation	E.520–E.539
Grade of service	E.540–E.599
Definitions	E.600–E.649
Traffic engineering for IP-networks	E.650–E.699
ISDN traffic engineering	E.700–E.749
Mobile network traffic engineering	E.750–E.799
QUALITY OF TELECOMMUNICATION SERVICES: CONCEPTS, MODELS, OBJECTIVES AND DEPENDABILITY PLANNING	
Terms and definitions related to the quality of telecommunication services	E.800–E.809
Models for telecommunication services	E.810–E.844
Objectives for quality of service and related concepts of telecommunication services	E.845–E.859
Use of quality of service objectives for planning of telecommunication networks	E.860–E.879
Field data collection and evaluation on the performance of equipment, networks and services	E.880–E.899

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

ITU-T Recommendation E.412

Network management controls

Summary

Network management controls provide the means to alter the flow of traffic in the network in support of the network management entities given in ITU-T Rec. E.410. Most network management controls are taken by or in the exchange (see ITU-T Rec. Q.542), but certain actions can be taken external to exchange. This Recommendation provides specific information on network management controls and gives guidance concerning their application. However, it should be noted that the suggested use for each network management control is given only for the purpose of illustration. Other controls, separately or in combination, may be more appropriate in any given situation.

Source

ITU-T Recommendation E.412 was prepared by ITU-T Study Group 2 (2001-2004) and approved under the WTSA Resolution 1 procedure on 13 January 2003.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. 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 Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

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

NOTE

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

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

ITU-T Recommendation E.412

Network management controls

1 Introduction

1.1 Network management controls provide the means to alter the flow of traffic in the network in support of the network management entities given in ITU-T Rec. E.410. Most network management controls are taken by or in the exchange (see ITU-T Rec. Q.542), but certain actions can be taken external to the exchange. This Recommendation provides specific information on network management controls and gives guidance concerning their application. However, it should be noted that the suggested use for each network management control is given only for the purpose of illustration. Other controls, separately or in combination, may be more appropriate in any given situation.

1.2 The application or removal of network management controls should be based on network performance data which indicates that action is required in accordance with the network management principles in clause 4/E.410. Performance data will also measure the effect of any network management control taken, and will indicate when a network management control should be modified or removed (see ITU-T Recs E.411 and E.502).

1.3 Controls can be activated or removed in an exchange by input from a network management operations system or by direct input from a terminal. In some cases, controls can be activated automatically either by external or internal stimulus, or when a parameter threshold has been exceeded. The Automatic Congestion Control (ACC) system is an example (see 4.1). When automatic control operation is provided, means for human override must also be provided.

2 Traffic to be controlled

2.1 Considerations for the application of controls

Exchanges should be capable of applying a range of network management controls (see ITU-T Rec. Q.542). For increased flexibility and precision, there is considerable advantage when the effect of a control can be limited to a particular specified traffic attribute.

A network management control may be specified by selecting the entities, traffic attributes and the operating parameters to be controlled.

The entities to which the control is applied can be:

– circuit groups;
– destinations;
– exchanges;
– intelligent network nodes.

The traffic attributes can include:

– traffic type (e.g., direct/alternate routed, hard-to-reach/easy-to-reach, priority/non-priority);
– service type (e.g., transmission medium requirements (see ITU-T Rec. E.172), ISUP preference indicator, calling party's category (see ITU-T Rec. Q.763), bearer services);
– traffic source (e.g., operator-originated, customer-originated, access indicator (ISDN or POTS), transit, rerouted, inbound from foreign network).

The operating parameters can include:

– amount of traffic to be controlled (i.e., percentage or call rate);
– threshold(s) for control activation;
– disposition of controlled call attempts (i.e., skip/cancel where applicable);
– handling of blocked calls (e.g., busy tone, special recorded announcement).

Only some of the entities, traffic attributes and operating parameters may be valid for a particular control. Although it would be convenient to have the maximum flexibility for the above parameters in the implementation of NM controls, only some of the parameters are strictly required for each control. The introduction of new parameters for controls in the ISDN and intelligent networks is for further study.

The specification of operating parameters and traffic attributes will enable a control to be more precise in its effect. Precision is of vital importance when applying controls, particularly in the case of protective controls.

In Annex A, an overall view of how the controls may be related to the managed entities, traffic types and the amount of traffic to be controlled are considered.

2.2 Hard-to-Reach (HTR) process

2.2.1 A hard-to-reach process for network management will enable exchanges to automatically make more efficient use of network resources during periods of network congestion by improving the performance of network management controls.

This improved performance is derived from the ability to distinguish between destinations that are Easy-to-Reach (ETR) and destinations that are Hard-to-Reach (HTR), (e.g., destinations with a low answer bid ratio) and applying controls to HTR traffic.

To determine if a destination is HTR by internal performance measurements, the Answer Bid Ratio (ABR) should be automatically calculated within an exchange or Network Management Operations System (NMOS) for the designated destination codes (e.g., countries, area codes, city codes, etc.) for a sufficient number of digits to identify the destination.

Thresholds for the ABR should be defined and manually set in the NMOS or exchange by network managers so HTR traffic can be determined based on the thresholds. (See ITU-T Rec. Q.542 for additional details.) The thresholds will vary for different destinations and should be based on historical data and adjusted by the network managers.

From network managers observations, destinations can be determined to be HTR and manually designated HTR. Network managers may also decide to exclude some destinations manually from automatic HTR determination based on their knowledge of current network events. Destinations may also be designated as HTR based on information automatically received from connected exchanges.

Once a destination has been determined to be HTR (either automatically by calculation or manually by the network manager, or by information received automatically from other exchanges), the destination should be placed on the "HTR control" list in the exchange. The network managers should have the capability to view the "HTR control" list through a terminal at the exchange or remotely through the NMOS. For destinations that were calculated as HTR it is recommended that every 5-minute period the "HTR control" list is updated, and destinations no longer calculated as HTR should be removed from the control list. To prevent destinations from repeatedly being put on and taken off the "HTR control" list, a hysteresis modifier should be applied to the threshold values. (See ITU-T Rec. Q.542 for additional details.) For manually declared HTR codes, the network manager should decide when to remove the HTR codes from the list; these manual codes should not be subject to the automatic 5-minute review. HTR destinations that were automatically placed on the HTR control list should be removed by the expiration of a timer if not refreshed by new information received from the connected exchange.

The use of Answer Seizure Ratio (ASR) for HTR determination is for further study.

2.2.2 Controlling traffic based on HTR status

When a call to a destination that is on the HTR list is being routed and a network management control on HTR traffic is encountered, the call should be controlled according to the relevant parameters. If a destination is considered HTR, it normally should be HTR for all outgoing circuit groups.

2.2.3 HTR information exchange

Although network managers can readily determine HTR traffic from information in their exchanges, it requires additional information to determine a destination's HTR status from exchanges in other Administration's networks. In situations where such an exchange is being used as a transit point, either for inbound traffic or for traffic destined for a third Administration, the network manager for the originating Administration may not know what happens beyond the next exchange unless that Administration provides him with that information. When two Administrations share HTR information, both can increase their number of call completions during periods of congestion. An Administration who has been sending HTR traffic can now, during periods of congestion, give preference to ETR traffic. During periods of network congestion, this would result in a higher utilization of available circuits for ETR traffic and increase call completions with the attendant increase in revenues. The Administration who would have received the HTR traffic will benefit by a decrease in the amount of HTR traffic received.

For the international exchange of HTR information, the identification of the destination is based on the international number that "consists of the country code of the required country followed by the national (significant) number of the called subscriber" (see ITU-T Rec. E.160).

2.2.3.1 Overview of HTR information exchange

ITU-T Rec. Q.542 describes the building of the "HTR control" list that contains problem destination codes used during the application of HTR network management controls. The exchange can use the control list to keep track of those HTR destination codes calculated by the exchange, the HTR destination codes received from other Administrations and any mutually entered HTR destination codes. This list would be used for controlling originating traffic while a second list, a source list, would keep track only of those HTR codes calculated by the exchange. When a call is received from an Administration destined for a destination on the source list, the exchange may use the HTR indicator to notify the Administration. Alternatively, the single control list may be used in the exchange.

2.2.3.2 Administration agreements

One subject to be considered by participating Administrations is the basis of the HTR information that will be transferred. The participating Administrations will want to know other details about the HTR status besides the state of being HTR and the number of digits of the called number. These details may include:

– minimum and maximum number of digits on which a control may be placed by the receiving Administration;
– the ABR and threshold on which the HTR status was based;
– the frequency with which the HTR data is calculated or updated in the source list;
– the actions taken by the Administration receiving HTR information.

As is the case with all information that is automatically transmitted between exchanges belonging to different Administrations, it must be determined through mutual agreement how the receiving Administration's exchange(s) should react to the received information. Of special concern is how frequently the HTR information is updated in the receiving Administration's exchanges. If a called number is HTR and a control is active, traffic to that destination may be controlled until the expiration of the HTR control list timer. At the end of this time, traffic to the destination may be resumed unless another HTR indicator is received.

2.2.3.3 Methods of exchanging HTR data

Methods for the international exchange of HTR data can be based on:

- Signalling System No. 7 messages;
- a dedicated facility between NMOSs to provide information exchange on an OS to OS basis;
- Foreign Administration manual notification (e.g., telephone).

2.3 Methods for specifying the amount of traffic to be controlled

2.3.1 Call percentage control

With the call percentage control method, exchange controls can be activated to affect a specified percentage of traffic (for example 10%, 25%, 50%, 75% or 100%).

2.3.2 Call rate control

With the call rate control method, an upper limit on the rate that calls are allowed to access the network is established (for example – 4 calls per minute).

Three methods of implementing call rate controls have been identified:

a) *Method 1 – (Continuous timer)*: With this method a continuously running timer with an adjustable duration is used. Once the allowable number of call attempt(s) are handled within a timer cycle, no further call attempts are allowed until the timer expires. This method has two variables: time and number of calls. (An example of an upper limit using this method would be no more than 2 calls per 30 seconds).

b) *Method 2 – (Asynchronous timer)*: With this method, a timer with a specified duration is started when a call attempt is allowed. No further call attempts are allowed until the timer expires. When another call attempt is allowed, the timer is restarted. This method has one variable (time). An example of an upper limit using this method would be one call per 15 seconds.

c) *Method 3 – (Leaky bucket):* With this method, a dynamic counter (leaky bucket counter) is used. The treatment of a call attempt depends on the current counter value. If the counter exceeds the defined maximum size, the call is rejected (bucket is full). If the counter is less than the maximum size, the call is accepted (bucket is not full) and the counter is incremented. The counter is decremented at defined intervals (bucket leaks) making it possible for new calls to be accepted. The method has two variables: the bucket size and the throughput (decrement per time unit).

The performances of such methods, with particular reference to their capability to handle bursts of traffic, are left for further study.

3 Exchange controls

Network management controls may be applied in exchanges to control traffic volume or to control the routing of traffic. The resulting effect on traffic of these controls may be expansive or protective, depending on the control used, its point of application and the object selected for control.

3.1 Traffic volume controls

Traffic volume controls generally serve to control the volume of traffic offered to a circuit group or a destination. These include the following.

3.1.1 Destination controls

3.1.1.1 Code blocking

This control bars routing for a specific destination on a percentage basis. Code blocking can be done on a country code, an area code, an exchange identifying code or an individual line number. The last of these is the most selective control available.

Typical application: Used for immediate control of focused overloads or mass-calling situations.

3.1.1.2 Call-gapping

This control sets an upper limit on the output rate that calls are allowed to be routed to the destination (for example – no more than 1 call every 30 seconds). With this control, the number of call attempts that are routed will never exceed the specified output rate, regardless of the arrival rate of the call attempts.

Typical application: Used for the control of focused overloads, particularly mass-calling to an individual line number. A detailed analysis may be required to determine the proper call-rate parameters.

3.1.2 Cancellation of direct routing

The control has effect on the amount of outgoing direct route traffic and can be achieved on one or more circuit subgroups. Two versions of the control are possible:

- Cancel Direct Routing To (DRT) is activated on outgoing circuit subgroup(s) and prohibits direct traffic to access the controlled circuit subgroup.
- Cancel Direct Routing From (DRF) is activated on outgoing circuit subgroup(s) and prohibits overflow of direct traffic from the controlled circuit subgroup.

This control blocks the amount of direct routed traffic accessing a circuit group.

Typical application: Used to reduce traffic to congested circuit groups or exchanges where there is no alternate routed traffic.

3.1.3 Circuit directionalization

This control changes both-way operated circuits to incoming operated circuits, either on a percentage basis or by a specified number of circuits. At the end of the circuit group for which access is inhibited, this is a protective action, whereas at the other end of the circuit group (where access is still available), it is an expansive action.

Typical application: To enhance the flow of traffic outward from a disaster area while inhibiting incoming traffic. To have an effect, it is recommended that the minimum amount of directionalization be at least 50%.

3.1.4 Circuit turndown/busying/blocking

This control removes one-way and/or both-way operated circuits from service, either on a percentage basis or by a specified number of circuits.

Typical application: Used to control exchange congestion when no other control action is available.

3.1.5 Specialized volume controls

The Automatic Congestion Control (ACC) system, the Selective Circuit Reservation control (SCR) and the Automatic Destination Control (ADC) can be considered as volume controls, but due to their specialized nature, they are described separately in 4.1, 4.2 and 4.3.

3.2 Routing controls

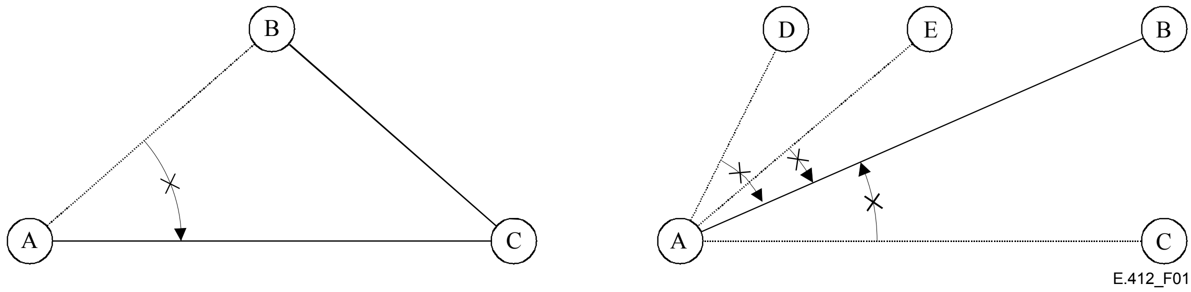
Routing controls are used to control the routing of traffic to a destination, or to or from a circuit group. However, it should be noted that in some cases a routing control may also affect the volume of traffic. Controls which are applied to circuit groups may also be applied to circuit subgroups, when appropriate.

3.2.1 Cancellation of alternative routing

The control has effect on the amount of outgoing alternative routed traffic and can be activated on one or more circuit groups. See Figure 1. Two versions of the control are possible:

- Cancel Alternative Routing From (ARF) is activated on an outgoing circuit group and prohibits traffic from overflowing to alternative circuit groups in the routing table.
- Cancel Alternative Routing To (ART) is activated on an outgoing circuit group and prohibits overflow traffic from accessing the controlled circuit group.

Typical application: There are many uses for this control. These include alternative routing in a congested network to limit multi-link connections, or to reduce alternative routed attempts on a congested exchange.



a) "Alternative Routing From" (ARF) cancellation on A-B circuit group

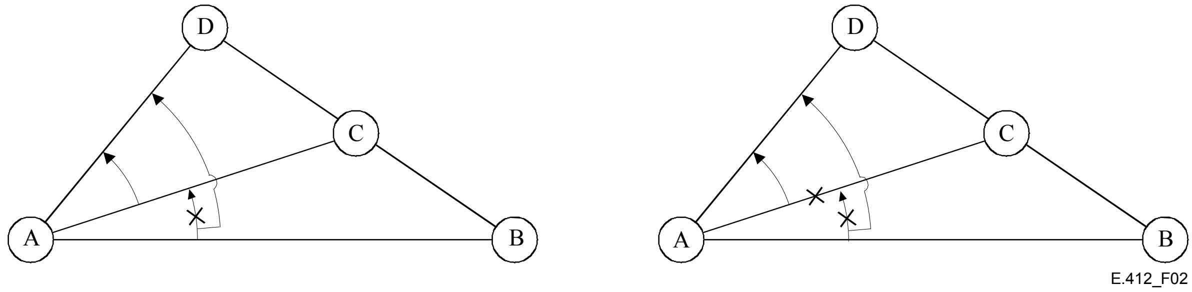
b) "Alternative Routing To" (ART) cancellation on A-B circuit group

Figure 1/E.412 – Examples of alternative routing mechanism

3.2.2 Skip control

The skip control is activated on an outgoing circuit group in a routing table and is used to force an amount of traffic to the next in-chain circuit group. The skip control can effect both direct and alternate routed traffic. The network manager must have the possibility to specify the type of traffic to be controlled.

Typical application: Used to bypass a congested circuit group or distant exchange when the next circuit group can deliver the call attempts to the destination without involving the congested circuit group or exchange. Application is usually limited to networks with extensive alternative routing. When used on both-way circuit groups, it has an expansive effect on traffic flow in the opposite direction. See Figure 2.



a) Skip alternative routing traffic on A-C circuit group

b) Skip direct and alternative routing traffic on A-C circuit group

Figure 2/E.412 – Examples of skip

3.2.3 Temporary alternative routing

Temporary Alternative Routing (TAR) is an expansive control which temporarily increases the number of routing possibilities for an amount of calls to controlled destinations. One or several circuit groups, which are not normally available in the normal routing plan are made available. The TAR circuit groups must terminate on an exchange that has the capability of reaching the destination. The entity to which the TAR is applied can be either destinations and/or circuit groups.

If during the period of application of the TAR control, the new circuit group(s) become congested or otherwise unavailable, it should be possible to either re-enter the original routing plan or to block the calls based on an operator-activated command.

The control should apply to all types of traffic except calls which previously have been controlled by TAR. This requires a unique identification of TAR controlled calls. If Signalling System No. 7 with ISUP is available the TAR controlled call could be indicated in the Initial Address Message (IAM), this indication must follow the call along its set-up path. This is important in order to prevent circular routing. The cancel re-routed overflow control can help to prevent circular routing (see 3.2.4).

These additional circuit group(s) can be:

a) added at the end of a routing table to provide additional overflow path(s);

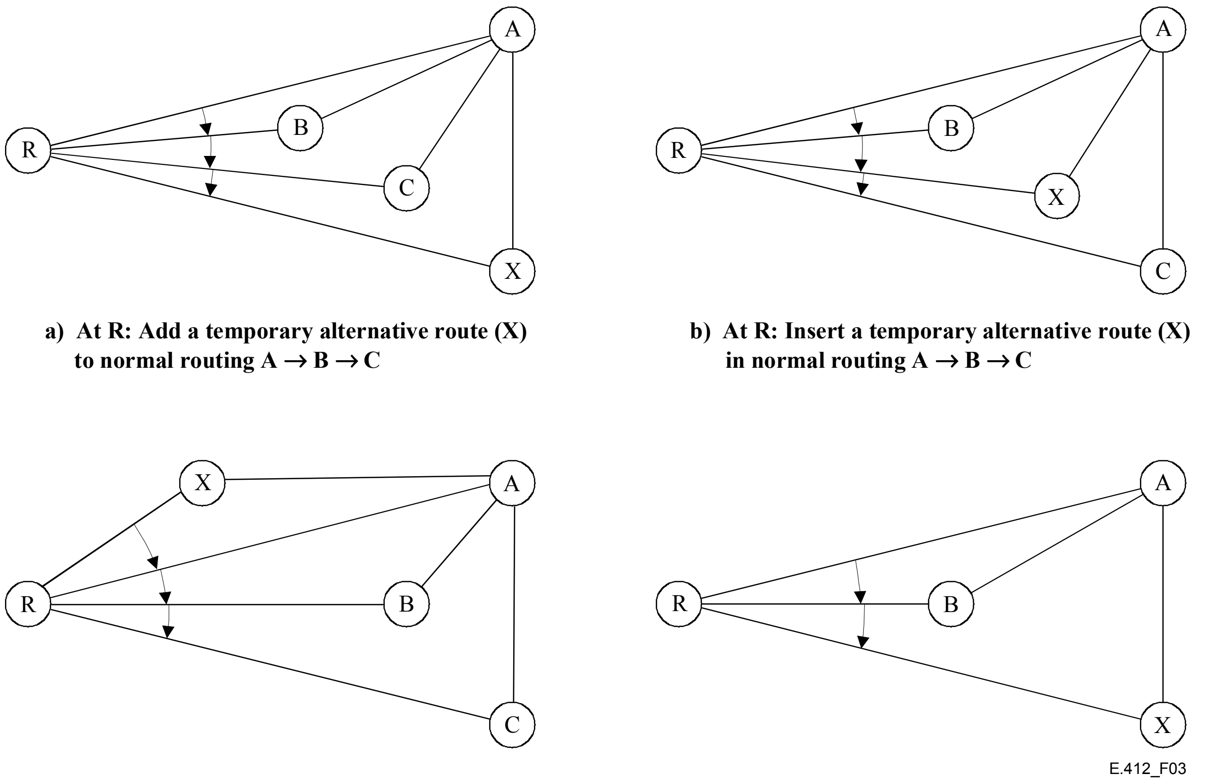
b) inserted into the routing table between existing circuit groups to provide additional overflow path(s);

c) added at the beginning of a routing table so traffic will be first offered to the additional circuit group(s);

d) used to replace circuit group(s) can also be used to replace circuit group(s) in the routing table.

Typical application: To increase the number of successful calls and to improve the quality of service to customers during periods of congestion.

Examples can be found in Figure 3.



a) At R: Add a temporary alternative route (X) to normal routing A → B → C

b) At R: Insert a temporary alternative route (X) in normal routing A → B → C

c) At R: Add a temporary alternative route (X) at the beginning of normal routing A → B → C

d) At R: Replace with a temporary alternative route (X) the route C in normal routing A → B → C

Figure 3/E.412 – Examples of temporary alternative routing

3.2.4 Cancel re-routed overflow

This control prevents additional re-routing or alternate routing of a re-routed call. Re-routed calls are not allowed to overflow the circuit group to which the cancel re-routed overflow control is applied, while normal overflow traffic is not affected. This requires the ability to uniquely identify re-routed calls.

Typical application: To prevent the use of an excessive number of international circuits in tandem and/or to prevent circular routing.

3.2.5 Special recorded announcements

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

Typical application: Used to notify customers of unusual network conditions, and to modify the calling behaviour of customers and operators when unusual network conditions are present. Calls that are blocked by other network management controls can also be routed to a recorded announcement.

4 Automatic exchange controls

Automatic dynamic network management controls represent a significant improvement over conventional controls. These controls, which are pre-assigned, can quickly respond to conditions internally detected by the exchange, or to status signals from other exchanges, and are promptly removed when no longer required. Automatic control applications should be planned, taking into account the internal overload control strategy provided in the exchange software.

4.1 Automatic congestion control system

4.1.1 Automatic congestion control system: method 1

4.1.1.1 Exchange congestion

When a digital international/transit exchange carries traffic above the engineered level, it can experience an overload that diminishes its total call processing capability. Because of the speed of the onset of such congestion and the critical nature of the condition, it is appropriate that control be automatic. The Automatic Congestion Control (ACC) system consists in the congested exchange sending a congestion indicator to the connected exchange(s) using common channel signalling. The exchange(s) receiving the congestion indication can respond by reducing a certain percentage of the traffic offered to the congested exchange, based on the response action selected for each application.

4.1.1.2 Detection and transmission of congestion status

An exchange should establish a critical operating system benchmark, and when continued levels of nominal performance are not achieved (e.g., due to excessive traffic), a state of congestion is declared. Thresholds should be established so that the two levels of congestion can be identified, with Congestion Level 2 (CL2) indicating a more severe performance degradation than Congestion Level 1 (CL1). When either level of congestion occurs, the exchange should have the capability to:

1) code an ACC indication in the appropriate common channel signalling messages; and
2) notify its network management centre and support system of a change in its current congestion status.

4.1.1.3 Reception and control

When an exchange receives a signal that indicates a congestion problem at a connected exchange, the receiving exchange should have the capability to reduce the number of seizures sent to the congested exchange.

An exchange should have the capability of:

1) assigning an ACC response action on an individual circuit group[1] basis, as specified by the network manager; and
2) notifying its network management centre and support system of a change in congestion status received from a distant exchange.

There should be several response categories available in the exchange. Each category would specify the attribute and amount of traffic to be controlled in response to each of the received ACC indicators. The categories could be structured so as to present a wide range of response options.

---

[1] In this context, the term "circuit group" refers to all of the outgoing and both-way circuit subgroups which may directly connect the congested exchange and the responding exchange.

For a specific ACC response category, if the received ACC indicator is set to a CL1 condition, then the receiving exchange could, for example, control a percentage of the alternate routed to (ART) traffic to the affected exchange. The action taken by the control would be to either skip or cancel the controlled calls, depending on the ACC response action that was assigned to that circuit group. In a similar manner, if a CL2 condition is indicated, then the receiving exchange could control all ART traffic and some percentage of Direct Routed (DR) traffic. Other options could include the ability to control hard-to-reach traffic, or transit traffic. Response categories could also be expanded to include service-specific controls. This would be particularly useful in the transition to ISDN.

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

Table 1 is an example of the flexibility that could be achieved in response to a signal from an exchange that is experiencing congestion. In this example, different control actions would be taken based upon the distinction between ART and DR traffic types. These actions could represent the initial capabilities available with the ACC control. Other alternatives could include the ability to control hard-to-reach traffic (see 2.2), or transit traffic or to provide other controls such as call-gapping. Additional response categories could also be added to Table 1 to give greater flexibility and more response options to the ACC control. It could also be possible to exclude priority calls from ACC control.

Table 1/E.412 – An example of ACC control response

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

4.1.1.4 Any international application of ACC should be based on negotiation and bilateral agreement among the affected Administrations. This includes an agreement as to whether the controlled calls should be skipped or cancelled. Application within a national network would be a national matter. An exchange that is capable of "ACC receive and control" should not indiscriminately assign ACC to all routes since a distant exchange may be equipped for common channel signalling, but may not yet have an ACC transmit capability. This could result in invalid information in the ACC fields in the signalling messages and the inappropriate application of ACC controls at the receiving exchange. Additional details on the ACC system are in UIT-T Rec. Q.542.

4.1.2 Automatic congestion control system: method 2

4.1.2.1 Terminology

Source exchange. An exchange that receives a call cleardown message (in ISUP, a Release message) containing an overload indication (in ISUP, with the Automatic Congestion Level (ACL) parameter set to 1 or 2) from an (overloaded) exchange to which it is directly connected.

4.1.2.2 Exchange behaviour under overload

When a digital international/transit exchange receives call set-up requests at a sufficiently high rate, it can experience processing overload that leads to long call set-up times. These in turn will make it likely that customers will abandon their calls in set-up, and make subsequent repeat attempts. To counter this, the exchange must have an internal overload control that rejects part of the stream of call set-up requests in order to maximize the rate at which calls are admitted and successfully processed, subject to keeping processing delays suitably low, and maintaining correct call handling.

In an exchange with a distributed processing architecture, call processing is divided between different sets of resources, with each call being processed by several resources. For example, call processing is often divided between several peripheral processors that handle subsets of customer lines or trunk routes, and one or more pools of load-balanced central processors that handle call routing, charging, IN triggering, etc. A call would then usually be processed by two peripheral processors (one on the incoming side and one on the outgoing side), and by one or more central processors.

For a distributed architecture, the internal overload control has to be able to monitor the processing load of the different resources, and to take action to reject some of the call set-up requests that require processing at an overloaded resource. The act of rejecting call set-up requests will itself consume some of the processing capacity available at an exchange. This is due either to the processing made before rejecting a call set-up request, or due to the processing required for the rejection itself. (Some processing before a call is rejected is necessary in order to discriminate in favour of priority-marked calls, or so that subsequent demand, after the initial admitted set-up request, is not lost).

Now, in a distributed architecture, the rejection of call set-up requests may itself consist of several individual rejection processes distributed over various internal processing resources. It then matters, when a resource is overloaded, whether:

1) there are *no* internal points of rejection that can protect it (i.e., points where set-up requests that are going to be processed by the overloaded resource may be rejected before arriving at it) but the overloaded resource can itself reject set-up requests arriving at it; or
2) there are *no* internal points of rejection that can protect it, nor can the overloaded resource itself reject set-up requests arriving at it; or
3) there *are* one or more internal points of rejection that can protect it.

These 3 cases are illustrated in Figures 4, 6 and 7, respectively. (In each figure 'R' denotes a point of rejection, and a circle denotes a processing resource, or pool of load-balanced resources.)

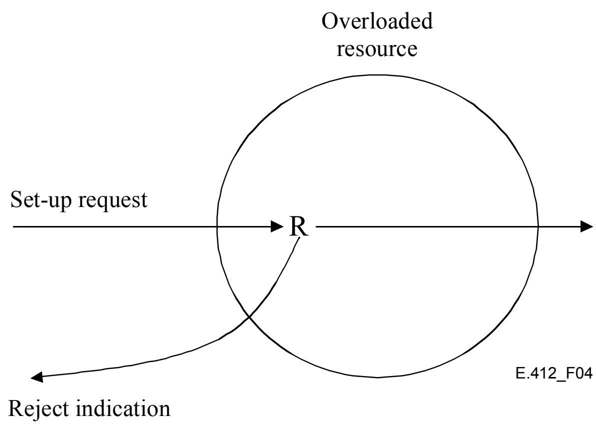


Figure 4/E.412 – Case 1

In case 1, when a call set-up request arrives at an overloaded resource and is rejected by the rejection process running on the resource, then a rejection indication is returned to the neighbouring exchange. The processing effort to reject a call set-up request will erode the useful capacity of the overloaded resource. That erosion will increase as the rate of call set-up requests that require the overloaded resource grows. This can lead to a significant erosion of the useful call processing capacity at the overloaded exchange, and ultimately to failure of the exchange, as illustrated in Figure 5.

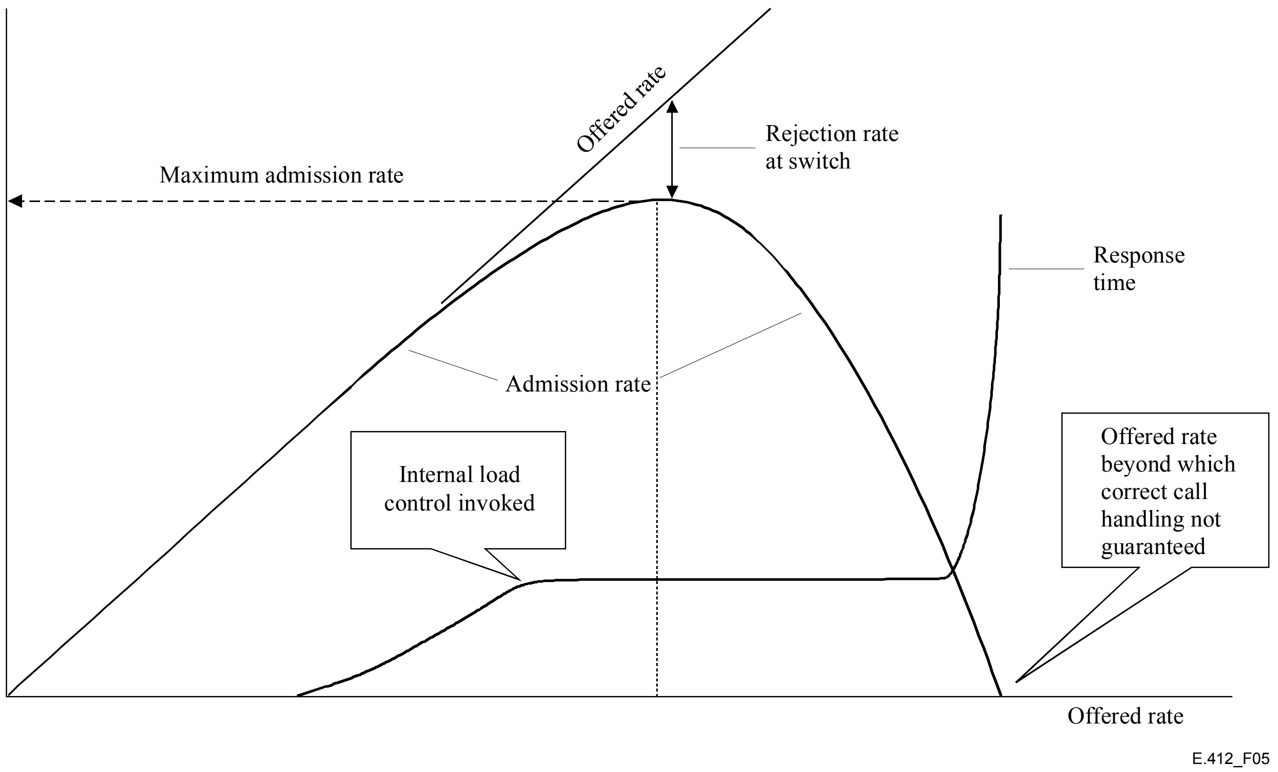


Figure 5/E.412 – Throughput curve of overloaded resource

In this case, it is therefore essential to reject call set-up requests (destined for the overloaded exchange) at its neighbouring exchanges: external call rejection is required. Note that if the external overload controls adapt the rate they admit call set-up requests so that the reject rate from the overloaded resource is small, then the successful admission rate at the overloaded resource will be close to its maximum.

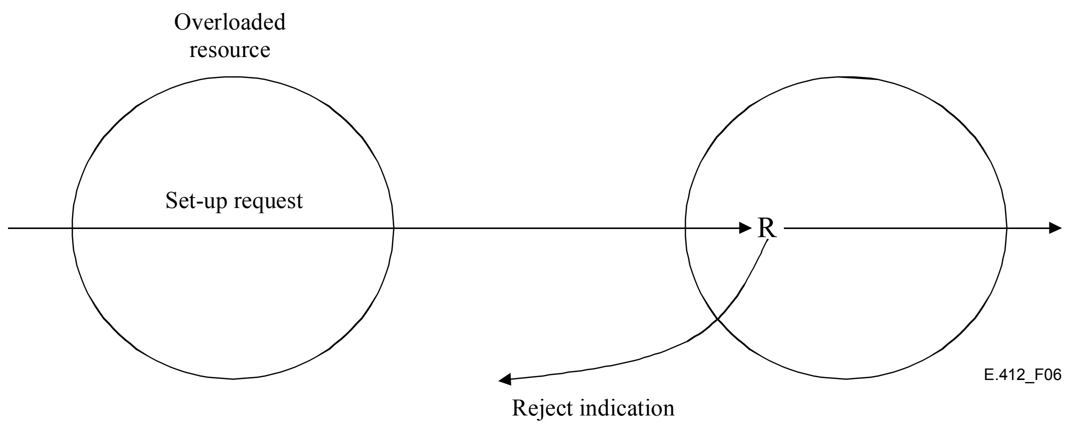


Figure 6/E.412 – Case 2

In case 2, the overloaded resource is not itself able to reject call set-up requests, and no points of restriction are encountered by call set-up requests *before* arriving at it. As with case 1, it is necessary to invoke external call rejection at the appropriate neighbouring exchange in order to protect the overloaded resource.

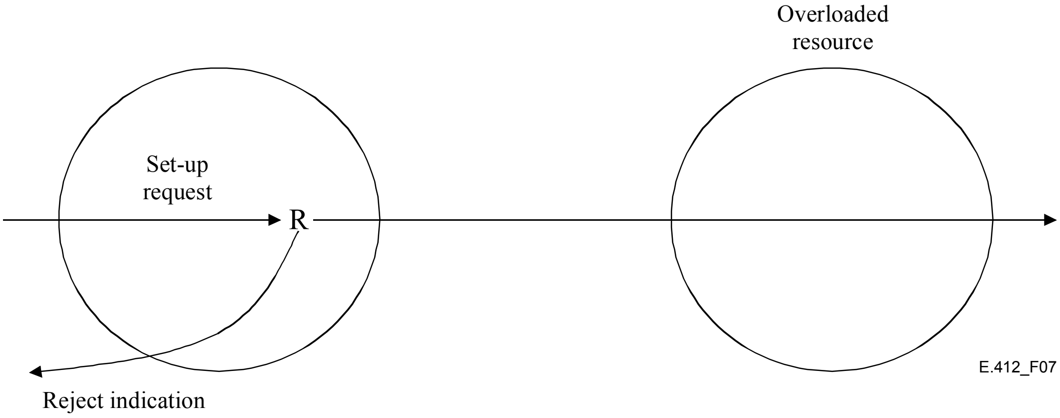


Figure 7/E.412 – Case 3

In case 3, call set-up requests encounter an internal point of rejection which serves to protect the overloaded resource. In this case there is no need to invoke external call rejection. Internal call rejection has the advantage of only rejecting call set-up requests which use the overloaded resource – whereas invoking external call rejection at a neighbouring exchange would impact all call set-up requests including those not using the overloaded resource, because a neighbouring exchange has no way of knowing which of the call set-up requests it is sending to the overloaded exchange actually use the overloaded resource, and which do not.

It is concluded that an exchange should invoke external call restriction only when one or more overloaded resources cannot be protected by internal points of rejection (cases 1 and 2). The corresponding exchange state is called Overloaded-ExternalControlRequired (OECR).

If one or more internal resources are overloaded, but the exchange is not in state OECR, then it is said to be in state Overloaded-InternalControlRequired (OICR). If it is in neither of these two states, then it is in state NotOverloaded (NO).

Because of the speed of the onset of such congestion and the critical nature of the condition, it is appropriate that this invocation of external control be automatic. The Automatic Congestion Control (ACC) system consists in an exchange in state OECR sending a congestion indicator to the connected exchange(s) using common channel signalling. The exchange(s) receiving the congestion indication can respond by reducing the rate at which they send call set-up requests to the overloaded exchange.

4.1.2.3 Detection and transmission of congestion status

An exchange should establish one or more critical operating system benchmarks (for example processor occupancies, queue lengths, internal processing delays), and when continued levels of nominal performance are not achieved (e.g., due to excessive processing load), a state of congestion is declared (either Overloaded-InternalControlRequired or Overloaded-ExternalControlRequired). Thresholds should be established so that, when in state Overloaded-ExternalControlRequired, two levels of overload can be identified, with Congestion Level 2 (CL2) indicating a more severe performance degradation than Congestion Level 1 (CL1). When in state Overloaded-ExternalControlRequired, the exchange should have the capability to:

1) code an ACC indication in the appropriate common channel signalling messages; and

2) notify its network management centre and support system of a change in its current congestion status.

For ISUP, the ACC indication is made by coding the corresponding congestion level in the Automatic Congestion level (ACL) parameter added to all Release messages generated by the overloaded exchange (see 2.11/Q.764) when in state Overloaded-ExternalControlRequired.

When an exchange in state Overloaded-ExternalControlRequired or Overloaded-InternalControlRequired rejects a call, it shall do so as soon as possible, by sending a call cleardown message (i.e., for ISUP a Release message) in response to the call set-up request message (i.e., in response to the Initial Address Message).

NOTE 1 – This rules out the use of timers at source exchanges to detect that a neighbouring exchange is congested.

When a call is rejected because of processing overload by an exchange in state Overloaded-InternalControlRequired, the exchange shall include the appropriate call rejection cause in the call cleardown message generated (for ISUP, the Release message), but not the Automatic Congestion Level (ACL) parameter. This is to avoid invoking external control when it is not required. The cause value "switching equipment congestion" shall be used (for ISUP this is cause #42 – see ITU-T Rec. Q.850).

When a call is rejected because of processing overload by an exchange in state Overloaded-ExternalControlRequired, the exchange shall include the appropriate call rejection cause and an automatic congestion level (ACL) parameter, with the congestion level set according to the severity of the exchange congestion, in the call cleardown message generated. For ISUP, the rejection message is a Release message. The cause value "switching equipment congestion" shall be used where a call attempt is rejected because the exchange is congested.

NOTE 2 – Use of cause #42 is essential to avoid the external overload control (wrongly) counting calls rejected for reasons other than exchange overload. Otherwise, over-restriction is likely and the control may not converge to a steady state.

Under exchange congestion (that is, in states Overloaded-ExternalControlRequired and Overloaded-InternalControlRequired), a high proportion of the response times at the congested exchange, of calls carried by it, should be short in the attained steady state. (For example, the 95%-ile should typically not exceed 200 milliseconds). The response time is defined as the time from a call set-up request (in ISUP, an Initial Address Message) being admitted by the congested exchange to either a call set-up request being forwarded (if the congested exchange is not the destination for that call), or reception of the first backward call set-up message (if the congested exchange is the destination exchange for that call).

NOTE 3 – This requirement serves a dual purpose: it ensures that, when the control has settled down to a steady state, customers do not clear down due to long call set-up times (this is necessary to limit customer-initiated repeat attempts). It also limits the round trip delay from source exchange to congested exchange to source exchange, which improves the stability of the control.

When an exchange is in state NoOverload or in state Overloaded-InternalControlRequired, it should not add an ACC indication to the call cleardown messages that it generates.

4.1.2.4 Reception and control

When an exchange receives an ACC indication in a call cleardown message from a connected exchange, the receiving exchange should have the capability to reduce the rate it sends call set-up requests to the congested exchange. It should be possible for an operator to configure ACC method 2 so that this rate reduction is done only for calls that are not identified as having priority (for ISUP, see 3.11/Q.763).

An exchange should have the capability of:

1) applying ACC throttling on an individual circuit group[1] basis; and

2) notifying its network management centre and support system of a change in congestion status received from a distant exchange.

After taking appropriate action, the exchange shall discard any ACC parameter received in a call cleardown message; that is, it should not be passed on in the call cleardown message at an intermediate exchange.

4.1.2.4.1 Control activation

When a source exchange receives a message (which is a Release message in the case of ISUP) containing an ACL parameter, in response to a call set-up request sent to the overloaded exchange, then load restriction shall automatically cut in at the source exchange if it is not already active.

In order that an exchange congestion control should respond rapidly to the initial surge of calls in a congestion event, it is necessary that when restriction is activated at the source exchange, the initial level of restriction can be independently configured to be suitably severe.

NOTE 1 – It may be desirable to impose a more severe restriction in response to ACL2s than that in response to ACL1s.

It shall be possible to configure the control (at overloaded exchange and source exchanges) so that, during the initial transient response of the control (i.e., prior to the steady state being reached), the total calling rate (set-up requests/s) offered by all sources to the congested exchange should not reach a level at which correct call handling fails, in each 1 second period of all successive 1 second periods.

NOTE 2 – This requirement ensures that the exchange congestion controls react fast enough to prevent the load offered to the congested exchange from jeopardizing correct call handling. This requirement implies that when an exchange is in state Overloaded-ExternalControlRequired, and the exchange's internal congestion control rejects a call, it shall at once send a backward message containing an ACL parameter and indicating that the call has been rejected due to exchange congestion.

4.1.2.4.2 Adaptation of restriction level

If the rate at which an exchange in state Overloaded-ExternalControlRequired rejects calls from a source exchange indicates that the congested exchange's load is causing internal processing loads to be close to the capacity of the overloaded internal call processing resources, small changes only should be made by the source exchange to its restriction level.

NOTE 1 – This is to ensure convergence to the steady state.

The changes to the restriction level should be progressively larger (or more frequent) as the congested exchange's indicated load causes internal processing loads to depart further from the capacity of one or more overloaded internal call processing resources.

NOTE 2 – This is to ensure a rapid response to sudden changes (increases or decreases) in the offered calling rate.

If the rate at which an exchange in state Overloaded-ExternalControlRequired rejects calls is determined at the source exchange by counting released calls, then only calls in respect of which a cleardown message containing an ACC indication (in ISUP, a Release message containing an ACL1 or ACL2 parameter) and cause "switching equipment congestion" (#42 for ISUP, see ITU-T Rec. Q.850) is received in response to a call set-up request, shall be counted.

NOTE 3 – This requirement, together with an effective internal load control, ensures that the control will maximize the effective throughput of the overloaded internal call processing resources.

NOTE 4 – The congested exchange's condition could be estimated in ISUP, for example, by a source exchange measuring the rate at which the congested exchange sends Release messages containing an ACL parameter and Cause #42 in response to this source exchange's Initial Address Messages, and comparing this to a locally configured call reject rate for that congested exchange.

4.1.2.4.3 Termination of control

Automatic Congestion Control shall be terminated at a source exchange towards an overloaded exchange only when:

a) the rate the source's ACC mechanism rejects calls destined for the overloaded exchange; and

b) the rate the overloaded exchange rejects calls it receives from the source (by returning a call cleardown message with an ACC indication and cause switching equipment congestion),

have both been low for sufficient time (e.g., 2 minutes) to indicate that the exchange congestion has abated. This is essential to prevent the control repeatedly ending and restarting (at its initial severe restriction level).

4.1.2.4.4 Range of overload scenarios

The requirements on ACC method 2 should be automatically achieved for any overload scenario characterized by:

- A wide range in the number of source exchanges (e.g., 1 to 100 sources).
- A step increase in the total call set-up requests per second offered to the source exchanges (and destined for the overloaded exchange) from 0 to several times (e.g., 5 times) the rate of call set-up requests offered to the overloaded exchange at which it enters state Overloaded-ExternalControlRequired.
- A ramp increase over a short period (e.g., of duration 30 seconds) in the total call set-up requests per second offered to the source exchanges (and destined for the overloaded exchange) from 0 to several times (e.g., 5 times) the rate of call set-up requests offered to the overloaded exchange at which it enters state Overloaded-ExternalControlRequired, followed by a ramp decrease to 0 over a longer period (e.g., of duration 10 minutes).
- Any distribution of total call set-up requests per second among the source exchanges.
- A wide range of overloaded exchange capacities (e.g., 50 to 1000 calls per second).

4.1.2.5 Any international application of ACC should be based on negotiation and bilateral agreement among the affected Administrations. This includes an agreement as to whether the controlled calls should be skipped or cancelled. Application within a national network would be a national matter, but should also involve bilateral agreement between national telcos. An exchange that is capable of "ACC receive and control" according to method 2 should not indiscriminately assign ACC to all routes since a distant exchange may be equipped for common channel signalling, but may not yet have an ACC transmit capability. Additional details on the ACC system are in ITU-T Rec. Q.542.

4.2 Selective circuit reservation control

4.2.1 The selective circuit reservation control enables an exchange to automatically give preference to specific traffic attributes over others (e.g., direct routed calls over alternate routed calls) at the moment when circuit congestion is present or imminent. The selective circuit reservation control can be provided with one or more thresholds, with the latter being preferred due to its greater selectivity. Specific details on the selective circuit reservation control may be found in ITU-T Rec. Q.542.

4.2.2 General characteristics

The selective circuit reservation control has the following operating parameters:

- a reservation threshold(s);
- a control response;
- disposition of controlled call attempts.

The reservation threshold defines how many circuits or how much circuit capacity should be kept idle for those traffic attributes to be given preferred access to the circuit group. The control response defines which traffic attributes should be given a lesser preference in accessing the circuit group, and the quantity of each type of traffic to control. The disposition of controlled call attempts defines how those calls denied access to the circuit group should be handled. The disposition for processing of calls denied access to the circuit group may be skipped or cancelled.

When the number of idle circuits or the idle capacity in the given circuit group is less than or equal to the reservation threshold, the exchange would check the specified control response to determine if calls 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 be set locally in the exchange for each selected circuit group or by input from a network management operations system. 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). Further, the network manager should have the ability to set the values for the response categories.

4.2.3 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 2 is an example of the flexibility that could be achieved in the control's response to circuit group congestion. Other distinctions between traffic could be identified that would expand the number of traffic attributes in Table 2. An example would be to control service specific traffic, or to give preference to priority calls.

4.2.4 Multi-threshold selective circuit reservation control

The multi-threshold control provides several reservation thresholds for the specified circuit group. The purpose of multiple reservation thresholds is to allow a gradual increase in the severity of the control response as the number of idle circuits in the circuit group decreases. The only restriction on the assignment of 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, or circuit capacity.

Table 3 is an example of the flexibility that could be achieved in the control's response to circuit group congestion with a two-reservation threshold control. Other distinctions between traffic could be identified that would expand the number of traffic attributes in Table 3.

An example would be to control hard-to-reach traffic as indicated in 2.2.

Table 2/E.412 – An example of a single threshold selective circuit reservation percentage control response table

Circuit group reservation threshold	Traffic attribute	Response category assigned to circuit group		
		A	B	C
RT1	HTR	25	50	100
	ETR	0	0	25
RT Reservation Threshold				

Table 3/E.412 – An example of a two-threshold selective circuit reservation percentage control response table

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

4.3 Automatic destination control

When a destination (destination exchange, subtending network, PBX or subscriber) receives too many call attempts that cannot be completed, it can experience congestion which results in focused overload effects within the international network. Traffic volume control must then be activated so as to decrease the number of call attempts towards the congested destination. With the deployment of Signalling System No. 7 and new global services, such congestion may occur very rapidly and require fast and automated response. Automatic Destination Controls (ADCs) are traffic volume controls that first automatically detect the focused destination and then dynamically control traffic volume towards the destination.

Two examples of automatic destination control implementation may be considered.

– Decentralized method: In this approach, destination congestion is locally detected at source on a per call basis upon receipt of backward failure messages including subscriber busy. A call rate control is then triggered at source which limits the number of call attempts towards the congested destination.

– Centralized method: Detection is performed at the destination exchange when the call arrival rate, periodically calculated on a short-time interval, exceeds the threshold set for the destination. The call arrival thresholds are estimated according to parameters such as overflow rate, occupancy, mean holding-time and circuit group size. If a destination is detected as a point of focused overload, the information is transferred and traffic volume controls (call gapping or others) based on the excess traffic amount should be activated, at each originating node, until the destination is determined as normal. The degree of control is driven by the magnitude of the difference between the actual indicator and the threshold.

4.4 Automatic controls deriving from state-dependent routing

ITU-T Rec. E.170 describes the features of state-dependent routing and pinpoints the network management functionalities it inherently includes.

State-dependent routing can perform most of the expansive actions which are used in network management: traffic is automatically directed over spare capacity which exists in the network.

Furthermore, automatic protective actions are incorporated with state-dependent routing which includes:

– avoiding congested circuit groups;

– not using overloaded exchanges for transit.

It may be necessary to complement state-dependent routing with traffic volume controls in order to restrict traffic towards congested destinations during focused overload circumstances.

The implementation of state-dependent routing represents a new step in the automation of network management controls. Further studies are required to analyse its impact on traditional NM operation.

5 Status and availability of network management controls

5.1 The exchange and/or network management operations systems should provide information to the network management centre and/or the exchange staff as to what controls are currently active and whether the controls were activated automatically or by human intervention. Measurements of calls affected by each control should also be available (see ITU-T Rec. E.502).

5.2 To help insure the viability of network management functions during periods of exchange congestion, network management terminals (or exchange interfaces with network management operations systems), and functions such as controls, should be afforded a high priority in the exchange operating software.

6 Operator controls

Traffic 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 normal procedures to reduce repeated attempts (in general, or only to specified destinations), or to use alternative routings to a destination. They can also provide information to customers and distant operators during unusual situations, and can be provided with special call handling procedures for emergency calls.

7 Controls for intelligent network

A Service Switching Function (SSF)/Call Control Function (CCF) (of ITU-T Rec. Q.1204) can offer large volumes of message traffic to a Service Control Function (SCF) (of ITU-T Rec. Q.1204) in a relatively short period of time. Congestion can occur within an SCF if traffic is allowed to grow beyond engineered levels, increasing message response time and call failure rates. (The above statements are quoted from 5.4.2.1/Q.1214.) When congestion occurs, proper controls can improve the overall performance of the network.

Controls for an SCF depend on communication between the SCF and an SSF/CCF. If an SCF communicates to an SSF/CCF via a signalling network, controls can be performed via the signalling network. If an SCF communicates with an SSF/CCF via circuit groups, controls can be performed via the circuit groups.

7.1 Controls for an SCF via a signalling network

To cope with overload at an SCF, traffic volume controls are suggested. Because of possible prompt propagation of overload in the IN environment, call rate control is preferred to call percentage control.

Two situations can occur:

1) An SCF detects that the destination of a dialled number, which is generally at customer premises, receives a relatively high volume of ineffective call attempts. The SCF then issues a signalling message to an SSF to request for a call rate control. In return, the SSF activates a call rate control to reduce the rate of service requests that are sent to the SCF. This detection and control is similar to automatic destination control of 4.3; the main difference is that the traffic here consists of signalling messages of service requests, whereas the traffic referred to in 4.3 consists of call attempts.
2) An SCF detects that the SCF itself is under overload condition, rather than detecting a dialled number destination's problem. The SCF then issues a message to the SSF to request for a call rate control. In return, the SSF automatically activates a call rate control that reduces the rate of service requests that are sent to the SCF. This detection and control can be viewed as automatic call rate control.

The above two situations are different in overload detection, but identical in call rate control activation and mechanism. In both situations, messages requesting for call rate controls are sent from an SCF to an SSF/CCF, and consequent call rate controls are activated at the SSF/CCF. Specific information in such a control-request message is described in 5.4.2/Q.1214.

In situations when network managers are notified of possible SCF overload before the overload occurs, it might be advantageous to manually activate call rate controls in a pre-planned event. As an SCF periodically sends network managers a measurement of the number of service requests that are ineffective because of overload, network managers can manually place a call rate control at an SSF/CCF as a supplementary or override action to an automatic control. Further, when an SCF malfunctions and cannot send correct messages to an SSF/CCF to request for call gap controls, manual control can serve as backup.

7.2 Controls for an SCF via circuit groups

An SCF can be implemented in an Adjunct (AD), Intelligent Peripheral (IP) or Service Node (SN) (of ITU-T Rec. Q.1205) that connects to a Service Switching Point (SSP) via circuit groups with, e.g., ISDN interface. In case such an SCF is overloaded, part of the traffic can be redirected to another SCF via another SSF/CCF by means of circuit group control concepts. For example, temporary alternate routing control can redirect the overflowed traffic to another SCF; skip or cancel control can reduce the traffic sent from an SSF/CCF to an SCF.

8 Hierarchy of NM controls

In general, the destination control shall take precedence over any circuit group controls, and manual controls shall take precedence over automatic controls. When multiple controls are applied to the circuit group, the following hierarchy shall apply:

1) TAR (add at the beginning of routing table, replace circuit group);
2) cancel Direct Routing To (DRT) and cancel Alternative Routing To (ART);
3) skip;
4) selective circuit reservation;
5) automatic congestion control;
6) cancel re-routed overflow;
7) TAR (added at the end of the routing table, inserted into the routing table between existing circuit groups);
8) cancel Direct Routing From (DRF) and cancel Alternative Routing From (ARF).

Annex A

Example of Network management controls selectivity

Control	Managed object				Traffic attribute																		Operating parameters					
	Circuit group	Destination a)	Exchange	IN node	Traffic type								Service type				Traffic source						Amount			Threshold	Disposition	
					DR	AR	TAR	HTR	ETR	Priority	Non-priority	...	TMR	ISUP preference indicator	Calling party's category	...	Operator	Customer	Transit	Incoming	Access Ind. (PSTN, ISDN)	...	%	Continuous/ Asynch. timer/ Leaky bucket	No. of circuits		Cancel	Skip
Code block		X			–	–	–	–	–								!	!	!	!			X				X	
Call gap		X			–	–	–	–	–								!	!	!	!				X			X	
Cancel Direct Routing To	X				X			!	!								X	X	X				X	X			X	
Cancel Direct Routing From	X				X			!	!								X	X	X				X	X			X	
Circuit directionalization	X																						X		X			
Circuit turndown/ busying/blocking	X																						X		X			
Cancel Alternative Routing From (ARF)	X					X		!	!	!	!						X	X	X				X	X			X	
Cancel Alternative Routing To (ART)	X					X		!	!	!	!						X	X	X				X	X			X	
Skip	X				X	X		!	!	!	!						X	X	X				X	X				X

Control	Managed object				Traffic attribute																		Operating parameters					
	Circuit group	Destination a)	Exchange	IN node	Traffic type								Service type				Traffic source						Amount			Threshold	Disposition	
					DR	AR	TAR	HTR	ETR	Priority	Non-priority	...	TMR	ISUP preference indicator	Calling party's category	...	Operator	Customer	Transit	Incoming	Access Ind. (PSTN, ISDN)	...	%	Continuous/ Asynch. timer/ Leaky bucket	No. of circuits		Cancel	Skip
Temporary Alternative Routing (TAR)	X	X			X	X		!	!	!	!						X	X	X				X	X				
Cancel Re-routed Overflow (CRO)	X	X					X																				X	
Automatic Congestion Control (ACC)	X				X	X		X	X	X	X						X	X	X				X	X		X	X	X
Selective Circuit Reservation (SCR)	X				X	X		X	X	X	X						X	X	X				X	X		X	X	X
Automatic Destination Control (ADC)		X			–	–	–	–	–	–	–												X	X		X		

a) According to the definition of a destination (dialled digits), it can cover an exchange. The column exchange refers to the identification of the exchange based on its identification label (not derived by the dialled digits).

DR	Direct Routed (traffic)	ETR	Easy-To-Reach	...	Future extensions
AR	Alternative Routed (traffic)	TMR	Transmission Medium Requirement	!	Optional
TAR	Temporary Alternative Routing (traffic)	X	Required (in the Amount column, select at least one of the "X")	Blank	represents items for further study
HTR	Hard-To-Reach	–	Not required		

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	**Overall network operation, telephone service, service operation and human factors**
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

23595

Printed in Switzerland
Geneva, 2003