INTERNATIONAL TELECOMMUNICATION UNION

# CCITT

# E.412

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

(10/92)

**TELEPHONE NETWORK AND ISDN**

**QUALITY OF SERVICE,
NETWORK MANAGEMENT AND TRAFFIC
ENGINEERING**

## NETWORK MANAGEMENT CONTROLS

**Recommendation E.412**

## FOREWORD

The CCITT (the International Telegraph and Telephone Consultative Committee) is a permanent organ of the International Telecommunication Union (ITU). CCITT 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 Plenary Assembly of CCITT which meets every four years, establishes the topics for study and approves Recommendations prepared by its Study Groups. The approval of Recommendations by the members of CCITT between Plenary Assemblies is covered by the procedure laid down in CCITT Resolution No. 2 (Melbourne, 1988).

Recommendation E.412 was revised by Study Group II and was approved under the Resolution No. 2 procedure on the 30th of October 1992.

---

CCITT NOTE

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

**Recommendation E.412**

# NETWORK MANAGEMENT CONTROLS

*(revised 1992)*

## 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 objectives given in Recommendation E.410. Most network management controls are taken by or in the exchange (see Recommendation 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 Recommendation E.410, § 4. 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 Recommendations 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 Recommendation 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 Object(s), Traffic Attributes and the Operating Parameters to be controlled.

The Objects 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. ISDN Circuit Mode Bearer Service Category, Call category);

– Traffic source (e.g. Operator-originated, Customer-originated, 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 certain of the Objects, Traffic Attributes and Operating Parameters, may be valid for a particular control. Although, in the implementation of NM controls it would be convenient to have the maximum flexibility for the above parameters, only some of the parameters arc 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 are related to the managed objects, 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 Recommendation 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 Recommendation 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 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 Rec. E.160).

2.2.3.1 *Overview of HTR information exchange*

Recommendation 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 1 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 focussed 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 focussed 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*

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*

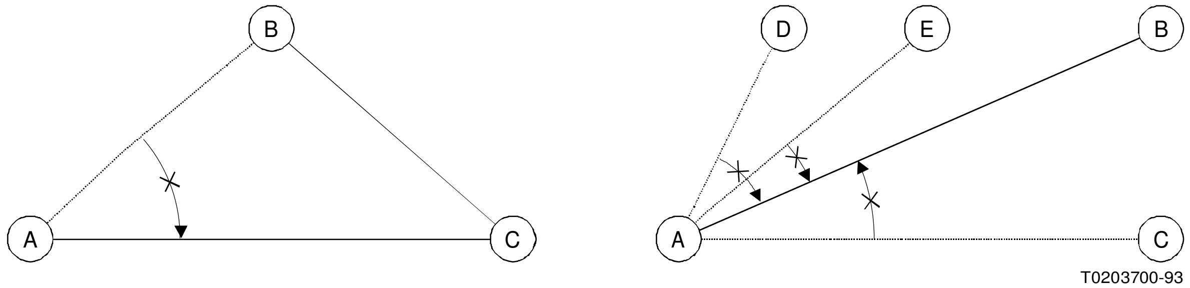
Routing controls are used to control the routing of traffic to a destination, or to or from a circuit group. However, it should be noted that in some cases a routing control may also affect the volume of traffic. Controls which are applied to circuit groups may also be applied to circuit sub-groups, 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. 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. The control will remove all alternative circuit groups in the routing table where the controlled circuit group is the first choice circuit group.
- 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 Rounting From" (ARF) cancellation on A-B circuit group

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

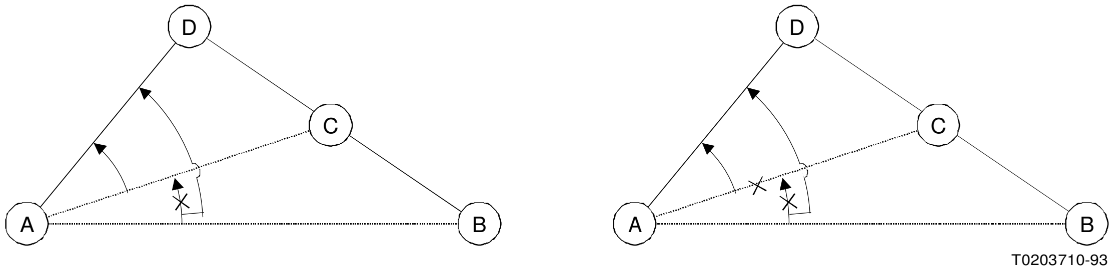
FIGURE 1/E.412

**Examples of alternative routing cancellation**

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 by-pass 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.




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 object 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 reenter 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 muting. The Cancel Rerouted 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/E.412.

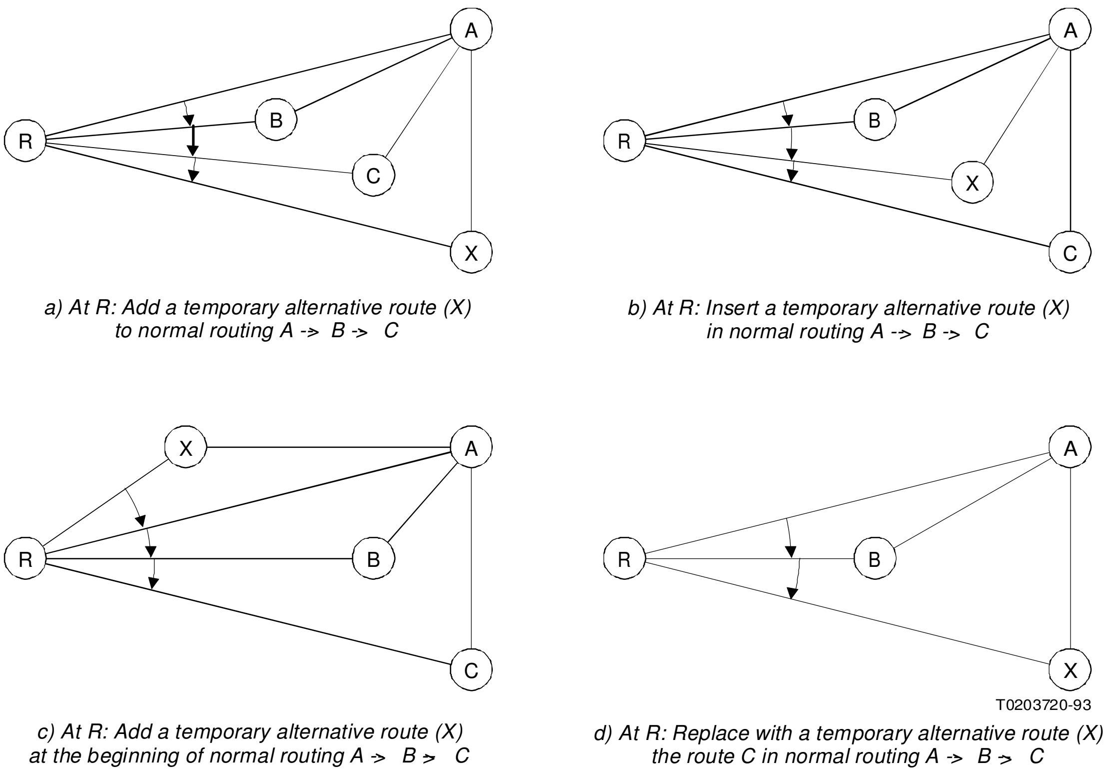



FIGURE 3/E.412

**Examples of Temporary Alternative Routing**

#### 3.2.4 *Cancel rerouted overflow*

This control prevents additional rerouting or alternate routing of a rerouted call. Rerouted calls are not allowed to overflow the circuit group to which the Cancel Rerouted Overflow control is applied, while normal overflow traffic is not affected. This requires the ability to uniquely identify rerouted 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 preassigned, 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 *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.

#### 4.1.2 *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.

#### 4.1.3 *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.

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/E.412 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/E.412 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**

**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 |

4.1.4 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

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

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 Recommendation 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 Recommendation 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 skip or cancel.

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/E.412 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/E.412. 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/E.412 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/E.412.

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 |

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 (ADC) 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 considers.

– *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*

Rec. E.170 describes the features of state-dependent routing and pin-points 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 ar e 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 analyze 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 Recommendation 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.

ANNEX A

(to Recommendation E.412)

**Network management controls selectivity**

| Control | Managed object | Traffic Attribute | | | Operating parameters | | |
|---|---|---|---|---|---|---|---|
| | | Traffic type | Service type | Traffic source | Amount | Thresholds | Disposition |
| Code Block | Destination | | | | % of calls | – | Cancel |
| Call Gap | Destination | | | | Call rate | – | Cancel |
| Cancel direct route | Circuit group | Direct Routed | | | % of calls<br>Call rate | – | Cancel |
| Circuit directionalization | Circuit group | – | | Incoming | Number/<br>% of circuits | – | Skip |
| Circuit lum-down/busying/blocking | Circuit group | – | | | Number/<br>% of circuits | – | Skip |
| Cancel Alternative Route From (ARF) | Circuit group | Alternative Routed | | | % of calls<br>Call rate | – | Cancel |
| Cancel Alternative Route To (ART) | Circuit group | Alternative Routed | | | % of calls<br>Call rate | – | Cancel/<br>Skip |
| Skip | Circuit group | All | | | % of calls<br>Call rate | – | Skip |
| Temporary Alternative Routing (TAR) | Circuit group<br>Destination | All except previously TAR rerouted | | | % of calls | – | – |
| Cancel Rerouted Overflow (CRO) | Circuit group | | | | All calls | – | Cancel |

**Network management controls selectivity**

*(continued)*

| Control | Managed object | Traffic Attribute | | | Operating parameters | | |
|---|---|---|---|---|---|---|---|
| | | Traffic type | Service type | Traffic source | Amount | Thresholds | Disposition |
| Automatic Congestion Control (ACC) | Circuit group | Variable per traffic type | | | % of calls | Congestion level | Cancel/ Skip |
| Selective Circuit Reservation (SCR) | Circuit group | Variable per traffic type | | | % of calls | Number of idle circuits | Cancel/ Skip |
| Automatic Destination Control (ADC) | Destination | Variable per traffic type | | | % of calls<br>Call rate | | Cancel |

– Non applicable

*Note* – Since the exchange can apply more than one control at a time to a destination and/or circuit group the order of precedence is:

1) Destination controls take precedence over circuit group controls;

2) Manual controls override automatic controls.