International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

E.417

(02/2005)

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

Network management – International network management

Framework for the network management of IP-based networks

ITU-T Recommendation E.417

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.404
International network management	**E.405–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.417

Framework for the network management of IP-based networks

Summary

This Recommendation lays down a framework for supporting and defining the role of network management in IP-based telecommunications networks. IP-based networks generally make use of various telecommunications technologies that support a range of multimedia services such as voice, data, still image and video. Such IP-based networks are referred to here as converged networks. Network Management (NM) goals, principles and functions that are intended for use with IP-based equipment are defined. The major part of this Recommendation suggests ways to monitor traffic and provides some indication of parameters for promptly detecting abnormal network traffic conditions. After detection of an abnormal condition, automatic and possibly manual controls must be temporarily applied to the network to alleviate the problem until it is resolved. It is also necessary to frequently check the performance of the network after applying the NM controls to note whether the control is mitigating the problem and to determine when to modify or remove it from the network.

Source

ITU-T Recommendation E.417 was approved on 24 February 2005 by ITU-T Study Group 2 (2005-2008) under the Resolution 1.

History

1.0	E.417	2001-02-02
2.0	E.417	2005-02-24

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.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

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

ITU-T Recommendation E.417

Framework for the network management of IP-based networks

1 Scope

This Recommendation is intended to support and define the role of network management in IP-based telecommunications networks. IP-based networks generally make use of various telecommunications technologies that support a range of multimedia services such as voice, data, still image and video. In this Recommendation, such IP-based networks are referred to as *converged networks*. Addressed here are the Network Management (NM) goals, principles and functions intended for use with IP-based equipment operating in such converged networks or in dedicated IP networks.

This Recommendation lays down a framework for IP network management. It shall, however, be enhanced as the research in the field of IP network management is progressed. The major part of this Recommendation suggests ways to monitor traffic and provides some indication of parameters for promptly detecting abnormal network traffic conditions. After detection of an abnormal condition, automatic and possibly manual controls must be temporarily applied to the network to alleviate the problem until it is resolved. It is also necessary to frequently check the effects of the NM controls to note whether the control is mitigating the problem and to determine when to modify or remove it from the network.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation

- ITU-T Recommendation E.370 (2001), *Service principles when public circuit-switched international telecommunication networks interwork with IP-based networks*.
- ITU-T Recommendation E.410 (1998), *International network management – General information*.
- ITU-T Recommendation E.411 (2000), *International network management – Operational guidance*.
- ITU-T Recommendation E.412 (2003), *Network management controls*.
- ITU-T Recommendation E.413 (1988), *International network management – Planning*.
- ITU-T Recommendation E.414 (1988), *International network management – Organization*.
- ITU-T Recommendation E.415 (1991), *International network management guidance for common channel signalling system No. 7*.
- ITU-T Recommendation E.416 (2000), *Network management principles and functions for B-ISDN traffic*.
- ITU-T Recommendation E.800 (1994), *Terms and definitions related to quality of service and network performance including dependability*.
- ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication*.

– ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.

– ITU-T Recommendation I.371 (2004), *Traffic control and congestion control in B-ISDN*.

– ITU-T Recommendation M.3000 (2000), *Overview of TMN Recommendations*.

– ITU-T Recommendation Y.1540 (2002), *Internet protocol data communication service – IP packet transfer and availability performance parameters*.

In addition, other standards bodies such as the Internet Engineering Task Force (IETF) have been working in related areas such as IP Quality of Service. These include the following:

– IETF RFC 2330 (1998), *Framework for IP Performance Metrics*.

– IETF RFC 2386 (1998), *A Framework for QoS-based Routing in the Internet*.

3 Definitions

This Recommendation defines the following terms:

3.1 call: An association between two or more users or between a user and a network entity within a telecommunications network for the purpose of exchanging information. The call begins with the call set-up procedure and ends with the call termination procedure.

3.2 class of service: Any of the network-oriented designations or features that can distinguish between various services, or application-layer uses, of lower-layer telecommunications capabilities for the purpose of more effectively accommodating the specialized network performance needs of specific services.

3.3 connection-oriented: Connection-oriented refers to the transfer of information between two entities by first establishing a path (or connection) for the information transfer. The communication proceeds through three well-defined phases: connection establishment, information transfer, and connection release. The most common example of connection-oriented information transfer is a telephone call over a circuit-switched network. Other examples of connection-oriented information exchange are networks based on ITU-T Rec. X.25, Frame Relay (FR), Transmission Control Protocol (TCP) and Asynchronous Transfer Mode (ATM).

3.4 connectionless: Connectionless refers to the transfer of information between two entities without first establishing a path (or connection) for the information transfer. Examples of connectionless transport include the Internet Protocol (IP) and User Datagram Protocol (UDP).

3.5 converged network: IP-based networks that generally make use of various telecommunications technologies to support a range of multimedia services such as voice, data, still image and video.

3.6 gateway: A network element that enables real-time communication between other network elements and/or customer premises equipments (CPE) that have dissimilar protocols. This includes supporting voice communication between terminals on a packet network, e.g., IP network, and terminals on a circuit-switched network.

3.7 link: A point-to-point (physical or virtual) connection used for transporting information between two nodes. A link could, for example, be a leased line, or it could be implemented as a logical connection over an Ethernet, a frame relay network, an ATM network, or any other network technology that functions below the network layer of the Open Systems Interconnection (OSI) model.

3.8 multimedia service: A telecommunications service that supports the simultaneous use of multiple media types (e.g., voice, data, video).

3.9 network performance: The performance of a portion of a telecommunications network that is measured between a pair of network-user or network-network interfaces using objectively defined and observed performance parameters.

3.10 quality of service (QoS): QoS is defined in ITU-T Rec. E.800 as "collective effect of service performance, which determine the degree of satisfaction of a user of the service".

3.11 router: In the broadest sense, any communications equipment that forwards information on a connectionless basis. Typically, routers are special purpose computers, which operate at Layer 3 of the OSI reference model and forward information based on a Layer 3 address which has network-wide significance. For example, Internet routers forward IP packets based on their destination addresses. Routers operate without using connections, as opposed to switches which do establish connections.

3.12 switch: A switch is a device that dynamically interconnects physical or virtual links to form a connection for information transfer.

3.13 virtual connection: A type of connection used for packet data transfer in which apparent connections are established through appropriate correlation of link-layer addresses.

4 Abbreviations

This Recommendation uses the following abbreviations:

APS	Automatic Protection Switching
ATM	Asynchronous Transfer Mode
B-ISDN	Broadband Integrated Services Digital Network
CPE	Customer Premises Equipment
FR	Frame Relay
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
NE	Network Element
N-ISDN	Narrow-band Integrated Services Digital Network
NM	Network Management
NTM	Network Traffic Management
OAM	Operation, Administration and Maintenance
OSI	Open Systems Interconnection
PDH	Plesiochronous Digital Hierarchy
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
TCP	Transmission Control Protocol
TMN	Telecommunications Management Network

UDP User Datagram Protocol

UNI User Network Interface

URL Uniform Resource Locator

WAN Wide Area Network

WDM Wavelength Division Multiplexing

5 Introduction

This Recommendation presents a framework for extending the network management aspects given by ITU-T Recs E.410, E.411 and E.412 to the services based on the Internet Protocol (IP). It also establishes a direction for further study in the important area of Network Traffic Management (NTM) for IP. Extension of these Network Management aspects to IP requires consideration of the IP transfer capabilities, the multiple Quality of Service (QoS) classes, Service Level Agreements (SLAs) and automated routing control procedures that can exist in IP-based networks. This Recommendation also describes some network management functions of the IP-based network. These IP network management functions are intended to interwork with traffic and congestion controls and the measurements of traffic and performance that exist in IP routing equipment for the purpose of maintaining adequate network performance under abnormal conditions.

Significant differences exist between connectionless and connection-oriented networks. For connection-oriented networks, both the physical connections that support circuit-switched telephony and the virtual connections that support other forms of packet-oriented telecommunications, such as Asynchronous Transfer Mode (ATM) and Frame Relay (FR), provide an end-to-end path that remains associated with a telecommunications session (for example, a phone call) throughout the life of that session. For connectionless IP-based networks, all of the IP packets associated with a particular session can be sent without reference to any such underlying end-to-end path. However, practical experience in managing converged networks is showing the desirability of establishing, at least in some cases, associations between the IP packets relating to a particular session and a path provided by means of accompanying technologies such as ATM, SDH or WDM.

To assure a satisfactory level of network performance, a robust and fast network management capability is desired to promptly detect any traffic-related problem in the network and try to resolve it as quickly as possible. The role of manual controls has been minimized due to specific IP-based network characteristics such as:

a) the capabilities of a connectionless network to manage most situations automatically;

b) volatility of congestion-related incidents and the minimal time scale available for human intervention;

c) complexity of IP-based networks due to the implementation of various service categories.

Before a definitive synthesis of NM principles and solutions for IP-based networks can occur, further technical information is needed concerning the characterization of IP performance (including the impacts of performance impairments on IP-based services) and the resource management problems facing IP equipment in a converged network context. Accordingly, this Recommendation is properly viewed as a framework Recommendation that will guide further research in this field.

6 Network management goals, concerns and policies

Network management concerns itself with the maintenance of adequate network performance under a variety of conditions, which can include exceptional traffic loads within some network portions, system failure, element outage, etc. The overall process of network management involves the observation of relevant traffic and performance data, suitable analysis of that data, and the resulting

implementation of appropriate network management controls. The effectiveness of an implemented set of network management controls is then evaluated based on new observations of traffic and performance data, which are then analysed and used as a basis to remove or further modify, if necessary, the current set of network management controls.

6.1 Network management goals

IP-based applications are most effectively managed in the context of converged voice and data networks, which typically involve substantial amounts of both IP-specific and non-IP-specific equipment types. As an example, Figure 1 illustrates some of the generic equipment types often found in these converged networks.

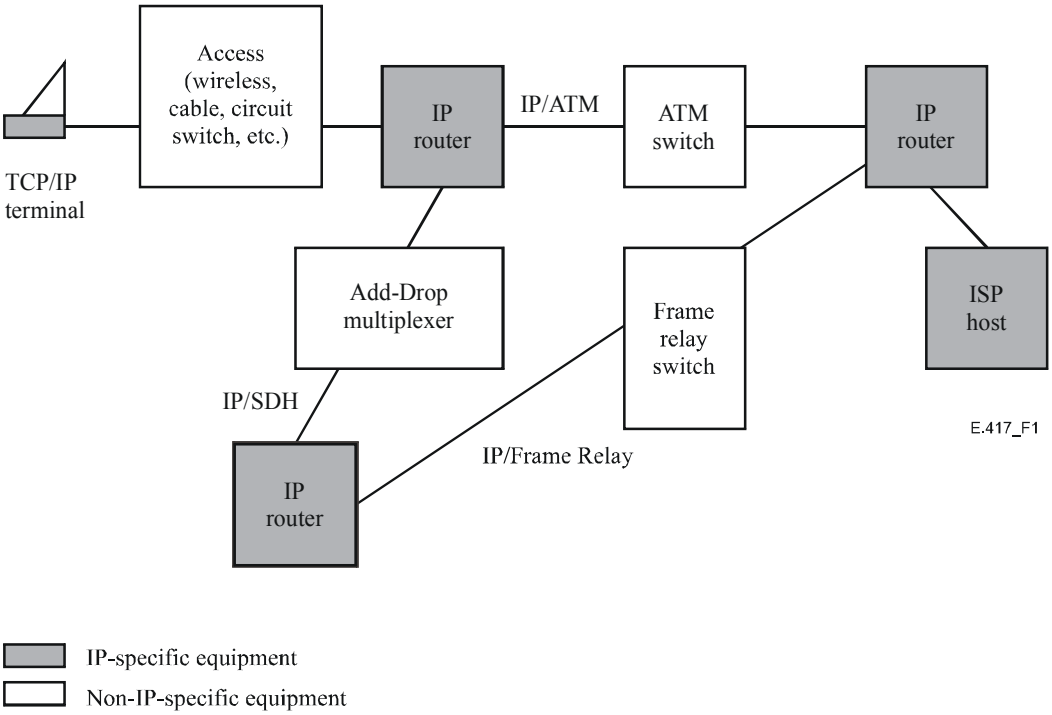

Figure 1/E.417 – An example of a converged voice and data network

General network management goals for circuit-switched telephony have been described in ITU-T Rec. E.410. Although they have been defined for international network management based on circuit switching, they can be extended and may be applied to other networks. With some modifications and enhancements, such goals are still valid for IP applications in converged networks. The enhanced set will constitute the initial set of IP network management goals. Further study and experience will be needed to validate the application of these principles to IP-based networks. The following is the initial set of network management goals for converged networks:

- utilize all possible network resources when dealing with a network traffic problem;
- inhibit traffic congestion and prevent its spread;
- make economically efficient use of network resources by rejecting attempts that have a poor chance of succeeding;
- when the offered load is approaching the network capacity limit, favour completing those communication attempts that require the least amount of resources.

6.2 Network management concerns

Network management concerns can be resolved by automatic or manual detection of the problem and then the network manager may take appropriate actions to resolve the problem in order to provide adequate network performance to customers. Such action in a converged network must be done in the shortest time possible by the network manager or preferably by a support system. Some IP-based services such as Voice over IP require special attention due to their low tolerance for delay and delay variation.

The following are some of the major concerns of IP network management.

6.2.1 Transmission failure

When a transmission failure occurs (e.g., when a cable is cut or extremely damaged), network performance may become degraded unless the failure can be quickly detected and an alternate path found (e.g., via Automatic Protection Switching (APS)).

The impact of a transmission failure can have different effects in connection-oriented and connectionless networks. Such effects are listed in Table 1 below:

Table 1/E.417 – The effect of transmission failure on connection-oriented and connectionless networks

	Connection-oriented	Connectionless
At the time of failure	• With APS, a short interruption until connectivity is restored on an alternate path[a)] • Without APS, existing connections are lost; no impact on new connections • Without APS, potential congestion on alternate routes	• Effectively no break as packets are rerouted around the failure • Potential congestion on the alternate path
At the time of restoration to "normal" configuration	• With APS, a short break • Without APS, no impact on switched services	• Buffer overflow due to packets arriving from both alternate and normal paths • Packets out of sequence
a) For a physical layer APS, the typical interruption is of the order of tens of milliseconds, and no connection is lost.		

6.2.2 Network node failure

There may be occasions when a node (e.g., IP router module, gateway, switch, etc.) fails, adversely impacting the Network Performance. In such cases, network managers require near real-time status of node availability thus enabling the affected node to be quickly identified and the appropriate action rapidly undertaken.

6.2.3 Network node overload

A network node such as a router or a switch can be overloaded, that is, when the capacity of a network node has been exceeded by the demand, because, for example:

- more IP packets are entering the node than can be effectively processed and transmitted (for example, resulting in buffer overflows);
- more call requests are being offered to a switch within the IP-based network than can be supported by that switching fabric;
- more signalling messages are being offered to a switch than can be processed.

6.2.4 Network overload

There are occasions when the network becomes overloaded, that is, when the capacity of the network has been exceeded by the demand. This may be caused by, for example:

- peak days;
- natural disasters;
- focused overloads;
- node or transmission failures which have widespread impact.

6.2.5 Interference among services

In a converged network there is the potential for interference between different services that share common network resources. Some of the services may be of a critical nature (e.g., emergency services, business services and government services) and may need to be given special attention by network management in a manner consistent with an Administration's policies.

6.2.6 Inter-networking

Inter-networking between different network operators and technologies must be addressed to ensure that adequate network performance is achieved for all IP-based applications. Such inter-networking can be within an operator's network using multiple technologies or between two network operators.

- Within an operator's network:

  On an end-to-end basis, IP packets may be transported over multiple network technologies such as ATM or wireless. It is appropriate for network management to correlate NM functions, measurements and actions among distinct network technologies in order to monitor and control the overall network.

- Between network operators:

  It is appropriate that NM methods and procedures be developed between various network operators to ensure the adequate service performance of the IP connections.

6.3 Network management policies

Based on network management goals and concerns, a set of NM policies needs to be devised. Besides NM goals listed in 6.1, individual network operators may have additional network management policies that support their business objectives. Such policies may, for example, include:

- meeting service and performance standards set by regulatory bodies, where applicable;
- meeting a network operator's own service and performance objectives;
- meeting service level agreements established with individual customers and other groups;
- protecting the performance, stability and operating margins of network equipment;
- minimizing the interference by one customer, product or service upon another.

NTM policies can be stated in an internal company policy document.

7 Network management functions

In the ITU-T M.3000-series Recommendations, ITU-T has categorized the functional areas supported by the Telecommunications Management Network (TMN) as performance, fault, configuration, accounting and security management. The focus of network traffic management is mostly on performance management and some fault management. Network management functions include the following:

- **Status and performance monitoring on a near real-time basis**

  This task is based on the use of periodically collected measurements, alarms (i.e., major, minor, critical) and notifications generated upon occurrence of significant events. These are sent from the network elements to the NM systems in a NM centre. The measurements may be used directly or they may be processed by a NM tool in order to provide useful parameters. Relevant measurements and parameters are discussed in clause 8.

- **Detecting abnormal conditions**

  This is performed through analysis of the collected and derived parameters, e.g., measurements, alarms, notifications and correlation with other data. Abnormal conditions can also be detected with the help of statistical algorithms and thresholding procedures.

- **Investigating and identifying abnormal network conditions**

  This task should provide a diagnosis of the situation that may lead to a corrective control (see clause 9). The abnormal condition is usually expressed in terms of service or traffic identifiers with their traffic characteristics.

- **Initiating corrective actions and/or controls**

  Once an abnormal situation has been detected and its causes identified, traffic control actions should be executed. Actions may include controls to bypass a congested or overloaded portion of the network.

- **Operational relationship**

  In an increasingly complex and competitive telecommunications market, it is unlikely that one network operator will be solely responsible for end-to-end delivery of traffic. Network operators will need to develop and maintain strong operational relationships with interconnecting networks, carriers or operators who deliver traffic to, or receive traffic from them and their customers.

  There may be opportunities to understand the sorts of interactions required to fulfil these relationships by considering the interactions which form a regular part of International operations, or inter-carrier operations in competitive markets. The following three items signify this importance:

  – **Cooperating and coordinating actions with other NM centres**

    Different applications (e.g., telephony service) may have distinct NM centres. Cooperation between the centres may be necessary to meet a global, regional and/or customer network performance target.

  – **Cooperating and coordinating with other work areas**

    As in the PSTN, information coming from equipment surveillance and maintenance is important. Since IP packets in a converged network may traverse through other networks such as ATM, strong cooperation must be established between all work centres.

  – **Cooperating and coordinating with other network operators**

    IP packets may traverse from one operator's network to another. Cooperation and coordination between network operators will strengthen the network management support of IP-based network services.

- **Issuing reports about network traffic management activities**

  As in the PSTN, these reports are important for managers, training and planning network performance improvements.

- **Provide advanced planning for known or predictable network situations**

  This planning should take into consideration the impact of abnormal or special events on network traffic flows, and should also consider the requirements of particular service and traffic categories.

TMN ITU-T Rec. M.3000 provides a framework for considering the functions described in this clause.

8 Network status and performance data

Network status and performance data is required to establish a rational basis for guiding the application of network management actions (e.g., applying controls and contacting other centres), and to provide a means of evaluating the effectiveness of previously applied network management controls.

8.1 Network status of IP-based traffic

A network traffic manager may be directly involved in mitigating the effect of failures, errors or external events, such as mass calling, that impacts the traffic load or pattern. It is desirable that most network traffic-related problems be detected and resolved automatically. However, network traffic managers must be informed of such automatic actions and should be able to intervene and change or override the controls.

Monitoring the network is one of the primary tasks of network management that should be done in near real-time in order to observe and protect network performance. As the network is enhanced and more services are supported, the need for real-time collection and analysis of data becomes more significant. The time to deliver the data to NM systems should be minimized, and a balance should be developed between the measurement interval and the statistical significance of data. For example, a balance is needed between immediately reporting each individual lost packet and the integration of packet loss data over a measurement interval chosen to give a statistically meaningful performance estimate. Research is needed concerning time correlation in packet flows and their impacts on optimum measurement intervals for packet loss performance. In general, this monitoring function should provide network traffic managers with the current operational status of the network and its components, the traffic load, and the resulting performance.

NM controls (see clause 9) must also be reviewed in conjunction with current network status data by network traffic managers to observe whether the problem has ceased or lessened in severity. Based on such review, a network traffic manager can determine whether to retain, modify or remove previously applied NM controls. Network traffic managers must also review the duration of controls. It is also necessary to investigate the amount of affected traffic to verify that traffic is properly controlled.

8.2 Measurements

To detect and isolate a problem, various data must be collected or derived. The data may, for example, come directly from NEs, or from independent measurement systems. These measurements can assist network traffic managers in controlling the traffic and safeguarding network performance and service level agreements.

In this clause, measurements have been categorized into three different areas: the *network-level*, the *link-level* and the *node-level*.

8.2.1 Some network-level measurement examples

Network-level measurements provide information concerning the health of the network. Some examples of the network-level measurements include (note that the measurement interval for the following must be defined):

Attempted call count: Total number of call attempts made to the network during the measurement interval.

Accepted call count: The number of call attempts that are successfully completed by the network during the measurement interval.

Failed call count: Number of call attempts that are not successfully completed by the network during the measurement interval. Calls may fail due to limited resources or any other reason.

Usage: A measure of the intensity of calls, packets or bytes sent on the network.

Average packet count: This parameter provides the average number of packets entering the network during the measurement interval.

Ingress packet count (IPC): Total number of packets entering the network during the measurement interval.

Egress packet count (EPC): Total number of packets departing from the network during the measurement interval.

Average cross-network delay: The average difference between the time that a packet enters a network and the time it leaves the same network.

Cross-network delay variation: A measure of the variation in cross-network delay.

It is anticipated that the measurements given in this framework Recommendation will be expanded based upon further research and operating experience.

8.2.2 Some link-level measurement examples

Link-level measurements provide information about the inter-nodal activities. By having such parameters available to the network management, a possible problem can be isolated to the node or the link with abnormal parameters. Some examples of the link-level measurements include the following (note that the measurement interval for the following must be defined):

Attempted call count: The number of call attempts on a link during the measurement interval.

Accepted call count: The number of call attempts that are successfully placed on a link during the measurement interval.

Failed call count: The number of call attempts that are not placed on a link during the measurement interval. The reasons for which call attempts may not be placed on this link include failures, overflows and other reasons.

Usage: A measure of the intensity of calls, packets or bytes sent on a link.

As this framework expands, additional measurements will be defined.

8.2.3 Some node-level measurement examples

Node-level measurements characterize traffic and performance from the view of a specific network node (e.g., switch, and router). Some examples of these measurements are as follows (note that the measurement interval for the following must be defined):

Attempted call count: The number of call attempts processed by a node during the measurement interval.

Accepted call count: The number of call attempts that are successfully completed by a node during the measurement interval.

Failed call count: The number of call attempts that are not successfully completed by a node during the measurement interval.

Usage: A measure of the intensity of calls, packets or bytes processed by a node.

Ingress packet count (IPC): Total number of packets arriving at the switch or router during the measurement interval.

Egress packet count (EPC): Total number of packets departing from the switch or router during the measurement interval.

Per cent packet loss: $[1 - (EPC/IPC)] \times 100$

Average cross-node delay: The average difference between the time that a packet enters a switch or router and the time that it leaves the same switch or router.

As this framework expands, additional measurements will be defined.

8.3 Alarms and notifications

A notification provides an indication of a change in status of the network or network elements. Alarms are a subset of notifications and indicate abnormal network conditions. Some alarms are generated upon violation of a pre-set condition. For example, a predefined threshold may be reached, in which case an alarm will notify the network manager of such an abnormal condition. Such alarms must be sent to the network management centre on occurrence. Some examples of the conditions under which an alarm can be generated are as follows:

- when the NE is in congestion or overload condition;
- when the NE is no longer in congestion or overload condition;
- when a failure is detected in the NE (i.e., node or link);
- when the failure in the NE is resolved.

9 Network management controls

To resolve network management problems pertaining to equipment handling IP packets in a converged network, a network manager should be able to apply appropriate NM controls, or such NM controls should be applied automatically. If NM controls are applied automatically, then the network manager must have the capability to remove or modify them manually. This is feasible only if proper tools are built in the network or are available to network traffic managers. Such tools can be utilized to, for example, set parameters, re-route traffic, block traffic and set thresholds.

ITU-T Recommendations cover NM controls for various networks – for example ITU-T Rec. E.412 for N-ISDN and ITU-T Rec. I.371 for B-ISDN. A comparable set of NM controls for IP-based networks is needed. Some considerations and issues pertaining to the development of NM controls for IP-based networks are now described.

The traditional NM concept of applying controls as close to source as possible is equally valid for IP-based networks. This may mean applying controls in an access network to protect a downstream IP network, by blocking or diverting traffic before it enters that IP network.

An important class of NM controls for the PSTN includes the alterations to normal call routing procedures. Such controls are based upon a thorough knowledge of the underlying approaches for PSTN call routing under normal conditions. While ITU-T Rec. I.371 focuses on controls for ATM networks, such controls have not been standardized for IP-based networks.

The development of appropriate NM controls for converged networks will likely extend those controls from the PSTN that are based upon the destination address (e.g., code blocking and call gapping). Such controls are categorized here as address-based controls.

The process for developing such NM controls consists of:

a) adequately characterizing IP-related performance (see clause 8);

b) developing in-depth understanding of the resource management problems facing IP equipment in a converged network context;

c) synthesizing NM goals and principles (see clauses 6 and 7) and solutions based upon such performance characterization and in-depth understanding.

In the following, some examples of possible NM controls are discussed.

9.1 Information-transfer-based controls

A set of controls at the information-transfer level is desired for automated activation by appropriate NEs handling IP packets in a converged network. It is noted that ITU-T Rec. I.371 provides such controls for ATM equipment.

With additional research and operating experience, it is possible that a basis can be established for modifying this Recommendation to establish IP information-transfer-based controls, which would better support the network management of converged networks.

9.2 Routing-based controls

NM controls that alter the normal call routing procedures in response to congestion or to non-typical traffic loads can be valuable tools for network management. Such controls have been standardized for circuit-switched networks. When considering the operation of equipment handling IP packets in a converged network, it may be feasible to exploit the routing-based controls in circuit switches to alter the routing of at least some IP packet traffic in support of network management needs.

It is generally useful to consider both expansive and restrictive NM controls based upon temporary alterations of normal routing procedures.

9.3 Address-based controls

Restrictive NM controls can be based upon destination and/or source address (e.g., URL, IP address, sub-net address, E.164 address and e-mail address). Examples of destination address-based NM controls from the circuit-switched networks include code blocking controls and call gapping controls. These controls have proven to be effective and selective in managing focussed overloads in circuit-switched networks. An address-based control is required which limits the amount of traffic forwarded to a specified destination address or set of destination addresses. To provide additional selectivity, a source address or set of addresses may also be specified.

9.4 Flow admission control

Though, in a best effort IP network, there is no such thing as a connection, traffic between any source destination pair of hosts typically follow the same path. It is useful to model traffic at a network element on this path in terms of "flows" where by flow we designate the set of packets using that element and relating to a particular instance of some user application. If we wish additionally to perform traffic control actions at flow level, it is necessary to introduce a more formal definition. For present purposes, an IP flow consists of a succession of packets sharing common header address attributes such as IP source and destination addresses and transport protocol port numbers and occurring with an inter-packet spacing less than a certain threshold, typically of a few seconds.

The considered address attributes determine the flow identifier. A minimal flow identifier for present purposes would be the combination of the origin and destination addresses. At a much finer scale, a so-called microflow is specified by the values of the 5-tuple: IP addresses, transport protocol and port numbers. In this case the flow would typically be confined to a single TCP or UDP connection. It would be useful for traffic control to allow more flexible flow identification where, for example, the multiple components of a single Web page could be considered as a single entity. This would be possible with an adapted use of the IPv6 flow label. The feasibility of such use remains for further study.

The semantics of an IP flow are comparable to those of a call in terms of the level at which quality of service is perceived. It is suggested in the present section that traffic control actions typically applied to calls in a connection-oriented network could usefully be applied to flows in an IP network. In particular, it is natural to consider the use of network management operations where admission control is applied selectively to individual flows.

Admission control appears as a basic requirement to maintain network efficiency in times of network overload. In situations of overload, admission control blocks new IP flows, which would otherwise cause performance degradation to existing flows. The precise definition of overload depends on the nature of offered traffic and performance requirements. For best effort traffic with no specific performance guarantees (e.g., class 5 in ITU-T Rec. Y.1541), a link may be said to be in overload whenever demand (i.e., flow arrival rate × mean flow size) exceeds currently available capacity over a prolonged period. For traffic with more stringent requirements (generated by audio and video applications, for example), a link will be considered to be in overload whenever demand is such that these requirements are not fulfilled. Overloads occur for a variety of reasons including equipment failures and forecasting errors.

In some network architectures, admission control can be applied to connections materialized by an exchange of signals. In the present text, scope is restricted to the case of a best effort Internet. In this case, admission control can be applied to IP flows using an implicit procedure with no signalling or nominal resource reservation. Application of admission control in other IP networking architectures is for further study.

In overload, an accumulation of flows due to the excess of traffic leads to very poor flow performance, causing some users or protocols to prematurely interrupt the underlying transfers. Applying admission control to IP flows to a congested link preserves the quality of service of admitted flows by ensuring them sufficient throughput even in situations of overload.

In the envisaged approach, new flows are detected on the fly and implicitly rejected, when necessary, by discarding their first packets. Admitted flows acquire the status of protected flow and are stored in a list. Any packet belonging to a protected flow is forwarded and the last packet emission time is updated. Any packet not belonging to a protected flow corresponds to a new flow and will be discarded if the admissibility conditions are not satisfied. Otherwise, the packet is forwarded and the corresponding flow added to the list. Flows are removed from the list when the time since the last packet exceeds the inactivity period.

The admissibility conditions to be applied may depend on the value of packet header fields such as the traffic class or the source and destination addresses or fields explicitly designating a class of service (as defined in ITU-T Rec. Y.1541). Hence, different admissibility conditions can be defined to realize effective class of service differentiation. High priority flows are blocked only in extreme congestion but all admitted flows receive excellent quality.

9.5 Other NM controls

Since the operation of equipment handling IP packets in converged networks is relatively new, it is likely that additional NM controls may be identified in the future. Other NM controls are for further study.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
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	Telecommunication management, including TMN and network maintenance
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, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2005