Title:	Document Version:
Deliverable D2.6 **6QM and ITU-T Activities**	3.1

Project Number:	Project Acronym:	Project Title:
IST-2001-37611	6QM	IPv6 QoS Measurement

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
28/02/2003	18/05/2003	R – PU

* Type: P - Prototype, R - Report, D - Demonstrator, O - Other
** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible and Editor/Author:	Organization:	Contributing WP:
Jean Raymond Louvion	FT	WP2

Authors (organizations):

Jordi Palet (Consulintel), Alexandre Dubus (FT), Renée Le Viol (FT), Emile Stephan (FT).

Abstract:

This document presents the ITU-T activities related to the 6QM Project.

Keywords:

ITU-T, Standardization.

Revision History

The following table describes the main changes done in the document since its creation.

Revision	Date	Description	Author (Organization)
v0.0	05/12/2002	Document creation	Emile Stephan (FT)
v0.1	15/01/2003	Update	René Le Viol (FT) Jean-Raymond Louvion (FT)
v1.0	15/02/2003	Document ready for delivery	René Le Viol (FT) Jean-Raymond Louvion (FT)
v1.1	20/02/2003	IPv6 concerns, ITU standard test packet	Emile Stephan (FT)
v1.2	24/02/2003	Document review to prepare the final delivery	Emile Stephan (FT)
v1.3	28/02/2003	FT final deliverable	Jean-Raymond Louvion (FT)
v2.0	30/03/2003	Esthetic review	Jean-Raymond Louvion (FT)
v3.0	30/04/2003	Final version	Alexandre Dubus (FT)
v3.1	18/05/2003	Final Review and corrections	Jordi Palet (Consulintel)

Executive Summary

ITU-T and IETF collaboration must be strengthened in the new industry emphasis on Internet and IP structured signals. Neither the IETF nor the ITU-T is able to adequately address IP based networks independently. For example, the IETF strength lies in the protocol and application areas, whereas the ITU-T has a great deal to offer in the areas of architectural, network interworking and network evolution.

This document details the state of the art of the standardization of IPv4 and IPv6 at the ITU-T. In particular, it emphasizes the necessity of developing a standard test packet structure that can be used for both IPv4 and IPv6.

In addition, the related activity will be in charge of the dissemination inside ITU-T recommendations of the work that will be realized by the 6QM project.

Table of Contents

Table of Figures

1. INTRODUCTION

Network operators usually sign Service Level Agreements (SLAs) with their customers. Measurements are performed for different purposes; they are used to:

- Analyze the long-term behavior of the network (they produce monthly management control data).
- Control the quality of the service that has been delivered (as some users may receive a guaranteed QoS).
- Control the network behavior and interact with resource dimensioning like Connection Access Control (CAC) and dynamic routing.

Thus, the key point is that the different equipment (test equipments, measurement functions implemented in the network equipment) involved in this measurement process should work together constructively. It is therefore extremely important to standardize the measurement procedures:

- A unique test packet structure should be chosen with adequate fields (packet numbering, time stamps, error detection procedures).
- A method for estimating (in the statistical meaning) the performance parameters should be uniquely defined (this method should solve problems like consecutive multiple errors).
- An interface allowing measurement information exchange between different test equipments should be defined.

In the ITU-T IP-related matters are mainly studied inside Study Group 13 which has defined among others the performance parameters that should be considered in an IP based network. In addition, objectives have been attached to these parameters. Study Group 4 is complementing this work by defining measurement methods and bringing-into-service procedures. All these activities are structured inside an "IP project" comprising twelve work areas that cover the whole range of network problems. Furthermore, an area is fully dedicated to IPv6 and to the utilization of IPv6 in telecommunication networks.

2. STATE OF ART AT ITU-T

2.1 Introduction to ITU-T

The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the International Telecommunication Union (ITU), which was founded in 1865. ITU-T was established on 1 March 1993 within the framework of the "new" ITU, replacing the former International Telegraph and Telephone Consultative Committee (CCITT).

ITU-T aims to continue to be recognized as the pre-eminent worldwide telecommunication standards body.

The function of ITU-T is to provide global telecommunication standards by studying technical, operating and tariff questions. The results of these studies are published as **ITU-T Recommendations**. Although ITU-T Recommendations are non-binding, they are widely used because they guarantee the interconnectivity and interoperability of networks and enable telecommunication services to be provided worldwide.

Standardization work is carried out by 13 Study Groups (SGs) in which representatives of the ITU-T membership develop Recommendations for the various fields of international telecommunications.

The ITU Telecommunication Standardization Study Groups and their Working Parties are at the core of the standardization work. Every Study Group has assigned items of study. These items are grouped under a set of so called Questions. Serving as reference guides Recommendations are elaborated as result of treating the Questions.

2.2 QoS Measurement Activities within ITU-T

ITU-T is working on a specific project that deals with IP and the following twelve work areas have been identified as being of current major concern to the ITU-T:

- Area 1 - Integrated architecture.
- Area 2 - The impact of access to IP applications on telecommunications access infrastructures.
- Area 3 - Interworking between IP based network and switched-circuit networks, including wireless based networks.
- Area 4 - Multimedia applications over IP.
- Area 5 - Numbering and addressing.
- Area 6 - Transport for IP-structured signals.
- Area 7 - Signaling support, IN and routing for services on IP-based networks.
- Area 8 - Performance.
- Area 9 - Integrated management of telecom and IP-based networks.
- Area 10 - Security aspects.
- Area 11 - Network capabilities including requirements for resource management.
- Area 12 - Operations and Maintenance (OAM) for IP.
- Area 13 - Utilization of IPv6 in telecommunication networks.

The following is a schematic representation of the scope of the Project.

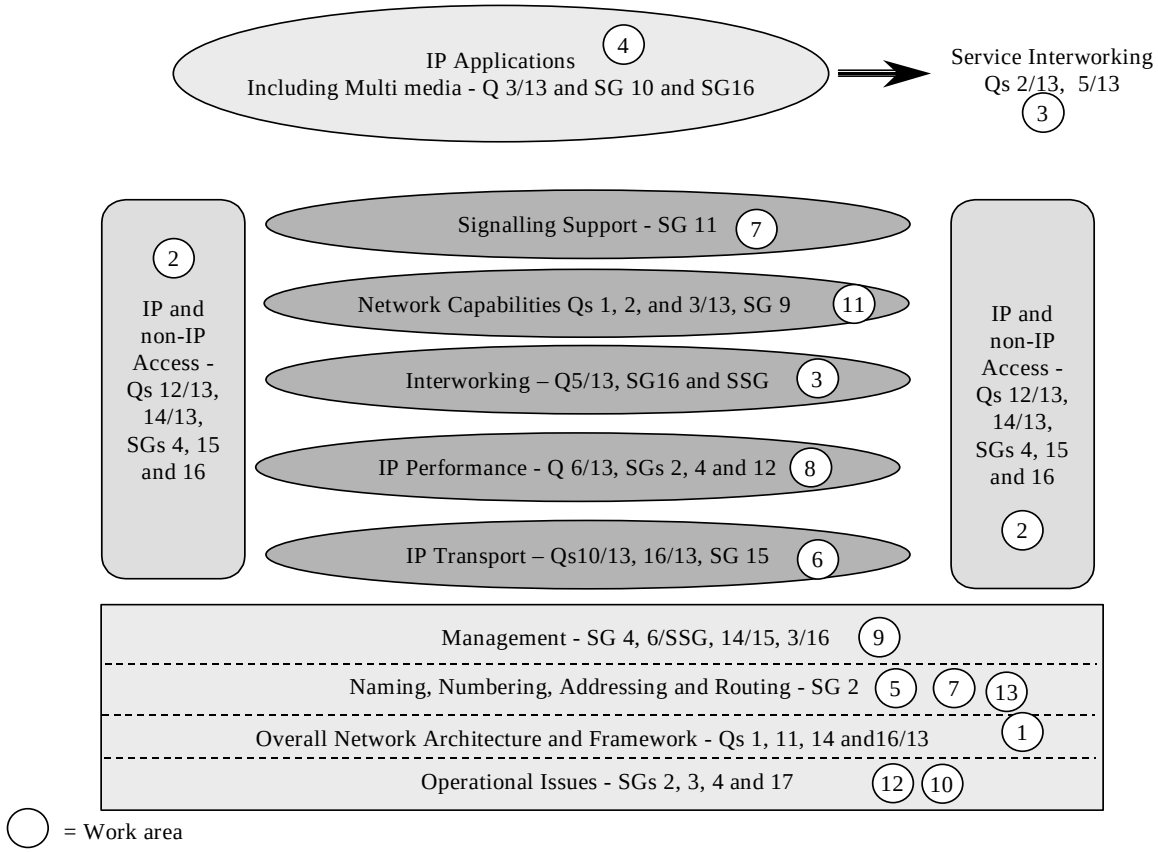


Figure 2-1: Scope of the ITU-T IP Project

Many recommendations are intended to cope with IP and the following table gives their organization.

Organization of the IP related Recommendations Y.1000-series	
General	**Y.1000 Series**
Services and Applications (including Multimedia)	**Y.1100 Series**
Architecture, Access, Network Capabilities and Resource Management	**Y.1200 Series**
Transport	**Y.1300 Series**
Interworking	**Y.1400 Series**
Quality of Service and Network Performance	**Y.1500 Series**
Signaling	**Y.1600 Series**
OAM	**Y.1700 Series**
Charging	**Y.1800 Series**

A primary management issue is the coordination of ITU-T technical activities in this project area, externally and internally. Specific issues include:

- Articulation of quantitative QoS requirements that can shape the development of IP telephony and other real-time services provided by IP networks. Development of corresponding IP packet transfer performance parameters, objectives, and QoS classes.

- Promotion, contribution and support of elaboration of network mechanisms (e.g. IETF IntServ, DiffServ, MPLS) that could enable the delivery of services differentiated by QoS characteristics.
- Provision of recommendations for co-operative implementation of QoS assurance mechanisms in interconnected IP network domains (e.g., policy management among service providers, traffic engineering guidelines). Study the introduction of dynamic bandwidth reservation/protection mechanisms such as “shaping” and “policing”.
- Development of recommendation covering the reliability and availability of IP networks and of services supported by IP networks. Fulfill the emergency service requirements (e.g. recommendation E.106 on International Emergency Preference Service).

2.3 Relationship between the ITU-T Working Groups

As shown in Figure 2-1, many Study Groups are involved in IP. This document describes activities of SG 13 and 4 and especially work related to specific questions dealing with performance and maintenance.

2.3.1 SG 13 Multi-protocol and IP-based Networks and their Internetworking

Lead Study Group for IP related matters, B-ISDN, Global Information Infrastructure and satellite matters.

This Study Group is responsible for studies relating to internetworking of heterogeneous networks encompassing multiple domains, multiple protocols and innovative technologies with the goal to deliver high-quality, reliable networking. Specific aspects are architecture, interworking and adaptation, end-to-end considerations, routing and requirements for transport.

One question, Q6, deals with the specific aspect of performance, where metrics and objectives are defined in two Recommendations Y.1540 and Y.1541.

2.3.2 SG 4 Telecommunication Management, including TMN

Lead Study Group on TMN.

This Study Group is responsible for studies regarding the management of telecommunication services, networks, and equipment using the telecommunication management network (TMN) framework. Additionally the group is also responsible for other telecommunication management studies relating to designations, transport-related operations procedures, and test and measurement techniques and instrumentation.

Question 3 (Q3) deals with specific aspects of IP operational procedures in Recommendation M.2301 and Question 4 (Q4) deals with test and measurement techniques and instrumentation in draft Recommendation O.iptest.

2.3.3 Work on OAM Facilities for IP-based Networks

This work is being carried out in Study Groups 4, 13 and 15. Study Group 13 is developing OAM network techniques that can be used to control and manage IP layer functions required in operations and maintenance (Recommendations Y.1710 and Y.1711 on OAM for MPLS). Study Group 15 is responsible for defining the implementation of these functions in IP network equipment, although much of this work is being done by IETF. Study Group 4 makes use of

these OAM facilities to carry out management functions in the transport plane and control plane in concert with the TMN management capabilities. In an IP-based network environment, the distinction between control-plane, signaling plane and management plane (TMN) is blurring.

Issues to be looked at include:

- Supporting mechanisms for collection of information which can be used for charging users of the resources, specifically the end users of the services
- Supporting mechanisms for collection of information which can be used for the Settlement between users of the resources, specifically between Network Operators and/or Service Providers
- Supporting mechanisms for collection of performance and QoS information that can be used to support management of QoS and SLAs.

Relationship between these groups is shown in Figure 2-2.

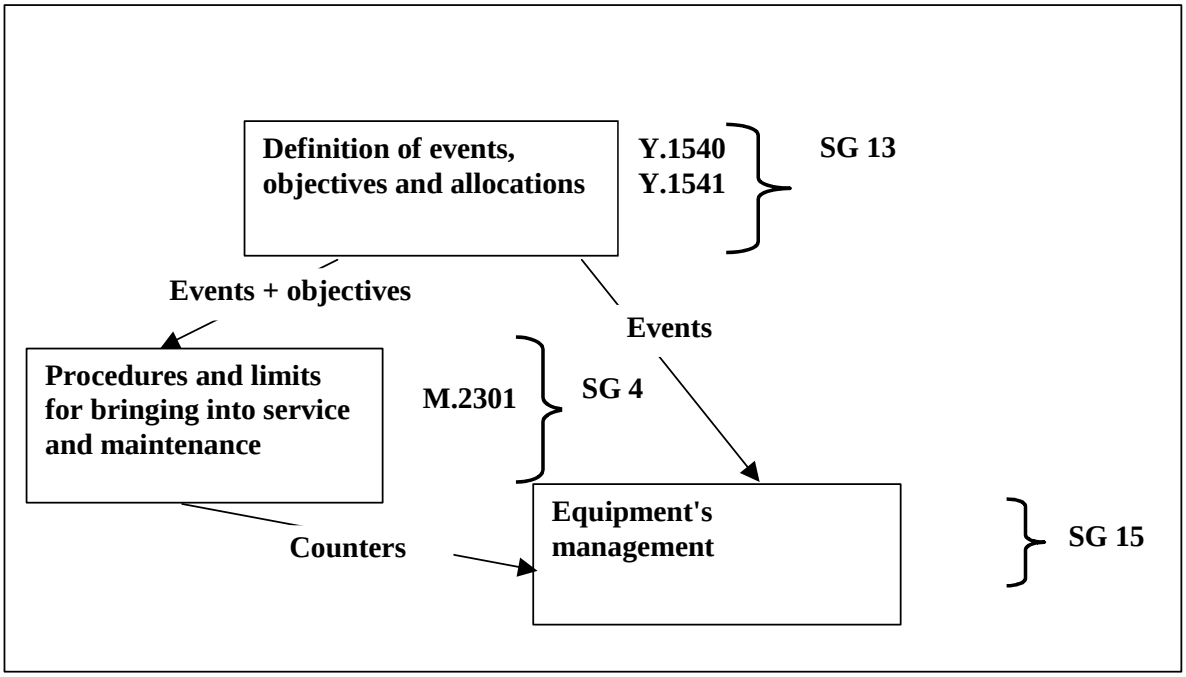


Figure 2-2: Relationship between ITU-T SGs

2.4 Results-Methodologies-Techniques and Work under Study in SG 13

ITU-T Recommendation Y.1540 defines parameters that may be used in specifying and assessing the performance of speed, accuracy, dependability, and availability of IP packet transfer of international IP data communication service. The defined parameters apply to end-to-end, point-to-point IP service and to the network portions that provide, or contribute to the provision of such service. End-to-end IP service refers to the transfer of user-generated IP datagram referred to as IP packets between two end hosts as specified by their complete IP addresses.

Basically this Recommendation defines parameters that can be used to characterize IP service provided using IPv4; applicability or extension of Y.1540 to other IP services (e.g. guaranteed service) and other protocols (e.g. IPv6, RSVP) is for further study. The performance of point-to-multipoint IP service is also for further study.

The IP service performance parameters are defined on the basis of IP packet transfer reference events that may be observed at measurement points (MPs) associated with specified functional and jurisdictional boundaries. For comparability and completeness, IP service performance is considered in the context of the 3×3 performance matrix that identifies three protocol-independent communication functions: access, user information transfer and disengagement. Each function is considered with respect to three general performance concerns (or "performance criteria"): speed, accuracy and dependability.

Future ITU-T Recommendations may be developed to provide standard methods of measuring the Y.1540 performance parameters in an international context. The Y.1540 parameters may be augmented or modified based upon further study of the requirements of the IP applications (e.g. interactive, block, stream) to be supported.

The Y.1540 speed, accuracy, and dependability parameters are intended to characterize IP service in the available state.

The Y.1540 parameters are designed to characterize the performance of service provided by network elements between specified section boundaries. However, users of this recommendation should be aware that network elements outside the specified boundaries could sometimes influence the measured performance of the elements between the boundaries.

Y.1540 does not provide the tools for explicit characterization of routing stability. However, the effects of route instability can be quantified using the loss and delay parameters defined. Specification of numerical performance objectives for some or all of the Y.1540 performance parameters may be found in Y.1541.

2.4.1 Network Components

Y.1540 defines the following network components:

- **Host**: A computer that communicates using the Internet protocols. A host implements routing functions (i.e. it operates at the IP layer) and may implement additional functions including higher layer protocols (e.g. TCP in a source or destination host) and lower layer protocols (e.g. ATM).
- **Router**: A host that enables communication between other hosts by forwarding IP packets based on the content of their IP destination address field.
- **Source host (SRC)**: A host and a complete IP address where end-to-end IP packets are originated. In general, a host may have more than one IP address; however, a source host is a unique association with a single IP address. Source hosts also originate higher layer protocols (e.g. TCP) when such protocols are implemented.
- **Destination host (DST)**: A host and a complete IP address where end-to-end IP packets are terminated. In general, a host may have more than one IP address; however, a destination host is a unique association with a single IP address. Destination hosts also terminate higher layer protocols (e.g. TCP) when such protocols are implemented.
- **Link**: A point-to-point (physical or virtual) connection used for transporting IP packets between a pair of hosts. It does not include any parts of the hosts or any other hosts; it operates below the IP layer. For example, a link could 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 IP layer.

2.4.2 Exchange Links and Network Sections

Y.1540 defines the following parts to be used in an IP connection:

- **Exchange link (EL)**: Can be the link connecting:
  - A source or destination host to its adjacent host (e.g. router) possibly in another jurisdiction, sometimes referred to as an access link, ingress link or egress link.
  - A router in one network section with a router in another network section.

  "Exchange link" is roughly equivalent to the term "exchange" as defined in RFC 2330.
- **Network Section (NS)**: A set of hosts together with all of their interconnecting links that together provide a part of the IP service between a source and a destination, and are under a single (or collaborative) jurisdictional responsibility. Some network sections consist of a single host with no interconnecting links. Source NS and destination NS are particular cases of network sections. Pairs of network sections are connected by exchange links.

  "Network section" is roughly equivalent to the term "cloud" as defined in RFC 2330. Any set of hosts interconnected by links could be considered a network section. However, for the purpose of IP performance allocation, it will be relevant to focus on the set of hosts and links under a single (or collaborative) jurisdictional responsibility (such as an ISP or an NSP). These hosts typically have the same network identifier in their IP addresses. Typically, they have their own rules for internal routing. Global processes and local policies dictate the routing choices to destinations outside of this network section (to other NS via exchange links). These network sections are typically bounded by routers that implement the IP exterior gateway protocols.
- **Source NS**: The NS that includes the source within its jurisdictional responsibility. In some cases the source is the only host within the source NS.
- **Destination NS**: The NS that includes the destination within its jurisdictional responsibility. In some cases the destination is the only host within the destination NS.

2.4.3 Measurement Points and Measurable Sections

The boundary between a host and an adjacent link at which performance reference events can be observed and measured is called a Measurement Point (MP). The standard Internet protocols can be observed at IP measurement points.

A section or a combination of sections is measurable if it is bounded by a set of MPs. The following sections are measurable:

- **Basic section**: An EL, an NS, a source, or a destination. Basic sections are delimited by MPs. The performance of any EL or NS is measurable relative to any given unidirectional end-to-end IP service. The *ingress MPs* are the set of MPs crossed by packets from that service as they go into that basic section. The *egress MPs* are the set of MPs crossed by packets from that service as they leave that basic section.
- **End-to-end IP network**: The set of EL and NS that provide the transport of IP packets transmitted from source to destination. The MPs that bind the end-to-end IP network are the MPs at the source and the destination. The end-to-end IP network performance is measurable relative to any given unidirectional end-to-end IP service. The *ingress MPs* are the MPs crossed by packets from that service as they go into the end-to-end network at the source. The *egress MPs* are the MPs crossed by packets from that service as they leave the end-to-end network at the destination.
- **Network section ensemble (NSE)**: An NSE refers to any connected subset of NSs together with all of the ELs that interconnect them. The term NSE can be used to refer to a single NS, two NSs, or any number of NS and their connecting EL. Pairs of distinct

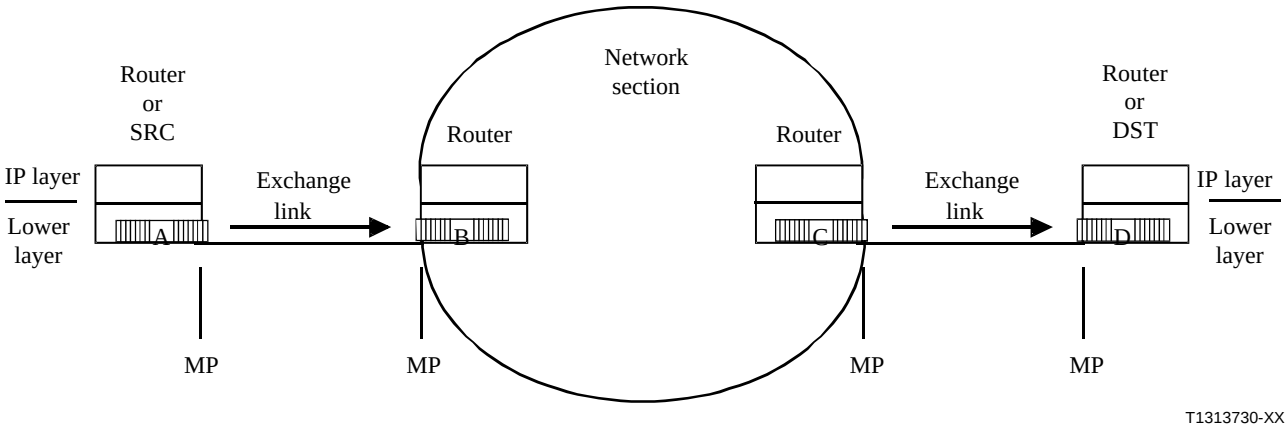
NSEs are connected by exchange links. The term NSE can also be used to represent the entire end-to-end IP network. MP delimits NSEs. The performance of any given NSE is measurable relative to any given unidirectional end-to-end IP service. The *ingress MPs* are the set of MPs crossed by packets from that service as they go into that NSE. The *egress MPs* are the set of MPs crossed by packets from that service as they leave that NSE.

2.4.4 Reference Events

The following definitions apply on a specified end-to-end IP service. The defined terms are illustrated in Figure 2-3. An IP packet transfer event occurs when:

- An IP packet crosses a measurement point (MP).
- Standard IP procedures applied to the packet verify that the header checksum is valid.
- The source and destination address fields within the IP packet header represent the IP addresses of the expected source and destination.

IP packet transfer reference events are defined without regard to packet fragmentation. They occur for every IP packet crossing any MP regardless of the value contained in the "more-fragments flag".



NOTE 1 – IP exit events for packets A and C.
NOTE 2 – IP entry events for packets B and D.

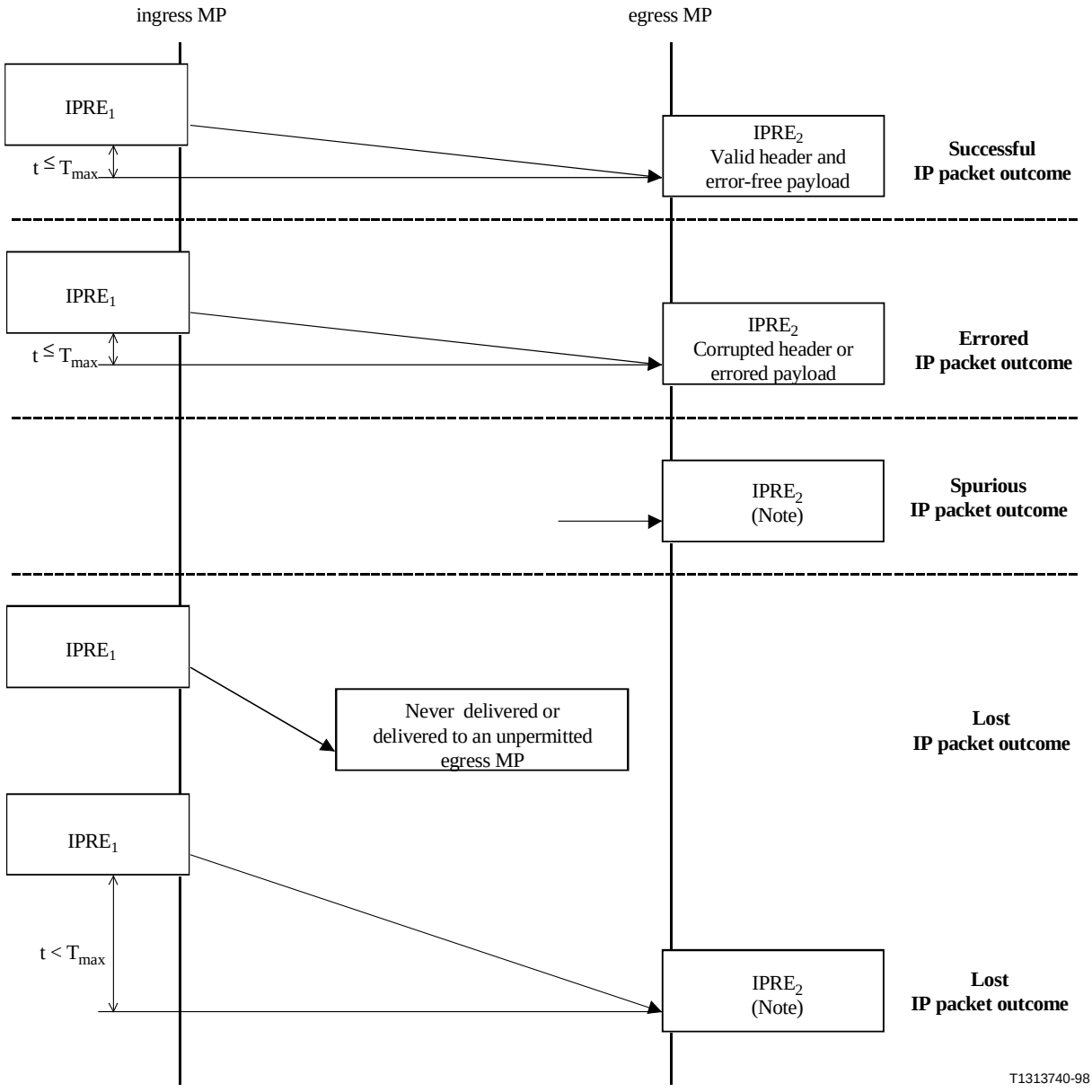
Figure 2-3: Example IP Packet Transfer Reference Events

Four types of IP packet transfer events are defined:

- **IP packet entry event into a host**: An IP packet transfer entry event into a host occurs when an IP packet crosses an MP entering a host (NS router or destination) from the attached EL.
- **IP packet exit event from a host**: An IP packet transfer exit event from a host occurs when an IP packet crosses an MP exiting a host (NS router or source) into the attached EL.
- **IP packet ingress event into a basic section or NSE**: An IP packet transfer ingress into a basic section or NSE event occurs when an IP packet crosses an ingress MP into a basic section or a NSE.
- **IP packet egress event from a basic section or NSE**: An IP packet transfer egress event from a basic section or NSE occurs when an IP packet crosses an egress MP out of a basic section or a NSE.

IP packet entry and exit events always represent, respectively, entry into and exit from a host. IP packet ingress events and egress events always represent ingress into and egress from a section or an NSE. To illustrate this point, note that ingress into an EL creates an exit event from the preceding host, while ingress into an NS is an entry event because, by definition, NSs always have hosts at their edges.

For practical measurement purposes, IP packet transfer reference events need not be observed within the IP protocol stack of the host. Instead, observing the IP packets crossing an associated physical interface can approximate the time of occurrence of these reference events. This physical interface should, however, be as near as possible to the desired MP. In cases where reference events are monitored at a physical interface, the time of occurrence of an exit event from a host is approximated by the observation of the first bit of the IP packet coming from the host or test equipment. The time of occurrence of an entry event into a host is approximated by the observation of the last bit of the IP packet going to the host or test equipment.



NOTE – Outcome occurs independent of IP packet contents

Figure 2-4: IP Packet Transfer Outcomes

2.4.5 IP Packet Transfer Outcomes

By considering IP packet transfer reference events, a number of possible IP transfer outcomes may be defined for any packet attempting to cross a basic section or an NSE. A transmitted IP packet is *successfully transferred, corrupted or lost*. A delivered IP packet for which no corresponding IP packet was offered is said to be *spurious*.

Figure 2-4 illustrates the IP packet transfer outcomes.

The definitions of IP packet transfer outcomes are based on the concepts of *permissible ingress MP*, *permissible egress MP* and *corresponding packets*.

These outcomes are defined without restriction to a particular packet type (TOS, DSCP, protocol, etc.). IP performance will differ by packet type.

2.4.5.1 Global Routing Information and Permissible Output Links

In theory, in a connected IP network, a packet can be delivered to any router, NS, or NSE, and still arrive at its destination. However, global routing information defines a restricted set of destination addresses that each network (autonomous system) is willing and able to serve on behalf of each of its adjoining NS. It is reasonable to assume that (in the worst case) an NS will completely discard any packets with destination addresses for which that NS has announced an inability (or an unwillingness) to serve. Therefore all IP packets (and fragments of packets) leaving a basic section should only be forwarded to other basic sections as *permitted* by the available global routing information.

For performance purposes, the transport of an IP packet by an NSE will be considered successful only when that NSE forwards all of the packet contents to other basic sections as permitted by the currently available global routing information. If the destination address corresponds to a host attached directly to this NSE, the only permitted output and the only successful IP transport is forwarding to the destination host.

IP procedures include updating of global routing information. A NS that was permissible may no longer be permissible following an update of the routing information shared between NSs. Alternatively a NS that was not previously permissible may have become permissible after an update of the global routing information.

At a given time, and relative to a given end-to-end IP service and a basic section or NSE:

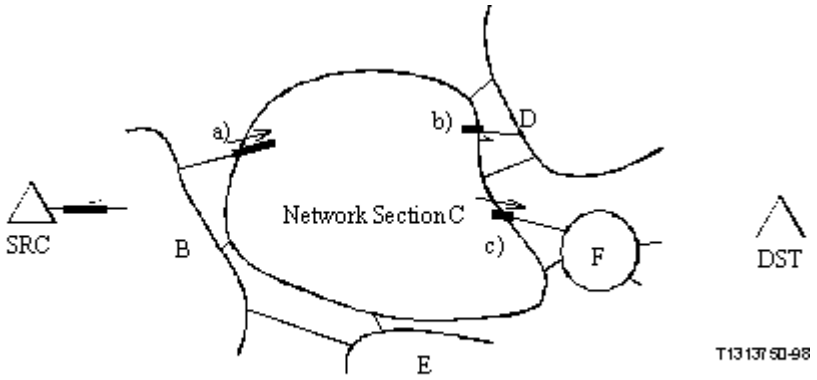
- An ingress MP is a *permissible ingress MP* if the crossing of this MP into this basic section or NSE is permitted by the global routing information.
- An egress MP is a *permissible egress MP* if the crossing of this MP leads into another basic section that is permitted by the global routing information.

2.4.5.2 Corresponding Events

Performance analysis makes it necessary to associate the packets crossing one MP with the packets that crossed a different MP. Connectionless routing means a packet may leave a basic section on any one of (possibly) several permissible egresses MP. Packet fragmentation means that a packet going into a basic section may leave in fragments, possibly into several different other basic sections. Finally, connectionless IP routing may even send a packet or a fragment back into a basic section it has already traversed (possibly due to the updating of routing tables).

An IP egress event is said to *correspond* to an earlier ingress event if the "same" IP packet created them. This concept applies whether the packet at the egress MP is the whole packet or just a fragment of the original. Figure 2-5 illustrates the case of a packet, which goes into NS C from NS B, and is fragmented into two parts in NS C. One of the fragments is sent to NS D and the other to NS F. Both of these egress events *correspond* to the single ingress event. To avoid confusion resulting from packets re-entering the NSE, this concept of *correspondence* also requires that this be the first time (since its ingress) this particular content has departed from the NSE.

The practical determination of whether IP reference events are corresponding is usually *ad hoc* and will often rely on consideration of the IP addresses, the global routing information, the IP packet identification field, other header information and the IP packet contents.



An IP packet from SRC to DST enters NS C, creates an ingress event, is fragmented, and creates two corresponding egress events, b) and c).

Figure 2-5: Corresponding Events when Fragmentation Occurs

In each definition, the possibility of packet fragmentation is accounted for by including the possibility that a single IP reference event could result in several subsequent events. Note that if any fragment is lost the complete original packet is considered lost. If no fragments are lost, but some are corrupted, the entire original packet is considered corrupted. For the delivery of the original packet to be considered successful, each fragment must be successfully delivered to one of the permissible output EL.

2.4.5.3 Successful IP Packet Transfer Outcome

A successful packet transfer outcome occurs when a single IP packet reference event at a permissible ingress MP_0 results in one (or more) corresponding reference event(s) at one (or more) egress MP_i, all within a specified time T_{max} of the original ingress event and:

- All egress MP_i where the corresponding reference events occur are permissible.
- The complete contents of the original packet observed at MP_0 are included in the delivered packet(s).
- The binary contents of the delivered IP packet information field(s) conform exactly with that of the original packet.
- The header field(s) of the delivered packet(s) is (are) valid.

The value of T_{max} is provisionally set at 3 seconds. Some global end-end paths may require a larger value of T_{max}. The value of 3 seconds has been used in practice.

2.4.5.4 Corrupted IP Packet Outcome

An corrupted packet outcome occurs when a single IP packet reference event at a permissible ingress MP_0 results in one (or more) corresponding reference event(s) at one (or more) egress MP_i, all within T_{max} time of the original reference event and:

- All egress MP_i where the corresponding reference events occur are permissible.
- The complete contents of the original packet observed at MP_0 are included in the delivered packet(s).
- Either the binary contents of the delivered IP packet information fields do not conform exactly from those of the original packet or one or several of the header fields of the delivered packets are corrupted.

Most packets with corrupted headers that are not detected by the header checksum at the IP layer will be discarded or redirected by other IP layer procedures (e.g. based on corruption in the address or TOS/DSCP fields). The result is that no reference event is created for the higher layer protocols expecting to receive this packet. Because there is no IP reference event, these packet transfer attempts will be classified as lost packet outcomes. Corrupted headers that do not result in discarding or misdirecting will be classified as corrupted packet outcomes.

2.4.5.5 Lost IP Packet Outcome

The definition of a lost IP packet outcome is predicated on a definition for a *misdirected packet*.

A misdirected packet occurs when a single IP packet reference event at a permissible ingress MP_0 results in one (or more) corresponding reference event(s) at one (or more) egress MP_i, all within a specified T_{max} time of the original reference event and:

- The complete contents of the original packet observed at MP_0 are included in the delivered packet(s).
- One or more of the egress MP_i where the corresponding reference events occur are not permissible egress MP.

A lost packet outcome occurs when a single IP packet reference event at a permissible ingress MP_0 results in a misdirected packet outcome or when some or all of the contents of that packet do not result in any IP reference event at any egress MP within the time T_{max}.

2.4.5.6 Spurious IP Packet Outcome

A spurious IP packet outcome occurs for a basic section, an NSE, on end-to-end when a single IP packet creates an egress event for which there was no corresponding ingress event.

2.4.5.7 IP Packet Severe Loss Block Outcome

An IP packet severe loss block outcome occurs for a block of packets observed during time interval T_s at ingress MP_0 when the ratio of lost packets at egress MP_i to total packets in the block exceeds s1.

The value of time interval T_s is provisionally set at 1 minute. The value of threshold s1 is provisionally set at 0.2. Evaluation of successive blocks (time intervals) should be non-overlapping.

These values are intended to identify IP path changes due to routing updates, which cause significant degradation to most user applications.

2.4.6 Performance Parameters

A set of IP packet information transfer performance parameters may thus be defined using the IP packet transfer outcomes defined above. All of the parameters may be estimated based on observations made at MP that bound the basic section or NSE under test.

2.4.6.1 Populations of Interest

Most of the performance parameters are defined over sets of packets called *populations of interest*. For the *end-to-end case*, the population of interest is usually the total set of packets being sent from source to destination. The measurement points in the end-to-end case are the MP at the source and destination.

For a basic section or NSE and relative to a particular source and destination pair, the population of interest at a particular permissible ingress MP is that set of packets being sent from source to destination that are routed into the basic section or NSE across that specific MP. This is called the *specific-ingress case*.

The total population of interest for a basic section or NSE relative to a particular source and destination pair is the total set of packets from source to destination that are delivered into the section or NSE across any of its permissible ingress MP. This is called the *ingress-independent case*.

Each of these IP performance parameters are defined without reference to a particular packet type (TOS, DSCP, protocol, etc.) Performance will differ by packet type and any statement about measured performance should include information about which packet type or types were included in the population.

2.4.6.2 IP Packet Transfer Delay (IPTD)

IP packet transfer delay is defined for all successful and corrupted packet outcomes across a basic section or an NSE. IPTD is the time, $(t_2 - t_1)$ between the occurrence of two corresponding IP packet reference events, ingress event $IPRE_1$ at time t_1 and egress event $IPRE_2$ at time t_2, where $(t_2 > t_1)$ and $(t_2 - t_1) \leq T_{max}$. If the packet is fragmented within the NSE, t_2 is the time of the final corresponding egress event. The end-to-end IP packet transfer delay is the one-way delay between the MP at the source and destination as illustrated in Figure 2-6 (illustrated for the end-to-end transfer of a single IP packet).

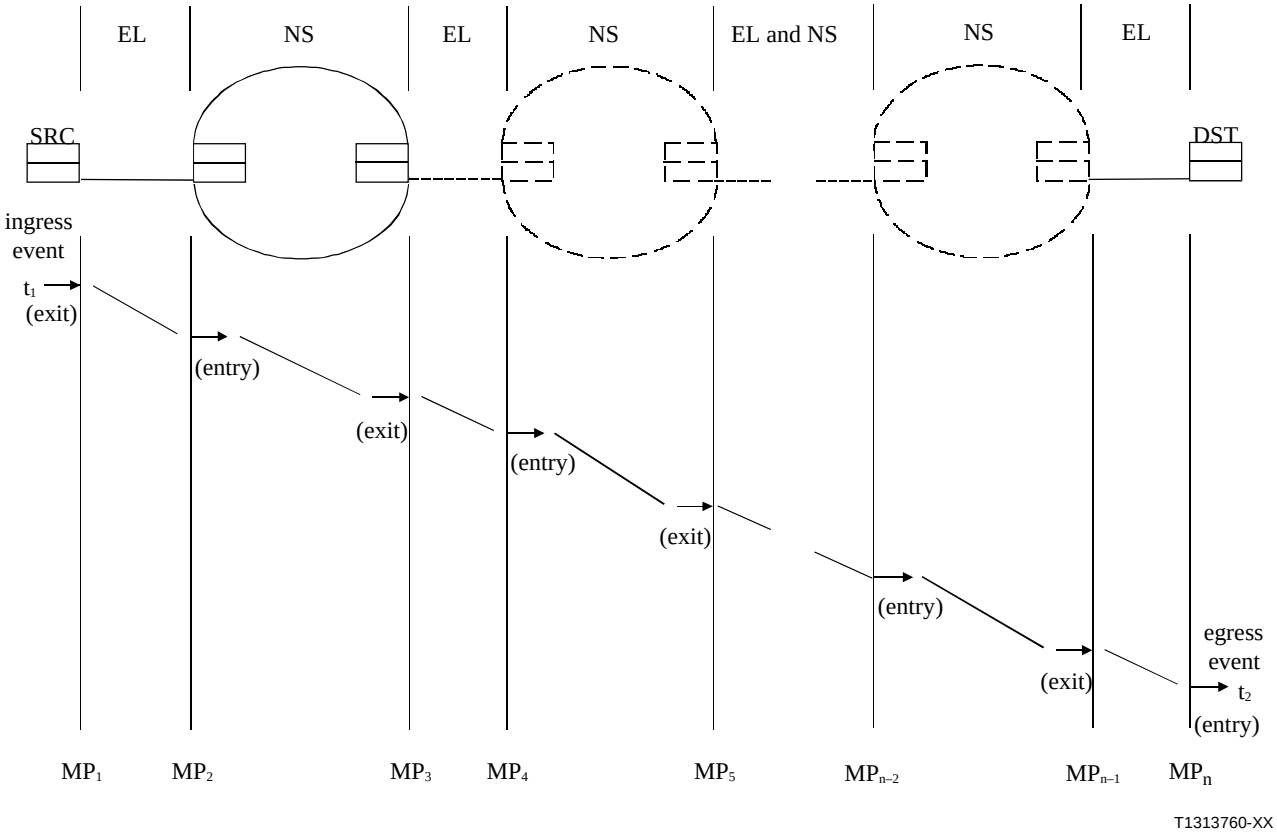


Figure 2-6: IP Packet Transfer Delay Events

The mean IP packet transfer delay is the arithmetic average of IP packet transfer delays for a population of interest.

The variations in IP packet transfer delay are also important. Streaming applications might use information about the total range of IP delay variation to avoid buffer underflow and overflow. Variations in IP delay will cause TCP retransmission timer thresholds to grow. Delay variation may cause packet retransmissions to be delayed or causes packets to be retransmitted unnecessarily.

End-to-end 2-point IP packet delay variation is defined based on the observations of corresponding IP packet arrivals at ingress and egress MP (e.g. MP_{DST}, MP_{SRC}). These observations characterize the variability in the pattern of IP packet arrival reference events at the egress MP with reference to the pattern of corresponding reference events at the ingress MP.

The 2-point packet delay variation (v_k) for an IP packet k between source and destination is the difference between the absolute IP packet transfer delay (x_k) of the packet and a defined reference IP packet transfer delay, $d_{1,2}$, between those same MPs (see Figure 2-7): $v_k = x_k - d_{1,2}$.

The reference IP packet transfer delay, $d_{1,2}$, between source and destination is the absolute IP packet transfer delay experienced by the first IP packet between those two MPs.

Positive values of 2-point IPDV correspond to IP packet transfer delays greater than those experienced by the reference IP packet; negative values of 2-point IPDV correspond to IP packet transfer delays less than those experienced by the reference IP packet. The distribution of 2-point IPDVs is identical to the distribution of absolute IP packet transfer delays displaced by a constant value equal to $d_{1,2}$.

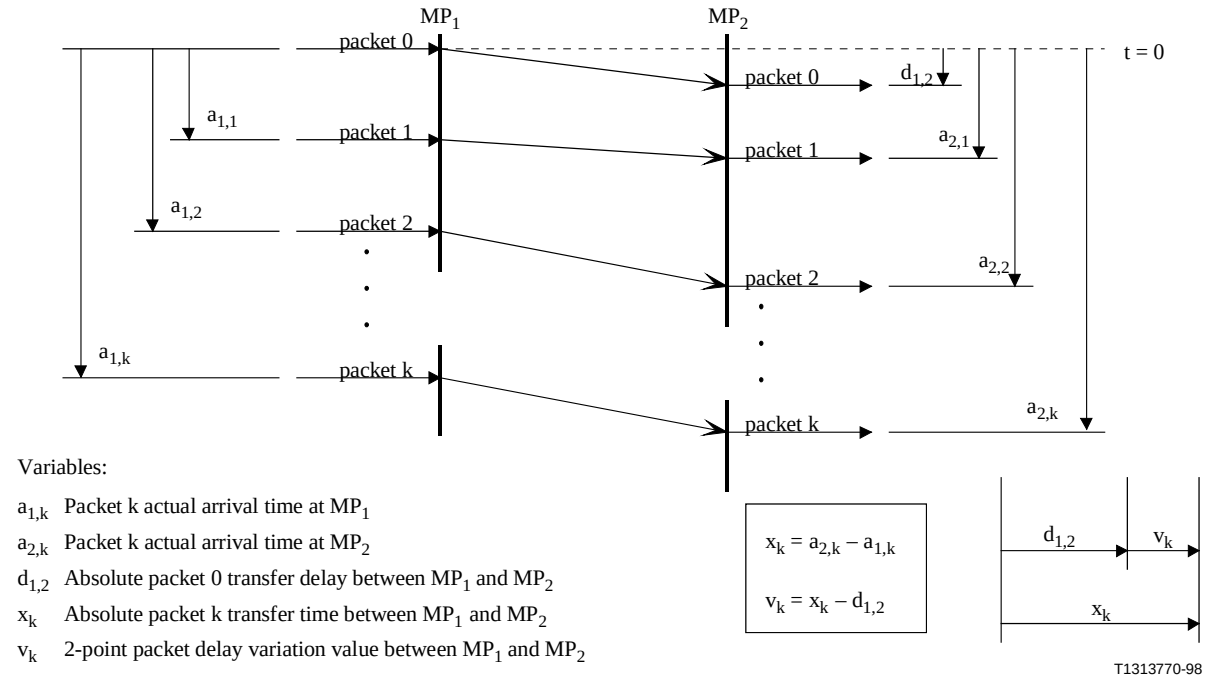


Figure 2-7: 2-Point IP Packet Delay Variation

As illustrated in Figure 2-7, the delay variation of an individual packet is naturally defined as the difference between the actual delay experienced by that packet and a nominal (expected) delay. An alternative to using the first packet delay as the nominal delay is to use the average delay of the population of packets as the nominal delay. This has the effect of centering the distribution of delay variation values on zero (when the distribution is symmetrical). It simplifies the analysis of delay variation range to use the packet with the minimum delay as the reference delay, and this is a recognized alternative.

One method for summarizing the IP packet delay variation experienced by a population of packets is to pre-specify a delay variation interval, e.g. ±30 milliseconds, and then observe the percentage of individual packet delay variations that fall inside and outside of that interval. If the ±30 millisecond interval were used, application with fixed buffer sizes of at or near 60 milliseconds would then know approximately, how many packets would cause buffer over- or underflow.

If this method is used for summarizing IP packet delay variation, the delay variant of individual packets should be calculated using the average delay as nominal, instead of the previous definition, because the pre-selected interval (e.g. the ±30 milliseconds) might occasionally be centered on an unusually large or small value.

An objective for IP packet delay variation could be established by choosing a lower bound for the percentage of individual packet delay variations that fall within a pre-specified interval. For example, "≥ 95% of packet delay variations should be within the interval [–30 msec, +30 msec]".

An alternative for summarizing the delay variation of a population of IP packets is to select upper and lower quantiles of the delay variation distribution and then measure the distance between those quantiles. For example, select the 99.9 percentile and then 0.1 percentile, make measurements, and observe the difference between the delay variation values at these two quantiles. This example would help application designers decide how to design for no more than 1% total buffer over- and under-flow.

An objective for IP packet delay variation could be established by choosing an upper bound for the difference between pre-specified quantiles of the delay variation distribution. For example, "The difference between the 99.1 percentile and the 0.1 percentile of the packet delay variation should be no more than 100 milliseconds".

One or more parameters that capture the effect of IP packet delay variations on different applications may be useful. It may be appropriate to differentiate the (typically small) packet-to-packet delay variations from the potentially larger discontinuities in delay that can result from a change in the IP routing.

2.4.6.3 IP Packet Error Ratio (IPER)

IP packet error ratio is the ratio of total corrupted IP packet outcomes to the total of successful IP packet transfer outcomes plus corrupted IP packet outcomes in a population of interest.

2.4.6.4 IP Packet Loss Ratio (IPLR)

IP packet loss ratio is the ratio of total lost IP packet outcomes to total transmitted IP packets in a population of interest.

Metrics for describing One-way Loss Patterns may be found in RFC 3357. Consecutive packet loss is of particular interest to certain non-elastic real-time applications, such as voice and video.

2.4.6.5 Spurious IP Packet Rate

Spurious IP packet rate at an egress MP is the total number of spurious IP packets observed at that egress MP during a specified time interval divided by the time interval duration (equivalently, the number of spurious IP packets per service-second)[1].

2.4.6.6 IP Packet Severe Loss Block Ratio (IPSLBR)

An IP packet severe loss block ratio is the ratio of the IP packet severe loss block outcomes to total blocks in a population of interest.

This parameter can identify multiple IP path changes due to routing updates, also known as route flapping, which causes significant degradation to most user applications.

2.4.7 Performance Objectives

ITU-T Recommendation Y.1541 specifies IP performance values to be achieved internationally for each of the performance parameters defined in ITU-T Recommendation Y.1540. Some of these values depend on which Quality of Service (QoS) class the end-users and network providers agree on. This Recommendation defines six different QoS classes. This Recommendation applies to international end-to-end IP network paths. The QoS classes are intended to be the basis of agreements between end-users and network service providers, and between service providers. The classes should continue to be used when static agreements give way to dynamic requests supported by QoS specification protocols.

[1] *Since the mechanisms that cause spurious IP packets are expected to have little to do with the number of IP packets transmitted across the sections under test, this performance parameter is not expressed as a ratio, only as a rate.*

The limited number of QoS classes supports a wide range of applications, including the following: point-to-point telephony, multimedia conferencing, and interactive data transfer. While the performance needs of these applications are more demanding than most, there may be other applications that require new or revised classes. Any desire for new classes must be balanced with the requirement of feasible implementation, and the number of classes must be small for implementations to scale in global networks.

The QoS objectives are applicable when access link speeds are at the T1 or E1 rate and higher.

The QoS objectives are stated in terms of the IP layer performance parameters defined in ITU-T Recommendation Y.1540. A summary of the objectives can be found in Figure 2-9. All values in Figure 2-9 are provisional and they need not be met until they are revised (up or down) based on real operational experience.

The QoS class definitions in Figure 2-9 present bounds on the end-to-end network performance. As long as the users (and individual networks) do not exceed the agreed capacity specification or traffic contract, and a path is available (as defined in Y.1540), network providers should collaboratively support these end-to-end bounds for the lifetime of the flow.

The actual QoS offered to a given flow will depend on the distance and complexity of the path traversed. It will often be better than the bounds included with the QoS class definitions in Figure 2-9.

Static QoS class agreements can be implemented by associating packet markings (e.g., Type of Service precedence bits or Diff-Serv Code Point) with a specific class.

Protocols to support dynamic QoS requests between users and network providers, and between network providers, are under study. When these protocols and supporting systems are implemented, users or networks may request and receive different QoS classes on a flow-by-flow basis. In this fashion, the distinct performance needs of different services and applications can be communicated, evaluated, and acknowledged (or rejected, or modified).

2.4.7.1 Reference Path for End-to-End QoS

The end-to-end performance objectives are defined for the IP performance parameters corresponding to the IP packet transfer reference events (IPREs). The end-to-end IP performance objectives apply from Network Interface to Network Interface in Figure 2-8 (Source: cited Recommendation Y.1541 from the ITU). The end-to-end IP network path includes the set of Network Sections (NS) and inter-network links that provide the transport of IP packets transmitted from SRC to DST; the protocols below and including the IP layer (layer 1 to layer 3) within the SRC and DST may also be considered part of an IP network. NS are synonymous with operator domains, and may include IP Access Network Architectures as described in Recommendations E.651 and Y.1231.

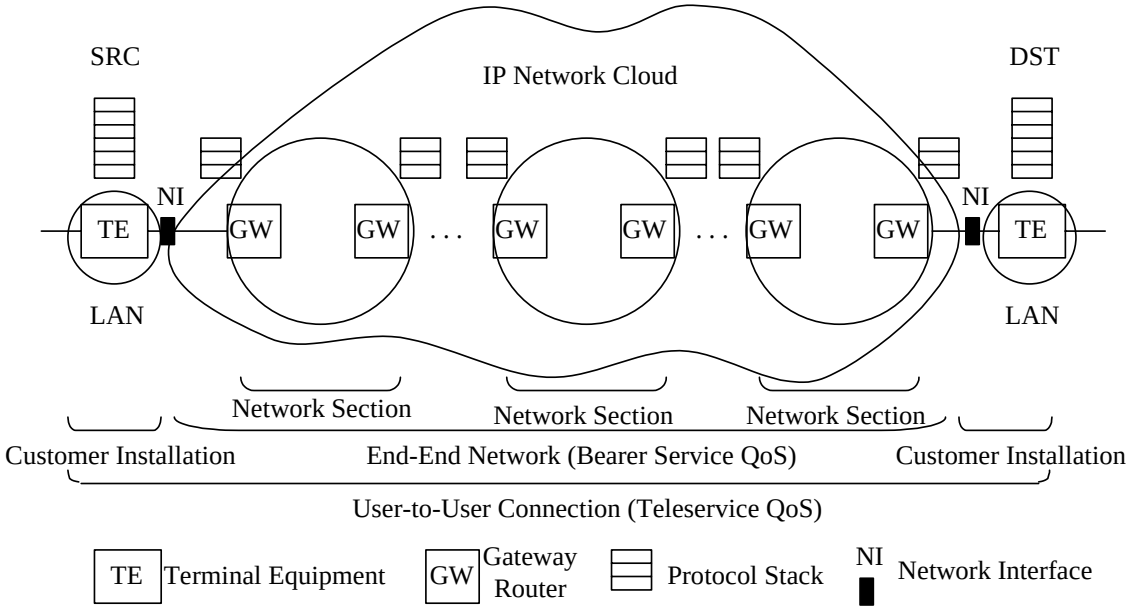


Figure 2-8: End-to-end Reference Path for QoS Objectives

The Customer Installation includes all Terminal Equipment (TE), such as a host and any router or LAN if present. The gateways that connect with terminal equipment may also be called Access Gateways.

Reference Paths have the following attributes:

- IP clouds may support User-to-User connections, User-to-Host connections, and other endpoint variations.
- Network Sections may be represented as clouds with Gateway routers on their edges, and some number of interior routers with various roles.
- The number of Network Sections in a given path may depend upon the Class of Service offered, along with the complexity and geographic span of each Network Section.
- There may be one or more Network Sections in a path.
- The Network Sections supporting the packets in a flow may change during its life.
- IP connectivity spans international boundaries, but does not follow circuit switched conventions (e.g., there may not be identifiable gateways at an international boundary if the same network section is used on both sides of the boundary).

2.4.7.2 QoS Classes

Each QoS class creates a specific combination of bounds on the performance values.

The objectives in Figure 2-9 apply to public IP networks, between MPs that delimit the end-to-end IP network. The objectives are believed to be achievable on common implementations of IP Networks.

The left-hand part of Figure 2-9 indicates the statistical nature of the performance objectives that appear in the subsequent rows.

The performance objectives for IP packet transfer delay are upper bounds on the underlying mean IPTD for the flow. Although many individual packets may have transfer delays that exceed

this bound, the average IPTD for lifetime of the flow (a statistical estimator of the mean) should normally be less than the applicable bound from Figure 2-9.

The performance objectives for 2-point IP Packet Delay Variation are based on an upper bound on the $1\text{-}10^{-3}$ quantile of the underlying IPTD distribution for the flow. The $1\text{-}10^{-3}$ quantile allows short evaluation intervals (e.g. a sample with 1000 packets is the minimum necessary to evaluate this bound). Also, this allows more flexibility in network designs where engineering of delay build out buffers and router queue lengths must achieve an overall IPLR objective on the order of 10^{-3}. Use of lower quantile values will result in under-estimates of de-jitter buffer size, and the effective packet loss would exceed the overall IPLR objective (e.g., an upper quantile of $1\text{-}10^{-2}$ may have an overall packet loss of 1.1%, with IPLR=10^{-3}).

The performance objectives for the IP packet loss ratios are upper bounds on the IP packet loss for the flow. Although individual packets will be lost, the underlying probability that any individual packet is lost during the flow should be less than the applicable bound from Figure 2-9.

Objectives for less-prevalent packet transfer outcomes and their associated parameters are for further study, such as the Spurious Packet Ratio (SPR) defined in Y.1540.

2.4.7.2.1 Evaluation Intervals and Reporting Requirements

The objectives in Figure 2-9 cannot be assessed instantaneously. Evaluation intervals produce subsets of the packet population of interest (as defined in ITU-T Recommendation Y.1540). Ideally, these intervals are:

- Sufficiently long to include enough packets of the desired flow, with respect to the ratios and quantiles specified.
- Sufficiently long to reflect a period of typical usage (flow lifetime), or user evaluation.
- Sufficiently short to ensure a balance of acceptable performance throughout each interval (intervals of poor performance should be identified, not obscured within a very long evaluation interval).
- Sufficiently short to address the practical aspects of measurement.

For evaluations associated with telephony, a minimum interval on the order of 10 to 20 seconds is needed with typical packet rates (50 to 100 packets per second), and intervals should have an upper limit on the order of minutes. A value of 1 minute is provisionally suggested, and in any case, the value used must be reported, along with any assumptions and confidence intervals.

2.4.7.2.2 Packet Size for Evaluation

Packet size influences the results for most performance parameters. A range of packet sizes may be appropriate since many flows have considerable size variation. However, evaluation is simplified with a single packet size when evaluating IPDV, or when the assessment targets flows that support constant bit rate sources, and therefore a fixed information field size is recommended. Information fields of either 160 octets or 1500 octets are suggested, and the field size used must be reported. Also, an information field of 1500 octets is recommended for performance estimation of IP parameters when using lower layer tests, such as bit error measurements.

2.4.7.2.3 Unspecified (Unbounded) Performance

For some QoS classes the value for some performance parameters is designated "U". In these cases, the ITU-T sets no objectives regarding these parameters. Network operators may unilaterally elect to assure some minimum quality level for the unspecified parameters, but the ITU-T will not recommend any such minimum.

Users of these QoS classes should be aware that the performance of unspecified parameters could be, at times, arbitrarily poor. However, the general expectation is that mean IPTD will be no greater than 1 second.

		QoS Classes					
Network Performance Parameter	**Nature of Network Performance Objective**	**Class 0**	**Class 1**	**Class 2**	**Class 3**	**Class 4**	**Class 5 Un-specified**
IPTD	Upper bound on the mean IPTD (Note 1)	100ms	400ms	100ms	400ms	1 s	U
IPDV	Upper bound on the 1-10^{-3} quantile of IPTD minus the minimum IPTD	50ms (Note 3)	50ms (Note 3)	U	U	U	U
IPLR	Upper bound on the packet loss probability	$1*10^{-3}$ (Note 4)	$1*10^{-3}$ (Note 4)	$1*10^{-3}$	$1*10^{-3}$	$1*10^{-3}$	U
IPER	Upper bound	1*10-4 (Note 5)					U

The objectives apply to public IP Networks. The objectives are believed to be achievable on common IP network implementations. The network providers' commitment to the user is to attempt to deliver packets in a way that achieves each of the applicable objectives. The vast majority of IP paths advertising conformance with Recommendation Y.1541 should meet those objectives. For some parameters, performance on shorter and/or less complex paths may be significantly better.

An evaluation interval of 1 minute is provisionally suggested for IPTD, IPDV, and IPLR, and in all cases the interval must be reported.

Individual network providers may choose to offer performance commitments better than these objectives.

"U" means "unspecified" or "unbounded". When the performance relative to a particular parameter is identified as being "U" the ITU-T establishes no objective for this parameter and any default Y.1541 objective can be ignored. When the objective for a parameter is set to "U", performance with respect to that parameter may, some times be arbitrarily poor.

Note 1 – Very long propagation times will prevent low end-to-end delay objectives from being met. In these and some other circumstances, the IPTD objectives in Classes 0 and 2 will not always be achievable. Every network provider will encounter these circumstances and the range of IPTD objectives provides achievable QoS classes as alternatives. The delay objectives of a class do not preclude a network provider from offering services with shorter delay commitments. According to the definition of IPTD in Y.1540, packet insertion time is included in the IPTD objective.

Note 3 –This value is dependent on the capacity of inter-network links. Smaller variations are possible when all capacities are higher than primary rate (T1 or E1), or when competing packet information fields are smaller than 1500 bytes.

Note 4 – The Class 0 and 1 objectives for IPLR are partly based on studies showing that high quality voice applications and voice coders will be essentially unaffected by a 10-3 IPLR.

Note 5 – This value ensures that packet loss is the dominant source of defects presented to upper layers, and is feasible with IP transport on ATM.

Figure 2-9: Provisional IP QoS Class Definitions and Network Performance Objectives

2.4.7.2.4 Discussion of the IPTD Objectives

Very long propagation times will prevent low end-to-end delay objectives from being met. In these and some other circumstances, the IPTD objectives in Classes 0 and 2 will not always be achievable. It should be noted that the delay objectives of a class do not preclude a network provider from offering services with shorter delay commitments. Every network provider will encounter these circumstances (either as a single network, or when working in cooperation with other networks to provide the end-to-end path), and the range of IPTD objectives in Figure 2-9 provides achievable QoS classes as alternatives. Despite different routing and distance considerations, related classes (e.g., Classes 0 and 1) would typically be implemented using the same node mechanisms.

2.4.7.2.5 Guidance on Class Usage

The following table gives some guidance for the applicability and engineering of the QoS Classes.

QoS Class	Applications (Examples)	Node Mechanisms	Network Techniques
0	Real-Time, Jitter sensitive, high interaction (VoIP, VTC)	Separate Queue with preferential servicing, Traffic grooming	Constrained Routing and Distance
1	Real-Time, Jitter sensitive, interactive (VoIP, VTC).		Less constrained Routing and Distances
2	Transaction Data, Highly Interactive, (Signalling)	Separate Queue, Drop priority	Constrained Routing and Distance
3	Transaction Data, Interactive		Less constrained Routing and Distances
4	Low Loss Only (Short Transactions, Bulk Data, Video Streaming)	Long Queue, Drop priority	Any route/path
5	Traditional Applications of Default IP Networks	Separate Queue (lowest priority)	Any route/path

Figure 2-10: Guidance for IP QoS Classes

2.4.8 IP Service Availability

IP service availability is applicable to end-to-end IP service, basic sections and NSE.

An availability function serves to classify the total scheduled service time for an IP service into available and unavailable periods. Based on this classification, both percent IP availability and percent IP unavailability are defined.

2.4.8.1 IP Service Availability Function

The basis for the IP service availability function is a threshold on the IPLR performance.

The IP service is available on an end-to-end basis if the IPLR for that end-to-end case is smaller than the threshold c_1.

The value of 0.75 for c_1 has been proposed but is considered provisional. Values of 0.9 and 0.99 have also been suggested for c_1. However, at this time, the majority of causes for unavailability appear to stem from failures where the loss ratio is essentially 100%, and unavailable periods of more than 5 minutes accompany such failures. When IP networks support multiple qualities of service, it may be appropriate to consider different values of c_1 for different services. In this case, c_1 values of between 0.03 and 0.2 (based on resilience of different speech coders) have been suggested for services.

Relative to a particular source and destination pair, *a basic section or an NSE is available for the ingress-independent case*, if the IPLR for that pair is smaller than the threshold c_1, as measured across all permissible ingress MPs.

Relative to a particular source and destination pair, *a basic section or an NSE is available for the specific-ingress case*, if the IPLR for that pair is smaller than the threshold c_1, as measured from a specific permissible ingress MP.

From an operations perspective, it will be possible to measure and/or monitor availability from specific ingress MP and then use this information to create inferences about the ingress-independent availability.

The quantitative relationship between end-to-end IP service availability and the IP service availability of the basic section or NSE remains for further study.

If the outage criteria are satisfied (i.e. IPLR exceeds c_1), the IP service is in the unavailable state (experiences an outage). The IP service is in the available state (no outage) if the outage criteria are not satisfied. The minimum number of packets that should be used in evaluating the IP service availability function is M_{av}. (The value of M_{av} is for further study. When tests of availability use end-user generated traffic, M_{av} of 1000 packets has been suggested.) The minimum duration of an interval of time during which the IP service availability function is to be evaluated is $T_{av.}$ (T_{av} is provisionally defined to be five minutes. Study has revealed that this value is consistent with practical limits on IP layer operations. Monitoring of lower layer performance and network element faults may be able to identify impending unavailability in a shorter time, and direct corrective action.)

This unidirectional definition of availability is motivated by the fact that IP packets often traverse very different routes from source to destination than they traverse from destination to source. If, from an IP network user perspective, a bi-directional availability definition is needed, a bi-directional definition can be easily derived from this unidirectional definition.

It is intended that this definition of IP service availability be applicable to both end-user generated IP traffic (i.e. the normal flow of IP packets between the SRC and the DST) as well as to traffic generated by test sets and test methodologies. In either case, the source of the IP traffic should be documented when reporting availability findings. Such documentation should include the specific types of packets used in each direction of flow.

Traffic generated specifically to test the availability state should be limited so that it does not cause congestion. This congestion could affect other traffic and/or could significantly increase the probability that the outage criteria will be exceeded.

2.4.8.2 IP Service Availability Parameters

The IP service availability may be equally described by one of the following parameters:

- **Percent IP service unavailability (PIU)**: The percentage of total scheduled IP service time (the percentage of T_{av} intervals) that is (are) categorized as unavailable using the IP service availability function.
- **Percent IP service availability (PIA)**: The percentage of total scheduled IP service time (the percentage of T_{av} intervals) that is (are) categorized as available using the IP service availability function.

It should be noted that PIU = 100 – PIA.

2.5 Results-Methodologies-Techniques and Work Under Study in SG 4

Two Questions of the Study Group 4 deal with maintenance and test of IP networks.

2.5.1 Question 3

Question 3 is related to "transport network and service operations procedures for performance and fault management". In this Question, one Recommendation has been developed, *M.2301*, which attends to performance objectives and procedures for provisioning and maintenance of IP based networks.

M.2301 provides performance objectives and procedures for provisioning and maintenance for IP based networks owned by different operators. This is regardless of the transport technology supporting the IP network and the higher layers to be implemented over IP. These objectives include error performance, delay performance and availability.

M.2301 defines parameters and their associated objectives based on the principles given in Y.1540. It uses a reference model based on the concept of IP Operator Domain (IPOD) and their interconnecting links.

2.5.1.1 Reference Model

Figure 2-11 shows a typical flow of an IP customer's traffic, through an IP network across a number of IPODs to the distant end.

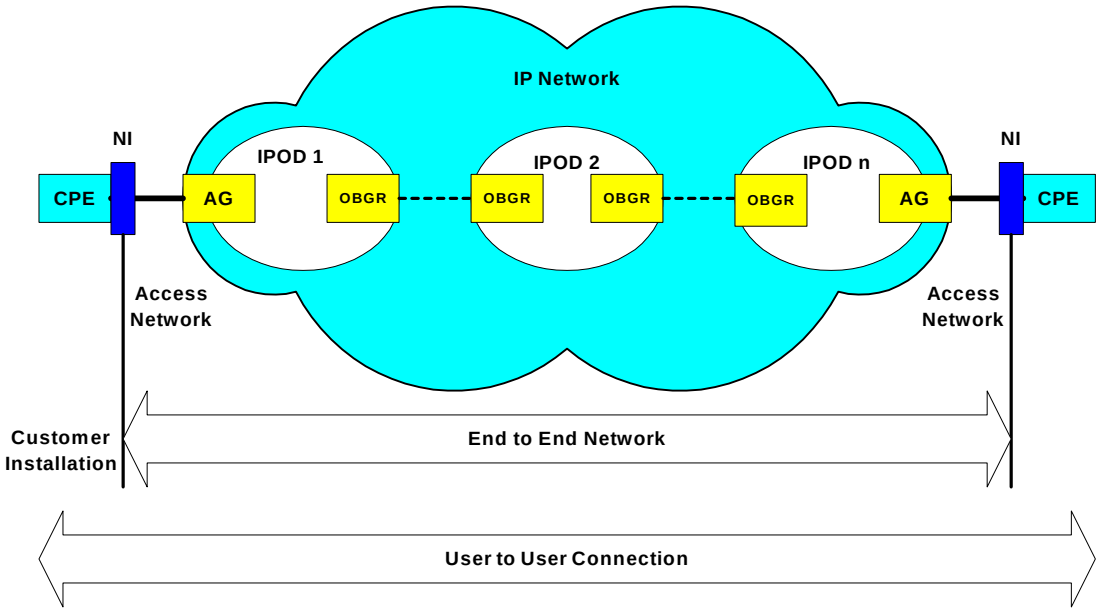


Figure 2-11: Reference Model for an End-to-end IP Flow

An IPOD consists of one or more Autonomous Systems (ASs) and their interconnecting links. The connecting links between IPODs involve a change in jurisdictional responsibility.

Operator Border Gateway Routers (OBGR) delimits each IPOD. Note that the IPOD may or may not include the access network portion. From that point, Access Gateway (AG), the routing is delegated to the routing policies of the operator.

The reference model is a network consisting of two access links and eight IPODs connected by seven OBGR to OBGR connecting links, for a total length of 27 500 km.

2.5.1.2 Performance Parameters

Parameters used in M.2301 are those of Y.1540 and Y.1541:

- IPTD (One way IP packet Transfer Delay).
- IPDV (One way IP packet Delay Variation).
- IPLR (IP packet Loss Ratio).
- IPER (IP packet Error Ratio).

A supplementary parameter has been introduced, IPDR (IP packet Discard Ratio). It is the ratio of total discarded IP packet outcomes to total transmitted IP packets in a population of interest. Discarded packets are those packets that are deliberately lost although they are without error. Packets are usually discarded because there is insufficient buffer space to store the packets while they wait for processing. Thus IP packet discard ratio is a measurement of network congestion.

2.5.1.3 Performance Objectives

Performance objectives are given for each parameter for an end-to-end IP flow, an IP flow across a single IPOD and a single link between OBGRs. They are defined according to the QoS classes specified in Y.1541. Since the stringent IPTD objectives of QoS classes 0 and 2 cannot be guaranteed on long distances, a reduced reference model consisting of two access links and three

IPODs connected by two OBGR-to-OBGR connecting links, for a total length of 10 000 km has been used for these QoS classes.

2.5.1.3.1 End-to-end IP flow

The following table gives the performance objectives for an end-to-end IP flow through two or more IPODs.

Parameter	IPTD	IPDV	IPLR	IPER	IPDR
QoS Class					
Class 0	100 ms	50 ms	5×10^{-4}	5×10^{-5}	5×10^{-4}
Class 1	400 ms	50 ms	5×10^{-4}	5×10^{-5}	5×10^{-4}
Class 2	100 ms	U	5×10^{-4}	5×10^{-5}	5×10^{-4}
Class 3	400 ms	U	5×10^{-4}	5×10^{-5}	5×10^{-4}
Class 4	1 sec	U	5×10^{-4}	5×10^{-5}	5×10^{-4}
Class 5	U	U	U	U	U

U means "unspecified" or "unbounded".

If the route distance across the IPOD exceeds 200 km then a propagation delay term, P, is added. This allows 1 ms for each integer multiple of 200 km.

2.5.1.3.2 IP flow across a single IPOD

The reference model proposes eight IPODS and therefore the performance objectives for one IPOD are given by the formulae:

- Single IPOD objective = End-to-end objective x 2/3 x 1/8 (for QoS classes 1, 3, 4 and 5).
- Single IPOD objective = End-to-end objective x 2/3 x 1/3 (for QoS classes 0 and 2).

The following table gives the performance objectives for a single IPOD.

Parameter	IPTD	IPDV	IPLR	IPER	IPDR
QoS Class					
Class 0	11 + P ms	FFS (For Further Study)	1.1×10^{-4}	1.1×10^{-5}	1.1×10^{-4}
Class 1	22 + P ms	FFS	4.2×10^{-5}	4.2×10^{-6}	4.2×10^{-5}
Class 2	11 + P ms	U	1.1×10^{-4}	1.1×10^{-5}	1.1×10^{-4}
Class 3	22 + P ms	U	4.2×10^{-5}	4.2×10^{-6}	4.2×10^{-5}
Class 4	72 + P ms	U	4.2×10^{-5}	4.2×10^{-6}	4.2×10^{-5}
Class 5	U	U	U	U	U

2.5.1.3.3 Single link between two adjacent IPODs

The following performance objectives are specified for the single link between the two OBGRs across the boundary between two IPODs. There are eight IPODs in the reference model, and

therefore the performance objective for one connecting link between adjacent IPODs is given by the formulae:

- Single link objective = End-to-end objective x 1/3 x 0.65 x 1/7 (for QoS classes 1, 3, 4, 5).
- Single link objective = End-to-end objective x 1/3 x 0.65 x ½ (for QoS classes 0 and 2).

Parameter	IPTD	IPDV	IPLR	IPER	IPDR
QoS Class					
Class 0	5 + P ms	FFS	5.4×10^{-5}	5.4×10^{-6}	5.4×10^{-5}
Class 1	8 + P ms	FFS	1.5×10^{-5}	1.5×10^{-6}	1.5×10^{-5}
Class 2	5 + P ms	U	5.4×10^{-5}	5.4×10^{-6}	5.4×10^{-5}
Class 3	8 + P ms	U	1.5×10^{-5}	1.5×10^{-6}	1.5×10^{-5}
Class 4	27 + P ms	U	1.5×10^{-5}	1.5×10^{-6}	1.5×10^{-5}
Class 5	U	U	U	U	U

2.5.1.3.4 Access links

The following performance objectives are specified for the access link between the NI and the AG. The performance objective for one access link is given by the formula:

- Access link objective = End-to-end objective x 1/3 x 0.175

Parameter	IPTD	IPDV	IPLR	IPER	IPDR
QoS Class					
Class 0	3 + P ms	FFS	3×10^{-5}	3×10^{-6}	3×10^{-5}
Class 1	15 + P ms	FFS	3×10^{-5}	3×10^{-6}	3×10^{-5}
Class 2	3 + P ms	U	3×10^{-5}	3×10^{-6}	3×10^{-5}
Class 3	15 + P ms	U	3×10^{-5}	3×10^{-6}	3×10^{-5}
Class 4	50 + P ms	U	3×10^{-5}	3×10^{-6}	3×10^{-5}
Class 5	U	U	U	U	U

2.5.1.4 Performance Measurements

There are two basic approaches to performance measurement defined in M.2301. These are “intrusive” and “non-intrusive” which equate to the terms “active” and “passive” used by the IETF. Some performance parameters can be measured only intrusively, others only non-intrusively, and some both intrusively and non-intrusively as illustrated, for example using MIB monitoring, in the following table:

Parameter	Intrusive	Non-intrusive
IPTD	√	
IPDV	√	
IPER	√	√
IPLR	√	√
IPDR		√

Intrusive performance measurements are made by inserting test packets interleaved with the normal traffic flows between two MPs. This kind of measurement allows detailed investigation of specific performance parameters e.g. one-way delay using time stamped packets, effect of packet size and number of packets on performance.

It should be noted that intrusive performance measurement causes additional traffic through the network so care must be taken to ensure that the use of this test does not cause congestion and the subsequent loss of customer's packets. It is also important that the test is not carried out when customer traffic is so low that the results of the test are invalid.

The test packet stream and the measurement period should be appropriate to the application service to be supported. The packet length and characteristics, and the intervals between measurements are for further study.

Non-intrusive performance measurements (using MIB monitoring) can be assessed by interrogating all the routers for performance statistics and thus obtaining a real time view of the effect of the network on the traffic passing through that network.

It should be noted that non-intrusive measurements could realistically be done only within one IPOD since it may be difficult or undesirable for one operator to access the routers in another's IPOD.

The elapsed time between two readings of MIB monitoring, depend on the interface bit rate and is given in the annex of M.2301.

2.5.1.5 Procedures

2.5.1.5.1 Bringing-into-service procedure

When a new AS or new network resource are brought into service, the following procedure shall be adopted in order to check that the performance across an IPOD still meets the limits M.2301 Recommendation.

End-to-end flow tests should be carried out between each pair combination of OBGRs. Each test pair should meet the performance objectives of the corresponding table. Upon successful completion of this test, the AS or network resources can be brought into service.

The tests should be repeated 24 hours after the AS or network resources have been brought into service in order to check that the introduction of them has not impaired the end-to-end performance.

If either the initial test or the repeat test fails, appropriate fault management procedures should be initiated.

Similarly, when a new link between two IPODs (pairs of OBGRs) or access links are brought into service, the same procedure should apply and the corresponding limits should be met.

2.5.1.5.2 Maintenance procedure

It is desirable that performance monitoring of an IPOD and links between IPODs is performed on a regular basis to check that performance is not degraded and to indicate possible congestion or fault conditions. The overall set of measurements or a subset of them can be used for this purpose. This procedure may include the application of maintenance thresholds to one or more performance parameters. If these are exceeded, corrective maintenance actions should be initiated. The limits given in the tables should also be used for maintenance.

2.5.2 Question 4

Question 4 is related to "test and measurement techniques and instrumentation for use on telecommunications systems and their constituent parts". One Recommendation is under study, *O.iptest*, which deals with test instrumentation to assess performance of transmission systems supporting IP.

This study is just beginning.

2.6 Current Task of the SGs Involved

2.6.1 Activity of SG 13

Applicability or extension to other protocols (e.g. IPv6) is for further study.

SG 13 will complement Recommendations Y.1540 and Y.1541 adding IP performance measurement methods. These complements will describe the effects of conditions external to the sections under test, including traffic considerations, on measured performance.

The following conditions should be specified and controlled during IP performance measurements:

- Exact sections being measured:
  - Source and destination for end-to-end measurements.
  - MP bounding an NSE being measured.
- Measurement time:
  - How long samples were collected.
  - When the measurement occurred.
- Exact traffic characteristics:
  - Rate at which the SRC is offering traffic.
  - SRC traffic pattern.
  - Competing traffic at the SRC and DST.
  - IP packet size.
- Type of measurement:
  - In-service or out-of-service.
  - Active or passive.
- Summaries of the measured data:

- Means, worst-case, empirical quantiles.
- Summarizing period, short period (e.g. one hour), long period (e.g. one day, one week, one month).

2.6.2 Activity of SG 4

2.6.2.1 New Recommendation O.iptest

The development of a new Recommendation *O.iptest* is started describing test and measurement equipment to perform tests at the IP layer based on a common format for a standard IP test packet.

When doing network provisioning and turned-up tests, it is important to use an IP test packet stream that stimulates the kinds of application services to be supported. Ping gives no indication of performance expected under normal traffic conditions since ping is a simple short packet. Variable length IP test packets should be available with at least a short test packet for VoIP and longer test packets for video and bulk data services.

Therefore, the IP test packet format will be defined with considerations on the performance measurement. Measurement modes will be studied as well as error performance measurements and the evaluation intervals.

2.6.2.2 Evolution of Recommendation M.2301

Recommendation M.2301 uses parameters defined in Y.1540 that can be used to characterize IP network performance provided using IPv4. Applicability or extension to other protocols (e.g. IPv6) is to be studied.

The test packet stream and the measurement period should be appropriate to the application service to be supported. The packet length and characteristics, and the intervals between measurements have to be studied, in conjunction with the draft Recommendation O.iptest.

Furthermore, reference model defined in M.2301 slightly differs from this of Y.1541. Those models should be redefined in order to have the same reference model in the two Recommendations.

2.7 IPv6 Concerns

The ITU-T and the Internet Engineering Task Force (IETF) are collaborating in a number of areas, taking account of the industry emphasis on Internet and IP structured signals. This collaboration is now well established concerning the current version (Version v4) of the IP protocol. Thus, a mapping already exists between the main Questions of different ITU-T Study Groups involved in the development of Recommendations in IP areas of the IP project and the different Work Groups of IETF.

However, no activity exists so far in ITU-T concerning the version 6 of IP protocol (IPv6). This lack must be rapidly filled regarding the market expectations on future advanced services based on IPv6 technology which are recognized as the future drivers by all the IPv6 actors (operators, ISPs, industry, users, academic world…). ITU-T has an important role to play to guarantee a large development of IPv6 networks and services.

Bearing in mind that foundations of IPv6 are already defined, the role of ITU-T is to extend to IPv6 protocol the activities currently conducted in the twelve areas of the IP project. As a result, Area 13 should have a transverse scope, and it will impact some of the other areas.

Due to the rapid evolution of the work related to IPv6 development in the world and to the growing interest for this technology, ITU-T must capitalize on the activities and on the experience achieved by standardization bodies and forums specialized on IPv6 such as IPv6 Forum, European IPv6 Task Force, Japanese IPv6 Promotion Council, North America IPv6 Task Force, etc. Consequently, area 13 will maintain a list of these standardization bodies and forums in order to establish relevant collaborations with them. The objective is to accelerate the work in different ITU-T Questions involved in IP technology (networking, interworking, interoperability, services, management, QoS, security, mobility) towards IPv6 protocol. Figure 2-12 provides a list of relations between main bodies involved in IPv6 technology.

Besides, when mapping activities related to IPv6 conducted in these bodies to similar activities in ITU-T Questions, some issues that are not yet addressed or that need further study could be identified. The result could be the identification of new ITU-T recommendations to be developed, based on the work and the knowledge that could be imported and shared with IETF and with other bodies and forums to meet rapidly the market expectations in IPv6 domain.

Organization	Background in IPv6	Objective	Main scope & results	Contact
ITU-T	New area in IP Project in SG13 (March 2002)	* Introduction of IPv6 as an item to be addressed in the ITU-T SGs * Consider the impact of IPv6 on the 12 areas of the IP project	Many SGs must be impacted: SG4, SG9, SG11, SG13, SG15, SG16, SSG	TSB Secretary to SG13: Georges Sebek WP 1/13 Chairman: Jean-Yves Cochennec
IETF	Initiated the work in 1992. WGs: IPng, ngTrans	Standardization of IPv6 protocol	A large number of RFCs WG IPng, ngTrans	
IPv6 Forum	Since 1999, + 150 members	Promotion of IPv6 through the world	Proceedings, dissemination	President: Latif Ladid Technical Directorate: Jim Bound
UMTS Forum	Promotion of UMTS & 3G	* IPv6 is a main topic	Dissemination	
GSM Association		* IPv6 is a main topic	Dissemination	
3GPP	Main body in standardization of 3G technology	UMTS R5, 6, 7, IMS domain IPv6 mandatory	IPv6, SIP mandatory in ISM	
ETSI		IPv6 interworking tests campaigns	Validation of IPv6 vendors implementations	Manager Philippe Cousin
OIF	Tampa OIF meeting in January 2001	Recommendations on Addressing of Optical Network (ONA) IPv4 and ONA to IPv6 Transition	Partnership with IPv6 Forum on 2001, IPv6 Strategy	

ISOC	Supervision of Internet activities (IETF, …)		Dissemination, Collaboration ISOC(IETF)/ITU-T	Chairman Brian Carpenter
ICANN	Elaboration of early rules of management of IPv6 addressing space	Management of IPv6 addressing space and supervision of RIRs. Improvement and adaptation of the existing rules	IPv6 space allocation rules to RIRs	
ARIN	Experimentation of early rules of management of IPv6 addressing space	Management of IPv6 addressing space and supervision of RIRs. Improvement and adaptation of the existing rules	IPv6 space allocation rules to LIRs in American Region	
APNIC	Experimentation of early rules of management of IPv6 addressing space	Management of IPv6 addressing space and supervision of RIRs. Improvement and adaptation of the existing rules	IPv6 space allocation rules to LIRS in Asia-Pacific region	
RIPE-NCC	Experimentation of early rules of management of IPv6 addressing space	Management of IPv6 addressing space and supervision of RIRs. Improvement and adaptation of the existing rules	IPv6 space allocation rules to LIRS in Europe region	
European IPv6 Task Force	03/2001-15/01/2002 4 WGs	Acceleration of development of IPv6 in Europe	Recommendations for *European Commission *Member States *Industry IST IPv6 Projects	President: Latif Ladid
Japan IPv6 Promotion Council		Acceleration of development of IPv6 in Japan	Recommendations to *Government *Industry *Academic world	Chairman Professor Jun Murai
North America IPv6 Task Force	First meeting 12/2001	Acceleration of development of IPv6 in USA	Recommendations	President: Michael Brig

Figure 2-12: ITU-T and other Standardization Bodies and Foras Involved in IPv6

2.8 Issues

Several aspects have to be addressed. A list of main issues to be addressed is provided hereafter, following an arbitrary classification of these issues in two major classes.

2.8.1 IPv6 Architecture/Interworking/Interoperability/Transition

- Addressing/Numbering/Naming.
- Routing.

- Transition and Coexistence IPv4/ IPv6.
- IPv6 Core/Transport Networks.
- IPv6 ADSL and Optical access Networks.
- GPRS/UMTS IPv6/IMT-2000 mobile access and core network.
- WLAN MIPv6 access networks.
- IPv6 satellite access network.
- IPv6 optical networks (OTN, ASON).
- Home networking.

2.8.2 IPv6 Services and Applications

- VPNv6.
- DNSv6.
- AAAv6/ Security v6.
- IPv6 Multicast.
- IPv6 on-line gaming.
- VoIPv6.
- Video/IPv6.
- Stream audio/Video.
- Web v6.
- Servers v6.
- Mobility v6.
- Management SNMP v6.
- IPv6 QoS Measurement/IPv6 performance.

2.9 Current Work within ITU-T

Decision to introduce a new area 13 in the IP Project has been taken in March 2002 SG13 meeting. Technical description and relations of this area are to be provided in November 2002 SG13 meeting.

2.10 Related Work within IETF

The collaboration between ITU-T and IETF in IPv4 is already in place, it should be extended to IPv6 protocol and increased with the context of the acceleration of IPv6 activities and the corresponding interest for IPv6. Besides, ITU-T activities should benefit from experience obtained by specialized IPv6 Working Groups (ipng, ngtrans) during the 10 last years through experimentations (e.g. 6Bone the first experimental worldwide IPv6 network, and experimentations conducted in regions or countries). Moreover, as IETF has established collaborations and cooperation with other bodies and forums involved in the development and the promotion of IPv6, the ITU-T will also benefit from results of these collaborations.

IETF and ITU-T have their respective action fields: the IETF strength lies in the protocol and application areas (it is also true for IPv6), whereas the ITU-T has a great deal to offer in the areas of architectural, network interworking and network evolution (it will be the case for IPv6). There is an opportunity for ITU-T to give a new dimension to IPv6 protocol regarding the deployment issue on a large scale.

Figure 2-13 provides a mapping of issues already mentioned to existing ITU-T Questions, with corresponding IETF Working Groups.

Question /SG	Addressing Numbering Routing DNS	Security AAA	QoS Measure-ment Perfor-mance Manage-ment	IPv6 Mobility UMTS /WLAN 3G-IMT-2000	Transport Equipment Inter-working Inter-operability Transition v4/v6	Access Networks: ADSL, Cable, Fibre	IPv6 Multimedia Services Applica-tions
ITU-T	Q.1/2 Q.2/2 Q.3/17 Q.2/16 Q.3/16 Q.7/SSG	Q.10/17	Q.3/4 Q.4/4 Q.5/4 Q.9/4 Q.13/12 Q.6/13 Q.9/2 Q.18/4 Q.8/17 Q.13/15 Q.14/15 Q.6/13 Q.8/13 Q.5/2 Q.9/2	Q.1/SSG	Q.9/15 Q16/15 Q10/15 Q.3/16 Q.10/13 Q.11/13 Q.11/15	Q.2/15	Q.C/16 Q.8/17 Q.1/16 Q.2/16 Q.6/9 Q.7/9 Q.1/16 Q.4/16 Q.6/16 Q.7/16 Q.9/16 Q.10/16 Q.15/16 Q.8/16
IETF	Enum nat msdp int seamoby	aaa tls wts pkix	Ippm tewg ccamp mpls diffserv ppvn snmpv3 sming idapv3	seamoby	pint ion ipfc gsmp mospf rohc tsvwg ipo iporpr	ppext Ipcdn ipfc	Iptel avt sip
IETF (IPv6)				IPv6 Working Groups (ipng, ngtrans) +40 RFCs & Drafts			

Figure 2-13: Mapping between ITU-T Questions and IETF WGs

It is generally accepted that the major commercial drivers of IPv6 will be those that "consume" a large number of address space and that support the "always-on" services such as:

- 3G wireless networks & services.
- ADSLv6.
- On-line games.
- Home networking.

The rapid growth of cellular devices and the potential lack of IPv4 addresses make inevitable the deployment of IPv6 addressing plans. 3GPP has already chosen in its Release 5 that IPv6 and SIP be mandatory protocols for IMS (Internet Multi-media Subsystem). This IMS will open a significant number of new business opportunities. In fixed networks, SIP and IP are used to offer multimedia services and the migration towards IPv6 of these services is a new issue that needs to be solved by operators and ISPs. The same scheme goes for the three other IPv6 drivers afore-

mentioned. In these conditions, ITU-T is expected to play a major role regarding interworking, interoperability and migration issues.

Main features of IPv6 are recalled below:

- Addressing, Naming & Numbering.

  With IPv6, there is no address space exhaustion. This principle will permit to operators to design network architectures less complex and cost effective, because there is no need to deploy NATs, and the renumbering becomes an automatic operation thanks to the hierarchical structure of the IPv6 address scheme.
- Routing.

  IPv6 is designed on routing hierarchy with aggregation, thus it will reduce routing tables.
- Management.

  IPv6 is based on plug and play thanks to an auto-configuration scheme. A reduction of the management costs of IPv6 networks and services is expected.
- Mobility .

  With the help of auto-configuration and IPv6 Neighbour Discovery, the host will operate in any location. Moreover, optimization of traffic and security associated to the update messages of mobile IPv6 protocol, between the mobile and its correspondent and with its Home Agent, are achieved and guaranteed.
- Security.

  With IPv6, the support of IPsec protocol becomes mandatory. Then, it allows end-to-end applications and especially that security-sensitive to operate in easier way and without NATs.

IETF RFCs and Drafts

Near 40 RFCs and Drafts are related to IPv6. Some of them are mentioned below:

- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification.
- RFC 2461: Neighbor Discovery for IP Version 6 (IPv6).
- RFC 2462: IPv6 Stateless Address Auto configuration.
- RFC 2463: Internet Control Message Protocol (ICMPv6).
- RFC 2373: IP Version 6 Addressing Architecture.
- RFC 2374: An IPv6 Aggregatable Global Unicast Address Format.
- RFC 2375: IPv6 Multicast Address Assignment.
- RFC 2464: Transmission of IPv6 Packets over Ethernet Network.
- RFC 2472: IP Version 6 over PPP.
- RFC 1933: Transition Mechanisms for IPv6 Hosts and Routers.
- RFC 2766: Network Address Translation - Protocol Translation.

3. TEST PACKETS: O.IPTEST

ITU is standardizing a test packet to perform tests of IP based networks and services. An IP measurement signature is a regular Internet packet that contains a standard block of fields needed for performing the measure. This block of fields is named IP measurement signature (IMS).

3.1 Framework

ITU-T SG4 is working on a topic with regard to performance measurements of IP networks and services. Question 4 of Study Group 4 is standardizing test and measurement equipment. The draft Recommendation, O.iptest, focuses on the standardization of a test packet format to perform tests of IP based networks and services.

The Type-P [RFC2330] is corresponds to the suite of protocols present in the IP and SUB-IP headers of the packet. The basic Types-P are UDP and TCP. In order to support provisioning and maintenance of IP-based networks, in order to measure the performance of IPv4 and IPv6 networks and services for different Type-P, a common standard IP Test Packet format is desirable such that interoperability between heterogeneous test equipment and comparison of measurement results can be achieved.

A standard IP test packet should meet the following requirements:

- **Network level**: It is necessary to define a test packet suitable for performing the measurement of existing IP performance metrics and flexible enough to permit proprietary extension and new format definition in the future. The format should be compatible with all SUB-IP media on IP versions and should allow accurate measurements in the Gbit range.
- **Application level**: The concern is not only the performance measurement of IP networks, but of numerous application services. To permit IP test packets to be transported in the same manner as regular application packets, it is necessary to use test packets with the same behaviour as regular packets of the tested IP service. The IP test packet format defined should accept the header of any regular IP application.
- **Interoperability**: There is a need for interoperability between instruments of different manufacturers to monitor consistently network performance and QoS. That will offer measurement results comparison against SLAs and correlation between measurement points and instruments.
- **Inter-domain interoperability**: This is motivated by the need to perform end-to-end tests across administrative areas and composite networks.

It is necessary to increase operational interoperability by promoting the sharing of the same measurement identification mechanism in the test packet to permit the managers of the measurement systems to exchange results among administrative domains.

The signature is flexible enough to define several classes of measurement packets, mainly transport and application classes.

Signature classes

Some examples of signature classes are given hereafter, for illustration purpose only:

	Classes	Length data	Extension	Type	Signature length (bytes)
Applications	VoIP	RTP SDU-Signature	0	1	20
	HTTP	Variable	1	1	28
Transport	UDP	Variable	0	1	20
	TCP	Variable	1	1	28
Network	IPv4	Variable	0	1	20
	IPv6	Variable	0	1	20

Figure 3-1: Examples of Signature Classes

3.1.1 Requirements and Benefits

3.1.1.1 Requirements

M.2301 (ex-M.23ip) has defined two basic IP network measurement approaches – intrusive (active[2]) and non-intrusive (passive[1]) measurements. The intrusive measurements use an IP test packet stream to create an IP flow over the route to be tested during network provisioning and service turn-up. Non-intrusive measurements use one of two methods – monitoring and collection of MIB data from network elements such as routers for performance assessment and maintenance, or monitoring of low-levels of test traffic interspersed with Customers' traffic using non-intrusive probes attached at key MPs in the network such as IP peering points.

M.2301 (ex-M.23ip) suggests that three of the key performance parameters IPER, IPLR and IPDV (1pt) can be measured using MIB monitoring, but IPTD must be done intrusively using an IP test packet stream. A way round this is to insert IP test packets at a low rate interspersed with Customers' traffic (as noted above) and monitor the time-stamped IP test packets at key network nodes. This might be thought of as a "mixed mode" where the test packets are inserted intrusively, but they are monitored non-intrusively.

Furthermore, using simple methods such as ICMP "ping" or Trace Route can only measure IP round trip delay (IPRTD) and one-way delay is of course not equal to half the IPRTD in a packet network. Two other problems with using ping are that the ping response function in routers is increasingly being turned off to reduce hacker and denial-of-service attacks and, even if activated, ping has the lowest priority in router packet processing. Delay measured by ping is therefore not a true measure of delay experienced by Customers' traffic. In fact, ping is really only a basic, but useful, connectivity check.

When doing network provisioning and service turn-up tests, it's important to use an IP test packet stream that simulates the kinds of application services to be supported. Ping gives no indication of performance expected under normal traffic conditions since ping is a simple short packet. Variable length IP test packets should be available with at least a short test packet for VoIP and longer test packets for video and bulk data services.

For measuring the quality of service, it is important to have operational interoperability among heterogeneous manufacturers and to perform delay and lost measurement across administrative

[2] *Note: IETF uses the term "active" for intrusive and "passive" for non-intrusive measurements.*

areas or composite networks for the different Type-P. The basics Type-P are obviously UDP and TCP.

It should be possible to use varying packet sizes and network services.

It should be possible to make test packets as small as possible, to be able to accurately measure paths where packet-splitting technologies such as ATM are used.

To gain interoperability, the manager of the measurement system must unambiguously identify the owner of results of the measure performed on a test packet. The IMS must identify the owner of the measure.

The definition must consider the measure of the performance of multicast services, mobile IP services and IPv6.

The protocol translation mechanisms and the coexistence between IPv4 and IPv6 are potential sources of interoperability of the measurements. The test packet must be not be rejected by IPv6/IPv4 translation functions (NAT-PT).

3.1.1.2 Benefits

The principal benefits to be gained by standardizing an IP test packet can be summarized:

- IP-based services can be provisioned and turned-up consistently and QoS established against negotiated SLAs. This enables operators to establish a “baseline” or “footprint” set of QoS parameters for real-time services.
- Network performance and QoS can be monitored consistently and measurement results compared against SLAs and correlated between different MPs and instruments.
- More effective fault isolation and trouble-shooting of network problems results in faster service restoration and lower operations and maintenance costs.
- Network dynamics and potential problems (e.g. congestion) can be investigated using different simulated application service IP traffic.
- Interoperability between instruments of different manufacture can be assured.
- Interoperability between administrative domains can be assured.
- Interoperability between composite networks can be assured.

3.1.1.3 IP Measurement Signature Format

The proposed IP test packet can be used for intrusive measurements of IP network performance to support QoS service level and as a stimulus for non-intrusive IP performance monitoring at key points in the network. It can also be used for checking throughput if programmable features are set to the selected IP transfer capability (traffic contract) for a given application service.

It consists of SUB-IP header and trailer, an IP header suite, a data block and an IP measurement signature. The signature is inserted at the end of the packet. The SUB IP and IP header suites determine the type-P of the packet.

3.1.1.4 IP Test Packet Size

Figure 3-2: IP Test Packet

To satisfy the different needs, the test packet includes a data area that is typically padded according to the length required in the measure.

The SUB-IP encapsulation and the IP headers suite of the packet define the type-P of the test packet.

3.1.1.5 Format

The IP measurement signature is inserted at the end of the packet.

The signature is composed of fields that are described below.

Figure 3-3: Signature Fields

The ID permits to distinguish measurement packets among regular packets. The last field of the IMS is the IMS identifier (ID).

The version field, named 'Ver', offers the capability to define up to three versions of signature. By now, only the version 1 is defined. The value 0 of the version field is reserved.

The field type values are:

- type=0: Basic IMS
- type=1: Interdomain IMS
- type=2: RoundtripDelay IMS
- type=3: Interdomain RoundtripDelay IMS
- type=4: Checksum IMS

A lot of metrics computation relies on the analysis of the order of the packets. The IMS includes a sequence number (SN).

Manufacturers may insert proprietary extension at the beginning of the IMS while preserving measurement interoperability. The field 'Ext' indicates the number of blocks of 8 bytes, which carried proprietary data.

Points of measure will need the ability to populate and read the transmit timestamp field. The transmit timestamp field must be consistent with the time the packet is inserted on the network.

3.1.1.5.1 Inter-domain measure identification

To permit the management of the measurement results, the IMS carries a field that identifies the owner, named 'ownerID', and a field that carries the measurement identifier, named 'measureID'

chosen by the owner. That permits the results of the measure to be collected and shared. This framework is defined in the IPPM-REPORTING-MIB.

3.1.1.5.2 Specific information

Points of measure may insert specific information at the beginning of the IMS while preserving measurement interoperability.

3.1.2 Security

To avoid the measurements systems to be used to make attacks, there is a strong requirement to propose a security mechanism to control the access to the set-up of the network measurements.

From the network security point of view, the main security hole in a network measure is the control test packet. The standardization of a packet signature does not facilitate the control of a probe to perform a DOS attack.

4. SNMP OVER TCP

ITU is standardizing a SNMP over TCP transport mapping [SNMPoverTCP].

It allows SNMP messages to be transferred on a well-known connection-oriented transport protocol TCP.

5. SECURITY REVIEW

Bearing in mind that foundations of IPv6 are already defined, the role of ITU-T is to extend to IPv6 protocol for a utilization of IPv6 in telecommunication networks. The ITU capitalizes on the activities and on the experience achieved by standardization bodies and forums specialized in IP. So there is no security aspect that applies directly to this document.

6. SUMMARY AND CONCLUSIONS

Complementing the work being carried-on inside other standard bodies, ITU-T is focusing on IP services. Mainly two Study Groups are working on this subject:

- SG 13 (Multi-protocol and IP-based networks and their internetworking).
- SG 4 (Telecommunication management, including TMN).

The capability of measuring the quality of service of IPv6 based networks and services has been recognized as a major item for network operators. The key result provided by ITU-T on this subject is the standardizing (ITU-T Recommendation O.iptest) of a test packet format usable on both IPv4 and IPv6.

The 6QM project should use the format in its measurement system to demonstrate that QoS troubleshooting is feasible between IPv4 and IPv6 networks. That will help to convince the community that IPv6 is ready for deploying inter-domain SLA while preserving IPv4 interoperability. The use of SNMP over TCP may provide a secure inter-domain configuration interface.

7. REFERENCES

Here after is a list of Recommendations available from ITU-T.

Name	Title	date
E.651	Reference connections for traffic engineering of IP access networks	(03/2000)
M.2301	Performance objectives and procedures for provisioning and maintenance of IP-based networks	(07/2002)
O.iptest	Test and measurement equipment to perform tests at the IP layer	*Draft*
SNMPoverTCP	A proposed SNMP over TCP Transport Mapping for using in TNM	*Draft*
Y.100	General overview of the Global Information Infrastructure standards development	(06/1998)
Y.101	Global Information Infrastructure terminology: Terms and definitions	(03/2000)
Y.110	Global Information Infrastructure principles and framework architecture	(06/1998)
Y.120 Annex A Cor. 1	Global Information Infrastructure scenario methodology Examples of use	(06/1998) (02/1999) (11/2000)
Y.130	Information communication architecture	(03/2000)
Y.140	Global Information Infrastructure (GII) – Reference points for interconnection framework	(11/2000)
Y.800	Performance framework for the GII	*Draft*
I.351/Y.801/Y.1501	Relationships among ISDN, Internet Protocol, and GII performance recommendations	(10/2000)
Y.1001	IP Framework – A framework for convergence of telecommunications network and IP network technologies	(11/2000)
Y.1221	Traffic control and congestion control in IP-based networks	*Draft*
Y.1231	IP access network architecture	(11/2000)
Y.1241	Support of IP-based services using IP transfer capabilities	(02/2001)
Y.1310	Transport of IP over ATM in public networks	(03/2000)
Y.1311	Network-based VPNs - Generic architecture and service requirements	(consent 02/2002)
Y.1401	General requirements for interworking with Internet Protocol (IP)-based networks	(10/2000)

Y.1402/X.371	General arrangements for interworking between Public Data Networks and the Internet	(02/2001)
I.351/Y.801/Y.1501	Relationships among ISDN, Internet Protocol, and GII performance Recommendations	(10/2000)
Y.1530	Call processing performance for voice service interworking in ISDN and IP networks	*Draft*
Y.1540	Internet Protocol data communication service – IP packet transfer and availability performance parameters	(02/1999)
Y.1541	Network performance objectives for IP-based services	(consent 02/2002)
G.7710/Y.1701	Common equipment management requirements	(11/2001)
G.7712/Y.1703	Architecture and specification of Data Communication Network (DCN)	(11/2001)
G.7713/Y.1704	Distributed call and connection management	(12/2001)
G.7714/Y.1705	Generalized automatic discovery	(11/2001)
Y.1710 Cor. 1	Requirements for OAM functionality for MPLS networks	(07/2001) (consent 02/2002)
Y.1711	OAM mechanism for MPLS networks	(consent 02/2002)