International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

O.211

(01/2006)

SERIES O: SPECIFICATIONS OF MEASURING EQUIPMENT

Equipment to perform measurements on IP networks

Test and measurement equipment to perform tests at the IP layer

ITU-T Recommendation O.211

ITU-T O-SERIES RECOMMENDATIONS

SPECIFICATIONS OF MEASURING EQUIPMENT

General	O.1–O.9
Maintenance access	O.10–O.19
Automatic and semi-automatic measuring systems	O.20–O.39
Equipment for the measurement of analogue parameters	O.40–O.129
Equipment for the measurement of digital and analogue/digital parameters	O.130–O.199
Equipment for the measurement of optical channel parameters	O.200–O.209
Equipment to perform measurements on IP networks	**O.210–O.219**

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

ITU-T Recommendation O.211

Test and measurement equipment to perform tests at the IP layer

Summary

This Recommendation specifies an IP performance measurement signature (IPPMS) and test packets which may be used to measure the performance and the availability of IP network services across administrative areas, composite networks and among heterogeneous devices. The IPPMS may be used to support provisioning and maintenance of IPv4 as well as IPv6 networks.

Source

ITU-T Recommendation O.211 was approved on 13 January 2006 by ITU-T Study Group 4 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

Active measurement, network performance.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

CONTENTS

		Page
1	Scope	1
2	References	1
3	Definitions	2
4	Abbreviations	3
5	State of the art considerations	5
5.1	ICMP PING & Traceroute	5
5.2	Existing active measurement solutions	5
6	Requirements and benefits of a standard IP test packet	5
6.1	General requirements	5
6.2	Benefits of standardizing an IP test packet	6
6.3	Interoperability	6
6.4	IP multicast and mobility	6
6.5	IPv4 and IPv6 coexistence	6
6.6	Transport protocol	7
6.7	Representative test packet	7
6.8	Relationship with other organizations or forums	8
6.9	Metrics and parameters	8
7	IP performance measurement packet framework	9
7.1	Discussion on the IPPMS location within the test packet	10
8	IP performance measurement signature (IPPMS) specification	13
8.1	IP test packet size	14
8.2	Measurement interval	14
8.3	IP performance measurement signature (IPPMS)	14
8.4	Detailed IPPMS format	15
9	IP measurement packets for IPv4 and IPv6 levels	19
9.1	IPPMS options	20
9.2	Payload size of 32 bytes (with IPPMS only)	20
9.3	Payload size of 52 bytes	20
9.4	Payload size of 132 bytes	20
9.5	Payload size of 164 bytes	21
9.6	Payload size of 564 bytes	21
9.7	Payload size of 1464 bytes	21
10	Security	21
BIBLIOGRAPHY		22

ITU-T Recommendation O.211

Test and measurement equipment to perform tests at the IP layer

1 Scope

In order to support provisioning and maintenance of IP-based networks, a common standard IP test packet format is desirable such that *interoperability* between test equipment and comparison of measurement results can be achieved. In order to measure the performance of IPv4 and IPv6 networks and services for different Type-P, there is a need for interoperability among heterogeneous manufacturer equipment in order to perform measurements of ITU-T Recs Y.1540 [4] and M.2301 [1] parameters (IPER, IPLR, IPTD, IPDV, IPSLB, IPRR) across administrative domains or composite networks. The packet format should facilitate not only the achievement of measurements between operator domains, but also the identification of the test manager who is in control of the measurement.

This is analogous to previous requirements at the PDH/SDH (layer 1) and ATM (layer 2) network layers specified in ITU-T Recs O.181 [2] and O.191 [3]. The test packet must contain appropriate information needed to measure the main network performance parameters specified in ITU-T Recs Y.1540 [4] and M.2301 [1].

This Recommendation deals with the performance measurement of IP network services.

Measurement techniques should also support the metrics specified by ITU-T Study Groups 2, 4, 9, 12, 13, 15 and 16, ATIS T1A1, ETSI TIPHON, EURESCOM, 3GPP and the IETF.

The aim of this Recommendation is to standardize a common IP performance signature named IPPMS and test packets in order to measure the performance and the availability of IP network services across administrative areas, composite networks and among heterogeneous devices. The IP-layer supports many different IP-based services which may have different performance requirements, therefore the test packets must be, as far as possible, *representative* of *the services* being carried by the IPv4 and/or IPv6 layer for service turn-up tests, maintenance, troubleshooting and SLA monitoring.

It is not in the scope of this Recommendation to specify the way in which the measures are activated or torn down, nor to define how measurements' results are managed. Nevertheless, the measurement signature should give room to identify a measure and its initiator.

2 References

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

[1] ITU-T Recommendation M.2301 (2002), *Performance objectives and procedures for provisioning and maintenance of IP-based networks*.

[2] ITU-T Recommendation O.181 (2002), *Equipment to assess error performance on STM-N interfaces*.

[3] ITU-T Recommendation O.191 (2000), *Equipment to measure the cell transfer performance of ATM connections*.

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

[5] ITU-T Recommendation Y.1541 (2006), *Network performance objectives for IP-based services*.

[6] ITU-T Recommendation Y.1241 (2001), *Support of IP-based services using IP transfer capabilities*.

[7] ITU-T Recommendation I.353 (1996), *Reference events for defining ISDN and B-ISDN performance parameters*.

[8] ITU-T Recommendation G.7041/Y.1303 (2005), *Generic framing procedure (GFP)*.

[9] ITU-T Recommendation M.1400 (2004), *Designations for interconnections among operators' networks*.

[10] IETF RFC 4148 (2005), *IP Performance Metrics (IPPM) Metrics Registry*.

[11] ISO 3166-1:1997, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*.

3 Definitions

The following definitions are taken from ITU-T Rec. Y.1241 [6]:

3.1 IP-based service: An IP-based service is defined as a service provided by the service plane to an end user (e.g., a host (end system) or a network element) and which utilizes the IP transfer capabilities and associated control and management functions, for delivery of the user information specified by the service level agreements.

3.2 IP network service: An IP network service is defined as a data transmission service in which the data passed across the interface between the user and provider is transferred in the form of IP (Internet protocol) packets (sometimes called datagrams). IP network service includes the service provided by using the IP transfer capabilities.

3.3 IP transfer capability: IP transfer capability is defined as the set of network capabilities provided by the IP layer. It may be characterized by the traffic contract as well as performance attributes supported by control and management functions of the underlying protocol layers.

ITU-T Rec. Y.1540 [4] defines end-to-end IP-service and measurement point (MP) as follows:

3.4 end-to-end IP service: For the purpose of this Recommendation, end-to-end IP service refers to the transfer of user-generated IP datagrams (referred to in this Recommendation as IP packets) between two end hosts as specified by their complete IP addresses.

3.5 measurement point (MP): The boundary between a host and an adjacent link at which performance reference events can be observed and measured. Consistent with ITU-T Rec. I.353 [7], the standard Internet protocols can be observed at IP measurement points. ITU-T Rec. I.353 provides more information about MPs for digital services.

3.6 Type-P: RFC 2330 defines a performance measurement framework. It introduces the notion of type of packet, the Type-P. It corresponds to the suite of protocols present in the IP and SUB-IP headers of the packet. A Type-P is represented as a list of protocol identifier names. Protocol identifiers' names for IP are defined in RFC 2896. Specific protocol identifiers' names for IPv6 are defined in RFC 3919. As an example, the Type-P ip.udp.snmp differs from the Type-P ip.ip6.udp.snmp because the latter is not only an SNMP packet over IPv6 but is also an IPv6 packet encapsulated over IP. This definition is only used in this Recommendation to give clear encapsulation examples.

3.7 IP performance measurement signature (IPPMS): An IP test packet is a regular IP packet that contains a standardized block of fields needed to perform the measurement. This block of fields is named IP performance measurement signature (IPPMS).

4 Abbreviations

This Recommendation uses the following abbreviations:

3GPP	Third Generation Partnership Project
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CAC	Connection Admission Control
CIF	Controller Identifier Format
CRC	Cyclic Redundancy Check
CRC32	32-bit Cyclic Redundancy Check
DiffServ	Differentiated Service
DoS	Denial of Service
DSCP	Differentiated Service Code Point
DST	Destination
ETSI	European Telecommunications Standards Institute
EURESCOM	European Institute for Research and Strategic Studies in Telecommunications
FR	Frame Relay
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identifier
IETF	Internet Engineering Task Force
IntServ	Integrated Service
IP	Internet Protocol
IPDR	IP Packet Discard Rate
IPDV	IP Packet Delay Variation
IPER	IP Packet Error Ratio
IPLR	IP Packet Loss Ratio
IPOD	IP Operator Domain
IPPM	IP Performance Metrics
IPPMS	IP Performance Measurement Signature
IPRR	IP Packet Reordering Ratio
IPRTD	IP Packet Round Trip Delay
IPSLBR	IP Packet Severe Loss Block Ratio

IPTD	IP Packet Transfer Delay
IPv4	IP version 4
IPv6	IP version 6
LL	Lower Layers
MIB	Management Information Base
MP	Measurement Point
MPEG	Moving Picture Experts Group
MTTR	Mean Time To Restore
NAT	Network Address Translation
NTP	Network Termination Point
OBGR	Operator Border Gateway Router
PAM	Passive and Active Measurement
PAT	Protocol Address Translation
PDH	Plesiochronous Digital Hierarchy
PDU	Protocol Data Unit
PING	Packet Internetwork (Internet) Grouper
PPP	Point-to-Point Protocol
QoS	Quality of Service
RMON	Remote Network Monitoring
RTP	Real Time Transport Protocol
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SLA	Service Level Agreement
SN	Sequence Number
SRC	Source
STM-N	Synchronous Transport Module, level N
SUB-IP	Sub IP Layer
TCP	Transmission Control Protocol
TIPHON	Telecommunications and Internet Protocol Harmonization Over Networks
TSC	Timestamp Control
TSF	Timestamp Format
Tx	Transmitter
UDP	User Datagram Protocol
VoIP	Voice over IP

5 State of the art considerations

5.1 ICMP PING & Traceroute

Using simple methods such as ICMP PING or Traceroute can only measure IP round trip delay (IPRTD), and one-way delay is, of course, not exactly 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.

5.2 Existing active measurement solutions

Existing systems of performance measurement of IP networks and services do not interoperate among heterogeneous manufacturers, but they share the same semantic and methods. The test packet is built on top of a regular IP packet. The suite of protocols present in the IP header describes the Type-P of the packet. Pieces of information dedicated to performance measurement are inserted in the packet.

Measurement packets differ by the field meanings, field orders, field names, field units, field sizes, and the location of the test information in the data of the packet. Common fields are the following:

– the device that has sent the packet;

– the interface that has sent the packet;

– the identifier of the stream the packet belongs to;

– the absolute timestamp corresponding to the time the packet is sent;

– the sequence number of the packet; and

– a checksum or a CRC computed on the previous fields or on the whole IP packet.

Existing implementations insert the test information either at the beginning or at the end of the SDU of the IP test packet.

This Recommendation covers these two designs.

6 Requirements and benefits of a standard IP test packet

This Recommendation specifies an IP test packet format to be used when doing network provisioning and maintenance tests in order to verify the IP-transfer performance requirements of IP-based services by measuring the IP metrics defined in ITU-T Recs Y.1540 [4] and M.2301 [1].

This clause discusses general requirements and benefits of a standard test packet.

6.1 General requirements

ITU-T Rec. M.2301 [1] presents two basic measurement approaches – intrusive and non-intrusive.

Intrusive measurements use IP test packet streams to create IP flows on the path to be tested. These test packets are interleaved with the normal traffic flows between two measurement points (MPs), or transmitted as a continuous stream of pseudo-customer traffic.

Non-intrusive measurements use one of two methods:

– Monitoring and collecting of MIB data from network elements such as routers for performance assessment and maintenance;

– Measuring the network performance for customer IP packets.

Non-intrusive measurements monitor not only customer IP packets, they also monitor IP test packets as regular IP traffic. Therefore, a passive and active measurement approach, named PAM, exits. This might be thought of as a "mixed mode" where the test packets are inserted intrusively, but they are monitored non-intrusively. As an example, non-intrusive probes attached at key MPs in the network such as gateway routers may monitor the test packets to measure inter-domain performance.

To measure the quality of service, it is important to have operational interoperability among heterogeneous manufacturers and to perform one-way delay and one-way packet loss measurement across administrative areas or over composite networks for different Type-P packets.

Consequently, this Recommendation considers two main points:

– When doing network provisioning and service turn-up tests, it is crucial to use an IP test packet stream that simulates the kinds of application services to be supported.

– IP data are never carried directly over IP. User traffic is carried mainly on top of UDP or TCP, but not exclusively.

6.2 Benefits of standardizing an IP test packet

Standardizing an IP test packet has a number of advantages, including the following:

– IP-based services can be provisioned and activated consistently, and QoS established against negotiated SLAs;

– network performance and QoS can be monitored consistently, and measurement results compared against SLAs and correlated between different MPs and instruments;

– interoperability between instruments of different manufacturers can be evaluated;

– interoperability of measurement between administrative domains and over composite networks can be evaluated.

6.3 Interoperability

The definition of the IP test packet must offer interoperability among heterogeneous manufacturers in order to perform metric measurements across administrative areas and among composite networks.

Currently, in a test involving heterogeneous equipment and/or administrative areas, the identifier of the measurement set by the source (essentially, the identification of the source) has no meaning for the sink.

To gain interoperability, the IP test packet must carry information to unambiguously identify the controller of the measure.

6.4 IP multicast and mobility

The definition of the IP test packet must consider the measurement of the performance of multicast services, mobile IP services.

6.5 IPv4 and IPv6 coexistence

To permit end-to-end measurement, the test packet must not depend on either IPv4 or IPv6.

The protocol translation mechanisms between, IPv4 and IPv6 and the coexistence of, IPv4 and IPv6 are potential sources of non-interoperability of the measurements.

Whenever possible the test packet should not be rejected by IPv6/IPv4 translation or transition mechanisms.

6.6 Transport protocol

Figure 1 shows a layered model of performance for IP Service which includes UDP and TCP described initially in ITU-T Rec. Y.1540 [4].

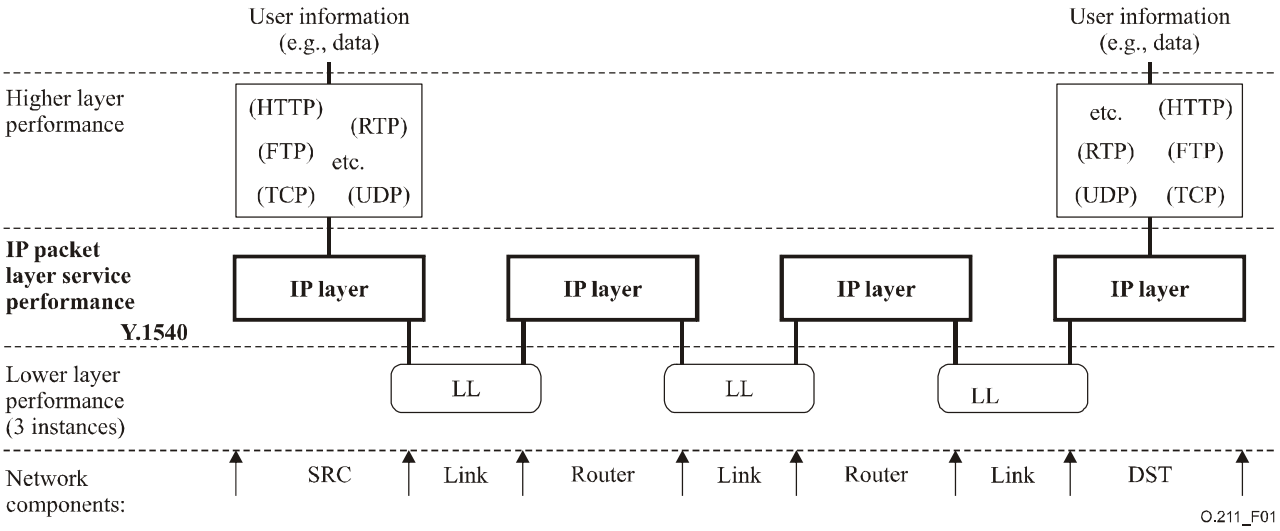

Figure 1/O.211 – Y.1540 layered model of performance for IP service – Example

IP data are rarely carried directly on top of IP. Currently, user information is carried mainly on top of UDP or TCP. Consequently, the test packet must permit the measure of the performance of UDP and TCP streams.

But user information is not carried only over UDP or TCP. There are currently 46 protocols defined to be encapsulated directly over IP. Ideally, the test packet definition should permit the measurement of the performance of IP-based networks and services relying on these protocols.

It is not in the scope of this Recommendation to identify for which of these protocols the performance should be measured. Moreover, this Recommendation takes account of the fact that new protocols will be defined in the future.

Consequently, this Recommendation provides flexible test packet structure to measure the performance of any protocol encapsulated directly on the top of IPv4 or IPv6.

6.7 Representative test packet

To be representative of an IP service an IP test packet stream must often respect the encapsulation of that service.

Most professional applications, so accessed from the office, are available through a NAT/PAT or a firewall. Most of them run on the top of TCP, but not exclusively:

The test packets should cross the NAT/PAT and the firewall in the same manner as the packets of the IP services.

QoS is normally ensured using CAC mechanisms that set up the DiffServ code point in the header of each IP packet. Routers prioritize packets according to their code point values:

– The CAC should classify the test packet with the same code point as that of the service the test packet is intended to measure the performance of.

As IP-based services are not encapsulated directly on IP, it does not make sense to define an IP test packet at raw IP level.

6.8 Relationship with other organizations or forums

The aim of this Recommendation is to increase operational interoperability. This consists of promoting the need to share the same measurement packets between various organizations and forums and in reusing existing standards.

6.9 Metrics and parameters

ITU-T Recs Y.1540 [4] and M.2301 [1] define performance metrics and performance objectives for IP-based networks.

Clause 6/M.2301 [1] presents the measurement methods and identifies the metrics which may be measured using test packets. Table 1 updates this mapping.

Table 1/O.211 – Intrusive and non-intrusive measurement of performance parameters

Parameter	Intrusive	Non-intrusive
IPTD	√	(Note)
IPDV	√	(Note)
IPER	√	√
IPLR	√	√
IPDR		√
NOTE – IPTD and IPDV may be computed with non-intrusive measurement. As an example, the same packet is detected and timestamped in two places, then this information is collected to compute the difference of time. Documents of the IETF packet sampling working group describe such techniques.		

6.9.1 IP packet transfer delay (IPTD)

IPTD is a primary metric defined in 6.2/Y.1540 [4].

Delay performance measurements are carried out between MPs. The test consists of sending a stream of time-stamped packets, distributed throughout the traffic, from one end to the other. The time each packet is received is recorded.

The time each packet was transmitted is subtracted from the received time to produce the one-way IPTD result for that packet.

Consequently, the IPPMS should have an absolute timestamp field.

6.9.2 IP packet delay variation (IPDV)

ITU-T Rec. Y.1540 [4] gives several definitions of IP packet delay variation. Appendix II/Y.1541 [5] clearly defines IPDV as the inter-packet delay variation. It uses the same definition as RFC 3393.

For IPDV, the smaller IPTD figure is subtracted from the greater during the measurement interval to produce the delay variation.

In order to calculate the error limits of the IPDV measurement the sender of the IPPMS should have a field to carry the accuracy of the clock of the sender.

6.9.3 IP packet error ratio (IPER)

IPER is a secondary metric defined in 6.3/Y.1540 [4].

Error performance measurements are carried out between MPs. The test consists of sending a stream of numbered packets, distributed throughout the traffic, from one end to the other. Each test

packet contains error-checking bits. At the receiving end the packets are checked for errors and to see if any are missing.

For IPER, the total number of errored packets is recorded, together with the total number of packets received. The ratio between the two figures is the IPER.

The test packet should carry information that may be used to detect bit errors in the packet when its performance measurement is carried out at the IP level or at the SUB IP level.

6.9.4 IP packet loss ratio (IPLR)

IPLR is a secondary metric defined in 6.4/Y.1540 [4].

For IPLR, the missing packets are recorded, together with the total number of packets sent. The ratio between the two figures is the IPLR.

Consequently the IPPMS should have one field to number the packets in the test packet stream.

6.9.5 IP packet severe loss block ratio (IPSLBR)

IPSLBR is a secondary metric defined in 6.6/Y.1540 [4].

IPSLBR requires long observation periods. As they may be performed on high speed links they require a large sequence number to identify sequences of test packets. Consequently, the sequence number of the IPPMS should be 32 or 64 bits long.

6.9.6 IP packet reordering ratio (IPRR)

IPRR is defined in Appendix VII/Y.1540 [4].

An out-of-order or reordered packet occurs when the packet has a sequence number lower than expected and therefore the packet has been reordered.

Consequently, the packet sequence number of the definition should be long enough to count a long sequence of test packets. A length of 32 or 64 bits is appropriate.

6.9.7 Unavailability

ITU-T Rec. Y.1540 defines the criteria for declaring unavailability periods. The IP service is defined as unavailable on an end-to-end basis if the IPLR is greater or equal to 75% during an evaluation interval of 5 minutes. These values should be considered as provisional.

The timestamp field should be long enough to store 5 minutes of time.

6.9.8 IP packet routing consideration

Appendix I/Y.1540 introduces the need for measuring the influence of IP routing on IP performance.

As BGP convergence duration is close to 30 seconds, a 64-bit long timestamp field is appropriate.

6.9.9 Packet detection

The IPPMS should provide means to support the detection of test packets in the intermediary nodes crossed by the stream of test packets.

7 IP performance measurement packet framework

The aim of this Recommendation is to standardize a packet signature which may be used to measure the performance and the availability of IPv4 and IPv6 networks and services across administrative areas, composite networks and among heterogeneous devices.

In doing this, the first step consists of defining a common information block, the IPPMS.

The second step consists of specifying test packets according to the requirements and the constraints. The main constraint is the location of the IPPMS within the test packet.

The recommended framework for defining test packets is as follows:

– take into account current measurement best practices;

– specify a format that permits interoperability between the measurement plane of different manufacturers' measurement systems;

– specify a format that gives room to identify measurement controller to facilitate measurement systems dialog and measure management in the future;

– specify a format that permits the measurement of ITU-T performance parameters based on the IP performance metrics defined in RFC 4148 [10];

– specify a format that permits the measurement of the performance of IP protocols defined in the future;

– specify a test packet compatible with IPv4, IPv6 and with both versions coexisting;

– specify a test packet format similar to packets sent by real IP applications;

– specify a test packet format that may be recognized and processed at high speed;

– specify a test packet that permits manufacturers to include specific information while preserving interoperability.

7.1 Discussion on the IPPMS location within the test packet

The IPPMS is designed to be inserted either at the beginning or the end of the packet as presented in Figure 2.

IP	Encaps 1	Encaps2...	Data	IPPMS extensions	IPPMS
Header suite: variable length			Variable length	Variable length	Fixed length

a) IPPMS after the IP SDU

IP	Encaps 1	Encaps2...	IPPMS	IPPMS extensions	Data	Trailer (if any)
Header suite: variable length			Fixed length	Variable length	Variable length	Variable Length

b) IPPMS before the application SDU

Figure 2/O.211 – IP test packet format options

When the test information is inserted at the beginning of the Type-P data unit, senders and receivers must agree on the Type-P before the measurement.

When the test information is inserted at the end of the IP packet, its location does not depend on the Type-P, provided this Type-P PDU does not have any trailer. Consequently, senders, intermediary nodes and receivers do not need to agree on the Type-P before the measurement.

Example:

In the following example we consider an RTP test packet, where its Type-P is IP.UDP.RTP.

IPPMS at the beginning of the Type-P SDU

The sender sends the test packet IP.UDP.RTP.IPPMS.data and, as the receiver has only UDP level analysing capabilities, the receiver will look for the IPPMS at the beginning of the UDP SDU instead of at the beginning of the RTP SDU and consequently, it will not recognize the packet as a valid test packet.

IPPMS at the end of the IP packet

The sender sends the test packet IP.UDP.RTP.data.IPPMS and, as the receiver will look for the IPPMS at the end of the IP SDU, it will recognize the IPPMS.

7.1.1 IPPMS at the end of the IP SDU

Inserting the IPPMS at the end of the IP packet has many advantages.

One advantage is that the test packet specification does not depend on any protocol on top of IP. Consequently, it is potentially representative of any application packet.

The proposed IP test packet presented in Figure 3, consists of:

– IP protocols headers suite (e.g., ip.udp.snmp, ip6.tcp.http, etc.);

– a data block;

– an IPPMS.

7.1.2 IPPMS at the beginning of the application SDU

The application level determines the IP encapsulation and consequently the location of the IPPMS in the packet. Inserting the IPPMS at the beginning of an application SDU of the packet requires fixing of the encapsulation or parsing of each packet header.

Most user data are carried on top of UDP or TCP.

7.1.2.1 Position of the IPPMS field

The IPPMS field is located directly after the application header in the IP test packet. Since the header length is known for a given type of measurement point, it is easy to find the start of the IPPMS field.

Other advantages of locating the IPPMS directly after the header are:

– automatic 32-bit alignment simplifies parallel processing;

– simple extension of the standard IPPMS field by attaching proprietary information elements.

7.1.2.2 Relation between Type-P and QoS mechanisms at the IP layer

Service-specific requirements (e.g., priorities, max. delay, etc.) are handled by mapping specific end-to-end applications into different QoS classes or by reserving network resources exclusively for these applications.

The IP routers may implement different QoS mechanisms such as IntServ or DiffServ where different forwarding rules are applied to individual flows (IntServ) or packets are assigned to certain QoS classes (DiffServ).

IntServ forwarding decisions are based on the destination IP address and port number.

Diffserv forwarding decisions are based on the value of the DSCP field in the IP header. The value of the DSCP field is set by the CAC of an ingress router of the path. This value is obtained by analysing the packet header.

7.1.2.3 Representing higher layer services at the IP layer

The only application-specific parameters besides IP address, protocol number, port number and DSCP that are visible at the IP layer are the packet length and the traffic pattern.

Therefore, the IP test packet should have a variable length data field following the IPPMS.

7.1.2.4 Fixed header structure

The simplest test packet that contains all the information listed above, has a fixed header format consisting of the standard IP header followed by the UDP header.

This is in line with other activities dealing with active measurements in frame-based networks (see ITU-T Recs M.2301 [1], O.181 [2] and O.191 [3]).

7.1.3 Raw IP packet

IETF does not recommend sending raw IP packets, therefore this Recommendation proposes the use of UDP as the default Type-P of the test packet.

7.1.4 UDP test packet

Applications sending datagrams to a host need to identify a target that is more specific than the IP address since datagrams are normally directed to certain processes and not to the system as a whole.

UDP simply serves as a multiplexer/demultiplexer for sending and receiving datagrams, using ports to direct the datagrams.

The IP/UDP test packet has a unique format characterized by:

– a fixed header structure for the IP test packet;

– a fixed position of the IP performance measurement signature (IPPMS) directly after the UDP header.

This packet format allows measurement of end-to-end IP service performance as defined in ITU-T Rec. Y.1540 [4].

7.1.5 TCP

Performance tests above the IP layer, such as TCP connection performance (see ITU-T Rec. Y.1540 [4]) may require more information elements in the test frame.

This clause will be extended in the future.

7.1.6 Test packet with only the IPPMS in the Type-P payload

Inserting a measurement block either at the beginning or the end of the Type-P SDU differs only by the location of the IPPMS within the packet.

When there is no data in the SDU, the IPPMS is located both at the beginning and at the end of the test packet. This is illustrated by Figure 3.

This case permits interoperability between the two modes of encapsulation.

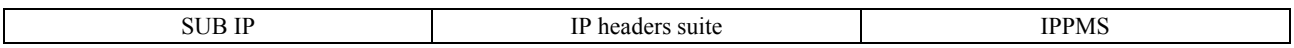

Figure 3/O.211 – Common test packet format

7.1.7 Usages summary

Table 2 shows the various possibilities for the IPPMS location in the test packet and their influence on interoperability and packet size.

Table 2/O.211 – IPPMS location

IPPMS location	Interoperability	Packet size
1) At the end of the payload	No need to analyse the complete header suite	Any
2) At the beginning of the payload	Requires parsing of the header suite. May require the knowledge of the header structure.	Any
3) IPPMS = Payload	With 1 and 2	Packet size different from application packet size Small packet size only

7.1.8 Generalization to class of service performance measurement

The measurement of IP performance may require the presence of transport or application encapsulation to ensure that test packets are treated the same way as regular application packets.

To measure the performance of an application relying on a specific protocol it is recommended to use the format defined in 7.1.6.

As an example, Figure 4 presents an RTP test packet.

Figure 4/O.211 – Example RTP test packet format

Recommendations which need to define test packets for measuring the performance of network applications may use this framework.

NOTE – Some protocol encapsulations require a trailer. In this case, it may be necessary to analyse the trailer and the header to localize the IPPMS.

7.1.9 Other potential usages for the IPPMS

The IPPMS specifies an information block for measuring network performance and availability. Consequently, it may be used for measuring the performance of frame-based networks. In this case, the IPPMS may be inserted directly in a raw frame without any IP header.

8 IP performance measurement signature (IPPMS) specification

The following clauses define an IP test packet format including frame format and payload considerations. This can be used for intrusive measurements of IP network performance to support QoS 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. A tester needs SUB IP connectivity to be able to send or receive IP test traffic to measure IP network performance and QoS. This could include a variety of link layer formats including PPP, FR, ATM, Ethernet etc. Moreover, the tester has to enable each IP service prior to measuring its performance.

The Type-P of a test packet is defined by the SUB-IP encapsulation and the IP headers suite of the packet.

8.1 IP test packet size

The maximum size for an IP packet is 65 535 bytes, with a common default size of 570 bytes. Every packet consists of a suite of headers and payload information. The size of IP header suites depends on the version of IP and depends on the application encapsulated. The packetization and processing delay increase with the size of the packet, which is one of the factors affecting QoS applications.

Packet size influences the results for most IP performance parameters. A range of packet sizes may be appropriate since many flows have considerable variation in the size of the packets. For example, VoIP uses short packets and video over IP uses much longer packets. 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. According to the definition of IPTD in ITU-T Rec. Y.1540 [4], packet insertion time is included in the IPTD performance objectives. ITU-T Rec. Y.1541 [5] suggests information fields of either 160 octets or 1500 octets, but whatever field size is used must be reported. Also, an information field of 1500 octets is recommended for estimation of IP performance parameters when using lower layer tests, such as bit error measurements. It is suggested that IP test packets of fixed lengths 80, 160, 200, 600 and 1500 bytes be available as a minimum capability in order to simulate VoIP, video and MPEG video traffic.

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

8.2 Measurement interval

ITU-T Recs Y.1541 [5] and M.2301 [1] specify IP performance in terms of the upper bound of each parameter. ITU-T Rec. Y.1541 [5] suggests an evaluation interval of 1 minute for IPTD, IPDV, IPER and IPLR. ITU-T Rec. Y.1540 [4] suggests a measurement period of 5 minutes for availability metrics measurements. Existing ITU-T Recommendations and operations procedures measure performance over periods of 15 minutes, 24 hours, 7 days or 1 month.

To take into account the constraints of metrics measurement, the IPPMS timestamp permits two different usages:

– Firstly, it permits absolute timestamping for end-to-end network and service performance measurement across different kinds of equipment.
– Secondly, it permits relative timestamping for link performance measurement.

8.3 IP performance measurement signature (IPPMS)

The IPPMS is 32 bytes long.

It is the combination of the following information elements:

– an IP performance measurement signature control (IPPMS Control);
– a field to identify metrics to measure (Metric_ID);
– a field reserved for future usage (Reserved);
– a sequence number (Seq_Number);
– a transmit timestamp information element (Tx_Timestamp);
– a controller identifier (Controller_ID);
– an identifier of a flow of test packets (Flow_ID);
– an IPPMS protection field (CRC32).

To guarantee the maximum interoperability it is mandatory to only have one format of the test packet signature and a minimum number of options.

The following is a proposal of a test packet signature. It integrates all the requirements and has a constant size of 32 bytes. Table 3 gives the list of the fields of the IPPMS.

Table 3/O.211 – IPPMS Information elements

Information elements	Size (Bytes)
Control	2
Metric_ID	1
Reserved	1
Seq_Number	4
Tx_Timestamp	8
Controller_ID	10
Flow_ID	2
CRC32	4

This gives a common IPPMS format, as illustrated in Figure 5.

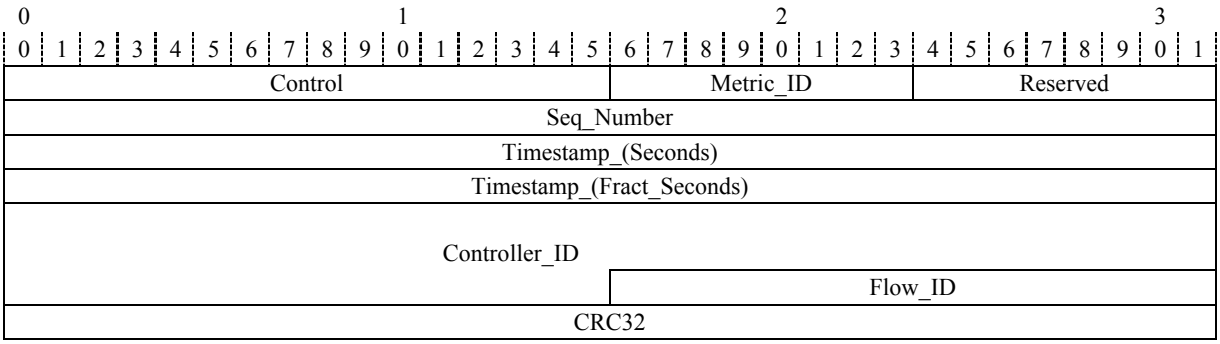

Figure 5/O.211 – IPPMS format

8.4 Detailed IPPMS format

8.4.1 IPPMS control field (Control)

The IPPMS control field is 2 bytes long. It is made of 6 fields:

– the timestamp format (TSF);
– the timestamp control of the clock which sent the packet (TSC);
– the extension presence (Ext);
– the version of the IPPMS (Ver);
– the controller identifier format (CIF);
– a reserved field.

Table 4 gives the sizes of each field.

Table 4/O.211 – IPPMS header format

Fields	Size (Bits)
Timestamp format (TSF)	1
Timestamp control (TSC)	3
Extension presence (Ext)	1
Version (Ver)	2
Controller identifier format (CIF)	3
Reserved	6

8.4.1.1 Timestamp format (TSF)

This field indicates if the time reference of the timestamp is absolute or not.

"0" means that no absolute timestamp is used.

"1" means that an absolute timestamp is used.

8.4.1.2 Timestamp control (TSC)

This field carries the accuracy of the clock of the sender. The possible values are listed in Table 5.

Table 5/O.211 – Timestamp control

TSC	Value	Meaning: The accuracy of the clock is better than:
000	0	Value 0 means that at the time the packet was sent, the source was not synchronized to an absolute time reference
001	1	10 ns
010	2	50 ns
011	3	500 ns
100	4	10 µs
101	5	50 µs
110	6	500 µs
111	7	≤10 ms

8.4.1.3 Extension presence (Ext)

This field is 1 bit long.

Points of measure may insert proprietary data in the test packet while preserving measurement interoperability. The field 'Ext' indicates the presence of such information.

A value of 0 means there is no extension (default).

A value of 1 means there is an extension.

To perform IPER measurement the extension should be protected using a CRC32.

8.4.1.4 IPPMS version (Ver)

This field is 2 bits long.

The version field, named 'Ver', offers the capability to define up to four IPPMS versions.

Currently, 'Ver' has the value 0.

8.4.1.5 Controller identifier format (CIF)

This field is 3 bits long.

It identifies the current type of controller. Table 6 lists the different values.

Table 6/O.211 – Controller identifier format

CIF	Value	Meaning: Current controller value carries:
000	0	Reserved
001	1	An operator code
010	2	An enterprise number
011	3	The IPv4 address, the protocol type and the port of the controller
100	4	The first 10 bytes of an IPv6 address of the controller
101	5	The last 6 bytes of an IPv6 address, the protocol type and the port of the controller
110	6	Proprietary
111	7	Reserved

8.4.2 Metric identifier (Metric_ID)

RFC 4148 [10] defines an initial registry of the "IP performance metrics (IPPM) Metrics Registry". It is an extensible registry maintained by IANA which assigns each metric defined by the IETF IPPM WG with an identification number.

Metric_ID is 1 byte long. It carries the identifier of the IPPM metric corresponding to the performance parameter to measure.

A value of 0 means the field is not used (default).

Subsequent test packets may carry the list of metrics (primary and secondary parameters) to perform. This helps the receiver to limit the resource consumption.

8.4.3 Reserved

This field is 1 byte long.

It is unused in version 0 of the IPPMS. Its value should be ignored by the receiver.

8.4.4 Sequence number (Seq_Number)

Packet loss measurement requires a sequence number identify breaks in the received packet sequence.

More and more IP services cross gateways, which may change the sequence numbering of the packets present in the IP header (e.g., the initial value). A lot of metric computation relies on the analysis of the order of the packets. To provide a trustable sequence of results, there is a need for the sequence number to be integrated within the IPPMS. The point of measure will need the ability to populate and read the sequence number. The IPPMS sequence number (Seq_Number) is incremented for every test frame in a measure.

This field is 32 bits long. It is mandatory.

8.4.5 Transmit timestamp (Tx_Timestamp)

This field is 64 bits long.

It is used either as a rollover counter of 64 bits when the TSF flag of the control field is set to 0, or it is used as a NTP timestamp when TSF flag is set to 1.

8.4.5.1 NTP 'Seconds'

It is a 32-bit length field which represents the integer part of the NTP timestamp.

8.4.5.2 NTP 'Fract_Seconds'

It is a 32-bit length field which represents the fractional part of the NTP timestamp.

8.4.6 Controller identifier (Controller_ID)

Current testers interoperate only when they belong to the same manufacturer. To manage the measurement, testers insert three fields:

– the device that has sent the packet;

– the interface that has sent the packet;

– the identifier of the stream that the packet belongs to.

Such a framework is not suitable for tester interoperability and for inter-domain interoperability mainly because the meanings of 'device', 'interface' and 'stream' are not shared by the sender and the receiver. Consequently in the context of a test between two testers of different manufacturers, each tester will use its own numbering rules to identify the test. That makes interoperability impossible because it does not provide a unique identifier of the test by the controller of the measurement.

To permit interoperability, it is required that a test identifier be chosen by the controller of the test. As a tester may be used simultaneously by several controllers, the IPPMS must carry the identification of the controller.

This identifier provides the transmitter and the receiver of the measurement with an unambiguous identifier for the controller of the measurement running over different administrative domains.

Its type depends on the value of the field CIF of the IPPMS control field (see Table 6).

Its value and type may change between subsequent test packets. This permits transmission of the complete identification of the controller and, consequently, the identification of the flow.

Several types are defined to complete the identification of the controller of the measurement.

8.4.6.1 Operator code

The operator code is 10 bytes long. Its format is:

– 6 bytes for the operator ID defined in ITU-T Rec. M.1400 [9];

– 1 byte for the character "/";

– 3 bytes for the country code defined in ISO 3166-1 [11].

8.4.6.2 Enterprise number

This number identifies the manufacturer of the point of measure which sends the packets. This information increases the interoperability between different manufacturers.

The enterprise number should be set to 0 if the field is unused.

8.4.6.3 IPv4 address

This value carries the address, the protocol type and the port identifier of the controller.

8.4.6.4 IPv6 address

This value carries the IPv6 address, the protocol type and the port identifier of the controller. This is performed in 2 steps described in the definition of the CIF field (Table 6).

8.4.6.5 Proprietary

This value carries some proprietary information.

8.4.6.6 Inter-domain and inter-operability usage

Controller IP address and flow ID provides an absolute identifier of the measure.

Operator code, enterprise number and controller IP address are mandatory when performing measurement between two administrative domains or two different manufacturers.

8.4.7 Flow_ID

The IPPMS must include an identifier of the flow of test packets corresponding to the measurement.

The Flow_ID identifies the test packets associated with one measurement.

It is 2 bytes long.

The Flow_ID is assigned by the originator of the measurement.

8.4.8 IPPMS protection (CRC32)

This field is 32 bits long. The presence of this field is mandatory.

It is used to protect the IPPMS.

The sender computes a CRC32 on the IPPMS and inserts the result in the last 4 bytes of the 'CRC32'.

To verify the integrity of the IPPMS the receiver computes a CRC32 and compares the result with the value of the 'CRC32' field. If the values are the same then the IPPMS does not contain any bit errors and the received packet is classified as a test packet.

Intermediary nodes may use it to detect the presence of an IPPMS in a packet.

The following definition of the generator polynomial for the CRC32 calculation shall be used:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

The calculation of the CRC shall follow the procedure described e.g., in ITU-T Rec. G.7041/Y.1303 [8].

9 IP measurement packets for IPv4 and IPv6 levels

This clause defines six test packets according to the requirements of measuring the IP layer performance between IP measurement points.

A payload cannot be directly encapsulated on the IP layer. So the proposed test packets are actually UDP packets as illustrated in Figure 6.

SUB IP	IP	UDP	IPPMS	padding

Figure 6/O.211 – UDP test packet format

Fixed-length packet size facilitates the detection and the extraction of IPPMS by intermediary nodes.

Permissible IPv4 test packet sizes are 80, 160, 200, 600 and 1500 bytes. With 20 bytes reserved for the IPv4 header and 8 bytes for the UDP header, and 32 bytes for the IPPMS, the sizes of the corresponding padding fields are 20, 100, 130, 530, 1430 bytes. To improve high speed processing it was decided to align the padding on 32-bit boundaries. Consequently, the sizes of the payloads used are 52, 132, 164, 564 and 1464 bytes.

In addition we propose a UDP test packet which carries only the 32 bytes of the IPPMS.

9.1 IPPMS options

The IPPMS format defined in 8.3 offers a lot of flexibility. In order to maximize interoperability, the following default settings shall be applied:

– there is no extension;

– the CIF field may carry only an operator code (e.g., inter-domain), and/or the IPv4 address, the protocol type and the port of the controller (e.g., distributed), and/or proprietary information (e.g., local usage);

– Metric_ID field value is 0. Other values are ignored by the receiver;

– fill pattern:

  • any bit pattern can be used as a fill pattern;

  • for IPER measurements, the fill pattern needs to be protected using the CRC32 as defined in 8.4.8, in order to allow error detection. The CRC32 shall be calculated over the first N-4 Bytes of the fill pattern, where N is the length of the padding field. The last 4 bytes of the padding field are the CRC32;

  • the receiver shall ignore the padding field for all other measurements.

Changing these default settings is under the responsibility of the test manager and outside the scope of this Recommendation.

9.2 Payload size of 32 bytes (with IPPMS only)

This test packet is illustrated in Figure 7.

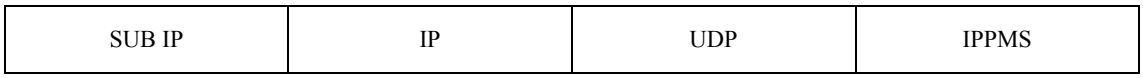

Figure 7/O.211 – Payload size of 32 bytes

9.3 Payload size of 52 bytes

This test packet is illustrated in Figure 8.

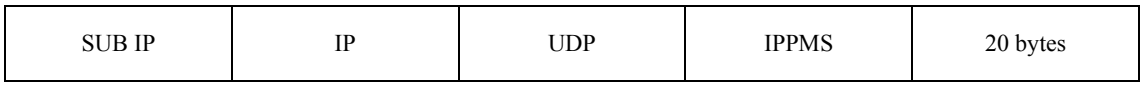

Figure 8/O.211 – Payload size of 52 bytes

9.4 Payload size of 132 bytes

This test packet is illustrated in Figure 9.

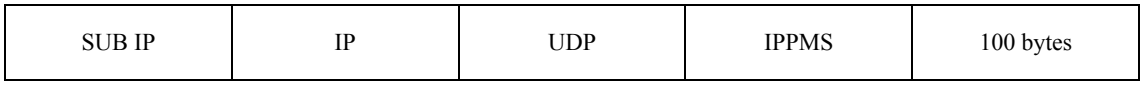

Figure 9/O.211 – Payload size of 132 bytes

9.5 Payload size of 164 bytes

This test packet is illustrated in Figure 10.

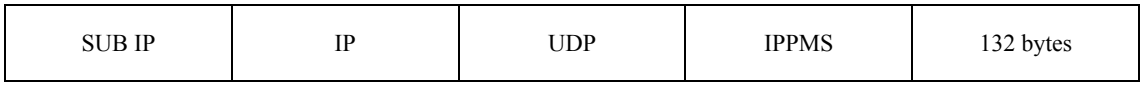

Figure 10/O.211 – Payload size of 164 bytes

9.6 Payload size of 564 bytes

This test packet is illustrated in Figure 11.

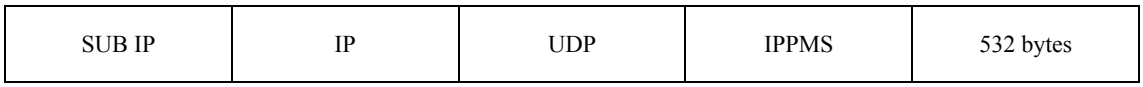

Figure 11/O.211 – Payload size of 564 bytes

9.7 Payload size of 1464 bytes

This test packet is illustrated in Figure 12.

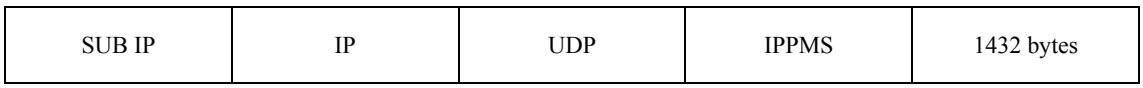

Figure 12/O.211 – Payload size of 1464 bytes

10 Security

ITU-T Rec. M.2301 [1] recommends that 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 packets.

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

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

BIBLIOGRAPHY

– IETF RFC 1305 (1992), *Network time protocol (Version 3) specification, implementation and analysis*.

– IETF RFC 2330 (1998), *Framework for IP performance metrics*.

– IETF RFC 2679 (1999), *A one-way delay metric for IPPM*.

– IETF RFC 2680 (1999), *A one-way packet loss metric for IPPM*.

– IETF RFC 2896 (2000), *Remote network monitoring MIB protocol identifier macros*.

– IETF RFC 3919 (2004), *Remote network monitoring (RMON) protocol identifiers for IPv6 and multi protocol label switching (MPLS)*.

– IETF RFC 3393 (2002), *IP packet delay variation metric for IP performance metrics (IPPM)*.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2006