International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.1543

(06/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet protocol aspects – Quality of service and network performance

---

Measurements in Internet protocol networks for inter-domain performance assessment

Recommendation ITU-T Y.1543

ITU-T

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	**Y.1500–Y.1599**
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.1543

Measurements in Internet protocol networks for inter-domain performance assessment

Summary

Recommendation ITU-T Y.1543 specifies a set of Internet protocol (IP) performance parameters and methods of measurement applicable when assessing the quality of packet transfer on inter-domain paths. The methods anticipate that there will be multiple measurement systems, each conducting measurements of a segment of the customer-to-customer path, and recommend configurations that should produce useful results in this cooperative scenario. The methods rely on existing parameter definitions and encompass both active and passive measurement techniques. Recommendation ITU-T Y.1543 also specifies requirements for trustworthy IP quality of service (QoS) monitoring, to ensure that results have a foundation in scientific method where sources of error are quantified. Thus, meaningful discussions of network QoS between users and service providers (SPs) are most relevant when based on measurements at measurement points (MPs) that correspond to the demarcation points (DPs) of the service agreement.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.1543	2007-11-13	12	11.1002/1000/9269
2.0	ITU-T Y.1543	2018-06-13	12	11.1002/1000/13627

Keywords

IP quality of service, performance.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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 received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

Network performance expectations must be set and monitored among users and service providers (SPs) to raise confidence in network delivery. Users typically only see the end-to-end performance, i.e., the concatenation of performance over multiple network segments or across multiple heterogeneous SPs, including their own private networks in many cases. Private networks are not reflected in service-level agreements when they are present and measurements that include subscriber-managed private networks are likely to underestimate the performance offered by the SP. Thus, meaningful discussions of network quality of service (QoS) between users and SPs are most relevant between measurement points (MPs) that correspond to the demarcation points (DPs) of the service agreement. Additional measurements are also possible within this framework.

Existing standards specify several metrics and measurement methods for point-to-point performance. Notable are [ITU-T Y.1540] and [ITU-T Y.1541] and the IETF Internet protocol packet performance metrics (IPPM) Working Group standards. However, many options and parameters are left unspecified, as is mapping between IP and non-IP metrics, accuracy and data handling. Each of these topics must be specified in order to support QoS across multiple heterogeneous SPs. Therefore, this Recommendation specifies essential measurement options, so that performance measurements conducted by operators in their administrative domains can be easily combined to estimate the end-to-end network performance or the inter-domain QoS, and to ensure that results will have a foundation in scientific method where sources of error are quantified. Further, measurements conducted by users or subscribers, or on their behalf by their SPs, will benefit from using the full specifications provided here, and in ITU-T and IETF standards.

Recommendation ITU-T Y.1543

Measurements in Internet protocol networks for inter-domain performance assessment

1 Scope

This Recommendation describes measurements that are applicable to:

1) provider delivery assurance of customer network performance;

2) providers to supply performance information for prospective customers;

3) provider troubleshooting among networks along defined paths;

4) provider internal indication of performance impact of changes within networks;

5) provider monitoring of performance of other network operators;

6) providing information to other network components, e.g., automated network management.

This Recommendation covers active and passive measurement and combinations of these two techniques. Active measurement employs packets dedicated to the measurement function inserted at one measurement point (MP) and collected at a remote MP. Passive measurement usually involves observations of user packet traffic at one or more MPs. Spatial measurement is a special category of active measurement that employs both active and passive techniques. It utilizes observations of measurement-dedicated packets at three or more MPs, where one or more point(s) simply monitor(s) [and do(es) not terminate] the test packets.

This Recommendation presents requirements for performance measurement including performance attributes and time-scales. Building upon existing standards, it recommends best practice in these areas based on [ITU-T Y.1540]. Comparisons with IETF RFC standards are included. This Recommendation also defines one possibility for the probe packet format, based on [IETF RFC 5357].

This Recommendation describes a network model that locates key points of demarcation and measurement. It categorizes various measurements and shows how they may be applied to the network model. It reviews time synchronization and sets targets for equipment that is located at various points in the network model.

Security requirements for measurement traffic are analysed, approaches are considered, and then a set of approaches is selected. The security of the border gateway protocol (BGP), synchronization systems and customer equipment lie outside the scope of this Recommendation.

Customer interactions with their service provider (SP) are discussed at a high level. Details of transferring results to customers lie outside the scope of this Recommendation.

The target networks of this Recommendation are IP networks, including those enabled by multi-protocol label switching (MPLS); pure layer 2 (L2) and other non-native IP networks lie outside the scope of this Recommendation.

This Recommendation specifies how to measure the minimally required set of metrics to determine network performance. Specification of advanced analysis and dissemination of measurement data lie outside the scope of this Recommendation.

Impairment allocation and mapping performance among IP and non-IP networks lie outside the scope of this Recommendation.

Methods to determine the exact network path that packets will follow lie outside the scope of this Recommendation.

2 References

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

[ITU-T O.211] Recommendation ITU-T O.211 (2006), *Test and measurement equipment to perform tests at the IP layer*.

[ITU-T Y.1540] Recommendation ITU-T Y.1540 (2016), *Internet protocol data communication service – IP packet transfer and availability performance parameters*.

[ITU-T Y.1541] Recommendation ITU-T Y.1541 (2011), *Network performance objectives for IP-based services*.

[ITU-T Y.1711] Recommendation ITU-T Y.1711 (2004), *Operation & maintenance mechanism for MPLS networks*.

[ITU-T Y.1731] Recommendation ITU-T G.8013/Y.1731 (2015), *Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks*.

[IETF RFC 792] IETF RFC 792 (1981), Internet control message protocol.

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

[IETF RFC 3432] IETF RFC 3432 (2002), *Network performance measurement with periodic streams*.

[IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A transport protocol for real-time applications*.

[IETF RFC 5357] IETF RFC 5357 (2008), *A two-way active measurement protocol (TWAMP)*.

[IETF RFC 5481] IETF RFC 5481 (2009), *Packet delay variation applicability statement*.

[IETF RFC 6576] IETF RFC 6576 (2012), *IP performance metrics (IPPM) standard advancement testing*.

[IETF RFC 7398] IETF RFC 7398 (2015), *A reference path and measurement points for large-scale measurement of broadband performance*.

IETF RFC 7679] IETF RFC 7679, STD 81 (2016), *A one-way delay metric for performance metrics (IPPM).*

[IETF RFC 7680] IETF RFC 7680, STD82 (2016), *A one-way loss metric for IP performance metrics (IPPM).*

[IETF RFC 7799] IETF RFC 7799 (2016), *Active and Passive Metrics and Methods (with Hybrid Types In-Between).*

[IETF RFC 8337] IETF RFC 8337 (2018), *Model-based metrics for bulk transport capacity*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 aggregate loss ratio (ALR): The loss aggregated along a path across multiple provider networks.

3.2.2 demarcation point (DP) (in IP networks): Generally, a point that separates two domains.

NOTE – In this Recommendation, a DP is the separation between the access and transit networks.

3.2.3 fraction lost: The fraction of real-time transport protocol (RTP) data packets from a source lost since the previous sender report (SR) or receiver report (RR) real-time control protocol (RTCP) packet was sent.

NOTE – Based on [IETF RFC 3550].

3.2.4 interarrival jitter (J): An estimate of the statistical variance of the real-time transport protocol (RTP) data packet interarrival time. The mean deviation (smoothed absolute value) of the difference D in packet spacing at the receiver compared to the sender for a pair of packets.

NOTE – Based on [IETF RFC 3550].

3.2.5 landmark system: A proxy system for customer premises terminal equipment.

3.2.6 measurement point (MP) (in IP networks): A point in the network containing functionality that may initiate or respond to measurements with other measurement points [located at peering points, demarcation points (DPs), provider edges (PEs), customer edges (CEs) and landmark customer premises equipment].

3.2.7 packet delay variation (PDV): The distribution of one-way packet delay of a packet stream, where the reference delay is the minimum delay of the stream and variation is assessed with respect to the minimum.

NOTE – PDV is further described in section 4.2 of [IETF RFC 5481] and [ITU-T Y.1540].

3.2.8 path unavailability: The period of time from when losses exceed a threshold until they drop below another threshold.

3.2.9 period path unavailability: The total period of unavailability during a customer reporting period (typically 1 month).

3.2.10 probe: An individual Internet protocol (IP) packet associated with active performance testing, i.e., a test packet.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ALR	Aggregate Loss Ratio
BG	Border Gateway
BGP	Border Gateway Protocol
CE	Customer Edge
CICP	Commercial Internet Connectivity Provider
CoS	Class of Service
DiffServ-MIB	Differentiated Service-Management Information Base
DP	Demarcation Point
DSCP	DiffServ Code Point
DSL	Digital Subscriber Line

DV	Delay Variation
ECMP	Equal Cost Multi-Path
FSD	Flow Summary Data
GLONASS	Global Navigation Satellite System
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
ICMP	Internet Control Message Protocol
ID	Identifier
IDQ	Inter-Domain Quality
IP	Internet Protocol
IPDV	Internet protocol Packet Delay Variation
IPLR	Internet protocol Packet Loss Ratio
IPPM	Internet protocol Packet Performance Metrics
IPPMS	Internet Protocol Performance Measurement Specification
IPsec	Internet Protocol security
IPTD	Internet protocol Packet Transfer Delay
IPUA	Internet Protocol Unavailability
KPI	Key Performance Indicator
L2	Layer 2
L2TP	Layer 2 Tunnelling Protocol
L3	Layer 3
LAN	Local Area Network
LSP	Label Switched Path
MP	Measurement Point
MPLS	Multi-Protocol Label Switching
MPM	Management of Performance Measurement
MTU	Maximum Transmission Unit
NAT	Network Address Translator
NE	Network Element
NGN	Next Generation Network
NTP	Network Time Protocol
OAM	Operations, Administration and Maintenance
OC	Optical Carrier
OWAMP	One-Way Active Measurement Protocol
PDV	Packet Delay Variation
PE	Provider Edge
PL	Packet Loss

PLR	Packet Loss Ratio
POP	Point Of Presence
PTP	Probe Transmission Period
PW	Policing Window
QoS	Quality of Service
RP	Rollup Period
RR	Receiver Report
RTCP	Real-time Transport Control Protocol
RTCP-XR	Real-time Transport Control protocol extended Report
RTP	Real-time Transport Protocol
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SP	Service Provider
SR	Sender Report
STM	Synchronous Transport Module
TCP	Transmission Control Protocol
TE	Terminal Endpoint
TWAMP	Two-Way Active Measurement Protocol
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

5 Conventions

This Recommendation uses the following conventions:

MSNG	Missing
N_T_{max}	Number of probes exceeding T_{max}
T_{max}	Maximum waiting time for a packet

6 Performance attributes

It is important to recognize that the model of inter-domain quality of service (QoS) is an extension of the Internet architecture, which supports a connectionless IP service that delivers user payloads in the form of packets or bytes in each direction. Since outbound and inbound traffic routes may differ, the targets and measurements for all performance attributes in inter-domain quality (IDQ) are one-way, and reflect the connectionless nature of the service.

The performance attributes that are used to characterize the network performance (inter-domain QoS) of a path are:

- mean one-way delay;
- one-way packet delay variation (PDV);
- packet loss ratio (PLR);
- path unavailability.

Each of these attributes has a corresponding performance parameter defined in [ITU-T Y.1540]. Although methods of measurement lie outside the scope of [ITU-T Y.1540], many relevant details may be obtained from the IETF Internet protocol packet performance metric (IPPM) RFCs (but noting that the IPPM definitions differ slightly in ways that do not detract from the clauses on measurement procedures).

The list of attributes purposely omits some common metrics. For example, application throughput depends upon many factors including PL, transit delay and others not under the control of the SP. Application throughput is not an independent IDQ performance attribute in its own right.

The traffic rate offered is also important as part of service descriptions and inter-SP contracts, but this is not considered a performance attribute.

Other performance metrics such as delay equivalent to loss and packet reordering are known to be useful. However, their incremental value over the metrics selected in the preceding paragraphs is currently believed not to be worth the additional complexity they would require specification, implementation and deployment. Time may prove otherwise and other basic network metrics may be added in the future.

6.1 Mean one-way delay

Delay is important to the support of many applications including telephony, multimedia conferencing, financial transactions and online gaming. In addition, delay is indirectly related to throughput and impacts file transfer speeds and email delays.

The delay attributes of a QoS class are characterized by the mean one-way delay. Optionally, the minimum delay and a specific set of upper percentile delay variations may be provided. The percentile approach is used in preference to a standard deviation or variance model due to the occasional occurrence of bi-modal or multi-modal delay distributions.

The mean delay is as specified in [ITU-T Y.1540].

Delay is distance sensitive due to the non-infinite signal propagation speed. Mean delay may vary between QoS classes due to priority queuing, which is taken into account when setting objectives.

6.1.1 Relationship to existing standards

The mean delay specified here corresponds to Type-P-Finite-One-way-Delay, if extrapolated from [IETF RFC 7679]. This metric requires a conditional distribution of delay (conditioned on arrival within a fixed waiting time that is set long enough to distinguish packets with long delays from those that are truly lost, e.g., discarded or corrupted), where lost packets have undefined delay.

6.2 One-way packet delay variation

In addition to the mean delay, PDV is important to many applications including telephony, gaming and transactions.

PDV is specified in [ITU-T Y.1540], and is essentially the difference between the 99.9th percentile of delay and minimum delay. The minimum delay of a sample or set of individual delay measurements is taken as the reference for variation. The percentiles of the actual delay distribution can be estimated by summing the minimum delay and the delay variation (DV) percentile of interest.

Other useful DV percentiles that can be recorded include:

- 90th percentile – DV90
- 99th percentile – DV99

Conceptually, percentiles are measured by stack-ranking all measurements of successfully delivered packets, discarding a top percentage e.g., 0.1% in the case of 99.9th percentile, then selecting the remaining highest value. In reality, we measure a subset of packets, the active probes. All lost packets or packets delivered while the network is considered unavailable are ignored by other metrics.

By taking multiple percentile readings and a minimum delay reading, the distribution of delays can be better understood. This information is more useful than a simple standard deviation metric that can be easily used only when assuming a mathematically friendly underlying probability distribution function. In reality, network delay characteristics may be multi-modal. There is added complexity and cost associated with engineering a network to closely match a particular delay distribution and in measuring that distribution accurately. Therefore only QoS classes that require multiple percentiles will have them specified and measured.

Delay variation is loosely correlated to distance (since distance is loosely correlated to number of hops) and allows targets to be set independently of site locations. Delay variation is correlated to link bandwidth and utilization and therefore, access links are a common source of DV, owing to their low bandwidth with respect to other network links.

6.2.1 Relationship to existing standards

The DV specified here is based on observations of the delay distribution, rather than on the difference between two successive delay measurements, as is the usual formulation associated with [IETF RFC 3393]. However, [IETF RFC 3393] has sufficient flexibility to produce either the inter-PDV or the DV by using a fixed minimum delay reference.

6.3 Packet loss ratio

PL is important to most applications. It significantly impacts either quality or throughput of the network.

A packet is considered lost if conditions satisfy the qualifications of a lost packet outcome as specified in [ITU-T Y.1540]. The maximum waiting time threshold, T_{max}, should be set long enough to differentiate a packet with long delay from a packet that is truly lost, e.g., discarded or corrupted. In practice, this waiting time may need to be set at 10 s or more, and requires knowledge of the network under test to set correctly.

IP PLR is the ratio of total lost IP packet outcomes to total transmitted IP packets in a population of interest, as defined in [ITU-T Y.1540]. The population of interest is usually the total set of packets sent between a particular source and destination with specific type, payload size, DiffServ code point (DSCP) and class assignment, etc.

PL is largely insensitive to distance and objectives can be set independently of the end site locations. PLRs are sensitive to access technologies, bandwidth and utilizations, and number of hops; objectives must be set accordingly.

6.3.1 Relationship to existing standards

ITU-T Y.1540 PL differs from Type-P-One-way-Packet-Loss as defined by the IETF IPPM, in that errored packets are designated lost in [IETF RFC 7680]. In practice, this difference is not significant to measurement results, because packets with errors are usually discarded before they reach the destination. However, if the last link entering the MP is error prone, then the difference between the [IETF RFC 7680] and [ITU-T Y.1540] definitions may be significant.

6.4 Path unavailability

Path unavailability is significant when a human observer detects a business-impacting application failure due to network loss. For a typical application such as telephony, a network path is considered unavailable by the user if there is an inability to connect or a connection is lost. The measurement of unavailability attempts to approximate this view by detecting periods during which network path unavailability would have noticeable impacts on applications and individual or business productivity.

Unlike delay and loss attributes, the unavailability attribute is not statistically simple to define and an approximation is required.

In IDQ, unavailability is calculated from the distribution of loss measurements over time; see clause 7 of [ITU-T Y.1540] for details of the service availability function. A period is considered unavailable if there is an excessive PLR (e.g., >25%) over a specific fixed time interval. The interval may be set independently for each QoS class, but currently only one interval is specified, 1 min.

This definition is intended to capture periods of very poor performance and requires network performance to return to normal levels before unavailability is ended. During a period of unavailability, none of the delay or DV metrics are valid.

Internet protocol unavailability (IPUA) is measured by summing the periods of unavailability and dividing by the total period being covered. The period being covered to be used is the default reporting to customer period. It should be noted that the IDQ system keeps track of each individual period of unavailability for reporting to customers.

Unavailability is largely insensitive to distance, but is sensitive to single points of failure in a network architecture. It will vary significantly with access technologies and configurations. To achieve a low level of unavailability, diverse transmission paths are required.

6.4.1 Relationship to existing standards

[b-IETF RFC 2678] defines parameters for unidirectional connectivity and bidirectional instantaneous connectivity. Both these metrics can be used to assess connectivity over time, similar to the ITU-T Y.1540 service availability function.

7 Performance measurement requirements

Inter-domain QoS is intended to increase the level of confidence in the expected service characteristics of the next generation network (NGN). Increased confidence will enable new applications, services and revenue streams. An integral part of achieving this confidence is the continuous measurement of service performance. The purpose of taking measurements is to provide information for customers, potential customers and SPs, and includes the following.

1) For customers and potential customers:
   a) reports to customers of what service has been delivered;
   b) reports to potential customers to support marketing claims on service characteristics.
2) For SPs and third party delivery assurance entities:
   a) reports to design service offerings;
   b) reports for troubleshooting;
   c) data for marketing collateral;
   d) reports to enable capacity planning and service development.

The IDQ measurement system and the statistics that it produces must:

a) be easily understood by SPs and customers;

b) be well defined (non-ambiguous);

c) be relevant to customers' applications;

d) enable SPs to diagnose issues and anticipate capacity requirements;

e) be independently repeatable (multiple SP measurements over the same time get the same result);

f) be independently verifiable by customers (customer measurements should be close to SP estimates);

g) be widely applicable (traffic type, link size, load independent, any IP network);

h) be appropriately sensitive to distance and path;

i) not significantly impact the forwarding of other data;

j) be sufficiently scalable to support millions of customer sites;

k) be sufficiently reliable to enable service level agreements (SLAs) with financial penalties to be administered;

l) be sufficiently accurate to enable SLAs with financial penalties to be administered.

Since outbound and inbound traffic routes may differ, all measurements will be one-way. Customers or SPs may aggregate the statistics of two directions to estimate the round-trip performance.

Measurements will be taken from each of the segments of the measurement network model (described in clause 9) and may be combined to form multi-segment, site-to-site, edge-to-edge or IP Terminal-to-IP Terminal metrics. A subset of these metrics will be used for reports for the offered services.

Quantitative requirements for end-to-end and segment accuracy have not yet been developed. The following incomplete list of measurement aspects should be considered when requirements are set, and when systems and components are designed:

- number of segments (due to concatenation errors);
- impact of measurement equipment not being directly in user data path;
- measurement equipment processor load;
- time synchronization errors;
- errors related to equal cost multi-path (ECMP);
- measurement granularity (unit);
- number of measurement samples per evaluation period to support required statistical accuracy;
- active probe frequency;
- active probe size.

In clauses 7.1 to 7.7, the terms active and passive are used consistently with the definitions of the terms for metrics and methods of measurement in [IETF RFC 7799].

7.1 Active measurement requirements

The performance of active probes will be used as a predictor of the performance of user data. Time-stamped delay and loss measurements will be collected. Probes will be injected into the network on certain devices and sent to extracting devices, which will return the measured information to the injection device.

7.1.1 High-level requirements

The probes will be:

a) based on the user datagram protocol (UDP) or transmission control protocol (TCP), as long as the stream and open control-loop designs of [IETF RFC 8337] are met;

b) usable for the measurement of both delay and loss, preferably in both directions between two devices;

c) marked with the appropriate DiffServ QoS class, preferably both in the header and body for each direction;

d) preferably transmitted at periodic intervals with pseudo-random start times near the beginning of the evaluation interval;

e) time stamped by injection and extraction devices;

f) preferably marked with source and destination addresses from address pools (to minimize impact of load-balancing);

g) able to indicate a loss in confidence of local clock sync back to initiating device;

h) capable of allowing probe packets to be marked with the appropriate MPLS traffic class bits, if the underlying network uses MPLS technology.

7.1.2 Specific requirements

[IETF RFC 3432] requires that a periodic sequence be started with a small random variation from the specified start time and subsequent probes each keep the same offset from coordinated universal time (UTC).

A separate set of probes will be used for each of the IDQ network QoS classes. Packet size is selected to represent user packets in each QoS class. Current preferences are listed in Table 1.

Table 1 – Probe packet size for selected network QoS classes

Network QoS class	Description	Probe payload size (octets)
Class 0	Telephony	20
Class 2	Low latency data	256

Probe packet sizes for other QoS classes are given in Appendix I.

NOTE – The probe size should be constant when measuring DV, since the delay metric includes probe serialization time. Serialization time will vary with probe size, possibly causing error in the assessment of DV.

Consideration of the pattern of inter-probe timing is important. The current preference is to use continuous probing with an equal inter-probe interval referenced to the first bit of each packet.

The following segment metrics are derived from the probe delay, probe loss and probe timestamp measurements:

a) mean delay;

b) minimum delay;

c) 99.9 percentile of DV (90, 99 percentiles optional);

d) unavailability;

e) loss ratio.

The inter-probe transmission period is determined by the number of measurement samples required for sufficient accuracy of delay percentiles. This will be referred to as the probe transmission period (PTP). The PTP may be different for each QoS class and by default is 100 ms. Measurement samples are aggregated over a period of time to be referred to as the rollup period (RP). The RP for all measurements will be 5 min.

The start of RP is synchronized among all participating SPs to UTC and is based on the beginning of each UTC hour. Accuracy is derived from the global positioning system (GPS).

An estimated average probe rate of 1 000 probes per 5 min RP is to be used for all percentiles and QoS classes. This includes an allowance of 1% for lost probes. The estimated probe rate will be validated before deployment, since too low a choice impacts accuracy and too high a choice wastes resources.

(Note that with this probe packet rate, the minimum loss ratio that can be reported is 10^{-3}, and this may not be sufficient to characterize some QoS classes accurately, such as ITU-T Y.1541 classes 6 and 7. More study is required for measurements in those classes.)

Looking at the bandwidth consumption that each-way probing consumes, assume:

- an average of 10 probe packets/s;
- measurements of three network QoS classes;
- using 64 byte probe packets.

Each probe stream consumes 5 120 bit/s, so for three QoS classes, the total probe stream is 15 360 bit/s. This is 0.003% of the total traffic of an optical carrier 12/synchronous transport module 4 (OC-12/STM-4) link, 1% of a T1 link or 0.8% of an E1 link.

A typical CE having IDQ service would use two-way probing. Total probe stream traffic on the customer edge-provider edge (CE-PE) link would be 15,360 bit/s in each direction.

Calculations for [IETF RFC 8337] streams are for further study.

The bandwidth consumption within a backbone is dependent upon the number of probe streams. The purposes of different probe streams are described in clause 8.2. Once a probing scheme has been designed, the evaluation of bandwidth consumption may occur.

7.1.3 Operations, administration and maintenance-based active measurement requirements

This clause provides several examples of possible operations, administration and maintenance (OAM) packet formats that meet the requirements for OAM-based measurements. The examples in this clause are shown strictly to clarify the usage of OAM for passive measurement. The standardization of the OAM packet formats and their semantics lie outside the scope of this Recommendation.

- Example of MPLS OAM packet format (see [ITU-T Y.1711]).
- Ethernet OAM packet format (see [ITU-T Y.1731]).
- Internet control message protocol (ICMP) packet format (see [IETF RFC 792]).

7.2 Passive measurement requirements

7.2.1 High-level requirements

The passive measurement general requirements are:

- passive measurement entity shall be one of the following: network element (NE) resident measurement entity or standalone measurement entity;
- every single measurement shall have at least source and destination addresses, an associated QoS metric, and accurate starting and ending time;
- timestamps should be traceable to UTC and sufficiently accurate to meet the requirements in clause 7.6;
- passive measurement shall capture a copy of the traffic without introducing modifications in the original traffic;

- passive measurement shall classify traffic in different granularity (e.g., 5-tuple, virtual private network identifier (VPNID), IPv4/6, etc.);
- passive measurement should support probabilistic (e.g., random) and hash sampling methods;
- passive measurement should support flow-based sampling methods;
- passive measurement shall perform sampling operation at wire-speed;
- passive measurement should support sampling both before and after classification;
- passive measurement should measure the performance of fragmented packets;
- passive measurement shall have the capability to measure various packet sizes, up to the maximum transmission unit (MTU) for a path;
- passive measurement shall derive various performance metrics such as delay, jitter, PL and unavailability.

7.3 Measurement time-scales

A common option, namely time-scales, is considered in this clause. Inter-domain QoS requires that all performance metrics be measured over the same time-scales. This greatly simplifies analysis of inter-domain performance.

The selected time-scales for performance measurement support the following criteria:

- the overhead load due to measurement traffic must be kept at a low level;
- the basic time-scale must be large enough to contain the start and end of a large number of traffic flows;
- the basic time-scale must be common and synchronized globally among SPs (preferably independent of network characteristics that may impact the timing path, e.g., link/ NE failures, congestion and DV);
- the time-scale must be meaningful to network users and capture any productivity or service quality issues they perceive in the network;
- the time-scales should not unduly emphasize momentary glitches, such as link outages or rerouting events, where they do not significantly impact network user experience.

Given these criteria, the default time-scales selected are as follows.

- Measurement: Time-scale unit is 5 min. This is synchronized via GPS or similar service and aligned with UTC. This allows all SPs to synchronize their measurement periods and correlate measurements. The targets and measurements for mean delay, DV and PL apply to 5 min periods. Measurement samples are aggregated over this period of time, which is referred to as the RP.
- Customer reporting: Time-scale unit is 1 "month" with start and end hour and date defined by the SP offering the IDQ service. The start and end monthly definitions may not be aligned between SPs. To be able to correlate measurements from one time zone to another and one SP's "month" to another, all timestamps are referenced to UTC, as well as any local time references. The actual time-scale of customer reporting needs to be determined by agreement between the network provider and each customer.

7.3.1 Relationship to existing standards

[IETF RFC 3432] refers to the rollup time as defined above as T_{cons}, a time interval for consolidating parameters collected at the MPs.

[ITU-T Y.1541] refers to the RP as the evaluation interval and suggests an evaluation time of 1 min for the Internet protocol packet transfer delay (IPTD), Internet protocol packet delay variation (IPDV) and Internet protocol packet loss ratio (IPLR).

7.4 Measurement system unavailability

If parts of the measurement system itself are unavailable, that will inhibit the ability of the provider to demonstrate that his QoS targets have been met during the period of unavailability. However, it is almost certainly not as serious for the measurement system to be unavailable as for the IDQ service itself to be unavailable as described in clause 6.4. We therefore suggest that while unavailability of the measurement system should be tracked, it should not be automatically treated as equivalent to unavailability of the service. If a customer claims that an SLA target was violated during some measurement interval, the provider would normally have measurement data to show how its segment of the network was performing at that time. If the provider cannot produce data to show that SLA targets were being met because its measurement system was not operational during that interval, it may have no choice but to assume that it did in fact violate the SLA. Thus providers will be highly motivated to keep their measurement systems operational all the time, but will not automatically be penalized for measurement system outages.

7.5 Interaction of policing and performance measurement

Ingress and egress segment performance is sensitive to the level of customer traffic. The performance levels of each IDQ network QoS class can only be delivered assuming that the traffic is within the subscription bounds for that QoS class.

If traffic does exceed its subscription bounds, packets may be delayed, discarded or have their DSCP remarked. These actions will potentially change the delay and loss characteristics of the data streams, as well as any probes that traverse the policing point. There is no fail-safe mechanism to detect which probes are impacted by a policing event.

To handle the interaction between policing and performance measurement, inter-domain QoS discounts measurements taken during a period when there is a policing-detected violation for that QoS class.

The determination of when policing-detected violations occur for a network QoS class is made through simple network management protocol (SNMP) polling of the differentiated service-management information base (DiffServ-MIB). The DiffServ-MIB keeps a counter of any policing-detected violation in each QoS class and, by comparing the counters at the start and end of the policing window (PW), the determination is made whether any policing-detected violations occurred. The interaction or communication between routing systems that perform policing and network measurement systems (that must indicate when measurements may be affected by the policing operation) should be accomplished in the measurement management system (see Appendix II).

The PW is the periodic rate at which SNMP polling takes place and by default is 5 min for each QoS class.

If a policing-detected violation occurs for a QoS class during a PW, the delay, loss and availability statistics for that RP shall be marked as possibly affected by an excess traffic condition. Measurements that are collected during customer traffic overload may not be suitable for comparison with SLAs, but might be useful for other purposes. The list of these RPs, and the associated number of packets that exceeded the agreement for each QoS class, is kept. These details and an aggregate of the total time and total exceeding packet count are reported to customers.

This method encourages customers to subscribe to the appropriate level of bandwidth in order to ensure that their QoS class characteristics are maintained at all times.

Policing-detected violations between SPs will similarly be detected and reported for each RP.

7.6 Clock synchronization

Clock synchronization specifies the extent to which multiple clocks agree on the time.

It impacts:

1) common understanding of when a measurement or event occurred or is planned to occur;

2) accuracy of certain network performance measurements.

The magnitude of time offset between MPs is critical to the accuracy of the one-way measurement attributes of minimum delay, mean delay and delay percentile. The attributes of DV and loss are unaffected by offset magnitude. Unavailability is unaffected, although there may be minor inaccuracies in the reported time of occurrence.

The MPs per the network models can be grouped into three categories:

1) demarcation and peering MPs;

2) CE and PE MPs;

3) customer host MPs.

We allocate a maximum offset to each category:

1) the clock of demarcation and peering MPs can have an offset from GPS of no more than 100 μs magnitude;

2) the clock of the CE router, PE router or co-located non-router measurement device can have an offset from its paired demarcation MP of no more than 1 ms magnitude;

3) the clock of certain customer host MPs can have an offset from its paired CE router of no more than 1 ms magnitude.

If a PE is also a DP, then the tighter offset is to be applied.

Providing clock synchronization at these points supports the measurements described in clause 9.

Figure 7-1 shows these three categories and where the specified offsets apply.

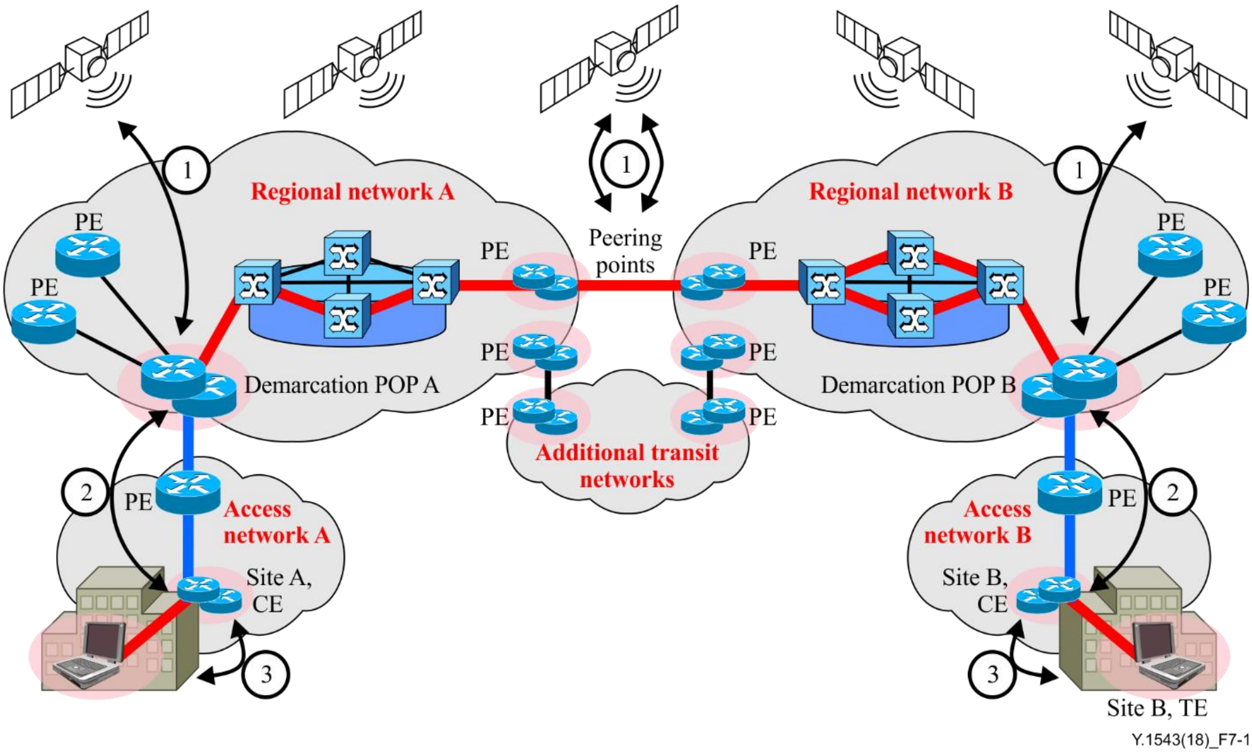


Figure 7-1 – Three categories of equipment at which offset maxima apply

7.6.1 Relationship to existing standards

[IETF RFC 2330] describes clock terminology and wire time.

The term "synchronization" is used in accordance with [IETF RFC 7679]. Synchronization measures the extent to which two clocks agree on what time it is. [IETF RFC 7679] loosely maps the IPPM group terminology to that of ITU-T (e.g., [b-ITU-T G.810] and [b-ITU-T I.356]). It analyses measurement errors.

[IETF RFC 3393] discusses the minimal impact of clock synchronization on differential measurements, of which DV is an example.

7.6.2 Implementation methods

GPS is used as a reference; however, other implementation methods [e.g., Galileo, global navigation satellite system (GLONASS)] may be used to synchronize demarcation and peering points as long as the offsets to GPS requirements are met. In cases of inadequate reception, the use of pseudolites or other techniques to provide accurate clocks derived from GPS may be required.

Figure 7-2 shows an example clock synchronization configuration for a terminal endpoint- terminal endpoint (TE-TE) scenario, where:

1) GPS receivers are used to set the time of shadow routers at both demarcation POPs;
2) the network time protocol (NTP) is used to set the time at the CEs, which are NTP clients using a demarcation POP shadow router as an NTP server;
3) NTP is used to set the time at selected customer hosts, which are NTP clients using the CE as an NTP server.

CE clock synchronization should be via NTP to the GPS system closest to the SP as client. This may not be their associated demarcation POP. Since NTP offset from client to server is a function of delay asymmetry between client and server, using NTP in some cases may not meet the clock synchronization offset requirements, in which case alternatives must be found.

CE routers may be used to provide a multi-homed IDQ service from single or multiple SPs. In any case, clock synchronization should be set using "prefer" via NTP from the closest measurement POP. It will automatically switch upon loss of synchronization.

This Recommendation does not address how SPs may set up GPS and NTP to meet these requirements, nor how to validate the offsets of their systems relative to a GPS-derived time. These topics will be the subjects of other Recommendations.

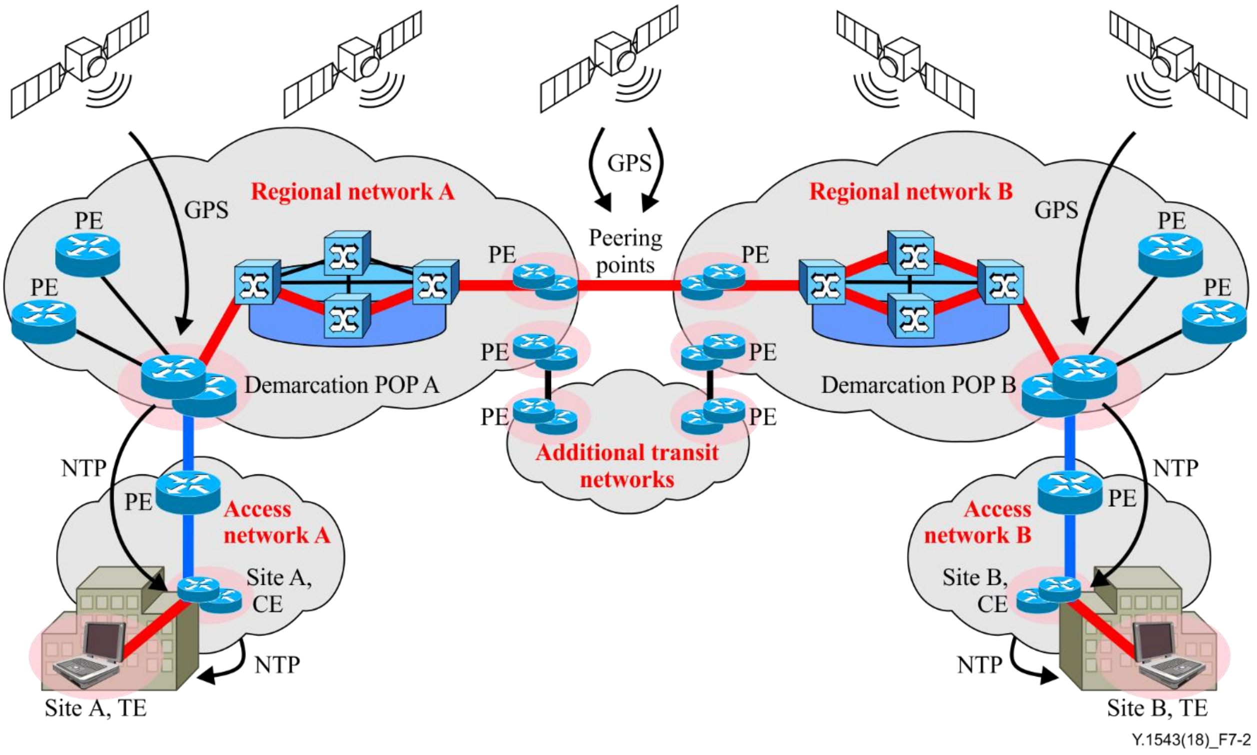


Figure 7-2 – Example of clock synchronization implementation

7.6.3 Loss of synchronization

MPs should be able to detect when they have low confidence of being adequately synchronized, e.g., if the NTP server becomes unreachable, MPs should:

1) notify a management station;
2) provide other MPs with information about the probes to which they are responding.

There are several degrees of timing inaccuracy in the context of performance measurements. There is always some error between the clocks of the sending and receiving measurement device:

- some degree of error is tolerable for all measurement types (e.g., <1 ms);
- some degree of error is tolerable for loss measurements, but excessive inaccuracy for one-way delay measurements would make them useless (e.g., >100 ms);
- some degree of error causes failure for all measurements (e.g., 1 s).

Loss measurements have a large tolerance to time error because of the substantial waiting time for packets to arrive at the destination. While normal one-way delays are <400 ms, the waiting time to declare a lost packet is usually 3 s. Therefore, loss measurements are less susceptible to errors in time synchronization when compared to delay measurements. It is important to detect synchronization issues (low confidence) and record this condition with all the results, including the degree of error if it can be determined.

7.7 Measurement granularity

QoS in NGN can be provided at various levels depending on service requirements. Its granularity can be as fine as a flow level or as coarse as a class of service (CoS) level. More specifically, the granularity levels consist of a flow, various layer 2 (L2) tunnels [e.g., tunnelling protocol (L2TP), L2VPN], an MPLS label switched path (LSP), layer 3 (L3) tunnels [e.g., Generic Routing Encapsulation (GRE), Internet protocol security (IPsec), L3VPN], any other class-based logical paths (e.g., an IP path associated with a DiffServ class), and an application session. Various mappings are possible among them. For example, a number of flows can be aggregated to form a tunnel. Several tunnels or logical paths may represent an application session.

There are several definitions of the term "flow" in use. This Recommendation adopts the definition used in [b-IETF RFC 3917] as follows: A set of IP packets passing an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties. Each property is defined as the result of applying a function to the values of:

1) one or more packet header field (e.g., destination IP address), transport header field {e.g., destination port number), or application header field (e.g., real-time transport protocol (RTP) header fields [IETF RFC 3550]};
2) one or more characteristics of the packet itself (e.g., number of MPLS labels);
3) one or more of fields derived from packet treatment (e.g., next hop IP address, the output interface, etc.).

A packet is defined to belong to a flow if it completely satisfies all the defined properties of the flow.

Flow level performance measurement may be needed for a high quality user service that needs special care or has a special billing purpose. Due to performance complexity, it may not be practical to have continuous real-time flow level measurement for all service flows. However, it is necessary to define such functional capabilities to meet a special service requirement. Fortunately, it may be possible to meet both flow level measurement and scalability requirements. If entire flows are measured at a particular MP of interest, it is not scalable. Typically, meaningful flows that take most traffic volume (e.g., over 95% of a particular link bandwidth) comprise a small portion of the entire number of flows. Thus, if these meaningful flows can be identified, they can be measured in real-time continuously and measurement of unnecessary flows avoided. Measurement on the tunnel level and other higher level paths introduces much less stringent performance burdens and thus scalability is not an issue.

Tunnel level, logical path level, as well as application session level measurement also needs to be supported to meet various measurement requirements, such as tunnel statistics, per class statistics, and per application statistics. These measurements are meaningful for an entire end-to-end path, whether it is a tunnel, a logical path or an application session. Measurement at the flow, tunnel and logical path level is relatively straightforward, since each has a unique means of identification. However, an application session level measurement requires mapping or aggregation of lower-level measurement results. For instance, a video telephony session can be composed of a voice and video flow. Each flow can be a class-based logical path or part of a L2VPN path.

The selected granularity for performance measurement shall support the following criteria.

- The measurement overhead must be kept at as low a level as possible.
- The measurement may support all levels of granularity as described in the preceding paragraphs.
- Both active and passive measurement methods can be used as applicable.
- The flow level and other fine-grained (e.g., LSP level) measurement shall be supported on a demand basis.
- The flow level measurement should have an end-to-end context. Concatenation of segment-based flow measurement may not reflect the original flow characteristics.
- The measurement may support relevant levels of granularity for multicast traffic.

8 Measurement network model

Ideally, measurements to ensure performance of customer traffic are taken between the same endpoints as each customer's traffic. Whether these endpoints are the customer's TE, CE router or PE router, the number of measurements would be so great as to make this impracticable. Therefore, a practical solution is to segment the network into a measurement network model.

Segmenting a network is a trade-off between the following requirements:

- cost minimization;
- support service flexibility;
- accurate end-to-end measurements;
- support measurement comparison to each providers' impairment target.

Costs associated with each segment include (assuming one-way active probing):

- clock synchronization at each segment end;
- initiation and response of probes at respective segment ends;
- associated measurement data which needs retrieval, storage and distribution;
- contribution to concatenation error.

The greater the leverage of a single measurement produced by a segment probe, the fewer probes will be needed. If fewer segment measurements may be used in the calculations of thousands of concatenated estimates, then there will be a lower total probe overhead.

Providers ensure delivery services between different endpoints. The following shorthand terminology is used.

1) "edge-edge" for services that extend to the edge of a providers' network.
2) "site-site" for services that extend to the edge of a customer's premises (this is sometimes called end-to-end).
3) "TE-TE" for a managed customer network service, this will be considered as extending to a customer's terminal. We note that some service architectures place one instance of TE within the traditional network boundaries, e.g., IP television services.

All three services must be supported by the models. There is no requirement that both endpoints have similar services (i.e., DPs). This terminology is used to emphasize the distinction in endpoints. Network segmentation provides service differentiation opportunities to providers who may ensure delivery and reporting for a subset of segments.

The models must support measurements that will enable comparison of measured performance to impairment targets. MPs located at CE or PE locations may use capabilities of the CE or PE routers themselves or separate co-located measurement equipment.

Note that NGN terminology differs from that of the communication industry used in this Recommendation. Table 2 is a mapping between the terms.

Table 2 – Mapping between the terminology of NGN and the communication industry

PE	one of	access node, access border gateway, edge node, or interconnection border gateway
CE	maps to	(new term) customer premises edge node

8.1 Network partitioning

The network is partitioned into segments, each being monitored independently. This partitioning enables the scaling of the network with sublinear growth in the amount of monitoring traffic and equipment relative to the number of customer sites involved.

Typically, the network is considered to consist of ingress and egress access segments, and a transit segment. It is assumed that one regional SP will provide an access network that supports both ingress and egress segments for a specific site. There may be a backbone SP(s) providing transit services between the regional SPs.

A specific SP may act as either or both an access provider for some traffic and as a transit provider for some traffic. A DP between access and transit segments is called a "demarcation POP".

DPs at the customer end of the ingress and egress segments are dependent upon the service.

- For "edge-edge" services, DPs are typically PEs.
- For "site-site" services, DPs are typically managed CEs.
- For "TE-TE" services, DPs are typically customer's terminals.

These DPs are illustrated in Figures 8-1, 8-2 and 8-3, where the models are named "edge-edge", "site-site" and "TE-TE".

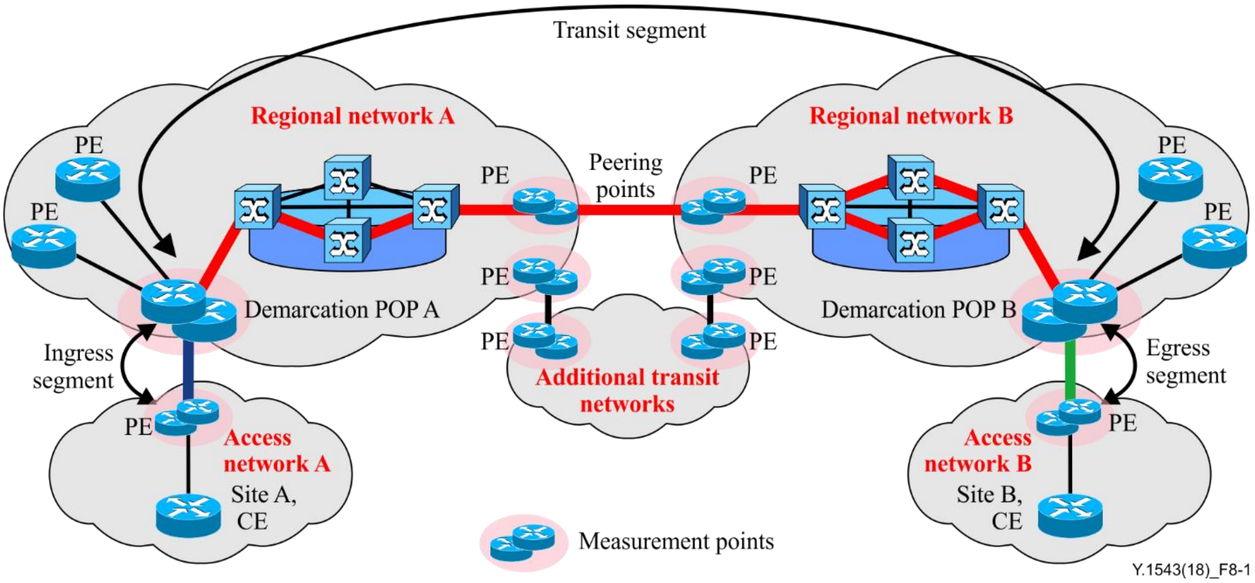


Figure 8-1 – Edge-edge model

In the edge-edge model, delivery is ensured to the PE nearest a customer, service between customer terminals or CE to the PE is not ensured. The ensured performance characteristics of the network comprise the aggregate of the performance characteristics of the ingress, transit and egress segments.

The ingress and egress segments do not include the CE-PE link, but do include the PE router as well as regional switching and transport.

The transit segment is measured from demarcation POP of the ingress regional SP to the demarcation POP of the egress regional SP. This segment may or may not include separate backbone SPs. The transit segment may span a city, country or state, a continent or multiple continents.

The transit segment may include parts of the ingress and egress regional networks, interconnects between the regional and backbone providers, and transit service across any backbone networks. The transit service of the backbone network is a subsegment of the entire transit service.

Partitioning of measurement responsibility may follow network boundaries. However, measurement responsibilities may cross boundaries in any configuration that serves the goal of complete measurement coverage. For example, two or more networks may be covered by MPs of a single measurement system.

The models support multiple peering connections between providers. Only one is shown for simplicity. The models support ECMP as indicated by the multiple paths shown within providers. In many instances, there may be multiple paths over which traffic may traverse. By having probes follow a plurality of paths, performance contributions from each path will be included in the reported statistics. Covering this path diversity as part of the measurement is achieved by using a range of addresses for each demarcation POP, each of which will be configured to respond to probes sent to any of 16 addresses and will be able to send probes sourced from any of 16 addresses. This will support a total of 256 flows, which increases the likelihood that, in the case of load balancing, active probes will follow all paths that a customer's data follows between two sites.

Note that results collected using multiple addresses cannot be pooled for metrics such as DV; otherwise the results would not be representative of customer flow performance.

Since there is limited load balancing expected between CE or PE and the demarcation POP, the CE/PE need only have one address, which in combination with the 16 addresses of the DP's measurement device will provide sufficient route diversity to include measurement contributions from all load-balanced paths. If the CE/PE is configured to probe across the transit segment, then 16 addresses would be preferable.

This approach to ECMP emphasizes coverage of all the paths that can be seen. Other approaches conduct measurements on a subset of paths that are representative of user traffic.

The ingress, transit and egress segments are monitored from demarcation POPs that are specifically located for the role. Demarcation POP selection is an SP choice. Each customer site is assigned to a demarcation POP within its network of regional providers. The POP is selected on the basis that the majority of the traffic from that site to others goes through this specific POP, which is within the same geographical region as the customer site. There is a minimum number based on the location of customer sites. SPs may increase the number of measurement POPs as they see fit, and some SPs may elect to make every PE POP a measurement POP.

The demarcation POP will have one or more measurement systems. It will monitor the backbone network and initiate tests with PE and CE devices. Thus it will be capable of measuring ingress, egress and transit segment performance. It will also collect and collate all necessary statistics.

Inter-domain QoS relies on the ability to collect inter-SP statistics on a continuous basis and for SPs to be able to resolve the causes of performance targets not being met. To support this monitoring and troubleshooting requirement, there are a set of requirements that must be met by SPs:

- each participating provider must provide MPs that act as performance characteristic test points for their use, and possibly for restricted use by other SPs;
- MPs must be located at any participating SP’s major interconnection peering POP;
- there must be an MP (demarcation POP) nominated by regional providers for each participating customer site;
- a service-dependent MP at PE, and possibly at CE or customer TE if this scope of performance security is supported.

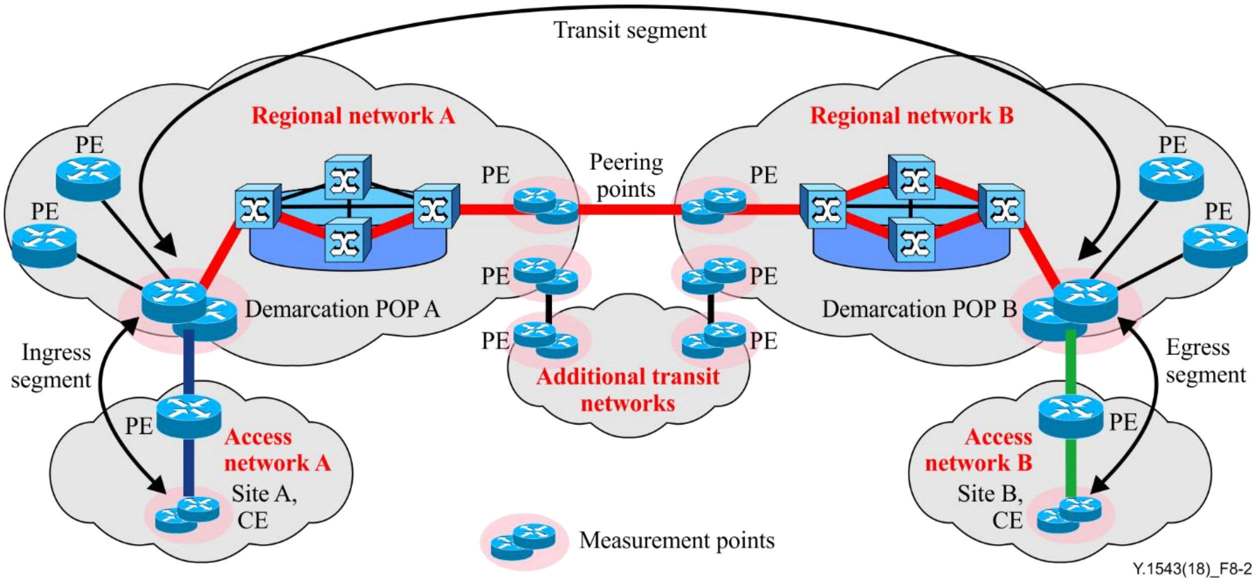


Figure 8-2 – Site-site model

In the site-site model, delivery is ensured to the CE. Service among customer terminals and the CE is not ensured by the SP; this is the responsibility of the customer. The ensured performance characteristics of the network comprise the aggregate of the performance characteristics of the ingress, transit and egress segments.

The ingress and egress segments include an access segment [digital subscriber line (DSL), cable, synchronous optical network/synchronous digital hierarchy (SONET/SDH), Ethernet, etc.] including the CE router, as well as regional switching and transport.

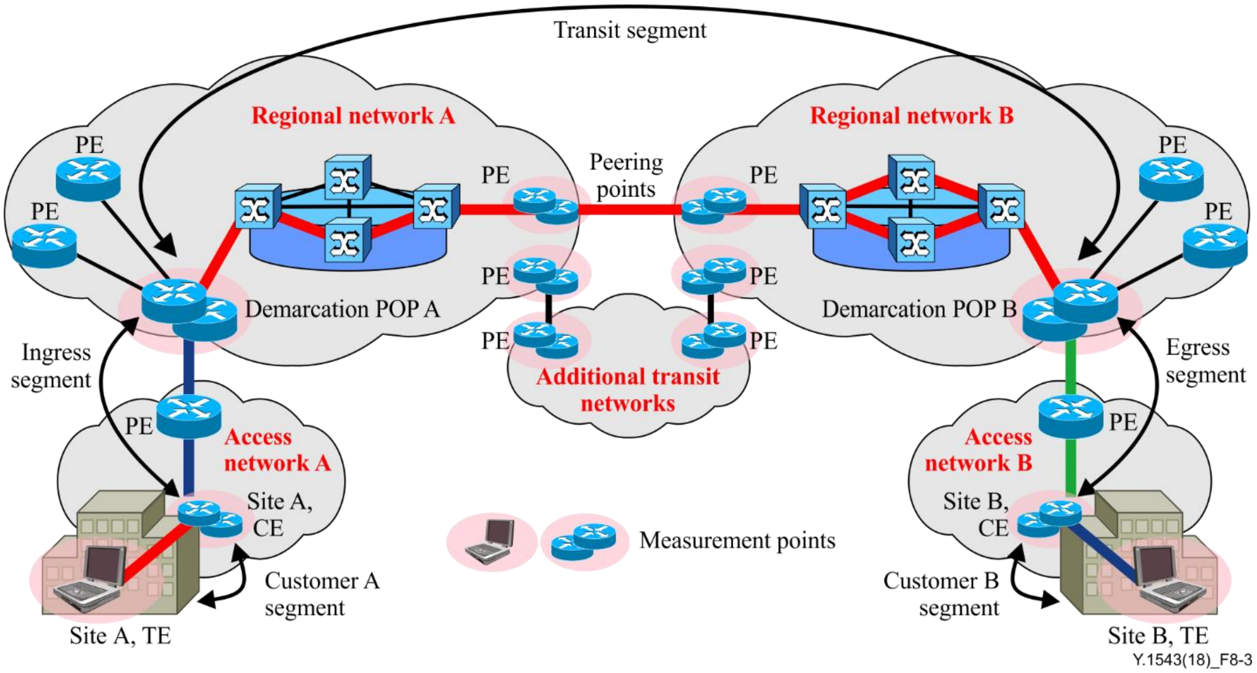
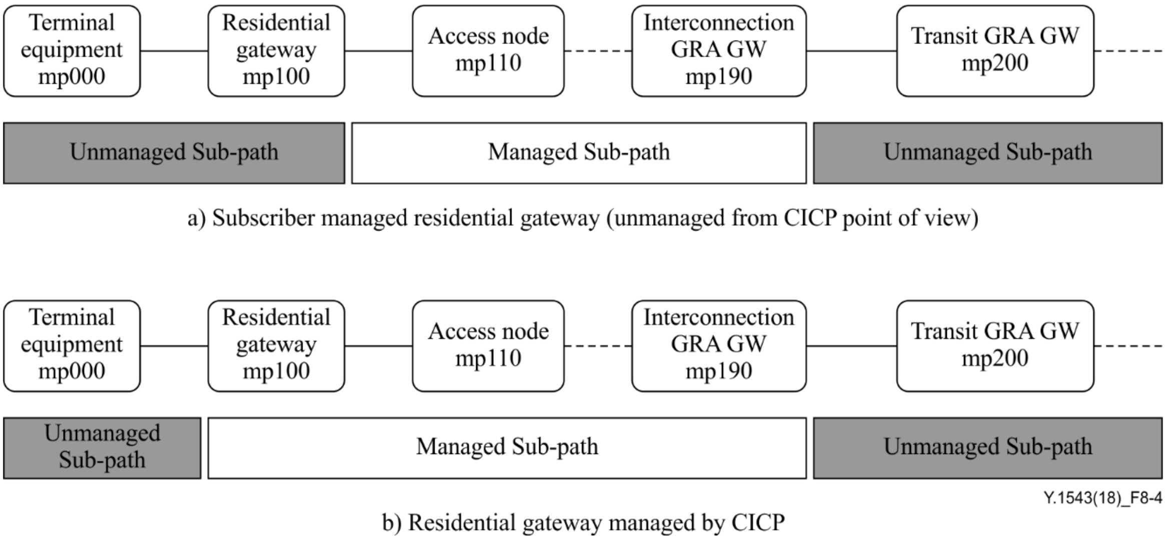


Figure 8-3 – TE-TE model

In the TE-TE model, the ensured performance characteristics of the network comprise the aggregate of the performance characteristics of the ingress, transit egress and customer segments.

The customer segment includes the network between a CE and a customer's TE. This may include home networking arrangements to company local area networks (LANs), computers and appliances.

This CE-TE segment is a private network and its contribution to CE-CE performance is unknown, but generally non-negligible. In the Figure 8-4, MP designations from [IETF RFC 7398] have been provided as a cross-reference (e.g., mp000). CICP is the commercial Internet connectivity provider.



a) Subscriber managed residential gateway (unmanaged from CICP point of view)

b) Residential gateway managed by CICP

Figure 8-4 – TE-CE-PE model (TE=mp000, CE=mp100, Ingress PE=mp110)

Selection of customer TEs to be used for measurements include consideration of the following.

1) Stability:
   a) static address or directory lookup;
   b) stationary rather than mobile;
   c) always online.
2) Performance:
   a) probe response not impacted by other programs.
3) Clock synchronization:
   a) required for one-way delay and delay percentile measurements.
4) Representativeness of many other TEs:
   a) analysis or measurement may show that measurements between a CE and a particular TE is representative of many other TEs, called "landmark" TEs.
5) Number of TEs probed:
   a) to minimize the number of probes, a minimum number of landmark TEs should be used;
   b) to minimize the complexity of data handling and reporting, a minimum number of landmark TEs should be used.

Communication from a CE to a TE may require a network address translator (NAT) traversal. Depending upon the administration of these devices, pre-provisioning or NAT traversal protocols may need to be used. Alternatively, the NAT device may be used as an MP as a proxy for TEs.

It is expected that there will be cases when there will be very little performance variation in the customer network. In these cases, instead of the use of operating measurements, fixed impairment values may be agreed.

8.2 Applied measurements

Measurement purposes fall into three broad categories, operating, supporting and testing.

- **Operating** measurements are those that are made on an ongoing basis between MPs to monitor normal operation of the ensured segments along customer data paths, e.g., measurements of ingress, transit and egress segments.
- **Supporting** measurements, which may be taken continuously, are used to provide information for SPs. These measurements occur in addition to operating measurements and can be between various MPs, e.g., measurements of each SP's contribution to the transit segment.
- **Testing** measurements are made on an exception basis following the detection of abnormal operating measurements for troubleshooting or to test a new path. These measurements occur in addition to operating or supporting measurements and are between MPs that do not have operating or supporting measurements being taken, e.g., measurement of a particular CE-to-CE path for a prospective customer.

Some measurements may fall into multiple classes. For example, a CE-to-CE measurement may be used for a prospective customer (testing), as a sanity check for providers (supporting), or as a premium (unscalable) customer service (operating).

Different views of the same measurement data may be useful for different purposes. For example, a provider that collects and analyses ongoing measurements at subintervals of RP may evaluate the impact of remedial action upon network performance more quickly than if they had waited for the RP before doing so.

The following scenarios show how the various performance measurement techniques may be applied to the measurement network models. The flexibility of the models supports more applied measurements than those described previously.

In the following scenarios, the measurement information exchanged among providers every RP includes:

1) minimum delay;
2) mean delay;
3) high delay percentiles;
4) loss ratio;
5) unavailability period information;
6) miscellaneous information.

All measurement scenarios described in clauses 8.2.1 to 8.2.5 are applicable to active, passive and spatial measurement techniques, unless otherwise noted. When measurement results have been obtained, the results should be conveyed from the collection points to management systems with oversight responsibility. Appendix II gives a description of a generic management process for measurement systems. However, the details of the management process lie outside the scope of this Recommendation.

8.2.1 Operating measurements scenario

The site-site operating measurement scenario is shown in Figure 8-5, where the endpoints are CEs.

Figure 8-5 represents two connected SPs, A and B, each having regional and access networks on which end customers have managed CEs. The following operating measurements are needed to estimate the site-to-site performance being delivered for customer site A.

1) SP A initiates measurements between:
   a) DP A and site A CE; and
   b) DP A and DP B.
2) SP B initiates measurements between:

a) DP B and site B CE.

3) SP A retrieves results of measurements between:

a) DP B and site B CE from SP B.

4) SP A compares the aggregated metric of the three segments to the guarantee and provides a report to site A customer.

The supporting measurements for the above service are detailed in Figure 8-5.

The edge-edge operating measurement scenario is shown in Figure 8-1, where the endpoints are PEs.

Similar to Figure 8-2, the following operating measurements are required to estimate the edge-to-edge performance being delivered for customer site A. Note that the only difference from Figure 8-2 is the use of PEs versus the use of CEs.

1) SP A initiates measurements between:

a) DP A and site A PE; and

b) DP A and DP B.

2) SP B initiates measurements between:

a) DP B and site B PE.

3) SP A retrieves results of measurements between:

a) DP B and site B PE from SP B.

4) SP A compares the aggregated metric of the three segments to the guarantee and provides a report to site A customer.

The supporting measurements are similar to those shown in Figure 8-5.

The TE-TE operating measurement scenario is shown in Figure 8-3, where the endpoints are TEs.

Similar to Figure 8-5, the following operating measurements are required to estimate the TE-to-TE performance being delivered for customer A. Note that the only difference from Figure 8-5 is the addition of CE-TE measurements and the retrieval of those measurements from SP B.

1) SP A initiates measurements between:

a) DP A and site A CE;

b) Site A CE and Site A TE;

c) DP A and DP B.

2) SP B initiates measurements between:

a) DP B and site B CE;

b) Site B CE and site B TE.

3) SP A retrieves results of measurements from SP B for measurements between:

a) DP B and site B CE;

b) Site B CE and site B TE.

4) SP A compares the aggregated metric of the five segments to the guarantee and provides a report to site A customer.

This scenario assumes a single TE; measurements with multiple TEs may be supported.

8.2.2 Supporting measurements scenario

To provide measurements for purposes in the support category, SPs may choose to perform measurement across their network to key MPs in other cities or regions in their networks. SPs may choose the mechanism used for internal support measurements, which may be the same as used for operating measurements. It is recommended, however, that each SP implement sufficient support tools to enable resolution of performance issues within their networks.

In many cases, sending and receiving customer sites will be connected to the same regional SP. To support these cases, the regional SP is fully responsible for the transit segment of the network and should perform the appropriate measurement functions.

The transit segment of the network will often comprise two regional SPs, one backbone SP and their interconnections. Each of these SPs should enable resolution of performance issues that may occur. This resolution process will include monitoring of specific sections of the transit segment. The collection of these statistics is part of the support process.

An SP should measure performance to each neighbouring POP of the other directly connected regional SPs and backbone SPs. This enables issue resolution of the interconnect performance and dimensioning as opposed to the network performance of the neighbouring SPs. In some cases, the interconnects may be through peering points with more complex performance characteristics and in other cases, a high-speed SONET/SDH interconnect may be used. The interconnect egress performance and dimensioning is the responsibility of the regional SP to which the customer connects. In the case of a regional SP interconnect to a backbone SP, the performance and dimensioning of both directions through the interconnect is the responsibility of the regional SP. The backbone SP may supply services that simplify this process and ensure performance targets are met.

In Figure 8-5, SP A and B each measure their own contribution to the transit segment, and may allow other interconnected SPs to retrieve those measurements. In this case, SP A and SP B each include in their measurements one direction through the interconnect. SP A may retrieve the measurements of the contribution of SP B to the transit segment.

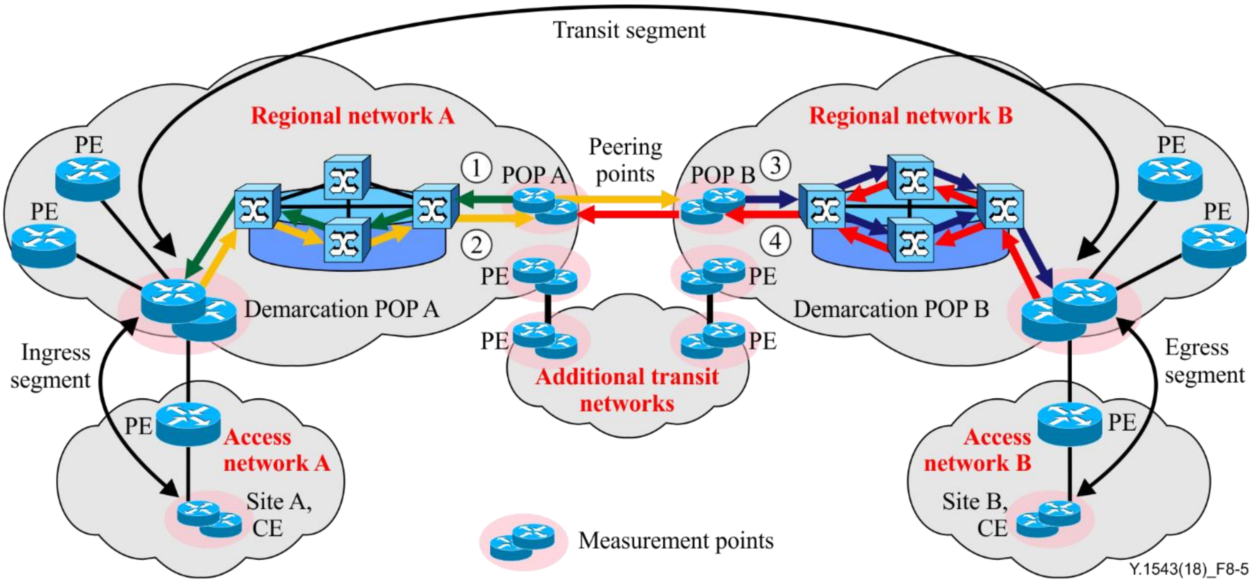


Figure 8-5 – Site-site supporting measurements

In this scenario, assume that each SP is responsible for performance security of their egress traffic over peering point links.

In order to obtain supporting measurements for the customer service indicated in Figures 8-2 and 8-1, the following activities would be performed as indicated in Figure 8-5:

1) SP A initiates measurements between DP A and its peering point POP A, for the direction from peering point POP A to DP A;

2) SP A initiates measurements between DP A and network B peering point POP, for the direction DP A to peering point POP B;

3) SP B initiates measurements between DP B and its peering point POP B, for the direction from peering point POP B to DP B;

4) SP B initiates measurements between DP B and network A peering point POP, for the direction from DP B to peering point POP A.

In addition to this data being used for an SP to confirm its own transit performance, these measurements may be concatenated:

- if aggregated with DP-CE measurements it is an estimator of the total CE-peering point performance of an SP;
- this data may be exchanged with partner SPs to provide security, and if aggregated with other supporting measurements, may be used as a sanity check for operating measurements.

Note that in Figure 8-6, four additional supporting measurements are required, two for each part of the transit segment of the SP. Further addition of IDQ services across this network would not require additional transit segment measurements, but would reuse the results of these measurements. Extension of the model in Figure 8-6 to include more SPs would require additional supporting measurement of that SP transit segment.

The description of supporting measurements in the preceding paragraph is for the case where each SP is responsible for its egress traffic over a single peering link. Similar scenarios may be used in the case of:

1) dual links (in parallel) where each provider pays for one of the links, and both links are actively used;

2) third party Internet exchange points.

8.2.3 Test measurements scenario

Information useful for troubleshooting or prospective customers may require additional measurements.

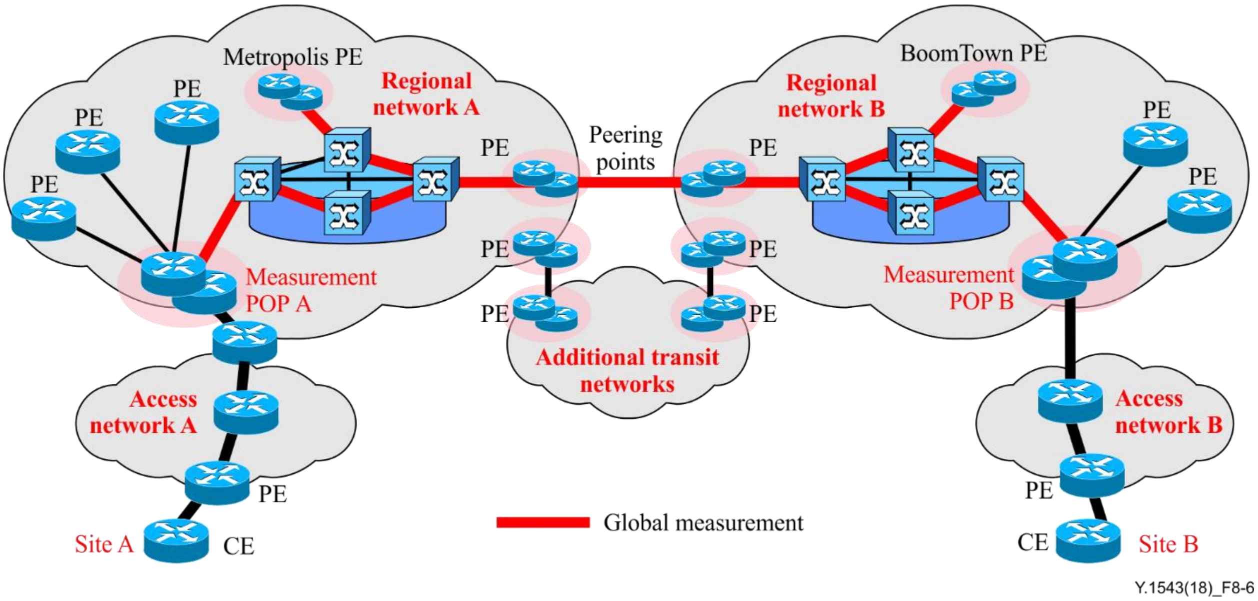


Figure 8-6 – Global-global measurements

In Figure 8-6, SP A or SP B initiates measurements between major global POPs named Metropolis POP and BoomTown POP, and publishes them in a report. This report indicates whether the transit performance targets are met for a significant set of destinations and approximates the expected performance for nearby POPs. This is useful for SP A and SP B as a basis for offering prospective services to customers who connect through or close to the Metropolis and BoomTown POPs.

SP A may wish to initiate measurement between DP A and the Metropolis measurement POP. This may be useful for SP A as a basis for offering prospective services to customers who connect both source and destination CEs to the SP A network.

Measurements from each demarcation POP to a significant set of high-profile global measurement POPs of multiple SPs may occur for similar purposes. This set of measurements characterizes the transit segment of the network for a representative set of customer traffic flows. The selected global POPs should cover all major cities and continents and include many other SPs. It is expected that a minimum of 50 global POPs would be monitored from each demarcation POP.

In some cases, a customer may not be satisfied that any of the chosen set of global measurement POPs is sufficient to characterize a specific transit segment. On customer request, an SP may initiate measurements between the customer DP and a set of selected POPs. This would normally be viewed as a custom service. Along with custom end-points, additional statistics and reports could be provided.

8.2.4 Example passive measurement scenario based on the real-time transport protocol/real-time transport control protocol-

Most real-time multimedia applications on IP-based networks use RTP. Passive measurement based on the real-time transport protocol/real-time transport control protocol (RTP/RTCP) is effective in that it can assist in collecting network performance data. A per-segment based measurement scenario is shown in Figure 8-7, where the MPs are TEs and border gateways (BGs) that handle RTP/RTCP and RTCP extension packets.

Delay and delay variation are important to real-time applications such as VoIP and video-streaming. The RTP [IETF RFC 3550]) is a transport layer protocol for real-time applications. RTP is designed to be independent of transport or network layer protocols. An RTP packet has timestamp and sequence number fields in its header. A passive collection system that resides in either TEs or BGs can evaluate PL and DV.

RTCP is an optional control protocol for RTP. Furthermore, RTCP extensions, such as real-time transport control protocol extended reports (RTCP-XRs [b-IETF RFC 3611]) are also optional control protocols for RTP. Participating TEs exchange RTCP and RTCP-XR packets. In an RTCP and RTCP-XR packet, performance metrics of its application services are reported. TEs are also able to evaluate rough round-trip delay with these packets.

Figure 8-7 represents two connected SPs, A and B, each having regional and access networks to which end customers have managed TEs.

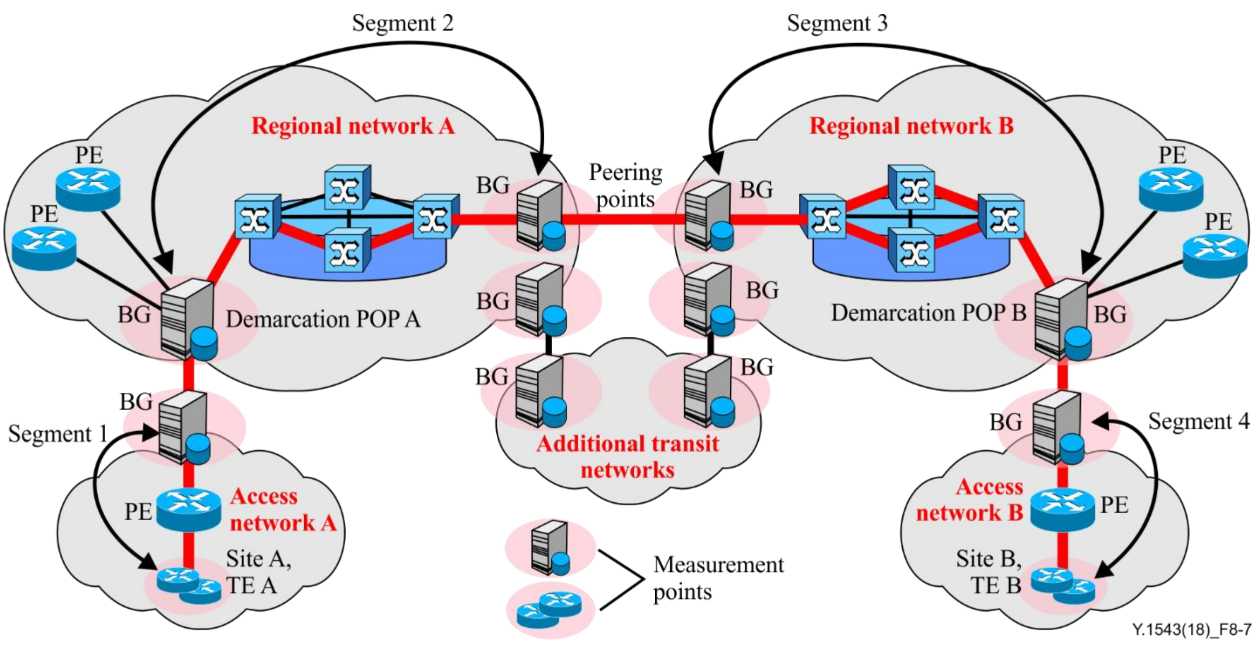


Figure 8-7 – Passive measurement based on the real-time transport protocol/real-time transport control protocol

The following operating measurements are required to estimate the per-segment based performance between TE A and TE B using RTP/RTCP and RTCP extension packets:

1) TE A initiates RTP sessions between TE A of site A and TE B of site B;

2) when the sessions are established, TE A and TE B communicate RTP/RTCP packets, as well as RTCP-XR packets;

3) BGs, which are located over the path of the RTP/RTCP flows, measure the performance based on the information provided in the RTP/RTCP/RTCP-XR packets;

4) TEs and BGs can independently collect the performance metrics of their own segment;

5) the reports of metrics collected at TEs and BGs are sent to the management system.

The TE-to-TE, site-to-site, edge-to-edge scenarios do not apply in the case of RTP/RTCP-based passive measurement procedures, since it is an application level performance measurement. It only has significance in terms of the TE-to-TE case. However, the performance metrics of other scenarios (site-to-site and edge-to-edge) can still be reported as described by the procedure in the preceding paragraph.

NOTE 1 – For conversational applications, metric reports of both directions between TE A and TE B are collected at BGs at the same time.

NOTE 2 – For one-way streaming applications, metrics reports of the selected direction between TE A and TE B are collected at BGs.

NOTE 3 – Management systems can choose TEs and BGs that send metrics reports depending on the type of application.

8.2.5 Example spatial measurement scenario

Active and passive measurement procedures can be used independently to meet specific purposes. However, there may be a situation where passive measurements can take advantage of active probes, enabling both methods to be used cooperatively. For example, a TE-to-TE operating active measurement procedure requires separate measurement of several segments, and each segment requires a pair of active MPs. The measurement results from each segment are aggregated to make end-to-end metrics. Another possible solution is to have a single TE-to-TE active measurement and a number of passive measurement devices deployed at some MPs, such as demarcation POPs, PEs and CEs. Each passive collection system can recognize the target active probe packets and measure network level performance metrics from the initiating TE to the passive MPs. For this method to be possible, the Internet protocol performance measurement specification (IPPMS) that is specified in [ITU-T O.211] is used to uniquely identify the active probe packet across multiple administration domains. It defines controller ID and flow ID to make a unique identification across multiple administration domains. The passive measurement devices that can recognize IPPMS capture the desired packets for various measurement operations.

The main advantage of this method is to reduce a large number of active probes in the middle of managed networks since one passive measurement device can handle a large number of active measurement sessions. The procedure in the following paragraph gives one possible measurement scenario (refer to Figure 8-3 and Appendix II).

The following operating measurements are required to estimate the performance between TE A and TE B by hybrid methods of active and passive measurement.

1) SP A initiates active inter-domain measurement between TE A and TE B:
   a) TE A sends active probe packets (conforming to [ITU-T O.211]) to TE B.
2) SP A initiates passive measurements by observing target probe packets:
   a) site A CE, PE, DP A and peering point A collect target packets;
   b) site A CE, PE, DP A and peering point A report to their management system;
   c) management system A generates performance metrics of each segment.
3) SP B initiates measurements by observing target probe packets:
   a) site B peering point B, DB B, PE and CE collect target packets;
   b) site B peering point B, DB B, PE and CE report to its management system;
   c) management system B generates performance metrics of each segment.
4) SP A and B can exchange and compare metrics to generate customer reports.

Besides TE-to-TE measurement, site-to-site and edge-to-edge measurement can be similarly performed. Thus, their procedures are not repeated.

9 Measurement procedures

9.1 Active measurement procedures

9.1.1 Mean one-way delay

The delay attributes of a network QoS class over a network segment are characterized by minimum delay, mean delay and a specific set of upper percentile delays. The percentile approach is used in preference to a standard deviation or variance model due to the frequent occurrence of bi-modal or multi-modal delay distributions.

In real networks, there are occasional events, such as rerouting and momentary link outages, that cause significant additional delays over and above the normal propagation and queuing delays. Packets that are delayed excessively are of little or no value to the application being supported and could be treated as lost packets; however, the incremental value of doing so is not considered to be worth the additional complexity, therefore delay outliers will be included in the delay statistics.

The segment one-way mean delay is calculated as follows:

1) collect measurements from N probes generated every PTP for each RP;
2) discard all measurements from periods of unavailability;
3) mean delay = sum(1..M) measurements/M (where M is the number of successful packet transfers, possibly less than N).

Multi-segment mean delay is calculated by aggregating the mean delays of each segment mean delay through a simple summation.

Measurement samples from unavailability periods are not included in statistics.

9.1.2 One-way delay variation

Segment (one-way) DV is derived from the minimum delay and percentile. It is derived on an RP basis. For each segment,

$$DV = One\text{-}way\_Delay\_Percentile - Minimum$$

For specific percentiles,

$$DV99.9 = 99.9Percentile - Minimum$$

$$DV99 = 99Percentile - Minimum$$

$$DV90 = 90Percentile - Minimum$$

Multiple segment DVs are used per network QoS class as listed in Table 3.

Table 3 – Segment delay variations used per network QoS class

DV	Most stringent QoS class	Mid-level stringency QoS class	Least stringent QoS class
DV99.9	×		
DV99	×	×	
DV90	×	×	×

Segment one-way delay percentiles are calculated as follows:

1) collect measurements from N probes generated every PTP for each RP;
2) discard all measurements from periods of loss or unavailability, leaving M samples;
3) stack rank the measurement set;
4) discard the top D measurements (D = round((100 – percentile) × M));
5) percentile = delay value of top remaining sample.

Multi-segment DV is calculated by aggregating the DVs of each segment through a provisional method defined in [ITU-T Y.1541]. It is also derived on an RP basis.

Since minimum delay and percentiles from unavailability periods are not included in statistics, derived DVs are also not included from unavailability periods.

9.1.3 Packet loss ratio

Segment (one-way) PL is measured over the same period as delay. It is derived on an RP basis. Segment PL is the number of probes whose measured one-way delay was $\geq T_{max}$ (N_T_{max}) and those that never made it to their destination or missing (MSNG). Note that T_{max} is the waiting time specified in [ITU-T Y.1540].

$$PL = (N\_T_{max} + MSNG)$$

PLR is PL divided by the number of transmitted packets (N)

$$PLR = PL/N = (N\_T_{max} + MSNG)/N$$

Measurements from unavailability periods are not included in PL statistics. Both the number of lost packets and the number of transmitted packets are reduced accordingly. This process avoids the PLRs being unduly impacted by network unavailability.

To combine these to produce a multi-segment PLR, called the aggregate loss ratio (ALR), the following method is used.

$$\text{ALR} = 1 - (1 - \text{PLR for segment 1}) \times (1 - \text{PLR for segment 2}) \times (1 - \text{PLR for segment 3})$$

ALR is derived for each RP.

9.1.4 Path unavailability

Unavailability is determined on a per QoS class, per direction basis, from one-way PL measurements. The ITU-T Y.1540 service availability function is the basis for measurement of unavailability.

The window for availability evaluation (T_{av}) should be aligned with the RP (5 min). The loss threshold for state determination is $c_1 = 0.75$ (75% PLR).

In order to calculate one-way unavailability, the absence of a one-way delay measurement must be understood to be due to an outbound loss rather than an inbound loss.

Delay, DV and loss measurements and their derived metrics are ignored for a segment for the duration of its unavailability.

For each segment, unavailability is calculated by summing all the RPs determined to be in the unavailable state.

Multi-segment path unavailability is calculated by calculating the total of unavailable time by adding the non-overlapping unavailable RPs from each segment in the path.

9.2 Passive measurement procedures

These procedures follow the general inter-domain measurement procedure, and specifics regarding passive measurement functions at the MPs are the only difference.

Two passive measurement collection systems extract flow summary data (FSD) from the packets of target flow and attach timestamps. The collection system may be dedicated hardware tapping the optical signal from the transmission link, or may be a software or hardware module installed in an NE. FSD from the two collection systems are sent to each management system. Single probe results are compiled by the initiating management system. Unlike active measurement procedures, the path of target flow may change during the measurement period. In such a case, one or both of the collection systems may not be able to extract the necessary FSD. This should be perceived by the management systems and appropriate measurement actions initiated, such as relocating MPs and restarting the measurement activity.

10 Requirements for trustworthy IP QoS measurement and monitoring

The following concise requirements are necessary to achieve a monitoring system with sufficient accuracy, comparability and trustworthiness to compare measurements with SP agreements, or to make comparisons between operator performance measurements.

1) A measurement system must be independent of the monitored IP network access technology.

2) The measurement method must support the state of the art in determining optimum parameters characterizing IP network access.

3) All parameters and parameter-values of a measurement implementation must be well defined and published.

4) The results of different measurement methods and implementations must be identical and repeatable (i.e., there must be no systematic error only impacting one or a set of measurement methods). The results of different implementations must be statistically identical independent from the following.

   a. ~~T~~he IP version used for testing, e.g., IPv4 or IPv6.

b. The IP packet size.

c. The IP payload packet size.

d. The transport layer protocol used for the measurement, e.g., UDP or TCP

e. The transport layer protocol version and configuration, e.g., different flavours of TCP, TCP window sizes and so on.

f. Overheads caused by higher layer protocols, e.g., FTP or HTTP, presence or absence of TLS.

g. Accuracy of clocks and timestamps involved in the measurement process.

h. Commodity IP network access usage impacting the measurement result, but outside the responsibility of the CICP, e.g., background traffic or home network sections and technologies like WiFi or powerline.

i. Subscriber terminal properties, e.g., operating system, CPU speed, buffer operation.

j. Concurrent IP connections on the residential gateway, as well as on the monitoring server.

k. Monitoring server configuration, e.g., server response time.

l. The reference path of the monitoring infrastructure set up. Configuration and network properties beyond the network access, e.g., PL and queuing delays caused by a peering interface, varying routes for up- and downstream measurement traffic caused by commodity IP routing, must not impact the result.

m. A measurement must contain the WAN and LAN traffic counters of the residential gateway prior to and after a single measurement, as well as both values read at the relevant network interface of the monitoring application server.

n. All measurements should be accompanied by IP traceroute measurements.

o. Repeated measurements under otherwise stable conditions along a measurement path must achieve equivalent results, as described in [IETF RFC 6576].

5) Transparent and public information on the measurement set up, the measurement software and the results and all systematic errors contained in these results must be available. The impact of each systematic error must be analysed, calculated or estimated, and the analysis as well as the error calculation must be published. This is one of the reasons why raw measurement data (i.e., measurement data containing systematic errors without correction) should not be published.

11 Security considerations

11.1 Impact of security on measurement of performance

The strength of security measures used in a solution can burden systems or cause extra security-related traffic. Since a heavily burdened router or firewall, or waiting for security-related traffic to return, may delay measurements; some risks versus benefits need to be considered.

To meet the high level of security requirements listed in the previous paragraph by implementing authentication and data integrity into the probes would require additional overhead on the measurement devices to do the authentication and establish data integrity. Depending on the number of probes, this could impact measurement devices with the overhead caused by this operation.

Authentication could be done on the measurement device itself or off-loaded to another system. The preference is to do the authentication on the measurement device itself, since it would likely allow for faster response than off-loading to another device requiring security-related network traffic.

11.2 Impact of performance measurement on security

User traffic may be collected as a result of passive measurements. Since user payloads may be temporarily stored for later analysis, suitable precautions must be taken to keep this information safe and confidential.

Appendix I

Summary of performance objectives and measurements

(This appendix does not form an integral part of this Recommendation.)

Table I.1 – Summary of performance objectives and measurements

Network parameter acronym	Parameter description	Performance objective	Units	ITU-T Y.1541 network QoS classes								Relative to [ITU-T Y.1541]	Covered in clauses
				Class 0	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6	Class 7		
IPTD	Mean IP packet transfer delay	Upper bound over RP	ms	100	400	100	400	1.000	U	100	400	Complies. Classes 1 and 3 are for less constrained distance than 0 and 2 respectively	6.1, 9.1.1
DV90	IP packet delay variation 90th percentile – minimum IPTD	Upper bound on delay variation over RP	ms	future	future	future	future	future	future	future	future	Not covered	6.2, 9.1.2
DV99	IP packet delay variation 99th percentile – minimum IPTD	Upper bound on delay variation over RP	ms	future	future	future	future	future	future	future	future	Not covered	6.2, 9.1.2
IPDV, DV99.9	IP packet delay variation 99.9th percentile – minimum IPTD	Upper bound on delay variation over RP	ms	50	50	U	U	U	U	50	50	Comply	6.2, 9.1.2
IPLR, ALR	IP packet loss ratio, aggregate loss ratio	Upper bound on the packet loss probability over RP	%	0.1	0.1	0.1	0.1	0.1	U	0.001	0.001	Comply	6.3, 9.1.3

Table I.1 – Summary of performance objectives and measurements

Network parameter acronym	Parameter description	Performance objective	Units	ITU-T Y.1541 network QoS classes								Relative to [ITU-T Y.1541]	Covered in clauses
				Class 0	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6	Class 7		
IPUA	Total period of excessive short term loss during which the network is considered unavailable	Upper bound on the percentage over month	%	0	0	0	0	0	1	0	0	Not covered	6.4, 9.1.4
PW	Policing window	Corollary	Minutes	5	5	5	5	5	5	5	5	Not covered	7.5
PPS	Probe payload size(s)	Corollary	Octets	20	20	256	256	256	256	20	20	Complies with the proposal of 160 or 1 500 octets	7.1.2
RP	Rollup period	Corollary	Minutes	5	5	5	5	5	5	5	5	Complies with proposal of 1 min	7.1.2
PTP	Probe transmission period (continuous)	Corollary	ms	100	100	100	100	100	100	100	100	Y.1541 suggests 10 to 20 ms for telephony. Y.1541 proposal suggests 20 ms for classes 0, 1 or 50 ms for classes 2, 3, 4 for 1 min sampled out of 5 min	7.1.2

NOTE 1 – Classes 6 and 7 are provisional classes.

NOTE 2 – U means unspecified (unbounded).

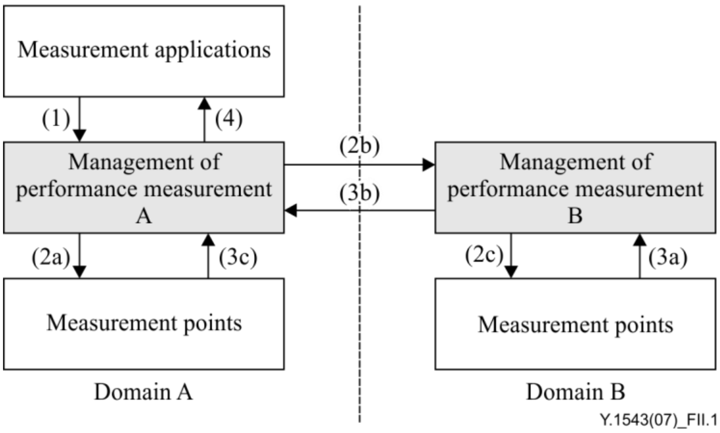
NOTE 3 – Regarding the ITU-T Y.1541 network QoS classes, note that certain pairs of classes collapse into node mechanisms/per hop behaviours/queues. These are classes 0 and 1, 2 and 3, and 6 and 7. Therefore, to probe all classes would require four measurement flows. Measurement results for these pairs would be used in comparison to objectives for each class.

Appendix II

Generic inter-domain management process for measurement systems

(This appendix does not form an integral part of this Recommendation.)

Figure II.1 depicts the general procedures for management of inter-domain performance measurement systems. An MP is a functional entity located in the transport, transport control or service control networks. In case of active measurement, it is responsible for initiating and receiving probe packets. In the case of passive measurement, it is responsible for capturing target packets. Management of performance measurement (MPM) functions include the interaction with measurement applications and the MPs, configuration of MPs, as well as exchanging the required configuration and measured information. The details of this process are a topic of active study in ITU-T SG 13. The following procedures are described based on such capabilities.



(1) The measurement application of SP A initiates a measurement task by sending measurement request to MPM.

(2a) Upon receipt of measurement request, MPM A locates the MPs involved. For the MPs located in domain A, MPM A sends the measurement parameters to MPs.

(2b) Upon receipt of measurement request, MPM A locates the MPs involved. For the MPs located in domain B, MPM A sends the measurement request to MPM B.

(2c) Upon receipt of measurement request, MPM B locates the MPs involved. For the MPs located in domain B, MPM B sends the measurement parameters to MPs.

(3a) MPM B collects the measured data from MPs located in domain B.

(3b) MPM B sends the measurement information to MPM A.

(3c) MPM A collects the measured data from MPs located in domain A.

(4) Based on the received measurement information from domain A and domain B, MPM A sends the response to the measurement applications.

Figure II.1 – Generic inter-domain management process

Appendix III

Measuring IP network performance with the two-way active measurement protocol

(This appendix does not form an integral part of this Recommendation.)

III.1 Introduction

The most common tool used to measure service quality parameters in IP networks is the ping tool. Ping is supported by almost all systems and uses the ICMP for packet delivery. Although ping is a commonly used measurement tool, it can be limited on devices or incoming packets may be completely rejected. This shows that the measurement method is limited. ICMP (ping) is a good enough to give some indication regarding the IP connectivity of equipment in a network and get a rough value of the round-trip delay measurement, but this tool cannot be used as a reference. Along with the high correctness of the measurements in the tested environment, the two-way active measurement protocol (TWAMP) should be considered as a successful active measurement method. It can also be established as a competitive alternative for performance measurement of IP networks [IETF RFC 792], [b-Mnisi].

In the literature, the measurement of IP network performance with TWAMP protocol cases has remained on theoretical bases and there are a few experimental studies. Generally, it is possible to see many analyses of the ICMP (ping) protocol. The experimental study and proposed performance measurement method described in this appendix are presented in [b-Kocak].

III.2 Two-way active measurement protocol

TWAMP is a new generation technology that measures the QoS key performance indicators (KPIs) between any two points in an IP Network [IETF RFC 5357]. See also [b-Kocak], [b-Backstrom], [b-Soumyalatha] and [b-IETF RFC 6802]. The TWAMP protocol is a standard-based and effective performance monitoring process that expands upon the one-way active measurement protocol (OWAMP) specified in [b-IETF RFC 4656], with the addition of the performance measurement of round-trip and two-way metrics for IP-based networks. The TWAMP measurement architecture is usually comprised of two hosts with specific roles, which allows for some protocol simplifications, making it an attractive alternative in some circumstances. This protocol delivers a flexible method for accurately measuring unidirectional and round-trip performance between two TWAMP-supported endpoints, regardless of device type or vendor. Unlike the OWAMP protocol, synchronization of the clocks of hosts participating in the protocol is not required to obtain two way metrics namely round-trip time, jitter and PL, see [b-Kocak], [b-Backstrom], [b-Soumyalatha] and [IETF RFC 5357].

The TWAMP consists of two interrelated protocols: TWAMP-Control and TWAMP-Test. The TWAMP-Control protocol is responsible for initiating, and then starting and stopping test sessions, whereas the TWAMP-Test protocol is used to exchange packets between the two TWAMP entities. The TWAMP architecture is shown in Figure III.1, see [IETF RFC 5357], [b-IETF RFC 6802].

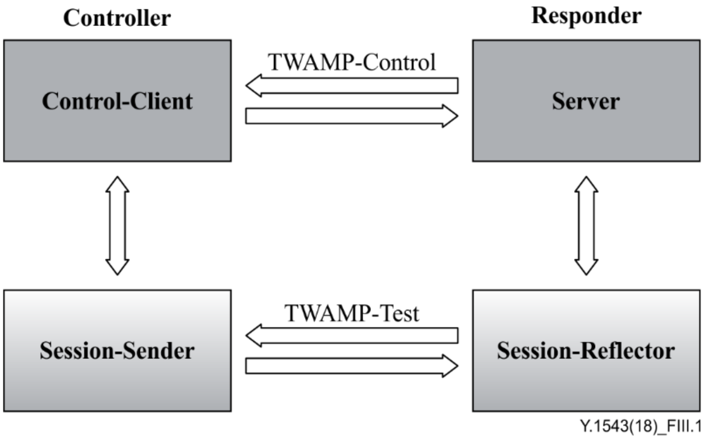


Figure III.1 – Two-way active measurement protocol architecture

The TWAMP-Control protocol consists of two subcomponents: Control-Client and Server. The Control-Client is a network node that starts and stops TWAMP-Test sessions. The Server is a network node, which facilitates one or more test sessions. The role of the server is similar to OWAMP; it configures the test end points. All metrics are obtained, analysed and published by the Session-Sender only. This protocol runs over TCP port number 862 by default and is used to initiate and control measurement sessions, see [IETF RFC 5357] and [b-IETF RFC 6802].

The TWAMP-test protocol exchanges test packets between two network nodes used to obtain metrics. This protocol consists of two sub-components: Session-Sender and Session-Reflector. The Session-Sender is a network node, which sends and receives test packets to and from the Session-Reflector during test sessions. In the TWAMP architecture, the Session-Sender is able to receive measurement data and to communicate the results back to the Control-Client. The Session-Reflector reflects test packets sent by the Session-Sender, as part of a test session. Unlike the Session-Receiver, it does not collect any information from the test packets as round-trip delay information is available only after the reflected test packet has been received by the Session-Sender. The TWAMP-Test runs over UDP and exchanges TWAMP-Test packets between Session-Sender and Session-Reflector. The Session-Sender and the Session-Reflector will use the same UDP port to send and receive packets. These packets include timestamp fields that contain the instant of packet egress and ingress. The packet includes a sequence number as well, see [IETF RFC 5357] and [b-IETF RFC 6802].

TWAMP-Light is an idea [b-Morton] with a simple architecture to easily provide a network with light test points. The idea does not require the TWAMP-Control protocol. It can be implemented in a two host scenario where the client side, known as "Controller", constitutes the roles of the server, the control-client and the session-sender. The reflecting side of the implementation is called "Responder", and contains the session-reflector. The test sessions are established through non-standard means and TWAMP-Test packets are exchanged. The architecture of the TWAMP-Light is shown in Figure III.2, see [b-Soumyalatha] and [IETF RFC 6802].

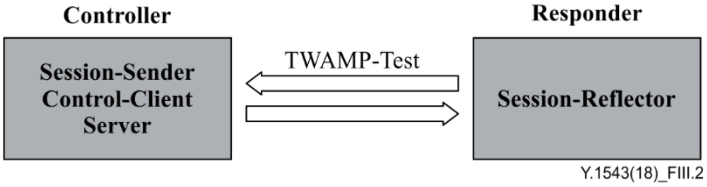


Figure III.2 – TWAMP-Light Architecture (missing control to Session-Reflector)

Bibliography

[b-ITU-T G.810] Recommendation ITU-T G.810 (1996), *Definitions and terminology for synchronization networks*.

[b-ITU-T I.356] Recommendation ITU-T I.356 (2000), *B-ISDN ATM layer cell transfer performance*.

[b-IETF RFC 2678] IETF RFC 2678 (1999), *IPPM Metrics for Measuring Connectivity* <http://www.ietf.org/rfc/rfc2678.txt?number=2678>.

[b-IETF RFC 3611] IETF RFC 3611 (2003), *RTP control protocol extended reports (RTCP XR).*

[b-IETF RFC 3917] IETF RFC 3917 (2004), *Requirements for IP flow information export (IPFIX).*

[b-IETF RFC 4656] IETF RFC 4656 (2006), *A one-way active measurement protocol (OWAMP).*

[b-IETF RFC 6802] IETF RFC 6802 (2012), *Ericsson two-way active measurement protocol (TWAMP) value-added octets.*

[b-Backstrom] Backstrom, I. (2009). *Performance measurement of IP network using the two-way active measurement protocol*. Master of Science Thesis, Stockholm, Sweden. See: https://www.nada.kth.se/utbildning/grukth/exjobb/rapportlistor/2009/rapporter09/backstrom_ingmar_09038.pdf

[b-Kocak] Kocak, C., Zaim, K. (2017). Performance measurement of IP networks using two-way active measurement protocol. In: *8th International Conference on Information Technology (ICIT)*, Amman, Jordan. New York, NY: IEEE.

[b-Morton] Morton, A., Mirsky, G. (2017). *OWAMP and TWAMP well-known port assignments: draft-morton-ippm-port-twamp-test-01*. Fremont, CA: IETF. Available from https://tools.ietf.org/html/draft-morton-ippm-port-twamp-test-01

[b-Mnisi] Mnisi, N.V, Oyedapo, O.J., Kurien, A. (2008). Active throughput estimation using RTT of differing ICMP packet sizes. In: *3rd International Conference on Broadband Communications, Information Technology and Biomedical Applications*, Gauteng, South Africa, pp. 480-486. New York, NY: IEEE.

[b-Soumyalatha] Soumyalatha, N., Ambhati, R.K., Kounte, M.R. (2013) Performance evaluation of IP wireless networks using two way active measurement protocol., In: *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Mysore, India, pp. 1896-1901. New York, NY: IEEE.

[b-Zaim, 2016] Zaim, K, Kocak. C. (2016). Performance analysis of IP network using two-way active measurement protocol (TWAMP) and comparison with ICMP (Ping) protocol in a saturated condition. In: *4th Int. Symp. on Innovative Technologies in Engineering and Science* (ISITES-2016), Alanya-Antalya, Turkey, pp.1618-1627.

[b-Zaim, 2017] Zaim, K. (2017). Performance analysis of IP networks using two-way active measurement protocol (TWAMP). Master of Science Thesis, Gazi University, Institute of Informatics, Turkey.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018