International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2173

(09/2008)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Quality of Service and performance

Management of performance measurement for NGN

Recommendation ITU-T Y.2173

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

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
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
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

Recommendation ITU-T Y.2173

Management of performance measurement for NGN

Summary

Recommendation ITU-T Y.2173 specifies requirements, reference measurement network model, high-level and functional architectures, and procedures for performance measurement management. This Recommendation together with Recommendation ITU-T Y.1543 provides overall consistency for performance measurement and management of NGN.

Source

Recommendation ITU-T Y.2173 was approved on 12 September 2008 by ITU-T Study Group 13 (2005-2008) under Recommendation ITU-T A.8 procedures.

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 not 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/.

CONTENTS

Page

Recommendation ITU-T Y.2173

Management of performance measurement for NGN

1 Scope

This Recommendation specifies the management aspects of performance measurement. Its scope is as follows:

– Requirements for management of performance measurement.

– A reference measurement network model as an extension of clause 8 of [ITU-T Y.1543], which allows for various measurement scenarios for NGN.

– A general and functional architecture for the management of performance measurement and the related stage-2 requirements.

– Management procedures covering various management scenarios such as discovery of measurement entities, initiation of measurement and exchange of measurement data among different NGN domains.

– Application scenarios for management of performance measurement (MPM) use cases such as procedures for performance measurements, degradation resolution and RTP/RTCP-based performance notification.

Note that the pertinent protocol specifications for reference points and procedures are expected to be described in separate Recommendations.

This Recommendation also describes the following MPM use cases:

1) Performance degradation resolution information reporting.

2) RTP/RTCP-based performance notification.

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 M.3050.x] Recommendation ITU-T M.3050.x-series (in force), *Enhanced Telecom Operations Map (eTOM)*.
<http://www.itu.int/rec/T-REC-M>

[ITU-T M.3060] Recommendation ITU-T M.3060/Y.2401 (in force), *Principles for the Management of the Next Generation Networks*.
<http://www.itu.int/rec/T-REC-M.3060>

[ITU-T O.211] Recommendation ITU-T O.211 (in force), *Test and measurement equipment to perform tests at the IP layer*.
<http://www.itu.int/rec/T-REC-O.211>

[ITU-T X.805] Recommendation ITU-T X.805 (in force), *Security architecture for systems providing end-to-end communications*.
<http://www.itu.int/rec/T-REC-X.805>

[ITU-T Y.1540] Recommendation ITU-T Y.1540 (in force), *Internet protocol data communication service – IP packet transfer and availability performance parameters*.
<http://www.itu.int/rec/T-REC-Y.1540>

[ITU-T Y.1541] Recommendation ITU-T Y.1541 (in force), *Network performance objectives for IP-based services*.
<http://www.itu.int/rec/T-REC-Y.1541>

[ITU-T Y.1543] Recommendation ITU-T Y.1543 (in force), *Measurements in IP networks for inter-domain performance assessment*.
<http://www.itu.int/rec/T-REC-Y.1543>

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (in force), *Functional requirements and architecture of the NGN release 1*.
<http://www.itu.int/rec/T-REC-Y.2012>

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (in force), *Security requirements for NGN release 1*.
<http://www.itu.int/rec/T-REC-Y.2701>

3 Definitions

This Recommendation defines the following terms:

3.1 active measurement: A method of measuring performance on a network by injecting specially marked test packets into the network.

3.2 measurement point: A point in the network containing functionality that may initiate or respond to measurements.

NOTE – Measurement point may perform either active or passive measurement. It is located at peering points, demarcation points, provider edges, customer edges and customer premises equipment.

3.3 OAM-based passive performance measurement: A general OAM-based performance measurement mechanism which can be applied in a similar way for any packet-based transport technology such as MPLS OAM and Ethernet OAM.

3.4 passive measurement: A method of observing user data packets on a network link non-intrusively.

3.5 spatial measurement: A measurement that involves collection of performance data at one or more measurement points that are not measurement endpoints.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABG Access Border Gateway

AN Access Network

ANE Access Network Edge

AS Autonomous System

BPS Bytes Per Second

CNE Core Network Edge

CoS Class of Service

CPE Customer Premises Equipment

CPN	Customer Premises Network
CPNE	Customer Premises Network Edge
DLSR	Delay since Last Sender Report
DNS-ALG	Domain Name System – Application Level Gateway
DoS	Denial of Service
DP	Demarcation Point
DSL	Digital Subscriber Line
ECMP	Equal Cost Multi-Path
EN	Edge Network
FCAPS	Fault, Configuration, Accounting, Performance and Security Management
FPS	Flow Per Second
FSD	Flow Summary Data
GPS	Global Positioning System
IBG	Interconnection Border Gateway
IPDV	Internet Protocol Packet Delay Variation
IPFIX	Internet Protocol Flow Information eXport
IPLR	Internet Protocol Packet Loss Ratio
IPPM	Internet Protocol Packet Performance Metrics
IPPMS	Internet Protocol Performance Measurement Signature
IPTD	Internet Protocol Packet Transfer Delay
IPUA	Internet Protocol UnAvailability
LAN	Local Area Network
LSR	Last Sender Report
LT	Line Termination
MPLS	MultiProtocol Label Switching
MPM	Management of Performance Measurement
NAPT	Network Address Port Translation
NAT	Network Address Translation
NAT-PT	Network Address Translation – Protocol Translation
NT	Network Termination
NTP	Network Time Protocol
OAM	Operations, Administration and Maintenance
PME-FE	Performance Measurement Execution Functional Entity
PMP-FE	Performance Measurement Processing Functional Entity
PMR-FE	Performance Measurement Reporting Functional Entity
PPS	Packet Per Second
RACF	Resource and Admission Control Functions

RTCP Real-time Transport Control Protocol

RTP Real-time Transport Protocol

RTT Round-Trip Time

SCF Service Control Function

SLA Service Level Agreement

SPE Service Provider Edge

SSRC Synchronization Source

TE Terminal Equipment

UDDI Universal Description, Discovery and Integration

VoIP Voice over Internet Protocol

5 Conventions

None.

6 Requirements

6.1 High-level requirements

This clause provides the high-level requirements on management of performance measurement for NGN networks and services. Additional information related to these requirements is provided in Appendix III.

The requirements, all mandatory, are as follows:

1) Support inter-domain performance measurement.
2) Enable inter-domain performance measurement functional entities to discover each other.
3) Enable distribution of measured performance data from one domain to another.
4) Enable aggregation of measured performance data from different domains.
5) Enable management of performance measurement in a NAT/NAPT environment.
6) Enable management of performance measurement in a NAT-PT environment.
7) Enable management of performance measurement in an ECMP environment.
8) Enable identification of performance degradation problems based on performance measurements in a multi-domain environment.

6.2 Functional requirements

This clause describes the functional requirements on management of performance measurement for next-generation networks and services.

The performance measurement management architecture is required to:

1) Be distributed; and the distributed architecture may be federated, hierarchical, or cascading neighbour.
2) Enable the partitioning of networks to provide accurate end-to-end measurement, and support comparison of measurement with provider impairment targets.
3) Support a common information model for storing the measured data for the management of inter-domain performance measurement.

4) Support a reference point for exchanging the measured data for the management of inter-domain performance measurement.

5) Support configuration and monitoring measurement entities.

6) Support control measurement entities.

7) Enable collection, aggregation and storage of measurements.

8) Support management of the collection of measurement data.

9) Support derivation of performance metrics from measured data.

10) Support of exchange of performance metrics among domains.

11) Support provision of performance data to the RACF or the like for resource and admission control purposes.

12) Support provision of performance data to a management application for resolving inter-domain performance degradation problems.

13) Support management of active measurements, passive measurements and spatial measurements.

6.3 Non-functional requirements

The performance measurement management architecture is required to:

1) Meet the performance objectives for the latency of transfer of performance data among providers and performance data registries.

2) Take into account events that have performance impacts (e.g., policing events).

3) Enable performance management information to be exchanged efficiently, reliably, securely, and with scalability.

4) Be consistent with a common information model that is protocol neutral, extensible, and flexible.

7 Reference measurement network model for performance management

7.1 General reference network model

Figure 7-1 shows a general reference network model for performance measurement in an NGN environment. Along the end-to-end path, there are two CPNs, two access networks, one or multiple core networks, zero or multiple transit networks, and one or multiple service provider networks. The access networks, core networks, transit networks and service provider networks may belong to the same or different network or service providers. One example service provider is an IPTV service provider of a central head-end or regional head-end.

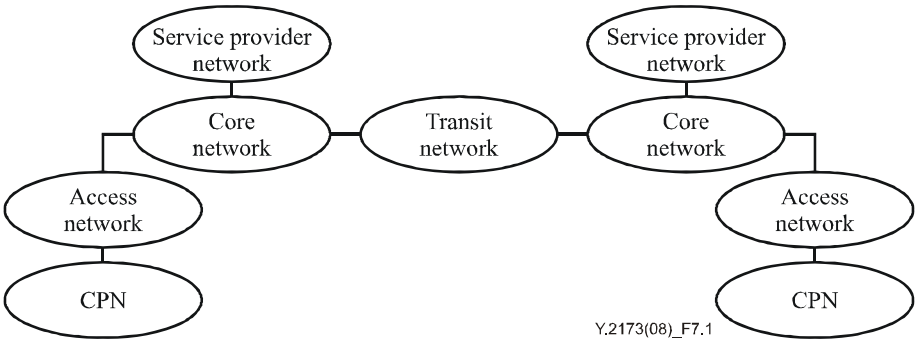

Figure 7-1 – General reference network model

7.2 Principles of network partitioning

It is desirable to partition the network for the purpose of inter-domain performance measurement.

Partitioning a network is a trade-off between the following factors:

- Minimize cost.
- Support service flexibility.
- Provide accurate end-to-end measurements.
- Support comparison of measurement results with provider impairment targets.

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

- Clock synchronization at each segment end.
- Initiation and response of probes at respective segment ends.
- Initiation and collection of probing packets by passive measurement 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 lower total probe overhead.

NGN providers typically offer three types of assured delivery services between different endpoints. These are commonly referred to as:

1) "Edge-to-edge" for services that extend to the edges of a provider's network.
2) "Site-to-site" for services that extend to the edges of customer premises' networks.
3) "TE-to-TE" for a managed customer network service, this is considered as extending to the network edge of customer terminals.

All three services must be supported by the measurement models. Endpoints need not have similar services (i.e., demarcation points). This terminology is used to emphasize the distinction in measurement endpoints. Network segmentation provides service differentiation opportunities to providers, who may offer assured delivery and reporting for a subset of segments.

Besides these three services, measurements between other combinations of endpoints to support various NGN services are required to be supported by the model. Figure 7-2 below illustrates some examples. TE-to-SPE is an example for measurement between an IPTV service provider and a customer. TE-to-ANE measurement can be used for the case where IPTV's content is mirrored at the access network edge. ANE-to-SPE may also be required when all three involved operators are owned separately and performance assurance is required between all measurement endpoints. Measurement at one endpoint is also required to be supported for passive measurement.

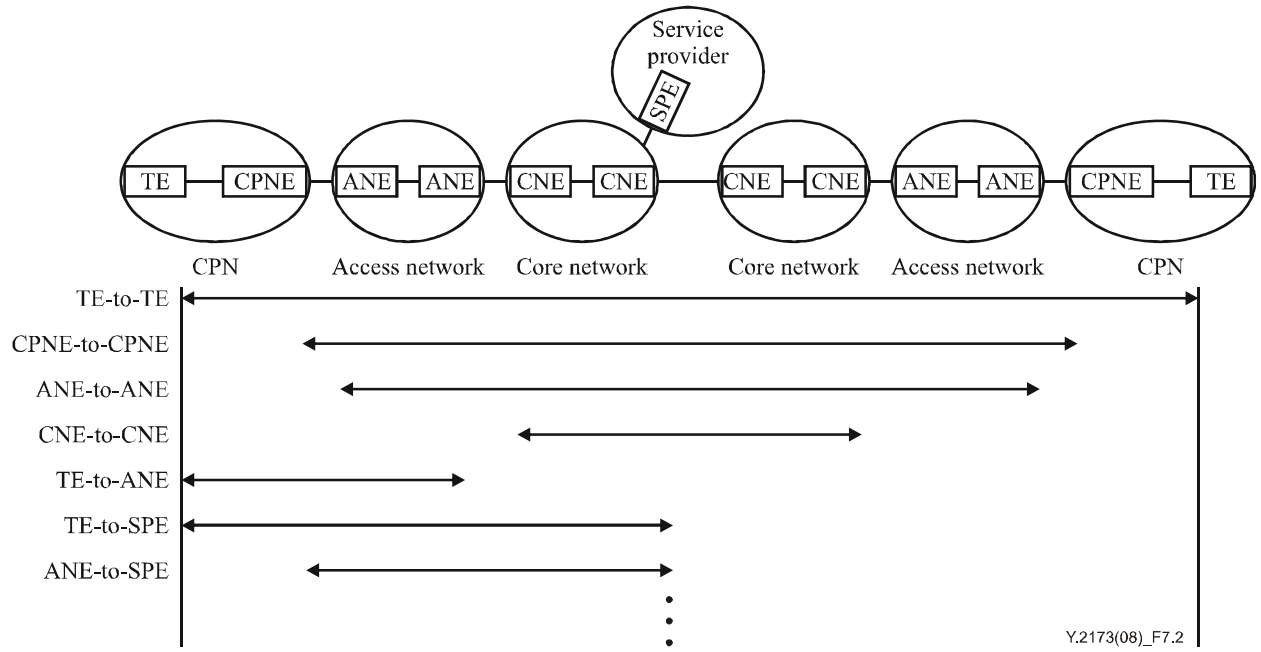

Figure 7-2 – Generalized principles of network partitioning

Generalization of network partitioning allows greater flexibility to meet various measurement requirements of NGN services.

The measurement models support measurements which enable comparison of measured performance to impairment targets. Measurement points located at terminal edge (TE), customer premises network edge (CPNE), access network edge (ANE), core network edge (CNE) or service provider edge (SPE) locations may use measurement capabilities of the TE, CPNE, ANE, CNE or SPE devices themselves if they are resident or separate co-located measurement equipment.

7.3 Network partitioning

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

Typically, an NGN is considered to consist of ingress and egress access segments, a core transport segment, a transit segment and a service provider segment. It is assumed that one regional service provider will provide an access network that supports both ingress and egress segments for a specific site. There may be a core transport provider and a transit transport provider providing transit services between the core transport providers.

A specific NGN provider may act as either or both an NGN access transport provider for some traffic and as an NGN core transport provider for some traffic.

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

- For "edge-to-edge" services, demarcation points are typically ANEs or CNEs
- For "site-to-site" services, demarcation points are typically managed CPNEs.
- For "TE-to-TE" services, demarcation points are typically the network edge of customer's terminals.

These demarcation points are illustrated in Figures 7-3, 7-4 and 7-5, where the models are named "edge-to-edge", "site-to-site" and "TE-to-TE".

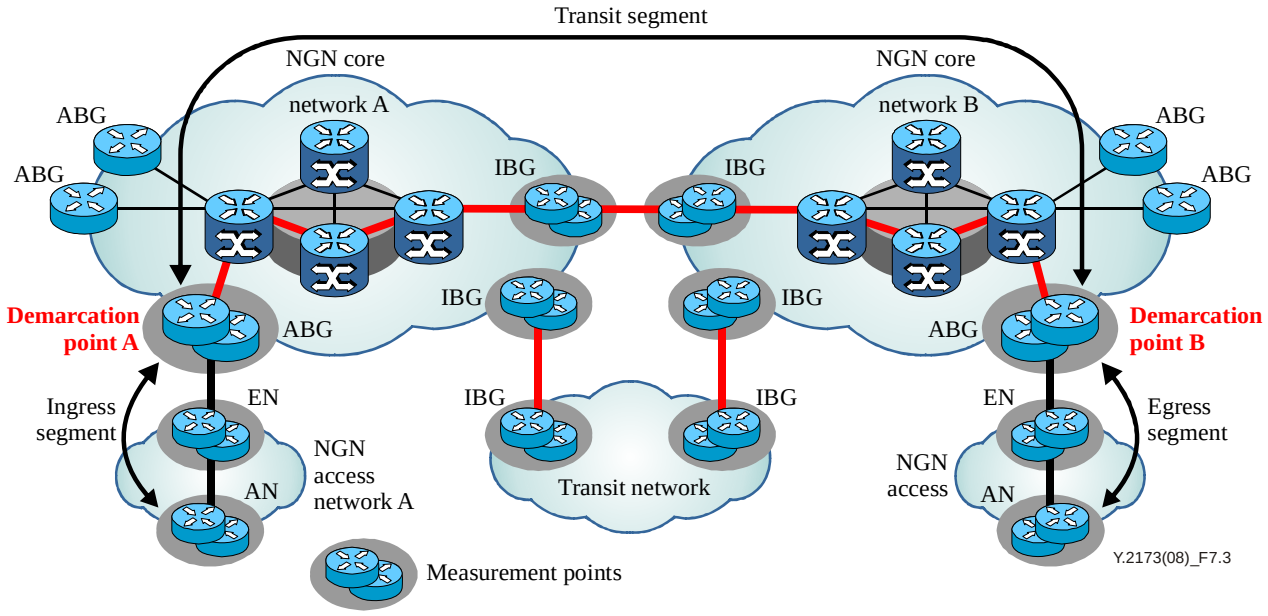

Figure 7-3 – Edge-to-edge model

In the edge-to-edge model depicted in Figure 7-3, delivery is assured to the CNE nearest to a customer; however, service between customer terminals or between the CPNE and the CNE is not assured. Depending on the situation, the ANE can also be a demarcation point. The assured performance characteristics of the network are comprised of the aggregate of the performance characteristics of the ingress, transit and egress segments.

The ingress and egress segments do not include the CPNE-ANE link, but do include the CNE as well as core network switching and transport.

The transit segment is measured from the demarcation point of the ingress NGN core transport provider to the demarcation point of the egress NGN core transport provider. This segment may or may not include separate NGN transit transport providers. The transit segment may span a city, country/state, continent or multiple continents.

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

The ingress, transit and egress segments are monitored from demarcation points that are specifically located for the role. Demarcation point selection is an NGN provider's choice. Each customer site is assigned to a demarcation point within its NGN regional provider's network. It is selected on the basis that the majority of the traffic from that site to others goes through this specific point, which is within the same geographic region as the customer site. There is a limited number of demarcation points based on the location of customer sites. NGN providers may increase the number of measurement demarcation points as they see fit, and some NGN providers may elect to make every CNE a measurement point.

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

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

- Each provider is required to provide measurement points that act as performance characteristic test points for their use, and for restricted use by other SPs.
- Measurement points are required to be located at every major service provider interconnection peering point.
- Measurement point (demarcation point) nominated by regional providers for each customer site is required to be provided.
- A service-dependent measurement point at CNE, CPNE and/or customer TE.

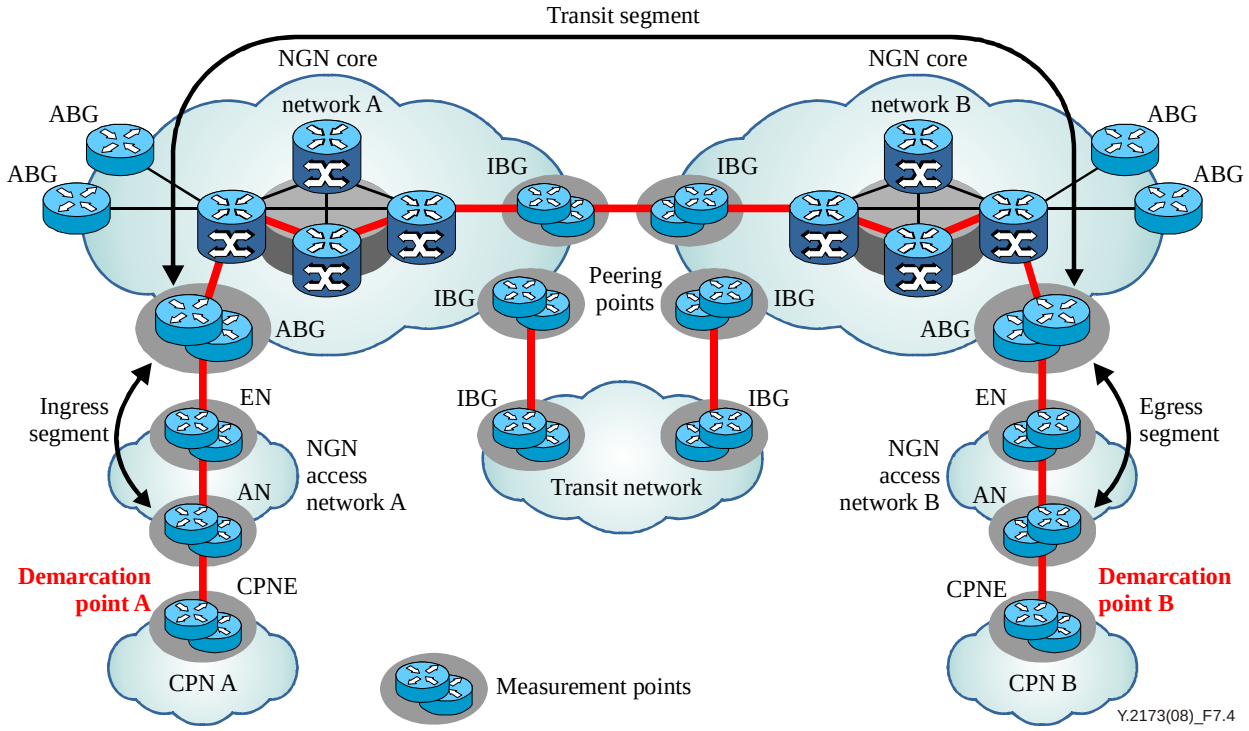

Figure 7-4 – Site-to-site model

In the site-to-site model, delivery is assured to customer CPNE, service between customer terminals and the CPNE is not assured by the service provider, it is the responsibility of the customer. The assured performance characteristics of the network are comprised of the aggregate of the performance characteristics of the ingress, transit and egress segments.

The ingress and egress segments include an access segment (DSL, cable, SONET/SDH, and Ethernet, etc.), including the CPNE as well as access network switching and transport.

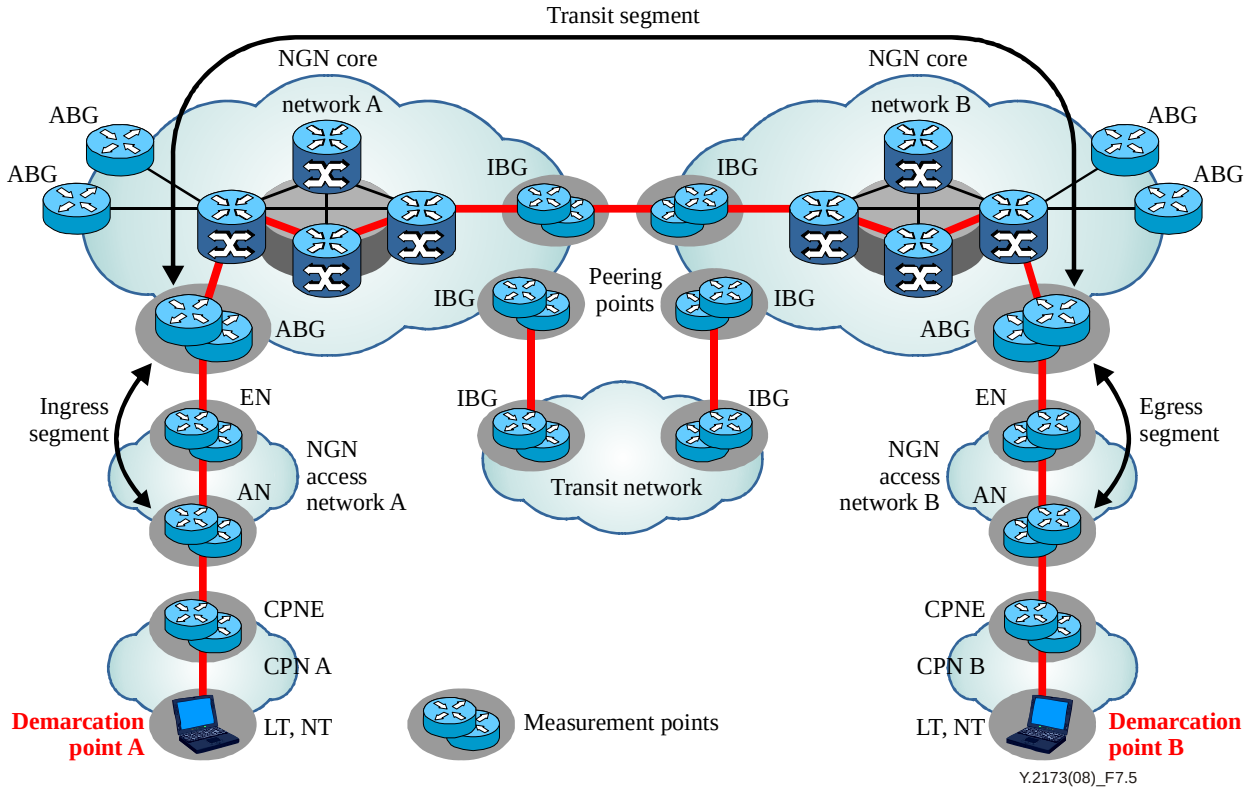

Figure 7-5 – TE-to-TE model

In the TE-to-TE model, the assured performance characteristics of the network are comprised of the aggregate of the performance characteristics of the ingress, transit, egress and customer segments.

The customer segment includes the network between a CPNE and a customer's TE. This may include home networking arrangements to company LANs, computers and appliances.

Selection of the customer's TEs to be used for measurements includes consideration of:

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 CPNE and a particular TE are representative of many other TEs. Call these "landmark" TEs.
5) Number of TEs probed:
   a) To minimize the number of probes, a minimum number of landmark TEs are required to be used.
   b) To minimize the complexity of data handling and reporting, a minimum number of landmark TEs are required to be used.

Communication from a CPNE to a TE may require 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 a measurement point as a proxy for TEs.

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

Since measurement endpoints are located either in the customer premises (e.g., for CPN) or in the premises of the network or service provider (e.g., for access network, core network or service provider network), the measurement model can be classified according to the location of the endpoints. Appendix I provides some example cases based on the location of the measurement endpoints.

Table 7-1 – Measurement models associated with measurement locations

Location of measurement endpoints	Measurement model	Measurement objectives
Customer-to-customer	CPNE-CPNE, LT/NT-LT/NT	Monitoring operational performance Resolving performance degradation
Customer-to-provider	LT/NT-AN, LT/NT-EN, LT/NT-ABG, LT/NT-SPE, CPNE-EN, CPNE-ABG, CPNE-SPE	Monitoring operational performance Monitoring SLA assurance Resolving performance degradation
Provider-to-provider	AN-AN, EN-EN, ABG-ABG, IBG-IBG	Monitoring operational performance Monitoring SLA assurance Testing and maintenance of performance Resolving performance degradation

8 Management architecture for performance measurement

8.1 Relationship with NGN management architecture and management processes

[ITU-T M.3050.x] contains a reference framework for categorizing the business activities that a service provider will use. This framework, which is also known as eTOM, describes the enterprise processes required by a service provider and analyses them to different levels of detail according to their significance and priority for the business. This business process approach has been built on the concepts of management services and functions in order to develop a framework for categorizing all the business activities.

[ITU-T M.3060] contains the management requirements, general principles and architectural requirements for managing next generation networks (NGNs) to support business processes to plan, provision, install, maintain, operate and administer NGN resources and services.

The architectural components, as described in this clause, and the procedures, as described in clause 9, can be viewed as specializations of the architectural components defined in [ITU-T M.3060] and of the management processes defined in [ITU-T M.3050.x]. The exact relationship between the MPM and [ITU-T M.3050.x]/[ITU-T M.3060] and the eventual MPM interfaces is for further study.

8.2 General architecture

Figure 8-1 depicts the overall architecture for the management of NGN performance measurement.

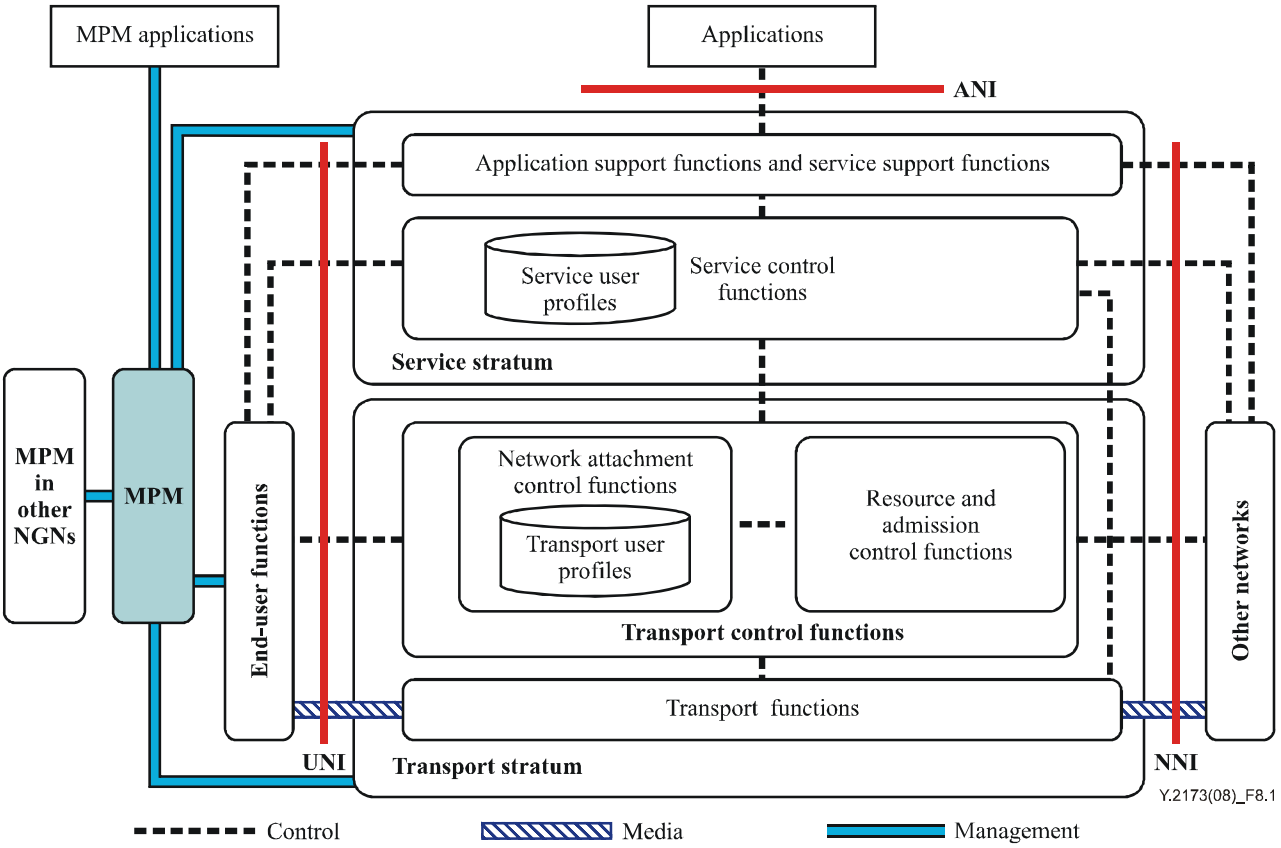

Figure 8-1 – Overall architecture for NGN performance management

The current NGN consists of transport, transport control, service control and application/service support functions. The first three functions are related with performance management in various aspects. Transport functions consist of access network functions, edge functions, core transport functions and gateway functions. They provide support for the transfer of media information, as well as the transfer of control and management information. Performance measurement and management of these functions are needed. Transport control functions consist of network access control and resource and admission control functions (RACFs). Especially, RACFs require reasonably accurate real-time network resource performance and usage data to enable effective resource-based admission control decisions. NGN performance management functions can provide such information to the RACF. Also, transport control traffic measurement is important for ensuring the performance of NGN transport control functionality. Service control functions include resource control, registration, and authentication and authorization functions at the service level for both mediated and non-mediated services. Service control traffic measurement is essential to ensure the quality of services offered and to account for their usage. Figure 8-1 illustrates the position of MPM in relation with the overall NGN architecture. It is one of the NGN management functions. It interacts with various NGN functional entities to collect and analyse performance of NGN networks and services. It can interact with transport functions for performance measurement of NGN transport services. It can interact with transport control functions for performance measurement of NGN transport control traffic. It can also interact with service control and application support functions for performance measurement of NGN application and service control traffic. The results of such measurements can be provided to MPM applications or MPM of other NGN providers for inter-domain NGN performance measurement. The mapping of the MPM functionality to the

management architecture [ITU-T M.3060] is for further study; however, it is anticipated that some functionality (e.g., PME-FE) of MPM can reside in the transport FEs as necessary. More details of MPM functions are described in the following clauses.

8.3 Functional architecture

The functional architecture shown in Figure 8-2 is the detailed view of the general architecture based on the requirements identified in clause 6.

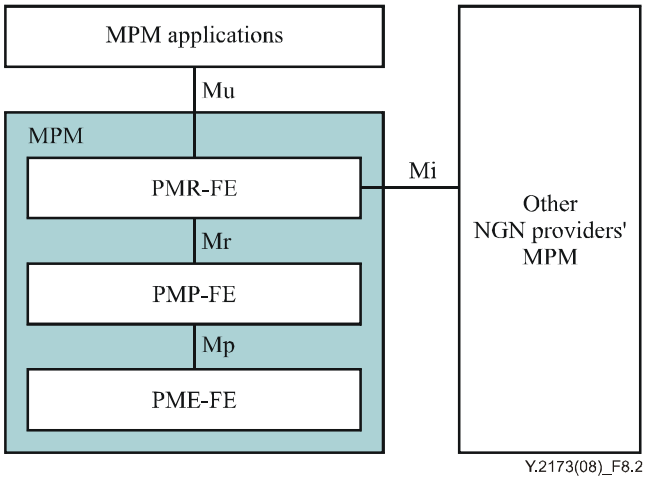

Figure 8-2 – Functional architecture for the management of NGN performance measurement

The architecture includes the following functional entities:

- Performance measurement execution functional entity (PME-FE)

  The PME-FE is responsible for three groups of functionality: measurement execution, single measurement processing and measurement device configuration. Measurement execution includes active probe initiation, active probe termination and passive measurement. Single measurement processing includes collection of time-stamped packets and calculation of the single probe delay and loss. Measurement device configuration includes configuration of measurement-related policies received from PMP-FE. More specifically, the PME-FE is responsible for:

  – Receiving configuration information from the PMP-FE via the Mp reference point.
  – Clock synchronization among functions.
  – Performance measurements, by initiating "per-class" active probes with the timestamp.
  – Time-stamping the received active probes and packets collected.
  – Suspending initiation of the probes and collection of packets and reporting to the PMP-FE via the Mp reference point if loss of clock synchronization occurs.
  – Processing the time-stamped probes and packets.
  – Generating a flow identification and packet identification for each captured packet.
  – Collecting time-stamped packets.
  – Calculating delay and loss of single probe under measurement based on the time-stamped packets.
  – Exporting single probe delay and loss results to PMP-FE via the Mp reference point.

- Performance measurement processing functional entity (PMP-FE)

  PMP-FE is responsible for two groups of functionality: measurement processing and network-wide measurement configuration. The measurement processing function includes measurement report collection, passive measurement report analysis, measurement data aggregation and rollup period analysis. It receives single measurement processing result from the PME-FE via the Mp reference point and sends the results of analysis to the PMR-FE via the Mr reference point. The network-wide measurement configuration function includes the creation of network-wide performance measurement configuration policies, the selection of appropriate measurement points at which to apply them, and the deployment of the policies into the measurement points. More specifically, it performs the following functions:

  – Collecting active measurement, passive measurement or spatial measurement reports from the PME-FE via the Mp reference point.
  – Performing flow-based passive measurement analysis using (for example) an RTP/RTCP-based scheme.
  – Collecting single probe delay and loss results from the PME-FE via the Mp reference point.
  – Calculating the rollup metrics including IPTD, IPDV, IPLR and IPUA, etc., based on single probe delay and loss results.
  – Exporting rollup metrics to the PMR-FE via the Mr reference point.
  – Performing measurement data aggregation to reduce the amount of data to be processed.
  – Performing correlation analysis among data received from various PME-FEs.

- Performance measurement reporting functional entity (PMR-FE)

  The PMR-FE collects rollup metrics from the PMP-FE via the Mr reference point and provides reports to MPM applications (e.g., RACF), or other NGN provider's MPM. It performs the following functions:

  – Collecting rollup metrics from the PMP-FE via the Mr reference point.
  – Reporting to MPM applications via the Mu reference point.
  – Requesting and responding to requests from other NGN providers' PMR-FE for network performance metrics via the Mi reference point.
  – Authenticating requests for initiation of measurements from MPM applications or other NGN providers, and initiating the requested measurements.

8.4 Reference points

8.4.1 Reference point Mi

The Mi reference point allows measured and analysed performance-related information to be exchanged between the intra/inter-provider performance reporting function and its counterpart in another NGN provider.

This reference point is required to carry the following information:

- Network-wide rollup period analysis report for MPM applications among NGN provider domains.
- Network-wide rollup period analysis report for MPM of other NGN provider domains.
- Acknowledgement of the receipt of transferred reports.
- IP addresses and other identification information to communicate among MPMs.

The reference point is required to support the following capabilities:

- Request/response transactions.
- Notifications of asynchronous events.
- Reliable and secure delivery of messages.
- One-to-many and many-to-one operation modes.

The Mi reference point is an inter-domain reference point. The additional security considerations for such a reference point in clause 10 apply.

8.4.2 Reference point Mu

The Mu reference point allows measured and analysed performance-related information to be exchanged between PMR-FE and MPM applications (e.g., RACF). Note that the extensions to RACF to support Mu are for further study.

This reference point is required to carry the following information:

- Network-wide rollup period analysis report for MPM applications within the same NGN provider domain.
- Acknowledgement for the report transfer receipt.
- The description of media flows to measure performance.

The reference point is required to support the following capabilities:

- Request/response transactions.
- Notifications of asynchronous events (e.g., PMP-FE or PME-FE failure).
- Reliable and secure delivery of messages.
- One-to-many and many-to-one relationships between the PMR-FE and an MPM application.

The Mu reference point is an intra-domain reference point.

8.4.3 Reference point Mr

The Mr reference point allows processed performance information to be exchanged between PMP-FE and PMR-FE. It also allows network-wide configuration information for active and passive measurement to be exchanged between PMR-FE and PMP-FE.

This reference point is required to support transfer of the following information in real-time:

- Analysed and processed measurement report based on active measurements and/or passive measurements (e.g., concatenated multiple single measurement reports).
- Acknowledgement of report delivery.
- Source network segments to be measured.
- Destination network segments to be measured.
- Source measurement points for active measurement.
- Destination measurement points for active measurement.
- Specific measurement points for passive measurement.
- Specific media flows to be measured.
- Frequency of network-wide measurement.
- Initiation times.
- Termination times.
- QoS classes.

- Metering policy (e.g., based on the 5-tuple information or source IP address) for passive measurement.
- Acknowledgement of network-wide configuration information delivery.

This reference point is required to support the following capabilities:

- Request/response transactions.
- Notifications of asynchronous events.
- Reliable and secure delivery of messages.
- One-to-many and many-to-one operation modes.

The Mr reference point is an intra-domain reference point.

8.4.4 Reference point Mp

The Mp reference point allows the results of multiple and single active and passive measurements to be exported to PMP-FE from PME-FE. It also allows device-specific configuration information for active and passive measurement to be exchanged between PMP-FE and PME-FE.

This reference point is required to able to support the exchange of the following information:

- Delay reports of single active/passive measurements.
- Delay variation reports of a single active/passive measurements.
- Loss reports of single active/passive measurements.
- Source measurement points for active measurement.
- Destination measurement points for active measurement.
- Specific measurement points for passive measurement.
- Frequency of a single measurement.
- Initiation times.
- Termination times.
- QoS classes.
- Metering policy for passive measurement.
- Acknowledgement of device configuration status.
- Description of media flows.
- Other metrics reports of passive measurement (e.g., throughput, traffic volume per QoS class, packets per second (PPS), bytes per second (BPS), flows per second (FPS), RTCP information).

This reference point is required to support the following capabilities:

- Request/response transactions.
- Notifications of asynchronous events.
- Reliable and secure delivery of messages.
- One-to-many and many-to-one operation modes.

The Mp reference point is an intra-domain reference point.

9 Procedures

This clause describes three procedures for NGN inter-domain performance measurement. The first procedure is for the discovery of measurement functional entities. The second procedure is for the initiation of actual measurements once the necessary measurement functional entities have been

found. The third procedure is for communication among performance measurement reporting functional entities (PMR-FEs).

9.1 Discovery

For various performance measurements, NGN providers need to be able to locate the following entities belonging to other NGN providers:

1) PMR-FE.

2) PME-FE at demarcation points.

3) CPNE/ANE/CNE/SPE.

9.1.1 Locating PMR-FE

The IP address of the performance measurement reporting functional entity is required to be listed in a registry, identifying the AS numbers, provider name and contact information (note that existing tools may be used to relate customer prefixes to AS numbers and hence to a related PMR-FE).

Although PMR-FE addresses or related information are not expected to change frequently, a registration update procedure provided in clause 9.3.1 is used to notify its address or related information change to other PMR-FEs with which it has contact.

9.1.2 Locating PME-FEs

The PME-FEs of other providers whose IP addresses are required to be located are:

1) The PME-FE in the demarcation point associated with the destination site (e.g., demarcation point B in Figure 9-1).
   a) This may be used to measure the total transit segment by the source access network provider.
   b) It is located by asking the PMR-FE associated with the destination site for its IP address (this seems preferable to listing demarcation points in the registry).

2) The PME-FE on the far side of a peering link (e.g., NGN transit provider C needs to know about IBG3 in Figure 9-1).
   a) This is needed for each provider to measure its own performance (assuming that it is responsible for the performance of egress traffic over a peering link) by measuring from an ingress peering measurement point to the PME-FE on the far side of a peering link.
   b) Since there may be multiple peering links among providers, the determination of which pair of measurement points is required to be monitored is important. The pair is required to be identified by the destination address. The method of doing this is left to the provider doing the measurement.

Measurement demarcation point addresses or related information are not expected to change frequently; however, a registration update procedure provided in clause 9.3.1 is used to notify its address or related information change to other PMR-FEs with which it has contact.

9.1.3 Locating CPNE/ANE/CNE/SPEs

NGN providers need to be able to find the location of CPNE/ANE/CNE/SPEs of other NGN providers so that occasional measurements may be taken between measurement points, CPNEs or ANE/CNEs of one provider to CPNEs or ANE/CNEs of the destination provider. The IP address of a CPNE/ANE/CNE/SPE associated with a destination prefix is located by asking the PMR-FE associated with the destination site (this seems preferable to listing CPNE/ANE/CNE/SPEs in the registry).

CPNE/ANE/CNE/SPE addresses or related information are not expected to change frequently; however, a registration update procedure provided in clause 9.3.1 is used to notify its address or related information change to other PMR-FEs with which it has contact.

IP address-information of LT, TE and CPNE, for example, can be provided by the service control function (SCF) to the MPM.

9.2 Initiation of measurements

While the segmentation of the network enables scalability through re-use of probes for many purposes, initiating a full mesh of measurements among measurement points globally is unlikely to be practical. Therefore, the initiation of measurements must be such that most of the measurements taken are actually required. Requests for the initiation of inter-provider measurements may be issued by any provider; these authenticated requests are required to be granted according to each provider's policy.

Measurements may be initiated independently of customers' traffic, for example, when they sign up for service to other particular sites; and/or dynamically when an "access" provider sees customer traffic going to a subscribing third party across other providers' networks which support inter-domain performance levels.

MPM applications (e.g., RACF or SCF) send requests to MPM in order to initiate the measurements.

Before describing the procedure, the nine measurements required for the scenario in Figure 9-1 are reviewed below.

As described in clause 7.2 of [ITU-T Y.1543], measurements are made for operating, supporting and testing purposes. The procedures for the initiation of each are described below.

Operating measurements between site A CPNE and site B CPNE require measurements in the following segments:

1) CPNE A and demarcation point A, bidirectionally (access segment).
2) Demarcation point A and demarcation point B, bidirectionally (total transit segment).
3) Demarcation point B and CPNE B, bidirectionally (access segment).

For troubleshooting purposes, measurements are required from:

4) Demarcation point A to IBG2 (egress transit traffic across provider A).
5) IBG1 to demarcation point A (ingress transit traffic across provider A).
6) IBG2 to IBG3 (egress transit traffic across provider C).
7) IBG4 to IBG1 (ingress transit traffic across provider C).
8) Demarcation point B to IBG4 (egress transit traffic across provider B).
9) IBG3 to demarcation point B (ingress transit traffic across provider B).

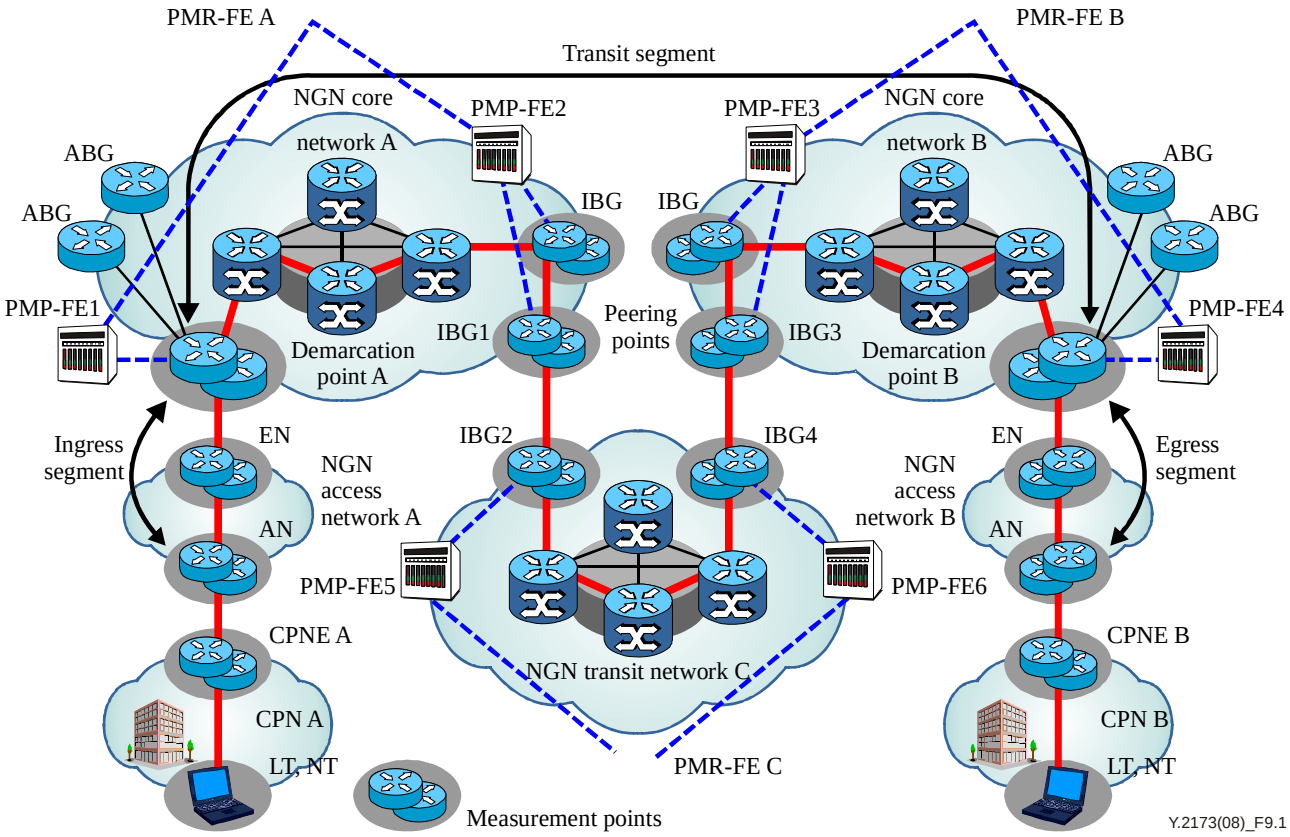

Figure 9-1 – Communications among PMR-FEs, PMP-FEs and measurement points

For a dynamic initiation of measurements, the following high-level procedure is applied. The measurement numbers identified below (e.g., 1, 2) refer to the measurements as numbered above in Figure 9-1.

1) PMR-FE A sees new destination prefixes for which measurements are required to be initiated (method left up to provider A).

2) PMR-FE A determines which other providers' networks the traffic will cross (method left up to provider A).

3) PMR-FE A learns the PMR-FE addresses of the other providers' networks the traffic will cross (from registry).

4) PMR-FE A contacts PMR-FE B and:

   a) Provides PMR-FE A address.

   b) Provides PMR-FE C address.

   c) Provides destination address and determines whether it is a subscriber to this service; if not, then requests PMR-FE A to abort the set-up sequence.

   d) Requests the IP address of the measurement point associated with the destination prefix.

   e) Requests that the above operating measurements be sent to PMR-FE A periodically.

   f) Requests that the above non-compliant supporting measurements be sent to PMR-FE A.

   g) Requests that any non-compliant customer use be sent to PMR-FE A.

   h) Requests that any fault events relating to these measurements be sent to PMR-FE A.

5) PMR-FE A initiates measurements 1, 2, 4 and 5.

6) PMR-FE B initiates measurements 3, 8 and 9.

7) PMR-FE A contacts PMR-FE C and:

   a) Provides PMR-FE A address.

   b) Provides PMR-FE B address.

   c) Provides destination address.

   d) Requests that non-compliant supporting measurements be sent to PMR-FE A.

   e) Requests that fault events relating to these measurements be sent to PMR-FE A.

8) PMR-FE C initiates measurements 6 and 7.

Note that it is assumed the routing used assures that only service providers which support the requested service are considered in the above.

Once a measurement has been initiated due to a request, it is required to exchange the duration and interval of measurements. For applications such as service level agreement verification, it is recommended that measurements be continued for two months. It is recommended that refresh requests be sent monthly for as long as the requesting provider wants the measurements. Note that a PMR-FE needs to keep track of which other PMR-FEs asked for which measurements and when.

9.3 Communications among registry and PMR-FEs

This clause names and describes the procedures for communications among the registry and the PMR-FEs, and how they are used. Following "registration", three phases are defined which are named "initiation", "measurement" and "shutdown".

9.3.1 Registration procedure

Each PMR-FE is responsible for initially registering or updating its own IP address in the registry. The registry is responsible for responding to authenticated PMR-FE requests to administer their IP addresses, and for providing those IP addresses to other PMR-FEs. Figure 9-2 describes the registrations procedure in detail.

Registration procedure requests and responses are described below:

Registry_IP_update_Request – Request from a PMR-FE A to registry to set its IP address (or related information).

Registry_IP_update_Response – Response from registry to request from a PMR-FE A to registry to set its IP address (or related information).

Registry_IP_access_Request – Request from PMR-FE B to registry for the IP address of PMR-FE A (or related information).

Registry_IP_access_Response – Response from registry to request from PMR-FE B to registry for the IP address of PMR-FE A (or related information).

Registry_update – Following a PMR-FE A update of its IP address (or related information), this response update is sent from registry to PMR-FEs (functionally, a broadcast) that have previously sent requests to registry for the IP address of PMR-FE A.

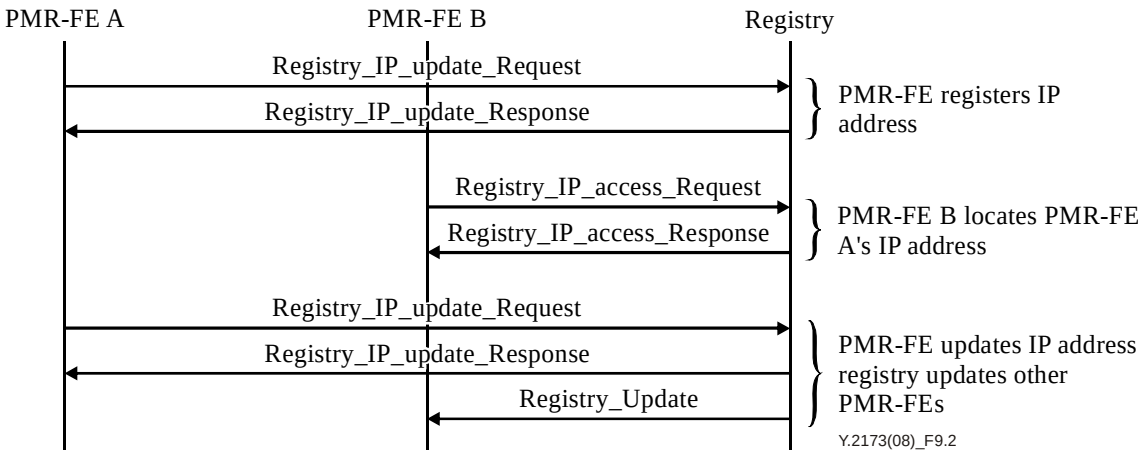

Figure 9-2 – Registration procedure

Successful registration must be completed by all PMR-FEs along a path prior to measurements along that path being initiated.

The initiation, measurement and shutdown phases occur following a provider's determination of:

1) A new destination prefix for which measurements might be initiated.
2) Which other providers' networks the traffic will cross to that destination.
3) Location of addresses of intermediate and destination PMR-FEs using the registry.

9.3.2 Initiation phase procedure

Before measurements are started, the PMR-FE that is the source of the measurement request (source PMR-FE) must first:

1) Confirm that the destination IP is a valid measurement point under the control of the destination PMR-FE.
2) Provide details of the measurement request to intermediate and destination PMR-FEs.
3) Receive responses indicating successful initiation.

Initiation phase procedure requests and responses are described below:

Query_CustomerIP_Request – Query the destination PMR-FE to see if the destination IP address is a valid measurement point under its control.

Query_CustomerIP_Response – Destination PMR-FE response to **Query_CustomerIP_Request**.

Query_DestinationIP_Request – Ask destination PMR-FE to identify the IP address of their appropriate measurement point.

Query_DestinationIP_Response – Destination PMR-FE response to a **Query_DestinationIP_Request**.

Start_Performance_Measurement_Request – Ask a PMR-FE along the path to initiate or allow measurements for a measurement segment.

Start_Performance_Measurement_Response – PMR-FE response to a **Start_Performance_Measurement_Request**.

9.3.3 Measurement phase procedure

Following successful completion of the initiation phase, the measurement phase occurs which includes:

1) Conduct of measurements over the requested network segments.

2) Distribution of reports to the source PMR-FE by the intermediate and destination PMR-FEs.

3) Maintenance due to changes in measurement elements or customer subscriptions.

Measurement phase procedure requests and responses are described below:

Performance_Metric_Report – Periodic report of performance metric values or response to Query_Performance_Metric_Request.

Query_Performance_Metric_Request – Ad hoc request for a performance report.

There are some cases when measurement point IP address is required to be changed, or the measurement point is no longer valid. Requests and responses related to maintenance during the measurement phase are the following:

DestinationIP_Change_Notification – Destination PMR-FE sends notification to source PMR-FE which relays to transit PMR-FEs.

DestinationIP_Change_Confirmation – Response to DestinationIP_Change_Notification.

9.3.4 Shutdown phase procedure

The shutdown phase may occur following:

1) Timeout of refresh requests from source PMR-FE no longer being received.

2) Source PMR-FE no longer requires measurement.

3) Destination measurement point is no longer valid.

4) Any providers on selected path no longer support measurement.

5) MPM applications send requests to MPM in order to stop the measurements.

The request and response involved in shutdown include:

Stop_Performance_Measurement_Request – Source PMR-FE's request message to all PMR-FEs engaged in the measurement to stop measurement.

Stop_Performance_Measurement_Response – Response to a Stop_Performance_Measurement_Request.

Initiation, measurement and shutdown procedures are shown in Figure 9-3.

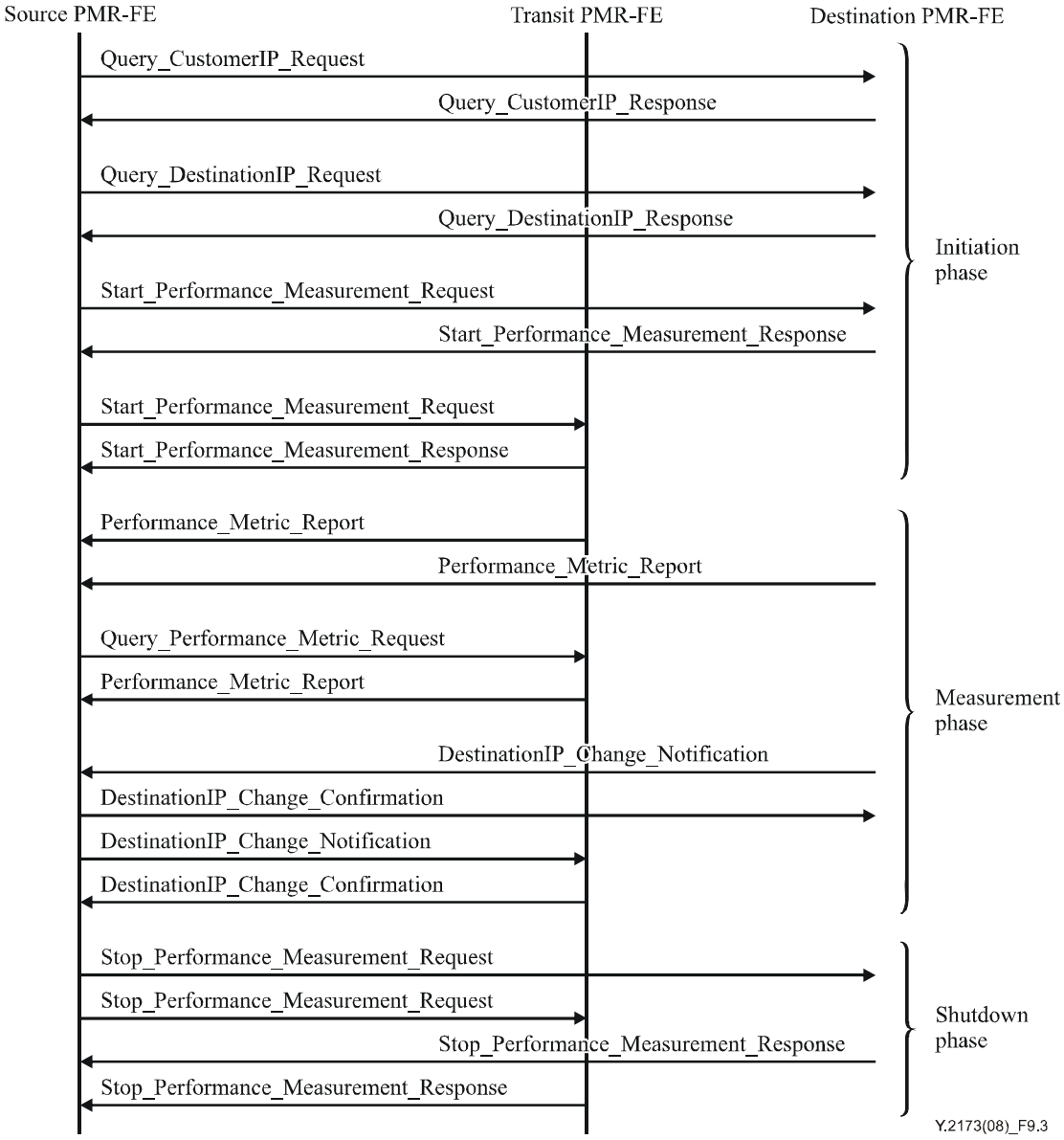

Figure 9-3 – Initiation, measurement and shutdown procedures

9.3.5 Requests and responses for initiation, measurement and shutdown procedures

Identification of measurements among PMR-FEs is based upon defining particular measurement segments and network service classes. A measurement flow can be identified by source IP address, destination IP address and network QoS class.

There are nine measurement segments in Figure 9-4. The source network has four for which it is responsible, whereas a transit network has two and a destination network has three.

In the request and responses below, Flow_Identification and Measurement_SegmentID are defined as follows:

Flow_Identification consists of {SourceIP, DestinationIP, Class}.

Measurement_SegmentID can be abstracted as:

a) Upstream IBG to downstream peer IBG (unidirectional measurement).

b) Downstream IBG to upstream peer IBG (unidirectional measurement).

c) Upstream IBG to downstream IBG (unidirectional measurement).

d) Downstream IBG to upstream IBG (unidirectional measurement).

e) Access: ABG to CPNE (bidirectional measurements).

f) Far-end IBG to downstream IBG (bidirectional measurements from a specified address to a downstream IBG).

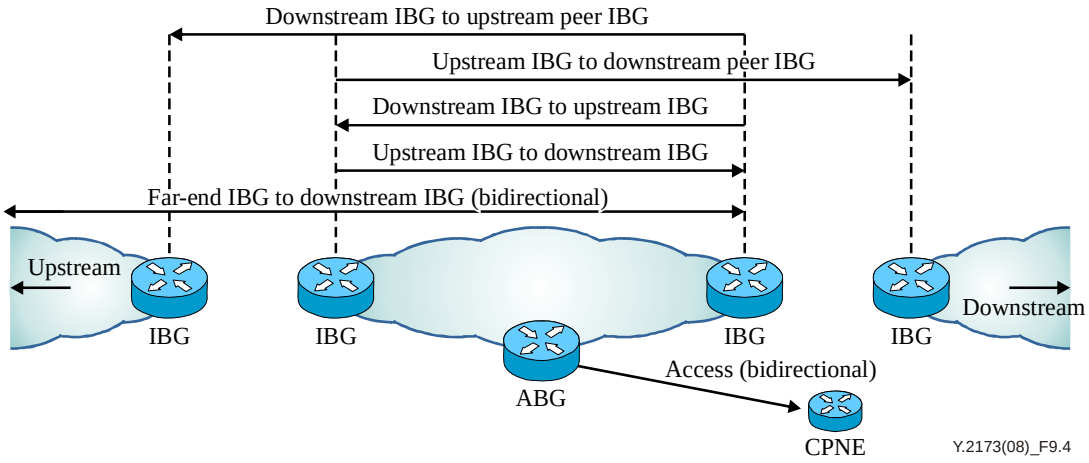

Figure 9-4 – Abstracted measurement segments

The above abstraction relates to the measurements identified in Figure 9-1 as follows:

1) Site A CPNE A and demarcation point A = access (bidirectional measurements).

2) Demarcation point A to demarcation point B = far-end to downstream (bidirectional measurements).

3) Demarcation point B and CPNE B = access (bidirectional measurements).

4) Demarcation point A to IBG2 = upstream to downstream peer (unidirectional measurements).

5) IBG1 to demarcation point A = downstream to upstream (unidirectional measurements).

6) IBG2 to IBG3 = upstream to downstream peer (unidirectional measurements).

7) IBG4 to IBG1 = downstream to upstream peer (unidirectional measurements).

8) Demarcation point B to IBG4 = downstream to upstream peer (unidirectional measurements).

9) IBG3 to demarcation point B = upstream to downstream (unidirectional measurements).

Note that communications with other PMR-FEs are only required regarding measurements within a source network when those measurements are requested by other PMR-FEs. So, in the case of the above nine measurements, no inter-PMR-FE communication is required for measurements 1 and 5. Note that measurement 4 requires inter-PMR-FE communications to obtain permission and the IP address of IBG2 from PMR-FE C.

There are three elements common to all request and responses:

InvokeID: Uniquely identifies the request/response, respectively, or request/response pair. The InvokeID of request-response and notification-confirmation pairs are required to be identical.

Invoking_PMR-FE/Reg: PMR-FE or registry IP address that sends this message.

Invoked_PMR-FE/Reg: PMR-FE or registry IP address that receives this message.

9.3.5.1 Registry_IP_update_Request

1) Description: Request to set the IP address associated with a PMR-FE.
2) Direction: From PMR-FE A to registry.
3) Elements:
   a) PMR-FE unique ID.
   b) AS numbers.
   c) Contact information.
   d) Period during which this IP address is valid.

9.3.5.2 Registry_IP_update_Response

1) Description: Response to Registry_IP_update_Request.
2) Direction: From registry to PMR-FE A.
3) Elements:
   a) OK_NOK.
   b) NOK reason code.

9.3.5.3 Registry_IP_access_Request

1) Description: Request for IP address associated with PMR-FE B.
2) Direction: From PMR-FE B to registry.
3) Elements: AS number.

9.3.5.4 Registry_IP_access_Response

1) Description: Response to Registry_IP_access_Request.
2) Direction: From registry to PMR-FE B.
3) Elements:
   a) IP address of requested PMR-FE.
   b) Period during which this IP address is valid.
   c) Contact information.

9.3.5.5 Registry_IP_update

1) Description: Following an update by a PMR-FE of its IP address (or other info) in the registry, this is a response to previously received Registry_IP_access_Request for that PMR-FE's IP address (functionally, this is a broadcast request).
2) Direction: From registry to PMR-FEs.
3) Elements:
   a) List of elements that have been updated.
   b) Old IP address of requested PMR-FE.
   c) New IP address of requested PMR-FE.
   d) Old period during which this IP address is valid.
   e) New period during which this IP address is valid.
   f) Old contact information.
   g) New contact information.

9.3.5.6 Query_CustomerIP_Request

1) Description: Query whether the customer IP prefix belongs to a subscriber of the destination network.
2) Direction: From source PMR-FE to destination PMR-FE.
3) Elements:
   a) Customer_IP_Prefix.
   b) Set of queried network QoS classes.

9.3.5.7 Query_CustomerIP_Response

1) Description: Response to Query_CustomerIP_Request.
2) Direction: From destination PMR-FE to source PMR-FE.
3) Elements: Set of OK_NOK for requested network QoS classes.

9.3.5.8 Query_DestinationIP_Request

1) Description: Query for the IP address of the measurement point at either the demarcation point, CPNE, ANE, CNE or SPE of the destination network.
2) Direction: From source PMR-FE to destination PMR-FE.
3) Elements:
   a) Customer_IP_Prefix.
   b) System_Type: Demarcation point/CPNE/ANE/CNE/SPE.

9.3.5.9 Query_DestinationIP_Response

1) Description: Response to Query_DestinationIP_Request.
2) Direction: From destination PMR-FE to source PMR-FE.
3) Elements:
   a) OK_NOK.
   b) DestinationIP.

9.3.5.10 Start_Performance_Measurement_Request

1) Description: Request for PMR-FE to start or allow performance measurements.
2) Direction: From source PMR-FE to destination or transit PMR-FE.
3) Elements:
   a) Flow_Identification: Uniquely identifies the target measurement flow (SourceIP, DestIP, Class).
   b) Measurement_SegmentID: Indicates which Measurement-segment is required to be performed (upstream→downstream, upstream→downstream peer, downstream→upstream, downstream→upstream peer, access or far-end to downstream).
   c) MetricID list: Lists the requested metrics that are to be measured and reported.
   d) Destination_Or_Transit_Flag: Indicates whether the network the target PMR-FE belongs to is destination or transit.
   e) UpstreamPeer_PMR-FE_Address: PMR-FE address of the adjacent upstream network.
   f) DownstreamPeer_PMR-FE_Address: PMR-FE address of the adjacent downstream network. Null for destination PMR-FE.
   g) Report_Frequency: Desired report frequency. The right to decide the report frequency is up to the target PMR-FE.

h) Probe_Injection_Frequency (applicable only for active measurement): Frequency of probe injection.

i) Measurement_Frequency (applicable only for passive measurement): Frequency of measurement at each passive measurement point.

j) Backward_Injection_Flag: Setting this flag to 1 means to request backward measurement. For a unidirectional test, this flag is required to be 0.

k) Start_Time: Null start-time means 'right now'.

l) Allow_Inform: Indicates that the target PMR-FE is being asked to allow the probe to enter the target provider's domain and be responded to by a measurement point, plus to inform the source PMR-FE of any IPaddress change of that measurement point.

m) Non-compliant customer report: Indicates if a report of the number of occurrences of a customer's SLA violations is required to be sent.

n) Fault event request: Indicates if a report is required to be sent when the performance of PMR-FE measurement system is below an expected level.

9.3.5.11 Start_Performance_Measurement_Response

1) Description: Response to Start_Performance_Measurement_Request.

2) Direction: From destination or transit PMR-FE to source PMR-FE.

3) Elements:

a) OK_NOK.

b) Reason_For_NOK (e.g., capability not supported, no such flow in transit network).

c) Backward_Injection_Flag: From destination PMR-FE. Indicates whether backward injection is possible or not.

d) List of {MetricID, OK_NOK}: For each performance metric, indicates whether the measurement of that metric is supportable or not.

e) Report_Frequency: May be different from that of Start_Performance_Measurement_Request.

f) Duration: Period of time for which the responding PMR-FE agrees to measure, notify and provide reports.

9.3.5.12 Query_Performance_Metric_Request

1) Description: Query performance values measured between From_Time and To_Time. This message can be requested on demand by the requesting PMR-FE. Report of performance value is initiated by destination or transit PMR-FEs periodically.

2) Direction: From source PMR-FE to destination or transit PMR-FE.

3) Elements:

a) Request_Mode (either bulk mode or single mode):

i) Bulk_Mode: Request for report for all measurements made by the target PMR-FE for the source PMR-FE.

ii) Single_Mode: Request for report for a particular flow and measurement segment.

b) Flow_Identification: Only if the Request_Mode is Single_Mode.

c) Measurement_SegmentID: Only if the Request_Mode is Single_Mode.

d) From_Time, To_Time.

9.3.5.13 Performance_Metric_Report

1) Description: Periodic report of performance metric values or response to Query_Performance_Metric_Request. InvokeID is NULL for periodic report.

2) Direction: From destination or transit PMR-FE to source PMR-FE.

3) Elements:

   List of {Flow_Identification, Start_Time, Stop_Time,

   1) List of {Measurement_SegmentID, Problem_Code,

      i) List of {MetricID, Metric_Value}}}: If this Problem_Code is not 0, it indicates that there was some problem, for example, reroute_occurred or MP_failure; thus, the metric values are not trustworthy.

9.3.5.14 DestinationIP_Change_Notification

1) Description: Notification that IP address of the destination measurement point has changed. This means that source and transit PMR-FE are required to re-target the route of this flow. Upon receiving this request, source PMR-FE is required to relay it to transit PMR-FEs. This request must be re-sent periodically (every 3 seconds) to the source PMR-FE until a confirmation message is received.

2) Direction: From destination PMR-FE to source PMR-FE or from source PMR-FE to transit PMR-FE.

3) Elements:

   a) Flow_Identification.

   b) New_DestinationIP.

   c) Date and time, when the address change will or did occur.

9.3.5.15 DestinationIP_Change_Confirmation

1) Description: Confirmation to DestinationIP_Change_Notification.

2) Direction: From source PMR-FE to destination PMR-FE or from transit PMR-FE to source PMR-FE.

3) Elements: New_Flow_Identification.

9.3.5.16 Stop_Performance_Measurement_Request

1) Description: Request to stop performance measurement. No response is needed.

2) Direction: From source PMR-FE to destination and transit PMR-FE.

3) Elements:

   a) Flow_Identification: Uniquely identifies the target flow.

   b) Measurement_SegmentID: On which measurement segment measurements are required to stop.

   c) Stop_IPaddress_Updates: Relieves the destination PMR-FE of notifying the source PMR-FE of subsequent IP address changes of measurement equipment until the next Start_Performance_Measurement_Request is received from that source PMR-FE.

9.3.5.17 Stop_Performance_Measurement_Response

1) Description: Response to Stop_Performance_Measurement_Request.

2) Direction: From destination or transit PMR-FE to source PMR-FE.

3) Elements:

a) Flow_Identification: Uniquely identifies the target flow.

b) Measurement_SegmentID: On which measurement segment measurements have stopped.

9.4 Timing requirements of procedures

Table 9-1 specifies the message timing required between providers, and between providers and the registry.

Table 9-1 – Timing requirements related to management requests and responses

Parameter	Action	Requirement	Comment
RP_latency	Latency time following rollup period to distribute rollup period report to other providers	10 minutes max	Where exchange is previously agreed
IP_setup	Lead time to update registry with new address information prior to changing address	1 hour min	Applies to PMR-FE and measurement points
Sync_out_latency	Latency time following detection of loss of sync until indicated in response to probes to other providers	1 second max	
InterP-Probe_request_latency	Latency time following inter-provider request to allow probe until a response is sent	1 second max	
Misc_request latency	Latency time following provider request for miscellaneous information until a response is sent	1 second max	
InfraP-Probe_request_latency	Latency time following inter-provider request for provider's internal measurement until a response is sent	1 second max	
Cust_compliance_latency	Latency time following inter-provider request for customer non-compliance report until a response is sent	1 second max	
Provider_compliance latency	Latency time following inter-provider request for provider non-compliance report until a response is sent	1 second max	
Registry_IP_access_latency	Latency time for registry to respond to IP address request	1 second max	
Registry_IP_update_latency	Latency time for registry to respond to update IP address request	1 second max	
Registry_update_latency	Latency time for registry to send update response to prior requesters following IP address update	10 seconds max	
Misc_update_setup	Lead time to update prior inter-provider requesters with new information prior to change in information	1 second max	

10 Security consideration and requirements

This clause describes security threats, potential attacks, impacts on performance of the measurement, and other important security considerations. It also defines security requirements for performance measurement and management. These security considerations and requirements are based on [ITU-T X.805] and the security requirements for NGN release 1 [ITU-T Y.2701].

10.1 Potential threats and attacks

Examination of the five threat categories, destruction, corruption, removal, disclosure and interruption as they relate to measurement and management, yields the following:

Destruction of information

This threat is defined to be the potential erasure of data pertaining to the management operations for performance measurement such as information stored on the PMR-FE system or registry. An example of potential consequences is that, when the information about the measurement of a particular period of time has been destroyed, a proper measurement calculation cannot effectively be made.

Corruption or modification of information

This threat can be categorized as follows:

1) Corruption of the recorded registry information so that such data are rendered meaningless or unusable. This can result in a total loss of measurement information, which is in itself a threat to the reliability of the performance management functionality.
2) Undetected modification of the recorded resource information or policy rules so that such data appear to be meaningful. An example is "undetectable changes in contents, such as the timestamp or clock sync monitor". This can result in producing inaccurate performance monitoring information.
3) Other types of the threat are as follows:
   - Acceptance of unauthorized requests for measurement reports.
   - Acceptance of unauthorized requests for customer subscription information.
   - Acceptance of unauthorized reports.
   - Different routing of probes versus regular traffic in the same QoS class.
   - Delaying/accelerating probes versus regular traffic in the same QoS class.

Theft, removal or loss of information and/or other resources

This threat refers to the potential theft or loss of recorded repository information such as customers' subscription information, measurement information, etc., or other physical resources. For the purposes of this Recommendation, it is assumed that the host security will be maintained by the provider per existing security policies.

Disclosure of information

This can take place because of the interception of the signalling messages between MPM systems or because of granting access to an illegitimate user. The consequence is the same, as in the case of theft, removal or loss of information. Some examples are as follows:

- Unauthorized disclosure of customer subscription information.
- Unauthorized disclosure of measurement report information.
- Unauthorized disclosure of MPM system or measurement point IP addresses.

Interruption of services

This threat is typically realized through a denial of service (DoS) attack. Such attacks can make the measurement devices partially or totally unavailable. Some examples of such threat are as follows:

- Acceptance and processing of misdirected probes.
- An unexpectedly huge number of probes impinging a measurement point.
- An unexpectedly huge number of requests impinging a measurement device.
- An unexpectedly huge number of response updates.
- Acceptance of unauthorized requests for initiation of measurements.
- Registry unavailability.
- Measurement device unavailability.
- Measurement point unavailability.
- Disruption of the distributed "time".
- Disruption of the measurement system.
- Huge sustained packet loss.

10.2 Security impact on measurement performance

The strength of security measures used in a solution can burden systems, and/or cause extra security-related traffic.

Implementation of authentication and data integrity into the measurement probing messages would require additional overhead on the measurement devices. Depending on the number of probing messages, this could impact the measurement devices with the overhead caused by this operation.

Authentication could be done on the measurement device itself or off-loaded to another system. It is recommended that authentication be on the measurement device itself since that would reduce security-related network traffic.

10.3 Scope consideration

This Recommendation uses [ITU-T X.805] as the architecture basis for NGN security solutions. Inter-provider measurement information transfers are the points to be secured.

The inter-provider measurement information transfers have dependencies upon systems whose security methods are not covered here.

1) Distributed time is important in the accuracy of measurements and logging. However, the security of the time sub-system is considered to be beyond the scope of this Recommendation.
2) Inter-provider measurements and management depend on the availability of providers' measurement and management systems. Methods to secure the host aspects of these systems are considered to be beyond the scope of this Recommendation.
3) Inter-provider measurements and management depend on the underlying transport network whose security aspects are considered to be beyond the scope of this Recommendation.

Also, it is assumed that the end-user plane, control plane, infrastructure layer and services layer are secured per the policies of the providers. It is considered outside the scope of this Recommendation to address end-user plane, control plane, infrastructure layer or services layer security.

The management security plane is concerned with the protection of OAM functions of the network elements, transmission facilities, back-office systems (operations support systems, business support systems, customer care systems, etc.) and data centres. The management plane supports the fault, capacity, administration, provisioning and security (FCAPS) functions. The management plane is

considered to be the appropriate location for where the information transfers would take place. Thus, for the purposes of this Recommendation, the management plane is the only applicable security plane.

Lastly, for the purposes of this clause, it is considered that all measurement and management reports and information fall under the application security layer, which is defined by [ITU-T X.805]. The information transfers fall into the application security layer.

10.4 Security requirements

In order to protect the management functionality for performance measurement from the potential threats and attacks described above, this clause identifies major security requirements from the viewpoints of the eight security dimensions and five threats.

10.4.1 Requirements from security dimensions viewpoint

- Access control
  - Only authorized probes can have access to measurement points.
  - It is required that only authorized provider MPM systems should be able to request measurement information, query the registry or request additional information from another provider's MPM system.
  - It is required to limit the ability of unauthorized systems or users from requesting potentially sensitive information that could be used to expose vulnerability.
  - Information from authorized systems is required to be accepted.
  - It is required that protection against spoofing must be provided.
- Authentication
  - It is required that only trusted systems have access to measurements, reports and additional information.
  - Identity of system requesting information is required to be verified.
  - Registry access is required to be limited to trusted resources.
  - Identity for measurement probes sent or received is required to be verified.
- Non-repudiation
  - Tracking of requests for measurement, reports or additional information is required to be provided.
  - Request origination for updates to registry is required to be recorded.
- Data confidentiality
  - Protection of non-authorized users from viewing information in measurement reports, or additional information provided by a provider's MPM system to another provider's MPM system is required to be provided.
  - Protection of unauthorized access or viewing of measurement reports and additional information stored on a provider's MPM system is required to be provided.
  - Protection of unauthorized access or viewing of information stored in the repository is required to be provided.
- Communication security
  - Measurement information, to be accurate, must follow a precise measurement path.
- Data integrity
  - Protection from unauthorized modification of measurement information is required to be provided.

– Protection from unauthorized modification of reports or additional information requested is required to be provided.
– Protection from unauthorized modification of updates to the registry is required to be provided.

- Availability
  – It is required to ensure that the availability of measurement and management devices is not impacted by information requests or probes.
- Privacy
  – Implementation of systems is required to allow individuals to control or influence what information related to them may be collected and stored, and by whom, and to whom that information may be disclosed.
  – Protection of information from observation that might be used to derive information about users or their activities is required.

10.4.2 Requirements from security threats viewpoint

- Destruction of information and/or other resources
  – It is required to protect information stored on the PMR-FE or registry from destruction.
- Corruption or modification of information

  It is required to have appropriate countermeasures against the following threats:
  – Undetectable changes in contents such as the timestamp or clock sync monitor.
  – Acceptance of unauthorized requests for measurement reports.
  – Acceptance of unauthorized requests for customer subscription information.
  – Acceptance of unauthorized reports.
  – Loss of registry data integrity.
  – Different routing of probes versus regular traffic in the same QoS class.
  – Delaying/accelerating probes versus regular traffic in the same QoS class.
- Theft, removal or loss of information and/or other resources
  – It is required to protect recorded repository information from theft or loss.
- Disclosure of information

  It is required to have appropriate countermeasures against the following threats:
  – Unauthorized disclosure of customer subscription information.
  – Unauthorized disclosure of measurement report information.
  – Unauthorized disclosure of IP addresses of MPM functional entities or measurement points.
- Interruption of services

  It is required to have appropriate countermeasures against the following threats:
  – Acceptance and processing of misdirected probes.
  – An unexpectedly huge number of probes impinging a measurement point.
  – An unexpectedly huge number of requests impinging a measurement device.
  – An unexpectedly huge number of response updates.

– Acceptance of unauthorized requests for initiation of measurements.
– Registry unavailability.
– Measurement device unavailability.
– Measurement point unavailability.
– Disruption of the distributed time.
– Disruption of the measurement system.
– Huge sustained packet loss.

Appendix I

Application scenario 1: Performance degradation resolution information reporting and network partitioning example

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

Performance degradation in any one of several concatenated NGN service providers will degrade the overall concatenated network performance. Therefore, it is important to determine which NGN provider is responsible for the observed performance degradation. This performance degradation information is used by MPM applications. Examples of performance degradation resolution procedure are illustrated in the following figures in terms of functional architecture.

Performance degradation resolution information reporting procedures are divided into two cases based on how the MPM application sends the request message to MPMs: one-to-one or one-to-many. Figures I.1 and I.2 describe these two cases. In Figure I.1, the MPM application sends the request message to only one MPM, and the MPM is in charge of collecting all measurement information from other NGN providers' MPMs. In Figure I.2, the MPM application sends the request messages to several MPMs, and the MPMs respond to the MPM application individually.

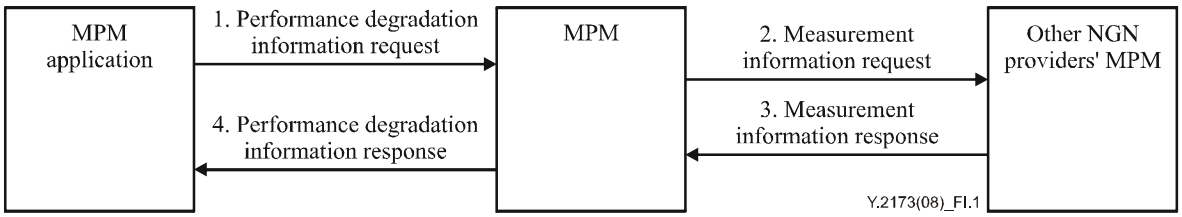

Figure I.1 – Performance degradation resolution information reporting procedure: One-to-one

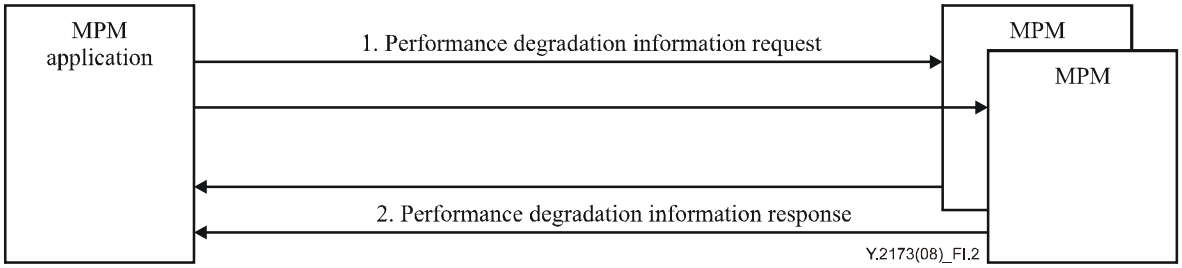

Figure I.2 – Performance degradation resolution information reporting procedure: One-to-many

Performance degradation resolution information reporting procedures are also divided into two cases based on how PMR-FE responds: on-demand and instant. Figures I.3 and I.4 describe these two cases. In the first case, the PMR-FE collects performance degradation information from a PMP-FE or other NGN providers' MPM after receiving a request from an MPM application. In the second case, the PMR-FE collects the performance degradation information in advance, and can respond to an MPM application request immediately.

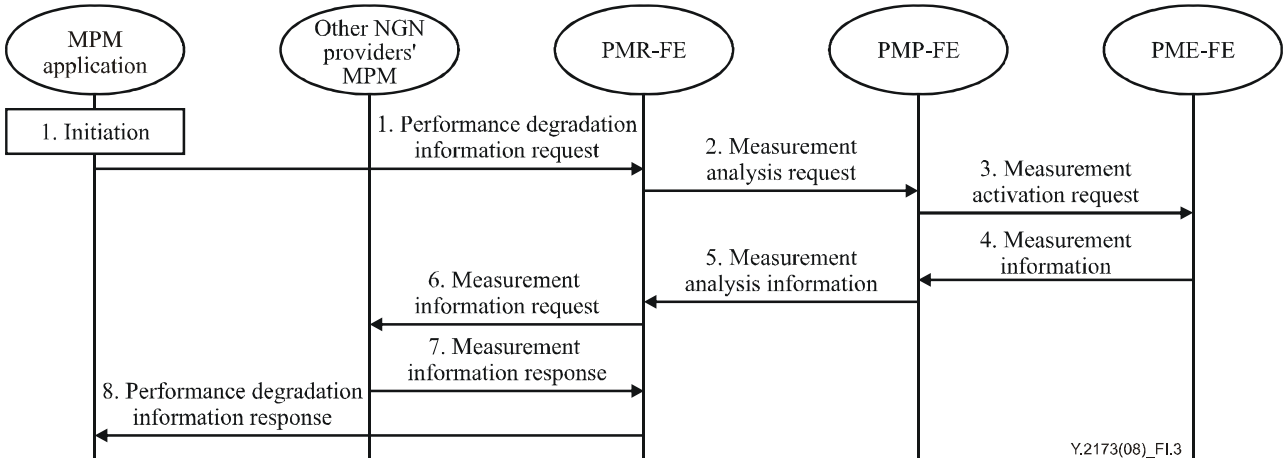

Figure I.3 – Performance degradation resolution information reporting procedure: On-demand

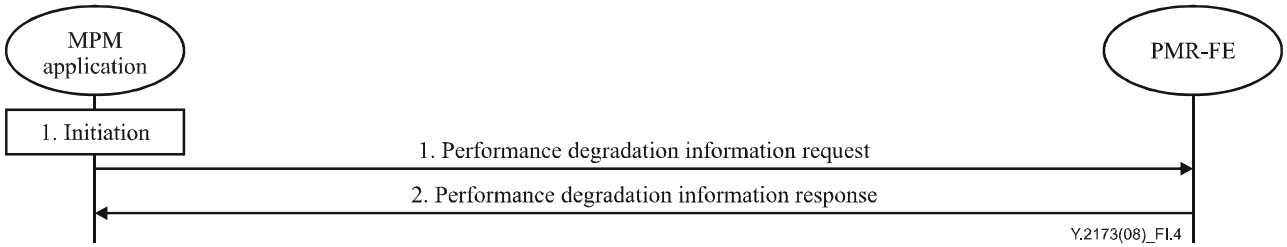

Figure I.4 – Performance degradation resolution information reporting procedure: Instant

Detailed performance degradation resolution processes are not defined in this Recommendation.

When a network is in the normal state, measurements are used to monitor quality of the service contracted. In this case, segmenting a network or selection of intermediate measurement points just depends on the principle of network partitioning or agreement among service providers. When performance degradation occurs, however, service providers need to consider segmenting a network or selection of intermediate measurement points as a process of resolving performance degradation. They may decide the demarcation points of target networks by segmenting the monitoring path as required to meet the objective. Figure I.5 shows an example of the segmentation of a site-to-site model to resolve performance degradation. This example illustrates four measurement segments to monitor for potential performance degradation points between two sites.

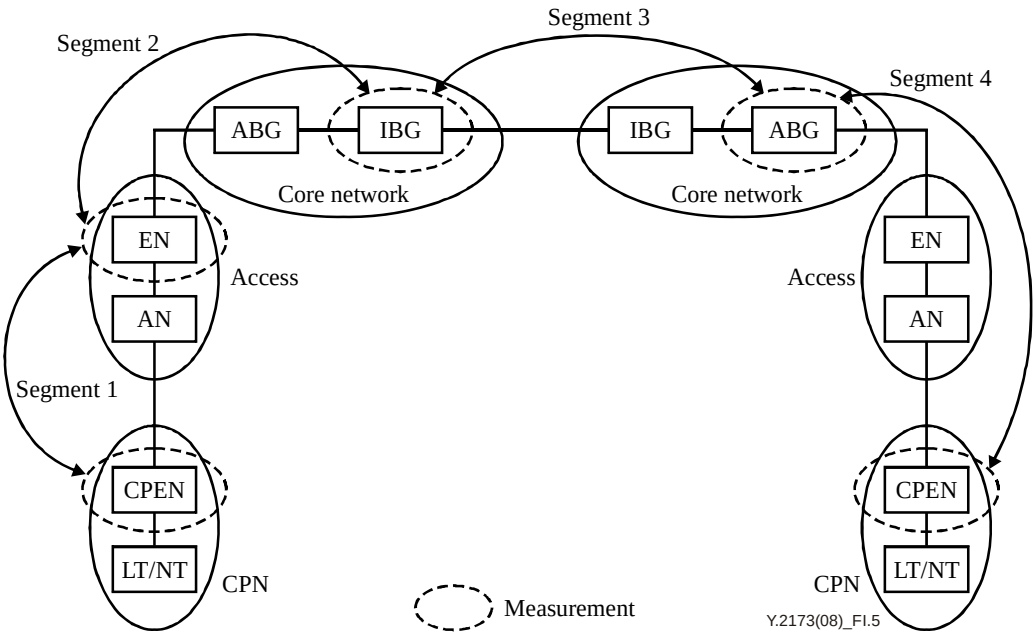

Figure I.5 – Example of network partitioning for resolving performance degradation

Appendix II

Application scenario 2: RTP/RTCP-based performance notification

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

II.1 Introduction

Most sessions of multimedia services over IP-based networks use real-time transport protocol (RTP). Real-time transport control protocol (RTCP) is an accompanying protocol for RTP to feed back IP-based network conditions from RTP receivers to RTP senders. RTCP enables data receivers to estimate downstream bandwidth by calculating round-trip times to senders. The RTP/RTCP flows are also described in the section on QoS resource information components in clause 8.1.3.2 of [b-ITU-T Y.2111]. Furthermore, the RTCP extended reports, called RTCP-XR [b-IETF RFC 3611], provide useful monitoring and diagnosis of VoIP performance between the RTP sender and receiver, such as NGN terminals (CPEs). Furthermore, several new block types for IP video metrics have also been studied, due to the superiority of RTCP as a firewall-friendly protocol over IP-based networks. Also, an RTP translator (an intermediate system that forwards RTP packets with their synchronization source identifier intact) can be a node that provides a capability to notify measured performance information. For example, the bandwidth which corresponds to the throughput of a TCP-like connection is periodically predicted using the loss rate and round-trip time (RTT) of the network provided by RTCP.

II.2 Performance notification

The packet headers from a customer's usual traffic in the transport layer and below do not have a timestamp for delay and delay variation calculation. Delay and delay variation are important in real-time applications, such as VoIP and video streaming. RTP is an additional transport layer protocol for real-time applications and is designed to be independent of the transport or network layer protocols. The RTP packet has timestamp and sequence-number fields in the header. A probing system of the transport function, such as the border gateway, can evaluate packet loss from the sequence-number field. A probing system can also evaluate delay and delay-variation performance from the timestamp field if it has some knowledge about the application of each target flow (for example, the encoding sampling rate), although the content and resolution depend on the category of the application.

In the RTCP packet, some performance-related parameters, such as fraction-lost and inter-arrival-jitter, are reported. CPEs also evaluate rough round-trip delay with these packets. By installing lightweight agent software in CPEs based on RTP/RTCP, network providers can collect performance parameters without any active probing systems. It is possible to evaluate performance metrics and reports by installing additional software and/or hardware modules in CPEs. Network level metrics (e.g., delay, jitter and loss) can be also evaluated and notified by the RTCP and RTCP extensions without using additional active probing systems on the network. Figure II.1 illustrates the configuration for the RTP/RTCP-based performance notification. Note that the support of Mu on RACF is for further study.

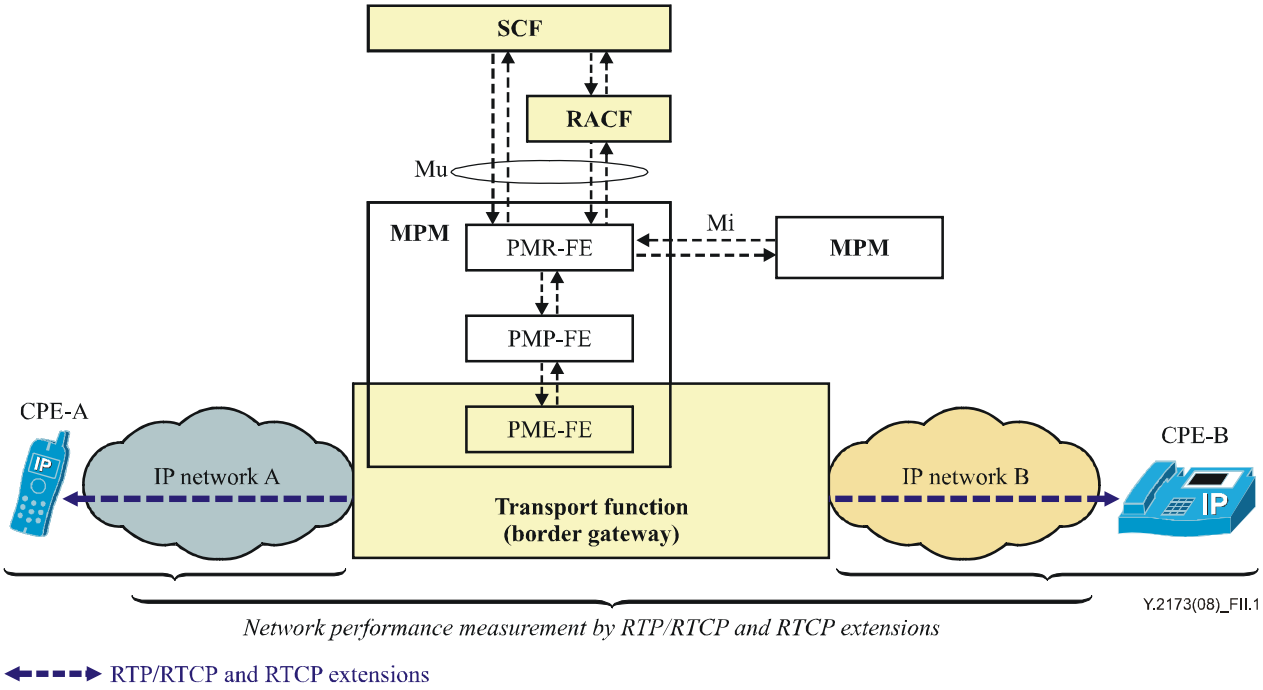

Figure II.1 – Configuration for the RTP/RTCP-based performance notification

II.3 Implementation example of the RTP/RTCP-based performance notification

II.3.1 RACF-based triggering scheme

Network performance between the CPEs is measured and reported to MPM on an end-to-end or per-segment basis using RTP/RTCP and RTCP extensions.

In this example, MPMs process the RTP/RTCP-based performance notification as follows:

– CPE-A sends a request to the SCF to establish a session or sessions with CPE-B.

– RACF receives the service resource request along with other relevant information of the incoming session(s) from the SCF via the Rs reference point, and passes this information to MPM over the Mu reference point.

– PME-FE in MPM recognizes the IP address(s) and RTP/RTCP-port numbers of the incoming session(s). Then, PME-FE observes the flows of the indicated RTP/RTCP and RTCP extensions.

– PMR-FE receives the performance information measured by the PME-FE.

– The performance information report is generated in PMR-FE and sent periodically to RACF over the Mu reference point, if needed.

– The report sent to the RACF might include network resource information such as the bandwidth calculated by the MPM.

The procedure stated above is shown in Figure II.2.

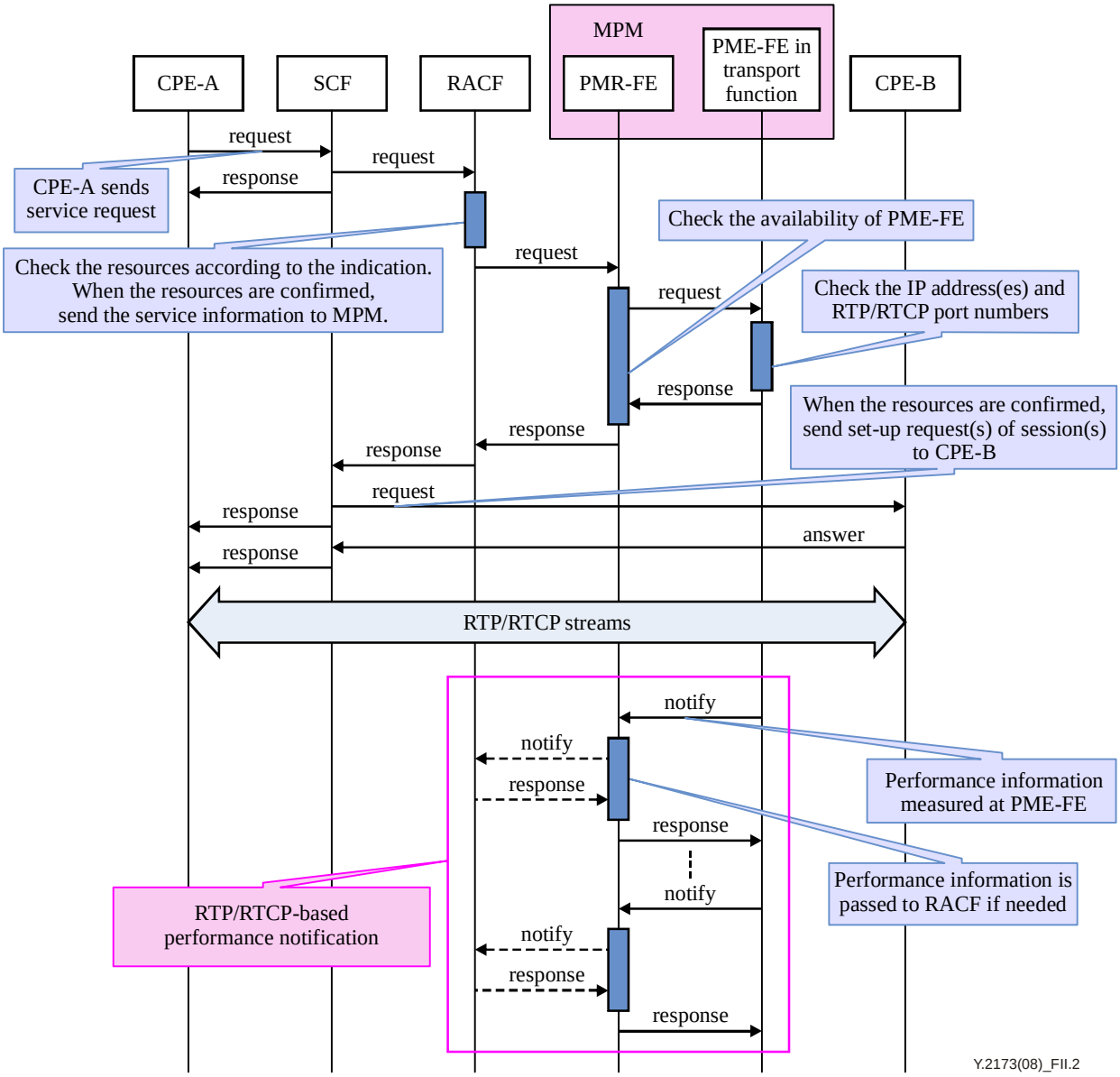

Figure II.2 – Example of the RTP/RTCP-based performance notification flow

II.3.2 SCF-based triggering scheme

In this example, MPM processes the RTP/RTCP-based performance notification as follows:

– CPE-A sends a service request to the SCF (e.g., call session control function (CSCF)) in order to establish a session or sessions with CPE-B.

– SCF receives the service request along with other relevant information of the incoming session(s) and passes this information to MPM over the Mu reference point.

– PME-FE in MPM recognizes the IP address(s) and RTP/RTCP port numbers of the incoming session(s). Then, PME-FE observes the flows of the indicated RTP/RTCP and RTCP extensions.

– PMR-FE receives the performance information measured by the PME-FE.

– The performance information report is generated in PMR-FE. For example, it is sent periodically to the management system for performance information over the Mu reference point.

The procedure stated above is shown in Figure II.3.

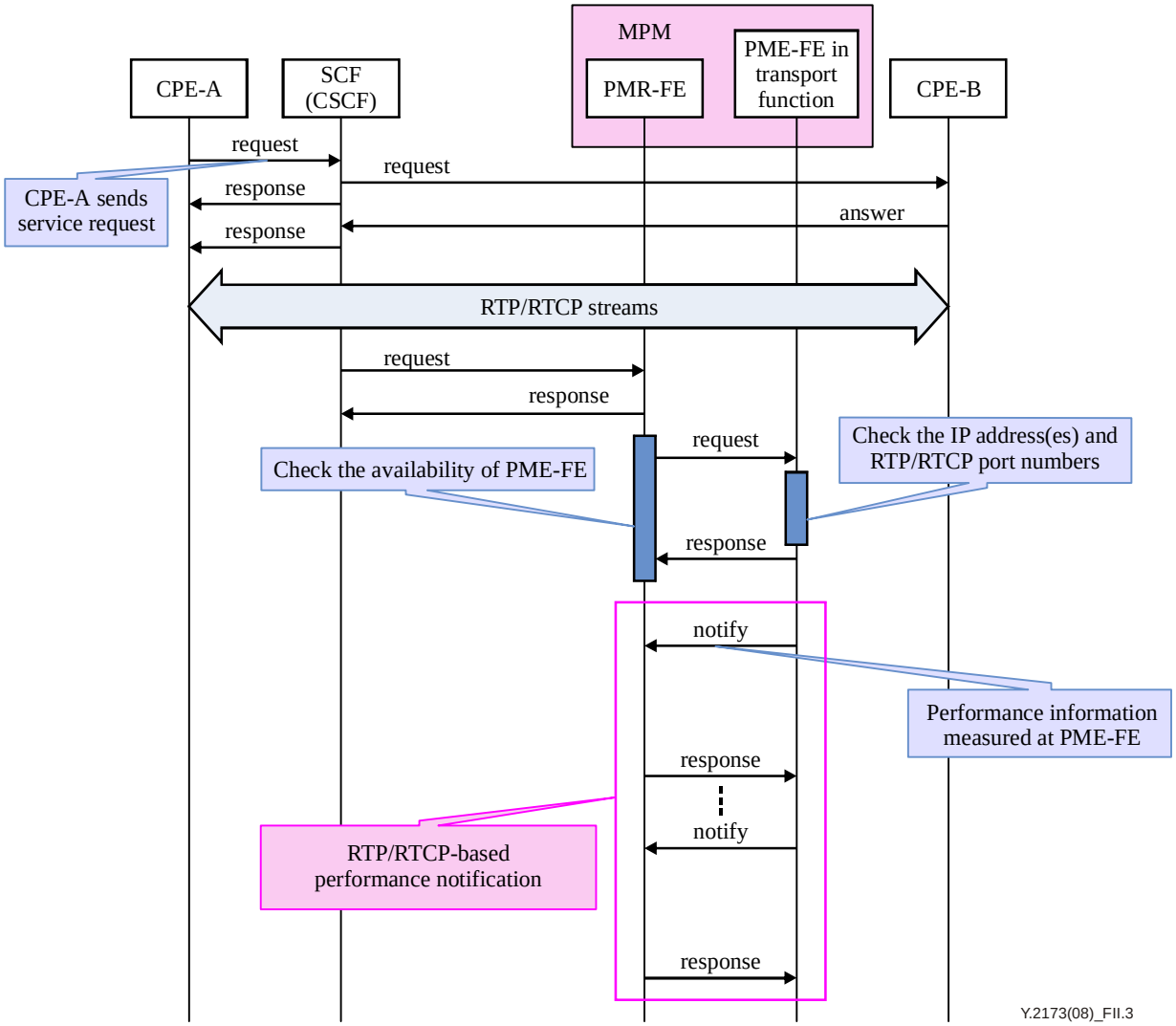

Figure II.3 – RTP/RTCP-based performance notification flow – SCF-based triggering scheme

II.3.3 Procedure for multi-MPM communication

The procedure for multiple MPMs working together is shown in Figure II.4. In this case, each MPM communicates via the PMR-FE over the Mi reference point. The IP addresses and port numbers of the RTP/RTCP streams are reported. Furthermore, the collected performance information can be sent to other MPMs via the PMR-FE.

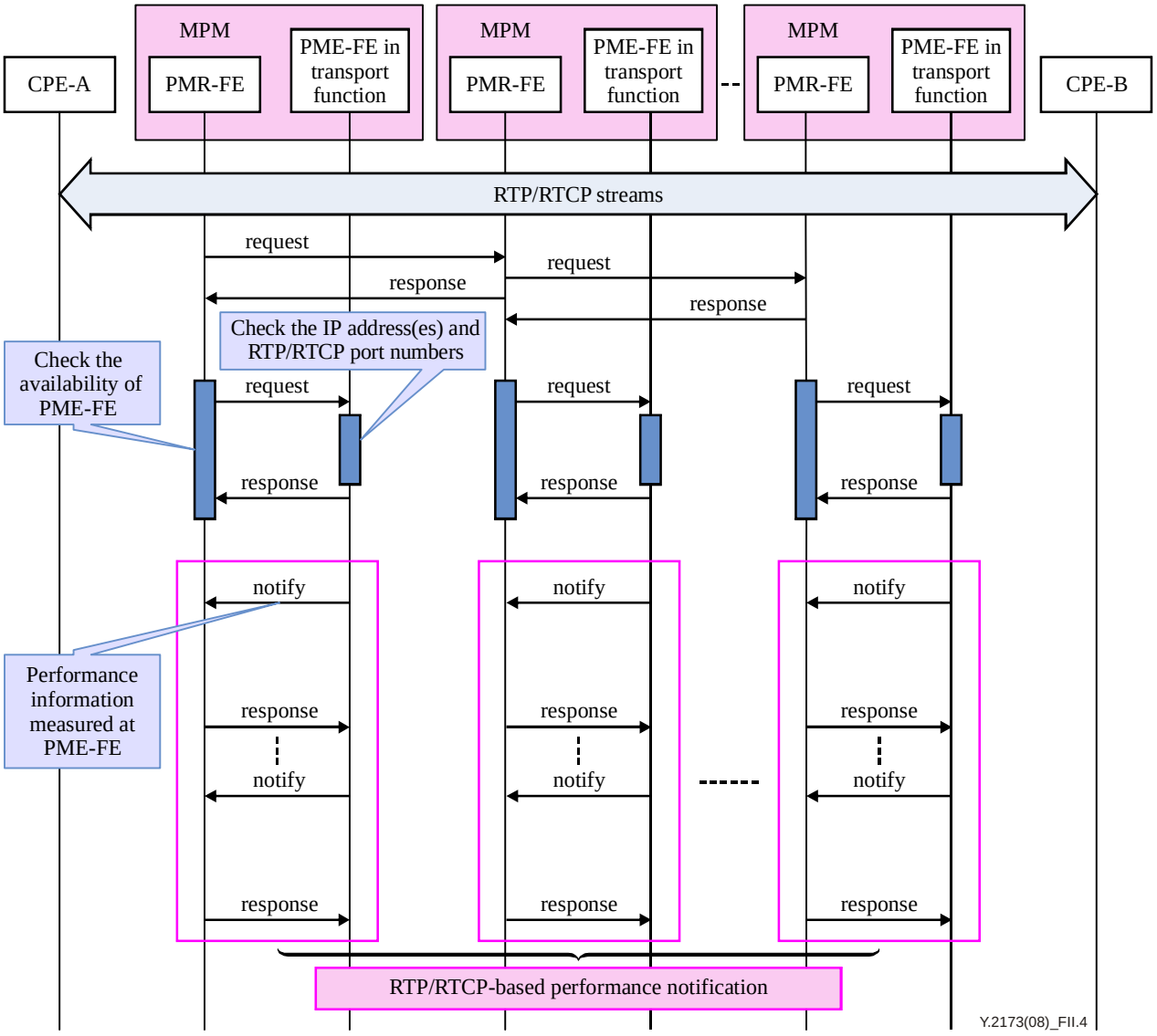

Figure II.4 – RTP/RTCP-based performance notification flow – SCF-based triggering scheme with multi-MPM communication

II.4 Multiplication scheme for RTCP report notification

When several border gateways that equip the PME-FE communicate the RTCP packets to each other, the header overhead of the individual RTCP report packets increases significantly. The RTCP packets from the multiple border gateways are forwarded into one compound packet, whenever feasible, in order to reduce packet overhead. However, the border gateways are not required to aggregate the sender report (SR) and receiver report (RR) packets from different gateways because this would degrade the accuracy of round-trip delay measurements based on the LSR and DLSR fields of the RTCP packets.

In Figure II.5, concatenation reduces the number of separate RTCP packets to three. The packet labelled "RTCP (CPE-A.R)" is the report from the end system, identified because its synchronization source (SSRC) is the same as the SSRC of the RTP flow in the same direction. This is forwarded without concatenation. The packet labelled RTCP (BG-A.1R, BG-B.1R, BG-C.1R) contains border gateway reports of measurements made on the RTP flow from CPE-A to CPE-B, identified because they report the measured flow having SSRC equal to the SSRC of CPE-A. The packet labelled RTCP (BG-A.2R, BG-B.2R, BG-C.2R) contains border gateway reports of

measurements made on the RTP flow from CPE-B to CPE-A, identified because they report the measured flow having SSRC equal to the SSRC of CPE-B.

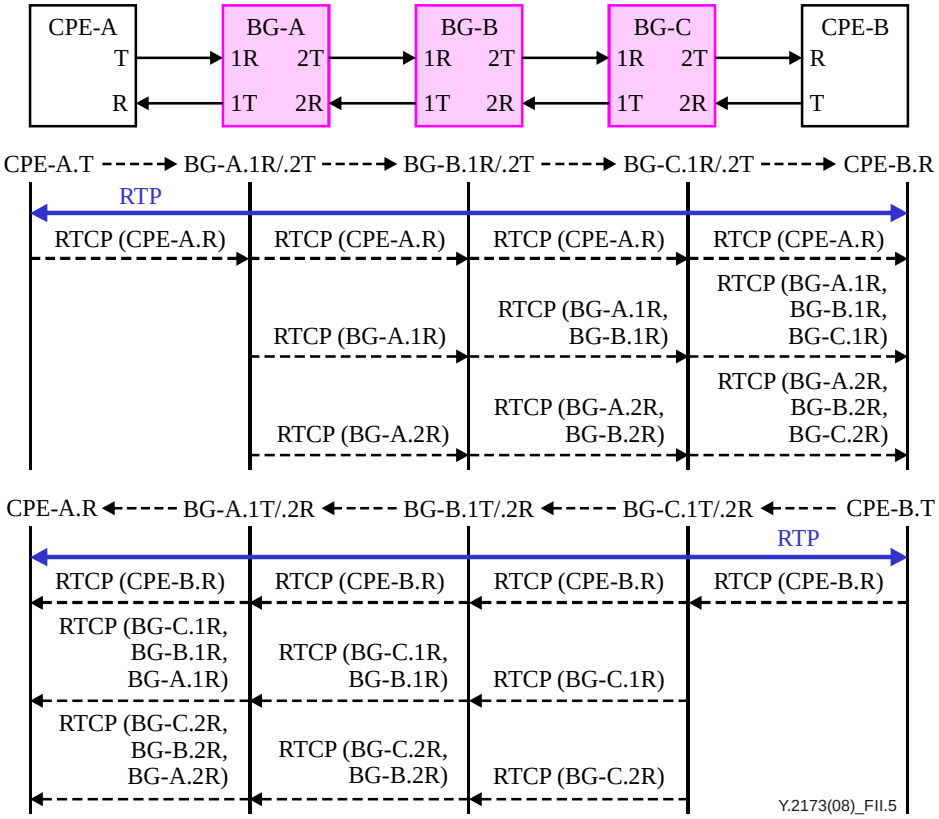

Figure II.5 – Multiplication scheme of the RTCP reports

Appendix III

Example realization for the management of NGN performance measurement

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

To provide better understanding of the general architecture, this appendix provides an example architecture for the realization of the management of NGN performance measurement. In this example, the performance reporting system represents the performance measurement reporting functional entity (PMR-FE). Collection platforms are used as an instance of performance measurement processing functional entity (PMP-FE). Measurement points are instances of the performance measurement execution functional entity (PME-FE). Other internal architectures may achieve the same functionality; however, communications among providers must be standardized.

Configuration, measurement and reporting are accomplished by a group of devices having different functions which are arranged in a hierarchy. There are three functional components: the performance reporting system, collection platform and measurement points (terminal equipment is not included here). The hierarchy and the communications among components are shown in Figure III.1.

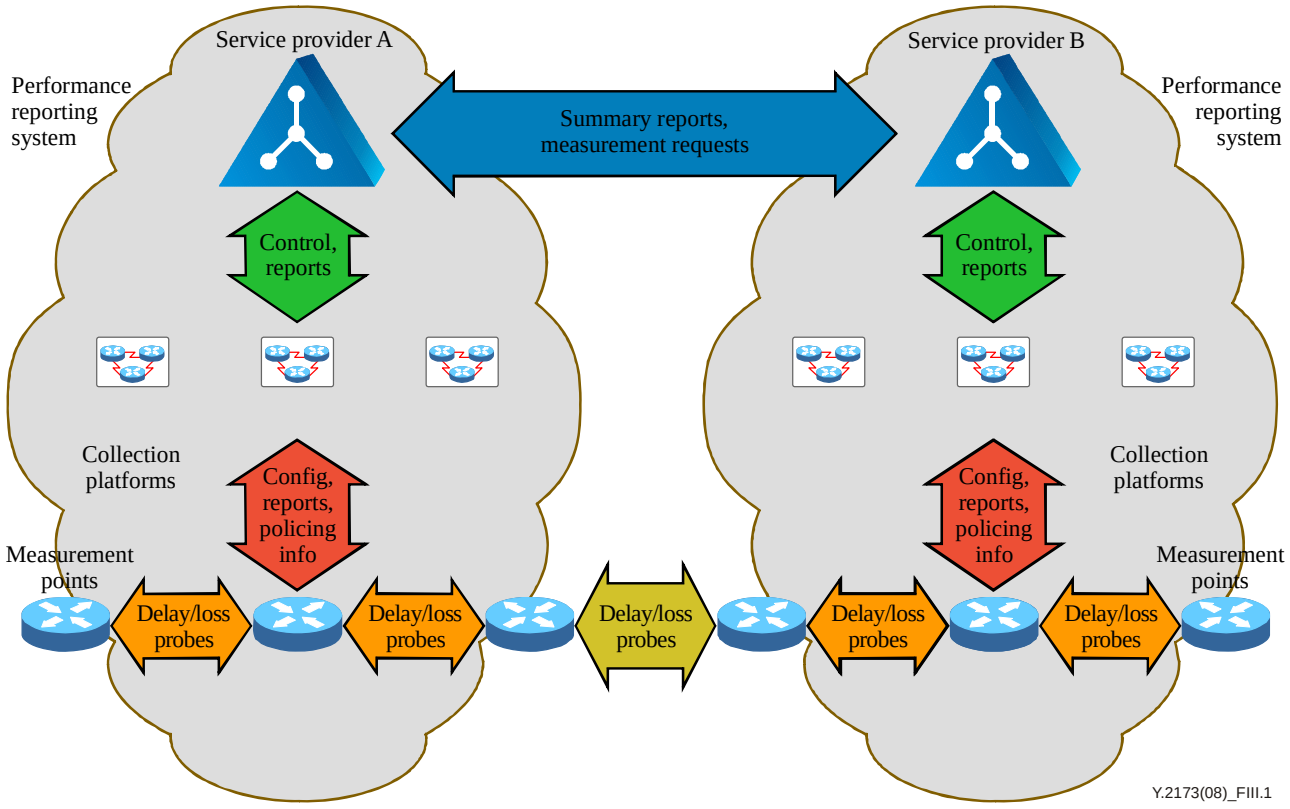

Figure III.1 – A hierarchical internal architecture of active measurement

III.1 Performance reporting systems

At the top of the hierarchy is the performance reporting system (PRS). While this may be implemented using multiple computers, it will appear as a single system to other SPs. The PRS is the primary configuration tool. The PRS pushes probe initiation commands to a collection platform associated with the measurement point that initiates probing. That collection platform then configures the measurement points.

The performance reporting system will simultaneously perform the following functions:

1) Control of collection platforms
   - 1.1) Probes required
     - 1.1.1) Source measurement point
     - 1.1.2) Destination measurement point
     - 1.1.3) Class(es)
     - 1.1.4) Frequency
2) Retrieval of rollup period reports from collection platforms
3) Storage and analysis of rollup period reports
   - 3.1) Storage of measurement data (e.g., a minimum of 12 months)
4) Location of probing destinations (measurement points)
5) Communication with other SPs' PRS
   - 5.1) Responses to rollup period report retrieval requests from other SPs, depending upon their customers' permissions
   - 5.2) Retrieval of rollup period reports from other SPs' PRS for specifically designated customer sites (managed service)
6) Reporting
   - 6.1) To other SPs' PRS, as required
   - 6.2) Real-time network status to SP operations
   - 6.3) To customers

III.2 Collection platforms

At the second level of the hierarchy are the collection platforms. Collection platforms communicate "up" to the PRS and "down" to the measurement points.

The collection platform will simultaneously perform the following functions:

1) Configuration of measurement points
   - 1.1) Probes required
     - 1.1.1) Destination measurement point
     - 1.1.2) Class(es)
     - 1.1.3) Frequency
2) Retrieval and storage of probe results from measurement points
   - 2.1) Storage of probe results (e.g., a minimum of 24 hours)
3) Monitoring of policing at measurement points
4) Monitoring of policing at peering points
5) Analysis of probe results
   - 5.1) Network unavailability determination
   - 5.2) Identification of performance issues
   - 5.3) Determination of rollup period metrics
6) Reporting to PRS
   - 6.1) Creation of rollup period reports
   - 6.2) Generation of critical event reports
     - 6.2.1) Clock synchronization loss

III.3 Measurement points

At the third level of the hierarchy are the measurement points that send and receive probes. Measurement points communicate "up" with associated collection platform(s), and "horizontally" with other measurement points, which may belong to other SPs.

A measurement point will simultaneously perform the following functions:

1) Take configuration from collection platform
   - 1.1) Probes required
     - 1.1.1) Destination measurement points
     - 1.1.2) Class(es)
     - 1.1.3) Probe frequency
2) Implement performance measurements, by initiating "per-class" active probes to measure delay and loss to many other measurement points
3) Provide "per-class" response to other measurement points
4) Store measurements
5) Perform clock synchronization
   - 5.1) Synchronize itself with GPS
   - 5.2) Synchronize associated measurement points
6) Suspend initiating probes while they are not meeting time offset requirements, and reinitiate when they meet time offset requirements
7) Indicate, in its response to probes from other measurement points, its current state of compliance with the time offset requirements
8) Report to collection platform
   - 8.1) When its time offset goes out of specification and back into specification
   - 8.2) When it detects in probe responses from the responding destination device that its time offset is out of specification
9) Respond to policing queries from the collection platform

III.4 Customer terminal equipment

The functions of customer "landmark" terminal equipment are to be defined. When TEs are included in a measurement scheme, the functionality of customer equipment is likely to be expanded.

Appendix IV

Management consideration for performance measurement

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

IV.1 Architectural considerations

The inter-domain performance measurement requires close collaboration between different administrative domains. Performance measurement in each domain can be relatively easily achievable. However, when a measurement crosses a domain boundary, the complexity increases dramatically. The main issues involved are the following:

- Who will measure what, and how?
- What is the common data model to store the measured data?
- How should the measured data be exchanged?
- Are PMR-FEs involved in the measurement collaboration?

Depending on the answers to these questions, we can classify the architectures as follows:

- Architectures not involving PMR-FE
  - Manual model

    In this model, performance measurement data is stored in a standardized common information object and exchanged among service providers through a standard protocol. Management of measurement processes such as configuration of active/passive probes, collection of performance metrics, conversion of metrics to common information objects, and triggering exchange protocols may be performed in a proprietary way in each domain. This model does not assume that there exists a representative performance measurement management system which coordinates all such processes. The advantage of this model is simplicity and cost effectiveness. However, configuration in each domain requires manual intervention, thus it has limitations in automation. This model may raise security issues if the exchange protocol is not secure.
- Architectures involving PMR-FEs

  In this case, one or more PMR-FEs exist in each domain and are responsible for both internal and inter-domain performance measurement management and collaboration.
  - Centralized model

    In the centralized model, a single PMR-FE is responsible for the management of all the active and passive measurement over each domain. It is simple to manage but has scalability limitations. Also, it is not easy to have one centralized PMR-FE control domains that fall under different administration responsibility. Scalability issues may arise since all performance measurement data are required to be reported to one centralized PMR-FE.
  - Distributed models
    - Federated model

      In the federated type of distributed model, PMR-FEs of the domains are structured into a freely federated process group for the management of active and passive measurement. This model distributes the responsibility of the centralized PMR-FE into a number of PMR-FEs across domains. Thus, it enhances the scalability greatly. PMR-FEs can be freely grouped and can exchange information to solve a common problem – in this case, inter-domain performance measurement. Figure IV.1 illustrates one example model. PMR-FE1, PMR-FE2 and PMR-FE3

are responsible for regional network A, regional network B and a transit network. Each PMR-FE measures performance data for its associated regional/transit network, and exchanges it with other PMR-FEs to collaborate in developing end-to-end performance data.

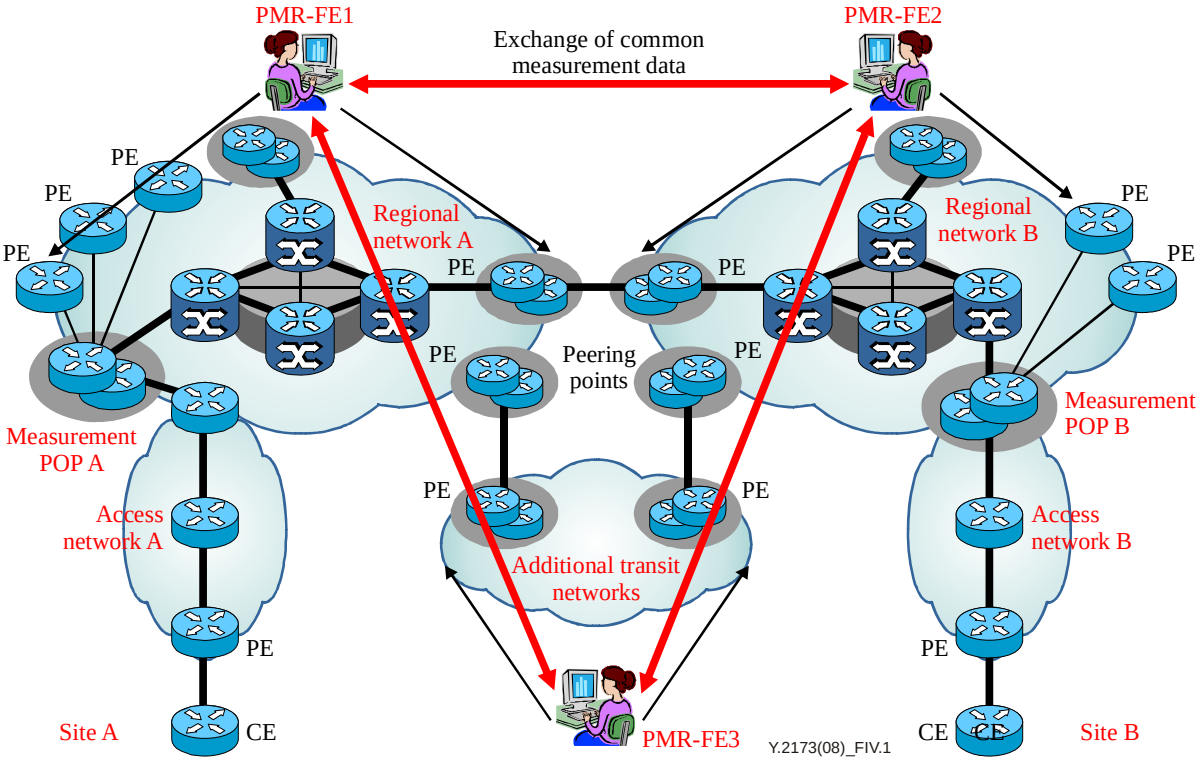

Figure IV.1 – An example federated inter-domain measurement model

- Hierarchical model

  In the hierarchical type of distributed model, PMR-FEs of the domains are hierarchically stratified into a process group of a well-defined structure for the management of active and passive measurement. The hierarchical model is similar to the federated model but involves a more rigid relationship and structure among PMR-FEs. A PMR-FE at a certain level can perform specifically defined functions only. Lower level PMR-FEs perform detailed functions and upper level PMR-FEs perform overall functions. For example, one lower-layer PMR-FE measures the access network segment, another measures the backbone segment, and still another measures the transit or peering segment. An upper-layer PMR-FE then correlates the results from lower layer PMR-FEs and exchanges them with peers in other domains. Figure IV.2 shows an example hierarchical model. PMR-FE1 manages two PMR-FEs which perform measurement of access and core networks. Similarly, PMR-FE2 manages two PMR-FEs. PMR-FE is the highest level PMR-FE which sits on top of PMR-FE1, 2 and 3.

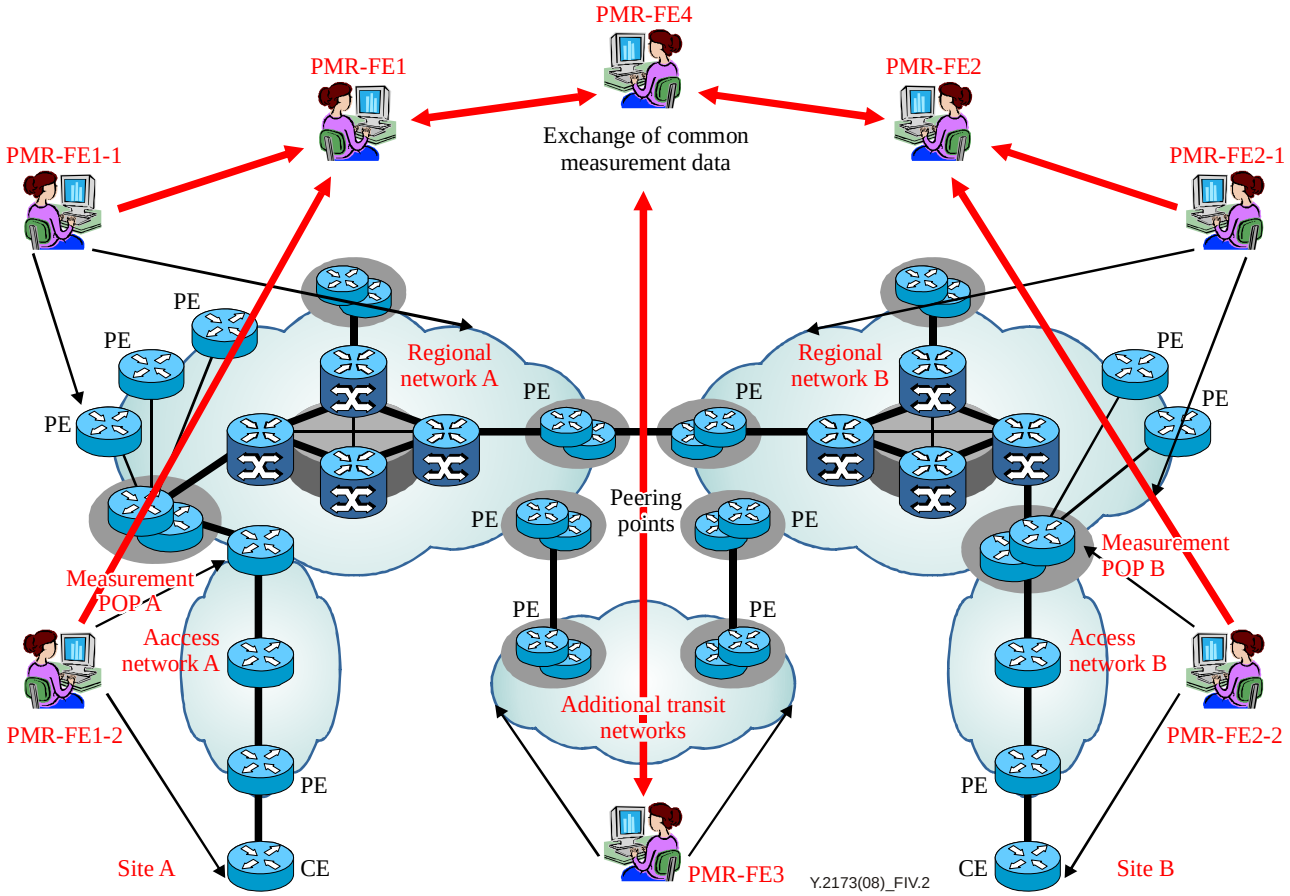

Figure IV.2 – An example hierarchical inter-domain measurement model

- Cascading neighbour model

  In the cascaded neighbour type of distributed model, PMR-FE of the domains are interconnected only with those of the neighbouring domains to create a well-defined structure for the management of active and passive measurement. Figure IV.3 illustrates a cascading neighbour inter-domain measurement model. Each PMR-FE exchanges measurement data with the neighbouring PMR-FE only. Direct interactions occur only among neighbouring PMR-FEs.

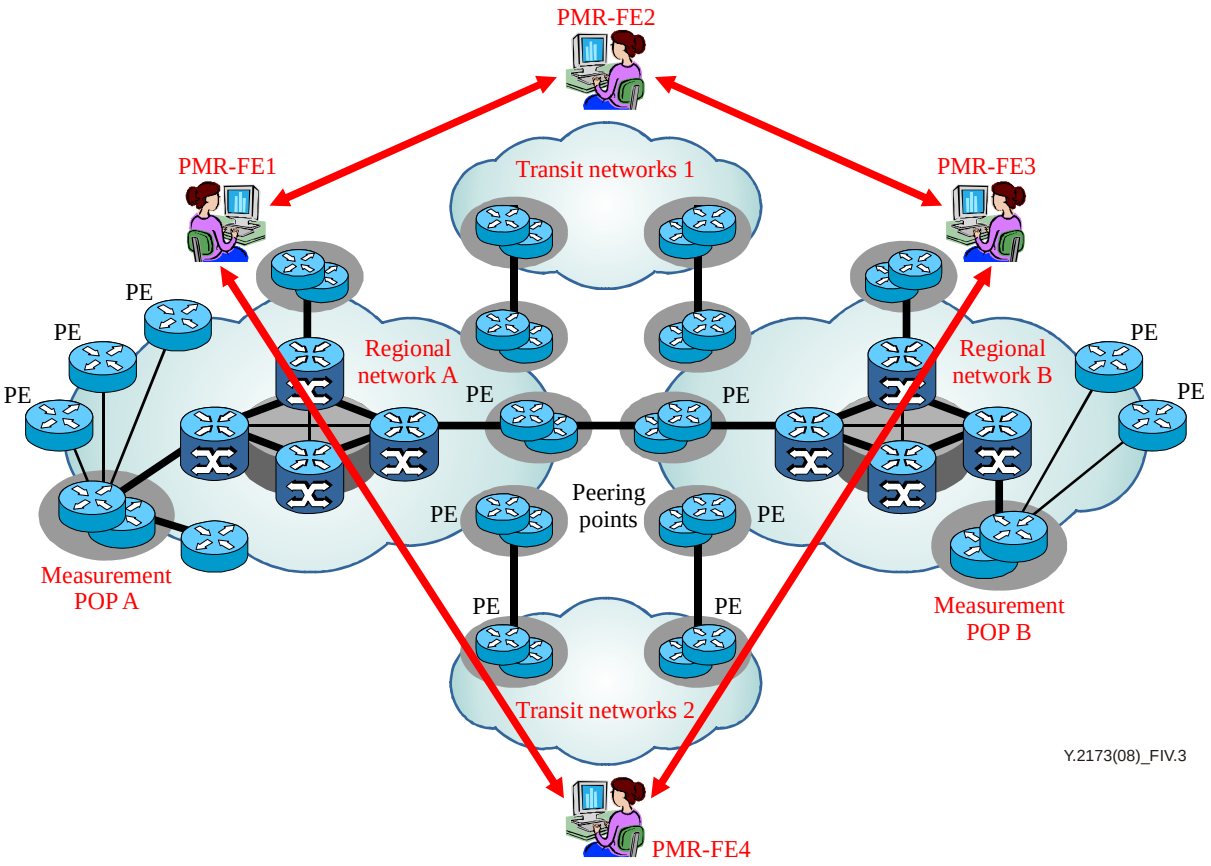

Figure IV.3 – An example cascading neighbour inter-domain measurement model

Depending on the requirements, hybrids of these basic models may also be considered.

IV.2 Discovery considerations

The PMR-FEs of each domain have to exchange performance data for end-to-end "aggregation" of data. Before they can exchange data, they have to discover each other. It is obvious that, in a multi-provider environment, a standard mechanism for discovery and performance data exchange will be required. It will be preferable to use a widely deployed mechanism for discovery and data exchange. A possible candidate is a web/XML- or web services-based mechanism, because of its wide acceptance and deployment in the industry and SP environment. The PMR-FE function of an SP can be provided as a web service with limited access and appropriate security. The discovery process then consists of learning the web service address of the PMR-FE. Three possible options of discovery are as follows:

1) Manual: When two neighbouring PMR-FEs negotiate for collaboration, they exchange manually (via agreement document or other manual means) the web service addresses (URL, for example) of the PMR-FEs.

   Propagate: The addresses can be further propagated to other PMR-FEs. For example, in Figure IV.4, PMR-FE B and PMR-FE C manually exchange their addresses. When PMR-FE Z exchanges initial (*capability*) messages with PMR-FE C, information about more distant PMR-FEs (PMR-FEs A and B) may be passed to PMR-FE Z.

2) Registry: The providers can agree upon a global PMR-FE web service registry. The service can be based on UDDI or other mechanism. When a PMR-FE is commissioned, information about it, including its capabilities, is registered in the registry service. PMR-FEs discover each other via the registry service.

3) A combination of 1 and 2.

The details of standard XML messages and format need to be defined.

When considering the choice of discovery mechanisms, a factor of key importance is security, since the exposure of information may have adverse impacts. The adverse impacts may be categorized as:

1) Competitive exposure – a competitor could take business advantage of the information exposed.

2) Attack exposure – an attacker could better target a provider's network and its customers.

Therefore, it is highly preferable to limit or hide the information made available about the providers' networks, especially when kept in centralized locations such as registries.

The dynamic nature of the network (adds, deletes and moves) is required to be taken into account when considering the methods to provide new data in a timely manner.

IV.3 Messaging considerations

The PMR-FEs can exchange the following "control" messages:

1) Capability: Metrics supported, data distribution and aggregation capabilities supported.

2) Collect: Request to start collecting requested set of metrics.

3) Pull: Request to get data that have been or are being collected based on "collect" request. It is useful, therefore, that a bulk get function be supported.

4) Push: Push data based on "collect" request, for example, when the specified (by the "collect" request) size or time interval has been reached.

5) Metrics.

The details of standard XML messages and format need to be defined.

IV.4 Data handling considerations

IV.4.1 Distribution

A PMR-FE may request data from multiple segments for end-to-end performance data "aggregation". Following are the potential options for data collection and distribution requests:

1) Mesh: The requesting PMR-FE requests all the PMR-FEs towards the destination PMR-FE. For example, in Figure IV.4, if PMR-FE Z collects delay data towards PMR-FE A, it will send requests to PMR-FE C, PMR-FE B and PMR-FE A. Data will be sent directly to PMR-FE Z from each PMR-FE (A, B and C).

2) Cascade: The requesting PMR-FE requests its immediate neighbour, which propagates the requests to the destination PMR-FE. The requested data may be transferred in a cascaded fashion (not further aggregated).

3) Combination of the above.

The capability of a PMR-FE may be exchanged during capability negotiation. For example, PMR-FE B can indicate to PMR-FE Z that it will not cascade.

Following are the reasons for the cascading support:

1) When collecting data end-to-end, an intermediate PMR-FE may need to retain and analyse data. For example, while Z collects delay data towards A, PMR-FE B may want to retain and aggregate data to find out the PMR-FE B to PMR-FE A delay.

2) When there is a need to mask individual components of performance values of a set of segments from another set of segments. For example, SP A and SP B may want to mask their individual components of performance values from Z.

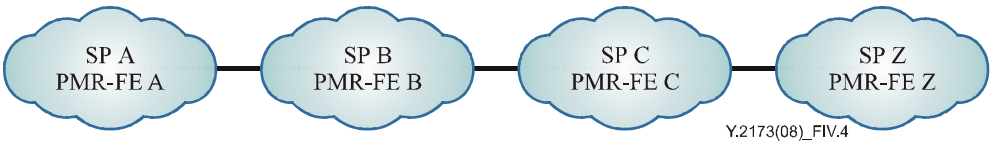

Figure IV.4 – Inter-provider PMR-FE network

IV.4.2 Aggregation

Performance data can be aggregated at various points in the network depending on distribution architecture, as described above. For example, in the case of Z to A delay data collection, data may be aggregated as follows:

- PMR-FE A aggregates its own data and data from any more distant PMR-FEs. PMR-FE B aggregates data received from PMR-FE A with its own, PMR-FE C aggregates data received from PMR-FE B with its own, and sends to PMR-FE Z; or
- PMR-FEs A, B and C send their own data to PMR-FE Z.

IV.4.3 Internal architecture considerations

It is useful that the internal architecture of a PMR-FE not have any impact on the overall (global) PMR-FE network. Within a single SP, any combination of the following protocol/mechanisms could be used:

1) SNMP;
2) XML-http-based;
3) IPFIX;
4) proprietary.

Except for the XML-based one, these protocols/mechanisms may not be suitable for multi-provider environments. For example, one of the disadvantages of SNMP or IPFIX is that these protocols are (mostly) UDP-based, and have limitations when firewall or SP boundaries have to be crossed.

The primary internal functions of a measurement PMR-FE include the following:

- Discovery of other PMR-FEs and their measurement components.
- Communications with other PMR-FEs to request and receive measurements.
- Comparison of measured and expected results.
- Collection, aggregation and storage of measurements.
- Initiation of and response to measurement probes.
- Configuration and monitoring fault events of the measurement components.
- Monitoring of policing.
- Time synchronization.
- Reporting.

The IPFIX protocol provides network administrators with access to IP flow information. The architecture for the export of measured IP flow information out of an IPFIX exporting process to a collecting process is defined in [b-IETF RFC 5101], per the requirements defined in [b-IETF RFC 3917]. The IPFIX protocol specifies how IPFIX data record and templates are carried via a congestion-aware transport protocol from IPFIX exporting processes to the IPFIX collecting process. IPFIX has a formal description of IPFIX information elements, their name, type and additional semantic information, as specified in [b-IETF RFC 5102]. Finally, [b-IETF RFC 5472] describes what type of applications can use the IPFIX protocol and how they can use the

information provided. It furthermore shows how the IPFIX framework relates to other architectures and frameworks.

IV.4.4 NAT considerations

IV.4.4.1 Introduction

At present, the deployment of NATs is very often due to the lack of IP addresses. Sometimes, the whole access network of a service provider might use private IP addresses. Since NATs have been deployed widely, we should consider how to perform end-to-end measurement when there is a NAT device in the end-to-end path. When a NAT device performs a network address translation procedure, packet loss or delay may occur, which will in turn affect the performance measurement results. Thus, network performance measurement needs to take NAT impact into account.

IV.4.4.2 The impact of NAT on performance measurement

NAT devices are typically located at the boundary between a private network and a public network. When a packet traverses a NAT device, the header of the packet will be translated by the NAT device. The fields to be translated depend on the type of NAT. For example, in the case of a basic NAT, for the direction from private network to public network, the source IP address and related fields such as IP, TCP, UDP and ICMP header checksums are translated. For the opposite direction, the destination IP address and the checksums, as listed above, are translated. In the case of NAPT, the transport layer identifier such as TCP/UDP port will also be translated.

To perform the network address translation, a NAT device binds private addresses with public addresses. Address binding may be static or dynamic. Dynamic address binding is created at the start of a session. In general, a session is required to be initiated by a host located in the private network.

The impact of NAT on network performance measurement can be summarized as follows:

- For active measurement, the measurement point in the public network cannot initiate measurement by sending probes to a measurement point in a private network until the private IP address has been bound to a public address. The measurement point in a public network may not be able to determine whether the probes received are generated from a measurement point located in a private network based on the source IP addresses of the probes. This may make it difficult to determine the measurement to which a received probe belongs.
- For passive measurement, in general, a flow under measurement is characterized by a 5-tuple consisting of source address, destination address, source port, destination port and protocol, while the measurement points located in the private and public network, respectively, cannot recognize the flow according to only one 5-tuple. The reason is that for a given flow under measurement, the 5-tuple to characterize the flow in the private network is required to be different from the 5-tuple in the public network. The FlowID and PacketID generalized based on captured packet are also different, so it is impossible to calculate packet loss and delay by comparing FlowID, PacketID and timestamps.

IV.4.4.3 Performance measurement in a NAT environment

As noted above, it is necessary for a measurement point to know the binding of private and public addresses when there is a NAT device in the end-to-end path. If a measurement point can obtain the binding information, it is possible to perform measurement in a NAT environment. To achieve this goal, we can use, for example, the following methods which will be appropriate for active or passive measurement, or both:

- The measurement point in the public network accesses the measurement point in the private network using its domain name (i.e., fully qualified domain name). DNS-ALG will be

deployed to facilitate name-to-address mapping. The domain name resolution is location-dependent. This method can only be used in active measurement.

- Carry the IP address and TU port in the payload of probe packets. This may enable the receiving measurement point to determine the address binding by comparing information carried in the probe packet header and the payload. As an example, the probe packet defined in [ITU-T O.211] contains IP performance measurement signature (IPPMS) and IPPMS extension fields. The IPPMS extension field can carry the IP address and TU port. It is also feasible to define a type-P packet to perform this type of measurement. This method can only be used in active measurement.
- The address binding can be sent to the measurement points in both the private and public networks. For passive measurement, the measurement points located in private and public network are required to use different 5-tuples to extract the same flow. A measurement controller (e.g., PRS) can get the address binding and set up an appropriate classification parameter for each measurement point according to its location. When measurement points extract the target packets from different locations, they can generate the same FlowID and PacketID according to the address binding and the information carried by captured packet headers. This method can be applied in passive measurement.
- Separate a measurement into two segments, with the demarcation point at the NAT device: one covering the private network and the other covering the public network. The measurement controller is responsible for aggregating the final measurement result from the two separated results. This method can be applied in active or passive measurement. Note that this method does not consider the impact of NAT to network performance.

IV.4.4.4 Other types of NAT and NAT-PT

In addition to the basic NAT and NAPT, described above, there are several other types of NAT (e.g., bidirectional NAT, twice NAT and multi-homed NAT). Methods similar to those described above can be used to enable performance measurement in bidirectional NAT and twice NAT environments. Since the purpose of multi-homed NAT is mainly for enhancement of availability, it is irrelevant to performance measurement.

NAP-PT devices may perform IPv4/IPv6 address translation at the boundary between IPv4 and IPv6 networks. The methods used in a NAT environment can also be applied in a NAT-PT environment.

IV.5 ECMP consideration for active measurement

The models support multiple peering connections between providers. The models support equal cost multi-path (ECMP), as indicated by the multiple paths shown within providers. If 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 these 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, increasing the likelihood that, in the case of load balancing, active probes will follow all the paths that customers' data follow between two sites.

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. A future approach may be able to conduct measurements on a subset of paths which match particular users' traffic.

IV.6 Performance degradation resolution among multiple NGN service providers

It is important for NGN service providers to be able to resolve NGN customer complaints about service performance. When a single NGN service provider is involved, resolution can be based on the applicable SLA and is not subject to standardization. However, when the service spans multiple NGN service providers, resolution involves identifying which provider is responsible for the indicated performance degradation, and can be complex. Performance information needs to be obtained from each service provider and exchanged among the involved parties. The following principles are recommended:

- Define a standardized information model and information exchange interface. Base the information model on the traffic performance metrics defined in [ITU-T Y.1543] and relevant specifications from other SDOs (e.g, [b-IETF RFC 4148]).
- Ensure that the performance information exchanged is detailed enough to resolve performance degradation (but does not include other information not essential to that goal).
- Ensure that each provider's MPM supports a reporting function and interface.
- The additional performance metrics further defined are the following:
  - Minimum delay [ITU-T Y.1543].
  - Packet error ratio [ITU-T Y.1540].
- Ensure that the following other information elements are also available for performance degradation resolution:
  - Measurement point.
  - Measurement granularity.
  - Measurement duration.

Bibliography

[b-ITU-T Y.2111] Recommendation ITU-T Y.2111 (in force), *Resource and admission control functions in Next Generation Networks*. <http://www.itu.int/rec/T-REC-Y.2111>

[b-IETF RFC 2330] IETF RFC 2330 (1998), *Framework for IP Performance Metrics*. <http://www.ietf.org/rfc/rfc2330.txt>

[b-IETF RFC 2679] IETF RFC 2679 (1999), *A One-way Delay Metric for IPPM*. <http://www.ietf.org/rfc/rfc2679.txt>

[b-IETF RFC 2680] IETF RFC 2680 (1999), *A One-way Packet Loss Metric for IPPM*. <http://www.ietf.org/rfc/rfc2680.txt>

[b-IETF RFC 3357] IETF RFC 3357 (2002), *One-way Loss Pattern Sample Metrics*. <http://www.ietf.org/rfc/rfc3357.txt>

[b-IETF RFC 3393] IETF RFC 3393 (2002), *IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)*. <http://www.ietf.org/rfc/rfc3393.txt>

[b-IETF RFC 3432] IETF RFC 3432 (2002), *Network performance measurement with periodic streams*. <http://www.ietf.org/rfc/rfc3432.txt>

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*. <http://www.ietf.org/rfc/rfc3550.txt>

[b-IETF RFC 3611] IETF RFC 3611 (2003), *RTP Control Protocol Extended Reports (RTCP XR)*. <http://www.ietf.org/rfc/rfc3611.txt>

[b-IETF RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*. <http://www.ietf.org/rfc/rfc3871.txt>

[b-IETF RFC 3917] IETF RFC 3917 (2004), *Requirements for IP Flow Information Export (IPFIX)*. <http://www.ietf.org/rfc/rfc3917.txt>

[b-IETF RFC 4148] IETF RFC 4148 (2005), *IP Performance Metrics (IPPM) Metrics Registry*. <http://www.ietf.org/rfc/rfc4148.txt>

[b-IETF RFC 5101] IETF RFC 5101 (2008), *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*. <http://www.ietf.org/rfc/rfc5101.txt>

[b-IETF RFC 5102] IETF RFC 5102 (2008), *Information Model for IP Flow Information Export*. <http://www.ietf.org/rfc/rfc5102.txt>

[b-IETF RFC 5472] IETF RFC 5472 (2009), *IP Flow Information Export (IPFIX) Applicability*. <http://www.ietf.org/rfc/rfc5472.txt>

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2009