Title: **Deliverable D2.7** **6QM and IETF Activities**	**Document Version:** 2.1

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

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

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

Responsible and Editor/Author: Alexandre Dubus	**Organization:** FT	**Contributing WP:** WP2

Authors (organizations):

Jordi Palet (Consulintel), Emile Stephan (FT).

Abstract:

This document presents the IETF activities related to the 6QM Project.

Keywords:

IETF, IPFIX, IPPM, Metrics, MIB, Netflow, PSAMP, RMON, Standardization.

Revision History

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

Revision	Date	Description	Author (Organization)
v0.0	5/12/2002	Document creation	Emile Stephan (FT)
v0.1	15/01/2003	Update	Emile Stephan (FT)
v1.0	15/02/2003	Document ready for delivery	Emile Stephan (FT)
v1.1	15/03/2003	Style update. Deliverable content balancing	Alexandre Dubus (FT)
v1.2	20/03/2003	Document delivery	Emile Stephan (FT)
v1.3	22/03/2003	AVT added	Vincent Barriac (FT)
v1.4	24/03/2003	Review	Emile Stephan (FT)
v1.5	28/30/2003	Update	Alexandre Dubus (FT)
v1.6	30/03/2003	Update	Emile Stephan (FT)
v1.7	15/04/2003	Review	Emile Stephan (FT)
v1.8	20/04/2003	Review	Emile Stephan (FT)
v1.9	30/04/2003	Review	Emile Stephan (FT)
v2.0	10/05/2003	Draft deliverable	Emile Stephan (FT)
v2.1	18/05/2003	Final review	Jordi Palet (Consulintel)

Executive Summary

This document examines the various working groups in the IETF that are relevant to the 6QM project. In particular, a general description of each working group is given, plus the goals and milestones, and the drafts and request for comments that are associated with each group.

The following groups have been included:

- IP Version 6 (ipv6): Provides a home for IPv6 work that spans multiple working groups.
- IP Version 6 Operations (v6ops): Develops guidelines for the operation of a shared IPv4/IPv6 Internet and provides guidance for network operators on how to deploy IPv6 into existing IPv4-only networks, as well as into new network installations.
- Benchmarking Methodology (bmwg): Focus is to make a series of recommendations concerning the measurement of the performance characteristics of various internetworking technologies.
- IP Performance Metrics (ippm): Develop a set of standard metrics that can be applied to the quality, performance, and reliability of Internet data delivery services.
- IP Flow Information Export (ipfix): Define a standard set of capabilities by which IP flow information can be transferred.
- Packet sampling (psamp): Define a standard set of capabilities to sample subsets of packets.
- Remote Network Monitoring (rmon): Chartered to define a set of managed objects for remote monitoring of networks.
- Internet Traffic Engineering (tewg): Traffic Engineering entails that aspect of network engineering which is concerned with the design, provisioning, and tuning of operational internet networks.
- Audio and Video Transport (avt): The Audio/Video Transport Working Group was formed to specify a protocol for real-time transmission of audio and video over UDP and IP multicast.
- Inter-domain routing (idr): The objective is to promote the use of BGP-4 to support IP version 4 and IP version 6. The working group will continue to work on improving the scalability of BGP.

Various standardized measurement architectures are described and then compared. These include, but are not limited to:

- RMON: Remote Monitoring is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.
- IPPM: defines a MIB for managing the measures using the IP performance metrics specified by the IPPM Working Group.
- RTFM: The RTFM architecture is an attempt by IETF to standardize several aspects of flow definition, capture and metering operations [RFC2722].
- Sflow: a technology for monitoring traffic in data networks containing switches and routers.
- IPFIX: Currently defining an architecture that employs the concept of collector, observation point, and metering process.

Table of Contents

Table of Figures

1. INTRODUCTION

There are various ongoing activities at the IETF that are relevant to the study of IPv6 QoS measurement. At the most basic level, there is the notion of “packet sampling”, or how one can capture IP packets as they traverse network elements and to report on them. This technique is used in “passive” point measurement systems.

Traffic between a source host {address,port} and a destination host {address,port} is referred to as “flows”. The real-time flow-monitoring group (RTFM) was focused on examining the mechanism to capture export flow data to external accounting systems. The working groups IPFIX and PSAMP supersede it. There are a number of different competing protocols being considered for standardization in the IPFIX WG. Under the strong influence of Cisco Netflow V9 is chosen as the basis protocol.

At a management level, the RMON group is focused on a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON delivers information in ten RMON groups of monitoring elements, each providing specific sets of data to meet common network-monitoring requirements.

The IPPM group has defined a number of different metrics based upon measurements that are taken between a source and destination host, such as one- way delay, packet loss, delay, and delay variation. A management MIB is in the process of being standardized that allows SNMP applications to access IPPM measurement data from the MIB.

The relationship can be depicted in the figure below:

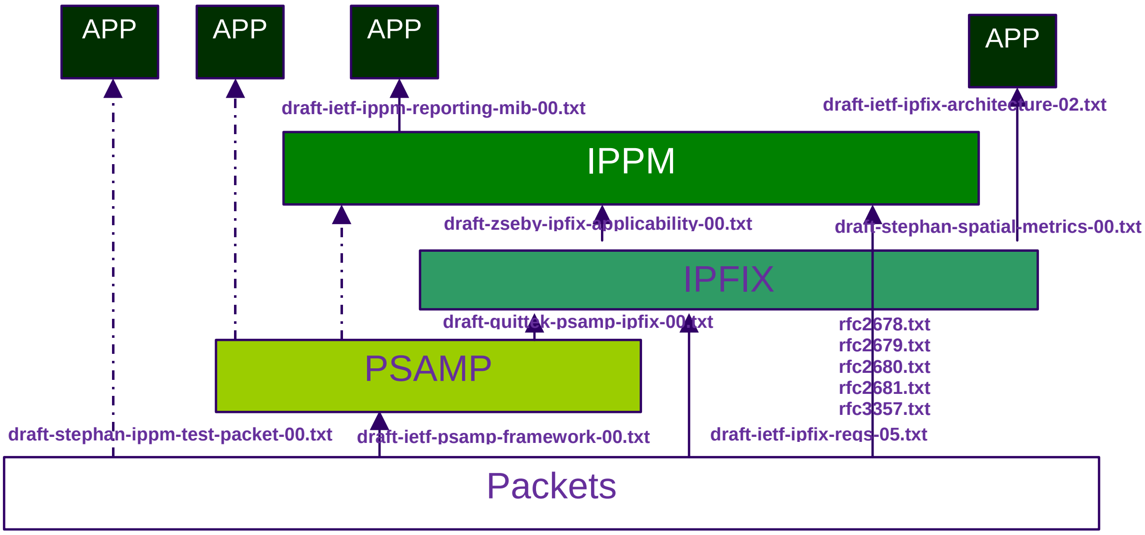
APP
APP
APP
APP
draft-ietf-ippm-reporting-mib-00.txt
draft-ietf-ipfix-architecture-02.txt
IPPM
draft-zseby-ipfix-applicability-00.txt
draft-stephan-spatial-metrics-00.txt
IPFIX
draft-quittek-psamp-ipfix-00.txt
rfc2678.txt
rfc2679.txt
rfc2680.txt
rfc2681.txt
rfc3357.txt
PSAMP
draft-stephan-ippm-test-packet-00.txt
draft-ietf-psamp-framework-00.txt
draft-ietf-ipfix-reqs-05.txt
Packets

Figure 1-1: Overall Working Groups Inter relations

2. QoS Measurement Activities within IETF

2.1 Standardization at IETF

2.1.1 Overview of the IETF

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). Much of the work is handled via mailing lists. The IETF holds meetings three times per year.

The IETF working groups are grouped into areas, and managed by Area Directors, or ADs. The ADs are members of the Internet Engineering Steering Group (IESG). Providing architectural oversight is the Internet Architecture Board, (IAB). The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. The IANA is chartered by the Internet Society (ISOC) to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters.

The following working groups are relevant when considering IPv6 QoS measurement activities.

3. IP VERSION 6 WORKING GROUP (IPV6)

The effort to prepare the next generation of Internet started 20 years ago. IPv6 is intended to support the continued growth of the Internet, both in size and capabilities, by offering a greatly increased IP address space and other enhancements over IPv4. Most of the tasks in that original charter have been completed, and the core IPv6 protocol specifications are now on the IETF standards track.

This charter focuses on completing the remaining work items and plans to refine its charter by the end of 2003.

3.1 Documents Distribution per Domain

The ipv6 WG is central Working for IPv6 standardization. The analysis of the number of documents per domain provides a synthetic view to compare IPv6 to IPv4, and to extract the issues for the measurement of the QoS of IPv6.

There are 25 documents (1/3) in the domains 'addressing' and ' IPv6 over Different Media'. It shows that the mapping of IPv6 is not obvious: IPv6 is a brand new protocol and its mapping must be completely defined. That motivated the need of a dedicated effort to standardized protocol identifier for IPv6 and SUB IP.

13 documents (more that 20%) relate to machine-to-machine address resolution or modification in the domains 'Auto Configuration', 'Multihoming', 'Header Compression' and 'mobility'. Consequently results consolidation in a contractual usage perspective look to be a real challenge.

Despite each of the domains 'Routing' and 'Domain Name System' have 4 documents and look mature, the DNS domain is not stable (2 of the documents are in work in progress), and the 'Routing' domain does not address the routing protocol ISIS.

3.2 56th IETF

3.2.1 Site local addresses

According to the large number of threads on the mailing list, the discussion on site local addresses is a main issue. This subject has been discussed many times in the past but no consensus has ever been reached. IPv6 site local address (FEC0::/10 address range) raises the issue of the controversial common usage of private addresses and NAT (Network Address Translation) boxes, but currently widely used and deployed within the legacy IPv4 Internet. This is actually a real issue for any ISPs and/or users, since it impacts end-to-end transparency of the network, and then, the services that can be designed over the global infrastructure. Proponents (to site local and scoped addresses) and opponents explained their own views. The WG came to the consensus that site local address is deprecated.

3.2.2 Flow label

This 2 pages document is going to last call while having a confusing scope and applicability.

Domain	**Number of documents**
Addressing	15
IPv6 over Different Media	10
Auto Configuration	6
Network Management	6
Security	5
Domain Name System	4
Routing	4
Program Interfaces	4
Multihoming	3
Header Compression	3
Transition Mechanisms	3
Internet Control Message Protocol	2
Hop by Hop Options	2
Neighbor Discovery	2
Multicast	1
Path MTU Discovery	1
Packet Tunneling	1
Renumbering	1
OSI NSAP Mapping	1
Mobility	1
Total	75

Figure 3-1: IPv6 Documents Distribution per Domain

3.3 6QM and IPv6 WG

Regarding the measurement the main issues look obviously related to the management of the measure while the addresses of the source or the sink of the flows get modified due to header compression, dual homing, auto configuration, mobility or get encapsulated in a tunnel.

While these issues are applicable for both for active and passive measurements techniques, they are more relevant for passive measurement when this technique is applied to arbitrary traffic.

3.3.1 Active Measure Issues

The measurement team controls active probes configurations. So either the address of the points of measure is fixed, either the instant of the modification of the address is detected and permit the new address value to be refreshed in the whole measurement system.

3.3.2 Passive Measure Issues

There are to issues when the address of a host involved in a measure change dynamically.

The huge number of hosts, the huge number of flows monitored makes it difficult the passive measurement system to detect the modification of the address of a flow.

The non-detection of the modification of the address of a flow make if impossible to consolidate consistently the statistics collected.

Header compression on slow links makes it difficult to perform passive analysis. This issue must be taken in account for 3 mains reasons. Troubleshooting small offices connectivity is costly due the absence of employees with network skill on these sites. It means that a technician has to go on site. As small offices are spread over large areas it is difficult to resolve the problem in the time defined in the contract. Finally as a global contract typically involves a huge number of small offices this point has an important economical influence.

At large, these issues should be addressed in prior by the 6QM project it aims to provide auditable measure results.

4. IP VERSION 6 OPERATIONS WORKING GROUP (V6OPS)

The IPv6 Operations Working Group (v6ops) develops guidelines for the operation of a shared IPv4/IPv6 Internet and provides guidance for network operators on how to deploy IPv6 into existing IPv4-only networks, as well as into new network installations to avoid the division of the Internet into separate IPv4 and IPv6 networks while ensuring global addressing and connectivity for all IPv4 and IPv6 nodes.

The aim of the WG is to collect issues experienced on operational IPv6 networks in a way to provide workarounds and inputs to the groups or areas responsible for the protocols or technologies involved. It publishes applicability statements and best current practice to facilitate IP version-independent applications developments, to fix security issues and permit IPv6 interoperability solutions.

Finally the V6OPS WG controls the usage made of the basic IPv6 transition mechanism already standardized.

4.1 Documents Distribution per Domain

This WG has not provided any RFC. It tracks the existence of IPv4 addresses in the documents written by the 9 IETF areas and proposes transition mechanisms for the different kind of networks, which are ISPs, enterprises, unmanaged networks and 3GPP.

Domain	Number of documents
Survey of IPv4 addresses in IETF areas	9
Transition scenarios	5
RFC	0
Total	14

Figure 4-1: V6OPS Documents Distribution per Domain

5. BENCHMARKING METHODOLOGY (BMWG)

The objectives of the Benchmarking Methodology Working Group are to define recommendations concerning the measurement of the performance characteristics of internetworking technologies. A topic is addressed while defining a terminology document and a methodology document. Despite these recommendations are applicable only to test performed in labs and despite they focus on the measurement of routing protocol performance and congestion, they define a lot of terminology and many metrics that may be potentially used as a basis for the measurement of the whole performance of an end to end service including both the signaling and the data.

5.1 Documents Distribution per Domain

Despite it focuses on the measure of the performance of the routing plane (6 documents), the BMWG provided the terminology and the methodology for various domain such as multicast, firewall and IPsec.

The large number of documents on the measurement of SUB IP layers (7 documents) indicates clearly that the QoS of the network layer relies mostly on the QoS provided by SUB IP layers including its signaling.

Domain	**Number of documents**
SUB IP	7
Routing	6
General purpose methodology	4
Multicast	2
Firewall	2
Packet Tunneling/IPsec	1
Total	22 (draft 10, RFC 12)

Figure 5-1: BMWG Documents Distribution per Domain

5.2 6QM and BMWG

As an IP service relies on both signaling and transfer capabilities, The QoS measured by the 6QM measurement system should integrate the traffic exchanged during the initiation of the service. Otherwise, as a signaling failure blocks the bandwidth consumption the measurement system will indicate excellent network performance despite the service is not available for customers.

5.2.1 Active Measure Issues

Regarding active probe it means initiating a service using the regular signaling, analyzing and measuring the performance of the initiation of the service, exchanging test packets corresponding to this service and measuring the corresponding network performance.

5.2.2 Passive Measure Issues

Regarding passive probe it means filtering and analyzing the packets exchanged during the initiation of a service, filtering the packets of data exchanged and analyzing the network performance.

6. IP PERFORMANCE METRICS (IPPM)

The IP Performance Measurement Working Group is developing a set of standard metrics that can be performed by network operators, end users, or independent testing groups to measure the quality, performance, and reliability of real Internet services. The metrics are:

- Connectivity.
- One-way delay and loss.
- Round-trip delay and loss.
- Delay variation.
- Loss patterns.
- Packet reordering.
- Bulk transport capacity.
- Link bandwidth capacity.

It is in charge of producing applicability statements of these metrics to characterize the performance of different services. Currently there is only one AS draft, which is proposed.

Despite the protocol requirement document that the control protocol should not depend on the test protocol, it is standardizing a unified solution to perform both the control and the measure, named OWAP.

The WG is standardizing the IPPM REPORTING MIB to retrieve the results of IPPM metrics, to optimize result reporting, to facilitate the communication of metrics to existing network management systems.

The WG is finalizing a registry of metrics to permit MIBs to refer to the same OBJECT IDENTIFIER.

The intent of the WG is to cooperate with other appropriate standards bodies and forums to promote consistent approaches and metrics. The ITU asked the IETF to cooperate on the definition of a general-purpose test packet named O.iptest.

6.1 Documents Distribution per Domain

The intent of the IPPM appears clearly: One document defines the framework, 9 documents define more that 30 metrics while 4 documents focus on the control or the management of the measurement of the metrics.

Domain	**Number of documents**
Metrics definition	9
Measurement protocol	2
Management	2
Framework	1
Applicability statement	1
Total	15 (draft 5, RFC 10)

Figure 6-1: IPPM WG Documents Distribution per Domain

6.2 6QM and IPPM WG

6.2.1 Active measure issues

OWAP control protocol is not flexible enough to perform measurement control among composite networks between administrative areas.

As OWAP test protocol is limited to UDP packets description its scope of usage is limited to 20 % of the cases.

6.2.2 Passive measure issues

Despite spatial measurement is described in the framework, the IPPM WG has not yet started to define spatial metrics. As a consequence active and passive measurement techniques cannot refer to a common superset of metrics definitions.

7. IP FLOW & PACKET INFORMATION EXPORT: IPFIX AND PSAMP

There are a number of IP flow information export systems in common use. These systems differ significantly, even though some have adopted a common transport mechanism; such differences make it difficult to develop generalized flow analysis tools. As such, there is a need in industry and the Internet research community for IP devices such as routers to export flow information in a standard way to external systems such as mediation systems, accounting/billing systems, and network management systems to facilitate services such as Internet research, measurement, accounting, and billing.

An IP flow information export system includes a data model, which represents the flow information, and a transport protocol. An "exporter," which is typically an IP router or IP traffic measurement device, will employ the IP flow information export system to report information about "IP flows," these being series of related IP packets that have been either forwarded or dropped. The reported flow information will include both (1) those attributes derived from the IP packet headers such as source and destination address, protocol, and port number and (2) those attributes often known only to the exporter such as ingress and egress ports, IP (sub)net mask, autonomous system numbers and perhaps sub-IP-layer information.

Packet exportation is a subset of flow exportation.

7.1 56th IETF

The IPFIX WG selected Netflow V9 as the basis exporter protocol but using TCP as transport protocol.

Before the next meting it will initiate the following documents:

- The IPFIX Architecture.
- The IPFIX Data Model.
- The IPFIX Protocol.
- The IPFIX Applicability.

The PSAMP WG is expected to use the same protocol for exporting the test packet description while defining templates for the test packet description.

Despite these 2 WG have a lot of common topics, the PSAMP WG is chartered to specify a MIB for the configuration of the packet sampling processes. This point is a potential issue for the next IETF meetings.

7.2 Documents Distribution per Domain

Domain	**Number of documents**
Architecture	2
Data Model	1
Protocol	1
Applicability	1
Requirement	1
Packet sampling	2
Total	8 drafts (4 to be create in IPFIX)

Figure 7-1: IPFIX WG Documents Distribution per Domain

7.3 6QM and IPFIX + PSAMP WG

Netflow V9 templates make it feasible to have a unique protocol to export packets and flow description to a collector that is in charge of performing instantaneous spatial metrics measurement using packets descriptions and statistics using the flows descriptions received.

8. REMOTE NETWORK MONITORING (RMONMIB)

The RMON MIB Working Group defines a set of managed objects for remote monitoring of networks. These objects will be the minimum necessary to provide the ability to monitor multiple network layers of traffic in remote networks; providing fault, configuration, and performance management, and will be consistent with the SNMP framework and existing SNMP standards.

8.1 Documents Distribution per Domain

It is important to notice that the framework is a still a draft. That explains while the different MIBs (12) specified do not interoperate and focus mainly on 'single point measure'.

Finally the 4 documents regarding the on the naming of protocol identifiers illustrates importance of operational interoperability in the monitoring.

Domain	**Number of documents**
Framework	1
Real time result Exportation	3
Performance monitoring MIB	3
SUB IP monitoring MIB	8
Protocol identifier	4
Total	19 (7 drafts + 12 RFC)

Figure 8-1: RMON WG Documents Distribution per Domain

8.2 6QM and RMON WG

The number of documents dedicated to naming of protocol identifiers illustrates the importance of operational interoperability in the monitoring.

8.3 56th IETF

FT requested a timeslot to present the need of protocol identifier for IPv6 and SUB IP. The need was recognized. In the 6QM context, Consulintel and FT will propose a draft to cover this aspect.

9. INTERNET TRAFFIC ENGINEERING (TEWG)

The Internet Traffic Engineering Working Group defines, develops, specifies, and recommends principles, techniques, and mechanisms for traffic engineering in the Internet. The primary focus of the tewg is the measurement and control aspects of intra-domain Internet traffic engineering. This includes provisioning, measurement and control of intra-domain routing, and measurement and control aspects of intra-domain network resource allocation. It also considers the problems of traffic engineering across autonomous systems boundaries.

9.1 Documents Distribution per Domain

The mapping of the QoS on SUB IP layers (6 documents) is the main concerns of traffic engineering. It relies on the routing protocols (2 documents) to exchange the traffic engineering information. It is clear that the main concern regarding QoS is service continuity.

Domain	**Number of documents**
SUB IP	6 (ATM 1, MPLS 5)
Routing	2
Service continuity	2
Framework	1
Management	1
Total	12 (9 drafts + 3 RFC)

Figure 9-1: TEWG WG Documents Distribution per Domain

9.2 6QM and TEWG

As TEWG has a strong requirement to guaranty end-to-end services continuity, the measurement system the 6QM project will develop should consider customer service continuity as the first level of QoS to control.

The measurement framework of the TEWG defines network monitoring in 4 points:

- Determining the operational state of the network, including fault detection.
- Monitoring the continuity and quality of network services.
- Evaluating the effectiveness of traffic engineering policies.
- Verifying peering agreements between service providers.

Coupling active and passive measurements techniques in the 6QM measurement system satisfies these 4 points while not depending nor on providers' networks specificities, nor on SUB IP. Moreover the resulting measurement system will be applicable for new services implemented on the top of IPv6 and new SUB IP.

10. INTER-DOMAIN ROUTING (IDR)

The Inter-Domain Routing Working Group is chartered to standardize and promote the Border Gateway Protocol Version 4 (BGP-4) [RFC 1771] capable of supporting policy based routing for TCP/IP Internets. The objective is to promote the use of BGP-4 to support IP version 4 and IP version 6. The working group will continue to work on improving the scalability of BGP.

10.1 Documents Distribution per Domain

This working group is quite mature: it has 12 documents related to applicability and 39 RFCs.

BGP do not depend on IP sub layers as illustrated by the small number of documents of SUB IP.

The 4 documents on route continuity shows that service connectivity is a concern of this working group.

There is one document, which addresses the IPv6 scoped unicast addresses.

Domain	Number of documents
Routing	21
Applicability	12
Route continuity	4
IPv6 & SUB IP	2
Security	2
Management	2
Multihoming	1
Total	44 (15 drafts + 39 RFC)

Figure 10-1: IDR WG Documents Distribution per Domain

10.2 6QM and IDR

BGP provides path information and AS information that not depends on network implementation and are need for inter domain peering QoS control. Netflow exports these pieces of information. Such information should be collected by the 6QM measurement system to identify the path of the flow in a way to help to troubleshoot connectivity problems.

11. AUDIO AND VIDEO TRANSPORT (AVT)

11.1 Description of Working Group

The Audio/Video Transport Working Group specified RTP, a protocol for real-time transmission of audio and video over UDP and IP multicast. Currently it revises the main RTP specification and completes the RTP MIB.

11.2 Documents Distribution per Domain

This working group specialty is the definition of RTP payload types (36 documents) and concentrates on video transmission, audio transmission and compression.

There are 5 documents to address network limitation and poor network performance.

Domain	**Number of documents**
Video	17
Compression	7
Audio	7
Network Performance	5
Management	1
Total	58 (27 drafts + 31 RFC)

Figure 11-1: IDR WG Documents Distribution per Domain

11.3 6QM and AVT

The huge number of payload type defined in this WG illustrates the fundamental need of technical optimization of the packetization of voice signals on asynchronous networks. Despite these efforts 5 documents concern themselves with considering network performance limitations.

Customers used to have phone services with high quality, continuity and availability. Consequently SLA describing VOIP services have strong quality, continuity and availability requirements.

Arming the network for controlling all the aspects of an VOIP service on IPv6 is a major case study the 6QM project should consider because that prefigures the constraints of the future interactive services IPv6 will carry.

12. RFC DIRECTLY RELATED TO QOS MEASUREMENTS

These three RFCs are directly related to Q0S measurements:

- Framework for IP Performance Metrics (RFC 2330).
- A One-way Delay Metric for IPPM (RFC 2679).
- A One-way Packet Loss Metric for IPPM (RFC 2680).

12.1 Standardized Measurement Architectures

In the case where measurement points, aggregation points, metrics computation and user application points are located on physically separated devices, transferring packets, aggregates and measurement results between these devices becomes essential. In this section we analyze existing standardized measurement architectures according to classifiers defined in the deliverable D2.2 and mostly in the IETF context.

12.1.1 RMON

[Wal02] defines the RMON framework. Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. The user community with the help of the Internet Engineering Task Force (IETF) defined RMON. It became a proposed standard in 1992 as RFC 1271 (for Ethernet). The current standard describing RMON is [RFC2819]. Several extensions have been defined that extend the capacity of RMON for different types of networks and environments.

RMON delivers information in ten RMON groups of monitoring elements, each providing specific sets of data to meet common network-monitoring requirements. Each group is optional so that vendors do not need to support all the groups within the Management Information Base (MIB). Some RMON groups require support of other RMON groups to function properly. Existing groups are described bellow:

The Ethernet statistics group contains statistics measured by the probe for each monitored Ethernet interface on this device.

The history control group controls the periodic statistical sampling of data from various types of networks.

The Ethernet history group records periodic statistical samples from an Ethernet network and stores them for later retrieval.

The alarm group periodically takes statistical samples from variables in the probe and compares them to previously configured thresholds. If the monitored variable crosses a threshold, an event is generated. A hysteresis mechanism is implemented to limit the generation of alarms.

The host group contains statistics associated with each host discovered on the network. This group discovers hosts on the network by keeping a list of source and destination MAC Addresses seen in good packets promiscuously received from the network.

The hostTopN group is used to prepare reports that describe the hosts that top a list ordered by one of their statistics. The available statistics are samples of one of their base statistics over an interval specified by the management station. Thus, these statistics are rate based. The management station also selects how many such hosts are reported.

The matrix group stores statistics for conversations between sets of two addresses. As the device detects a new conversation, it creates a new entry in its tables.

The filter group allows packets to be matched by a filter equation. These matched packets form a data stream that may be captured or may generate events.

The Packet Capture group allows packets to be captured after they flow through a channel.

The event group controls the generation and notification of events from this device.

12.1.2 IPPM

[Ste02] defines a MIB for managing the measures using the IP performance metrics specified by the IPPM Working Group. It specifies the objects to manage the results of the measure of metrics standardized by IPPM Working Group. They are built on notions introduced and discussed in the IPPM Framework document.

12.1.3 RTFM

The RTFM architecture is an attempt by IETF to standardize several aspects of flow definition, capture and metering operations [RFC2722]. The architecture has the following property:

- The traffic flow model can be consistently applied to any protocol, using address attributes in any combination at the 'adjacent', network and transport layers of the networking stack.
- Traffic flow attributes are defined in such a way that they are valid for multiple networking protocol stacks, and that traffic flow measurement implementations are useful in multi-protocol environments.
- Users may specify their traffic flow measurement requirements by writing 'rule sets', allowing them to collect the flow data they need while ignoring other traffic.
- The data reduction effort to produce requested traffic flow information is placed as near as possible to the network measurement point. This minimizes the volume of data to be obtained (and transmitted across the network for storage), and reduces the amount of processing required in traffic flow analysis applications.

From an architectural point of view the RTFM architecture is made of four components:

- Meters observe packets passing through measurement points classifies them into certain groups, accumulate usage data and store these results in flow tables. As such meters can be described as a combination of MP and AP according to our QoS measurement architecture classification.
- Manager: A traffic measurement manager is an application, which configures 'meter' entities and controls 'meter reader' entities. It sends configuration commands to the meters, and supervises the proper operation of each meter and meter reader. It may well be convenient to combine the functions of meter reader and manager within a single network entity.
- Meter reader: A meter reader transports usage data from meters so that it is available to analysis applications.

- Analysis applications: An analysis application processes the usage data so as to provide information and reports, which are useful for network engineering and management purposes.

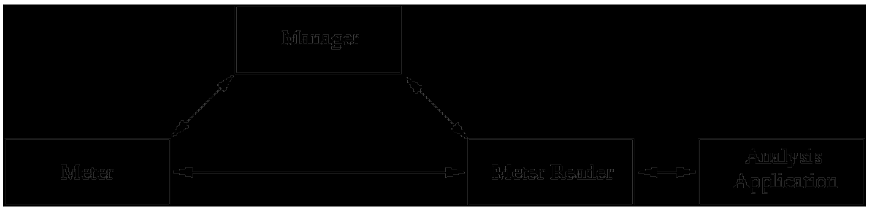

Figure 12-1: The RTFM Architecture

These components as well as the relation between components are presented in the RTFM architecture.

The RTFM working group has also defined additional components that may participate in the RTFM architecture:

- An RTFM MIB. [RFC2720] defines a Management Information Base (MIB) for use in controlling an RTFM Traffic Meter, in particular for specifying the flows to be measured. It also provides an efficient mechanism for retrieving flow data from the meter using SNMP.
- A rule set language. [RFC2723] defines a language for specifying rule sets, i.e. configuration files that may be loaded into a traffic flow meter so as to specify which traffic flows are measured by the meter, and the information it will store for each flow.
- Measurement Attributes Extensions for traffic flow measurement ([RFC2724]).

12.1.4 Sflow

[RFC3176] defines the sFlow technology. sFlow is a technology for monitoring traffic in data networks containing switches and routers. In particular, it defines the sampling mechanisms implemented in an sFlow Agent for monitoring traffic, the sFlow MIB for controlling the sFlow Agent, and the format of sample data used by the sFlow Agent when forwarding data to a central data collector.

The sFlow monitoring system consists of an sFlow Agent (embedded in a switch or router or in a stand alone probe) and a central data collector, or sFlow Analyzer. The sFlow Agent uses sampling technology to capture traffic statistics from the device it is monitoring. sFlow Datagrams are used to immediately forward the sampled traffic statistics to an sFlow Analyzer for analysis.

[RFC316] describes the sampling mechanisms used by the sFlow Agent, the SFLOW MIB used by the sFlow Analyzer to control the sFlow Agent, and the sFlow Datagram Format used by the sFlow Agent to send traffic data to the sFlow Analyzer.

12.1.5 IPFIX

[Nor02] defines the architecture for IPFIX. The main objectives of this document are to describe the key architectural components of IPFIX, define the architectural requirements, e.g., Recovery, Security, etc for the IPFIX framework, define the criteria to select the IPFIX Protocol and specify the control/data message formats and handshaking details to pass the IP flow information.

From an architectural point of view the IPFIX framework defines the following components:

- Collector: The collector receives flow records from one or more exporters. The collector might process or store received flow record.
- Observation Point: The observation point is a location in the network where IP packets can be observed. Examples are, a line to which a probe is attached, a shared medium, such as an Ethernet-based LAN, a single port of a router, or a set of interfaces (physical or logical) of a router.
- Metering Process: The metering process generates flow records. Input to the process are IP packets observed in an observation point. The metering process consists of a set of functions that includes packet header capturing, time stamping, sampling, classifying, and maintaining flow records.

Five protocols are currently proposed to implement the protocol specified in [Nor02]:

- Cisco Netflow is a feature available on almost all Cisco routers, which makes it the de facto standard. [Clai02] presents the version 9 of the architecture. Architecturally Netflow is based on two components:
    - The Exporter: A device with Netflow services enabled. The exporter monitors packets entering an observation point and creates flows out of these packets. The information from these flows is exported in the form of Flow Records to the collector.
    - Netflow Collector. The Netflow Collector receives Flow Records from one or more Exporters. It processes the received export packet, i.e. parses, stores the Flow Record information. The flow records may be optionally aggregated before storing into the hard disk.
- Diameter [Cal02] is a protocol under standardization by IETF for Authentication, Authorization, and Accounting purposes. Because of it's flexibility Diameter can be easily extended to support flow information transport. However this flexible and general architecture render him more complex than other protocols.
- The LFAP protocol [RFC2124] LFAP was developed specifically for IP flow accounting. As such it is well suited to support the communication between the Exporting Process and an IPFIX Collecting process. From an architectural point of view LFAP is made of three main components: IPFIX devices that produce flow information, Collecting processes and finally applications. One Collecting process services multiple IPFIX Devices. Each IPFIX Device may have one or more backup Collectors. An application then retrieves the flow data from the Collecting devices. The LFAP protocol is used between the IPFIX Devices and Collecting process to exchange flow accounting data.
- The CRANE protocol [Zha02] can be viewed as an application that uses the data transport service provided by lower layer protocols. It relies on a transport layer protocol to deliver reliable, in-sequence data packets.
- The IPDR protocol evaluation document [Mey02-1] defines a document format, which offers a compact and efficient representation of usage accounting data. The encoding format is based on XDR. The encoding supports a basic set of primitive data types and a number of additional types, which are derived from the primitive types. The mechanisms for encoding and transport are completely separate in IPDR. The Compact IPDR format can be used to serialize usage information to a file or it can be used to serialize usage information onto a reliable transport, such as TCP. For real time push oriented communication the streaming over a reliable transport is preferred, as described in Streaming IPDR [Mey02-0]. A file can also be used as the unit of exchange. IPDR's XML-Schema based format has the additional benefit of providing a well-defined equivalent XML encoding. Both the compact and XML formats are based on a common

service definition specification. The service specification is expressed as one or more XML Schema documents. Service specifications are the primary means of extension in IPDR.

[Zs02] provides an analysis of the ability of IPFIX flows be used by additional components to provide IPPM metrics compliant measurements. These findings are summarized in table 3 below:

Metric	IPFIX as standardized	IPFIX with extension
Type-P-*-Connectivity [RFC2678]	Not considered	
Type-P-*-One-Way-Delay [RFC2679]	X	
Type-P-*-Packet-Loss [RFC2680]		X
Type-P-*-Round-Trip-Delay [RFC2681]		X
Type-P-One-Way-Loss-* [RFC3357]	X	
Type-P-One-Way-ipdv-* [Dem02]		X
Type-P-Packet-Reordering-* [Mor02]	Not considered	

Figure 12-2: IPFIX Ability to Provide IPPM Compliant Measurements

12.1.6 PSAMP

[Du02] describes the framework for Passive Packet Measurement (PSAMP). It provides a framework for a standard set of capabilities for network elements to sample packets and report on them. One motivation to standardize these capabilities comes from the requirement for measurement-based support for network management and control across multi-vendor domains. This requires domain wide consistency in the types of sampling schemes available, the manner in which the resulting measurements are presented, and consequently, consistency of the interpretation that can be put on them.

The framework for passive measurement includes three main parts: the selection of packets for measurement, the creation and export of measurement reports, and the content and format of the measurement records.

Compared to other work the PSAMP measurement capabilities are positioned as suppliers of packet samples to higher-level consumers, including both remote collectors and applications, and on board measurement-based applications. Indeed, development of the standards within the framework described in the PSAMP framework should take into account the measurement requirements of standards in other IETF working groups, including IPPM and TEWG. Conversely, it is expected that aspects of the PSAMP framework not specifically concerned with the central issue of packet sampling may be able to leverage work in other working groups. The prime example is the format and export of measurement reports, which may leverage the work of IPFIX.

12.1.7 Conclusion

The table below provides a comparison between existing standardized proposals.

Architecture	Passive/Active	SCOPE	Components Included	Packet	Flow	Metric	METRICS/OUTPUT
RMON	Passive	Path	MP, AP, MCP	X		x	Throughput, Flows, Packets
IPPM	Active	End to End/ Path	MP, AP, MCP			X	OWC,RTC,RTD, OWD,OWPL,OWR, OWPDV
RTFM	Passive	Path	MP, AP, MCP		X	x	Flows Throughput
Sflow	Passive	Path	MP, AP		X		Flows
IPFIX	Passive	Path	MP, AP		X		Flows
PSAMP	Passive	Path	MP, AP	X			Packets

Figure 12-3: Comparison of Standardized Proposals

12.2 Test Packets Standardization in IPPM WG

OWAP **[OWAP]** scope id deliberately limited. It does respect the requirement on the independency of the Test protocol and of the Control protocol **[OWAP-Req]**. The test protocol is limited to UDP. So it does not permit the measurement of the performance of any type of applications. Especially it does not permit the measurement of the QOS of TCP based applications.

Standard test packets exchanged by active probes are filtered efficiently by passive points of measure available. Spatial metrics **[Ste03]** are computed using the end-to-end information and the intermediary information. These metrics are mandatory for troubleshooting and for SLA management.

ITU is standardizing a general-purpose test packet for IPv4 and IPv6 **[O.iptest]** directly inspired of an individual draft describing a standard test packets **[Ste04]**.

12.2.1 Security

To avoid the measurements systems to be used to make attacks there is a strong requirement to propose a security mechanism to control the access to the setup of the network measures.

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

13. SECURITY REVIEW

It should be recognized that conducting Internet measurements could raise both security and privacy concerns. Active techniques, in which traffic is injected into the network, can be abused for denial-of-service attacks disguised as legitimate measurement activity. Passive techniques, in which existing traffic is recorded and analyzed, can expose the contents of Internet traffic to unintended recipients.

Actually the working groups involved in the measurement do not address the security of the measurement system in details.

14. Summary and Conclusions

This document presents the high level IETF activities related to this project. The main working groups on this subject are:

- IP Version 6 Working Group (ipv6).
- Benchmarking Methodology (bmwg).
- IP Performance Metrics (ippm).
- IP Flow Information Export (ipfix).
- Packet Sampling (psamp).
- Remote Network Monitoring (rmonmib).
- Internet Traffic Engineering (tewg).
- Inter-Domain Routing (idr).
- Audio/Video Transport (avt).

14.1.1 Inputs for 6QM

The analysis of the document distribution per domain identifies the main WG concerns, which have to be considered as inputs to the 6QM project.

The traffic engineering Working Group synthesizes network monitoring as:

- Determining the operational state of the network, including fault detection.
- Monitoring the continuity and quality of network services.
- Evaluating the effectiveness of traffic engineering policies.
- Verifying peering agreements between service providers.

They are consistent with the requirements specified in D2.1 and D2.2. Moreover they are consistent with the order of the priorities specified by WP2:

- Troubleshooting
- Network and transport SLA.
- Standard configuration & reporting interfaces.
- Security and reliability of the control & reporting planes.
- Peering management of the measurement systems.

There are several standardized components related to the 6QM WG:

- RMON.
- IPPM.
- RTFM.
- Sflow.
- IPFIX.
- PSAMP.

IPPM specifies the measurements definitions and methodology while IPFIX and PSAMP provides the filtering and the exportation blocks.

The standardization of the operational measurements and the standardization of the management of operational measurements is addressed in the working groups RMON, IPPM, PSAMP and IPFIX.

Despite Working Groups IPv6, BMWG, TEWG and AVT are not directly involved in the process of standardization of the different aspects related to operational measurement. The analysis of these WG provides good indication of the complexity the protocol IPv6 added to a measurement system. It clearly demonstrates the limitation of the applicability of the results if the process of measurement does not survey the whole end-to-end service including initiation step.

During the 56th IETF (March 2003) 6QM partners participated actively to these working group sessions. IPFIX and PSAMP WG have chosen Netflow V9 has a basis protocol for exportation of packets and flows descriptions. The metrics registry of the IPPM WG identifies 33 metrics and is going to last call. During the RMON session, FT presented the need of protocol identifiers for configuring measures in active and passive IPv6 and SUB IP points of measures: 6QM (Consulintel and FT) will propose a draft on this topic.

6QM partners have 2 others potential inputs IETF that are tied together. FT would propose the definition of spatial metrics to become an IPPM WG item. Fokus and Hitachi would present a solution for measuring the delay per segment in IPFIX. As this spatial metric is not standardized and is defined in the proposal of FT, 6QM partners might break in Vienna, the 'chick and a egg' and permit to go further in coupling the existing measurement techniques.

These standardization actions would define the terminology and the minimal needs for reporting measure results of the QoS of IPv6 based network and services. The standardization of a general-purpose test packet in O.iptest recommendation of the ITU will permit to get a minimal interoperability between heterogeneous manufacturer devices and among composite networks.

This will be a condition to go further in the definition of inter domain SLAs and applicative SLAs. The role of 6QM in this context is to promote the dissemination of what is lacking in this area. The ability to build a shared IPv6 QoS measurement system providing the basis for peering European agreement should be a good point to leverage the proposals made in 6QM.

15. REFERENCES

Name	Title	Version	Date
[Cal02]	Diameter Base Protocol, draft-ietf-aaa-diameter-15.txt, Pat R. Calhoun, John Loughney, Erik Guttman, Glen Zorn, Jari Arkko, October 2002.		October 2002
[Clai02]	Cisco Systems NetFlow Services Export Version 9, draft-bclaise-netflow-9-00.txt, B. Claise, June 2002.		June 2002
[Dem02]	IP Packet Delay Variation Metric for IPPM, Internet Draft, draft-ietf-ippm-ipdv-10.txt, C. Demichelis, P. Chimento, August 2002.		August 2002
[Du02]	A Framework for Passive Packet Measurement, draft-ietf-psamp-framework-00, Nick Duffield, September 2002.		September 2002
[Mey02-0]	Reliable Streaming Internet Protocol Detail Records, draft-meyer-ipdr-streaming-00, J Meyer, August 2002.		August 2002
[Mey02-1]	Evaluation Of Streaming IPDR Against IPFIX Requirements, draft-meyer-ipfix-ipdr-eval-00, J. Meyer, September 2002.		September 2002
[Mor02]	Reordering Metric for IPPM, Internet Draft, draft-ietf-ippm-reordering-00.txt, A.Morton L.Ciavattone, G.Ramachandran, S.Shalunov, J.Perser, 2002.		2002
[Nor02]	Architecture Model for IP Flow Information Export, draft-ietf-ipfix-architecture-02.txt, K. Norseth, Ganesh Sadasivan, June 2002.		June 2002
[O.iptest]	Test and measurement equipment to perform tests at the IP layer		2003
[RFC2678]	IPPM Metrics for Measuring Connectivity, RFC 2678, J. Mahdavi, V. Paxson, September 1999.		September 1999
[RFC2679]	A One-way Delay Metric for IPPM, RFC 2679, G. Almes, S. Kalidindi, M. Zekauskas September 1999.		September 1999
[RFC2680]	A One-way Packet Loss Metric for IPPM, RFC 2680, G. Almes, S. Kalidindi, M. Zekauskas September 1999.		September 1999
[RFC2681]	A Round-trip Delay Metric for IPPM, RFC 2681, G. Almes, S. Kalidindi, M. Zekauskas September 1999.		September 1999

[RFC2124]	Cabletron's Light-weight Flow Admission Protocol Specification, Version 1.0, RFC 2124, P. Amsden, J. Amweg, P. Calato, S. Bensley, G. Lyons, March 1997.		March 1997
[RFC2722]	Traffic Flow Measurement: Architecture, RFC 2722, N. Brownlee, C. Mills, C. Ruth, October 1999.		October 1999
[RFC2720]	Traffic Flow Measurement: Meter MIB, RFC 2720, N. Brownlee, October 1999.		October 1999
[RFC2723]	SRL: A Language for Describing Traffic Flows and Specifying Actions for Flow Groups, RFC 2723. N. Brownlee, October 1999.		October 1999
[RFC2724]	RTFM: New Attributes for Traffic Flow Measurement. RFC 2724, S. Handelman, S. Stibler, N. Brownlee, C. Ruth, October 1999.		October 1999
[RFC2819]	Remote Network Monitoring Management Information Base, RFC 2819, S. Waldbusser, May 2000.		May 2000
[RFC3176]	InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks, RFC 3176, P. Phaal, S. Panchen, N. McKee, September 2001.		September 2001
[RFC3357]	One-way Loss Pattern Sample Metrics, RFC 3357, R. Koodli, R. Ravikanth, August 2002.		August 2002
[Ste02]	IPPM Reporting MIB, draft-ietf-ippm-reporting-mib-00.txt, E. Stephan, J. Jewitt, June 2002.		June 2002
[Ste02]	IPPM Reporting MIB, draft-ietf-ippm-reporting-mib-00.txt, E. Stephan, J. Jewitt.		June 2002
[Ste03]	IPPM spatial metrics measurement, draft-stephan-ippm-spatial-metrics-00.txt, E. Stephan		Sept 2002
[Wal02]	The RMON Framework, draft-ietf-rmonmib-framework-01.txt, Steve Waldbusser, R.G. Cole, C. Kalbfleisch, D. Romascanu, August 2002.		August 2002
[Zha02]	XACCT's Common Reliable Accounting for Network Element (CRANE) Protocol Specification Version 1.0, draft-kzhang-crane-protocol-05.txt, Kevin Zhang, Eitan Elkin, August 2002.		August 2002
[Zse02]	Sampling and Filtering Techniques for IP Packet Selection, T. Zseby, M Molina, F. Raspall, Internet Draft, draft-ietf-psamp-sample-tech-00.txt, April 2002.		April 2002

Figure 15-1: References