A Framework for Internet Traffic Engineering Measurement

1. Abstract

In this document, a measurement framework for supporting the traffic engineering of IP-based networks is presented. It is intended for the TEM (Traffic Engineering Measurement) category as described in the TEWG charter. Consideration for including this document as a TEWG working-group item for further development is requested.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119.

3. Introduction
This document describes a framework for Internet traffic engineering measurement, with the objective of providing principles for the development of a set of measurement systems to support the traffic engineering of IP-based networks [1]. A major goal is to provide guidance for establishing protocol-independent and platform-neutral traffic measurement standards to achieve multi-vendor interoperability. It is critical to minimize the possibilities of inconsistencies arising from, e.g., overlapping data collecting and processing at various protocol levels, due to the use of different measurement principles by different vendors or network operators.

The initial scope is limited to those aspects of measurement pertaining to intra-domain, i.e., within a given autonomous system as well as on its boundary with other domains. The focus is primarily on traffic engineering in Internet service provider environments.

In this document, the use of traffic measurement in traffic characterization, network monitoring, and traffic control is first described. Depending on the network operations to be performed in these tasks, three different time scales can be identified, ranging from months, through days or hours, to minutes or less. To support these operations, traffic measurement must be able to capture accurately, within a given confidence interval, the traffic variations and peaks without degrading network performance and without generating an immense amount of data. Therefore, specification of a suitable read-out period for each service class for traffic summarization is essential.

Traffic measurement can be performed on the basis of flows, interfaces, links, nodes, node-pairs, or paths. Based on these objects, different measurement entities can be defined, such as traffic volume, average holding time, bandwidth availability, throughput, delay, delay variation, packet loss, and resource usage. Using these measured traffic data, in conjunction with other network data such as topological data and router configuration data, traffic matrix and other relevant statistics can be derived for traffic engineering purposes. Traffic measurement also plays a key role in network performance management.

As a framework, this document is mainly concerned with a discussion of various technical issues surrounding traffic measurement. Requirements for traffic measurement are contained in the Annex. As far as possible and to avoid duplication of effort, relevant work done in this area by other standards organizations will be applied or adapted, and references to them will be made. These include, in particular,

- IP Performance Metrics (IPPM) Working Group of the IETF: its framework document [2] and documents on individual metrics [references to be added]
4. Terminology

The intent of this section is not to provide definition or description of terms used in this document. Rather, it is to highlight the difference in usage of related terms.

Path, route

A path refers to an MPLS tunnel, i.e., a label-switched path. A route is any unidirectional sequence of nodes and links, for sending packets from a source node to a destination node. (Note: There are also methods for creating paths with other technologies such as frame-relay or ATM. Applicability of the measurement described in this document to these technologies is to be covered in the next version of this document.)

Throughput, traffic volume

Both quantities can be applied to a network, a network segment, or an individual network element. Throughput of a network, as a measure of delivered performance, refers to the maximum sustainable rate of transferring packets successfully across the network, under given network conditions (e.g., a given traffic mix) while meeting QoS objectives. (This is consistent with the definition of throughput for a network interconnect device as specified in [5].) For real-time network control, active measurement of throughput by probing may be used to determine the currently available capacity of a network to carry additional traffic. Traffic volume, as a measure of the traffic carried, characterizes the level of traffic that a network is designed to support. Passive measurement of the traffic volume is usually used to estimate the long-term offered traffic for the purposes of network dimensioning in the capacity-management and network-planning processes (see the Section on Time Scales for Network Operations). A network should be properly dimensioned so that its throughput is adequate to handle the expected traffic volume.

Throughput is expressed in terms of number of data units per time unit. Traffic volume is expressed in data units with reference to a read-out period (see the Section on Read-Out Periods). For transmission systems, the data unit is usually a multiple of either bits or bytes. For processing systems, the data unit is usually a multiple of packets.

5. Uses of Traffic Measurement

Traffic measurement is used to collect traffic data for the following purposes:

Traffic characterization
identifying traffic patterns, particularly traffic peak patterns, and their variations in statistical analysis; this includes developing traffic profiles to capture daily, weekly, or seasonal variations.

determining traffic distributions in the network on the basis of flows, interfaces, links, nodes, node-pairs, paths, or destinations.
estimation of the traffic load according to service classes in different routers and the network.

observing trends for traffic growth and forecasting of traffic demands.

Network monitoring

determining the operational state of the network, including fault detection.
monitoring the continuity and quality of network services, to ensure that QoS/GoS objectives are met for various classes of traffic, to verify the performance of delivered services, or to serve as a means of sectionalizing performance issues seen by a customer (QoS reflects the performance perceivable by a user of a service, while GoS is used by a service provider for internal design and operation).
evaluating the effectiveness of traffic engineering policies, or triggering certain policy-based actions (such as alarm generation, or path preemption) upon threshold crossing; this may be based on the use of performance history data.

verifying peering agreements between service providers by monitoring/measuring the traffic flows over interconnecting links at border routers; this includes the estimation of inter- and intra-network traffic, as well as originating, terminating, and transit traffic that are being exchanged between peers.

Traffic control

adaptively optimizing network performance in response to network events, e.g., rerouting to work around congestion or failures.

providing a feedback mechanism in the reverse flow messaging of RSVP-TE or CR-LDP signaling to report on actual topology state information such as link bandwidth availability.
support of measurement-based admission control, i.e., by predicting the future demands of the aggregate of existing flows so that admission decisions can be made on new flows.

6. Time Scales for Network Operations

The information collected by traffic measurement can be provided to the end user or application either in real time or for record in non-real time, depending on the activities to be performed and the network actions to be taken. Traffic control will generally require real-time information. For network planning and capacity management
as described below, information may be provided in non-real time after the processing of raw data.

Broadly speaking, the following three time scales can be classified, according to the use of observed traffic information for network operations [6].

Network planning
Information that changes on the order of months is used to make traffic forecasts as a basis for network extensions and long-term network configuration. That is, for planning the topology of the network, planning alternative routes to survive failures or determining where capacity must be augmented in advance of projected traffic growth. Forecasting and planning may also lead to the introduction of new technology and architecture.

Capacity management
Information that changes on the order of days or hours is used to manage the deployed facilities, by taking appropriate maintenance or engineering actions to optimize utilization. For example, new MPLS tunnels may be set up or existing tunnels modified while meeting Service Level Agreements. Also, load balancing may be performed, or traffic may be rerouted for re-optimization after a failure.

Real-time network control
Information that changes on the order of minutes or less is used to adapt to the current network conditions in near real time. Thus, to combat localized congestion, traffic management actions may perform temporary rerouting to redistribute the load. Upon detecting a failure, traffic may be diverted to pre-established, secondary routes until more optimized routes can be arranged.

7. Read-Out Periods

A measurement infrastructure must be able to scale with the size and the speed of a network as it evolves. Hence, it is important to minimize the amount of data to be collected, and to condense the collected data by periodic summarization. This is to prevent network performance from being adversely affected by the unnecessarily excessive loading of router control processors, router memories, transmission facilities, and the administrative support systems.

A measurement interval is the time interval over which measurements are taken. Some traffic data must be collected continuously, while others by sampling, or on a scheduled basis. For example, peak loads and peak periods can be identified only by continuous measurement as traffic typically fluctuates irregularly during the whole day. If traffic variations are regular and predictable, it may be possible to measure the expected normal load on pre-determined portions of the day. This requires the definition of a busy period. Special studies on selected segments of the network may be conducted on a scheduled basis. Active measurement, with the
involvement of network operator, may be activated manually. For instance, active throughput measurement may be used to identify alternate routes during periods of network congestion.

A measurement interval consists of a sequence of consecutive read-out periods. Summarization is usually done by integrating the raw data over a pre-specified read-out period. The granularity of this period must be suitably chosen. It should be short enough to capture, with acceptable accuracy, the bursty nature of the traffic, i.e., the traffic variations and peaks. Since measurements represent a load for the router, the read-out period should not be so short that router performance is degraded while a voluminous quantity of data is produced. Also, read-out may be started when the measured data exceeds a preset threshold, or when the space allocated for temporarily holding the data in a router is exhausted.

For a multi-service IP-based network, each service typically has its own traffic characteristics and performance objectives. To ensure that service-specific features are reflected in the measurement process, different read-out periods may be needed for different classes of service.

8. Measurement Bases

Measurements can be classified on the basis of where, and at which level the traffic data are gathered and aggregated. This is similar to the concept of a population of interest as specified in ITU-T Recommendation I.380/Y.1540. As defined therein, this refers to a set of packets, possibly relative to a particular pair of source and destination hosts, for the purposes of defining performance parameters. However, measurement bases as used here may not have any association with a source-destination pair.

In this document, customer-based measurements are not considered. Service providers will make decisions on how to perform the measurements needed, and there are various tradeoffs involved. One option is to obtain the measurements directly from the network elements themselves, e.g., via SNMP. Collecting the measurements on the operational network elements such as routers is sometimes a performance concern. Currently, there are a number of third-party measurement/monitoring products available. Hence, another option is to deploy such equipment, which might have performance advantages but also introduces additional cost.

Regardless of the type of measurement source, either a network element or a third-party product, measurements should be collected, as far as possible, by a measurement source without requiring coordination with other measurement sources. Thus, it is desirable to perform those measurements that do not require the use of specialized monitoring equipment connected to the network at multiple locations. While each measurement source may act autonomously with regard to taking measurements, a network operator may specify some network-wide policy regarding measurement.
scheduling. Such policy may be, say, the use of the same time of
day, the same measurement interval, or measurement intervals that
are multiples of each other (e.g., nested intervals with
synchronized boundaries). A schedule therefore should include such
time information as the start, the duration, and periodicity of a
certain measurement.

The following measurement bases are considered in this document.

Flow-based

This is conceptually similar to the call detail record (CDR) in
telecommunication networks. It is primarily used on interfaces at
access routers, edge routers, or aggregation routers where traffic
originates or terminates, rather than on backbone routers in the
core network. Like CDR measurements, flow-based records are used to
collect detailed information about a flow. This includes such
information as source and destination IP addresses/port numbers,
protocol, type of service, timestamps for the start and end of a
flow, packet count, octet count, etc.

As flow is a fine-grained object, measuring every flow that passes
through all the edge devices may not be scalable or feasible.
Hence, per-flow data are usually used in a special study conducted
on a non-continuous schedule and on selected routers only. Sampling
of flow-based measurements may also be needed to reduce both the
amount of data collected and the associated overhead.

Interface-based, link-based, node-based

Passive, i.e., in-service non-intrusive, measurement can be taken at
each network element. For example, SNMP MIBs use passive monitoring
to collect raw data on an interface at an edge or backbone router.
This includes data such as counts on packets and octets
sent/received, packet discards, errored packets. While not intended
for core network, RMON can possibly be used in the access link of an
ISP to provide managed Internet service to corporate LANs.
(Consideration for link bundling in next version of this document.)

Node-pair-based

Active measurements by probing, as specified in the IPPM framework,
can be conducted between each pair of major routing hubs for
determining edge-to-edge performance of a core network. This
complements the passive measurements of the previous sub-section,
which provide local views of the performance of individual network
elements.

In telecommunications networks, each established call has an
associated node-pair. By maintaining a set of node-pair data
registers (usage, peg count, overflow, etc) in each switch, node-
pair-based measurements for traffic statistics such as the load
between a given node pair are taken directly. In contrast, in IP-
based networks, currently such kind of node-pair-based measurements cannot be taken directly. However, it is possible to infer them from flow-based passive measurements and other network information. A problem with this approach is that flow-based measurement data are voluminous. Also, another problem that must be accounted for is the routing changes among the multiple routes due to, e.g., a change in the configuration of intradomain routing, or a change in interdomain policies made by another autonomous system. This is further discussed in the Section on Traffic Matrix Statistics.

Path-based

In this document, the term path specifically refers to MPLS tunnel, or label-switched path.

The ability of MPLS to use fixed preferred paths for routing traffic, so-called route pinning, gives the means to develop path-based measurements. This may enable the development of methodologies for such functions as admission control and performance verification of delivered service.

Like a flow, a path is associated with a pair of nodes. However, path is a more coarse-grained object than flow, as paths are usually used to carry aggregated traffic. In addition, when routing changes occur, the amount of traffic to be carried by a path will either not be affected or be merged with that of another path. Because of these properties, path-based measurements are more scalable and may be used to provide more readily an accurate, network-wide, view of the traffic demands. (For example, the traffic between a given pair of nodes may be inferred from the aggregate of the traffic carried by all the paths either terminated by or passed through the same node-pair.)

9. Measurement Entities

A measurement entity defines what is measured: it is a quantity for which data collection must be performed with a certain measurement. A measurement type can be specified by a (meaningful) combination of a measurement entity with the measurement basis described in the previous section.

Entities related to traffic and performance

Some of the measurement entities listed below, such as throughput, delay, delay variation, and packet loss, are related to the IPPM performance metrics or the 1.380/Y.1540 performance parameters.

- Traffic volume (mean and variance for normal/high load, in bits, bytes, or packets transferred, as averaged over a given time interval), on a per service class basis, at various aggregation levels (IP address prefix, node, network edge, customer, or autonomous system)
Note: (1) This is a measurement for the traffic carried by a network, a network segment, or an individual network element. When measured during the busy period, this entity is normally used to estimate the traffic offered. However, the estimation procedure should take into account such factors as congestion, which may result in decreased carried traffic. In addition, congestion may lead to user behavior such as reattempt or abandonment, which may affect the actual traffic offered. (To include a discussion of the relevance and applicability of second-order statistics.) (2) Measurement of traffic volumes over interconnecting links at border routers can be used to estimate the traffic exchange between peers for contract verification.

Average holding time (e.g., flow duration or lifetime, duration of an MPLS path), on a per service class basis
Note: Similar to call holding time in telecommunications network, holding time statistics are useful in network planning for sizing network elements. Also, the holding time statistics of long-living static paths reflect the effect of network equipment failures, link outages, or scheduled maintenance, and hence may be used to derive information about up-time or service availability.

Available bandwidth of a link or path - useful for load balancing, measurement-based admission control to determine the feasibility of creating a new MPLS tunnel (real-time information can be used for dynamic establishment)

Throughput (in both bits (or bytes) per second and packets per second)
Note: (1) This is a measure of the "goodput." That is, the rate at which a given amount of traffic excluding lost, misdelivered, or errored packets, passes between a set of end points, where end points can be logically or physically defined. The condition of the network, e.g., normal or high load, under which the measurement is taken should be noted. (2) The protocol level at which a throughput measurement is taken must be specified, as the packet payload and packet overheads are protocol dependent. (3) The average packet size may be inferred from the bit rate and packet rate measurements. This quantity is useful to gauge router performance, since router operations are typically packet-oriented and small packets are more processing-intensive.

Delay (e.g., cross-router delay from node-based measurement may be used to measure queueing delay within a router; end-to-end one-way or round-trip packet delay can be obtained by node-pair-based measurement)
Note: The condition of the network, e.g., normal or high load, under which the measurement is taken should be noted. This is useful to determine if delay objectives are met.

Delay variation
Note: There are several ways to measure this quantity as specified in IPPM and I.380/Y.1540 (a brief summary to be included).
Packet loss

Note: (1) While packet losses due to transmission and/or protocol errors may not be traffic related, unexpected excessive loss may be used as a means of fault detection. (2) Packet losses due to policing or network congestion should be distinguished. The former is a result of user violation of service contract and the network operator should not be penalized for it. The latter, whether intentional or unintentional, is caused by network conditions such as buffer overflow, router forwarding process busy, and may not be the user’s fault. When policing is done by a network, measurement of non-conforming packets at the edge provides an indication on the extent to which the network is carrying this type of packets (which can potentially be dropped if network gets congested). Loss due to congestion of any packets, including loss of non-conforming packets, is a useful measure in traffic engineering to account for resource management. (3) Long-term averages can be measured by the I.380/Y.1540 IP packet loss ratio or by the IPPM Poisson sampling of one-way loss. However, during the convergence times associated with routing updating, the loss may be high enough as to cause service unavailability. This effect needs to be captured and statistics such as loss patterns, burst loss, or severe loss ratio may be required (reference to be included).

Resource usage, such as link/router utilization, buffer occupancy (e.g., fraction of arriving packets finding the buffer above a given set of thresholds)

Note: Trigger points may be set when resource usage consistently exceeds a certain threshold.

Entities related to establishment of connection or path

Where connection admission control is used, a measurement entity for monitoring network performance may be the proportion of connections denied admission. Also, it may be useful to score the requested bandwidth within the traffic parameters for the setup request. Corresponding to telecommunications network, connection request rate may be measured to characterize the offered traffic.

To characterize paths, the following measurement entities may be defined: path setup delay, path setup error probability, path setup denial (blocking) probability, path release delay, path disconnect probability, path restoration time.

10. Measurement Types

A measurement matrix can be defined wherein each column represents a measurement basis and each row represents a measurement entity. An entry in this measurement matrix, corresponding to a meaningful and measurable combination of an entity and a basis, defines a particular measurement type. For each measurement type, there should be a set of measurement points specified to bound the network
segment for the purposes of taking measurement. A measurement point may be the physical boundary between a node and an adjacent link, or the logical interface between two protocol layers in a protocol stack.

The following measurement matrix illustrates some of the measurement types related to traffic or performance. Potentially, there can be one such matrix for each service class.

<table>
<thead>
<tr>
<th>Bases:</th>
<th>Flow (passive)</th>
<th>Interface, Node (passive)</th>
<th>Node Pair (both)</th>
<th>Path (both)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entities:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic Volume</td>
<td>x(1)</td>
<td>x</td>
<td>x(3)</td>
<td>x(3)</td>
</tr>
<tr>
<td>Avg. Hold. Time</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avail. Bandwidth</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Throughput</td>
<td></td>
<td></td>
<td>x(4)</td>
<td>x(4)</td>
</tr>
<tr>
<td>Delay</td>
<td>x(2)</td>
<td></td>
<td>x(4)</td>
<td>x(4)</td>
</tr>
<tr>
<td>Delay Variation</td>
<td>x(2)</td>
<td></td>
<td>x(4)</td>
<td>x(4)</td>
</tr>
<tr>
<td>Packet Loss</td>
<td></td>
<td></td>
<td>x(5)</td>
<td>x(5)</td>
</tr>
</tbody>
</table>

Notes:
(1) This measurement type can be used to derive flow size statistics.
(2) These are 1-point measurements.
(3) As a starting point, statistics collected by passive measurement through the MPLS traffic engineering MIBs [7, 8, 9] may be used.
(4) Active measurements based on IPPM metrics are currently in use for node-pairs; they may be developed for paths.
(5) Besides active measurements based on IPPM, path loss may possibly be inferred from the difference between ingress and egress traffic statistics at the two endpoints of a path. However, such inference for the cumulative losses between a given node pair over multiple routes may be less useful, since different routes may have different loss characteristics.

Another measurement matrix can be constructed for resource consumption. This leads to a set of measurement types comprising the different usage, one for each network resource object such as router, link, and buffer, by different classes of traffic:

- control (e.g., routing control) traffic
- signaling traffic
- user traffic from different service classes

<table>
<thead>
<tr>
<th>Bases:</th>
<th>Node</th>
<th>Link</th>
<th>Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entities:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control Util.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Signaling Util.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Service Class Util.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

The amount of control and signaling traffic carried by a network is a function of many factors. To name a few, they include the size...
and topology of the network, the control and signaling protocols used, the amount of user traffic carried, the number of failure events, etc. The above utilization measurements for control and signaling traffic are intended to help develop guidelines for the proper dimensioning and apportionment of network resources so that a given level of user traffic can be adequately supported. As the primary focus here is on user traffic measurements, the additional needs and properties of control and signaling traffic measurements are beyond the scope of this document.

11. Traffic Matrix Statistics

An important set of data for traffic engineering is point-to-point or point-to-multipoint demands. This data is needed in the provisioning of intradomain routes and external peering in the existing network, as well as planning for the placement and sizing of new links, routers, or peers.

In current practice, estimates for traffic demands are usually determined from a combination of traffic projections, customer prescriptions, and SLAs. Under existing mode of operation, it is not easy to obtain network-wide traffic demands from the local interface measurements taken by different IP routers. As explained in [10, 11], information from diverse network measurements and various configuration files are needed to infer the traffic volume. Besides raw measurement data, additional information such as topological data and router configuration data are required to obtain a network view. Furthermore, destination-based routing/forwarding in IGP (such as OSPF or IS-IS) provides a network operator with primitive and limited control over the routing of traffic flows. This necessitates the association of a time sequence of forwarding tables from different routers to reconstruct the different routes used by the network over time. By using this auxiliary information, together with flow-based measurements, the above-cited references describe how to determine the traffic volume from an ingress link to a set of egress links by validating and joining various data sets together.

The routing control offered by MPLS can be used to avoid the above shortcomings of existing measurements. It is recommended that path-based passive measurement for traffic volume, average holding time, and available bandwidth be developed so that traffic matrix statistics, on a per service class basis, can be derived.

Besides traffic engineering, a major application of MPLS is the support of network-based virtual private networks (VPNs). A VPN can be an enterprise network or a carrier’s carrier network. Path-based measurement by a network operator on behalf of the VPN customers facilitates the estimation of the traffic offered by these VPNs.

12. Performance Monitoring
General aspects of measurements required to support the operation, administration, and maintenance of a network are outside the scope of this document (see [12] for a discussion of MPLS OAM). The focus of the measurements here is only on operations related to traffic engineering and network performance management.

A major component of performance management is performance monitoring, i.e., continuous real-time monitoring of the quality or health of the network and its various elements to ensure a sustained, uninterrupted delivery of quality service. This requires the use of measurement, either passively or actively, to collect information about the operational state of the network and to track its performance. For a discussion of passive monitoring and the use of synthetic traffic sources in active probing, see [13]. Alarms may be generated when the state of a network element exceeds prescribed thresholds.

Performance degradation can occur as a result of routing instability, congestion, or failure of network components. Periods of congestion may be detected when the resource usage of a network segment consistently exceeds a certain threshold, or when the cross-router delay is unexpectedly high. After the identification of a hot spot, active throughput measurement may be used to seek out alternate routes for congestion bypass. Unexpected excessive loss of packets or throughput drops may be used as a means of fault detection, and may result in restoration activities.

Internet utilities such as ping and traceroute have been useful to help diagnose network problems and performance debugging. Utilities with similar functions would be essential for path-oriented operations like in MPLS. This would include the capability to list, at any time, (1) for a given path, all the nodes traversed by it, and (2) for a given node, all the paths originating from it, transiting through it, and/or terminating on it. A proposal for route tracing is described in [14].

13. Report Generation

Data storage, data processing, statistics generation and reporting are outside the scope of this document.


(Note: This annex may be spun off as a separate document when it matures.)

The contents of this annex are to be provided. For example, it should specify some expected range of service-specific measurement intervals, read-out periods, and busy periods. Also, it should specify the different reference points in the traffic flow for both node-pair-based and path-based measurements, and their associated measurement types.
15. Security Considerations

Security considerations are not addressed in this version of the draft.

16. References


17. Acknowledgments

The support of Gerald Ash on this work and his comments are much appreciated. Also, thanks to the inputs from Robert Cole, Enrique Cuevas, Alfred Morton, Moshe Segal, and the Tequila project.
18. Author’s Addresses

Wai Sum Lai  
AT&T Labs  
Room D5-3D18  
200 Laurel Avenue  
Middletown, New Jersey 07748, USA  
Phone: +1 732-420-3712  
Email: wlai@att.com

Blaine Christian  
UU.NET  
Email: Blaine@uu.net

Richard W. Tibbs  
OPNET Technologies  
Email: rtibbs@opnet.com

Steven Van den Berghe  
Ghent University/IMEC  
St. Pietersnieuwstraat 41  
B-9000 Ghent, Belgium  
Phone: +32 9 267 35 86  
E-mail: steven.vandenberghe@intec.rug.ac.be

Full Copyright Statement

"Copyright (C) The Internet Society (date). All Rights Reserved.  
This document and translations of it may be copied and furnished to  
others, and derivative works that comment on or otherwise explain it  
or assist in its implementation may be prepared, copied, published  
and distributed, in whole or in part, without restriction of any  
kind, provided that the above copyright notice and this paragraph  
are included on all such copies and derivative works. However, this  
document itself may not be modified in any way, such as by removing  
the copyright notice or references to the Internet Society or other  
Internet organizations, except as needed for the purpose of  
developing Internet standards in which case the procedures for  
copyrights defined in the Internet Standards process must be  
followed, or as required to translate it into languages other than  
English.

The limited permissions granted above are perpetual and will not be  
revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an  
"AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING  
TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING  
BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION  
HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF  
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."