IPFIX Mediation: Problem Statement

draft-ietf-ipfix-mediators-problem-statement-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on March 30, 2009.
Abstract

Flow-based measurement is currently a popular method for various network monitoring usages. The sharing of flow-based information among orthogonal monitoring applications raises open issues in terms of scalability, reliability and flexibility that IPFIX Mediation may help resolve. IPFIX Mediation reroutes, replicates, filters, aggregates, correlates or modifies Flow Records or Packet Reports, or changes a transport protocol. This document describes the applicability of IPFIX Mediation and the problems that IPFIX Mediation might encounter.

Table of Contents

1. Introduction ............................................. 3
2. Terminology and Definition ............................... 4
3. Flow-Based Mediation: Applicability Examples ............ 9
   3.1. IPFIX Export Across Domains .......................... 9
   3.2. Data Retention ......................................... 9
   3.3. Interoperability between Legacy Protocols and IPFIX .... 9
   3.4. Rerouting Flow Records/Packet Reports ............... 10
   3.5. IPFIX Export from Branch Office ....................... 10
   3.6. Correlation of Flow Records/Packet Reports Information ... 11
4. Approaches to Scalability .................................. 12
   4.1. Adjusting Sampling Rates ............................... 12
   4.2. Flow Aggregation ....................................... 12
       4.2.1. Flow Aggregation on Original Exporters .......... 13
       4.2.2. Flow Aggregation on IPFIX Concentrators ......... 13
   4.3. Time Composition ....................................... 13
   4.4. Space Composition ..................................... 14
   4.5. Distributing Load among Collectors .................... 14
   4.6. Flow Selection Sampling ............................... 14
5. Problems with using IPFIX Mediators ...................... 15
   5.1. Loss of Observation Point Information ............... 15
   5.2. Loss of Base Time Information ........................ 16
   5.3. Loss of Option Template Information .................. 16
   5.4. Observation Domain ID and Template ID Management .... 16
   5.5. Transport Sessions Management ........................ 16
6. Conclusion .................................................. 18
7. Security Considerations .................................... 20
8. IANA Considerations ........................................ 21
9. References .................................................. 22
   9.1. Normative References .................................. 22
   9.2. Informative References ................................ 22
Authors’ Addresses ........................................... 23
Intellectual Property and Copyright Statements ............. 25
1. Introduction

While the IPFIX requirements defined in [RFC3917] mention an intermediate function, such as an IPFIX Proxy or a Concentrator, there is no document to define the function called IPFIX Mediation. IPFIX Mediation is an additional function to suit the needs of some measurement system. In this document, we describe several applicable examples of IPFIX Mediation. Furthermore, we describe the problems of IPFIX Mediation considering implementations. These problems can be solved by additional specifications without influencing the present IPFIX specification defined in [RFC5101].

Section 2 describes the terminology used in this document. Section 3 describes applicable examples of IPFIX Mediation. As more effective cases, section 4 describes some usages of the IPFIX Mediation in large-scale networks. Finally, section 5 describes the problems an implementation of an IPFIX Mediation device might face.
2. Terminology and Definition

The terms in this section are in line with those in the IPFIX specification document [RFC5101] and the PSAMP specification document [I-D.ietf-psamp-protocol]. Additional terms required for the IPFIX Mediation are also defined here. All these terms are capitalized in this document.

Observation Point

An Observation Point is a location in the network where IP packets can be observed. Examples include: 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.

Note that every Observation Point is associated with an Observation Domain (defined below), and that one Observation Point may be a superset of several other Observation Points. For example, one Observation Point can be an entire line card. That would be the superset of the individual Observation Points at the line card’s interfaces.

Observation Domain

An Observation Domain is the largest set of Observation Points for which Flow information can be aggregated by a Metering Process. For example, a router line card may be an Observation Domain if it is composed of several interfaces, each of which is an Observation Point. In the IPFIX Message it generates, the Observation Domain includes its Observation Domain ID, which is unique per Exporting Process. That way, the Collecting Process can identify the specific Observation Domain from the Exporter that sends the IPFIX Messages. Every Observation Point is associated with an Observation Domain. It is RECOMMENDED that Observation Domain IDs also be unique per IPFIX Device.

Flow Key

Each of the fields that:

1. belong to the packet header (e.g., destination IP address),
2. are a property of the packet itself (e.g., packet length),
3. are derived from packet treatment (e.g., Autonomous System (AS) number),
and that are used to define a Flow are termed Flow Keys.

Flow Record

A Flow Record contains information about a specific Flow that was observed at an Observation Point. A Flow Record contains measured properties of the Flow (e.g., the total number of bytes for all the Flow’s packets) and usually characteristic properties of the Flow (e.g., source IP address).

Packet Reports

Packet Reports comprise a configurable subset of a packet’s input to the Selection Process, including the Packet Content, information relating to its treatment (for example, the output interface), and its associated selection state (for example, a hash of the Packet Content).

Exporting Process

The Exporting Process sends Flow Records to one or more Collecting Processes. The Flow Records are generated by one or more Metering Processes.

Exporter

A device that hosts one or more Exporting Processes is termed an Exporter.

IPFIX Device

An IPFIX Device hosts at least one Exporting Process. It may host further Exporting Processes and arbitrary numbers of Observation Points and Metering Processes.

Collecting Process

A Collecting Process receives Flow Records from one or more Exporting Processes. The Collecting Process might process or store received Flow Records, but such actions are out of scope for this document.

Collector

A device that hosts one or more Collecting Processes is termed a Collector.
IPFIX Message

An IPFIX Message is a message originating at the Exporting Process that carries the IPFIX records of this Exporting Process and whose destination is a Collecting Process. An IPFIX Message is encapsulated at the transport layer.

Information Element

An Information Element is a protocol and encoding-independent description of an attribute that may appear in an IPFIX Record. The IPFIX information model [RFC5102] defines the base set of Information Elements for IPFIX. The type associated with an Information Element indicates constraints on what it may contain and also determines the valid encoding mechanisms for use in IPFIX.

IPFIX Mediation

IPFIX Mediation is a function located between Exporting Processes and Collecting Processes. The IPFIX Mediation can be included in any IPFIX Devices. The IPFIX Mediation consists of a set of some functions:

* rerouting input Flow Records/Packet Reports to a appropriate Collecting Process
* replicating input Flow Records/Packet Reports
* filtering and selecting input Flow Records/Packet Reports
* aggregating input Flow Records/Packet Reports based on new Flow Keys
* correlating a set of Flow Records/Packet Reports for creating new Flow Records/Packet Reports with new metrics
* modifying input Flow Records/Packet Reports
* changing a transport protocol which carries IPFIX Messages

The modification of Flow Records/Packet Reports includes these functions:

* changing the value of specified Information Elements
* adding new Information Elements by deriving further Flow or packet properties from existing fields or calculating new
metrics

* deleting specified Information Elements.

IPFIX Mediation can be included in any devices, such as routers, switches, NMS (Network Management Systems), or be deployed in stand-alone devices.

Flow-Based Collector Selection

The Flow-Based Collector Selection evaluates an input Flow Record/Packet Report based on the value of the specified Information Element and then selects Collector for each input Flow Record/Packet Report.

IPFIX Mediator

An IPFIX Mediator contains one or more functions defined in IPFIX Mediation. The IPFIX Mediator can be a stand-alone or a virtual device. It also contains one or more Collecting Processes and one or more Exporting Processes.

Original Exporter

An Original Exporter is an IPFIX Device which hosts Observation Points where IP packets can be directly observed.

IPFIX Proxy

An IPFIX Proxy is an IPFIX Mediator that receives IPFIX Messages from Original Exporter, and sends IPFIX Messages to one or more Collectors. It may alter a part of IPFIX Message in order to comply with IPFIX Protocol specifications. It may also change type of transport protocol, such as UDP, TCP, SCTP and PR-SCTP, and convert a legacy protocol message to an IPFIX Message, if necessary.

IPFIX Concentrator

An IPFIX Concentrator is an IPFIX Mediator that receives Flow Records/Packet Reports, aggregates them, then exports the aggregated Flow Records.

IPFIX Distributor

An IPFIX Distributor is an IPFIX Mediator that reroutes input Flow Records/Packet Reports based on the result of Flow-Based Collector Selection. It may filter or replicate input Flow Records/Packet
Reports, if necessary.

IPFIX Masquerading Proxy

An IPFIX Masquerading Proxy is an IPFIX Mediator that screens out a part of data of input Flow Records/Packet Reports according to configured policies. It can thus, for example, hide the network topology information or customers’ IP addresses.
3. Flow-Based Mediation: Applicability Examples

3.1. IPFIX Export Across Domains

IPFIX export across administrative domains can be used to measure traffic for wide-area traffic engineering, or to analyze the trend of Internet traffic. In such cases, operators need to adhere to privacy policies and prevent the transmission of confidential information. Using an IPFIX Masquerading Proxy allows them to operate on Flow Records safely by anonymizing and filtering them. IP Flow anonymisation is described in [I-D.boschi-ipfix-anon] in detail.

3.2. Data Retention

Data retention refers to the storage of traffic data by service providers and commercial organizations. According to European Commission directives, operators are required to retain both IP and voice traffic data, in wired and wireless networks, generated by end users while using a service provider’s services. The goal of data retention is to ensure that call detail records and Flow Records are available for the purpose of detection, investigation, and prosecution of serious crimes, if necessary. The European Commission directives define the following data retention services:

- Fixed telephony (includes fixed voice, voicemail, and conference and data calls)
- Mobile telephony (includes mobile voice, voicemail, conference and data calls, SMS, and MMS)
- Internet telephony (includes every multimedia session associated with IP multimedia services)
- Internet e-mail
- Internet access

By monitoring Flow Records, IPFIX can fulfill these requirements of Internet access services.

3.3. Interoperability between Legacy Protocols and IPFIX

During the migration process from a legacy protocol such as NetFlow [RFC3954] to IPFIX, both NetFlow and IPFIX Exporters will need to co-exist in the same network. An IPFIX Proxy which converts a legacy protocol to IPFIX will allow operators to continue measuring Flows from legacy Exporters, even after introducing IPFIX Collectors.
3.4. Rerouting Flow Records/Packet Reports

Recently, several networks seem to have shifted towards integrated networks, such as the Internet and MPLS, which includes IPv4, IPv6, and VPN traffic. Flow Records/Packet Reports of these types need to be analyzed separately and from different perspectives. However, handling them separately without improving the capability of the Collector is difficult. An IPFIX Distributor rerouting Flow Records/Packet Reports based on the result of Flow-based Collector Selection, would be necessary. Thus, it allows individual Collectors related to each network to analyze traffic data for their own specific purposes.

As another example, in case of rerouting specific customer’s Flow Records, an IPFIX Distributor needs to identify each customer. As identification data, the RD (Route Distinguisher), ingress IF, peering AS number, or BGP next hop are listed. As shown in the following figure, the IPFIX Distributor reroutes Flow Records based on the RD value. This system allows each customer’s traffic to be inspected independently.

![Figure A: Rerouting Flow Records to Collectors using IPFIX Distributor](image)

3.5. IPFIX Export from Branch Office

Generally, in big enterprise networks, traffic data from branch offices is gathered in a central office. But, in the long distance branch office case, the bandwidth for transport IPFIX is not enough.
Therefore, it is beneficial that an IPFIX Concentrator located in a branch office exports aggregated Flow Records to cope with the limitation of bandwidth.

3.6. Correlation of Flow Records/Packet Reports Information

The correlation of Flow Records/Packet Reports information offers some new metrics. There are some examples as follows:

- One way delay follows from correlating Packet Reports exported from different Exporters on the path.
- The result of a queueing or rate-limiting function applied to ingress or egress interface follows from correlating Flow Records with the same Flow Key observed at both interfaces.
- Average/maximum/minimum values follow from correlating each in a set of Flow Records.
4. Approaches to Scalability

Usually, operators measure traffic at several Observation Points for a specific purpose, typically sampling packets with rates ranging from 1/10,000 to 1/100. This value depends on several factors, such as the capacity of the management network, the available storage and speed of the Collector, and the load on the routers/switches.

On the one hand, the number of Observation Points in the networks can even be increased to improve the effectiveness of these methods. In the near future, we anticipate that the advanced features of IPFIX, such as the monitoring of wide-area traffic matrices and QoS performance, will accelerate IPFIX utilization.

On the other hand, the increasing amount of traffic brought about by broadband users might have an impact on measurement parameters, such as the sampling rate or granularity of Flows. Generally, large-scale networks already have multiple 10 Gb/s links, their total traffic exceeding 100 Gb/s. In the near future, broadband users’ traffic will increase by approximately 50% per year according to [TRAFFGRW]. When operators monitor traffic of 500 Gb/s with a sampling rate of 1/1000, the amount of exported Flow Records from Exporters could exceed 50 kFlows/s. This value is beyond the ability of a single Collector.

This section explains how operators can cope with such a huge amount of Flow Records using available IPFIX solutions. Generally, the solutions encompass two approaches: reducing the amount of exported Flow Records or increasing the capacity of the Collecting Process. The following sub-sections show each solution.

4.1. Adjusting Sampling Rates

Adjusting the sampling rate can reduce the amount of Flow Records, and a flow-based measurement system can thus easily adapt to the ability of the Collecting and Exporting Processes. However, in that case, Flows with small traffic volumes could easily get lost. If traffic incidents happened, operators would no longer be able to investigate traffic change. While traffic volumes on networks continue to increase, operators will not be able to maintain the sampling rates currently used. In the near future, flow-based measurement systems possibly will not be able to detect traffic anomalies which can currently be detected.

4.2. Flow Aggregation

The simplest types of Flows are those comprised of all packets having a fixed five tuple of protocol, source and destination IP addresses,
and source and destination port numbers. On the other hand, choosing a shorter Flow Key, such as a three tuple or two tuple, or a single Flow Key, such as a network prefix, peering AS number, or BGP Next-Hop, creates more aggregated Flow Records. This solution is especially useful for measurements of traffic exchange in an entire network domain and for easy adjustments to the performance of a Collector.

4.2.1. Flow Aggregation on Original Exporters

Original Exporters can aggregate Flow Records to reduce the amount of them. But, in-depth traffic monitoring might not be possible, as it is with the five tuple. One way to this is to be able to specify the Template Records for specific needs. This extra flexibility in the Metering Process allows operators to specify their own set of Flow Keys and extra Information Elements in the Template Record. Specifically, Original Exporters classify the Flow Records by their contents, and then aggregate them with appropriate Flow keys based on a specific application. There is an application for security, another for capacity planning, and so on. The content and granularity of the Flow can satisfy the requirements of each Collector with a specific application.

On one hand, this optimizes the Metering Process, because only Flows of interest are looked at. On the other hand, it optimizes the Exporting Process, because only the information of interest is exported. Finally, this reduces load of the Collecting Process as less Flow Records are handled, and Flow Record filtering and aggregating are required.

4.2.2. Flow Aggregation on IPFIX Concentrators

Another approach involves a hierarchical measurement system using IPFIX Concentrators. Aggregation and storage for input Flow Records on IPFIX Concentrators makes a most useful distributed-collection system. It allows other devices to retrieve the stored Flow Record. This method increases the capacity of Collecting Process of whole system. Flow aggregation method is described in [I-D.dressler-ipfix-aggregation] in detail.

4.3. Time Composition

Time composition is defined as aggregation for consecutive Flow Records with same Flow Keys. It leads to the same output as setting a longer active interval timer on Original Exporters. However, an IPFIX Mediation can calculate average, maximum and minimum values of each counter from Flow Records received with shorter interval time. The output allows operators to keep track of changes that might have
happened during the time interval.

4.4. Space Composition

Space composition is defined as aggregation for one or more Flow Records involved in a larger Observation Domain or a set of Observation Points. It is divided into two types:

- Space Composition within one Exporter

  In that case, the spatial range is within one Exporters. For example, the Flow Records observed at physical interfaces which belong to virtual interface by link aggregation can be composed to one Flow Records.

- Space Composition within some Exporters

  In that case, the spatial range consists of some different Exporters. For example, the Flow Records observed at same domain, such as west area and east area of an ISP network, can be composed to one Flow Records.

4.5. Distributing Load among Collectors

As described in the previous section, an IPFIX Distributor reroutes Flow Records/Packet Reports to appropriate Collectors based on the result of the Flow-based Collector Selection. It can thus distribute the load among multiple Collectors according to a specific application, each area, or each customer.

4.6. Flow Selection Sampling

A Flow selection sampling method is described in [I-D.peluso-flowselection] in detail. Generally, the distribution of the number of packets per Flow seems to be heavy-tailed. Most types of Flow Records are likely to be small Flows consisting of a small number of packets. The flow-based measurement system, in particular the Collecting Process and Exporting Process, is burdened with a huge amount of these small Flows. If statistics information of small Flows is exported as merging data by applying a policy or threshold, the burden on measurement system is reduced.
5. Problems with using IPFIX Mediators

In this section, we focus on the problems related to the use of IPFIX Mediators in consideration of implementation.

5.1. Loss of Observation Point Information

Both the Exporter IP address indicated by the source IP address of the IPFIX session as well as the Observation Domain ID included in the IPFIX header are likely to be lost in the mediation process performed by an IPFIX Mediator. This IP address and Observation Domain ID indicate the Observation Point information from the viewpoint of the entire network domain. Such information is necessary for guaranteeing the continuity of the work of the top level Collector. Even if an IPFIX Mediator could, with some new mechanism, notify Collectors of this Observation Point information, older Collectors might not accept it. These Collectors would then wrongly assume that the IP address of the IPFIX Mediator is that of the Original Exporter. The Collector, however, needs to recognize the precise Observation Point whether Flow Records go through an IPFIX Mediator or not.

In the following figure, a Collector could identify 2 Exporters with IP addresses of 10.1.1.3 and 10.1.1.2, respectively. The Collector, however, needs to somehow recognize Router#1 and Router#2, which are the Original Exporters. Defined notification methods that can be interpreted by Collectors and Mediators are thus necessary.

![Diagram](image)

Figure B: Loss of Observation Point Information.
5.2. Loss of Base Time Information

The Export Time field included in the IPFIX header indicates the base time for Flow Records. In IPFIX Information Elements, described in [RFC5102], there are delta time fields that indicate the time difference from the value of the Export Time field. If the Flow Records include any delta time fields and the IPFIX Mediator overwrites the Export Time field when sending IPFIX messages, the delta time fields become meaningless and, because Collectors can not recognize this situation, wrong time values are propagated.

5.3. Loss of Option Template Information

In some cases, depending on the implementation of the IPFIX Mediators, the information that is reported by the Option Templates could also be lost. If, for example, the sampling rate is not communicated to the Collectors, a Collector would miscalculate the traffic volume. This might bring crucial problems. Even if an IPFIX Mediator were to simply relay received Option Template Information, the value of its scope fields would become meaningless in the context of a different session. It should be noted that the minimal information to be communicated by an IPFIX Mediator needs to be defined.

5.4. Observation Domain ID and Template ID Management

The Observation Domain ID is locally unique to the Exporting Process in an IPFIX Mediator, just like the Template ID is unique on the basis of the Observation Domain ID. These renewed identifiers should be managed using the Transport Session Information of the Collecting Process. If IPFIX Mediators could not manage the relations among these identifiers and the received Transport Session Information, the Mediators would, for example, relay wrong values for the scope fields of the Option Template and for a "Template Withdraw Message". In most cases, a Collector would not be able to interpret the Template ID of a "Template Withdraw Message" and the scope fields of an Option Template. The Collector would then shut down the IPFIX Session.

5.5. Transport Sessions Management

How an IPFIX Mediator maintains relationships between the Transport Sessions of Collecting Processes and of Exporting Processes depends on its implementation. If multiple Transport Sessions of the Collecting Process are relayed to single Transport Session of the Exporting Process and the IPFIX Mediators shuts down the Transport Session of the Exporting Process, Flow Records on other Transport Sessions of the Collecting Processes would not be relayed at all. In the case of resetting a session of the Collecting Process, the
behavior of the IPFIX Mediator needs to be defined.

Figure C: Relaying from Multiple Transport Sessions to Single Transport Session.
6. Conclusion

This document has covered the applicability of IPFIX Mediation and a multitude of problems related to the implementation of IPFIX Mediators. To assist the ability of the Exporters and Collectors, it should be noted that there are various IPFIX Mediation functions for the operators to select from. Examples of the applicability of IPFIX Mediation are as follows.

- Regarding IPFIX Exporting across domains, IPFIX Masquerading Proxies help operators to anonymize or filter Flow Records/Packet Reports, preventing privacy violations.

- Regarding data retention, IPFIX Mediators enhance the storage of the measurement system.

- Regarding interoperability, IPFIX Proxies provide interoperability between legacy protocols and IPFIX, even during the migration period to IPFIX.

- Regarding the Flow-based Collector Selection function, in integrated networks, which mix MPLS VPN and IPv4/IPv6, this could be utilized more frequently. More sophisticated implementation methods would enhance the effectiveness.

- Regarding scalability in large-scale networks, IPFIX Concentrators or IPFIX Distributors help to achieve high sample rates and fine-grained Flow analysis even as networks grow. As IPFIX Mediation functions, Flow selection sampling, aggregation and composition are beneficial.

As a result, the benefits of IPFIX Mediation become apparent. However, there are still some open issues.

- With the use of IPFIX Mediators, both Observation Point and IPFIX header information, such as the Exporter IP address, Observation Domain ID, and Export Time field, might be lost. This data should therefore be communicated between the Original Exporter and Collector via the IPFIX Mediator.

- With the use of IPFIX Mediators, data advertised by Option Templates from the Original Exporter, such as the sampling rate and sampling algorithm used, might be lost. If a Collector is not informed of current sampling rates, traffic information might become worthless.

- IPFIX Mediators are required to manage Transport Sessions, Template IDs, and Observation Domain IDs. Otherwise, anomalous
IPFIX messages could be created.

These problems stem from the fact that no standards regarding IPFIX Mediation have been set. In particular, the minimum set of information which should be communicated between Original Exporters and Collectors, interworking between different IPFIX Transport Sessions, and the internal components of IPFIX Mediators should be standardized.
7. Security Considerations

A flow-based measurement system might lead to privacy violations, such as the export of Flow Records to an outside address, if the system is not confined to the large-scale network under observation. General security issues of the IPFIX protocol are covered by the security considerations section in [RFC5101]. Security MUST be considered if different networks exchange Flow information. As the security of the exchange relies mostly on the protocol used, UDP does not seem appropriate for the exchange of information between networks.
8. IANA Considerations

This document has no actions for IANA.
9. References

9.1. Normative References

[I-D.ietf-psamp-protocol]


9.2. Informative References

[I-D.boschi-ipfix-anon]

[I-D.dressler-ipfix-aggregation]

[I-D.peluso-flowselection]

Authors’ Addresses

Atsushi Kobayashi  
NTT Information Sharing Platform Laboratories  
3-9-11 Midori-cho  
Musashino-shi, Tokyo  180-8585  
Japan  
Phone: +81-422-59-3978  
Email: akoba@nttv6.net  
URI:  http://www3.plala.or.jp/akoba/

Haruhiko Nishida  
NTT Information Sharing Platform Laboratories  
3-9-11 Midori-cho  
Musashino-shi, Tokyo  180-8585  
Japan  
Phone: +81-422-59-3978  
Email: nishida.haruhiko@lab.ntt.co.jp

Christoph Sommer  
University of Erlangen-Nuremberg  
Department of Computer Science 7  
Martensstr. 3  
Erlangen  91058  
Germany  
Phone: +49 9131 85-27993  
Email: christoph.sommer@informatik.uni-erlangen.de  
URI:  http://www7.informatik.uni-erlangen.de/~sommer/

Falko Dressler  
University of Erlangen-Nuremberg  
Department of Computer Science 7  
Martensstr. 3  
Erlangen  91058  
Germany  
Phone: +49 9131 85-27914  
Email: dressler@informatik.uni-erlangen.de  
URI:  http://www7.informatik.uni-erlangen.de/~dressler/
Stephan Emile  
France Telecom  
2 avenue Pierre Marzin  
Lannion, F-22307  

Fax: +33 2 96 05 18 52  
Email: emile.stephan@orange-ftgroup.com

Benoit Claise  
Cisco Systems  
De Kleetlaan 6a b1  
Diegem 1831  
Belgium  

Phone: +32 2 704 5622  
Email: bclaise@cisco.com
Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.