

Internet Engineering Task Force  
Internet-Draft  
Intended status: Informational  
Expires: April 27, 2015

S. Jiang  
Huawei Technologies Co., Ltd  
H. Deng  
China Mobile  
F. Bari  
AT&T  
R. Zhang  
China Telecom  
S. Krishnan  
Ericsson  
Y. Fu  
Huawei Technologies Co., Ltd  
October 24, 2014

Application Enabled Collaborative NETworking Gap Analysis  
draft-conet-aeon-gap-analysis-01

Abstract

Identification and treatment of application flows have become more and more important for network operators. In order to efficiently distinguish ICPs' traffic, coordination between ISPs and ICPs is required. IP flow identification can be based on ICPs' traffic carrying some mutually agreed identifiers. This document analyzes the technical gap between the current network functions and required network capability to enable such functionality.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on April 27, 2015.

Internet-Draft

CONET/AEON Gap Analysis

October 2014

## Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Overview of Technical Considerations</a>	<a href="#">3</a>
<a href="#">3.</a>	<a href="#">Traffic Identifiers</a>	<a href="#">4</a>
<a href="#">4.</a>	<a href="#">Collaboration between ICPs and ISPs</a>	<a href="#">7</a>
<a href="#">5.</a>	<a href="#">Identifying Traffics between End Users and Network</a>	<a href="#">8</a>
<a href="#">6.</a>	<a href="#">Limitations of Existing Signaling Mechanisms</a>	<a href="#">9</a>
<a href="#">7.</a>	<a href="#">Efforts in Progress</a>	<a href="#">10</a>
<a href="#">8.</a>	<a href="#">Security Considerations</a>	<a href="#">12</a>
<a href="#">9.</a>	<a href="#">IANA Considerations</a>	<a href="#">12</a>
<a href="#">10.</a>	<a href="#">Acknowledgements</a>	<a href="#">12</a>
<a href="#">11.</a>	<a href="#">Change log [RFC Editor: Please remove]</a>	<a href="#">12</a>
<a href="#">12.</a>	<a href="#">References</a>	<a href="#">12</a>
<a href="#">12.1.</a>	<a href="#">Normative References</a>	<a href="#">12</a>
<a href="#">12.2.</a>	<a href="#">Informative References</a>	<a href="#">14</a>

## [1.](#) Introduction

While the Internet traffic is continually growing, more and more ICPs (Internet Content Providers) realize the essentiality and advantages of cooperating with ISPs (Internet Service Providers). In order to serve their users better, ICPs have an emerging requirement that the traffic of their products needs to be treated differently, both in traffic handling process as well as in traffic accounting process. [[I-D.conet-aeon-problem-statement](#)] has described such problems and related requirements.

The biggest technical challenge that network operators or the ISPs face is of distinguishing the traffic in finer granularity. Nowadays, DPI (Deep Packet Inspection) or DFI (Deep Flow Inspection) mechanisms have been widely used in identifying application information specific to individual IP flows. However, they are expensive both operationally and computationally. In many cases, they are also not able to interact with real-time network operations. An alternative approach would be that the traffic from ICPs carries traffic identifiers that the network entities of ISPs can recognize and act on. For that to properly work, the traffic identifiers must be mutually understood by ISPs and ICPs.

This document analyzes the technical gap between the current network functions and required network capability.

## [2.](#) Overview of Technical Considerations

Overall, there are four technical aspects that need to be considered, as listed below.

- o A traffic identifier.
- o An ICP notify/negotiate traffic identifiers and the desired processing way regarding both traffic handling and traffic accounting with an ISP. The policies of traffic processing need

to be propagated and corresponding network entities need to be configured within an ISP network.

- o Signaling/negotiation of traffic identifier by an end user host or application to/with network.
- o The information authentication and integrity protection mechanism.

Note: the application-level communication between ICP servers and their client applications on end user hosts, including dynamically deciding the traffic identifier that end user hosts may embed in

packets, is out of scope. This document focuses on only the network layer and transport layer.

### [3.](#) Traffic Identifiers

The precondition for a traffic flow to be handled differently is that it can be recognized by the network entities. In this document, the field in data packet that is used to distinguish a traffic flow or a type/category of traffic flow is called traffic identifier. There are a few requirements for traffic identifiers:

- o Traffic identifiers must be stable, at least for the lifetime of an IP flow.
- o Traffic identifiers should be easy to inspect by the network entities.
- o Traffic identifiers should accurately distinguish IP traffic flow or a type/category of traffic flow.
- o Traffic identifiers must be trustable and protected against tampering during transportation.
- o Some traffic identifiers may be aggregated in order to reduce the management complexity on stateful records/policies.
- o Some traffic identifiers may be dynamically decided just before the real traffic is generated. The decision of identifiers may dynamically involve ISPs, ICPs and end user devices.

- o Some traffic identifiers may not be set by the traffic initiators. A intermediate node, for example a CPE or an ingress router, may re-mark or set new traffic identifier based on its traffic recognition.
- o Some traffic identifiers may be meaningful across network administrative boundaries.

Current common approach to identify traffic flows of applications in a network is to rely on dedicated content aware devices. These devices not only parse fields on the IP and transport layers but also recognize application related information above transport layer. Content awareness ability mainly utilizes DPI function, which inspects characteristic signature (e.g. key string, binary sequence, etc.), and DFI function, which analyzes statistical characteristic and connection behavior of traffic flows, to identify application. However, there are limitations in deployment and operation of the ability.

- o Since both DPI and DFI are essentially deductive methods difficult to fully grasp the characteristics of applications, accuracy of application identification cannot be guaranteed. Error or omission is inevitable.
- o Internet applications are expected to change frequently, and so are their characteristics. There will be a time lag between a complete application traffic analysis and update of signature database when a new application or a new version appears, and this also contributes to the inaccuracy of identification.
- o Content identification mechanisms are usually proprietary and act as a black box. There is no standard way in their implementation or a way of benchmarking. So the ability highly depends on vendors. Different boxes are likely to give different identification results to the same traffic.
- o Content identification functionality requires parsing the payload of IP packets, leading to very high use of computational resources. Built-in content identification function modules in network elements will therefore affect the forwarding performance and thus impact data transmission.

- o Investment costs cannot be neglected. Sometimes the cost to identify the traffic is no less than that of forwarding the traffic. Operational cost of the additional nodes is also an important issue. More potential failure points will also affect network quality.
- o Furthermore, the usage of TLS (Transport Layer Security, [\[RFC5246\]](#)) and HTTPS [\[RFC2818\]](#) is increasing the difficulties of DPI.

Another simpler approach is to identify traffic by IP addresses. An example would be a white list of IP addresses of an application of the ICP, and network can match traffic with the list to pick the application. This approach will have limitations when dealing with more complex scenarios.

- o More granular traffic handling cannot be satisfied. If part of the application traffic or traffic of some of the users is to be treated separately, IP based identification is too coarse. For example, the real-time game traffic and video traffic for the same website are likely to receive different treatment but target to the same IP address; traffics from two users to the same server may also need to be distinguished.

- o If cache or CDN (Content Distribution Network) is deployed in the network, then different users are likely to visit different addresses, and the addresses are likely to be different from the original addresses of ICPs. Managing the list will have to consider the IP addresses of caches and CDN nodes deployed.
- o Configuring the IP address list is not always extensible as the addresses may change, and sometimes it is not supposed to expose the addresses of ICPs.

There are also other traffic identifiers or components that may get used as traffic identifiers:

- o IP addresses of end user devices. They are natural identifiers that can distinguish the communication nodes. However, one end

user node would have many IP traffic flows. There is requirement to recognize only the traffics associated with certain ICPs. So, only IP addresses of end user devices are not sufficient. Furthermore, many end user devices may be assigned private IPv4 addresses. These addresses are replaced by public IPv4 addresses after NAT (Network Address Translator, [[RFC3022](#)]).

- o Port numbers. They are useful to distinguish flows/services from the same node. However, it cannot be used to identify network traffic independently. It must be used together with identifiers that distinguish nodes.
- o Flow labels [[RFC6437](#)]. It is only available in IPv6 traffic. It is changed for every flow. Like port numbers, flow labels cannot be used to identify network traffics independently. Normally, it is used as triple-tuple with source and destination address. Because it is encoded in the IPv6 fixed header, it is easier to recognize than port numbers. However, another disadvantage of flow label is that it is not protected, particularly, there is no mechanism to validate its integrity.
- o DiffServ Field (Differentiated Services Field, [[RFC2474](#)]). It was defined to identify the differentiated services that network should apply on the packets. It is the explicit result for network entities to apply different handling policies accordingly. However, the precondition DiffServ field can be used is that there is strong trust relationship between the nodes that set DiffServ Field and network entities.

Each of the above mentioned traffic identifiers have their own suitable use cases and possible limitations.

For many scenarios, the combination of abovementioned traffic identifiers may be used. The 5-tuple (source IP address, destination IP address, source port number, destination port number, IP protocol number) is the most commonly used traffic identifier to identify a flow accurately in IP layer. However, 5-tuple itself is not tightly associated with upper-layer applications or contents. There are mapping gaps to use 5-tuple to identify traffics relevant to a certain ICP or its certain services. Another issue of 5-tuple is

that 5-tuple cannot be easily aggregated. Managing numerous 5-tuple may be a big burden for ISPs. Furthermore, the existence of NATs makes the use of the 5-tuple difficult. Consequently, the traffic identifiers associated with IPv4 addresses become a very complicated management issue.

#### [4.](#) Collaboration between ICPs and ISPs

Firstly, ICP needs to define traffic identifiers in consultation with ISP.

The ICP defines the specific traffic identifiers, which may have multiple categories, and the desired policies associated with each traffic category, in consultation with the ISP. Then the ISP network can apply these policies to actual network traffic.

The notification process between ICPs and ISPs can be dynamic through a protocol/interface. In 3GPP (3rd Generation Partnership Project) mobile network, Rx interface [[Rx-3GPP](#)] has been defined to allow interaction between ICPs and ISPs using Diameter [[RFC6733](#)], and AF-Application-identifier AVP has also been defined to indicate the particular service that the AF (Application Function) service session belongs to. This information may be used by the PCRF (Policy and Charging Rule Function) to differentiate QoS for different application services.

However, currently few ICPs have support for Diameter protocol. Considering ICP is more familiar with XML based protocol, 3GPP is working on the solutions for an XML based protocol (e.g. SOAP, Restful HTTP, etc.) over Rx interface between the AF and the PCRF [[XML AF PCRF](#)].

Within an ISP network, traffic management policy must be propagated to network entities that actually handle traffics. In 3GPP mobile network, Gx interface [[Gx-3GPP](#)] has been defined to enable PCRF autonomically configures matching rules regarding to a certain traffic on GGSN/P-GW.



Framework [BPCF] that meets the similar function of Rx and Gx interfaces in the fixed broadband networks.

This model has two limitations as below:

1. Some ICPs may have one server address, but with different sub-content behind that server address. Because current PCRF only focus on 5-tuple traffic description, it may be difficult to support fine-grained traffic identification.
2. Because of lack of involvement from end user devices/applications, it will be difficult and more complex to identify devices if they are behind NAT (they have NATed IPv4 addresses).

Another major issue is that this model is ISP-oriented. ICP traffics commonly cross multiple ISP networks. Hence, an ICP may have to work with multiple ISPs independently. The traffic handling across different administration domain may be different, giving the possibility that different ISPs may use different traffic identifiers and different policies. When there was a traffic issue, such as high latency or packet lost, it may be a challenge for the ICP to find out which network has problem.

## 5. Identifying Traffics between End Users and Network

When an end user host or application initiates traffic towards ICP contents, it is possible that the content instead is retrieved from a cache/CDN that is deployed in the operator network. In that case, the traffic identifier provided from the end user host or application to the network is used to classify traffic.

The traffic identifiers used by end user host or application:

- o may be authorized and assigned by the ICPs after application-level authentication or out-of-band authentication. Then, these traffic identifiers would be carried by packets.
- o may be dynamically decided by the negotiation between the end user host or application and the network. Out-of-band controlling policies, including network authentication and authorization, may also be notified/negotiated together.
- o may just describe the traffic characteristics, and leave the network to recognize them, then mapped into other traffic identifiers that have explicit meaning within the network.

Currently, there are not many in-band mechanisms, where traffic identifiers that the end user devices/applications set up are carried within packets. In-band mechanisms allow packet traversal across administration domains, with the traffic getting identical handling. The precondition of in-band mechanisms is that the integrity of traffic identifiers can be validated by network entities.

## 6. Limitations of Existing Signaling Mechanisms

The IETF has standardized several mechanisms involving explicit signaling between applications and the network that may be used to support visibility and differentiated network services workflows. These existing protocols were designed to serve their own purposes and scenarios. Unfortunately, none of these have experienced widespread deployment success, nor are they well suited for the usages described previously. Existing signaling options include the following:

- o RSVP (Resource Reservation Protocol, [[RFC2205](#)]), a resource reservation setup protocol, is the original on-path signaling protocol standardized by the IETF. It is transported out-of-band and could be used to signal information about any transport protocol traffic (it currently supports TCP and UDP). Its original goal was to provide admission control. It is mainly used among network entities. Its requirement for explicit reservation of resources end to end proved too heavy for most network environments. Its success was further impacted by its reliance on router-alert, which often leads to RSVP packets being filtered by intervening networks, and by its requirement for access to a raw socket, something that is generally not available to applications running in user space. To date, more lightweight signaling workflows utilizing RSVP have not been standardized within the IETF.
- o NSIS (next Steps in Signaling, [[RFC4080](#)]) is the next iteration of RSVP-like signaling defined by the IETF. It focused on the same fundamental workflow as RSVP admission control as its main driver, and because it did not provide significant enough use-case benefits over RSVP, it has seen even less adoption than RSVP.
- o DiffServ [[RFC4594](#)] and VAN Tagging [[IEEE-802.1Q](#)] style packet marking can help provide QoS in some environments, but such markings are often modified or removed at various points in the network or when crossing network boundaries. There are additional limitations when using DiffServ with real-time communications applications, and the DART working group has been chartered to

DiffServ when used with RTP in general as well in the specific RTCWeb use cases [[I-D.ietf-rtcweb-use-cases-and-requirements](#)].

- o DHCP (Dynamic Host Configuration Protocol, [[RFC2131](#)], [[RFC3315](#)]) was designed to provide information, including assigning host IP address, from network to hosts. It is a one-way information provisioning protocol. It does not provide authentication and information protection function.
- o Radius (Remote Authentication Dial In User Service, [[RFC2865](#)]) and Diameter [[RFC6733](#)] provides an Authentication, Authorization and Accounting for network access.
- o ALTO (Application-Layer Traffic Optimization) [[RFC7285](#)] was defined to help the application on the end user host or trackers to select proper peer hosts. The ALTO server provides network information (e.g. network topology information or cost, like AS number) of candidates peer hosts that is capable of providing a desired resource to the ALTO client where in AECON solution the client provided the Qos information and traffic identifiers to the server. The information in ALTO is transported by a request and response processing based on HTTP protocol where in AECON solution the information is notified by the client to the server. The ALTO sever provides the Map Service, the Map-Filtering Service and the Endpoint Cost (Ranking) Service to the ALTO client where the AECON server provides the authentication and registration service to the client.

## [7.](#) Efforts in Progress

Not surprisingly, there are several evolving proposals that aim to address the visibility and differentiated network services workflows where existing approaches are not sufficient. Protocol specific extensions are being defined, creating duplicate or inconsistent information models. This results in operational complexity and a need to convert information between protocols to leverage the best protocol option for each specific use case. Examples of evolving signaling options include the following:

- o STUN (Session Traversal Utilities for NAT, [[RFC5389](#)]) is an on-path, in-band signaling protocol that could be extended to provide signaling to on-path network devices. It provides an easily inspected packet signature, at least for transport protocols such as UDP. Through its extensions TURN [[RFC5766](#)] and ICE [[RFC5245](#)], it is becoming prevalent in application signaling driven by the initial use-case of providing NAT and firewall traversal capabilities and detecting local and remote candidates for peer-

to-peer media sessions. The TRAM working group is chartered to update TURN and STUN to make them more suitable for WebRTC.

- o PCP (Port Control Protocol, [[RFC6887](#)]) provides a mechanism to describe a flow to the network. The primary driver for PCP is creating port mappings on NAT and firewall devices. When doing this, PCP pushes flow information from the host into the network (specifically to the network's NAT or firewall device), and receives information back from the network (from the NAT or firewall device). It is not meant to be used end-to-end but rather independently on one "edge" of a flow.
- o RESTCONF [[I-D.ietf-netconf-restconf](#)] is a REST-like protocol that provides a programmatic interface over HTTP for accessing data defined in YANG, using the data stores defined in NETCONF [[RFC6241](#)]. It is meant to provide a standard mechanism for web applications to access the configuration data, operational data, data-model specific protocol operations, and notification events within a networking device, in a modular and extensible manner.
- o I2RS (Interface to the Routing System) is a working group chartered to provide interfaces for management applications, network controllers, and user applications to make specific demands on the network.
- o ACTN (Abstraction and Control of Transport Networks) is a non-working group mailing list intended to enable discussion of the architecture, use-cases, and requirements that provide abstraction and virtual control of transport networks to various applications/clients.
- o Prefix coloring has been proposed for use in HOMENET and 6MAN

working groups to provide differentiated services to applications based on IP address.

- o RMCAT (RTP Media Congestion Avoidance Techniques) has been chartered to address the lack of generally accepted congestion control mechanisms for interactive real-time media, which is often carried via sets of flows using RTP over UDP. Explicit exchanges of flow characteristics and congestion information between applications and the network could play an important role in such mechanisms.
- o TAPS (Transport Services) is an effort to create a working group to define transport services that are exposed to internet applications. A TAP enabled application identifies its needs of the locally available transports services via an API.

Jiang, et al.

Expires April 27, 2015

[Page 11]

---

Internet-Draft

CONET/AEON Gap Analysis

October 2014

Furthermore, the transport services of TAPS could benefit from this communication with the network.

- o SFC (Service Function Chaining) is a working group chartered to address issues associated with the deployment of service functions (e.g. firewalls, load balancers) in large-scale environments. Service function chaining is the definition and instantiation of an ordered set of instances of such service functions, and the subsequent "steering" of traffic flows through those service functions.

## 8. Security Considerations

A trust relationship should be established among end users, ICPs and ISPs. The authentication and authorization for end user access should be as easy as possible. OAUTH protocol [[RFC6749](#)] & OpenID [[OpenID](#)] may be adopted.

Traffic identifiers with packets should be protected against any tampering during transportation.

The protocol used to notify/negotiate the traffic identifiers to/with network should be protected.

## 9. IANA Considerations

This document includes no request to IANA.

## 10. Acknowledgements

Valuable comments were received from Peng Fan, and Weihua Qiao.

This document was produced using the xml2rfc tool [[RFC2629](#)].

## 11. Change log [RFC Editor: Please remove]

[draft-conet-aeon-gap-analysis-00](#): original version, 2014-05-29.

[draft-conet-aeon-gap-analysis-01](#): added gap analysis of the ALTO mechanism, 2014-10-24.

## 12. References

### 12.1. Normative References

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.

Jiang, et al. Expires April 27, 2015 [Page 12]

---

Internet-Draft CONET/AEON Gap Analysis October 2014

[RFC2205] Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", [RFC 2205](#), September 1997.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", [RFC 2474](#), December 1998.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), June 2000.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", [RFC 3022](#), January 2001.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C.,

and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.

- [RFC4080] Hancock, R., Karagiannis, G., Loughney, J., and S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework", [RFC 4080](#), June 2005.
- [RFC4594] Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", [RFC 4594](#), August 2006.
- [RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", [RFC 5245](#), April 2010.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), August 2008.
- [RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", [RFC 5389](#), October 2008.
- [RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", [RFC 5766](#), April 2010.
- [RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", [RFC 6241](#), June 2011.

Jiang, et al.

Expires April 27, 2015

[Page 13]

---

Internet-Draft

CONET/AEON Gap Analysis

October 2014

- [RFC6437] Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "IPv6 Flow Label Specification", [RFC 6437](#), November 2011.
- [RFC6733] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", [RFC 6733](#), October 2012.
- [RFC6749] Hardt, D., "The OAuth 2.0 Authorization Framework", [RFC 6749](#), October 2012.
- [RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", [RFC 6887](#), April

2013.

- [RFC7285] Alimi, R., Penno, R., Yang, Y., Kiesel, S., Previdi, S., Roome, W., Shalunov, S., and R. Woundy, "Application-Layer Traffic Optimization (ALTO) Protocol", [RFC 7285](#), September 2014.

## [12.2.](#) Informative References

- [BPCF] BroadBand Forum Technical Report 134, "Broadband Policy Control Framework", July 2012.
- [Gx-3GPP] 3GPP Work Item 13029, "Gx reference point for Policy and Charging Control", July 2008.
- [I-D.conet-aeon-problem-statement]  
Fan, P., Deng, H., Boucadair, M., Reddy, T., Eckel, C., and B. Williams, "Application Enabled Collaborative Networking: Problem Statement", [draft-conet-aeon-problem-statement-01](#) (work in progress), July 2014.
- [I-D.ietf-netconf-restconf]  
Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", [draft-ietf-netconf-restconf-02](#) (work in progress), October 2014.
- [I-D.ietf-rtcweb-use-cases-and-requirements]  
Holmberg, C., Hakansson, S., and G. Eriksson, "Web Real-Time Communication Use-cases and Requirements", [draft-ietf-rtcweb-use-cases-and-requirements-14](#) (work in progress), February 2014.
- [IEEE-802.1Q]  
IEEE 802.1Q, "IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks", 2005, <<http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf>>.

Jiang, et al.

Expires April 27, 2015

[Page 14]

---

Internet-Draft

CONET/AEON Gap Analysis

October 2014

- [OpenID] OpenID Foundation, "OpenID Authentication 2.0 - Final", December 2007, <<http://specs.openid.net/auth/2.0>>.
- [RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", [RFC 2629](#),



June 1999.

[RFC2818] Rescorla, E., "HTTP Over TLS", [RFC 2818](#), May 2000.

[Rx-3GPP] 3GPP Technical Specification 29.214, "Policy and charging control over Rx reference point", July 2008.

[XML\_AF\_PCRF]  
3GPP Technical Report 29.817, "Study on eXtensible Markup Language (XML) based access of the Application Function (AF) to the Policy and Charging Rules Function (PCRF)", March 2014.

#### Authors' Addresses

Sheng Jiang  
Huawei Technologies Co., Ltd  
Q14, Huawei Campus, No.156 Beiqing Road  
Hai-Dian District, Beijing, 100095  
P.R. China

Email: [jiangsheng@huawei.com](mailto:jiangsheng@huawei.com)

Hui Deng  
China Mobile  
Xuanwumenxi Ave. No.32  
Beijing 100053  
China

Email: [denghui@chinamobile.com](mailto:denghui@chinamobile.com)

Farooq Bari  
AT&T  
7277 164th Ave NE  
Redmond WA 98052  
USA

Email: [farooq.bari@att.com](mailto:farooq.bari@att.com)

Rong Zhang  
China Telecom  
No.109 Zhongshandadao avenue  
Guangzhou 510630  
China

Email: zhangr@gsta.com

Suresh Krishnan  
Ericsson  
8400 Decarie Blvd.  
Town of Mount Royal, QC  
Canada

Phone: +1 514 345 7900 x42871  
Email: suresh.krishnan@ericsson.com

Yu Fu  
Huawei Technologies Co., Ltd  
Q14, Huawei Campus, No.156 Beiqing Road  
Hai-Dian District, Beijing, 100095  
P.R. China

Email: eleven.fuyu@huawei.com

