

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: November 10, 2014

S. Jiang
Huawei Technologies Co., Ltd
R. Zhang
China Telecom
May 9, 2014

Collaborative NETwork (CONET) Gap Analysis
draft-jiang-intarea-conet-gap-analysis-00

Abstract

In order to efficiently distinguish ICPs' traffic, a new network operation model - Collaborative NETwork is proposed. The traffic recognition is based on traffic of ICPs' products actively carries collaborative identifiers that both ISPs and ICPs reach consensus in a coordination way. This document analyzes the technical gap between the current network functions and required network capability to support Collaborative NETwork.

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 November 10, 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

1.	Introduction	2
2.	Overview of Technical Considerations	3
3.	Traffic Identifiers	3
4.	Collaboration between ICPs and ISPs	5
5.	Identifying Traffics between End Users and Network	7
6.	Security Considerations	8
7.	IANA Considerations	8
8.	Acknowledgements	8
9.	Change log [RFC Editor: Please remove]	8
10.	References	8
10.1.	Normative References	8
10.2.	Informative References	9
	Authors' Addresses	10

[1.](#) Introduction

While the Internet traffic is continually growing, more and more Internet Content Providers (ICPs) realize the essentiality and advantages to cooperate with Internet Service Providers (ISPs). In order to serve their users better, ICPs raise an emerging requirement that the traffic of their products needs to be treated differently, both in traffic handling process and traffic accounting process. [\[I-D.fan-intarea-conet-ps-uc\]](#) has described such requirement and use cases in details.

The biggest technical challenge that network operators have to face is to distinguish the traffic in a finer granularity. Nowadays, DPI (Deep Packet Inspection) or DFI (Deep Flow Inspection) devices have been widely used in identifying application information of the traffic flows. However, they are expensive for both operational cost

and time consumption. They are not be able to interact with real-time network operations. A better approach would be traffic of ICPs' products carries traffic identifiers that the network entities of ISPs can easily recognise. The traffic identifiers must be consistent in collaboration between ISPs and ICPs. This approach is called Collaborative NETwork (CONET) in this document.

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

[2.](#) Overview of Technical Consideratins

Overall, there are three technical aspects that need to be considered in CONET, listed below. This section gives analysis to each aspects.

- o A traffic identifier.
- o An ICP notify/negotiate traffic identifiers and the desired processing way regarding to both traffic handling and traffic accounting with an ISP. The policies of traffic processing need to be propagated and network entities need to be configured correspondently within an ISP network.
- o An end user host or application notify/negotiate their traffic identifiers to/with network.

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 the network and transport layers only.

[3.](#) Traffic Identifiers

The precondition that a traffic flow can be differentially handling is that it can recognized by the network entities. In this document,

the character 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 a lifetime of flow.
- o Traffic identifiers should be easy to be inspected by network entities.
- o Traffic identifiers should accurately distinguish traffic flow or a type/category of traffic flow.

- o Traffic identifiers must be trustable and protected against any tampers occurring during transportation.
- o Some traffic identifiers may be convergencable in order to reduce the management complexity on stateful records/policies.
- o Some traffic identifiers may dynamically decide in the run time. Its decision may involve dynamic 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 remark or set new traffic identifier based on its traffic recognition.
- o Some traffic identifiers may be meaningful cross administrative boundaries.

[I-D.fan-intarea-conet-ps-uc] analyzes two current used traffic identifiers: application-level characteristic information used by DPI and IP addresses of ICP servers. Each of them has a few issues, summarized as below:

- o Application-level characteristic information used by DPI. Accuracy of application identification cannot be guaranteed. The ability highly depends on vendors. The computing resource consumption is very high. Furthermore, the usage of TLS [[RFC5246](#)] and HTTPS [[RFC2818](#)] is increasing the difficulties of DPI.

- o IP addresses of ICP servers. More granular traffic handling cannot be satisfied because a single server may hold multiple services that need to be distinguished. Cache/CDN uses different IP addresses, which may be also shared with other ICPs.

There are also other traffic identifiers or components that may compose traffic identifiers:

- o IP addresses of end user devices. They are nature identifiers that can distinguish the communication node. However, one end user node would have many traffics. CONET requires to recognize only these 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 Network Address Translator (NAT, [[RFC3022](#)]).
- o Port numbers. They are useful to distinguish flows/services from the same node. However, it cannot be used to identify network

traffics 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 abovementioned traffic identifiers has their own suitable scenarios and limitations. New traffic identifiers may be defined in

the future.

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 common 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 it is not convergencable. Managing numerous 5-tuple may be a big burden for ISPs. Furthermore, the existing of NATs change the 5-tuple of traffic in the way. Consequently, the traffic identifiers associated with IPv4 addresses have to very complicated management issues.

4. Collaboration between ICPs and ISPs

Firstly, an ICP need to reach consistent with an ISP on traffic identifiers, which network would recognize the ICP traffic accordingly.

Then, the ICP notify the specific traffic identifiers, which may have multiple categories, and the desired policies associated with each traffic categories, to the ISP. Then the ISP network can apply these policies when actual traffics happen.

The notification process between ICPs and ISPs should be dynamical through a protocol/interface. In 3GPP 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 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](#)].

With in 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.

BroadBand Forum has also defined the Broadband Policy Control 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 lacking involvement from end user devices/applications, user clients will be difficult to be identified if they are behind NAT (they have NATed IPv4 addresses). Even by correlating the authentication process which could send user information to PCRF, it will still make the whole process very complicated.

Another major issue is that this model is ISP-orientied. 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

Recognition of the traffic from ICP servers to end users may not be very difficult giving the natural convergency. However, when an end user host or application initiates traffic towards ICP contents, particularly some contents may be obtained cache/CDN deployed in the network, it is needed for the end user host or application actively notifying its traffic to the network.

The traffic identifiers used by end user host or application:

- o may be authorised 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 characters, and leave the network to recognize them, then mapped into other traffic identifiers that meaningful and explicit within the network.

There are many existing protocols that may be extended to realize the out-of-band controlling mechanism. However, these existing protocols were designed to serve their own purposes and scenarios. Defining a new dedicated protocol may also be an option.

- o Resource ReSerVation Protocol (RSVP, [[RFC2205](#)]) is a resource reservation setup protocol. However, so far, that is mainly used among network entities. Next Steps in Signaling (NSIS, [[RFC4080](#)]) provides duplicated function as RSVP. It is not widely deployed.
- o 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 [[RFC2865](#)] and Diameter [[RFC6733](#)] provides an Authentication, Authorization and Accounting for network access.

Currently, there is no many in-band mechanisms, in which traffic identifier that the end user devices/applications set up is carried within packets. In-band mechanisms is able to traverse administration domains, and it is possible the traffic gets identical handling. The precondition of in-band mechanisms is that the

integrity of traffic identifiers can be validated by network

entities.

6. 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 occurring during transportation.

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

7. IANA Considerations

This document includes no request to IANA.

8. Acknowledgements

Valuable comments were received from Peng Fan, Farooq Bari, Weihua Qiao and Hui Deng.

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

9. Change log [RFC Editor: Please remove]

[draft-jiang-intarea-conet-gap-analysis-00](#): original version, 2014-05-09.

10. References

10.1. Normative References

- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [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.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), August 2008.
- [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.

[10.2](#). 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.fan-intarea-conet-ps-uc]
Fan, P. and H. Deng, "CONET (Collaborative Network) Problem Statement and Use Cases", [draft-fan-intarea-conet-ps-uc-00](#) (work in progress), March 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.

Jiang & Zhang

Expires November 10, 2014

[Page 9]

Internet-Draft

Collaborative Network Gap Analysis

May 2014

[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

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

Email: zhangr@gsta.com

