Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 4, 2015

P. Fan
China Mobile
M. Boucadair
France Telecom
B. Williams
Akamai, Inc.
T. Reddy
C. Eckel
Cisco Systems, Inc.

July 3, 2014

Application Enabled Collaborative Networking Requirements
draft-conet-aeon-requirements-00

Abstract

Identification and treatment of application flows are important to many application providers and network operators. Historically, this functionality has been implemented to the extent possible using heuristics, which inspect and infer flow characteristics. But many application flows in current usages are dynamic, adaptive, time-bound, encrypted, peer-to-peer, asymmetric, used on multipurpose devices, and have different priorities depending on direction of flow, user preferences, and other factors. Any combination of these properties renders heuristic based techniques less effective and may result in compromises to application security or user privacy. The document states requirements for a solution that enables identification and treatment of application flows without suffering the limitations that plague existing solutions.

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 January 4, 2015.

Table of Contents

1. Introduction

Identification and treatment of application flows are important to many application providers and network operators. The problems faced by existing solutions that try to provide such visibility and to enable appropriate treatment of application flows are described in detail in [I-D.conet-aeon-problem-statement].

As the IETF establishes default behaviors that thwart pervasive surveillance (e.g. [RFC7258]), it will be important to provide mechanisms for applications that want to have the network provide differential flow treatment for their data. The intent is to have applications protect the contents of their flows, yet have the ability to opt-in to information exchanges that provide a more precise allocation of network resources and thus better user experience. The document provide a complete set of requirements for such a solution.

2. Terminology

The section clarifies the intended meaning of specific terms used within this document.

- 5-tuple: The combination of source IP address and port, destination IP address and port, and transport protocol used to transport an application flow.

- Application: An instance of an application running on end user's device, such as a web application running on an laptop or an application running on a mobile device.

- Flow characteristics: Characteristics of an individual application flow, such as 5-tuple used to transport the flow, tolerance to delay, loss, or jitter, anticipated average or maximum rate, relative priority with respect to the application's other flows, etc. Examples of individual application flows include an audio flow, a video flow, a data flow, etc.

- Network node: A network element, such as a router, switch, wireless access point, firewall, etc., that is in the path of one or more application flows.

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 [RFC2119].

3. Requirements

Rather than encourage independent, protocol specific solutions to this problem, this document advocates a protocol and application independent information model and individual data models that can be applied in a consistent fashion across a variety of protocols to enable explicit communication between applications and the networks on which they are used. The requirements are:

Req-1: MUST provide a mechanism for applications to explicitly signal the flow characteristics for their flows to the network.

Req-2: MUST provide network nodes visibility to the flow characteristics signaled by applications.

Req-3: MUST provide mechanism for applications to receive feedback from the network. This feedback communicates anticipated ability of the network node to accommodate the corresponding flow.

Req-4: MUST provide visibility for both directions of a flow, including flows that cross administrative boundaries.

Req-5: MUST provides mechanism for mutual authentication between applications and network nodes, such that applications signal flow characteristics and receive feedback from trusted network nodes

and network nodes process flow characteristics signaled by authorized applications.

Req-6: MUST provide mechanism for 3rd party authentication and authorization for over-the-top (OTT) applications.

Req-7: MUST provide mechanism for integrity protection and replay protection of exchanges between the application and the network.

Req-8: MUST provide mechanism for applications to opt-out of any explicit signaling of their flow characteristics to the network.

Req-9: MUST provide mechanism for flow characteristics signaled by applications to change over time, and in a timely manner, in response to changes in application operation.

Req-10: MUST provide mechanism for feedback provided by network nodes to change over time, and in a timely manner, in response to changes in network conditions.

Req-11: SHOULD provide mechanism for application flow characteristics to be propagated to all network nodes within a network.

Req-12: MUST NOT dramatically affect the performance of participating network nodes and other network infrastructure propagating the flow characteristics.

Req-13: MUST be applicable for both IPv4 and IPv6 deployments.

Req-14: SHOULD reuse or extend existing IETF standard protocols wherever possible.

Req-15: MUST provide considerations for protection against denial of service attacks against network nodes.

Req-16: MUST provide mechanism(s) that can be implemented as part of a user process or library that does NOT require any special privileges.

In designing a solution that meets these requirements, considerations should be made for existing deployments of heuristic based mechanisms. Such mechanisms are used in many networks and it is desirable that they continue to work as applications and networks nodes are incrementally enabled with functionality provided by this solution.

4. Informative References

[I-D.conet-aeon-problem-statement]
Fan, P., Deng, H., Boucadair, M., Reddy, T., and C. Eckel, "Application Enabled Collaborative Networking: Problem Statement and Requirements", draft-conet-aeon-problem-statement-00 (work in progress), May 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, May 2014.

Authors' Addresses

Peng Fan
China Mobile
32 Xuanwumen West Street, Xicheng District
Beijing 100053
P.R. China

Email: fanpeng@chinamobile.com

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Brandon Williams
Akamai, Inc.
8 Cambridge Center
Cambridge, MA 02142
USA

Email: brandon.williams@akamai.com

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tireddy@cisco.com

Charles Eckel
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

Email: eckelcu@cisco.com