Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: September 20, 2014

P. Fan
H. Deng
China Mobile

March 19, 2014

CONET (Collaborative Network) Problem Statement and Use Cases
draft-fan-intarea-conet-ps-uc-00

Abstract

This document describes problems of identifying and handling application traffic in an ISP' network, and use cases of collaborative network which enables active cooperation between ICPs and ISPs for better traffic operation.

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 September 20, 2014.

Table of Contents

1. Introduction

Internet service providers (ISPs) around the world have been seeing booming growth of subscriber population and traffic volume of internet service over the years. Data traffic congestion causes severe user experience degradation, which requires ISPs to better operate its data network. Today's ISPs are making efforts to handle the traffic that goes through their networks more effectively. [PCC] and [PCF] are some of the work that helps ISPs to solve the problems in data traffic operation.

Meanwhile, internet content providers (ICPs) which provide the applications are gradually realizing the necessity of cooperation with the ISPs rather than having them be the dumb pipe. By utilizing the ability of agile traffic management and classification provided by the network, ICPs intends to receive better treatment and differentiation on the traffic of their products, so as to meet user requirement and expectation, enhance user experience and viscosity, thus increase their revenue.

Unlike the past time when they are performing independently without concern for each other, there is growing needs for ICPs and ISPs to build collaborative connections, which will benefit both of them as well as users. There are also emerging operational models that reflect this connection.

- Content based charging offers customized, application specific billing strategy compared with traditional flat rate or time/ volume based charging.

- Application based traffic optimization, such as QoS guarantee and firewalling, also requires the knowledge of the type of the traffic.

One of the challenges ISPs meet in data traffic operation is to perceive the traffic in a finer granularity. A traditionally widely used approach is to deploy content aware devices which are

specialized in identifying application information of the traffic flows using technics like DPI (Deep Packet Inspection) or DFI (Deep Flow Inspection). Because of the tentative and deductive nature, these devices have met precision and timeliness limitation in practical deployment. If an ICP can actively notify its characteristics to the network, traffic identification will be much more applicable and precise, and no dedicated identification devices are needed.

2. Problem Statement

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.

- 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.

- Internet applications are apt to change frequently, so are the characteristics of themselves. There will be a time latency to complete application traffic analysis and update signature database when a new application or version appears, which also contributes to the inaccuracy of identification.

- Content aware devices usually act as a black box. There is no standard way in implementation or benchmarking. So the ability highly depends on vendors. Different boxes are likely to give different identification results to the same traffic.

- Content aware functions require parsing the payload of packets, leading to very high device resource consumption. Built-in content aware function modules in network elements like GGSN/BRAS will affect the forwarding performance and thus impact data transmission.

- Investment cost cannot be neglected. Sometimes the cost to identify the traffic is no less than that to forward the traffic. Operational cost of the additional identifying nodes is also an

important issue. More potential failure points and possible optical power split will affect network quality.

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 volume of the application. This approach will have limitations when dealing with more complex scenarios.

- 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, traffic for http://www.example.com/text/ and http://www.example.com/video/ is likely to receive different treatment but target to the same IP address; traffic from two users to the same server is a similar case.

- If cache/CDN 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.

- 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.

3. Use Cases

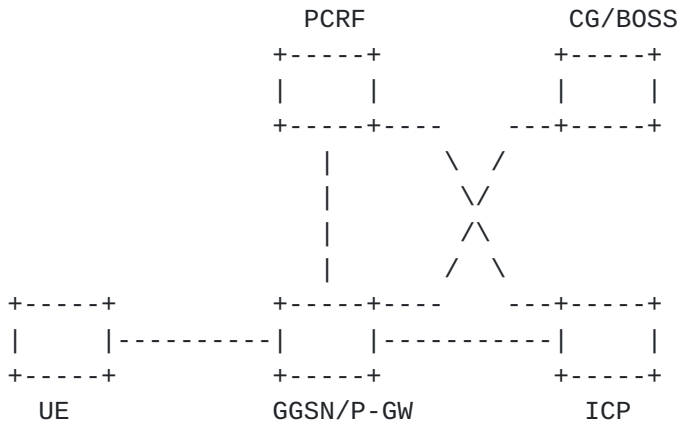
If there is a way for an application to actively notify its information to the network, passive inspection devices will not be needed. Bridging of application and network is also believed to be effective, precise and helpful in cooperation between ISPs and ICPs. Here we describe two use cases which benefit from active negotiation of application and network.

3.1. Content based charging

Commonly used billing method for mobile subscribers, e.g. volume based charging, does not distinguish from the angle of applications. It introduces difficulty for users to use applications consuming large volume in this billing model. ICPs also have to strive for volume apart from preference and time of users. Content based charging takes content related information into account and enables smarter pricing strategy. Operators can place different prices for different types of traffic, and help ICPs build tight relationship with their users, e.g. wholesaling the data volume of an application

to its developer ICP so that users can use the application free of charge.

An application intending to benefit from content based charging can notify its existence to the network and have its traffic charged in the desired way. The following diagram shows an architecture of content based charging in 3GPP mobile network.



A typical process of content based charging for an application is as follows:

1. ICP applies for content based charging for its application to PCRF. Information notified may include application identifier, description of flows needing special charging (e.g. signature, 5 tuples), intended charging model (e.g. data volume of the application is free of charge), etc.

2. PCRF configures matching rules on GGSN/P-GW.

3. End user uses the application.

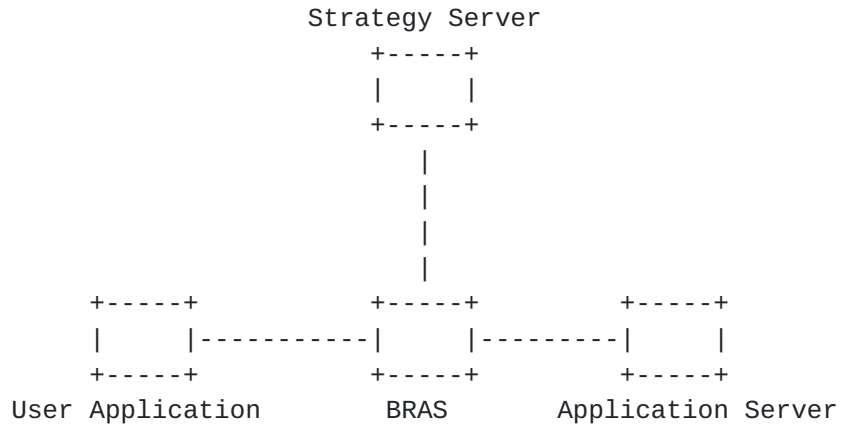
4. GGSN/P-GW receives and matches the traffic of the application, and provides charge records of the application to billing unit CG /BOSS.

3.2. QoS ability opening

QoS ability opening is provided by the network to enable dynamic access acceleration, priority guarantee and other service differentiation for ICPs, and new application based QoS selling business for operators.

QoS opening can be realized in mobile networks as well as fixed broadband networks. The following diagram depicts an architecture of open QoS ability in broadband access networks. Current QoS in

broadband access networks is usually circuit or user based, achieved by configuring policies on network nodes like an edge router, and is not dynamic, on-demand or application specific. If application characteristics are signaled to the network, network will be able to know the exact application information of the traffic, and thus perform QoS accordingly. By signaling characteristics, application can decide when and how to request the network to provide QoS for its traffic.



A typical process of the application initiated QoS can be described as follows:

1. End user application initiates data traffic. The application may be a downloading service, online video service, etc.

2. Application decides that QoS is needed for its traffic, e.g. the user is logged as VIP.

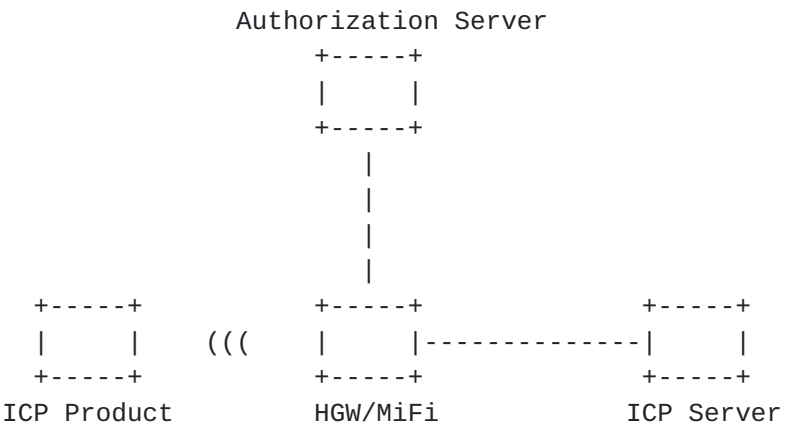
3. Application signals information of the traffic needing QoS to the strategy server in the network. Information signaled may include application identifier, flow description (e.g. 5 tuples), subscribed QoS contract, etc.

4. Strategy server validates the request from application and the contract with the ICP, and sends corresponding configuration to forwarding devices (e.g. BRAS) to perform requested QoS.

3.3. Application experience enhancement

There are many ICPs today providing internet based home products to users. For example, an internet TV box uses WiFi to connect the internet and provides video programs to users. ICPs wish to cooperate with ISPs providing the access service to improve the experience of their services, as access network is often congested due to extensive internet usage nowadays. But currently classifying

the traffic of the services is rather complex when the traffic is mixed with other normal traffic in a single pipe (e.g. WiFi). Collaboration of ICP and ISP can solve the problem.



A typical process of this enhancement can be described as follows:

1. ICP product communicates with access gateway (e.g. HGW, MiFi) to request special treatment of its traffic. Information signaled may include product identifier, authorization token, desired treatment (e.g. high priority, bandwidth reservation), etc.

2. Access gateway forwards the information to the authorization server, and authorization server signals back the result.

3. Access gateway coordinates with backhaul network to tag and classify the traffic of the product (can be specified by the address of the product).

4. Informative References

[PCC] 3GPP Technical Specification 23.203, , "Policy and charging control architecture", March 2012.

[PCF] BBF STRAW BALLOT WT-134, , "Broadband Policy Control Framework (PCF)", February 2012.

Authors' Addresses

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

Email: fanpeng@chinamobile.com

Hui Deng
China Mobile
32 Xuanwumen West Street, Xicheng District
Beijing 100053
P.R. China

Email: denghui@chinamobile.com