Broadband Carrier Access Group
DPI Solution

May 20, 2015

Broadcom Corporation
5300 California Avenue
Irvine, California, USA 92677
Phone: 949-926-5000
Fax: 949-926-5203
www.broadcom.com

Revision History

Revision	Date	Change Description
0.1	02/06/14	First draft
0.2	05/20/15	Second draft

Table of Contents

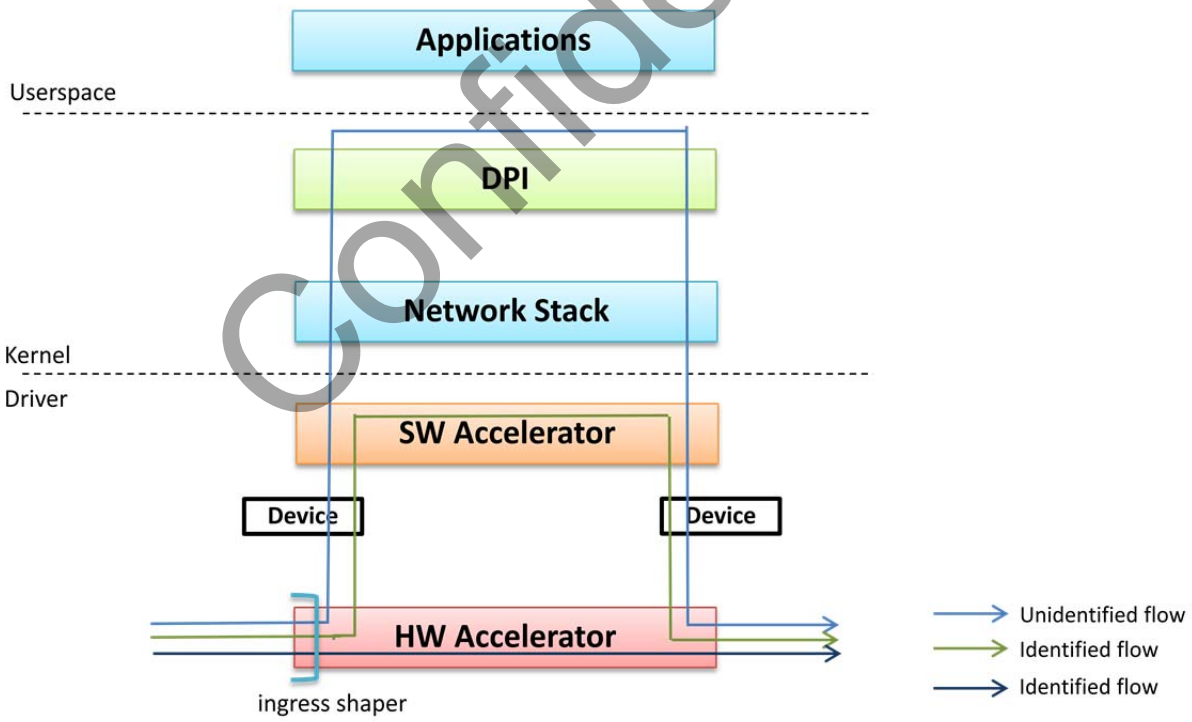
Overview

This application note describes statistics collection based on applications/devices. We will introduce the Deep Packet Inspection (a.k.a DPI) architecture followed by detailed description of major components. At last section, the commands to get application statistics are presented.

Architecture

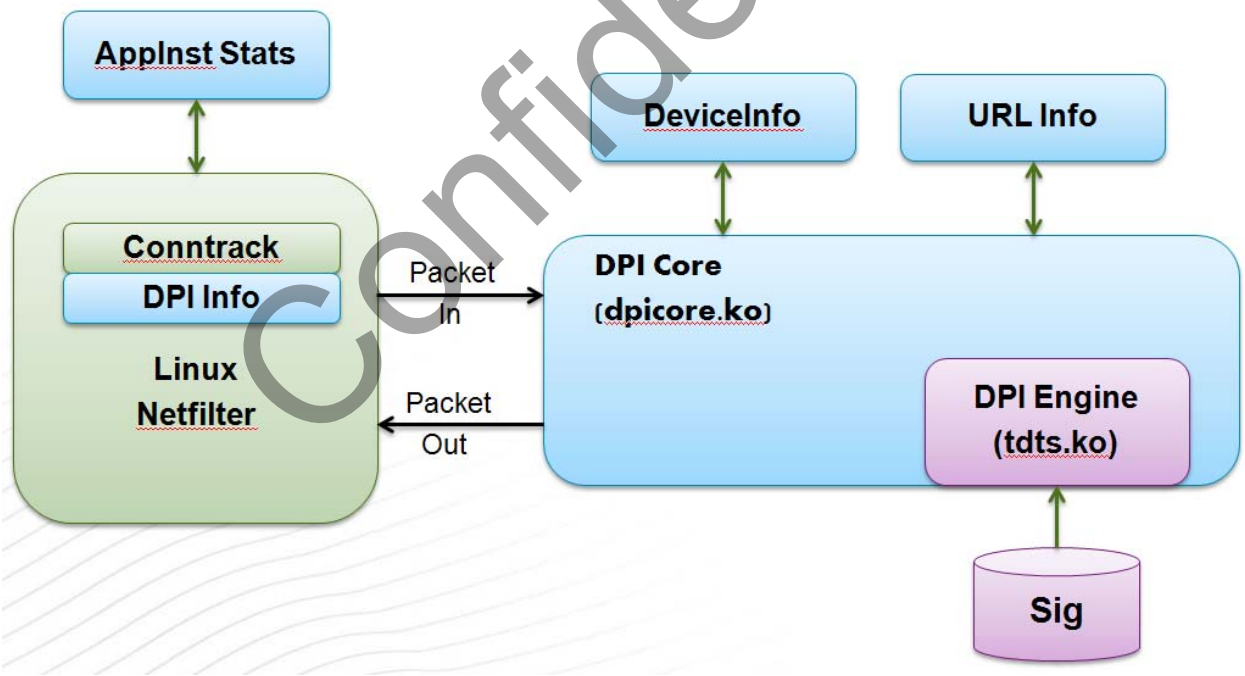
DPI engine can provide more information, like application identification, than standard 5-tuple. It is treated as a module with the knowledge of application layer. Therefore, DPI engine is to support advance packet classification so that operators and end-users can have better monitor/control of the network.

The DPI technology in kernel space includes both application identification and device identification. Because a flow (packets with the same 5-tuple) can only belong to one application, our learning based accelerators can still benefit in DPI scenario. As long as DPI module completes classification, our SW/HW accelerators can still accelerate the packets to prevent any performance hit. The following figure illustrates the concept.



In our design, DPI solution consists of multiple components:

1. DPI Engine (binary released): This module is responsible for application classification.
2. Device information table: This module is to record the information of LAN devices, including MAC address, device types, and etc.
3. Connection tracker: We enhance Linux conntrack to carry DPI information, including application ID, index to device information table, and identification status.
4. DPI Core: This module is the interface between DPI Engine and the system. It takes the packets from the network stack and sends to DPI Engine for classification. Then it saves the result from DPI Engine to connection tracker and Device information table. If DPI Engine completes the classification, this module will trigger our accelerator to accelerate the flow. Currently, DPI core registers at netfilter forwarding and input chain. (PS: input chain is for device identification only)
5. AppInst (unique combination of application ID and MAC address) statistics table: This module records accumulative statistics per appinst. This is example code that illustrates certain principles, and is meant as a head-start to the implementation of the statistic gather code, by our customers.



Operation

Four components are required to activate DPI feature:

1. */lib/modules/3.4.11-rt19/extra/tdts.ko*: DPI Engine
2. */bin/tdts-rule-agent*: This is user command to control DPI Engine
3. */etc/rule.trf*: Signature database
4. */lib/modules/3.4.11-rt19/extra/dpicore.ko*: DPI core

A script which is triggered at system bootup to activate DPI feature is at:
userspace/private/apps/dpieng/scripts/dpiinit.sh
Here is the summary:

1. insmod /lib/modules*3.4.11-rt19*/extra/tdts.ko: Load DPI Engine module.
2. tdts-rule-agent -r /etc/rule.trf –g: It configures DPI Engine with the signature database and generate some files at current directory which will be described below.
3. insmod /lib/modules/*3.4.11-rt19*/extra/dpicore.ko: Enable DPI feature at the system.

The files generated by tdts-rule-agent are as follows.
bwdpi.app.db (application ID and application name mapping):
AppCategoryID,AppID,AppBehaviorID,AppName
0,1,0,MSN
0,2,0,Yahoo Messenger
0,3,0,ICQ/AIM/iChat(Mac)
0,4,0,QQ/TM
…

bwdpi.beh.db (application behavior ID and application behavior name mapping):
AppBehaviorID,AppBehaviorName
1,authority
2,communicate
3,transfer
4,media
5,game
6,access
7,connect

bwdpi.cat.db (application Category ID and application category name mapping):
AppCategoryID,AppCategoryName
0,Instant messaging
1,P2P
3,File Transfer
4,Streaming Media
5,Mail and Collaboration
6,Voice over IP
7,Database

8,Games
9,Network Management
10,Remote Access Terminals
11,Bypass Proxies and Tunnels
12,Stock Market
13,Web
14,Security Update
15,Web IM
17,Business
18,Network Protocols
19,Network Protocols
20,Network Protocols
21,Mobile
23,Private Protocol
24,Social Network
28,TopSites-Adult
29,TopSites-Arts
30,TopSites-Business
31,TopSites-Computers
32,TopSites-Games
33,TopSites-Health
34,TopSites-Home
35,TopSites-KidsnTeens
36,TopSites-News
37,TopSites-Recreation
38,TopSites-Reference
39,TopSites-Regional
40,TopSites-Science
41,TopSites-Shopping
42,TopSites-Society
43,TopSites-Sports

bwdpi.devdb.db (device ID and device name mapping):
DevVendorID,DevOsID,DevClassID,DevTypeID,DevNameID,DevCatrgoryID,DevVendorName,DevOsName,DevClassName,DevTypeName,DevName,DevCategoryName
8,8,5,31,296,1,"Google Inc.","Android 3.0-4.1","Android","SmartTV","Chromecast","Smart TV & Set-top box"
47,19,15,17,298,2,"Microsoft Corp.","Windows","Windows","Game Console","Xbox One","Game Console"
…

DPI Statistics in Procfs

DPI statistics is recorded based on connection tracker. Therefore, in order to get appinst statistics, it is required to walk through all entries of connection tracker and aggregate the result. In addition, an application may consist of multiple connections and connections may be initiated or evicted at different time. Whenever a connection is evicted, the statistics has to be updated accordingly as well.

Due to our packet accelerators, most traffic does not enter Linux network stack/netfilter. In order to obtain accurate statistics, two hooks are provided in the kernel to get statistics from the accelerators: one for query current statistics in the accelerator and another one for statistics update of evicted entries in the accelerator. Because we support up to 16k entries in our accelerator, we don't support instantaneous statistics for performance concern. Instead, the statistics may be couple of seconds delayed. So timestamp information will be included while querying statistics from our accelerator.

We support two tables in procfs to show DPI statistics: conntrack_dpi and dpi_stat.

conntrack_dpi shows the conntrack statistics along with 5-tuple information for each entry in the connection tracker. Here is the layout of conntrack_dpi:

AppID, Mac, UpstreamPkt, UpstreamByte, UpstreamTimeStamp, DnStreamPkt, DnStreamByte, DnStreamTimStamp, AppStatus, UpStreamTuple, DnStreamTuple

Example:
cat /proc/net/conntrack_dpi
AppID Mac Vendor OS Class Type Dev UpPkt UpByte UpTS DnPkt DnByte DnTS Status UpTuple DnTuple URL
0d005400 f0:99:bf:22:2f:0a 11 25 16 29 118 6 389 0 4 454 0 10e src=192.168.1.3 dst=23.15.232.93 sport=51237 dport=80 src=23.15.232.93 dst=10.6.37.200 sport=80 dport=51237 static.ess.apple.com:80

dpi_stat is example code which shows the appinst statistics along with device information for each application instance. Here is the layout of dpi_stat:

AppID, Mac, VendorID, OsID, ClassID, TypeID, DevID, UpstreamPkt, UpstreamByte, DnStreamPkt, DnStreamByte

Example:
cat /proc/net/dpi_stat
08009b00 f0:99:bf:22:2f:0a 11 25 16 29 118 5 429 10 5060

DPI Command Utility

DPI command utility includes both dpictl command line and dpictl library. It is a standalone command utility which is independent of our Configuration Management System (CMS). It provides two functionalities: configuration and display status and statistics.

- Configuration: So far, dpi command utility can only enable/disable DPI classification. If disabled, all packets will not enter DPI engine.

- Display: dpi command can display whether dpi classification is enabled or not. In addition, unlike Procfs, it can show human readable statistics per application, per application category, per device, or per application instance.

Examples:
 # dpi app
67111424,iTunes,17,3142,15,9482
67129344,Web Streaming,21,3483,21,20378
67134720,Pandora,1047,115069,1133,1279745
67142144,Spotify,2339,207374,2746,3780269
218125312,Apple.com,43656,2882478,56507,81547098
402653952,Facebook,932,308590,908,572068

 # dpi appstat --id 402653952
402653952,Facebook,932,308590,908,572068

 # dpi dev
f0:99:bf:22:2f:0a,iPhone/iPad/iPod,53743,4049709,67580,94978685

 # dpi appcat
4,Streaming Media,5577,518589,6413,8082544
13,Web,45309,2993598,58453,84320471
24,Social Network,932,308590,908,572068
36,TopSites-News,5,272,3,160

 # dpi appinst
302006016,World Wide Web HTTP,f0:99:bf:22:2f:0a,iPhone/iPad/iPod,10,544,5,276
335587328,Google(SSL),f0:99:bf:22:2f:0a,iPhone/iPad/iPod,303,39632,289,275843
67129344,Web Streaming,f0:99:bf:22:2f:0a,iPhone/iPad/iPod,25,3691,23,20482
67142144,Spotify,f0:99:bf:22:2f:0a,iPhone/iPad/iPod,2439,218239,2840,3873509
67111424,iTunes,f0:99:bf:22:2f:0a,iPhone/iPad/iPod,40,6572,34,19310
335592704,Google User Content(SSL),f0:99:bf:22:2f:0a,iPhone/iPad/iPod,60,9174,49,17647
67134720,Pandora,f0:99:bf:22:2f:0a,iPhone/iPad/iPod,3092,293865,3527,4171175
218125312,Apple.com,f0:99:bf:22:2f:0a,iPhone/iPad/iPod,45346,2994364,58511,84438602
402653952,Facebook,f0:99:bf:22:2f:0a,iPhone/iPad/iPod,932,308590,908,572068

 # dpi url
cont-ch1-1.pandora.com
cont-sv5-2.pandora.com
stats.pandora.com
t1-1.p-cdn.com
cont-dc6-1.pandora.com
cont-sv5-1.pandora.com
appldnld.apple.com
captive.apple.com
static.ess.apple.com:80