How to find different Web User-Agents and classify them

The purpose of this document is to outline some simple steps to find Web User-Agents on your network and create sub-classes for them. You can easily provide a pie chart on HTTP differentiated User Agents.

I got Auto-Discovery enabled and found HTTP on my discovered classes. I created a policy to see Class Hits and Policy Hits.

Traffic Class Name	Class Hits	Policy Hits	Current (bps)	1 Min (bps)	Peak (bps)	Guar. Rate Failures	Pkt Exch (ms)	Partition Min-Max	Policy Type (Pri.) Guar.-Limit
HTTP	323	323	2.0M	885k	2.0M	0	11		Rate (3) 0

You can see all HTTP traffic be classified in one single class. As most users like their own browsers (as long there is no restriction, or control mechanism to avoid such different browser specific communication)

There's a CLI command, which enables application-specific criteria tracking, which can be used to sub-class on certain criteria. To get proper values for sub-classification, I was interested in finding all kind of user-agents, so I can sub-classify them below HTTP.

Connect to your PacketShaper using Telnet or Console and type following command. This enables the track feature on the class /inbound/http for the application "**web**" with the attribute "**user-agent**"

```
packetshaper# class criteria track /inbound/http web user-agent
```

Let it run for a while and see the output of different user-agents on your network.

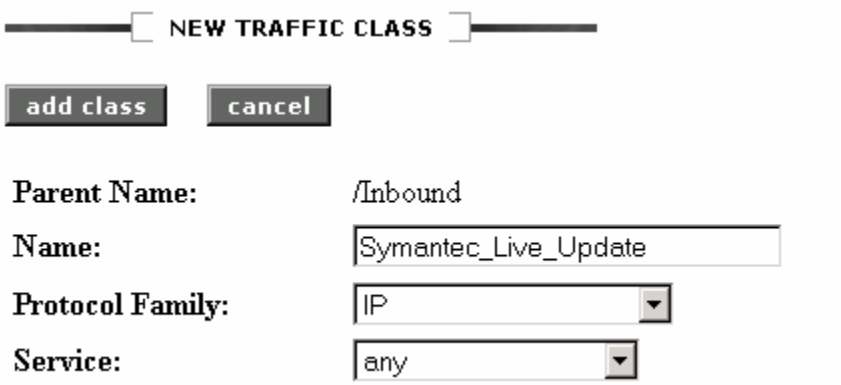
```
PacketShaper# class criteria recent /inbound/http

Traffic Class: /Inbound/HTTP
  Application: Web
    Attribute: user-agent (Web Browser or User Agent)

Recent Attribute Values (most recent first)
------------------------------------------------------------------------------
   1. Mozilla/4.0 (compatible; MSIE 5.0; Windows NT 5.1) Opera 5.02  [en]
   2. Symantec LiveUpdate
   3. Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)

PacketShaper#
```

I can now use this information, to sub-classify HTTP, based on the user-agent. In this example, I'd like to give them all the same policy, except Symantec Live Update, because Anti-Virus Update process should get bandwidth, before regular HTTP traffic will get.

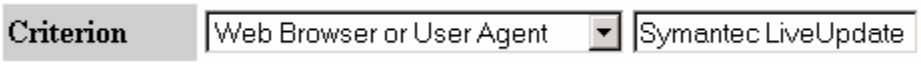
When you are done, turn off tracking using following CLI command

```
packetshaper# class criteria track /inbound/http off
```

Based on this tracking, I'm going to sub-class HTTP for better classification



Don't forget to classify the proper criterion at the end of the **add class page.** Make sure you type the exact match of the criterion track output



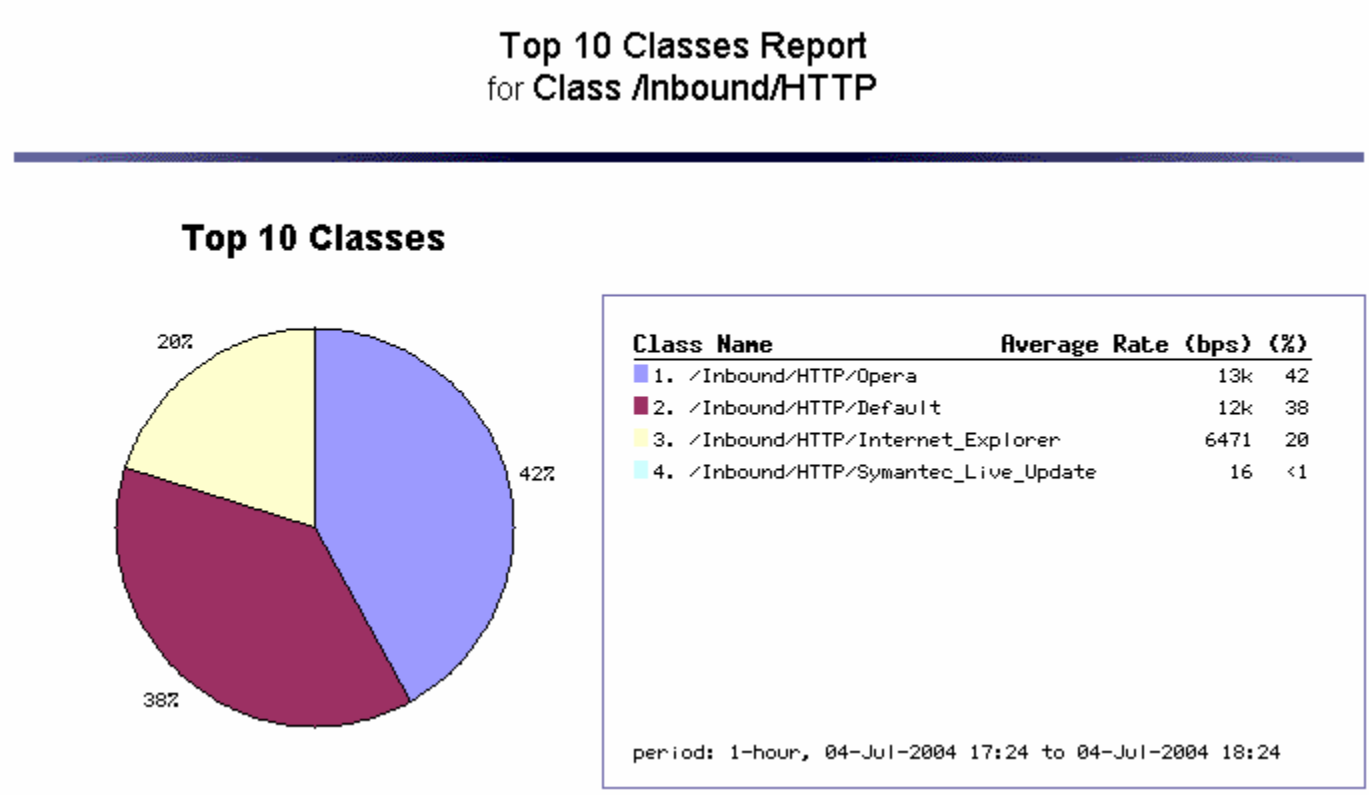
I did the same for Internet Explorer and Opera Web browser, with their corresponding values.

Traffic Class Name	Class Hits	Policy Hits	Current (bps)	1 Min (bps)	Peak (bps)	Guar. Rate Failures	Pkt Exch (ms)	Partition Min-Max	Policy Type (Pri.) Guar.-Limit
HTTP			192k	83k	282k	0	NA		
Internet_Explorer	14	14	161k	47k	238k	0	25		Rate (3) 0
Opera	37	37	0	8480	155k	0	35		Rate (3) 0
Symantec_Live_Update	6	6	0	26	2462	0	146		Rate (6) 0
Default	37	37	34k	17k	216k	0	33		Rate (3) 0

To view other applications and criterions:

```
packetshaper# class criteria attributes
```

Another way to get a nice VP graphical summary on the percentage of used HTTP user-agents; you can run Top 10 Class report.



What could you do next? There is still 38% HTTP Traffic going into the Default Class. Start again the class criteria track into the Default Class of HTTP. I could find some more user-agents, based on HTTP

```
Traffic Class: /Inbound/HTTP/Default
  Application: Web
    Attribute: user-agent (Web Browser or User Agent)

Recent Attribute Values (most recent first)
------------------------------------------------------------------------------
   1. Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4) Gecko/20030624 Netscape/7.1 (ax)
   2. Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.0.3705)
   3. Deepnet Explorer
   4. XSCHTTP
   5. Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Deepnet Explorer; .NETCLR 1.1.4322)
```

I can now sub-classify some other's and No. 4 - XSCHTTP, I probably "never-admit" ☺