

Blue Coat® Systems

# Using PacketShaper to Control “Bring Your Own Device” Traffic

*Tips and Tricks Supporting the BYOD  
Worldwide Phenomenon*



Copyright© 1999-2013 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of Blue Coat Systems, Inc. All right, title and interest in and to the Software and documentation are and shall remain the exclusive property of Blue Coat Systems, Inc. and its licensors. ProxyAV™, ProxyOne™, CacheOS™, SGOS™, SG™, Spyware Interceptor™, Scope™, ProxyRA Connector™, ProxyRA Manager™, Remote Access™ and MACH5™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, ProxySG®, WinProxy®, PacketShaper®, PacketShaper Xpress®, PolicyCenter®, PacketWise®, AccessNow®, Ositis®, Powering Internet Management®, The Ultimate Internet Sharing Solution®, Cerberian®, Permeo®, Permeo Technologies, Inc.®, and the Cerberian and Permeo logos are registered trademarks of Blue Coat Systems, Inc. All other trademarks contained in this document and in the Software are the property of their respective owners.

BLUE COAT SYSTEMS, INC. AND BLUE COAT SYSTEMS INTERNATIONAL SARL (COLLECTIVELY "BLUE COAT") DISCLAIM ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL BLUE COAT, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF BLUE COAT SYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Americas:

**Blue Coat Systems, Inc.**  
420 N. Mary Ave.  
Sunnyvale, CA 94085

Rest of the World:

**Blue Coat Systems International SARL**  
3a Route des Arsenaux  
1700 Fribourg, Switzerland

**Document History**

Date	Version	Note
January 15, 2013	v1.0	Initial release

---

## Contents

Introduction .....	1
Growth of BYOD (Smart phones and Tablets) Devices from 2009 to Present .....	1
Apple BYOD (iPhones and iPads) from 2009 to mid-2012.....	1
Impact of BYOD Recreational Traffic on Unmanaged Networks .....	2
Best Practices .....	3
PacketShaper Tips and Tricks.....	4
1. Identification/Classification.....	4
2. PacketShaper Classification/Subclassification of BYOD Traffic .....	4
3. Control/QoS Policies.....	5
4. Verify/Review .....	6
Appendix A – Strategies for Monitoring and Controlling BYOD Traffic .....	8
Device-Specific Applications.....	8
Impact of Web Browsing due to BYOD.....	9
Conclusion .....	12
About Technical Briefs .....	12

---

## List of Figures

PacketShaper on an Internet edge connection (T1 – 1.544Mbps) .....	3
Optimizing BYOD traffic within a partition setup .....	3
BYOD folder .....	5
Policy editor icon .....	5
Class Operations tab.....	6
Dashboard showing Internet traffic.....	7
Adding a class for the Android App Store .....	8
BYOD applications .....	9
URL categorization.....	10
Enable Traffic Discovery.....	10
Top 10 URL categories .....	11
HTTP settings to identify usage .....	11

---

## Introduction

Employee-owned mobility devices, such as smart phones and tablets, are quickly infiltrating the workplace. As such, Enterprises must develop mobile policies that secure the use of these devices within their corporate networks.

Bring Your Own Device, or BYOD, refers to a variety of devices that also includes personal laptops, but discussion of all mobility devices goes beyond the scope of this technical brief. This technical brief will focus on the following:

- ❑ Popularity of smart phones and tablets since 2009
- ❑ Apple iPhones and iPads since 2009

### *Growth of BYOD (Smart phones and Tablets) Devices from 2009 to Present*

The BYOD movement has been primarily driven by Apple iOS (iPhone & iPad) and Google Android OS-based devices. Other smart phone vendors using proprietary operating systems (for example, RIM and Nokia) have entered the marketplace; however, their products have suffered significant market losses and are currently non-factors in driving BYOD adoption or habits.

### *Apple BYOD (iPhones and iPads) from 2009 to mid-2012*

Since 2009, Apple has shipped 274 million iPhones and 116.67 million iPads. (See [Table 1–1](#).) This accounts for more than 390 million active BYOD devices worldwide from Apple alone. (Statistics are from Apple quarterly earnings reports that are available from the Apple Web site at (<http://www.apple.com>)).

---

**Note:** The totals shown in [Table 1–1](#) and [Table 1–2](#) do *not* include the 154+ million iPods that have shipped since 2009. The iPod Touch, which is based on the same platform as the iPhone, is part of the BYOD, but Apple does not break down unit counts for devices from the other iPods.

---

Table 1–1 Apple BYOD device sales<sup>1</sup>

Device type	2009	2010	2011	2012 (first half)	Cumulative 3.5 years total
iPhone	47.49	72.3	93.1	61.1	273.99
iPad	14.79	32.39	40.49	29	116.67

1. Android BYOD (smart phones and tablets) from 2009 to 2012 (Shipments and market prediction – Gartner/IDC)

The Android Mobile OS from Google drives smart phones and tablets from a number of different vendors. According to Gartner and IDC shipments and market predictions, Google Android sales totaled 635 million BYOD devices between the years 2009 and 2012, as shown in [Table 1–2](#).

Table 1–2 Smart phones and Tablet sales

Device type	2009	2010	2011	2012 (projected)	Cumulative 4 years total
Smart phone <sup>2</sup>	6.8	67.2	179.9	310	557.10
Tablet <sup>3</sup>	N/A	4.6	26.4	46.9	77.9

2. Gartner 2011 Android Smart phones Market Analysis

3. IDC 2010-2015 Tablet Market Analysis

If you combine cumulative Apple and Android BYOD device sales since the beginning of 2009, the total is 1.025 billion devices.

## Impact of BYOD Recreational Traffic on Unmanaged Networks

Three primary activities performed by BYODs can potentially create uncontrolled network traffic that can impact business applications and user productivity. These activities are:

- ❑ Automatic software updates/upgrades direct from the vendor, such as iOS, iTunes, and applications
- ❑ Universal access and ease of downloading recreational and business applications
- ❑ Uploading/downloading video content to/from recreational Web sites, such as Facebook, YouTube, and Flickr

Figure 1–1 shows the impact of a simple download of a game (Ragdoll Blaster 2) from the Apple App Store. As you can see, if a PacketShaper is either not configured at all, or configured incorrectly, downloading this application completely takes over a T1 connection until the application has been downloaded. BYOD activities such as this impact business-critical applications if left uncontrolled.

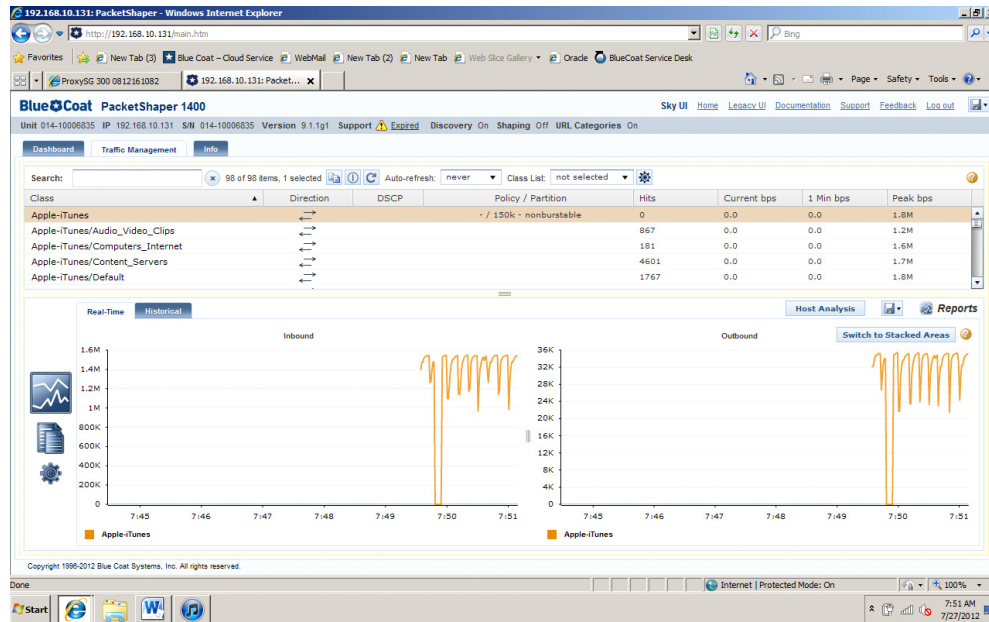


Figure 1-1 PacketShaper on an Internet edge connection (T1 – 1.544Mbps)

## Best Practices

Given the popularity of BYOD devices on a worldwide basis, the ability to completely block access to Web sites and Mobile applications would prove to be unpopular—and quite possibly impossible—given the preponderance of BYOD devices. The best approach is to set up a reasonable partition (lowest priority) for BYOD traffic (for example, iTunes, iCloud, Google Play, Flickr, and so on) that allows user activity but does not impact business-critical applications.

To optimize BYOD traffic within the partition setup for BYOD activities, MACH5 should be configured for both object and byte caching (for example, HTTP, CIFS, and so on). The partition setup enables the MACH5 to optimize/accelerate compression, protocol optimization, and object/byte caching of various BYOD traffic from the Internet. (See [Figure 1-2](#).)

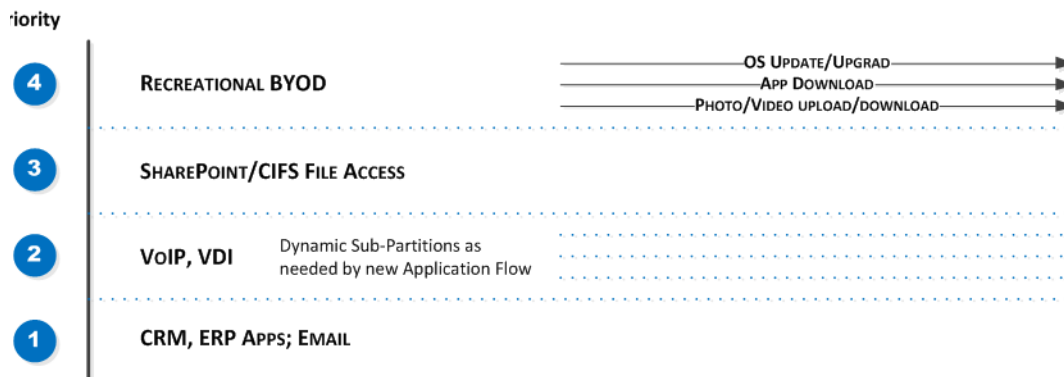


Figure 1-2 Optimizing BYOD traffic within a partition setup

---

## PacketShaper Tips and Tricks

The key to seeing and controlling recreational BYOD traffic is realizing that the content and context are constantly changing. Therefore you need to set up folders with global policies to group BYOD-based traffic together for visibility and control (policy-based partitions). BYOD-based recreational traffic can and should be segmented from business-oriented application traffic. The basic steps for mitigating the impact of recreational BYOD traffic on your network are listed below:

1. Identify all of the BYOD recreational traffic.
2. Set up a folder to group the BYOD recreational traffic.
3. Apply a policy (partition) to the folder that is compliant with company policy.
4. Verify the policy is working as expected.

### *1. Identification / Classification*

In version 8.6, PacketShaper added the ability to classify and categorize Internet HTTP/SSL traffic in a much more complete way, classifying 10's of millions of Web sites into 84 categories, and leveraging Blue Coat's WebPulse application and content intelligence. As a result, PacketShaper can get continuous access to new content classifications without the need for plugins or firmware updates.

Because the BYOD recreational traffic varies across the world, traffic spans many different classifications and content categories. Apple-iTunes can be further classified into the appropriate category. For example:

- ❑ Apple-iTunes/Audio/Video clips
- ❑ Apple-iTunes/Computers/Internet
- ❑ Apple-iTunes/Content servers

### *2. PacketShaper Classification / Subclassification of BYOD Traffic*

With the release of PacketShaper 9.1.x, new plugins are specifically designed to help classify and subclassify various traffic flows associated with BYOD devices. The plugins listed below are readily available to customers with current maintenance/support controls and can be found at: <https://bto.bluecoat.com/download/>.

- ❑ Apple Product Updates
- ❑ Google Services
- ❑ Jabber IM (Googletalk)
- ❑ Spotify Music Sharing Service
- ❑ Apple iCloud Service
- ❑ Netflix Video Streaming Service

For help with installing plugins into PacketShaper, please visit: <https://hypersonic.bluecoat.com/packetguide/current/nav/tasks/configure/download-plugins.htm>.



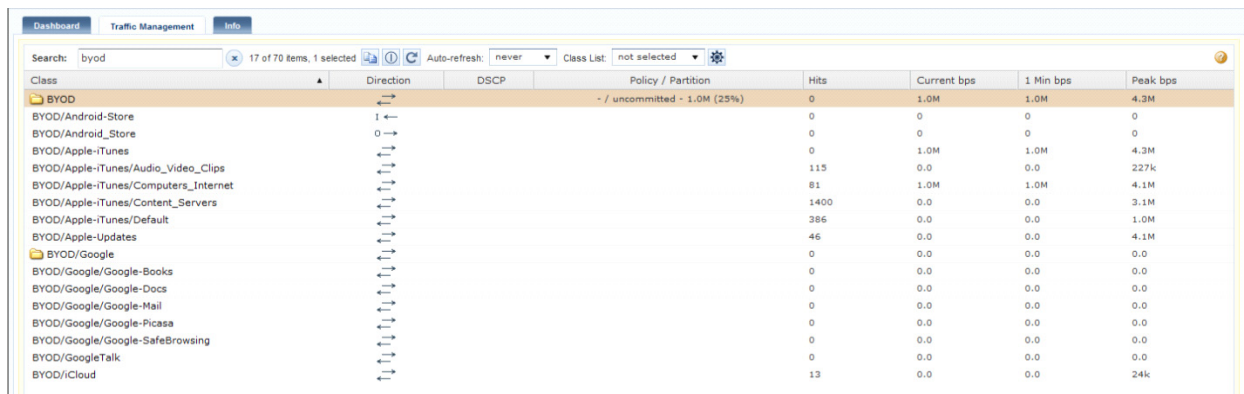
In addition to the new plugins, other strategies to help you control BYOD traffic are discussed in "[Appendix A – Strategies for Monitoring and Controlling BYOD Traffic](#)" on page 8.

### 3. Control / QoS Policies

Creating and consolidating recreational BYOD into a single folder enables you to apply a single policy for BYOD. Creating such a policy involves:

1. Creating a folder to use later as a partition
2. Moving the relevant BYOD classes into that partition folder

[Figure 1–3](#) shows a sample BYOD folder.



Class	Direction	DSCP	Policy / Partition	Hits	Current bps	1 Min bps	Peak bps
BYOD			- / uncommitted - 1.0M (25%)	0	1.0M	1.0M	4.3M
BYOD/Android-Store	1 ←			0	0	0	0
BYOD/Android_Store	0 →			0	0	0	0
BYOD/Apple-iTunes				0	1.0M	1.0M	4.3M
BYOD/Apple-iTunes/Audio_Video_Clips				115	0.0	0.0	227k
BYOD/Apple-iTunes/Computers_Internet				81	1.0M	1.0M	4.1M
BYOD/Apple-iTunes/Content_Servers				1400	0.0	0.0	3.1M
BYOD/Apple-iTunes/Default				386	0.0	0.0	1.0M
BYOD/Apple-Updates				46	0.0	0.0	4.1M
BYOD/Google				0	0.0	0.0	0.0
BYOD/Google/Google-Books				0	0.0	0.0	0.0
BYOD/Google/Google-Docs				0	0.0	0.0	0.0
BYOD/Google/Google-Mail				0	0.0	0.0	0.0
BYOD/Google/Google-Picasa				0	0.0	0.0	0.0
BYOD/Google/Google-SafeBrowsing				0	0.0	0.0	0.0
BYOD/GoogleTalk				0	0.0	0.0	0.0
BYOD/Cloud				13	0.0	0.0	24k


Figure 1–3 BYOD folder

After you set up the folder, set up and apply a policy (partition) to the folder to mitigate impact. To initiate policy set up for the new BYOD folder, simply select the policy editor icon, which is shown in [Figure 1–4](#).



Figure 1–4 Policy editor icon

Navigate to the **Class Operations** tab to set policy for the BYOD folder. (See [Figure 1–5](#).)



Class Operations
VoIP Optimization
Operations Log

Add Class
Add Folder
Delete Class
Modify Class
Host List Editor
Control Traffic

BYOD Folder

Policy Type: No Policy

DSCP No DSCP Assign Name

Partition Min: uncommitted ☒ Burstable Max: 1.0M

Apply Revert

Figure 1–5 Class Operations tab

Policy (partition) can be based on one of the following:

- ❑ Percentage of network bandwidth (for example, 10% of 20 Mbps Internet connection)
- ❑ Kbps/Mbps (for example, 250 Kbps of T1 connection)

After you have edited the policy, you must commit your changes. To do this, simply click **Apply**.

#### 4. Verify / Review

After policies have been created to mitigate BYOD traffic, verify that the policy is working as expected. Continual review of the policy is needed to maintain content/context evolution of the Internet traffic. (See [Figure 1–6](#).)

To learn more about monitoring using the PacketShaper, refer to the following:

<https://bto.bluecoat.com/packetguide/9.1/solutions/solutions-analysis-monitoring.htm>

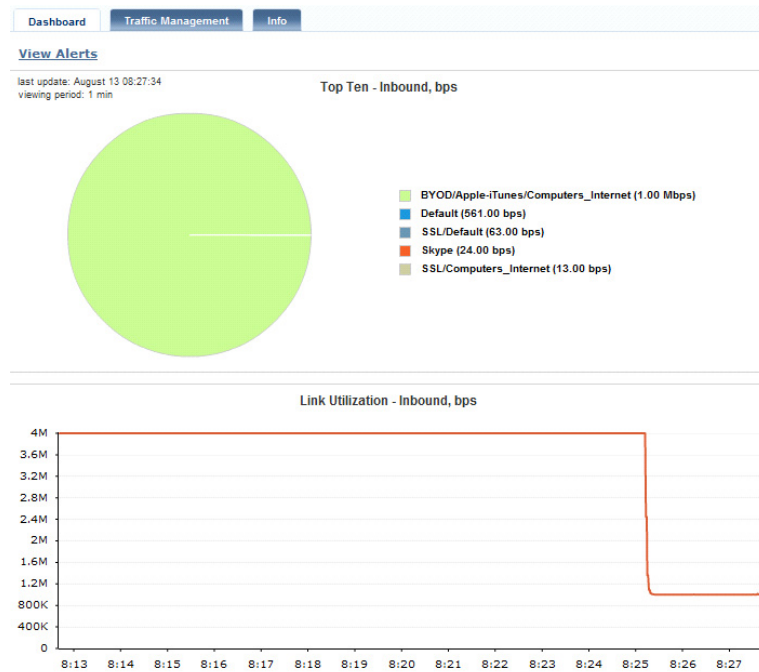


Figure 1-6 Dashboard showing Internet traffic

## Appendix A – Strategies for Monitoring and Controlling BYOD Traffic

### *Device-Specific Applications*

It is highly recommended that you install all plugins related to BYOD, which include:

- ❑ Apple Product Updates
- ❑ Google Services
- ❑ Jabber IM (Googletalk)
- ❑ Spotify Music Sharing Service
- ❑ Apple iCloud Service
- ❑ Netflix Video Streaming Service

You might need to classify the Android App Store if your BYOD users are able to access it. To classify the App Store, perform the following procedure.

#### **Procedure:**

1. From the Legacy user interface, click the **Class Operations** tab, then click **Add Class**.
2. Add a class to the BYOD folder (Android-Store) and select Ports.

The Android App Store uses port 5228.

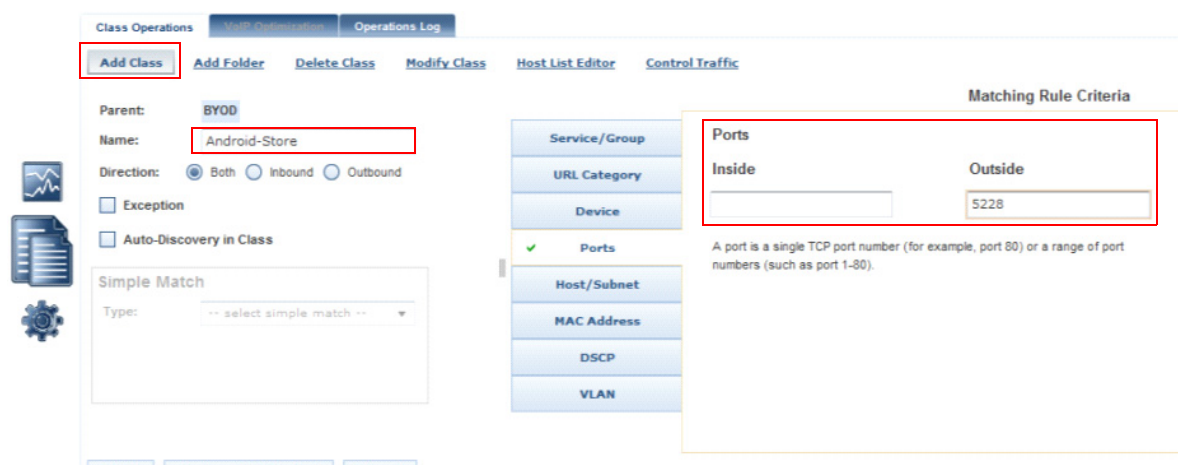


Figure 1–7 Adding a class for the Android App Store

3. Click **Apply**.

This enables visibility of BYOD applications. (See [Figure 1–8](#).)

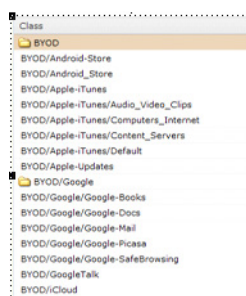
Android store (Classified by port number)	
Apple iTunes (Standard service) Traffic Discovery can be enabled.	
Apple updates (Plugins)	
Google Apps (Plugins) Traffic Discovery can be enabled.	
Google Talk (Standard service - Jabber)	
iCloud (Plugin)	

Figure 1–8 BYOD applications

## Impact of Web Browsing due to BYOD

In addition to the device-specific functions, administrators should be aware that the BYOD devices will also be accessing a rich variety of content on the Internet. Therefore, the same vigilance used for corporate devices regarding the type of traffic allowed should apply to the BYOD devices. In fact, users are more likely to use recreational applications on their own devices due to the perception that they are not being monitored.

As a result, increased media streaming and recreational browsing might result due to the fast speeds that corporate networks can provide when downloading content to the mobile devices. Mobile devices can also use known services to perform functions. Android can use Dropbox to back up documents. Spotify and Netflix are also common.

Should you share your corporate Internet connection with your BYOD users, Blue Coat recommends that you create a class for the BYOD network on the PacketShaper and monitor not just the impact of known BYOD services, but also URL categories and other Web applications within the BYOD usage. The BYOD class can be created by subnet or VLAN, depending on your network topology. Enabling discovery within this BYOD class allows you to not only monitor the Web applications usage, but also the Web categories that are being browsed by the BYOD users.

To generate these statistics, complete the following procedure.

### Procedure:

1. From the Legacy user interface, click the **Setup** tab. (See [Figure 1–9](#).)
2. Select **basic** from the drop-down list as the **Setup Page**.
3. Enable **Traffic Discovery** by selecting **on** from the drop-down list.
4. Enable **URL Categories** by selecting **on** from the drop-down list.

The screenshot shows the 'Setup' tab in the PacketShaper interface. Under the 'basic settings' sub-tab, there are buttons for 'apply changes ...' and 'reset form'. The 'Choose Setup Page' dropdown is set to 'basic'. Below this, four settings are listed with dropdown menus: 'Shaping' (off), 'Traffic Discovery' (on), 'URL Categories' (on), and 'Adaptive Response' (off). A link 'Go to URL Categories Setup' is visible next to the 'URL Categories' dropdown.

Figure 1–9 URL categorization

5. Enable Traffic Discovery for those protocols that you want to see content categorization (for example, HTTP, SSL, Apple-iTunes). (See [Figure 1–10](#).)

The screenshot shows the 'attributes' sub-tab for 'Web service (Hyper-Text Transport Protocol)'. It includes an 'apply changes ...' button. The settings are: 'Name' (HTTP), 'Parent' (/Inbound), 'Type' (radio buttons for Exception and Standard, with Standard selected), 'AutoDiscovered' (Yes), 'Host Analysis' (checkboxes for Top Talkers and Top Listeners, both unchecked), 'Traffic Discovery within Class' (checkbox for Enabled, which is checked), 'Comment' (empty text box), and 'Owner' (empty text box).

Figure 1–10 Enable Traffic Discovery

The PacketShaper will also need connectivity to the Internet, reachable DNS servers configured, and a valid support contract.

Normal browsing that can be increased by mobile devices include, but are not limited to, the following:

Audio/Video clips	News media
Blogs/Personal pages	Online meetings
Business/Economy	Reference
Chat/Instant Messaging	Search engines portals
Computers/Internet	Shopping
Content servers	Social networking
Entertainment	Software downloads
Financial services	Sports/Recreation
Games	TV/Video streams

Using URL category classification on the PacketShaper enables administrators to monitor the URL category usage of users and manage any extra recreational traffic generated by BYOD mobile devices.

Reporting in the Legacy user interface is useful for tracking URL categories that users are downloading most frequently. A sample report is shown in [Figure 1–11](#).

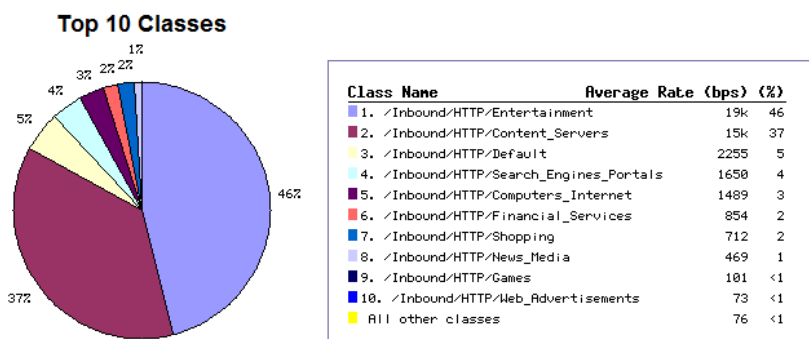


Figure 1–11 Top 10 URL categories

[Figure 1–11](#) shows the top 10 URL categories with a set time range defined. To generate this report, complete the following procedure.

**Procedure:**

1. From the Legacy user interface, select either the **Monitor** or **Manage** tab.
2. Select **HTTP**.
3. Click **Statistic** and **graph**
4. Set parameters as shown in [Figure 1–12](#).
5. Click **Apply**.

Include	Graph Type	Period	End date and time
1. <input checked="" type="checkbox"/>	Top 10 Classes	1 week	(now) (now) (now)
2. <input type="checkbox"/>	Network Efficiency	1 week	(now) (now) (now)
3. <input type="checkbox"/>	Link Utilization with Peaks	1 week	(now) (now) (now)
4. <input type="checkbox"/>	(none)	1 week	(now) (now) (now)

Figure 1–12 HTTP settings to identify usage

Using the information gathered from the URL classification and the reports that identify HTTP/SSL usage allows administrators to set appropriate controls for deterring pest/recreational browsing that impedes upon business-critical Web usage, thus mitigating the risks from introducing BYOD mobile devices onto the network.

---

## Conclusion

The Bring Your Own Device initiative introduces a challenging phenomenon for network administrators. Smart phones and tablets will increase recreational traffic on a corporate network while still being used for business purposes. Only the PacketShaper can analyze the impact of BYODs on your corporate network and control the additional recreational traffic, while at the same time, protecting the business-critical traffic important to an enterprise.

## About Technical Briefs

Technical briefs are designed to illustrate the features and capabilities of Blue Coat products. By describing generic solutions, technical briefs provide a foundation that Blue Coat customers can use to understand how Blue Coat products can be used to solve specific problems.

These technical briefs are not intended to solve customer-specific requests; if you need a customized solution to address a specific concern, contact Blue Coat Professional Services at [professional-services@bluecoat.com](mailto:professional-services@bluecoat.com).