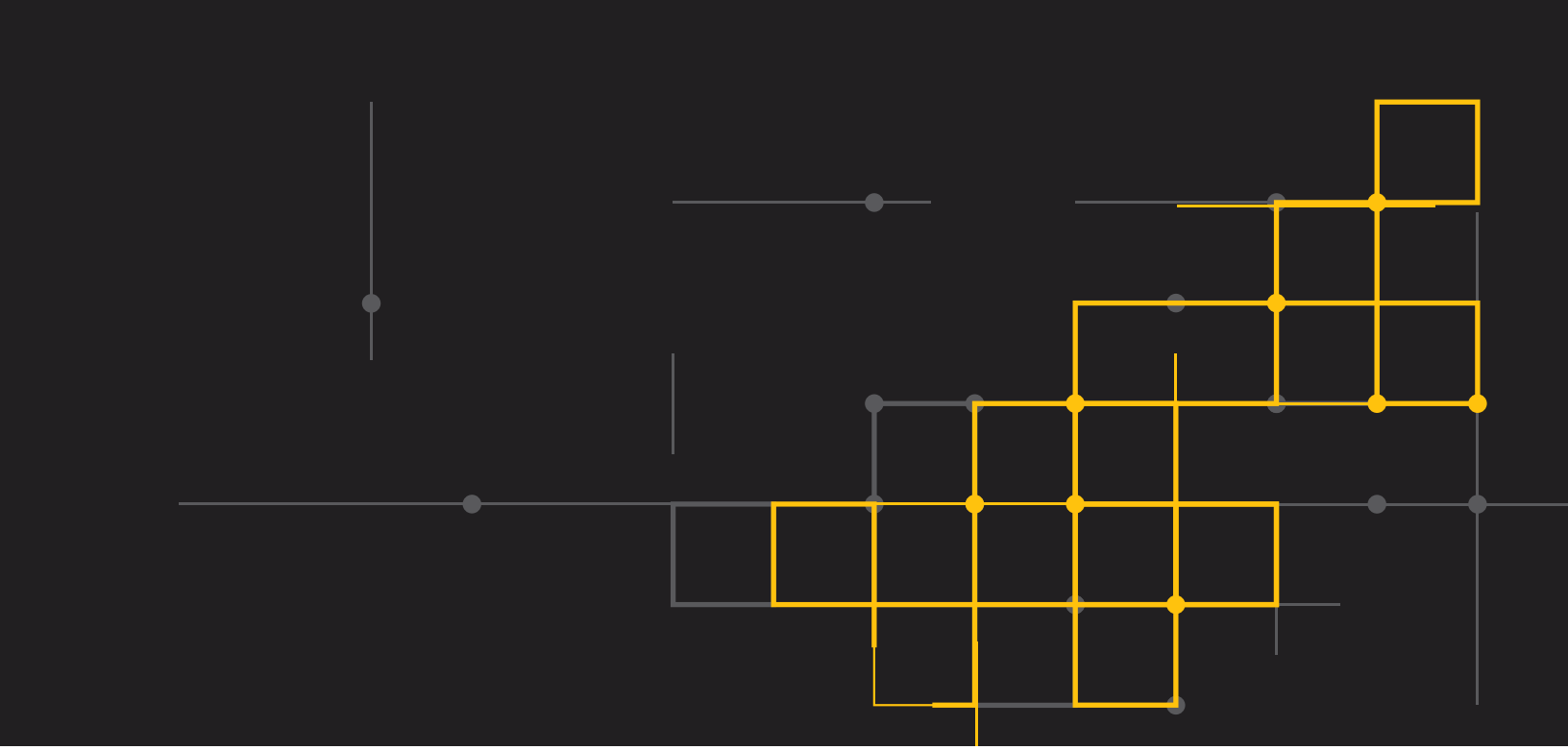


Boosting Internet Access Link Performance with Symantec WAN Optimization Technologies

Symantec

Executive Summary

Gateways to Internet traffic are facing unprecedented loads and growth rates in all types of industries and organizations due to the growth of mobile traffic carried by internal networks, growth in software-as-a-service (SaaS) in all kinds of fields, and through external events like product changes that organizations cannot control.

Symantec provides the tools you need to build a safe and cost-effective gateway to the Internet. With these powerful tools, you'll be able optimize the performance of your Internet access link by:

- Gaining clear visibility to the web and application traffic running in your network
- Exercising granular control by classifying and prioritizing traffic so that business-critical applications can be prioritized while recreational traffic is contained
- Accelerating web, video and cloud application performance with advanced caching technologies
- Redirecting recreational traffic directly to the Internet to save bandwidth and WAN connection cost

Overall, combinations of Symantec products placed at the Internet gateway on any production network can change the Internet experience for all involved. This paper will show you specific configuration options for Symantec products that enable this to happen.

The Constant Growth of Internet Traffic

Overall, Internet traffic growth is phenomenal. This is true across all types of usages and applications:

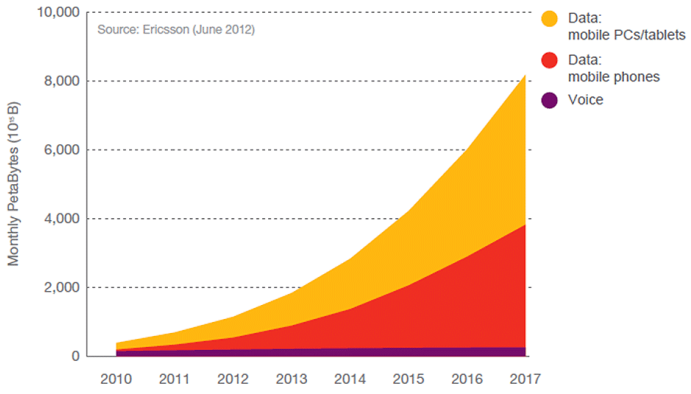
Internet bandwidth usage is driven in large part by the popularity of social networking and relaxed corporate policies about recreational use in the work place. For example, Facebook has seen an average 11.2 percent quarterly user-base growth from Q1 of 2011 to Q1 of 2012[1], and YouTube has seen video uploads increase by more than 100 percent in the period between May 2011 and May 2013[2]. This situation is further exacerbated by consumerization of the enterprise with BYOD devices. Recreational traffic can consume 30 to 90 percent of the WAN or Internet capacity of every branch site.

Netflix experienced a tenfold increase in traffic over the three months starting in October 2012, when their new mobile application was introduced. While their business is content delivery, this shows how external events can have a very dramatic impact on Internet bandwidth demand. Similarly, the iPhone 5 upgrade overloaded many corporate wireless networks.

Internet sensor and control technology is another high-growth area. Even non-IT-intensive industries like farming and ranching are experiencing 5 to10 percent productivity improvements by using Internet-based remote sensing and reporting. As new sensor and connectivity technologies are developed, demand for external connectivity can experience sudden growth. Sometimes these robotic, reporting, or video applications are not known to IT until they are brought on line.

Mobile Traffic Growth

Much of the growth in Internet traffic for all types of organizations, in both the public and private sectors, is due to growth in mobile traffic. Here's a chart that shows how dramatic this effect is.



(Kinsella, 2012)

This traffic can create unique problems for organizations because it often originates from user-owned devices that may or may not show up on the network on a regular basis.

SaaS and Cloud Growth

On top of all these developments, traffic from all organizations today contains many more types of applications than it used to. And SaaS is growing at 50 percent per year[3]. For example:

- CRM applications are rapidly being replaced by online sales applications.

[1] Facebook Usage and Facebook Growth Statistics by Internet World Stats
[2] KPCB Internet Trends 2013
[3] CloudReviews March 5, 2013

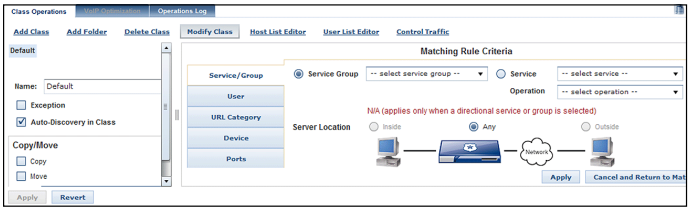
- Groups inside organizations are using outside resources as an expedient way to collaborate on design documents or proposals.
- Forrester believes the highest growth occurs in applications inside other SaaS applications such as CRM and ERP (Forrester, 2013)

Congestion and Peak traffic

Peak-usage Internet traffic is growing more rapidly than average Internet traffic. Cisco reports that busy-hour Internet traffic increased 41 percent in 2012 compared to 34 percent for average traffic. They also predict that busy-hour Internet traffic will increase by a factor of 3.5 times between 2012 and 2017, while average Internet traffic will increase 2.9-fold. This means that bandwidth and congestion control will become increasingly important for all types of organizations. Problems in congestion will show up when users need rapid and effective Internet access the most.[4]

Visibility into New Network Applications

Key to understanding how traffic is growing is visibility into network traffic. Symantec PacketShaper provides classification of close to 1,000 applications and tens of millions of URLs through the Symantec Global Intelligence Network service. This allows managers to quickly identify sources of new traffic. To allow classification of unknown traffic, the attribute box Auto-Discovery in Class is checked as shown below for the default group.



The default group is where unclassified traffic appears. When auto-classification is enabled, sub-classes are created for the traffic that PacketShaper can identify.

For example: if a heating and air-conditioning firm sets up remote management and sensing devices in a building, this traffic would likely show up as Oracle or SQL traffic, because the sensors from most HVAC vendors report to databases that can be queried. If the installers set up surveillance video, that bandwidth would be identified as one of the video protocols detected by PacketShaper.

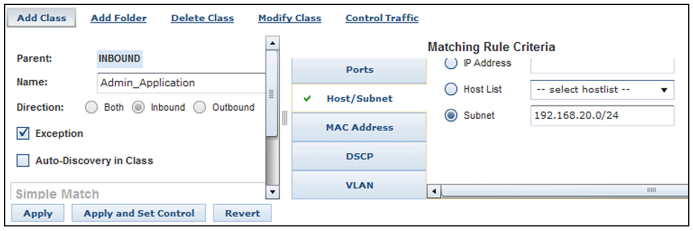
Traffic Classification and Prioritization Based on Business Needs

The main purpose of your network is to support your business goals and objectives. But your network must also operate with a complex internal and external ecosystem. You must balance and prioritize your limited resources to support and satisfy various applications and user needs. The QoS capabilities provided by PacketShaper, combined with its application and web traffic classification, will give you the ability to set up granular control policies that regulate the network resources available for applications and users. With the PacketShaper QoS tool, you can establish policies to:

1. Protect business-critical applications with high prioritization and bandwidth guarantee
2. Limit the impact of aggressive but non-business-essential applications such as print or FTP downloads
3. Enable but contain recreational and BYOD usage
4. Provide fair bandwidth allocation for all users

Bandwidth Guarantee of Critical Applications

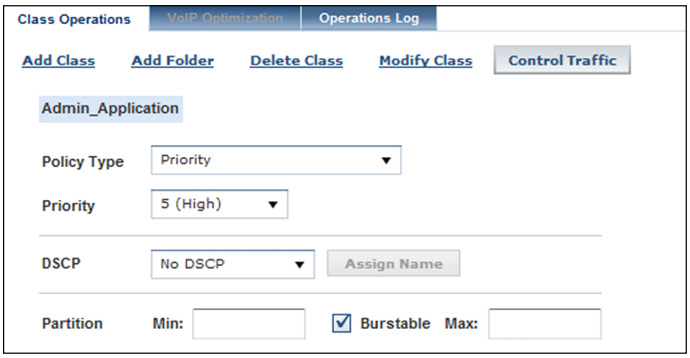
Important traffic, such as Management SaaS traffic, can be identified and put into a folder that is guaranteed bandwidth. With PacketShaper, a class can be created called “Administrative _Application”, which can be defined by a host list as shown below:



This administrative subnet contains the site that is connected to the administrative application. This allows users to login only to the application with no need to be authenticated or identified. They could also be identified by a host list or VLAN of the administrative network.

[4] Cisco Visual Networking Index: Forecast and Methodology, 2012-2017

This class is given priority over other applications as shown below:

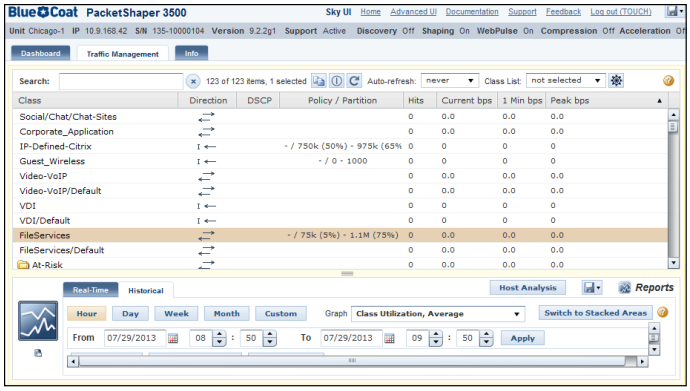


There is no reason to limit Admin_Application to a single class. For example, if applications like Salesforce.com or Google Educational Apps are used, it can also be protected by prioritizing a host list containing the sites used by the application.

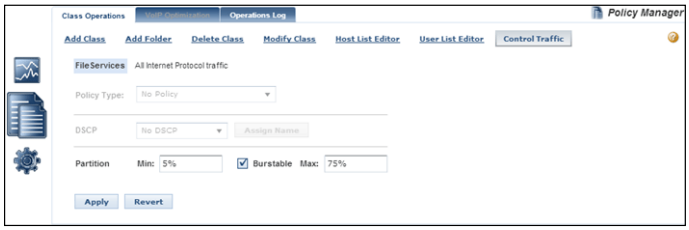
Minimize Impact of Aggressive Business Applications

Some business applications such as file backup and FTP downloading may require large bandwidth and are contentious in nature. But these types of applications are generally less sensitive to slight delays and low-grade performance lags. It is perfectly sensible and often preferable to categorize these traffics to a lower priority where they won't compete for network resources when business-critical or delay-sensitive applications are demanding bandwidth. Network QoS Policies can be used to minimize the potential network performance impact of these applications.

The screens below show the configuration steps for limiting the impact of SMS file updates. Here the idea is that a new update is scheduled in SMS. The PacketShaper contains a class called FileServices that contains all types of backup and file transfer protocols. Minimizing the impact of unexpected upgrade and backup traffic is as simple as limiting the bandwidth for this class. The Service is already defined, and if Auto-Discovery were turned on, it would already show up as a class.



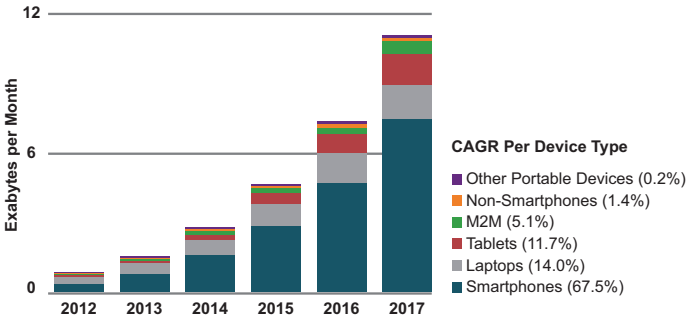
Click on Control Traffic and set up a partition where this class gets at least 5 percent of the bandwidth, but cannot get more than 75 percent of link bandwidth under any circumstances. Updates and backups can always occur, but can't completely consume the link.



Contain BYOD and Recreational Traffic; Ensure Fair Bandwidth Allocation

As much as 50 to 90 percent of branch-office network traffic is BYOD and recreational-related. A 5.9GB HD movie download and a 1.5Mbps YouTube video streaming can add up quickly to consume your available bandwidth and bring your business application traffic to a halt. A good deal of the Wi-Fi traffic on any network today is generated by employees and guests who bring their own equipment to the Wi-Fi site. This traffic comes from all types of devices as shown in the chart below.

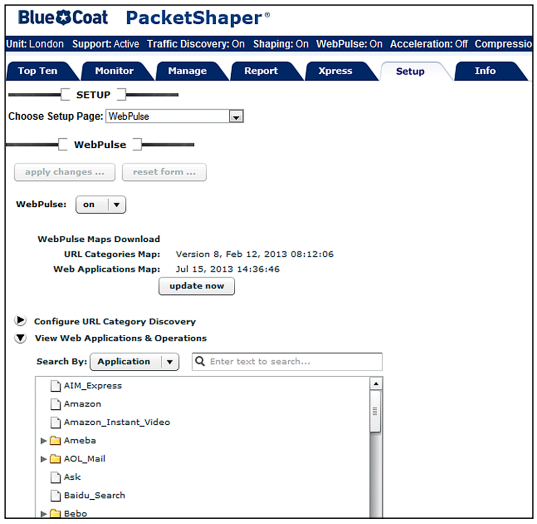
66% CAGR 2012 - 2017



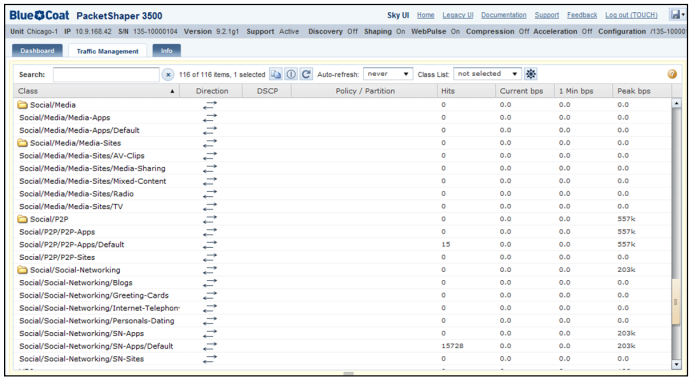
(Cisco)

PacketShaper can identify not only applications by network parameters or user groups, but it can also identify many layer 7 applications and classify websites by usage type. One of the easiest ways to identify recreational traffic is to use the Global Intelligence Network classification service.

The Global Intelligence Network service identifies tens of millions of websites and maintains an up-to-date listing of website classifications. To turn on Global Intelligence Network, you need a maintenance subscription. To enable it go to <Legacy Interface><Settings><Global Intelligence Network> as shown below:

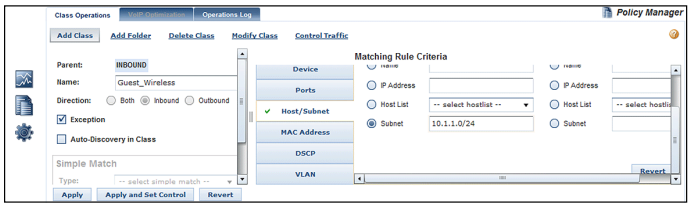


Turning on the service is as simple as clicking on the Global Intelligence Network On button shown above. You can limit the bandwidth of the applications and sites that are discovered the same way you would limit other applications. The screen below shows the depth to which social media traffic is classified; it can be throttled or even dropped based on these classifications.

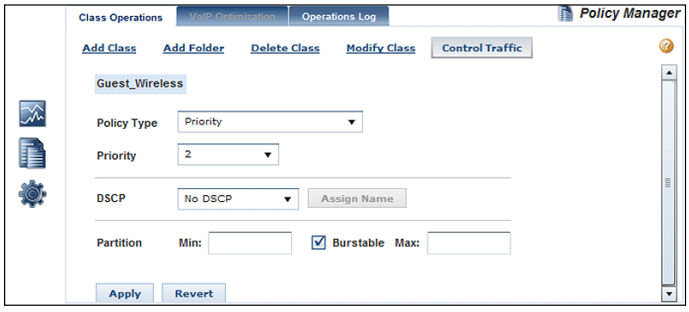


PacketShaper can be set up to identify traffic from cloud, mobile, and key applications to ensure that critical applications receive appropriate bandwidth allocations. Recreational traffic in the guest network can be classified at a low priority with low-priority bursting when unused bandwidth becomes available.

To control guest wireless traffic, or any other type of traffic identified by source, set up a class identifying the traffic on PacketShaper, as shown below. These screen shots show “Guest_ Wireless” being identified by its source on the wireless network, but it could be identified in other ways – say by a user group.

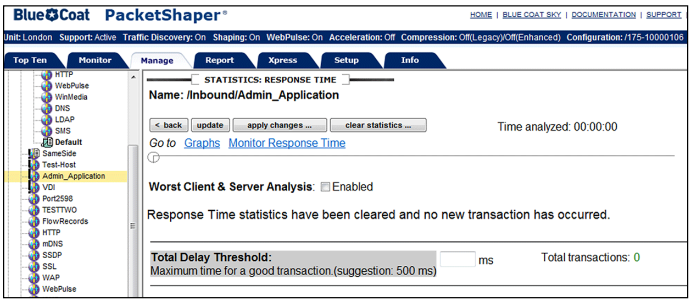


Add a policy for the class to limit its aggregate traffic by clicking on Control Traffic (note that Priority 2 is the second-lowest priority):



Application Monitoring

In all Symantec products, application status can be monitored. PacketShaper is no exception. In the legacy interface, click on our Admin_Application class and you will see a Response Time field as shown below:



Clicking on this entity brings up an Application Response Time screen that lets administrators set a threshold for the application, which enables alarms to be set. This allows an administrative application to be run in a monitored way on a congested network.

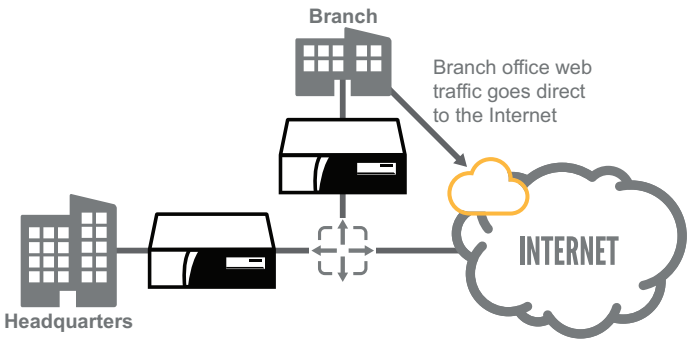
Acceleration Through Caching and Protocol Optimization

In some organizations, downloading materials needed for work and training is a major component of internet traffic. An excellent example is courseware and assignments for employees attending online training classes. The Blue Coat ProxySG MACH5 proxy can cache content to give users a favorable experience. They don't have to commit to waiting 5 or 10 minutes while the download takes place. In the Symantec scenario, the copy or application is fulfilled from the local cache on the MACH5 rather than the administrative server. This not only speeds up the download, but also keeps the load off the administrative server so it can serve low-demand content quickly. When it's obvious that some content is going to be needed by multiple users at the same time – say in the case of a training class – the MACH5 cache can be pre-loaded with the content.

The use of a proxy also makes these transfers secure. In the proxy environment, the types of services available to users can be controlled. For example, the only service afforded the special user download network might be the download service, with no uploads allowed.

Direct to Internet

While this paper has focused on applications and traffic to and from known servers, other traffic can be forwarded directly to the Internet in a safe fashion. This is shown in the network diagram below:



The MACH5 identifies and controls the traffic so that Internet traffic from the branch office is sent directly to the Internet and doesn't load down the organization's WAN bandwidth. This can lower the total cost of Internet-bound traffic and improve the performance of Internet applications. It also means that surges in Internet usage don't affect inter-site communication.

Additional Resources:

5. Four Steps to High Performance WAN and Internet
6. How to Assure Performance of SaaS Applications and Content
7. Preparing for the Impact of Recreational Traffic

Please visit www.symantec.com.

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com