Executive Summary

Blue Coat ProxySG appliances utilizing MACH5 WAN Optimization allow IT organizations to accelerate and secure the delivery of business applications for all users across the distributed enterprise - including those near Internet gateways, as well as in branch offices, data centers, and even individual end points. As an integral part of the MACH5 WAN Optimization framework, QoS and Bandwidth Management ensure that the appropriate level of service is provided to specific users, groups, or types of network traffic.

What are QoS and Bandwidth Management?

Quality of Service (QoS) and Bandwidth Management are techniques used to prioritize network traffic. Blue Coat MACH5 supports the QoS prioritization technique used by network devices that works by setting Type of Service (ToS) bits in the IP header of packets. By preserving or manipulating ToS information and using Bandwidth Management classes, administrators can use specific triggers and actions to set priority and assign resources to different types of traffic flow.

Why should I perform QoS and Bandwidth Management in my network?

In a world where clients, servers, and data all come in different types, treating all network connections as a single traffic flow does not give administrators the flexibility to ensure that business-critical applications perform as required. Imagine finding out that the CEO could not access critical reports because an employee spent his lunch break watching streaming videos. Using QoS and Bandwidth Management, administrators can control network traffic flow so that the appropriate users, groups, or applications receive the proper network resources.

How do QoS and Bandwidth Management work?

QoS and Bandwidth Management are separate MACH5 features that can be individually implemented to meet specific needs, or used together for added flexibility. Implementing QoS requires that the current network infrastructure support ToS bit prioritization of network traffic. If it does, the MACH5 QoS feature is able to manipulate ToS bits to dictate how the traffic is treated on the network. Bandwidth Management provides a similar function for traffic coming into or out of the appliance; administrators prioritize traffic by assigning bandwidth classes that guarantee minimum or maximum bandwidth based on applications, users, sources, destinations, or content. When used in conjunction with Bandwidth Management, external ToS values can dictate which bandwidth management class applies to a particular transaction, allowing the appliance to interoperate with other QoS-enabled networking equipment.

QoS

QoS is a prioritization technique (used by network devices) that works by setting ToS bits in the IP header of packets. The ToS values are then used to make decisions regarding traffic flow throughout the network. The value of the ToS bits is known as the Differentiated Services Code Point (DSCP) value and is represented in an eight bit field; six bits are used and two are reserved. The DSCP value typically reflects a standard set of values that range from 0 to 63 and includes conceptual classes for easier implementation. Similar to many network devices, ProxySG appliances have the ability to set DSCP values and make decisions based on existing DSCP values, if desired. In addition, ProxySG appliances are able to use policy to manipulate existing values
- preserving them, echoing them, or re-prioritizing them to new values. These decisions can be based on a number of different criteria including user, group, protocol, subnet, and more. This ability to change DSCP values based on user and application level policies provides a level of control not possible on other devices that are only Layer 3 and 4 aware.

**QoS Example**

A network administrator would like to ensure that the company CEO is guaranteed the highest level of service on the network; all other executives receive a higher priority of service than the rest of the company’s employees. The administrator would also like to ensure that Citrix ICA traffic is always given a higher priority than HTTP, for the general employee population. If the administrator has a ProxySG appliance in the network that is performing authentication and authorization, he can configure policy to identify connections made by the CEO and executives and set an appropriate DSCP value for those connections. He can also configure policy to set different DSCP values for the HTTP and Citrix ICA protocols.

![QoS Diagram](https://via.placeholder.com/150)

**Bandwidth Management**

Bandwidth Management relies on user-defined bandwidth classes and policy rules to manage the available bandwidth coming into or out of the ProxySG appliance. There are four characteristics of bandwidth classes - minimum bandwidth, maximum bandwidth, priority, and parent designation (used to configure class hierarchies). Minimum bandwidth works by guaranteeing a predefined amount of bandwidth (if available on the network) to the class. Similarly, maximum bandwidth limits the amount of bandwidth that a particular class may use. Classes can also be prioritized so that certain traffic receives bandwidth before others. To implement minimums or prioritization, a class hierarchy must be created with a maximum bandwidth allocation. This allows the appliance to determine how much bandwidth is “too much” for a low or medium priority bandwidth class. Creating class hierarchies provides the most flexibility for Bandwidth Management. Class hierarchies allow administrators to apply classes at a granular level, taking various criteria into consideration to determine the final bandwidth allocation allowed. To determine which class to assign to a particular connection, the ProxySG appliance evaluates the configured policy to determine if any of the connection attributes match the policy rules assigned to bandwidth classes. Blue Coat Policy has a rich set of triggers that can be evaluated to classify traffic flows – this comprehensive set of triggers include, but is not limited to, user, group, destination, protocol, subnet, content-filter category, or DSCP value. By creating classes and assigning specific types of traffic to them, you can effectively control how the available bandwidth is used.
Bandwidth Management Example

An administrator managing a branch office wants to ensure that no more than half of the total bandwidth available is used for HTTP or FTP traffic to guarantee that other business-critical applications continue to function. However, when the CEO visits this branch office, she should have priority over other employees when using this allocated bandwidth. To accomplish this, the administrator:

- Creates a bandwidth class Branch Office and configures the maximum bandwidth to an amount equal to half of the total available bandwidth.
- Creates a policy rule for the Branch Office class, assigning all HTTP and FTP traffic to this bandwidth class.
- Creates two additional bandwidth classes Employees and CEO and sets the appropriate priorities.
- Creates policy rules identifying the CEO and "everyone else"; these rules assign such traffic to either the Employees or CEO bandwidth class.
- Makes the Branch Office class the parent class of both the Employees and CEO classes.

The administrator now has a bandwidth hierarchy. Bandwidth is limited by the configuration of the parent class, and the two child classes are prioritized to determine how they share any unused bandwidth. Because no minimums have been set, the highest priority class has the first opportunity to use all of the available bandwidth; whatever is left then goes to the next priority class.

The Blue Coat Difference

Flexible, User-Based Bandwidth Control

Blue Coat policy enables administrators to make QoS and Bandwidth Management decisions based on a number of application-level factors including user login or group membership. This allows administrators to create policy assigning different levels of bandwidth to specific users or groups, for example. This breadth of control provides flexibility not available in other vendor products.

Content-Aware Bandwidth Management

In an enterprise, Bandwidth Management is often used to guarantee access to business-critical applications or Web sites. For other, more obscure traffic on the network, Bandwidth Management can be used in conjunction with content-filtering to make bandwidth management decisions based on the type of sites being accessed.