SOLARWINDS TECH TIPS

Quality of Service (QoS) for Enterprise Networks

Learn How to Configure QoS on Cisco® Routers

Share:

solarwinds
Unexpected Simplicity™

Quality of Service (QoS) Overview

Networks today are required to deliver secure, measurable and guaranteed services. For example, delay-sensitive applications like high-definition video and VoIP demand bandwidth-focused network capabilities and resources rely on the aforementioned to perform at an optimal level.

Quality of Service (QoS) is the ability of a network to provide improved services to business critical applications over other traffic. Enabling QoS in your network aids in providing better and more predictable network service by:

- Supporting dedicated bandwidth for each application
- Setting traffic priorities across the network
- Improving packet loss situations
- Avoiding and managing network congestion
- Shaping network traffic

QoS is determined by factors, such as throughput, bandwidth, latency, packet loss, error rate, jitter and so on. For the network administrator, QoS helps manage call-drops & static (voice), high-definition video, (video streaming) and rapid response time (data). In short, QoS aids in maximizing and optimizing network bandwidth utilization while meeting performance expectations.

QoS Mechanisms for Traffic Control

There are various QoS mechanisms that can be utilized to provide priority to business traffic and drop or shape less critical applications. The mechanism or combination of mechanisms chosen in an enterprise depends on the requirements of the network – for example, business critical applications and delay sensitive apps like VoIP and unified communications must be a high priority and even require assured bandwidth. Less important business applications or other network traffic, depending on their IP header values, may have to be remarked for best effort performance, instead of priority performance and finally, scavenger class traffic may have to be dropped.

Listed below are some major elements or features of QoS that can be used to manage traffic based on network requirements:

Classification and Marking: This feature identifies and classifies traffic packets that are to be treated differently. It allows you to partition network traffic into multiple priority levels or classes based on policies specified by the network operator. Policies can be set to include classification based on application port, IP protocol type, physical port, source or destination IP or MAC address, and other criteria specified by access lists.

Marking refers to tagging identified traffic groups so they can be recognized within the network. In the entire network, based on priority assigned, the particular tagged group will be provided with the allocated bandwidth.

Policing and Shaping: Policing determines if packets are conforming to defined traffic values, and then takes appropriate actions like marking, remarking or dropping a packet. In contrast to policing, traffic shaping retains excess packets in a queue and then schedules these excess packets for transmission depending on factors, such as available bandwidth or delay requirements of the receiving interface. The result of traffic shaping is a smoothed packet output rate.

Scheduling (Queuing & Dropping): Set up queuing techniques on a device interface to manage how packets are to be queued and sent through that interface. Some queuing techniques use the packet marking, while others ignore them. Queuing techniques are primarily used for managing traffic congestion on an interface. Meaning, they determine the priority on how to send packets when there's more data than can be sent at a particular time. Queuing algorithms are activated only when a device is experiencing congestion and are then deactivated when congestion clears.

There's a limit on the number of packets that the router can place onto each queue. This limit, referred to as the 'depth' can be specified as required. During cases of high traffic, a queue fills with packets waiting for transmission. When a queue reaches its limit and becomes full, the router by default drops packets until the queue is no longer full.

Configuration for QoS on a Cisco® Router

QoS configuration starts with identifying traffic that must be prioritized. This can be done using access lists, IP addresses, ports, MAC addresses, DSCP, (Differentiated Services Code Point) and so on. There are three steps to implementing a QoS policy in your network:

Step1: Create a traffic class

Step2: Define a policy for the class

Step3: Associate the policy to an interface

Creating a Traffic Class

After determining the traffic group that will be subjected to one of the QoS mechanisms we discussed earlier, create a traffic class and use match commands to bring the traffic group under that class.

```
router#enable
Password:*****
router#configure terminal
router2950(config)# access-list 101 permit tcp host 10.10.10.10 host 10.10.10.20 range
16384 20000
router2950(config)# access-list 102 permit tcp host 10.10.10.10 host 10.10.10.20 range
53000 56000

router2950(config)# class-map CRM
router2950(config-cmap)# match access-list 101
router2950(config-cmap)# exit
router2950(config-cmap)# class-map DataCenter
router2950(config-cmap)# match access-list 102
router2950(config-cmap)# exit
```

Grouping Traffic using ACL

Creating Traffic Class and associating the traffic group to the class

Mapping a Class to a Policy

In order to map a class to a policy, you must first create the class, then the policy. Next, the class and policy must be associated. Thereafter, the action being performed must be defined to the traffic group under each class. Some examples of characteristics are:

- Bandwidth - Traffic associated to this class has a guaranteed bandwidth
- Packet Weight - Packet drop does not happen if a weight is specified
- Queue Limit - Maximum number of packets that can be in the queue

```
router#enable
Password:*****
router#configure terminal
router2950(config)# policy-map GOLD
router2950(config-pmap)# class CRM
router2950(config-pmap-c)# bandwidth 3000
router2950(config-pmap-c)# queue-limit 30
router2950(config-pmap-c)# exit
router2950(config-pmap)# class DataCenter
router2950(config-pmap-c)# bandwidth 2000
router2950(config-pmap-c)# exit
router2950(config-cmap)# exit
```

Policy is created

Match class to assign marking

Specify characteristics for the class

Associate a Policy to an Interface

```
router#enable
Password:*****
router#configure terminal
router2950(config)# interface fa1/0/0
router2950(config-if)# service output GOLD
router2950(config-if)# exit
```

Policy map is applied on the interface

After setting up QoS policing on the interface, the administrator must monitor and verify if the traffic from the business critical application is smoothly shaped.

QoS Deployment Principles

Implementing QoS enables you to control and limit the use of network bandwidth. Mission critical applications can be given priority over less important ones. Ensure that your bandwidth is being used efficiently and that adequate bandwidth is provisioned for delay-sensitive applications like VoIP and multimedia. Eliminate issues of traffic congestion and high link utilization.

Listed below are a few tips for deployment of QoS in your network:

- Understand and define business objectives to be achieved with QoS
- Determine the number of classes of traffic required to meet business objectives
- Assign as few applications as possible to be treated as 'mission critical'
- Analyze the service-level requirements of traffic classes that need to be provisioned
- Design and verify performance of QoS policies prior to rollout
- Monitor service levels to ensure that the QoS objectives are being met

QoS technologies allow you to meet service requirements by detecting changes in network conditions, such as congestion or availability of bandwidth, and prioritizing - or throttling - network traffic. A network monitoring system must typically be deployed as part of QoS. Doing so ensures that your network is performing at a desired level.

QoS Monitoring

QoS monitoring is essential to verify effectiveness of QoS policies applied to the network and validating the performance of your QoS policies. Provided below are some options you can leverage for QoS policy monitoring:

CBQoS Monitoring: Use an advanced monitoring tool that can query, "WRITE the name of the MIB," for pulling information on the class based QoS policies you have created. Querying the QoS MIB will provide information on the pre and post policy traffic statistics and queuing. In turn, you can validate the performance of your QoS policies and determine if the policies created are performing as expected.

NetFlow Based Monitoring: NetFlow data carries information on the ToS (Type of Service) field of traffic, allowing you to determine the DSCP values for each traffic conversation. Using a NetFlow

based report can determine if the right application or IP conversation has the correct priority assigned to it.

In short, QoS enables you to cost-effectively manage network traffic and enhance user experience in your enterprise environment.

SolarWinds® NetFlow Traffic Analyzer

With SolarWinds NetFlow Traffic Analyzer (NTA), you can view network traffic segmented by classes and ensure that critical and delay-sensitive traffic, such as voice or video is prioritized and isn't dropped. In addition, it provides by-the-minute data required to monitor the bandwidth of each critical QoS segments. Further, it measures the effectiveness of your QoS policies by analyzing traffic before and after application. NTA easily quantifies bandwidth consumption for your critical applications.

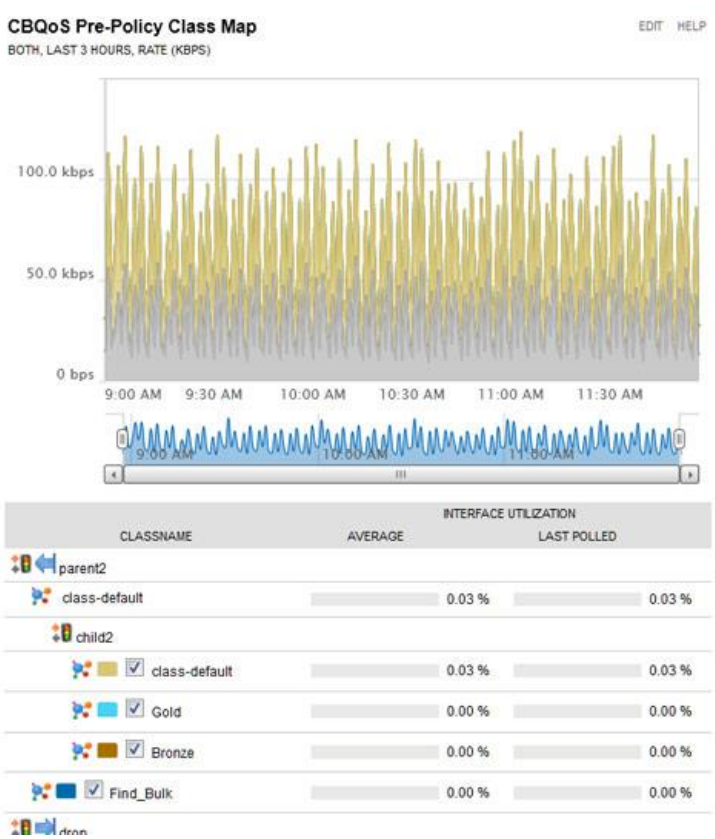
Some QoS reports that can be obtained from NTA are:

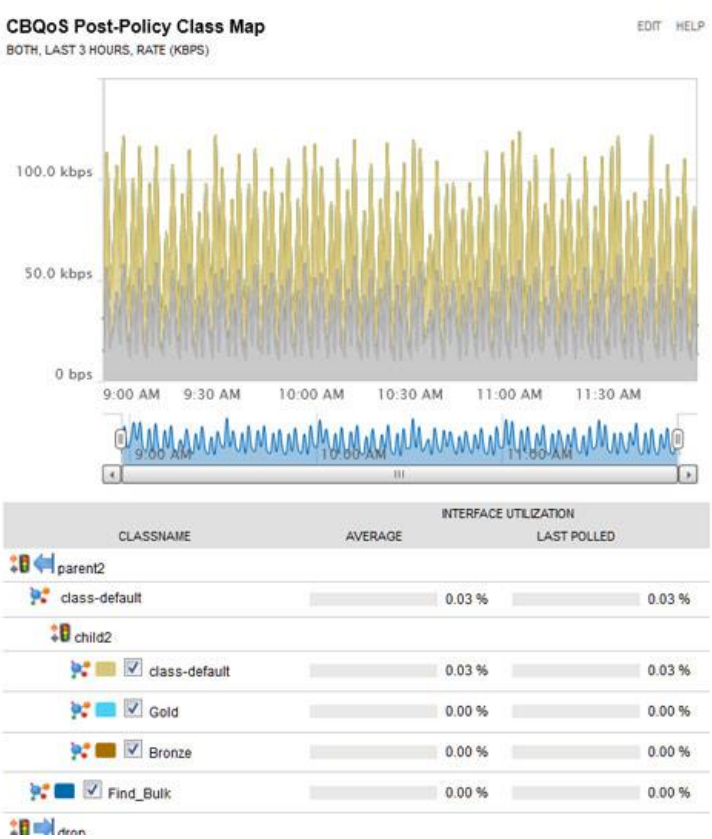
- Obtain details about QoS policies applied to an interface, including nested policies and direction
- Information on the amount of traffic before and after the effect of each QoS policy
- Pre and post policy statistics available for each class, as well as for nested policies
- Drop traffic details – Amount of traffic dropped on an interface per QoS policy, including each QoS class
- Validate the performance of your QoS policies

5 Reasons to Download NTA

- Obtain real-time analysis of peak traffic in the network
- Perform bandwidth sizing for new applications on the network
- Easily troubleshoot and understand network pain points like network choke or slowness
- Quickly detect unauthorized WAN traffic and network behavior anomalies
- View details to verify if QoS policies are met and need to be changed

By using SolarWinds NTA, you can view network traffic segmented by Class of Service methods, measure effectiveness of your CBQoS policies, and quantify bandwidth consumption by class map.





LEARN MORE » DOWNLOAD FREE TRIAL

References

Quality of Service Design Overview:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoSIntro.html#wp46092

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide. Focused exclusively on IT Pros, we strive to eliminate the complexity in IT management software that many have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, thwack, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more at http://www.solarwinds.com.

solarwinds
Unexpected Simplicity™