

IQrouter

Advanced game optimization

Most interactive online games use UDP packets to stream out information to servers/other users, so the action and information is as real-time as possible. Unlike TCP, UDP is 'send and forget', with no inherent retries or delivery guarantees. Suppose there is a drop due to something like line loss or, more commonly, congestion; then, too bad, so sad. But worse, if they are delayed, then gameplay is 'laggy'.

So, first, you want to eliminate bufferbloat, the primary source of delay, and your IQrouter is taking care of that. But now, you want to make sure your outbound UDP packets have priority over other **local** traffic, but game consoles do not mark this traffic as important, and it typically winds up in the Best Effort queue in the IQrouter.

The traffic manager generally does a good job of noticing that these frequent, small UDP packets are flowing and gives them precedence over large bulk flows (e.g. photos syncing to the cloud). Still, it would be nice to boost their priority so that they are assured a higher priority no matter what.

This guide is for advanced users only. We will be messing with the firewall rules, and if done wrong could impact anything from basic functions to potential security issues. If something does go wrong, then the fix is to [reset](#) the IQrouter back to factory settings and re-deploy it.

You will need to identify your console(s) by finding it in the list of DHCP leases shown in the Status-Advanced Overview and make a note of the IP and MAC so you can find it while following the steps below.

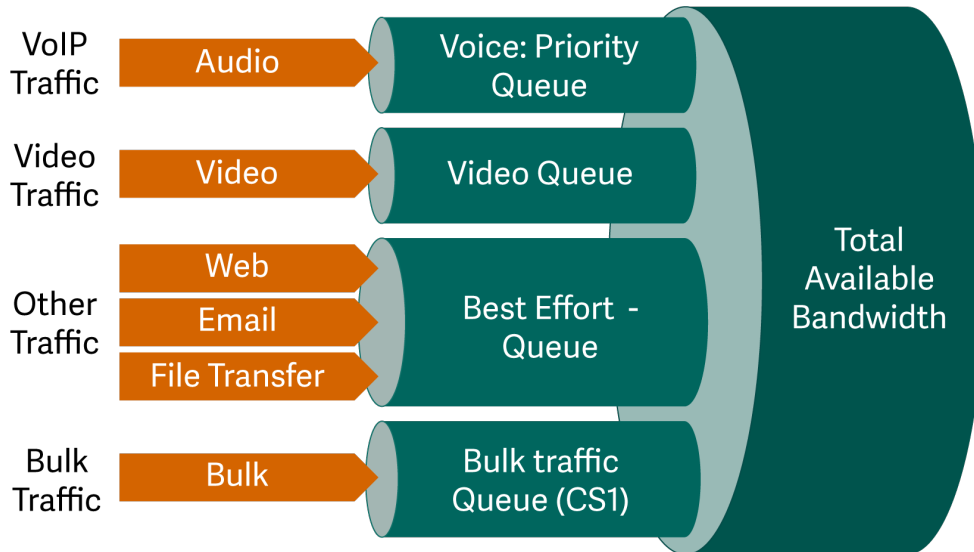
The gist of what we will be doing is that we will be marking (flagging) using DSCP marks, all UDP traffic from the console with tags that will make it land in the 'Video' queue of the advanced traffic manager.

By default, the IQrouter runs a three-tier traffic manager, with Bulk, Best Effort, and Voice (e.g. WiFi-calling or Ooma VoIP).

- Voice – Traffic marked as CS6 or CS7
- Best-Effort – All other (or marked CS0) or any unmarked traffic
- Lowest- Bulk traffic (marked CS1)

That is generally enough, but for advanced use cases, like [Zoom videoconferencing](#), or in this case, gaming, we need a four-tier mode with an additional Video Queue

- Latency Sensitive and VoIP traffic
 - Marks: CS7, CS6, CS5, CS4, Expedited Forwarding (EF) Voice Admit (VA)
- Video traffic for video conferencing / streaming
 - Marks: Assured Forwarding (AF)4x, AF3x, AF2x, CS3, CS2, TOS4, TOS1
- Best Effort (CS0, AF1x, Type of Service (TOS)2 and unmarked traffic lands here)
- Bulk (traffic marked CS1)



This assures that VoIP will get the highest possible priority and that video is not affected by bulk or best-effort traffic.

Steps to implement

First, you will need to find the MAC address of the console, it's shown in one of their settings or status screens, or you can find it on the Status->Advanced Overview DHCP leases listing.

The next thing is to enable the four-tier traffic manager mode.

Log in to the router (basic menus) and go to Configure->Network and, set VoIP optimization to checked on, click apply.

The unit will reboot. Log back in.

Go to the advanced menu, then Network->Firewall page.

There click the tab called 'Traffic Rules'



Scroll down to the bottom and click the Add button to create a new traffic rule.

Give it a name, in this example, and we called it BoostUDPtoAF33

Then use the Protocol drop-down to pick UDP as the only type we will apply this rule to.


Pick LAN for Source Zone and then Any zone (forward) for the Destination zone. And yes, it must be 'Any zone (forward)', not WAN. The marking must occur as the traffic is forwarded from the LAN so the traffic manager can see it.

Use the Action drop-down to pick 'DSCP Classification'

Then use the DSCP mark drop-down to pick 'AF33', which will cause traffic to land in the video tier.

When done, it will look like this (next page):

Firewall - Traffic Rules - BoostUDPToAF33

General Settings	Advanced Settings	Time Restrictions
Name	BoostUDPToAF33	
Protocol	UDP	
Source zone	lan lan: 	
Source address	-- add IP --	
Source port	any	
Destination zone	Any zone (forward)	
Destination address	-- add IP --	
Destination port	any	
Action	DSCP classification	
DSCP mark	AF33	

Apply the given DSCP class or value to established connections.

Now click the 'Advanced settings' sub-tab of the rule, and here we will pick which network device it will apply to by using the Source MAC address. Use that drop-down to locate the MAC of the Console (or PC if gaming on a PC). Use the IP address for confirmation you are picking the correct device.

If you have two consoles, then simply add the MAC of the second console to the list of source MAC addresses.

That looks like this when done:

Firewall - Traffic Rules - BoostUDPToAF33

General Settings | **Advanced Settings** | Time Restrictions

Match device

Restrict to address family

Source MAC address

Match helper
Match traffic using the specified connection tracking helper.

Match mark
Matches a specific firewall mark or a range of different marks.

Match DSCP
Matches traffic carrying the specified DSCP marking.

Limit matching
Limits traffic matching to the specified rate.

Extra arguments
Passes additional arguments to iptables. Use with care!

To finish, click save, and then click Save & Apply on the rules summary list.

This should ensure all UPD traffic from the console winds up prioritized ahead of other outbound traffic.

Remember, this is just prioritizing against your local traffic; once the packets are in the ISP or global backbone, they could be seeing packet loss, delays, etc., that is outside anyone's control.

Also, for gaming, certain inbound ports need to open (PS4 and Xbox usually open them via UPnP as needed), and the IQrouter reachability needs to be 'reachable' (see the Advanced Overview page).

Note: WiFi can **add** latencies due to poor signal, many local devices contending for airtime, etc. For truly optimal gaming, the console should be hardwired via Ethernet to the IQrouter. Alternatives to WiFi are discussed in this article on [networking quality](#). Actually, anything with an Ethernet port should be wired, especially set-top streaming boxes. Laptops should use a USB to Ethernet dongle if used for videoconferencing.

Finally, we'd like to point out that sometimes de-prioritizing certain devices can be a win overall, as there are plenty of chatty Internet of Things (IoT) hanging out on many home networks, constantly blasting data to the cloud. Power monitors are a good example, it's not a ton of data, but it is constant. So in this example, two power monitors, a washer and dryer and the Blink camera base unit are all deprioritized by marking their traffic with CS1, which pushes that traffic into the bulk tier. Note that we apply this to both UDP and TCP streams. Be careful with attempting to de-prioritize general-purpose devices like PCs; user experience might not be the best if traffic is all in the bulk tier.

Deprioritize	Forwarded IPv4 and IPv6, protocol UDP, TCP From lan , MAC C4:7F:51:01:A3:A5, C4:7F:51:01:98:6A, 4C:24:98:88:F0:0D, 2C:2B:F9:A0:4A:62, D8:BE:65:4B:02:E1 To any zone	Assign DSCP classification CS1	<input checked="" type="checkbox"/>
BoostUDPToAF33	Forwarded IPv4 and IPv6, protocol UDP From lan , MAC F0:6E:0B:F7:48:CF To any zone	Assign DSCP classification AF33	<input checked="" type="checkbox"/>