# Index.php

Version: 901

# Table of Contents

# Index.php

## Classifying Traffic Using iptables CLASSIFY

Now that we have configured the Quality of Service queues, we must sort traffic into the proper queues. While it is possible to do this from within the 'tc' QoS utility, using the iptables CLASSIFY directive provides a simpler, more flexible and more powerful method. In the router's firewall configuration (Option 1, Option 4, Option 2, Option 1 from the main menu), we will add the following statements below. For our VoIP phone, we can match traffic based on the source or destination IP address. We will map traffic coming from (Serial0) or going to (Ethernet0) the address 192.168.69.5 and add that traffic to class 1:10, which we mapped out originally and configured in the previous step:

```
#Phone traffic
iptables -A POSTROUTING -t mangle -o eth0 -d 192.168.69.5 \ -j CLASSIFY --set-class 1:10
iptables -A POSTROUTING -t mangle -o Serial0 -s 192.168.69.5 \ -j CLASSIFY --set-class 1:10
```

iptables CLASSIFY directives are always added to the POSTROUTING chain's mangle table. For more information about the path a packet follows through iptables, please see ImageStream's iptables tutorial or the official iptables HOWTO. Please note the significant difference between the two rules: the location of the "192.168.69.5" address. For traffic leaving the network on Serial0, 192.168.69.5 will be the source address. For reply traffic returning to the network (Ethernet0), the 192.168.69.5 will appear as the destination address.

The rules use several different elements, explained below:

**iptables**:

Specifies that the router is adding an iptables rule

**-A POSTROUTING**:

Appends (-A) a rule to the router's POSTROUTING chain

**-t mangle**:

Appends the rule to the mangle (-t mangle) table inside the specified chain

**-o eth0, -o Serial0**:

Specifies that only packets that match the specified outbound (-o) interface will match the rule. CLASSIFY rules will always be applied to an outbound interface.

**-d XX**:

Specifies that only packets with a destination address of "XX" will match the rule.

**-s XX**:

Specifies that only packets with a source address of "XX" will match the rule.

**-j CLASSIFY**:

Instructs iptables to take an action (-j) on packets matching this rule, in this case to CLASSIFY them into a QoS queue

**--set-class 1:XX**:

Instructs iptables to add matching packets to class ID 1:XX.

In the example below we have added rules for our interactive traffic class. First, we added the rules for telnet traffic, which uses port 23:

```
#telnet traffic
iptables -A POSTROUTING -t mangle -o eth0 -p tcp --sport 23 \ -j CLASSIFY --set-class 1:15
iptables -A POSTROUTING -t mangle -o Serial0 -p tcp -dport \ 23 -j CLASSIFY --set-class 1:15
```

Next, we added the rules for interactive SSH traffic. This traffic uses port 22, but we must also match the **ToS** bit for Minimize-Delay (0x10). Secure copy (SCP) traffic also uses port 22, but does not set the **ToS** bit. Please note that some SSH applications, such "putty" and "SecureCRT", do not set the ToS bit on interactive SSH traffic and will not match this rule. There is no workaround for programs that do not properly set the ToS bit.

```
#ssh traffic
iptables -A POSTROUTING -t mangle -o eth0 -p tcp -m tos \ --tos 0x10 --sport 22 -j CLASSIFY --set-c
iptables -A POSTROUTING -t mangle -o Serial0 -p tcp -m tos \ --tos 0x10 --dport 22 -j CLASSIFY --se
```

Notice that the above rules match both port 22 and the Minimize-Delay (0x10) ToS bit. The rules above use some additional elements, which are explained below:

**-p tcp**:

Specifies that only TCP packets will match the rule ("udp", "icmp" and others are accepted also). The -p directive must be included when using --dport or --sport.

**--dport XX**:

Specifies that only packets with a destination port number of "XX" will match the rule. Requires the use of -p.

**--sport XX**:

Specifies that only packets with a source port number of "XX" will match the rule. Requires the use of -p.

**-m tos**:

Load the Type of Service match module for iptables. The -m tos directive must be included when matching a ToS bit (--tos).

**--tos XX**:

Specifies that only packets with tos bit of "XX" will match the rule. Names such as "Minimize-Delay" are acceptable instead of binary values. Requires the use of -m tos.

Next, we have added rules for e-mail traffic class. We must match 3 ports: SMTP (25), POP (110) and IMAP (143):

```
#Mail traffic
iptables -A POSTROUTING -t mangle -o eth0 -p tcp --sport 25 \ -j CLASSIFY --set-class 1:30
iptables -A POSTROUTING -t mangle -o eth0 -p tcp --sport 110 \ -j CLASSIFY --set-class 1:30
iptables -A POSTROUTING -t mangle -o eth0 -p tcp --sport 143 \ -j CLASSIFY --set-class 1:30
iptables -A POSTROUTING -t mangle -o Serial0 -p tcp --dport \ 25 -j CLASSIFY --set-class 1:3
iptables -A POSTROUTING -t mangle -o Serial0 -p tcp -dport \ 110 -j CLASSIFY --set-class 1:3
iptables -A POSTROUTING -t mangle -o Serial0 -p tcp -dport \ 143 -j CLASSIFY --set-class 1:3
```

Finally, we will add rules to match FTP traffic from our security camera at 192.168.1.6. The rule will match both the IP address and port numbers (20 and 21):

```
iptables -A POSTROUTING -t mangle -o eth0 -p tcp -d \ 192.168.1.6 --sport 20:21 -j CLASSIFY
      iptables -A POSTROUTING -t mangle -o Serial0 -p tcp -s \ 192.168.1.6 --dport 20:21 -j
```

Please note the use of port ranges ("20:21" or "20,21", which is equivalent). Be careful to match the correct source or destination port. When the FTP replies to the security camera, it will reply from ports 20 or 21 to the 192.168.1.6 IP address. Accordingly, we have used the "-d" and "--sport" directives. It is not necessary to instate the rules immediately, but you will need to instate the rules before the configuration will take effect.