QOS CONFIGURATION
FOR SRX SERIES FOR THE
BRANCH WITH INTEGRATED
CONVERGENCE SERVICES
Table of Contents

Introduction .................................................................................................................. 3
Scope .............................................................................................................................. 3
Design Considerations .................................................................................................. 3
  Hardware Requirements: .............................................................................................. 3
  Software Requirements: .............................................................................................. 3
Description and Deployment Scenario .......................................................................... 3
  Defining your Forwarding Classes .............................................................................. 3
Port-Based QoS for IP Phones ....................................................................................... 6
Filter-Based Classification ............................................................................................. 7
DSCP-Based QoS for IP Phones (Thru-Traffic) .............................................................. 8
Configuration ................................................................................................................ 8
Implementing QoS on SRX Series Self-Traffic ............................................................... 10
Implementing DSCP Marking on SRX Series Self-VoIP Traffic ..................................... 11
Implementing Call Admission Control on SIP Trunks .................................................... 11
Summary ....................................................................................................................... 12
About Juniper Networks. ............................................................................................... 12

Table of Figures

Figure 1: CoS model for classification, queuing, and scheduling ................................. 4
Figure 2: In Junos OS, VoIP and other traffic are classified at the ingress interface, by BA or MF classifiers. Traffic Queuing, Shaping and DSCP rewriting is performed on the egress interface ................................. 6
Introduction

The purpose of this application note is to walk the reader through the steps necessary to configure class of service (CoS) and quality of service (QoS) for voice traffic on Juniper Networks® SRX Series Services Gateways for the branch with Integrated Convergence Services (ICS).

Scope

This paper introduces the Juniper Networks Junos® operating system command-line interface (CLI) and helps the reader configure an SRX Series device with Integrated Convergence Services with QoS and provides a building block for more advanced configurations. It does not include advanced security configuration examples or network design guidelines. Additional Juniper Networks documentation is available for readers at www.juniper.net/techpubs/software/junos/index.html#srx.

Design Considerations

Hardware Requirements:

Junos OS release 10.1 or later for all SRX Series Services Gateways with Integrated Convergence Services.

This includes the following SKU numbers:

• SRX210H-P-M
• SRX240H-P-M

Note: Certain features described in this document, including Integrated Convergence Services, are not available across the entire SRX Series platform. Readers should consult Juniper Networks product-specific literature for more details.

Software Requirements:

Junos OS release 10.1 or later for all SRX Series with Integrated Convergence Services.

Description and Deployment Scenario

This document describes several deployment options for configuring CoS and QoS for VoIP Traffic when using SRX Series Service Gateways for the Branch. After reading this document, you should be able to configure an SRX Series with ICS device to provide QoS for locally connected IP phones using either a port-based or DiffServ code point (DSCP)-based configuration. You should also be able to configure traffic prioritization, DSCP Marking and queuing for self-generated VoIP traffic to an external SIP trunk or peer call server. QoS over MPLS, IPsec VPN, and Frame Relay are outside the scope of this document.

Defining your Forwarding Classes

Before you can classify VoIP traffic, you must determine which forwarding classes you are using for VoIP. Junos OS has four default classes, but four additional “custom” classes can be configured—giving you eight total classes.

In these examples two classes are used, VoIP-5 for through-traffic (traffic for phones or other SIP endpoints) and VoIP-6 for self-traffic (traffic to or from the SRX Series itself—for trunks, FXS stations, or announcements). While you can use a single forwarding class for both types of traffic, using two allows you to give higher priority to outbound traffic to SIP trunks. Also, you can have separate QoS counters and statistics. VoIP-6 is given priority over VoIP-5, and network-control is the only class with higher priority then VoIP-6. This leaves six remaining classes for other traffic.

Figure 1: CoS model for classification, queuing, and scheduling
Forwarding class is assigned with packet loss priority (PLP) and DSCPs, which are used for queuing and BA in the core router. For the following UC applications, we recommend the following classifiers and PLP—also known as drop precedence (DP). PLP sets the packet drop precedence value (low or high) to help prevent queue congestion. Packets with a low PLP have higher buffer thresholds than packets with a high PLP. By default, the high threshold is 100 percent of the buffer. Table 1 lists the recommendations for using DiffServ and PLP for voice, video, and other traffic.

### Table 1: DiffServ Table

<table>
<thead>
<tr>
<th>APPLICATION</th>
<th>DIFFSERV</th>
<th>PLP</th>
<th>RECOMMENDED CODE POINT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network control</td>
<td>CS6</td>
<td>Low</td>
<td>110000</td>
</tr>
<tr>
<td>Voice</td>
<td>EF</td>
<td>Low</td>
<td>101110</td>
</tr>
<tr>
<td>Video</td>
<td>CS4, AF41, AF42, AF43</td>
<td>Low, High</td>
<td>1000000, 100010, 100100, 100110</td>
</tr>
<tr>
<td>Business application</td>
<td>AF21, AF22, AF23</td>
<td>Low, High</td>
<td>010010, 010100, 010110</td>
</tr>
<tr>
<td>Best effort</td>
<td>Remaining Code Points</td>
<td>Low</td>
<td>010001, etc.</td>
</tr>
</tbody>
</table>

1. Create a forwarding class called Voice-5 using queue #5 and Voice-6 using queue #6.
edit class-of-service forwarding-classes

| Set queue 5 | Voice-5         |
| Set queue 6 | Voice-6         |

2. Create a scheduler profile `VoiceSched` to map schedulers to a forwarding class.

top

edit class-of-service schedulers

| Set network-control-scheduler buffer-size percent 10 |
| Set network-control-scheduler priority strict-high |

| Set `voice6-scheduler` priority high         |
| Set `voice6-scheduler` buffer-size percent 10 |

| Set `voice5-scheduler` priority medium-high |
| Set `voice5-scheduler` buffer-size percent 10 |

| Set best-effort-scheduler priority low       |
| Set best-effort-scheduler transmit-rate remainder |
| Set best-effort-scheduler buffer-size remainder |

**Note:** If using a T1 or serial interface, you need to increase the size of the buffer by using the following command.

This increases the buffer to two seconds, allowing for more packets in the queue for mPIM slot 1.

top

| Set chassis fpc 1 pic 0 q-pic-large-buffer large-scale |

3. Create your scheduler maps (a group of forwarding classes), which map your voice schedulers to Junos OS forwarding-class.

top

edit class-of-service

edit scheduler-maps `VoiceSched`

| Set forwarding-class network-control scheduler network-control-scheduler |
| Set forwarding-class `Voice-6` scheduler `voice6-scheduler` |
| Set forwarding-class `Voice-5` scheduler `voice5-scheduler` |
| Set forwarding-class best-effort scheduler best-effort-scheduler |

4. Apply your scheduler maps to the interface(s). In this case, fe-0/0/6 and fe-0/0/7 are used. This allows outbound scheduling of voice traffic over the WAN to SIP trunks or peer call servers using Voice-6, and all other intra-enterprise voice endpoints using Voice-5.

| Set interface fe-0/0/6 scheduler-map `VoiceSched` |
| Set interface fe-0/0/7 scheduler-map `VoiceSched` |
Port-Based QoS for IP Phones

The following example shows how to classify traffic on a per-port basis. If your IP phones do not support DSCP, or you want certain ports to be configured as “voice only” switch ports on the SRX Series, this places all traffic on these ports in the Voice-5 class—regardless of IP, protocol, or DSCP information received in the packet. This is known as static port-based QoS and is the most simple to configure. The drawback and security risk is that anyone physically connected to that port, even if an IP phone isn’t being used, can abuse the forwarding class.

1. Apply the forwarding class Voice-5 to the physical interfaces. In this case, the four PoE ports on a Juniper Networks SRX210 Services Gateway are used.

   ```
   set class-of-service interfaces ge-0/0/0 unit 0 forwarding-class Voice-5
   set class-of-service interfaces ge-0/0/1 unit 0 forwarding-class Voice-5
   set class-of-service interfaces fe-0/0/2 unit 0 forwarding-class Voice-5
   set class-of-service interfaces fe-0/0/3 unit 0 forwarding-class Voice-5
   ```

2. You can also apply the forwarding class Voice-5 to a VLAN interface to classify all traffic on that VLAN.

   ```
   set class-of-service interfaces vlan unit 101 forwarding-class Voice-5
   ```

3. Once an IP phone has been connected to these ports, place a call and use the following show commands to validate that traffic is being assigned to the correct forwarding class. This command also shows packets queued, transmitted, and dropped.

   ```
   show interface queues ge-0/0/0 forwarding-class Voice-5
   Queue: 5, Forwarding classes: Voice-5
   Queued:
   Packets : 1603       49 pps
   Bytes   : 343042     85384 bps
   Transmitted:
   Packets : 1603       49 pps
   Bytes   : 343042     85384 bps
   Tail-dropped packets : 0         0 pps
   RED-dropped packets  : 0         0 pps
   ```

Figure 2: In Junos OS, VoIP and other traffic are classified at the ingress interface, by BA or MF classifiers, Traffic Queuing, Shaping and DSCP rewriting is performed on the egress interface.
Filter-Based Classification

In addition to port-based classification, (firewall) filter-based classification allows you to classify packets arriving at an interface based on Layer 3 or 4 header information—such as source IP, port number, and packet size. The following filter terms are used and applied to the ingress interface to classify traffic as either SIP or RTP. You can optionally put source or destination IP addresses in the filters to be more specific to your application.

1. Create a filter term for SIP by using destination-port 5060.

   ```plaintext
   set firewall filter VoIP-Thru term 1 from protocol udp port 5060
   set firewall filter VoIP-Thru term 1 then log count Voice5-SIP
   set firewall filter VoIP-Thru term 1 then forwarding-class Voice5 accept
   ```

2. Create a filter term for rTP by using a packet size of 200. This is the exact packet size of RTP messages when you use the G711 CODEC.

   ```plaintext
   set firewall filter VoIP-Thru term 2 from protocol udp packet-length 200
   set firewall filter VoIP-Thru term 2 then log count Voice5-RTP
   set firewall filter VoIP-Thru term 2 then forwarding-class Voice5 accept
   ```

3. Create a filter to match all other traffic with counting and enabled.

   ```plaintext
   set firewall filter VoIP-Thru term 3 from address 0.0.0.0/0
   set firewall filter VoIP-Thru term 4 then log count Any-Rule accept
   ```

4. Apply the filters as input filters to the ingress interfaces, connected to IP phones. In this case, VLAN101 is used along with fe-0/0/6 as examples.

   ```plaintext
   set interface vlan.101 family inet filter input VoIP-Thru
   set interface fe-0/0/6 family inet filter input VoIP-Thru
   ```

5. Test the filters by clearing them and sending SIP and RTP traffic through the SRX Series. Use the following show commands to see the firewall term counters incrementing.

   ```plaintext
   clear firewall all       # First clear the counters
   root> show firewall
   Filter: VoIP5
   Counters:
   Name          Bytes   Packets
   Any-Rule      120839   150
   Voice5-RTP    111400   557
   root> show firewall counter Voice5-RTP filter VoIP5
   Filter: VoIP5
   Counters:
   Name          Bytes   Packets
   Voice5-RTP    130800   654
   ```
DSCP-Based QoS for IP Phones (Thru-Traffic)

By having branch IP phones (and softphones) mark SIP and RTP traffic using a DiffServ bit, the SRX Series can prioritize and queue the VoIP traffic as it passes through the gateway. This technique can also be used for SIP trunks and peer call servers, provided the SRX Series receives DSCP market packets from these hosts.

The following assumptions are made about the QoS configuration:

- RTP/SIP traffic is classified, if this traffic has a DiffServ code point of 46 (binary 101110)
- Traffic classified as **Voice-5** is queued into forwarding-class 5, the third highest on the router.
- Classification is applied and occurs at the ingress interface,
- Queuing is performed only on the WAN egress interface (fe-0/0/7).
- The DiffServ marking is preserved as the packet enters the WAN, MPLS, or IPsec tunnel.

**Configuration**

1. Create a new classifier profile. Import the default classifier to avoid defining all DSCP values, and only reclassify the DSCP value of the VoIP traffic that needs to be prioritized. The IP telephone is configured to use the DSCP decimal value of 46 (101110 in binary) for signaling and media packets.

   **Note:** This DSCP value for Avaya is configured in the ip-network-region form of Communication Manager.

   ```
   top
   edit class-of-service classifiers
   set dscp 46 import default
   set dscp 46 forwarding-class Voice-5 loss-priority medium-low code-points 101110
   top
   edit class-of-service interfaces
   set ge-0/0/0 unit 0 classifiers dscp 46
   set ge-0/0/1 unit 0 classifiers dscp 46
   set fe-0/0/2 unit 0 classifiers dscp 46
   set fe-0/0/3 unit 0 classifiers dscp 46
   ```

2. Create a rewrite rule for DSCP 46 by using forwarding class Voice-5.

   ```
   top
   edit class-of-service rewrite-rules
   set dscp 46-VoIP forwarding-class Voice-5 loss-priority medium-high code-point 101110
   ```

3. Apply your rewrite rule to all the VoIP egress interfaces, including Untrust and locally connected IP phones.

   ```
   top
   edit class-of-service interfaces
   set ge-0/0/0 unit 0 rewrite-rules dscp 46-VoIP
   set ge-0/0/1 unit 0 rewrite-rules dscp 46-VoIP
   set fe-0/0/2 unit 0 rewrite-rules dscp 46-VoIP
   set fe-0/0/3 unit 0 rewrite-rules dscp 46-VoIP
   ```
4. Apply the scheduler profile VoiceSched and classifiers for DSCP 46 to the access (IP phones) and uplink (Untrust) ports.

```
edit class-of-service interfaces
set ge-0/0/0 scheduler-map VoiceSched
set ge-0/0/0 unit 0 classifiers dscp 46
set ge-0/0/1 scheduler-map VoiceSched
set ge-0/0/1 unit 0 classifiers dscp 46
set fe-0/0/2 scheduler-map VoiceSched
set fe-0/0/2 unit 0 classifiers dscp 46
set fe-0/0/3 scheduler-map VoiceSched
set fe-0/0/3 unit 0 classifiers dscp 46
```

5. Test the configuration by first setting up your IP phone to use DSCP code point of 46 for all SIP and RTP traffic. You might want to validate this using a sniffer to examine the IP headers being transmitted. Once confirmed, you can display statistics on the Junos OS device by using the following commands.

```
root> show interfaces queue fe-0/0/6 forwarding-class Voice-5
Physical interface: fe-0/0/6, Enabled, Physical link is Up
   Interface index: 137, SNMP ifIndex: 120
   Forwarding classes: 8 supported, 5 in use
   Egress queues: 8 supported, 5 in use
   Queue: 5, Forwarding classes: Voice5
   Queued:
      Packets : 1603       49 pps
      Bytes : 343042      85384 bps
   Transmitted:
      Packets : 1603       49 pps
      Bytes : 343042      85384 bps
      Tail-dropped packets : 0         0 pps
      RED-dropped packets : 0         0 pps
      Low : 0          0 pps
      Medium-low : 0      0 pps
      Medium-high : 0     0 pps
      High : 0        0 pps
      RED-dropped bytes : 0         0 bps
      Low : 0          0 bps
      Medium-low : 0      0 bps
      Medium-high : 0     0 bps
      High : 0        0 bps
```
Implementing QoS on SRX Series Self-Traffic

In addition to VoIP traffic passing through the SRX Series, it is also possible to configure QoS on VoIP traffic being initiated from the SRX Series, or terminating to the SRX Series. The following section covers this configuration—which enables queuing and prioritization of RTP packets leaving the WAN Interface—fe-0/0/6 in this example.

To prioritize traffic flowing to/from the DSP, the following Junos OS firewall term is created and applied to the mpu (DSP) interface of the SRX Series.

1. Create a filter term for SIP by using destination-port 5060.

```
set firewall filter VoIP-Self term 1 from protocol udp port 5060
set firewall filter VoIP-Self term 1 then log count Voice6-SIP
set firewall filter VoIP-Self term 1 then forwarding-class Voice5 accept
```

2. Create a filter term for RTP by using a packet size of 200. This is the exact packet size of RTP messages when you use the G711 CODEC.

```
set firewall filter VoIP-Self term 2 from protocol udp packet-length 200
set firewall filter VoIP-Self u term 2 then log count Voice6-RTP
set firewall filter VoIP-Self term 2 then forwarding-class Voice6 accept
```

3. Create a filter to match all other traffic with counting and enabled.

```
set firewall filter VoIP-Self term 3 from address 0.0.0.0/0
set firewall filter VoIP-Self term 4 then log count Any-Rule accept
```

4. Apply the filters as input filters to the MPU interface as RTP packets from the DSP on SRX Series comes from the MPU interface. This will classify the traffic as it comes into the SRX Series (from the DSP).

```
set interface mpu-0/0/9 family inet filter input VoIP-Self
```

5. Apply the filters as output filters to the WAB interface, fe-0/0/7 in this example. This is so that SIP and RTP packets leaving the box get classified appropriately before leaving the WAN Interface.

```
set interface fe-0/0/7 family inet filter output VoIP-Self
```

6. Be sure you have the scheduler maps applied to any LAN interfaces that IP phones are connected.

```
edit class-of-service interfaces
set ge-0/0/0 scheduler-map VoiceSched
set ge-0/0/1 scheduler-map VoiceSched
set ge-0/0/2 scheduler-map VoiceSched
```

7. Test the filters by clearing them and sending SIP and RTP traffic through the SRX Series. Use the following show commands to see the firewall term counters incrementing.

```
clear firewall all           # First clear the counters
root> show firewall counter Voice6-RTP
Filter: VoIP6
Counters:
Name        Bytes    Packets
Voice6-RTP  130800   654
```
Implementing DSCP Marking on SRX Series Self-VoIP Traffic

In addition to scheduling, DSCP marking may be desired on self-generated SIP or RTP traffic from the SRX Series. Junos OS 10.1 introduces new media-policy commands under services | convergence-services which allow you to mark outbound RTP traffic based on the address of the SIP Peer, which may be either an IP Address or FQDN. The following examples outline this configuration.

1. Create a media policy to match traffic for your local subnet with an action to mark the traffic with DSCP 46.

```
edit services convergence-services
set media-policy 1 term 1 from peer-address ip-address 10.0.0.0/8
set media-policy 1 term 1 then dscp 46
```

2. Create a media policy to match RTP traffic to/from a specific SIP trunk with an action to mark the traffic with DSCP 46.

```
set media-policy 1 term 2 from peer-address fqdn sipgate.com
set media-policy 1 term 2 then dscp 46
commit
```

After committing this configuration, RTP traffic destined to these endpoints will be marked with DSCP value of 46. If desired, separate DSCP values can be used for each term rule, for example RTP traffic destined for sipgate.com could be marked with DSCP 42, while local-subnets (10.0.0.0) could be marked with 46.

3. To mark outbound SIP traffic with a DSCP bit, the following rewrite-rules are created and applied to the fe-0/0/7 interface. This will mark all traffic in forwarding-class VoIP5 with DSCP value 46 (101110).

```
edit class-of-service
set rewrite-rules dscp sip-dscp forwarding-class VoIP5 loss-priority low code-point 101110
set interfaces fe-0/0/7 unit 0 rewrite-rules sip-dscp
```

Implementing Call Admission Control on SIP Trunks

In addition to Classification, Prioritization and Marking of SIP and RTP traffic, the SRX Series with ICS is also capable of performing call admission control on any SIP trunk configured on the box. Junos OS 10.1 supports static CAC and allows you to simply define the max number of concurrent calls that will be allowed on a specific SIP trunk. The following examples outline the configuration necessary to setup a SIP trunk and limit the max calls to 5.

1. Create a SIP trunk, in this example a SIP trunk service provider is used. If you already have a SIP trunk defined you can skip ahead to step 2.

```
edit services convergence-services
set trunk sipgate.com trunk-type sip peer-proxy-server address fqdn sipgate.com
```

2. Edit the SIP trunk and set the max-concurrent-calls to 5.

```
edit trunk sipgate.com
set max-concurrent-calls 5
```
3. Create a trunk group that includes both SIP trunk and PSTN, with SIP trunk as priority #1 and FXO as priority #2. Note that the third concurrent call will be routed over the FXO trunk because max-concurrent-calls are limited to 2 on the SIP trunk.

```
Set trunk-group Sip+PSTN trunk sipgate.com trunk fxo1 trunk fxo2 commit
```

After committing this configuration, the SRX Series will allow a maximum of 5 concurrent calls to be routed through the SIP trunk, the 6th call may routed to other trunks included in the trunk group (FXO trunks) or simply denied “All circuit are busy now.” For more information on setting up the dial-plan to use the SIP trunk, please see the SRX Series with ICS Golden Configurations document.

**Summary**

SRX Series for the branch provide all the features required to securely connect modern remote and branch offices in a one-box solution. Junos OS offers users unparalleled flexibility designed to meet the most demanding network requirements. After reading this document, you can configure an SRX Series for the branch device to securely pass traffic, support both analog and SIP phones, and provide basic calling features. With a little practice, you can create advanced configurations required for more complex deployments.

**About Juniper Networks**

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.