Quality of Service (QoS) in enterprise networks

Why QoS is critical to connect enterprise networks to a cloud voice service.

White paper

Quality of service in enterprise networks

Cloud voice service, or voice over IP in general, can be extremely cost-effective for the enterprise

Background

Enterprise customers embrace the return on investment (RoI) potential of the technology, execute small proof-of-concept (PoC) tests successfully, then opt for large-scale rollouts that may operate at a less than expected quality level. This issue is rarely caused by product or vendor issues; rather it is usually the result of improper (or no) configuration of quality of service (QoS) parameters.

A small PoC test typically involves very small amounts of voice network traffic and does not stress the network. A large-scale rollout, on the other hand, requires the network to handle large amounts of voice traffic. Depending on the loading of the enterprise data network, it may operate without issue most of the time, but encounter sporadic bursts of garbled voice or complete voice dropout. Normal network monitoring tools will not show any kind of issue, and the enterprise assumes that the voice service provider is at fault.

Problem causes

What is happening? Several possibilities, most likely...

1. A shared data network is used in which users are accessing file shares, email shares, etc. Modern internet protocols have been carefully crafted to maximize the speed and volume of large data transfers. These data transfers send a tremendous quantity of very large data packets all at once and only stop when the far end fails to acknowledge receipt of a packet.

When network load is high, data packets stack up in network devices and are queued on the output interfaces. The voice traffic, generally 50 small packets every second, must take its turn behind this stack of very large data packets and can be delayed beyond acceptable limits. This results in garbled voice and/or actual voice dropout.

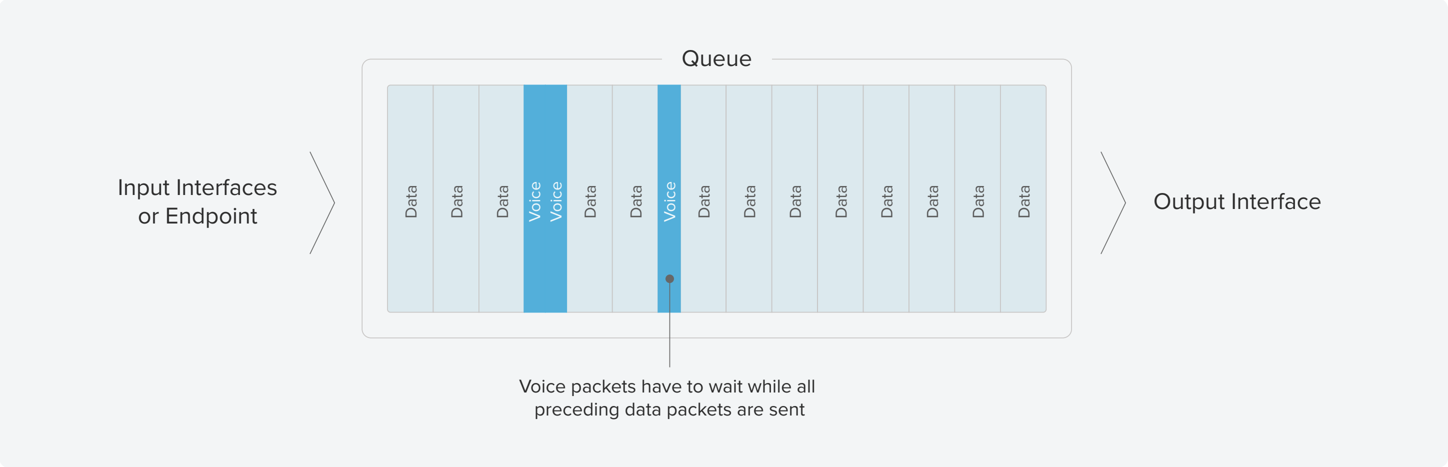

Queue
Input Interfaces or Endpoint
Data
Data
Data
Voice
Voice
Data
Data
Voice
Data
Data
Data
Data
Data
Data
Data
Data
Output Interface
Voice packets have to wait while all preceding data packets are sent

Image N°1. Transmitting System or Network Device No QoS Policy, Only Single Queue Used

A proper QoS policy makes use of multiple data queues, at least one being a priority queue from which packets are always taken and transmitted in the next available packet. The policy will take data packets, which have been classified as voice packets, and insert them in the priority queue. High-priority traffic will be transmitted before regular data traffic, which makes the less delay-sensitive data traffic wait longer to be transmitted. (Identification and classification of data packets will be discussed in a later section.)

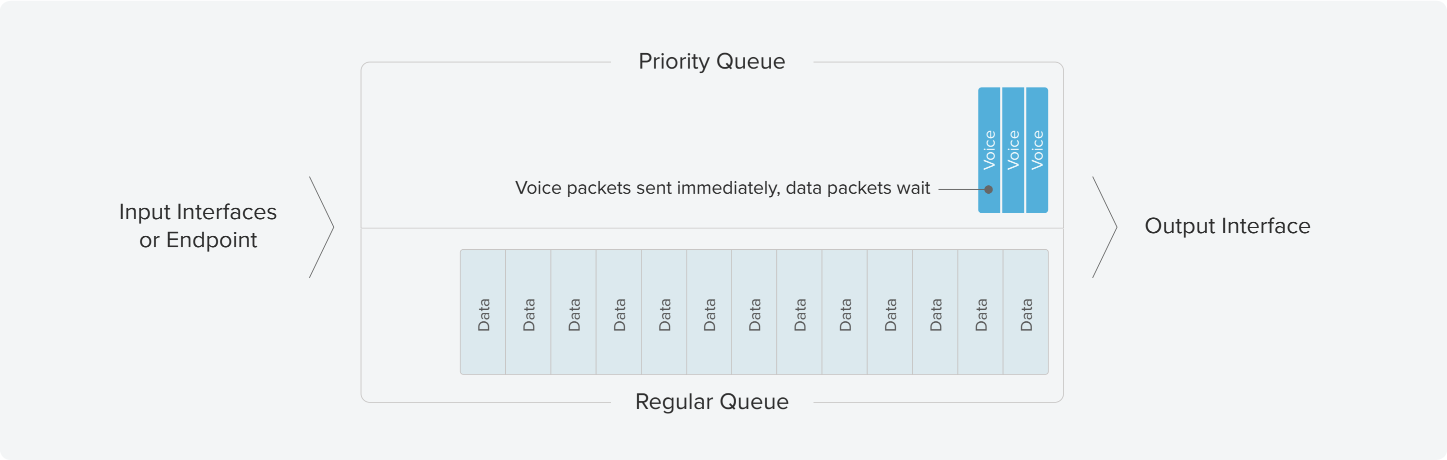


Image N°2. Transmitting System or Network Device QoS Policy Defined, Multiple Queues Used

2. The wide-area network (WAN) link that carries traffic to/from the internet or between offices experiences periods of very high utilization. The WAN carrier will only accept data packets at the contracted rate. If the enterprise sends data packets at a rate faster than the contracted rate, the carrier will respond by automatically dropping random data packets, some of which may be voice traffic. The carrier does not, as a rule, honor any QoS markings on customer traffic unless a proper QoS profile is part of the contract. A proper QoS policy applied to the WAN network egress device (e.g., a network border router/firewall) not only prioritizes voice traffic out of the WAN link, it will also “shape” the outbound traffic, ensuring that the enterprise does not exceed the speed of the WAN link.

Why do network-monitoring tools not show the issue?

Normal network-monitoring tools check traffic levels at large preset intervals, usually 1 minute (60 seconds) or 5 minutes (300 seconds). They also apply algorithms that effectively average the measured traffic flow over relatively long periods of time. A 10-second burst of heavy traffic can result in 10 seconds of severe voice impairment, yet the network-monitoring tools will not see any issue, due to this averaging effect.

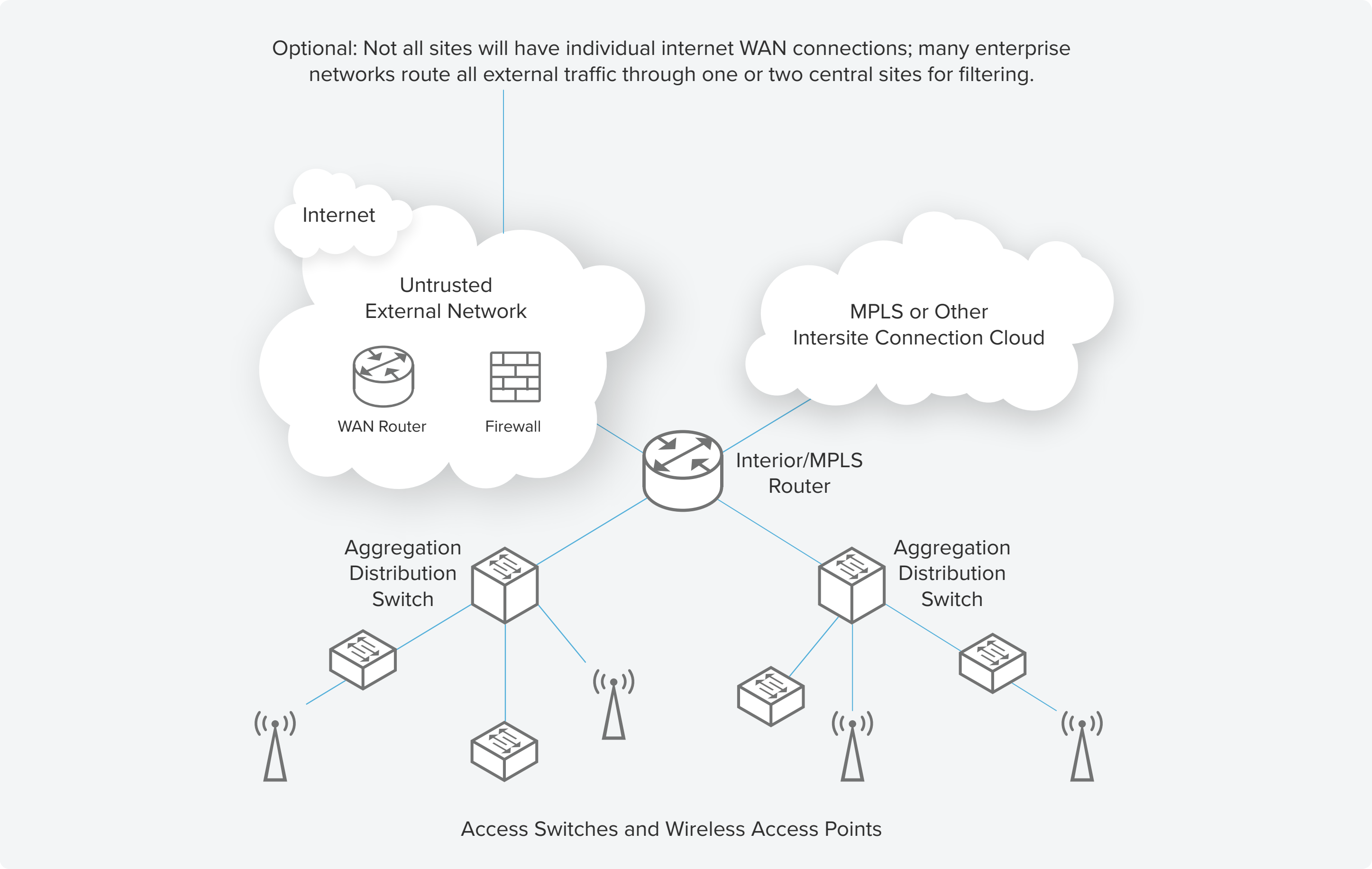
Enterprise network topology

An enterprise network absolutely **must** have a carefully planned QoS setup to avoid these issues. Every network device at Layer 2 and Layer 3 must fully participate in the QoS policy. Any device that does not support comprehensive QoS policies should be considered for elimination from the network. Enterprise network devices usually fall into the following categories (note that the functionality of two or more categories may be combined in some smaller networks

- **Endpoint devices** – Computers, phones, softphones, video conference devices, etc.
- **Access Switches** – Provide connectivity to computers, phones, and access points.
- **Wireless Access Points** (WAPs) – Provide connectivity to wireless users. They function like an access switch but have different QoS mechanisms.
- **Aggregation/Distribution switches** – Aggregate the traffic from multiple Access Switches and/or WAPs.
- **Interior/MPLS routers** – Control routing of packets between internal networks, both locally and across dedicated links

or MPLS network links. Frequently a large Layer-3 switch will be utilized for this purpose and is then called a **Core router** or a **Core Switch**.

- **Firewalls** – Provide access control to allow only preapproved traffic flows.
- **WAN Routers** – Provide access to the Internet and/or private carrier network(s).


Optional: Not all sites will have individual internet WAN connections; many enterprise networks route all external traffic through one or two central sites for filtering.
Internet
Untrusted External Network
WAN Router
Firewall
MPLS or Other Intersite Connection Cloud
Interior/MPLS Router
Aggregation Distribution Switch
Aggregation Distribution Switch
Access Switches and Wireless Access Points

Access Switches

An Access Switch is a portal through which multiple users access the corporate network and the greater internet. This is the first network device through which user traffic passes.

The Access Switch must:

1. Inspect user traffic entering the corporate network to ensure it has proper DSCP classifications and alter (re-mark) the DSCP tags of this traffic when needed.
2. Prioritize traffic exiting the corporate network to users/phones and ensure that voice traffic is expedited.
3. Inspect the traffic entering the corporate network from Wireless Access Points (WAPs) and re-mark the DSCP tags as needed.
4. Merge traffic from multiple user/phone devices into composite trunk connections that are fed upstream to Aggregation Distribution Switches.

The ports on Access Switches generally belong to the follow categories:

1. **User port** – Connects a user workstation to the corporate network. This connection may physically flow through a hardware VoIP phone. The port is generally set up with a voice VLAN for VoIP phones to keep voice traffic logically separated from user data traffic. This port may, in some instances, authenticate the connected user/device. The attached PC may have a soft VoIP phone application in addition to or in lieu of a hardware VoIP phone.

2. **WAP port** – Connects a Wireless Access Point (WAP) to the corporate network. These ports are often found on Access Switches rather than Aggregation/Distribution Switches due to logistical considerations. (WAPs must be deployed quite densely in order to obtain good pervasive wireless coverage and are often too far from an Aggregation/Distribution Switch.) Note that these are trunk ports and will have very high traffic levels.
3. **Phone port** – Connects a standalone VoIP phone to the corporate network. The port is set up as an access type port with the native (untagged) VLAN set to the voice VLAN ID.
4. **Printer port/Special port** – Connects printers or specialty devices to the corporate network.
5. **Trunk port** – Connects the switch to upstream aggregation/distribution switches or Interior/MPLS routers. This type of port is frequently a member of an 802.1ad Link Aggregation Group (LAG). It carries multiple VLANs tagged as 802.1q traffic. Note that trunk ports may have very high traffic levels.

Wireless Access Points

The Wireless Access Point (WAP) is a portal through which wireless users may access the corporate network and the greater internet in a manner similar to the Access Switches. This is the first network device through which wireless user traffic passes. The Wireless Access Point must:

1. Authenticate the user.
2. Inspect wireless traffic entering the corporate network to ensure it has proper DSCP classifications and alter the DSCP tags of traffic when needed. Some Wireless Access Points do not have the capability to alter DSCP tags of traffic and will require the upstream switch perform the re-marking task.
3. Merge traffic from multiple mobile devices and Wi-Fi-connected computers into a composite trunk connection that is fed upstream to Aggregation/Distribution Switches. This type of port can be a member of an 802.1ad LAG group. Note that in many configurations Wireless Access Point trunks are fed to/from Access Switches to reduce the complexity and device count of the corporate network.

Configuration of the Wireless Access Point devices to support QoS is vendor/model specific and outside the scope of this document.

Aggregation/Distribution Switches

The Aggregation/Distribution Switch concentrates traffic from multiple Access Switch and/or Wireless Access Point trunk ports into larger composite trunks. They are used to simplify the wiring of large corporate networks. The Aggregation/Distribution Switch must:

1. Inspect wireless traffic entering the corporate network to ensure it has proper DSCP classifications and alter the DSCP tags of traffic when needed. This is necessary because some Wireless Access Points and some Access Switches do not have the capability to alter DSCP tags of traffic.
2. Merge traffic from multiple Access Switches and/or Wireless Access Points into composite trunk connections that are fed upstream to Interior/MPLS routers.

The ports on Aggregation/Distribution Switches generally belong to the following categories:

1. **WAP port** – Connects a Wireless Access Point (WAP) to the corporate network. Note that these are a type of trunk port and will have very high traffic levels.
2. **Trunk port** – Connects the switch to upstream Interior/MPLS routers and downstream Access Switches. This type of port is frequently a member of an 802.1ad LAG group. It carries multiple VLANs tagged as 802.1q traffic. Note that trunk ports may have very high traffic levels.

Interior/MPLS routers (sometimes referred to as Core/Site Switches/routers)

The Interior/MPLS router controls the flow of traffic at Layer 3. It will route packets from the source to the destination across different Layer-2 VLANs. Many routers also provide some network service functionality such as DHCP services. Please note that even though the designation router is used, this device is very often an advanced Layer-3 capable switch. A Layer-3 switch with this capability is often referred to as a **Core** or **Site Switch** or a **Core** or **Site router**. Interior routers that are functioning as MPLS routers must also include QoS shaping policies to smooth traffic and to ensure that traffic flowing from the router toward the MPLS carrier does not exceed the contracted traffic rates of the MPLS link.

Firewalls

The firewall controls data flow between devices and/or VLANs based upon various security criteria. It may, in simple networks, act as a WAN access router. Trusted voice traffic in a complex network should, if possible, bypass firewalls and be handled directly by the WAN router. Please see individual notes regarding vendor-specific firewall configurations for interoperation with RingCentral.

WAN routers

The WAN router connects the enterprise network to the greater internet. It is usually responsible for performing Network Address Translation (NAT) and may perform some security functionality. It must shape the flow of data out to the outside world.

Quality of service (QoS)

There are multiple mechanisms that are used to ensure QoS. The most commonly supported is the use of the Layer 3 Differentiated Services Code Point, or DSCP value in the IP header.

The basic structure of the IP data packet contains a 6-bit field in the second byte of the packet header that associates a numerical value (0–63) with each data packet. This value is called the DSCP value. It can be used by network devices to control the flow of this packet through the network.

[Note: Prior to implementation of the DSCP system, the first 3 bits of this data field were called IP Precedence. This value (0–7) was used in a more primitive manner to control the flow of the packet through the network. Some endpoint devices still utilize it.]

IPv4 Header Format

<table>
<tr><td>Offsets</td><td>Octet</td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>Octet</td><td>Bit</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td>0</td><td>0</td><td colspan="4">Version</td><td colspan="4">IHL</td><td colspan="6">DSCP</td><td colspan="2">ECN</td><td colspan="16">Total length</td></tr>
<tr><td>4</td><td>32</td><td colspan="16">Identification</td><td colspan="3">Flags</td><td colspan="13">Fragment offset</td></tr>
<tr><td>8</td><td>64</td><td colspan="8">Time to Live</td><td colspan="8">Protocol</td><td colspan="16">Header Checksum</td></tr>
<tr><td>12</td><td>96</td><td colspan="32">Source IP address</td></tr>
<tr><td>16</td><td>128</td><td colspan="32">Destination IP address</td></tr>
<tr><td>20</td><td>160</td><td colspan="32" rowspan="4">Options (if IHL>5)</td></tr>
<tr><td>24</td><td>192</td></tr>
<tr><td>28</td><td>224</td></tr>
<tr><td>32</td><td>256</td></tr>
</table>

DSCP/ToS tagging

DSCP EF (46) is normally used to mark real-time voice traffic—the actual voice. Standard VoIP implementations send one data packet every 20 milliseconds or 50 packets every second; some schemes allow for this to be changed. Most VoIP phones and PBXs use a jitter buffer of 40–100 milliseconds to allow for packets to be slightly delayed in transit. Delay of a packet by more than the size of the jitter buffer results in dropped or garbled speech. This makes it critical to ensure that these packets are transmitted upon being generated and not held up by large bursts of other data.

DSCP AF41 (34) is normally used to mark real-time video traffic. This traffic is sensitive to jitter, but not to the same extent as voice traffic.

DSCP AF31 (26) is normally used to mark UDP and TCP traffic used for control and signaling—call setup and teardown. This traffic is important and must be guaranteed but is relatively insensitive to jitter.

DSCP AF21 (18) is used by RingCentral for other important traffic and needs to have some guarantee. It is not sensitive to jitter.

DSCP Value	Decimal	Name	Drop Prob	IP Prec
111 000	56	CS7		7
110 000	48	CS6		6
101 110	46	EF	N/A	5
101 000	40	CS5		5
100 010	34	AF41	Low	4
100 100	36	AF42	Medium	4
100 110	38	AF43	High	4
100 000	32	CS4		4
011 010	26	AF31	Low	3
011 100	28	AF32	Medium	3
011 110	30	AF33	High	3
011 000	24	CS3		3
010 010	18	AF21	Low	2
011 100	20	AF22	Medium	2
010 110	22	AF23	High	2
010 000	16	CS2		2
001 010	10	AF11	Low	1
001 100	12	AF12	Medium	1
001 110	14	AF13	High	1
001 000	8	CS1		1
000 000	0	BE (Best Effort)	N/A	0

The universally defined and accepted DSCP values/names are shown in the following table. The values normally used in VoIP communication are highlighted.

Traffic ingress marking

Data traffic entering the enterprise network from ISPs or endpoint devices may not have proper DSCP values applied to the data packets. The network devices must examine the incoming data packets and alter the DSCP field to the proper value. This is referred to as re-marking the packets.

Re-marking is usually needed for the following connection types:

- Internet connections – Many internet service providers (ISPs) strip the DSCP field from packets traversing their networks, usually setting the field to a default value of BE (0). A QoS policy must examine the data packets, determine their usage, and change the DSCP tag value to the correct value for that usage. Packets that do not match any defined criteria must be set to a DSCP value of BE (0).
- WAP Ports – The status of DSCP markings in WAP traffic is vendor dependent. It is best to assume the worst and plan to re-mark the traffic. Also, some wireless phone devices do not generate data packets with the correct DSCP value and must be re-marked. Windows® PCs operating in Wi-Fi mode require re-marking as discussed in the User Ports section.
- User Ports – Windows by default re-marks each data packet with a DSCP value of BE (0). Group Policy and setting of NetQoSPolicies can be used on Windows 7- and 10-based computers to enable proper transmission of DSCP values upstream. A sample of such a policy is given in Appendix A.

Re-marking ingress policies for certain switches and routers are given in Appendix B and subsequent appendices. Please note that many soft clients do not generate the correct markings. At this time it is considered safest to use the NetQosPolicy on Windows boxes or to utilize a switch-port ingress QoS policy to examine the data packets, determine their destination and usage, and change the DSCP tag value to the correct value for that usage.

Traffic shaping

ISP connections and MPLS links are set up by the carrier to only accept data packets at a certain contracted rate, which is usually less than the actual interface physical capacity. The carrier will discard any packets that arrive over that rate **regardless of DSCP marking**.

This can only be prevented by sending packets out at a rate no faster than the rate contracted with the carrier. This is called shaping the output. Traffic should be shaped to an average value of 95% of the contracted data rate.

Shaping is absolutely mandatory to provide effective QoS on any circuit that does not run at the maximum physical line speed of the port.

Shaping and prioritization QoS policies for certain switches and routers are given in the Appendices.

RingCentral: delivering the highest voice quality

RingCentral has a history of innovation and a proven track record of investment to ensure customers and end users enjoy the highest-quality HD voice. To back this goal, RingCentral offers SLAs for both availability (99.999% uptime) as well as voice quality (minimum MOS score of 3.8), irrespective of the mode of network connection.

Additionally, RingCentral invests in other areas to ensure the best end-user experience:

- **Global private backbone**: RingCentral was born in the cloud. Maximizing quality over any connection, including OTT and mobile, is a foundational principle of product and infrastructure architecture.

  RingCentral data centers—in close physical proximity to the world's top 20 internet exchange points—are co-located with all the major US telecommunications carriers to ensure the fastest response times and interconnect services possible. The geographic diversity of our locations acts as an additional safeguard, minimizing our risk of loss and service interruption due to natural disasters and other catastrophic situations.

  Our platform is our own, purpose-built to perform as a highly redundant, reliable, and secure global communications network. This is an important distinction, contrasting with leased lines or outsourced service delivery.

  We've established our own backbone and developed our own peering relationships to provide enterprise-grade reliability and quality of service. This allows us to interconnect directly with service providers, whether telcos or internet service providers. Direct peering (ASN to ASN) with over 200+ ISPs globally enables RingCentral to route around congested points of the network.

- **RingCentral Network Operations Center (NOC)**: Our NOC teams and dedicated engineering resources focus relentlessly on delivering quality of service with smart call routing and 24/7/365 quality metrics monitoring across all modes of communications. We conduct a full MOS score of every call and capture all relevant real-time data. Advanced analytics is then run on this data to ensure optimal performance, and routing metrics are adjusted to optimize for QoS, as needed. We build and maintain our own Host Media Processors and are consistently building technology around call improvement for any network conditions.

- HD media: To consistently deliver the highest HD quality possible, RingCentral employs the advanced Opus Interactive codec, as well as the wideband G.722 codec.

  HD voice with Opus codec is enabled by default on RingCentral apps, providing a better user experience with more clarity in HD voice, especially in limited bandwidth environments.

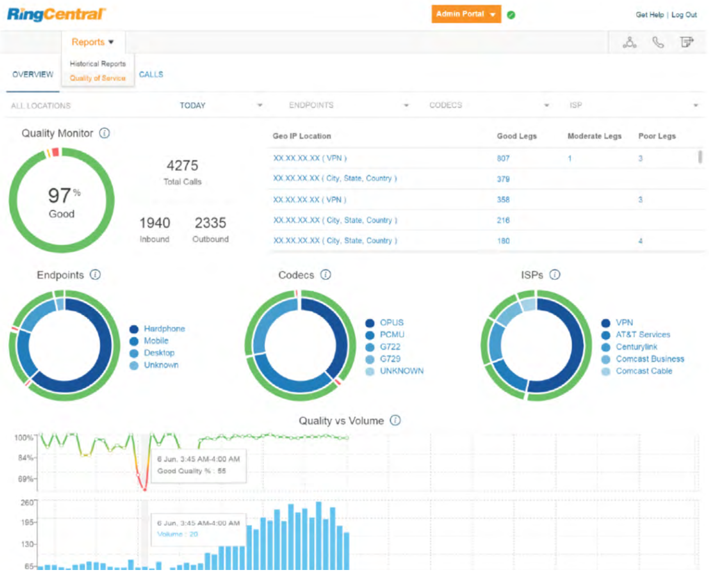
- QoS Analytics: RingCentral Quality of Service Analytics gives administrators access to key operational QoS metrics in near real time to monitor the global voice quality and to diagnose call quality issues impacting users.

  Our powerful reporting dashboard monitors voice quality and call volume at an aggregate organizational level. Administrators can also drill down into specific calls to identify specific call-quality information, including packet delay, jitter, and packet loss. This provides end-to-end visibility into network conditions, from one caller to RingCentral to the other caller and back. With this information, administrators can isolate potential problems affecting call quality for accurate resolution.

  Quality of Service Analytics can help administrators understand:

  - Overall quality of voice calls
  - Trends across regions, offices, and network providers
  - User experience for a particular group of users
  - Patterns in call quality over the course of a day due to overall call volume
  - How codecs perform against varying network issues

- **Professional Services:** Our Professional Services™ staff can help you set up, integrate, tailor, and extend your RingCentral service to meet specific business needs. Our site-preparedness and QoS guidelines help to get you up and running quickly by ensuring your network environment is properly configured to utilize our platform. As part of this exercise, we help conduct bandwidth analysis, make router and firewall recommendations, and assist with traffic prioritization efforts.



Geo IP Location	Good Legs	Moderate Legs	Poor Legs
XX.XX.XX.XX (VPN)	807	1	3
XX.XX.XX.XX (City, State, Country)	379		
XX.XX.XX.XX (VPN)	358		3
XX.XX.XX.XX (City, State, Country)	216		
XX.XX.XX.XX (City, State, Country)	180		4

Getting started

For more information on network connectivity, cloud communications and collaboration, and RingCentral's commitment to voice quality, visit ringcentral.com.

Appendix A – Microsoft Windows NetQos Policy

Microsoft Windows, by default, resets the DSCP value of all transmitted packets to BE (0). Special Operating System settings are required in order to allow properly marked packets to retain their DSCP value upon transmission. Once certain that the software clients are marking packets with the proper DSCP values follow these instructions (taken from Microsoft TechNet) to enable QoS Marking Pass-thru:

1. Enable the QoS Packet Scheduler Service.
2. Edit the Properties of the Network Connection on which you want to enable QoS Marking.
3. Ensure the connection uses "QoS Packet Scheduler" is checked.
4. Enable QoS pass-thru in registry.
5. Run regedit.exe as Administrator.
6. Open Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\QoS.
7. Edit (or add) REG_DWORD entry named "Do not use NLA" and set the value to 1.

Always test using Wireshark or some other packet capture/examination software to be sure that your applications are using and transmitting the correct DSCP values.

If they are not being set/transmitted correctly, use the following policy commands to force the correct markings on RingCentral soft client traffic:

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
markings on RingCentral soft client traffic:
#! DSCP Actions:
#! 10 - AF11 (Reserved for Customer Critical Markings)
#! 18 - AF21 (RingCentral traffic not otherwise classified)
#! 26 - AF31 (SIP Signaling Traffic)
#! 34 - AF41 (Video Real-Time Traffic)
#! 46 - EF (Voice Real-Time Traffic)
Remove-NetQosPolicy -Name RCMeetingOut _ 1 -Confirm:$false
Remove-NetQosPolicy -Name RCMeetingOut _ 2 -Confirm:$false
Remove-NetQosPolicy -Name RCMeetingOut _ 3 -Confirm:$false
Remove-NetQosPolicy -Name RCMeetingOut _ 4 -Confirm:$false
Remove-NetQosPolicy -Name RCMeetingOut _ 5 -Confirm:$false
Remove-NetQosPolicy -Name RCMeetingOut _ 6 -Confirm:$false
Remove-NetQosPolicy -Name RCMeetingOut _ 7 -Confirm:$false
```

```
New-NetQosPolicy -Name RCMeetingOut _ 1 -AppPathNameMatchCondition RingCentralMeetings.exe `
              -Precedence 127 -DSCPAction 26 -IPProtocolMatchCondition Both `
              -IPDstPortStartMatchCondition 3000 -IPDstPortEndMatchCondition 4000
New-NetQosPolicy -Name RCMeetingOut _ 2 -AppPathNameMatchCondition RingCentralMeetings.exe `
              -Precedence 127 -DSCPAction 26 -IPProtocolMatchCondition Both `
              -IPDstPortStartMatchCondition 5060 -IPDstPortEndMatchCondition 5061
New-NetQosPolicy -Name RCMeetingOut _ 4 -AppPathNameMatchCondition RingCentralMeetings.exe `
              -Precedence 127 -DSCPAction 26 -IPProtocolMatchCondition TCP `
              -IPDstPortMatchCondition 1702
New-NetQosPolicy -Name RCMeetingOut _ 5 -AppPathNameMatchCondition RingCentralMeetings.exe `
              -Precedence 127 -DSCPAction 34 -IPProtocolMatchCondition TCP `
              -IPDstPortMatchCondition 443
New-NetQosPolicy -Name RCMeetingOut _ 3 -AppPathNameMatchCondition RingCentralMeetings.exe `
              -Precedence 127 -DSCPAction 34 -IPProtocolMatchCondition Both `
              -IPDstPortMatchCondition 8801
New-NetQosPolicy -Name RCMeetingOut _ 6 -AppPathNameMatchCondition RingCentralMeetings.exe `
              -Precedence 127 -DSCPAction 46 -IPProtocolMatchCondition UDP `
              -IPDstPortStartMatchCondition 9000 -IPDstPortEndMatchCondition 10000
New-NetQosPolicy -Name RCMeetingOut _ 7 -AppPathNameMatchCondition RingCentralMeetings.exe `
              -Precedence 127 -DSCPAction 46 -IPProtocolMatchCondition UDP `
              -IPDstPortStartMatchCondition 5090 -IPDstPortEndMatchCondition 5099
#! Softphone.exe
Remove-NetQosPolicy -Name RCSPhoneOut _ 1 -Confirm:$false
Remove-NetQosPolicy -Name RCSPhoneOut _ 2 -Confirm:$false
Remove-NetQosPolicy -Name RCSPhoneOut _ 3 -Confirm:$false
Remove-NetQosPolicy -Name RCSPhoneOut _ 4 -Confirm:$false
Remove-NetQosPolicy -Name RCSPhoneOut _ 5 -Confirm:$false
Remove-NetQosPolicy -Name RCSPhoneOut _ 6 -Confirm:$false
Remove-NetQosPolicy -Name RCSPhoneOut _ 7 -Confirm:$false
New-NetQosPolicy -Name RCSPhoneOut _ 1 -AppPathNameMatchCondition Softphone.exe -DSCPAction 18 `
              -Precedence 127 -IPProtocolMatchCondition TCP -IPDstPortMatchCondition 80
New-NetQosPolicy -Name RCSPhoneOut _ 2 -AppPathNameMatchCondition Softphone.exe -DSCPAction 18 `
              -Precedence 127 -IPProtocolMatchCondition TCP -IPDstPortMatchCondition 443
New-NetQosPolicy -Name RCSPhoneOut _ 3 -AppPathNameMatchCondition Softphone.exe -DSCPAction 18 `
              -Precedence 127 -IPProtocolMatchCondition TCP -IPDstPortMatchCondition 636
New-NetQosPolicy -Name RCSPhoneOut _ 4 -AppPathNameMatchCondition Softphone.exe -DSCPAction 26 `
              -Precedence 127 -IPProtocolMatchCondition TCP -IPDstPortMatchCondition 5091
New-NetQosPolicy -Name RCSPhoneOut _ 5 -AppPathNameMatchCondition Softphone.exe -DSCPAction 26 `
              -Precedence 127 -IPProtocolMatchCondition TCP -IPDstPortMatchCondition 5097
New-NetQosPolicy -Name RCSPhoneOut _ 6 -AppPathNameMatchCondition Softphone.exe -DSCPAction 46 `
              -Precedence 127 -IPProtocolMatchCondition UDP `
              -IPDstPortStartMatchCondition 50000 -IPDstPortEndMatchCondition 59999
New-NetQosPolicy -Name RCSPhoneOut _ 7 -AppPathNameMatchCondition Softphone.exe -DSCPAction 46 `
              -Precedence 127 -IPProtocolMatchCondition UDP `
              -IPDstPortStartMatchCondition 60000 -IPDstPortEndMatchCondition 64999
New-NetQosPolicy -Name RCSPhoneOut _ 2 -AppPathNameMatchCondition Softphone.exe -DSCPAction 18 `
              -Precedence 127 -IPProtocolMatchCondition TCP -IPDstPortMatchCondition 443
New-NetQosPolicy -Name RCSPhoneOut _ 3 -AppPathNameMatchCondition Softphone.exe -DSCPAction 18 `
              -Precedence 127 -IPProtocolMatchCondition TCP -IPDstPortMatchCondition 636
New-NetQosPolicy -Name RCSPhoneOut _ 4 -AppPathNameMatchCondition Softphone.exe -DSCPAction 26 `
              -Precedence 127 -IPProtocolMatchCondition TCP -IPDstPortMatchCondition 5091
New-NetQosPolicy -Name RCSPhoneOut _ 5 -AppPathNameMatchCondition Softphone.exe -DSCPAction 26 `
              -Precedence 127 -IPProtocolMatchCondition TCP -IPDstPortMatchCondition 5097
New-NetQosPolicy -Name RCSPhoneOut _ 6 -AppPathNameMatchCondition Softphone.exe -DSCPAction 46 `
              -Precedence 127 -IPProtocolMatchCondition UDP `
              -IPDstPortStartMatchCondition 50000 -IPDstPortEndMatchCondition 59999
New-NetQosPolicy -Name RCSPhoneOut _ 7 -AppPathNameMatchCondition Softphone.exe -DSCPAction 46 `
              -Precedence 127 -IPProtocolMatchCondition UDP `
              -IPDstPortStartMatchCondition 60000 -IPDstPortEndMatchCondition 64999
#! Glip.exe
Remove-NetQosPolicy -Name RCGlipOut _ 1 -Confirm:$false
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 New-NetQosPolicy -Name RCGlipOut_1 -AppPathNameMatchCondition Glip.exe -DSCPAction 34 `
               -Precedence 127 -IPProtocolMatchCondition Both
 #! CustomerCritical.exe (fix program name to use)
 #! Duplicate as needed and increment trailing number
 Remove-NetQosPolicy -Name CustomerCritical_1 -Confirm:$false
 New-NetQosPolicy -Name CustomerCritical_1 -AppPathNameMatchCondition CustomerCritical_1.exe `
-DSCPAction 10 -Precedence 127 -IPProtocolMatchCondition Both
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

Appendix B – QoS policies for Cisco®

Access and Aggregation/Distribution Switches

The Access Switch must examine packets as they come in from user and WAP ports, determine their proper classification, set the appropriate DSCP value, and police the priority traffic to prevent a run-away process from harming the network. It has been determined empirically that a hard phone involved in a phone-initiated three-way conference call will require slightly less than 512 Kbps of real-time voice capacity in each direction. User's voice traffic destined to RingCentral and exceeding 512 Kbps will be dropped because it is not considered as meeting the specification.

Please note that cascading switches and hard phones on a port identified as a user port will drop valid voice traffic when multiple phones are in use simultaneously. Never cascade users/switches on a single user port. Always use a trunk port to feed another Access Switch to maintain control and QoS.

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
!=========================================================================
! QoS definitions for Access Switch ports to automatically mark all RC
! Traffic with appropriate DSCP markings as it ingresses a switch port.
!
! Critical hard phone traffic may already be marked but softphone and RC
! Meetings traffic is unmarked.
!=========================================================================
! Note: The following Prefixes/Acronyms are used in these scripts
!Prefixes are used in naming each entity to eliminate any possible
!confusion.
!--------------------------------------------------------------------
! ASW - Access or Aggregation Switch
! GEN - Switch or router (not specific to either)
! RTR - router or Layer3 Switch acting as a router
!
! ACL - Prefix and/or acronym for Access Control List
! CM - Prefix for Class Map definition
! PFX - Prefix List
! PM - Prefix for Policy Map
!
! In versions of IOS that support it, Object Groups can be used to
! massively reduce ACL complexity. They also provide ONE place where
! changes may be made.
!
! NOG – Network Object Group (where supported)
! SOG – Service Object Group (where supported)
!
! IB - Used to indicate Inbound traffic direction
! OB - Used to indicate Outbound traffic direction
! RC - Acronym standing for RingCentral
! RTP - Acronym standing for Real Time Priority
!
!--------------------------------------------------------------------
! Note: The following DSCP values are used in this document and are
! considered to be the default values for their purpose.
!
! EF (46) – Voice Real–Time Traffic
! AF41 (34) – Video Real–Time Traffic
! AF31 (26) – Signaling and Control
! AF21 (18) – All other RC traffic
! AF13 (14) – Customer Critical Traffic (must be defined)
! AF12 (12) – Customer Critical Traffic (must be defined)
! AF11 (10) – Customer Critical Traffic (must be defined)
! BE(0) – Best Effort
!
! Policy maps are provided for User, WAP, and Trunk ports.
!
! Please note that ALL trunk ports must be set to Trust QoS. This is
! The default on some switches, but not all. You must confirm for your
! Model and IOS release.
!
! If you are using the Microsoft Windows NetQosPolicy shown in
!
! Version 1.7, 20170922.0045Z Tim McKee
!--------------------------------------------------------------------
```

Use this Packet Matching syntax for iOS® versions that support object-groups

Object-groups are used to simplify Cisco Access Lists.Groups of addresses or service port tests allow for great simplification of the configuration. Object-groups are a Cisco feature that was introduced recently and may not be supported in your version of iOS.

```
!--------------------------------------------------------------------
! Define Access Lists to Identify and Classify traffic FROM users/WAPs
! going TO RingCentral.
!
! A hook has been included to allow classification of User Critical
! Traffic in 3 levels.
!--------------------------------------------------------------------
object-group network NOG-RingCentral
 description All RC Public Networks a/o 20170919
 103.44.68.0 255.255.252.0
 104.245.56.0 255.255.248.0
 185.23.248.0 255.255.252.0
 192.209.24.0 255.255.248.0
 199.255.120.0 255.255.252.0
 199.68.212.0 255.255.252.0
 208.87.40.0 255.255.252.0
 exit
!
object-group service SOG-RC-SIP
 description RC SIP service identifiers a/o 20170919
 tcp-udp source range 5060 6000
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 tcp-udp range 5060 6000
 exit
!
object-group service SOG-RC-SigMeeting
 description RC Meeting signaling service identifiers a/o 20170919
 tcp eq 5097
 exit
!
object-group service SOG-RC-RTPMeeting
 description RC Meeting RTP service identifiers a/o 20170919
 udp range 8801 8802
 udp eq 5091
 udp range 3478 3479
 exit
!
! All RC network traffic will be marked or premarked AF21/CS2 traffic
!
ip access-list extended ACL-ASW-IB-RC-Networks-All
 permit ip any any dscp af21
 permit ip any any dscp cs2
 permit ip any object-group NOG-RingCentral
!
! General SIP traffic or premarked AF31/CS3 traffic
!
ip access-list extended ACL-ASW-IB-RC-GeneralSIP
 permit ip any any af31
 permit ip any any cs3
permit object-group SOG-RC-SIP any object-group NOG-RingCentral
!
! Phone / Softphone voice RT traffic or premarked EF/CS5 traffic
!
ip access-list extended ACL-ASW-IB-RC-Voice-RTP
 permit ip any any dscp ef
 permit ip any any dscp cs5
 permit udp any object-group NOG-RingCentral range 9000 64999
!
! RC Meetings Signaling trafficor premaked AF31/CS3 traffic
!
ip access-list extended ACL-ASW-IB-RC-Meetings-Control
 permit ip any any dscp af31
 permit ip any any dscp cs3
 permit object-group SOG-RC-SigMeeting any object-group NOG-RingCentral
!
! RC Meetings Video RT traffic or premarked AF41/CS4 traffic
!
ip access-list extended ACL-ASW-IB-RC-Video-RTP
 permit ip any any dscp af41
 permit ip any any dscp cs4
 permit object-group SOG-RC-RTPMeeting any object-group NOG-RingCentral
!
! Customer Critical AF11 or premarked AF11 traffic
!
ip access-list ACL-ASW-IB-Cust-AF11
 remark Identify Customer Traffic for AF11 Classification
 permit ip any any dscp af11
 deny any any
!
! Customer Critical AF12 or premarked AF12 traffic
!
ip access-list ACL-ASW-IB-Cust-AF12
 remark Identify Customer Traffic for AF12 Classification
 permit ip any any dscp af12
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 deny any any
!
! Customer Critical AF13 or premarked AF12 traffic
!
ip access-list ACL-ASW-IB-Cust-AF13
 remark Identify Customer Traffic for AF13 Classification
 permit ip any any dscp af13
 deny any any
```

Use this Packet Matching syntax for iOS versions that do not support object-groups

```
!---------------------------------------------------------------------
! Define Access Lists to Identify and Classify traffic FROM users/WAPs
! going TO RingCentral.
!
! A hook has been included to allow classification of User Critical
! Traffic.
!---------------------------------------------------------------------
!
! All RC network traffic will be marked or AF21/CS2 traffic allowed
!
ip access-list extended ACL-RC-Networks-All
 permit ip any any dscp af21
 permit ip any any dscp cs2
 permit ip any 103.44.68.0 0.0.3.255
 permit ip any 104.245.56.0 0.0.7.255
 permit ip any 185.23.248.0 0.0.3.255
 permit ip any 192.209.24.0 0.0.7.255
 permit ip any 199.255.120.0 0.0.3.255
 permit ip any 199.68.212.0 0.0.3.255
 permit ip any 208.87.40.0 0.0.3.255
!
! General SIP traffic or premarked AF31/CS3 traffic
!
ip access-list extended ACL-ASW-IB-RC-GeneralSIP
 permit ip any any dscp af31
 permit ip any any dscp cs3
 permit tcp any 103.44.68.0 0.0.3.255 range 5060 6000
 permit udp any 103.44.68.0 0.0.3.255 range 5060 6000
 permit tcp any 104.245.56.0 0.0.7.255 range 5060 6000
 permit udp any 104.245.56.0 0.0.7.255 range 5060 6000
 permit tcp any 185.23.248.0 0.0.3.255 range 5060 6000
 permit udp any 185.23.248.0 0.0.3.255 range 5060 6000
 permit tcp any 192.209.24.0 0.0.7.255 range 5060 6000
 permit udp any 192.209.24.0 0.0.7.255 range 5060 6000
 permit tcp any 199.255.120.0 0.0.3.255 range 5060 6000
 permit udp any 199.255.120.0 0.0.3.255 range 5060 6000
 permit tcp any 199.68.212.0 0.0.3.255 range 5060 6000
 permit udp any 199.68.212.0 0.0.3.255 range 5060 6000
 permit tcp any 208.87.40.0 0.0.3.255 range 5060 6000
 permit udp any 208.87.40.0 0.0.3.255 range 5060 6000
!
! Phone / Softphone voice RT traffic or premarked EF/CS5 traffic
!
ip access-list extended ACL-ASW-IB-RC-Voice-RTP
 permit ip any any dscp ef
 permit ip any any dscp cs5
 permit udp any 103.44.68.0 0.0.3.255 range 9000 64999
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 permit udp any 104.245.56.0 0.0.7.255 range 9000 64999
 permit udp any 185.23.248.0 0.0.3.255 range 9000 64999
 permit udp any 192.209.24.0 0.0.7.255 range 9000 64999
 permit udp any 199.255.120.0 0.0.3.255 range 9000 64999
 permit udp any 199.68.212.0 0.0.3.255 range 9000 64999
 permit udp any 208.87.40.0 0.0.3.255 range 9000 64999
!
! RC Meetings Signaling traffic or premarked AF31/CS3 traffic
!
ip access-list extended ACL-ASW-IB-RC-Meetings-Control
 permit ip any any dscp af31
 permit ip any any dscp cs3
 permit tcp any 103.44.68.0 0.0.3.255 eq 5097
 permit tcp any 104.245.56.0 0.0.7.255 eq 5097
 permit tcp any 185.23.248.0 0.0.3.255 eq 5097
 permit tcp any 192.209.24.0 0.0.7.255 eq 5097
 permit tcp any 199.255.120.0 0.0.3.255 eq 5097
 permit tcp any 199.68.212.0 0.0.3.255 eq 5097
 permit tcp any 208.87.40.0 0.0.3.255 eq 5097
!
! RC Meetings Video RT traffic or premarked AF41/CS4 traffic
!
ip access-list extended ACL-ASW-IB-RC-Video-RTP
 permit ip any any dscp af41
 permit ip any any dscp cs4
 permit udp any 103.44.68.0 0.0.3.255 eq 5091
 permit udp any 103.44.68.0 0.0.3.255 eq 8801
 permit udp any 103.44.68.0 0.0.3.255 range 3478 3479
 permit udp any 104.245.56.0 0.0.7.255 eq 5091
 permit udp any 104.245.56.0 0.0.7.255 eq 8801
 permit udp any 104.245.56.0 0.0.7.255 range 3478 3479
 permit udp any 185.23.248.0 0.0.3.255 eq 5091
 permit udp any 185.23.248.0 0.0.3.255 eq 8801
 permit udp any 185.23.248.0 0.0.3.255 range 3478 3479
 permit udp any 192.209.24.0 0.0.7.255 eq 5091
 permit udp any 192.209.24.0 0.0.7.255 eq 8801
 permit udp any 192.209.24.0 0.0.7.255 range 3478 3479
 permit udp any 199.255.120.0 0.0.3.255 eq 5091
 permit udp any 199.255.120.0 0.0.3.255 eq 8801
 permit udp any 199.255.120.0 0.0.3.255 range 3478 3479
 permit udp any 199.68.212.0 0.0.3.255 eq 5091
 permit udp any 199.68.212.0 0.0.3.255 eq 8801
 permit udp any 199.68.212.0 0.0.3.255 range 3478 3479
 permit udp any 208.87.40.0 0.0.3.255 eq 5091
 permit udp any 208.87.40.0 0.0.3.255 eq 8801
 permit udp any 208.87.40.0 0.0.3.255 range 3478 3479
!
! Customer Critical AF11 or premarked AF11 traffic
!
ip access-list extended ACL-ASW-IB-Cust-AF11
 remark Identify Customer Traffic for AF11 Classification
 permit ip any any dscp af11
 deny ip any any
!
! Customer Critical AF12 or premarked AF12 traffic
!
ip access-list extended ACL-ASW-IB-Cust-AF12
 remark Identify Customer Traffic for AF12 Classification

 permit ip any any af12
 deny ip any any
!
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
! Customer Critical AF13 or premarked AF13 traffic
!
ip access-list extended ACL-ASW-IB-Cust-AF13
 remark Identify Customer Traffic for AF13 Classification
 permit ip any any dscp af11
 deny ip any any
```

Class-maps and policy-maps for all iOS versions

```
!--------------------------------------------------------------
! On switches that are MLS based (2960, 3560, 3750, etc) you must
! enable MLS QoS.  The following code will set things up properly.
!
mls qos map policed-dscp  0 24 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 1 2 4
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 46
mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22 25 32 34 36
mls qos srr-queue output dscp-map queue 2 threshold 1 38
mls qos srr-queue output dscp-map queue 2 threshold 2 24 26
mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
mls qos srr-queue output dscp-map queue 3 threshold 3 0
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 3 10 12 14
mls qos queue-set output 1 threshold 2 70 80 100 100
mls qos queue-set output 1 threshold 4 40 100 100 100
mls qos
!
!--------------------------------------------------------------
! Establish Class-Maps for matching User Port ingress traffic or
! WAP port ingress traffic
!
class-map match-any CM-ASW-IB-RC-GeneralSIP
 match access-group name ACL-ASW-IB-RC-GeneralSIP
!
class-map match-any CM-ASW-IB-RC-Phone-RTP
 match access-group name ACL-ASW-IB-RC-Phone-RTP
!
class-map match-any CM-ASW-IB-RC-Meetings-Control
 match access-group name ACL-ASW-IB-RC-Meetings-Control
!
class-map match-any CM-ASW-IB-RC-Video-RTP
 match access-group name ACL-ASW-IB-RC-Video-RTP
!
class-map match-any CM-ASW-IB-RC-Other
 match access-group name ACL-ASW-IB-RC-Networks-All
!
class-map match-any CM-ASW-IB-Cust-AF11
 match access-group name ACL-ASW-IB-Cust-AF11
!
class-map match-any CM-ASW-IB-Cust-AF12
 match access-group name ACL-ASW-IB-Cust-AF12

!
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
class-map match-any CM-ASW-IB-Cust-AF13
 match access-group name ACL-ASW-IB-Cust-AF13
!
!-----------------------------------------------------------------
! Create this Inbound QoS Markup/Police Policy for User or WAP
! Ports
!
! User ports are set to allow 512Kbps of voice RTP traffic (to

! allow for 3-way conferencing from the phone)
!
! WAP Ports are set to allow for up to 20 users.
!
! Policing of Cust classes is up to customer.
!
policy-map PM-ASW-IB-User
 class CM-ASW-IB-RC-Phone-RTP
  set ip dscp ef
  police 512000 16000 exceed-action drop
 class CM-ASW-IB-RC-Video-RTP
  set ip dscp af41
  police 756000 8000 exceed-action policed-dscp-transmit
 class CM-ASW-IB-RC-GeneralSIP
  set ip dscp af31
  police 32000 8000 exceed-action policed-dscp-transmit
 class CM-ASW-IB-RC-Meetings-Control
  set ip dscp af31
  police 32000 8000 exceed-action policed-dscp-transmit
 class CM-ASW-IB-RC-Other
  set ip dscp af21
 class CM-ASW-IB-Cust-AF13
  set ip dscp af13
 class CM-ASW-IB-Cust-AF12
  set ip dscp af12
 class CM-ASW-IB-Cust-AF11
  set ip dscp af11
 class class-default
  set ip dscp default
!
policy-map PM-ASW-IB-WAP
 class CM-ASW-IB-RC-Phone-RTP
  set ip dscp ef
  police 10240000 48000 exceed-action drop
 class CM-ASW-IB-RC-Video-RTP
  set ip dscp af41
  police 7560000 48000 exceed-action policed-dscp-transmit
 class CM-ASW-IB-RC-GeneralSIP
  set ip dscp af31
  police 512000 8000 exceed-action policed-dscp-transmit
 class CM-ASW-IB-RC-Meetings-Control
  set ip dscp af31
  police 512000 8000 exceed-action policed-dscp-transmit
 class CM-ASW-IB-RC-Other
  set ip dscp af21
 class CM-ASW-IB-Cust-AF13
  set ip dscp af13
 class CM-ASW-IB-Cust-AF12
  set ip dscp af12
 class CM-ASW-IB-Cust-AF11
  set ip dscp af11
 class class-default
  set ip dscp default
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

Application to switch ports

Policy maps must be applied to every user and WAP port to correctly establish QoS. When in doubt, apply a User policy to the port. Trunk ports need only be set to trust QoS.

```
!=============================================================================
!
! User ports
! use ‘mls qos trust dscp’ to set port to trusted mode if you are passing
! in marked traffic. Newer versions of IOS using MQC would be just
! ‘qos trust dscp’
!
! Please note that some models/versions may be trusted by default (WS-C3850,
! etc) while some require explicit trust configuration (WS-C2960, WS-C3750,
! etc).
!
!interface range Gi1/0/9-20
! mls qos trust dscp
! service-policy input PM-ASW-IB-User
!
!=============================================================================
!
! Wireless Access Point ports
! use ‘mls qos trust dscp’ to set port to trusted mode if you are passing
! in marked traffic. Newer versions of IOS using MQC would be just
! ‘qos trust dscp’
!
! Please note that some models/versions may be trusted by default (WS-C3850, etc)
! while some require explicit trust configuration (WS-C2960, WS-C3750, etc).
!
!interface Gi1/0/22
! mls qos trust dscp
! service-policy input PM-ASW-IB-WAP
!
!=============================================================================
!
! Trunk Ports
! use ‘mls qos trust dscp’ to set port to trusted mode. Newer versions
! of IOS using MQC would be just ‘qos trust dscp’
!
! All trunk ports must be set to trust dscp. Please note that some
! models/versions may be trusted by default (WS-C3850, etc) while some
! require explicit configuration (WS-C2960, WS-C3750, etc).
!
!interface Gi0/25
! mls qos trust dscp
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

Routers

Routers must examine packets as they come in from internet ISP ports, determine their proper classification, and set the appropriate DSCP value.

Object-groups are used to simplify Cisco Access Lists. Groups of addresses or service port tests allow for great simplification of the configuration. Object-groups are a Cisco feature that was introduced recently and may not be supported in your version of iOS.

```
!==========================================================================
! QoS Sample for Cisco routers
!
! Rev 20170919.1515Z
!==========================================================================

! Note: The following Prefixes/Acronyms are used in these scripts
!Prefixes are used in naming each entity to eliminate any possible
!confusion.

!---------------------------------------------------------------------
! ASW - Access or Aggregation Switch
! GEN - Switch or Router (not specific to either)
! RTR - Router or Layer3 Switch acting as a router
!
! ACL - Prefix and/or acronym for Access Control List

! CM -Prefix for Class Map definition
! PFX - Prefix List

! PM -Prefix for Policy Map
!
! In versions of IOS that support it, Object Groups can be used to
! massively reduce ACL complexity.They also provide ONE place where
! changes may be made.
!
! NOG - Network Object Group (where supported)
! SOG - Service Object Group (where supported)
!
! IB -Used to indicate Inbound traffic direction
! OB -Used to indicate Outbound traffic direction
! RC -Acronym standing for RingCentral
! RTP - Acronym standing for Real Time Priority
!
!---------------------------------------------------------------------
! Note: The following DSCP values are used in this document and are
!considered to be the default values for their purpose.
!
! EF (46) - Voice Real-Time Traffic
! AF41 (34) - Video Real-Time Traffic
! AF31 (26) - Signaling and Control
! AF21 (18) - All other RC traffic
! AF13 (14) - Customer Critical Traffic (must be defined)
! AF12 (12) - Customer Critical Traffic (must be defined)
! AF11 (10) - Customer Critical Traffic (must be defined)
! BE(0) - Best Effort
!
!==========================================================================
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

Classification of incoming ISP traffic

Use this Packet Matching syntax for iOS versions that support object-groups

```
!
object-group network NOG-RingCentral
 description All RingCentral Networks a/o 20170919
 103.44.68.0 255.255.252.0
 104.245.56.0 255.255.248.0
 185.23.248.0 255.255.252.0
 192.209.24.0 255.255.248.0
 199.255.120.0 255.255.252.0
 199.68.212.0 255.255.252.0
 208.87.40.0 255.255.252.0
 exit
!
object-group service SOG-RC-SIP
 description RingCentral SIP service identifiers a/o 20170919
 tcp-udp source range 5060 6000
 tcp-udp range 5060 6000
 exit
!
ip access-list extended ACL-RoutingProtocol
 permit udp any any eq rip
 permit udp any eq rip any
 permit eigrp any any
 permit ospf any any
 permit tcp any any eq bgp
 permit tcp any eq bgp any
!
! Phone / Softphone voice RT traffic
!
ip access-list extended ACL-RTR-IB-RC-Voice-RTP
 description RingCentral Voice Real-Time a/o 20170919
 permit udp object-group NOG-RingCentral range 9000 64999 any
!
! Meetings Video RT traffic
!
ip access-list extended ACL-RTR-IB-RC-Video-RTP
 description RingCentral Video Real-Time a/o 20170919
 permit udp object-group NOG-RingCentral any range 8801 8802
!
! General SIP traffic
!
ip access-list extended ACL-RTR-IB-RC-GeneralSIP
 description RingCentral SIP Signaling a/o 20170919
 permit object-group SOG-RC-SIP object-group NOG-RingCentral any
!
! All RC network traffic will be marked
!
ip access-list extended ACL-RTR-IB-RC-Networks-All
 description RingCentral ALL traffic a/o 20170919
 permit ip object-group NOG-RingCentral any
!
! Customer Critical AF11
!
ip access-list ACL-RTR-IB-Cust-AF11
 remark Identify Customer Traffic for AF11 Classification
 deny any any
!
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

Use this Packet Matching syntax for iOS versions that do not support object-groups

```
!
ip access-list extended ACL-RoutingProtocol
 permit udp any any eq rip
 permit udp any eq rip any
 permit eigrp any any
 permit ospf any any
 permit tcp any any eq bgp
 permit tcp any eq bgp any
!
! Phone/Softphone voice RT traffic
!
ip access-list extended ACL-RTR-IB-RC-Voice-RTP
 description RingCentral Voice Real-Time a/o 20170919
 permit udp 103.44.68.0 0.0.3.255 range 9000 64999 any
 permit udp 104.245.56.0 0.0.7.255 range 9000 64999 any
 permit udp 185.23.248.0 0.0.3.255 range 9000 64999 any
 permit udp 192.209.24.0 0.0.7.255 range 9000 64999 any
 permit udp 199.255.120.0 0.0.3.255 range 9000 64999 any
 permit udp 199.68.212.0 0.0.3.255 range 9000 64999 any
 permit udp 208.87.40.0 0.0.3.255 range 9000 64999 any
!
! Meetings Video RT traffic
!
ip access-list extended ACL-RTR-IB-RC-Video-RTP
 description RingCentral Video Real-Time a/o 20170919
 permit udp 103.44.68.0 0.0.3.255 any range 8801 8802
 permit udp 104.245.56.0 0.0.7.255 any range 8801 8802
 permit udp 185.23.248.0 0.0.3.255 any range 8801 8802
 permit udp 192.209.24.0 0.0.7.255 any range 8801 8802
 permit udp 199.255.120.0 0.0.3.255 any range 8801 8802
 permit udp 199.68.212.0 0.0.3.255 any range 8801 8802
 permit udp 208.87.40.0 0.0.3.255 any range 8801 8802
!
! General SIP traffic
!
ip access-list extended ACL-RTR-IB-RC-GeneralSIP
 description RingCentral SIP Signaling a/o 20170919
 permit udp 103.44.68.0 0.0.3.255 any range 5060 6000
 permit udp 104.245.56.0 0.0.7.255 any range 5060 6000
 permit udp 185.23.248.0 0.0.3.255 any range 5060 6000
 permit udp 192.209.24.0 0.0.7.255 any range 5060 6000
 permit udp 199.255.120.0 0.0.3.255 any range 5060 6000
 permit udp 199.68.212.0 0.0.3.255 any range 5060 6000
 permit udp 208.87.40.0 0.0.3.255 any range 5060 6000
 permit udp 103.44.68.0 0.0.3.255 range 5060 6000 any
 permit udp 104.245.56.0 0.0.7.255 range 5060 6000 any
 permit udp 185.23.248.0 0.0.3.255 range 5060 6000 any
 permit udp 192.209.24.0 0.0.7.255 range 5060 6000 any
 permit udp 199.255.120.0 0.0.3.255 range 5060 6000 any
 permit udp 199.68.212.0 0.0.3.255 range 5060 6000 any
 permit udp 208.87.40.0 0.0.3.255 range 5060 6000 any
 permit tcp 103.44.68.0 0.0.3.255 any range 5060 6000
 permit tcp 104.245.56.0 0.0.7.255 any range 5060 6000
 permit tcp 185.23.248.0 0.0.3.255 any range 5060 6000
 permit tcp 192.209.24.0 0.0.7.255 any range 5060 6000
 permit tcp 199.255.120.0 0.0.3.255 any range 5060 6000
 permit tcp 199.68.212.0 0.0.3.255 any range 5060 6000
 permit tcp 208.87.40.0 0.0.3.255 any range 5060 6000
 permit tcp 103.44.68.0 0.0.3.255 range 5060 6000 any
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 permit tcp 208.87.40.0 0.0.3.255 any range 5060 6000
 permit tcp 103.44.68.0 0.0.3.255 range 5060 6000 any
 permit tcp 104.245.56.0 0.0.7.255 range 5060 6000 any
 permit tcp 185.23.248.0 0.0.3.255 range 5060 6000 any
 permit tcp 192.209.24.0 0.0.7.255 range 5060 6000 any
 permit tcp 199.255.120.0 0.0.3.255 range 5060 6000 any
 permit tcp 199.68.212.0 0.0.3.255 range 5060 6000 any
 permit tcp 208.87.40.0 0.0.3.255 range 5060 6000 any
!
! All RC network traffic will be marked
!
ip access-list extended ACL-RTR-IB-RC-Networks-All
 description RingCentral ALL traffic a/o 20170919
 permit ip 103.44.68.0 0.0.3.255 any
 permit ip 104.245.56.0 0.0.7.255 any
 permit ip 185.23.248.0 0.0.3.255 any
 permit ip 192.209.24.0 0.0.7.255 any
 permit ip 199.255.120.0 0.0.3.255 any
 permit ip 199.68.212.0 0.0.3.255 any
 permit ip 208.87.40.0 0.0.3.255 any
!
! Customer Critical AF11
!
ip access-list ACL-RTR-IB-Cust-AF11
 remark Identify Customer Traffic for AF11 Classification
 deny any any
!
! Customer Critical AF12
!
ip access-list ACL-RTR-IB-Cust-AF12
 remark Identify Customer Traffic for AF11 Classification
 deny any any
!
! Customer Critical AF13
!
ip access-list ACL-RTR-IB-Cust-AF13
 remark Identify Customer Traffic for AF11 Classification
 deny any any
```

Class-maps and policy-maps for all iOS versions

```
!
! Define Inbound Class Maps for ISP circuits
!
class-map match-any CM-RTR-IB-RC-Voice-RT
 descriptionRingCentral Originated Traffic Voice RTP
 match access-group name ACL-RTR-IB-RC-Voice-RTP
!
class-map match-any CM-RTR-IB-RC-Video-RT
 descriptionRingCentral Originated Traffic Video RTP
 match access-group name ACL-RTR-IB-RC-Video-RTP
!
class-map match-any CM-RTR-IB-RC-SIP
 descriptionRingCentral SIP Traffic
 match access-group name ACL-RTR-IB-RC-GeneralSIP
!
class-map match-any CM-RTR-IB-RC-Other
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 description AllRingCentral Originated Traffic
 match access-group name ACL-RTR-IB-RC-Networks-All
!
class-map match-any CM-RTR-IB-Cust-AF11
 description Customer AF11 class traffic
 match access-group name ACL-RTR-IB-CustAF11
!
class-map match-any CM-RTR-IB-Cust-AF12
 description Customer AF12 class traffic
 match access-group name ACL-RTR-IB-CustAF12
!
class-map match-any CM-RTR-IB-Cust-AF13
 description Customer AF13 class traffic
 match access-group name ACL-RTR-IB-CustAF13
!
! Define Inbound Policy to apply for INPUT from ISP
!
policy-map PM-RTR-IB-Standard-QoS
 class CM-RTR-IB-RC-Voice-RT
  set dscp ef
 class CM-RTR-IB-RC-Video-RT
  set dscp af41
 class CM-RTR-IB-RC-SIP
  set dscp af31
 class CM-RTR-IB-RC-All
  set dscp af21
 class CM-RTR-IB-Cust-AF13
  set dscp af13
 class CM-RTR-IB-Cust-AF12
  set dscp af12
 class CM-RTR-IB-Cust-AF11
  set dscp af11
 class class-default
  set dscp default
!
!==============================================================
!
! Outbound Definitions
!
! It is assumed that by the time traffic reaches this point
! access switches and other intermediate devices have already
! remarked the DSCP tags appropriately.
!-----------------------------------------------------------
!
class-map match-any CM-GEN-OB-RT
 description Real-Time Traffic
 match ip dscp ef
 match ip precedence 5
!
class-map match-any CM-GEN-OB-Video
 description Interactive Video
 match ip dscp af41
 match ip precedence 4
 match access-group name ACL-RoutingProtocol
!
class-map match-any CM-GEN-OB-Signaling
 description Call-Signaling
 match ip dscp af31
 match ip precedence 3
!
class-map match-any CM-GEN-OB-RC-Other
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 description Elevated Priority
 match ip dscp af21
 match ip precedence 2
!
class-map match-any CM-GEN-OB-Cust-AF13
 match ip dscp af13
!
class-map match-any CM-GEN-OB-Cust-AF12
 match ip dscp af12
!
class-map match-any CM-GEN-OB-Cust-AF11
 match ip dscp af11
!
!---------------------------------------------------------------
! Standard Outbound QoS Policy
! Each class will rewrite the DSCP value for all packets that
! are part of the class into the standard value for that class.
! Must be a child of a shaping policy to be effective.
!
policy-map PM-GEN-OB-20-15-5-10
 class CM-GEN-OB-RT
  set dscp ef
  priority percent 20
 class CM-GEN-OB-Video
  set dscp af41
  bandwidth percent 15
 class CM-GEN-OB-Signaling
  set dscp af31
  bandwidth percent 5
 class CM-GEN-OB-RC-Other
  set dscp af21
  bandwidth percent 10
 class CM-GEN-OB-Cust-AF13
  set dscp af13
  bandwidth percent 5
 class CM-GEN-OB-Cust-AF12
  set dscp af12
  bandwidth percent 5
 class CM-GEN-OB-Cust-AF11
  set dscp af11
  bandwidth percent 5
 class class-default
  set dscp default
!
!-----------------------------------------------------------------
! Outbound QoS Policy to circuit peered with a RingCentral Data Center.
! Must be a child of a shaping policy to be effective. A peering
! link to RC will have higher percentages of traffic going to RC.
!
policy-map PM-OB-RCFeed-QoS
 class CM-OB-RT
  set dscp ef
  priority percent 75
 class CM-OB-Video
  set dscp af41
  bandwidth percent 10
 class CM-OB-Signaling
  set dscp af31
  bandwidth percent 9
 class CM-OB-Important
  set dscp af21
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
   bandwidth percent 5
  class class-default
   set dscp default
```

Applying to interfaces and shaping

```
! *******************************************************************
! * CRITICAL - Shaping *MUST* be applied to any circuit that operates*
! * at less than full physical link speed. This usually means *ALL* *
! * intersite links, ISP links, and may include others. Note that the *
! * ‘bandwidth’ element should also be set to the exact contracted *
! * value in the interface configuration.*
! **
! * Always reduce the bandwidth in the shaping statement to 5% less*
! * than the contracted capacity.*
! *******************************************************************
!
!=======================================================================
! Link toRingCentral Data Center
!
! Create shaping parent policy, set shaping average to 95% of the
! contracted data rate. You may use g, m, or k in the rate.
!
policy-map PM-RTR-OB-ToRC-100M
 class class-default
  service-policy PM-OB-RCFeed-QoS
!
! Apply shaping policy as outbound policy to interface.
! Apply standard QoS re-marking policy as inbound policy.
!
interface GigabitEthernet0/2
 description 100M link to RingCentral Vienna VA DataCenter
 bandwidth 100000
 priority-queue out
 service-policy out PM-RTR-OB-ToRC-100M
 service-policy in PM-RTR-IB-Standard-QoS
!
!=======================================================================
! Link to ISP
!
! Create shaping parent policy, set shaping average to 95% of the
! contracted data rate. You may use g, m, or k in the rate.
!
policy-map RM-RTR-OB-ToISP-100M
 class class-default
  shape average 95m
  service-policy PM-GEN-OB-20-15-5-10
!
! Apply shaping policy as outbound policy to interface.
! Apply standard QoS re-marking policy as inbound policy.
!
interface GigabitEthernet0/1
 description 100M link to an ISP
 bandwidth 100000
 priority-queue out
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 service-policy out PM-RTR-OB-ToISP-100M
 service-policy in PM-RTR-IB-Standard-QoS
!
!======================================================================
! All LAN/Trunk Links
!
! No inbound policy required so long as the interface trusts DSCP. All
! traffic should have been already marked with DSCP values by
! this point
!
interface GigabitEthernet0/0
 description Interior LAN/Trunk Interfaces
 priority-queue out
 service-policy out PM-RTR-OB-20-15-5-10
```

Applying to MetroEthernet (P2MP) and shaping per destination

A Metro-Ethernet is essentially a LAN that interconnects multiple sites over a carrier circuit. Each remote site may be fed with different bandwidths. Traffic going to each site must be individually shaped to match that site's contracted bandwidth. Access Lists are used to identify traffic going TO a site and to map it to a class

```
!-----------------------------------------------------------------
! Class Maps to identify individual sites. There MUST be exactly
! one per site. The Access list for the site must also be defined
! here.
!
! === Site3
ip access-list extended ACL-Site3
 permit ip any host 192.168.30.3
 permit ip any 10.200.3.0 0.0.0.255
 permit ip any 10.210.3.0 0.0.0.255
!
class-map match-any CM-Site3
 description Traffic destined for Site3
 match access-group name ACL-Site3
!
! === Site4
ip access-list extended ACL-Site4
 permit ip any host 192.168.30.4
 permit ip any 10.200.4.0 0.0.0.255
 permit ip any 10.210.4.0 0.0.0.255
!
class-map match-any CM-Site4
 description Traffic destined for Site4
 match access-group name ACL-Site4
!
! == repeat access-list and class-map for every site
!
!-----------------------------------------------------------------
! Outbound QoS Policy for Metro Ethernet Circuit. NOTE: This
! is a multi-tier QoS Shaping policy. Note that in the second level
! policy the class name CM-SiteX, X is the last octet of the
! 192.168.30.X MetroEthernet address.
!
! Each site must be shaped to 95% of it's own contracted data rate.
!-----------------------------------------------------------------
!
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
policy-map PM-RTR-OB-MetroE
 class CM-Site3
  shape average 9.5m
  service-policy PM-OB-20-25-5-10
 class CM-Site4
  shape average 190m
  service-policy PM-OB-20-20-5-10
!
! == repeat class, shape, and service-policy for every site
!
!
!-------------------------------------------------------------------
! Setup Access Link to the Metro-Ethernet
! This is essentially a point to multipoint TRUNK link, no input DSCP
! re-marking policy is needed as traffic will already be marked.
!-------------------------------------------------------------------
!
interface GigabitEthernet0/1
 description Link to Other sites via MetroEhernet
 ip address 192.168.30.1 255.255.255.0
 service-policy out PM-RTR-OB-MetroE
```

Applying to VLANs on a trunk

```
!
! Use the following in addition to that if a VLAN trunk (apply outbound to
! the physical trunk port. Modify based on other VLANS in trunk.
!
class-map CM-Vlan-ISP
 match vlan 999
!
class-map CM-Vlan31
 match vlan 31
!
policy-map PM-OB-MainTrunk
 class CM-Vlan-ISP
  shape average 95m
  service-policy PM-GEN-OB-20-15-5-10
 class CM-Vlan31
  shape average 895m
  service-policy PM-GEN-OB-20-15-5-10
!
policy-map PM-IB-MainTrunk
 class CM-Vlan-ISP
  service-policy PM-RTR-IB-Standard-QoS
!
!
interface GigabitEthernet0/0
 service-policy output PM-OB-MainTrunk
 service-policy input PM-IB-MainTrunk
 no shutdown
!
```

Appendix C – QoS policies for Juniper

Address Matches (RingCentral Network Prefix List)

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
edit policy-options prefix-list PFX-RC-Networks
 set 103.44.68.0/22
 set 104.245.56.0/21
 set 185.23.248.0/22
 set 192.209.24.0/21
 set 199.68.212.0/22
 set 199.255.120.0/22
 set 208.87.40.0/22
top
```

Forwarding Classes (Forwarding Class)

```
edit class-of-service forwarding-classes
 set class FC-Voice queue-num 7
 set class FC-Video queue-num 6
 set class FC-Signal queue-num 4
 set class FC-Important queue-num 2
 set class FC-BestEffort queue-num 0
top
edit class-of-service rewrite-rules dscp RWRL-RC-ReMark
 set forwarding-class FC-Voice loss-priority low code-point ef
 set forwarding-class FC-Voice loss-priority high code-point af41
 set forwarding-class FC-Video loss-priority low code-point af41
 set forwarding-class FC-Video loss-priority high code-point af41
 set forwarding-class FC-Signal loss-priority low code-point af31
 set forwarding-class FC-Signal loss-priority high code-point af31
 set forwarding-class FC-Important loss-priority low code-point af21
 set forwarding-class FC-Important loss-priority high code-point af21
 set forwarding-class FC-BestEffort loss-priority low code-point be
 set forwarding-class FC-BestEffort loss-priority high code-point be
top
# All interfaces must have re-mark rule applied
set class-of-service interfaces ge-0/0/* unit * rewrite-rules dscp RWRL-RC-ReMark
set class-of-service interfaces ae0 unit 0 rewrite-rules dscp RWRL-RC-ReMark
```

Input Classifiers (Standard User Ports)

```
edit firewall policer PLCR-UserVoice
 set filter-specific
 set if-exceeding bandwidth-limit 512k
 set if-exceeding burst-size-limit 64k
 set then discard
top
delete firewall family ethernet-switching filter FLTR-RC-IB-UserPort
edit firewall family ethernet-switching filter FLTR-RC-IB-UserPort
 set term TERM-EF from dscp [ ef cs5 ]
 set term TERM-EF then accept forwarding-class FC-Voice loss-priority low –
  policer PLCR-UserVoice
 set term TERM-EF then count us1-ef
 set term TERM-AF41 from dscp [ af41 cs4 ]
 set term TERM-AF41 then accept forwarding-class FC-Video loss-priority low
 set term TERM-AF41 then count us2-af41
 set term TERM-AF31 from dscp [ af31 cs3 ]
 set term TERM-AF31 then accept forwarding-class FC-Signal loss-priority low
 set term TERM-AF31 then count us3-af31
 set term TERM-AF21 from dscp af21
 set term TERM-AF21 then accept forwarding-class FC-Important loss-priority low
 set term TERM-AF21 then count us4-af21
 set term TERM-Phone-RT from protocol udp destination-port 9000-64999 –
  destination-prefix-list PFX-RC-Networks
 set term TERM-Phone-RT then accept forwarding-class FC-Voice loss-priority low –
  policer PLCR-UserVoice
 set term TERM-Phone-RT then count us1-ph-rt
 set term TERM-Meetings-RT from protocol udp destination-port 8801-8802 –
  destination-prefix-list PFX-RC-Networks
 set term TERM-Meetings-RT then accept forwarding-class FC-Video loss-priority low
 set term TERM-Phone-RT then count us1-ph-rt
 set term TERM-Meetings-RT from protocol udp destination-port 8801-8802 –
  destination-prefix-list PFX-RC-Networks
 set term TERM-Meetings-RT then accept forwarding-class FC-Video loss-priority low
 set term TERM-Meetings-RT then count us2-mt-rt
 set term TERM-Phone-Signal-udp from protocol udp destination-port 5060-6000 –
  destination-prefix-list PFX-RC-Networks
 set term TERM-Phone-Signal-udp then accept forwarding-class FC-Signal loss-priority low
 set term TERM-Phone-Signal-udp then count us3-phsg-udp
 set term TERM-Phone-Signal-tcp from protocol tcp destination-port 5060-6000 –
  destination-prefix-list PFX-RC-Networks
 set term TERM-Phone-Signal-tcp then accept forwarding-class FC-Signal loss-priority low
 set term TERM-Phone-Signal-tcp then count us3-phsg-tcp
 set term TERM-Meetings-Signal-tcp from protocol tcp destination-port 8801-8802 –
  destination-port 1720 destination-prefix-list PFX-RC-Networks
 set term TERM-Meetings-Signal-tcp then accept forwarding-class FC-Signal –
  loss-priority low
 set term TERM-Meetings-Signal-tcp then count us3-mtsg
 set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
 set term TERM-BE then count us9-be
# If you don’t trust the markings coming in you may deactivate the matching terms.
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 #deactivate term TERM-EF
 #deactivate term TERM-AF41
 #deactivate term TERM-AF31
top
edit interfaces interface-range IFR-Users
 # Alter membership to include all required ports
 set member-range ge-0/0/0 to ge-0/0/18
 set member [ ge-0/0/19 ge-0/0/20 ]
 set description UserPort
 edit unit 0 family ethernet-switching
  set port-mode access filter input FLTR-RC-IB-UserPort
  set VLAN members VLAN-User1
top
# Alter Voice VLAN ID as appropriate
set ethernet-switching-options voip interface IFR-Users VLAN VLAN-Lab2
set protocols rstp interface IFR-Users edge
set ethernet-switching-options bpdu-block interface IFR-Users shutdown
```

Wireless Access Point Trunking Ports

```
edit firewall policer PLCR-WAPVoice
 set filter-specific
 set if-exceeding bandwidth-limit 10240k
 set if-exceeding burst-size-limit 256k
 set then discard
top
delete firewall family ethernet-switching filter FLTR-RC-IB-WAPPort
edit firewall family ethernet-switching filter FLTR-RC-IB-WAPPort
 set term TERM-EF from dscp [ ef cs5 ]
 set term TERM-EF then accept forwarding-class FC-Voice loss-priority low –
  policer PLCR-WAPVoice
 set term TERM-EF then count wp1-ef
 set term TERM-AF41 from dscp [ af41 cs4 ]
 set term TERM-AF41 then accept forwarding-class FC-Video loss-priority low
 set term TERM-AF41 then count wp2-af41
 set term TERM-AF31 from dscp [ af31 cs3 ]
 set term TERM-AF31 then accept forwarding-class FC-Signal loss-priority low
 set term TERM-AF31 then count wp3-af31
 set term TERM-AF21 from dscp af21
 set term TERM-AF21 then accept forwarding-class FC-Important loss-priority low
 set term TERM-AF21 then count wp4-af21
 set term TERM-Phone-RT from protocol udp destination-port 9000-64999 –
  destination-prefix-list PFX-RC-Networks
 set term TERM-Phone-RT then accept forwarding-class FC-Voice loss-priority low –
  policer PLCR-UserVoice
 set term TERM-Phone-RT then count wp1-ph-rt
 set term TERM-Meetings-RT from protocol udp destination-port 8801-8802 –
  destination-prefix-list PFX-RC-Networks
 set term TERM-Meetings-RT then accept forwarding-class FC-Video loss-priority low
 set term TERM-Meetings-RT then count wp2-mt-rt
 set term TERM-Phone-Signal-udp from protocol udp destination-port 5060-6000 –
  destination-prefix-list PFX-RC-Networks
 set term TERM-Phone-Signal-udp then accept forwarding-class FC-Signal –
  loss-priority low
 set term TERM-Phone-Signal-udp then count wp3-phsg-udp
 set term TERM-Phone-Signal-tcp from protocol tcp destination-port 5060-6000 –
  destination-prefix-list PFX-RC-Networks
 set term TERM-Phone-Signal-tcp then accept forwarding-class FC-Signal –
  loss-priority low
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 set term TERM-Phone-Signal-tcp then count wp3-phsg-tcp
 set term TERM-Phone-Signal-tcp from protocol tcp destination-port 5060-6000 -
  destination-prefix-list PFX-RC-Networks
 set term TERM-Phone-Signal-tcp then accept forwarding-class FC-Signal -
  loss-priority low
 set term TERM-Phone-Signal-tcp then count wp3-phsg-tcp
 set term TERM-Meetings-Signal-tcp from protocol tcp destination-port 8801-8802 –
  destination-port 1720 destination-prefix-list PFX-RC-Networks
 set term TERM-Meetings-Signal-tcp then accept forwarding-class FC-Signal –
  loss-priority low
 set term TERM-Meetings-Signal-tcp then count wp3-mtsg
 set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
 set term TERM-BE then count wp9-be
 # If you don’t trust the markings coming in you may deactivate the matching terms.
 #deactivate term TERM-EF
 #deactivate term TERM-AF41
 #deactivate term TERM-AF31
top
edit interfaces interface-range IFR-WAPs
 # Alter membership to include all required ports
 set member ge-0/0/21
 set description “WAP Port”
 edit unit 0 family ethernet-switching
  set port-mode trunk filter input FLTR-RC-IB-WAPPort
  set VLAN members [ VLAN-User1 VLAN-Lab2 ]
top
# Alter Voice VLAN ID as appropriate
set ethernet-switching-options voip interface IFR-WAPs VLAN VLAN-Lab2
```

General Trunking Ports

```
# Adjust to the count of AE (trunk) devices required
set chassis aggregated-devices ethernet device-count 8
edit interfaces interface-range IFR-Uplink
 # Alter membership to include all required ports
 set member-range ge-0/0/22 to ge-0/0/23
 set description UpLinkPort
 set ether-options 802.3ad ae0
top
# Set names on physical ports
set interfaces ge-0/0/22 description switch-device-1
set interfaces ge-0/0/23 description switch-device-2
delete firewall family ethernet-switching filter FLTR-RC-TrunkPort
edit firewall family ethernet-switching filter FLTR-RC-TrunkPort
 set term TERM-EF from dscp [ ef cs5 ]
 set term TERM-EF then accept forwarding-class FC-Voice loss-priority low
 set term TERM-EF then count tr1-ef
 set term TERM-AF41 from dscp [ af41 cs4 ]
 set term TERM-AF41 then accept forwarding-class FC-Video loss-priority low
 set term TERM-AF41 then count tr2-af41
 set term TERM-AF31 from dscp [ af31 cs3 ]
 set term TERM-AF31 then accept forwarding-class FC-Signal loss-priority low
 set term TERM-AF31 then count tr3-af31
 set term TERM-AF21 from dscp af21
 set term TERM-AF21 then accept forwarding-class FC-Important loss-priority low
 set term TERM-AF21 then count tr4-af21
 set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 set term TERM-BE then count tr9-be
top
# Configure Aggregated Ethernet ports individually, repeat for each AE interface
set interfaces ae0 description us-celab-csw101-ae0
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 unit 0 family ethernet-switching port-mode trunk
set interfaces ae0 unit 0 family ethernet-switching VLAN members [ VLAN-User1 -
 VLAN-Voice2 VLAN-Lab3 VLAN-DMZ ]
set interfaces ae0 unit 0 family ethernet-switching filter input FLTR-RC-TrunkPort
```

ISP Inbound Ports

```
delete firewall family ethernet-switching filter FLTR-RC-IB-INetPort
edit firewall family ethernet-switching filter FLTR-RC-IB-INetPort
 set term TERM-EF from dscp [ ef cs5 ]
 set term TERM-EF then accept forwarding-class FC-Voice loss-priority low
 set term TERM-EF then count in1-ef
 set term TERM-AF41 from dscp [ af41 cs4 ]
 set term TERM-AF41 then accept forwarding-class FC-Video loss-priority low
 set term TERM-AF41 then count in2-af41
 set term TERM-AF31 from dscp [ af31 cs3 ]
 set term TERM-AF31 then accept forwarding-class FC-Signal loss-priority low
 set term TERM-AF31 then count in3-af31
 set term TERM-AF21 from dscp af21
 set term TERM-AF21 then accept forwarding-class FC-Important loss-priority low
 set term TERM-AF21 then count in4-af21
 set term TERM-Phone-RT from protocol udp source-port 9000-64999 -
  source-prefix-list PFX-RC-Networks
 set term TERM-Phone-RT then accept forwarding-class FC-Voice loss-priority low
 set term TERM-Phone-RT then count in1-ph-rt
 set term TERM-Meetings-RT from protocol udp destination-port 8801-8802 -
  source-prefix-list PFX-RC-Networks
 set term TERM-Meetings-RT then accept forwarding-class FC-Video loss-priority low
 set term TERM-Meetings-RT then count in2-mt-rt
 set term TERM-Phone-Signal-udp from protocol udp source-port 5060-6000 -
  source-prefix-list PFX-RC-Networks
 set term TERM-Phone-Signal-udp then accept forwarding-class FC-Signal -
  loss-priority low
 set term TERM-Phone-Signal-udp then count in3-phsg-udp
 set term TERM-Phone-Signal-tcp from protocol tcp source-port 5060-6000 -
  source-prefix-list PFX-RC-Networks
 set term TERM-Phone-Signal-tcp then accept forwarding-class FC-Signal -
  loss-priority low
 set term TERM-Phone-Signal-tcp then count in3-phsg-tcp
 set term TERM-Meetings-Signal-tcp from protocol tcp destination-port [ 8801-8802 -
  1720 ] source-prefix-list PFX-RC-Networks
 set term TERM-Meetings-Signal-tcp then accept forwarding-class FC-Signal -
  loss-priority low
 set term TERM-Meetings-Signal-tcp then count in3-mtsg
 set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
 set term TERM-BE then count in9-be
 # If you don’t trust the markings on inbound traffic deactivate these terms.
 deactivate term TERM-EF
 deactivate term TERM-AF41
 deactivate term TERM-AF31
top
edit interfaces interface-range IFR-ISP
 # Alter membership to include all required ports
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
 set member ge-0/0/23
 set description ISPPort
 edit unit 0 family ethernet-switching
  set port-mode access filter input FLTR-RC-IB-INetPort
top
set protocols rstp interface IFR-ISP edge
```

Schedulers (Voice RT Traffic – 20%/20%)

```
edit class-of-service schedulers SCH-EF-20
 set transmit-rate percent 20
 set buffer-size percent 20
 set priority strict-high
top
```

Schedulers (Voice RT Traffic – 40%/40%)

```
edit class-of-service schedulers SCH-EF-40
 set transmit-rate percent 40
 set buffer-size percent 40
 set priority strict-high
top
```

Voice RT Traffic – 75%/75%

```
edit class-of-service schedulers SCH-EF-75
 set transmit-rate percent 75
 set buffer-size percent 75
 set priority strict-high
top
```

Voice RT Traffic – 40%/40%

```
edit class-of-service schedulers SCH-AF41-40
 set transmit-rate percent 40
 set buffer-size percent 40
 set priority low
top
```

Video RT Traffic – 20%/20%

```
dit class-of-service schedulers SCH-AF41-20
 set transmit-rate percent 20
 set buffer-size percent 20
 set priority low
top
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

Video RT Traffic – 5%/5%

```
edit class-of-service schedulers SCH-AF41-5
 set transmit-rate percent 5
 set buffer-size percent 5
 set priority low
top
```

Signaling Traffic – 10%/10%

```
edit class-of-service schedulers SCH-AF31-10
 set transmit-rate percent 10
 set buffer-size percent 10
 set priority low
top
```

Priority Traffic – 10%/10%

```
edit class-of-service schedulers SCH-AF21-10
 set transmit-rate percent 10
 set buffer-size percent 10
 set priority low
top
```

Best Effort – Remainder

```
edit class-of-service schedulers SCH-BE
 set transmit-rate remainder
 set buffer-size remainder
 set priority low
top
```

Scheduler Maps – Standard

```
edit class-of-service scheduler-maps SMAP-OB-User
 set forwarding-class FC-Voice scheduler SCH-EF-20
 set forwarding-class FC-Video scheduler SCH-AF41-40
 set forwarding-class FC-Signal scheduler SCH-AF31-10
 set forwarding-class FC-Important scheduler SCH-AF21-10
 set forwarding-class FC-BestEffort scheduler SCH-BE
top
# All interfaces should have a scheduler-map applied to them
set class-of-service interfaces ge-0/0/* scheduler-map SMAP-OB-User
set class-of-service interfaces ae0 scheduler-map SMAP-OB-User
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

RC Feed for Direct Connection

```
edit class-of-service scheduler-maps SMAP-OB-RCFeed
 set forwarding-class FC-Voice scheduler SCH-EF-75
 set forwarding-class FC-Video scheduler SCH-AF41-5
 set forwarding-class FC-Signal scheduler SCH-AF31-10
 set forwarding-class FC-Important scheduler SCH-AF21-10
 set forwarding-class FC-BestEffort scheduler SCH-BE
top
# The interface used to connect directly to RingCentral using a dedicated circuit
# must use scheduler-map SMAP-OB-RCFeed
set class-of-service interfaces ge-0/1/1 scheduler-map SMAP-OB-RCFeed
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

Appendix D – QoS policies for FortiGate

Best practices for FortiGate configurations

- Never create a policy or base a reference on an individual interface, always use Zones. Create a Zone, even if it will only contain a single interface. This will enable you to shift/add/change interfaces without having to remove all the referencing items and put them back. It will also allow you to simplify the configuration because you won't have to replicate rules for each interface that is part of the Zone.
  Note that you can create dummy loopback interfaces to act as placeholders in Zones. This allows you to create Zones in anticipation of a need.
- Likewise, create Address Groups to use in lieu of individual address elements.

Case 1 – Traffic already policed and marked by Access Switches

Note: Use the highlighted lines *only* if you have enabled VDOM mode on your FortiGates.

Step 1: Use CLI to set up the FortiGate to utilize DSCP, establish queue priorities, and set outbound bandwidth on circuits DIRECTLY connected to WAN providers. Do NOT set outbound bandwidth on circuits if they feed WAN routers because the WAN router will be responsible for traffic shaping.

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
config global
    #
    # Set up to use DSCP
    #
    config system global
        set traffic-priority dscp
        set traffic-priority-level low
    end
    #
    # Set up DSCP priorities
    #
```

```
config system dscp-based-priority
        edit 46
        # EF
            set ds 46
            set priority high
        next
        edit 34
        # AF41
            set ds 34
            set priority medium
        next
        edit 26
        # AF31
set ds 26
            set priority medium
        next
    end
    #
    # set the outbound bandwidth on *EACH* WAN interface
    # specify the value in kilobits per second. The example shows 5.5Mbps.
    #
    config sys interface
        edit “wan1”
            set outbandwidth 5500
       next
    end
end
```

Step 2: Use the CLI to set up the SIP ALG parameters. Do this in each VDOM that sends voice traffic to RingCentral.

```
config vdom
    edit root
    #
    # Set up ALG Monitor ports
    #
    #
    config system settings
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
# VoIP settings are only available if Inspection mode is ”proxy.”
        set inspection-mode proxy

# Force ALG use in lieu of SIP Session Helper

        set default-voip-alg-mode proxy-based

        # The RC SIP proxy is normally on TCP\5090-5091

        # or UDP\5090-5091 or TCP-TLS\5096-5097

        # Note that the FortiGate ALG only supports one port for TLS

        set sip-tcp-port 5090 5091

        set sip-udp-port 5090 5091

        set sip-ssl-port 5096

    end
```

Step 3: Use the CLI to set up the following

```
config vdom

    edit root

#

# All communication with RingCentral occurs to a set of predefined public IP

# addresses. These are defined and placed in a convenient Address Group.

#

# Please change the associated interface to the name of your egress zone or

# interface.

#

config firewall address

    edit “ADR _ RingC _ 1”

        set associated-interface “ZN _ Outside”

        set subnet 103.44.68.0 255.255.252.0

    next

    edit “ADR _ RingC _ 2”

        set associated-interface “ZN _ Outside”

        set subnet 104.245.56.0 255.255.248.0

    next

    edit “ADR _ RingC _ 3”

        set associated-interface “ZN _ Outside”

        set subnet 185.23.248.0 255.255.252.0

    next

    edit “ADR _ RingC _ 4”

        set associated-interface “ZN _ Outside”

        set subnet 192.209.24.0 255.255.248.0
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
    next
edit “ADR _ RingC _ 5”
        set associated-interface “ZN _ Outside”
        set subnet 199.255.120.0 255.255.252.0
    next
    edit “ADR _ RingC _ 6”
        set associated-interface “ZN _ Outside”
        set subnet 199.68.212.0 255.255.252.0
    next
    edit “ADR _ RingC _ 7”
        set associated-interface “ZN _ Outside”
        set subnet 208.87.40.0 255.255.252.0
    next
    edit “ADR _ RingC _ 11”
         set associated-interface “ZN _ Outside”
         set type fqdn
         set fqdn “ringcentral.com”
    next
    edit “ADR _ RingC _ Prov _ 1”
         set associated-interface “ZN _ Outside”
         set type fqdn
         set fqdn “pp.ringcentral.com”
    next
edit “ADR _ RingC _ Prov _ 2”
         set associated-interface “ZN _ Outside”
         set type fqdn
         set fqdn “cp.ringcentral.com”
    next
    edit “ADR _ RingC _ Prov _ 3”
         set associated-interface “ZN _ Outside”
         set type fqdn
         set fqdn “yp.ringcentral.com”
    next
    edit “ADR _ RingC _ FwUp _ 1”
         set associated-interface “ZN _ Outside”
         set type fqdn
         set fqdn “pp.s3.ringcentral.com”
    next
    edit “ADR _ RingC _ API _ 1”
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
         set associated-interface “ZN _ Outside”
        set type fqdn
         set fqdn “platform.ringcentral.com”
    next
    edit “ADR _ RingC _ API _ 2”
         set associated-interface “ZN _ Outside”
         set type fqdn
         set fqdn “platform.devtest.ringcentral.com”
    next
#
# Define the convenient Address Groups
#
config firewall addrgrp
    edit “AG _ RingCentral _ All
        set member “ADR _ RingC _ 1” “ADR _ RingC _ 2” “ADR _ RingC _ 3” “ADR _ RingC _ 4” “ADR _ RingC _ 5” “ADR _
RingC _ 6” “ADR _ RingC _ 7” “ADR _ RingC _ Prov _ 1” “ADR _ RingC _ Prov _ 2” “ADR _ RingC _ Prov _ 3” “ADR _ RingC _ FwUp _ 1”
“ADR _ RingC _ API _ 1” “ADR _ RingC _ API _ 2”
    next
#
# Create a VoIP profile for RingCentral
#
config voip profile
    edit “VP _ RingCentral”
        config sip
            # enabling strict-register can cause issues since RC has
            # separate registrar from proxy
            set strict-register disable
            set open-via-pinhole enable
            set register-rate 50
            set invite-rate 50
     # force timeout after 100 seconds of silence
            set call-keepalive 100
            # idle after number of idle dialogs
            set max-idle-dialogs 200
            set malformed-request-line discard
            set malformed-header-via discard
            set malformed-header-from discard
            set malformed-header-to discard
            set malformed-header-call-id discard
            set malformed-header-cseq discard
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
            set malformed-header-rack discard
            set malformed-header-rseq discard
            set malformed-header-contact discard
            set malformed-header-record-route discard
            set malformed-header-route discard
            set malformed-header-expires discard
            set malformed-header-content-type discard
            set malformed-header-content-length discard
            set malformed-header-max-forwards discard
            set malformed-header-allow discard
            set malformed-header-p-asserted-identity discard
            set malformed-header-sdp-v discard
            set malformed-header-sdp-o discard
            set malformed-header-sdp-s discard
            set malformed-header-sdp-i discard
            set malformed-header-sdp-c discard
            set malformed-header-sdp-b discard
            set malformed-header-sdp-z discard
            set malformed-header-sdp-k discard
            set malformed-header-sdp-a discard
            set malformed-header-sdp-t discard
            set malformed-header-sdp-r discard
            set malformed-header-sdp-m discard
        end
    next
end
#
# Add the following policy rule. Adjust the source and destination interface
# names to your environment, then use the GUI to move this rule to the top of
# that interface pair section.
#
config firewall policy
    edit 0
        set name “RC _ SIP _ Outbound”
        set srcintf “ZN _ LAB”
set dstintf “ZN _ Outside”
        set srcaddr “all”
        set dstaddr “AG _ RingCentral”
        set action accept
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
        set schedule “always”
        set service “ALL”
        set utm-status enable
        set voip-profile “VP _ RingCentral”
        set ssl-ssh-profile “certificate-inspection”
        set nat enable
    next
end
end
```

Case 2 – Traffic fed to FortiGate unmarked

Note: Use the highlighted lines *only* if you have enabled VDOM mode on your FortiGates.

Step 1: Use CLI to set up the FortiGate to utilize DSCP, establish queue priorities, and set outbound bandwidth on circuits DIRECTLY connected to WAN providers. Do NOT set outbound bandwidth on circuits if they feed WAN routers because the WAN router will be responsible for traffic shaping.

```
config global
    #
    # Set up to use DSCP
    #
    config system global
        set traffic-priority dscp
        set traffic-priority-level low
    end
    #
    # Set up DSCP priorities
    #
    config system dscp-based-priority
        edit 46
        # EF
            set ds 46
            set priority high
        next
        edit 34
        # AF41
            set ds 34
            set priority medium
next
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
end
```

```
        edit 26
        # AF31
            set ds 26
            set priority medium
        next
    end
    #
    # set the outbound bandwidth on *EACH* WAN interface
    # specify the value in kilobits per second. The example shows 5.5Mbps.
    #
    config sys interface
        edit “wan1”
            set outbandwidth 5500
       next
    end
end
```

Step 2: Use the CLI to set up the SIP ALG parameters. Do this in each VDOM that sends voice traffic to RingCentral.

```
       config vdom
    edit root
    #
    # Set up ALG Monitor ports
    #
    #
    config system settings
        # VoIP settings are only available if Inspection mode is “proxy.”
        set inspection-mode proxy
        # Force ALG use in lieu of SIP Session Helper
        set default-voip-alg-mode proxy-based
        # The RC SIP proxy is normally on TCP\5090-5091
        # or UDP\5090-5091 or TCP-TLS\5096-5097
        # Note that the FortiGate ALG only supports one port for TLS
        set sip-tcp-port 5090 5091
        set sip-udp-port 5090 5091
        set sip-ssl-port 5096
    end
end
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

Step 3: Use the CLI to set up the following

```
config vdom
    edit root
#
# Create address objects for RFC1918 address space
# This is a very convenient element to have in your configuration
#
config firewall address
    edit “ADR_Private_10”
        set subnet 10.0.0.0 255.0.0.0
next
    edit “ADR_Private_172”
        set subnet 172.16.0.0 255.240.0.0
    next
    edit “ADR_Private_192”
        set subnet 192.168.0.0 255.255.0.0
    next
end
#
# Create an Address Group that includes ALL RFC1918 address space,
# again, it is very convenient to have in your configuration
#
config firewall addrgrp
    edit “AG_Private_ALL”
        set member “ADR_Private_10” “ADR_Private_172” “ADR_Private_192”
    next
end
#
# All communication with RingCentral occurs to a set of predefined public IP
# addresses. These are defined and placed in a convenient Address Group.
#
config firewall address
    edit “ADR_RingC_1”
        set associated-interface “ZN_Outside”
        set subnet 103.44.68.0 255.255.252.0
    next
    edit “ADR_RingC_2”
        set associated-interface “ZN_Outside”
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
        set subnet 104.245.56.0 255.255.248.0
    next
    edit “ADR _ RingC _ 3”
        set associated-interface “ZN _ Outside”
        set subnet 185.23.248.0 255.255.252.0
    next
edit “ADR _ RingC _ 4”
        set associated-interface “ZN _ Outside”
        set subnet 192.209.24.0 255.255.248.0
    next
edit “ADR _ RingC _ 5”
        set associated-interface “ZN _ Outside”
        set subnet 199.255.120.0 255.255.252.0
next
    edit “ADR _ RingC _ 6”
        set associated-interface “ZN _ Outside”
        set subnet 199.68.212.0 255.255.252.0
    next
    edit “ADR _ RingC _ 7”
        set associated-interface “ZN _ Outside”
        set subnet 208.87.40.0 255.255.252.0
    next
    edit “ADR _ RingC _ 11”
         set associated-interface “ZN _ Outside”
         set type fqdn
         set fqdn “ringcentral.com”
    next
    edit “ADR _ RingC _ Prov _ 1”
         set associated-interface “ZN _ Outside”
         set type fqdn
         set fqdn “pp.ringcentral.com”
    next
    edit “ADR _ RingC _ Prov _ 2”
         set associated-interface “ZN _ Outside”
         set type fqdn
         set fqdn “cp.ringcentral.com”
    next
    edit “ADR _ RingC _ Prov _ 3”
         set associated-interface “ZN _ Outside”
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
         set type fqdn
         set fqdn “yp.ringcentral.com”
    next
    edit “ADR _ RingC _ FwUp _ 1”
         set associated-interface “ZN _ Outside”
         set type fqdn
         set fqdn “pp.s3.ringcentral.com”
next
    edit “ADR _ RingC _ API _ 1”
         set associated-interface “ZN _ Outside”
         set type fqdn
         set fqdn “platform.ringcentral.com”
next
    edit “ADR _ RingC _ API _ 2”
         set associated-interface “ZN _ Outside”
set type fqdn
         set fqdn “platform.devtest.ringcentral.com”
    next
end
#
config firewall addrgrp
    edit “AG _ RingCentral”
        set member “ADR _ RingC _ 1” “ADR _ RingC _ 2” “ADR _ RingC _ 3” “ADR _ RingC _ 4” “ADR _ RingC _ 5” “ADR _
RingC _ 6” “ADR _ RingC _ 7”
    next
    edit “AG _ RingC _ Prov”
        set member “ADR _ RingC _ Prov _ 1” “ADR _ RingC _ Prov _ 2” “ADR _ RingC _ Prov _ 3”
    next
    edit “AG _ RingC _ FwUp”
        set member “ADR _ RingC _ FwUp _ 1”
    next
    edit “AG _ RingC _ API”
        set member “ADR _ RingC _ API _ 1” “ADR _ RingC _ API _ 2”
    next
end
#
# Define ports for RingCentral
#
config firewall service custom
    edit “SVC _ RingC _ SIP”
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
        set category “VoIP, Messaging & Other Applications”
        set tcp-portrange 5090-5091 5096-5097
        set udp-portrange 5090-5091
   next
    edit “SVC _ RingC _ Prov”
        set category “VoIP, Messaging & Other Applications”
        set tcp-portrange 443
    next
    edit “SVC _ RingC _ FwUp”
        set category “VoIP, Messaging & Other Applications”
        set tcp-portrange 443
    next
    edit “SVC _ RingC _ Pres”
        set category “VoIP, Messaging & Other Applications”
        set tcp-portrange 80 443
   next
    edit “SVC _ RingC _ API”
set category “VoIP, Messaging & Other Applications”
 set tcp-portrange 443
    next
    edit “SVC _ RingC _ Mtg”
        set category “VoIP, Messaging & Other Applications”
        set tcp-portrange 443 8801-8802
        set udp-portrange 3478-3479 8801-8810
    next
end
#
config voip profile
    edit “VP _ RingCentral”
        config sip
            # enabling strict-register can cause issues since RC has
            # separate registrar from proxy
            set strict-register disable
            set open-via-pinhole enable
            set register-rate 10
            set invite-rate 10
            # force timeout after 100 seconds of silence
           set call-keepalive 100
            # idle after number of idle dialogs
            set max-idle-dialogs 200
            set malformed-request-line discard
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
            set malformed-header-via discard
            set malformed-header-from discard
            set malformed-header-to discard
            set malformed-header-call-id discard
            set malformed-header-cseq discard
            set malformed-header-rack discard
            set malformed-header-rseq discard
            set malformed-header-contact discard
            set malformed-header-record-route discard
            set malformed-header-route discard
            set malformed-header-expires discard
            set malformed-header-content-type discard
            set malformed-header-content-length discard
            set malformed-header-max-forwards discard
            set malformed-header-allow discard
            set malformed-header-p-asserted-identity discard
            set malformed-header-sdp-v discard
            set malformed-header-sdp-o discard
            set malformed-header-sdp-s discard
            set malformed-header-sdp-i discard
            set malformed-header-sdp-c discard
            set malformed-header-sdp-b discard
      set malformed-header-sdp-z discard
            set malformed-header-sdp-k discard
            set malformed-header-sdp-a discard
            set malformed-header-sdp-t discard
            set malformed-header-sdp-r discard
            set malformed-header-sdp-m discard
        end
    next
end
#
# Create Traffic Shapers to control VoIP and Video traffic
# guaranteed and maximum bandwidth is in Kbps and should be adjusted
# to match site requirements. Maximum is not required, but can be
# used to prevent taking over the entire circuit.
#
config firewall shaper traffic-shaper
    edit TS _ VoIP
        set maximum-bandwidth 1000
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
        set guaranteed-bandwidth 800
        set per-policy disable
        set priority high
   next
    edit TS _ Video
        set maximum-bandwidth 1000
        set guaranteed-bandwidth 800
        set per-policy disable
        set priority high
    next
end
#
# Create firewall policies for *each* outbound interface pair that will
# carry RingCentral traffic. Keep these in the same order, but use the
# GUI to move them to the top of each interface pair. Make sure to
# adjust the srcintf and dstintf names. Replicate the entire section
# for each interface pair.
#
config firewall policy
    edit 0
        set name “RC _ Prov”
        set srcintf “ZN _ LAB”
        set dstintf “ZN _ Outside”
        set srcaddr “all”
        set dstaddr “AG _ RingC _ Prov”
        set action accept
        set schedule “always”
        set service “SVC _ RingC _ Prov”
        set utm-status enable
       set ssl-ssh-profile “certificate-inspection”
        set nat enable
    next
    edit 0
        set name “RC _ FW _ Update”
        set srcintf “ZN _ LAB”
        set dstintf “ZN _ Outside”
        set srcaddr “all”
        set dstaddr “AG _ RingC _ FwUp”
        set action accept
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

```
        set schedule “always”
        set service “SVC _ RingC _ FwUp”
        set utm-status enable
        set ssl-ssh-profile “certificate-inspection”
        set nat enable
    next
    edit 0
        set name “RC _ API”
        set srcintf “ZN _ LAB”
        set dstintf “ZN _ Outside”
        set srcaddr “all”
        set dstaddr “AG _ RingC _ API”
        set action accept
        set schedule “always”
        set service “SVC _ RingC _ API”
        set utm-status enable
        set ssl-ssh-profile “certificate-inspection”
        set nat enable
    next
    edit 0
        set name “RC _ Meeting _ Web”
        set srcintf “ZN _ LAB”
        set dstintf “ZN _ Outside”
        set srcaddr “all”
        set dstaddr “AG _ RingCentral”
        set action accept
        set schedule “always”
        set service “SVC _ RingC _ Mtg _ Web”
        set utm-status enable
        set ssl-ssh-profile “certificate-inspection”
        set nat enable
    next
    edit 0
        set name “RC _ Meeting _ Web”
        set srcintf “ZN _ LAB”
        set dstintf “ZN _ Outside”
        set srcaddr “all”
        set dstaddr “AG _ RingCentral”
        set action accept
        set schedule “always”
        set service “SVC _ RingC _ Mtg _ Web”
        set utm-status enable
        set ssl-ssh-profile “certificate-inspection”
        set nat enable
    next
    edit 0
        set name “RC_Meeting”
        set srcintf “ZN_LAB”
        set dstintf “ZN_Outside”
        set srcaddr “all”
        set dstaddr “AG_RingCentral”
        set action accept
        set schedule “always”
        set service “SVC_RingC_Mtg”
        set utm-status enable
        set ssl-ssh-profile “certificate-inspection”
        set nat enable
        set traffic-shaper TS_Video
        set traffic-shaper-reverse TS_Video
    next
    edit 0
        set name “RC_SIP_Outbound”
        set srcintf “ZN_LAB”
        set dstintf “ZN_Outside”
        set srcaddr “all”
        set dstaddr “AG_RingCentral”
        set action accept
        set schedule “always”
        set service “SVC_RingC_SIP”
        set utm-status enable
        set voip-profile “VP_RingCentral”
        set ssl-ssh-profile “certificate-inspection”
        set nat enable
 set traffic-shaper TS_VoIP
 set traffic-shaper-reverse TS_VoIP
    next
end
end
```

Appendices are constantly being updated, please ask your Sales Rep for the latest copy.

For more information, please contact a sales representative. Visit ringcentral.com or call 855-774-2510.

RingCentral, Inc. (NYSE:RNG) is a leading provider of global enterprise cloud communications and collaboration solutions. More flexible and cost-effective than legacy on-premises systems, RingCentral empowers today's mobile and distributed workforce to communicate, collaborate, and connect from anywhere, on any device. RingCentral unifies voice, video, team messaging and collaboration, conferencing, online meetings, and integrated contact center solutions. RingCentral's open platform integrates with leading business apps and enables customers to easily customize business workflows. RingCentral is headquartered in Belmont, California, and has offices around the world.

RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002. ringcentral.com