Quality of Service in Enterprise Networks

Background

Why is it critical when connecting an Enterprise Network to a Cloud Based Voice Service?

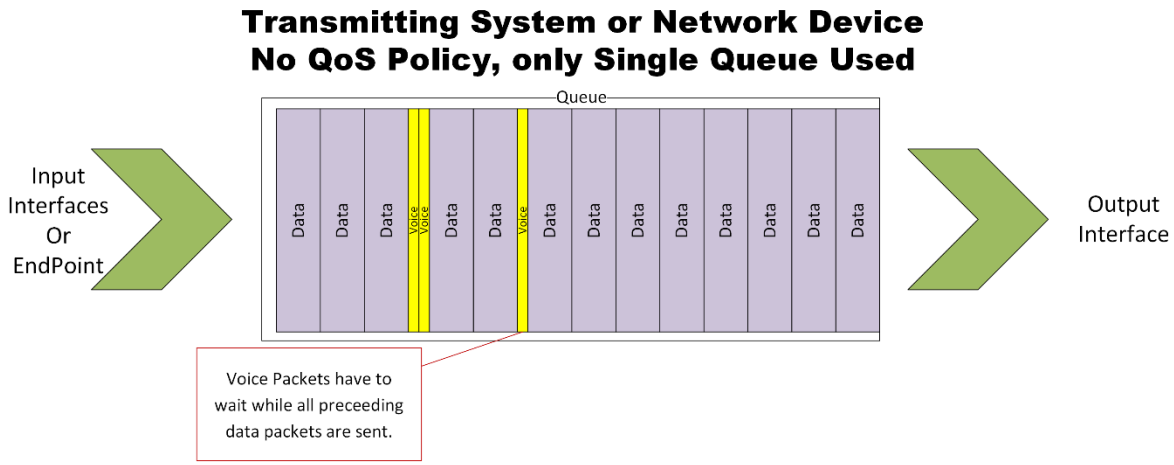
Cloud based voice service, or Voice over IP in general, can be extremely cost-effective for the Enterprise. Enterprise customers embrace the Return on Investment (RoI) potential of the technology, execute small Proof-of-Concept (PoC) tests successfully, then opt for large-scale rollouts which may operate 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.

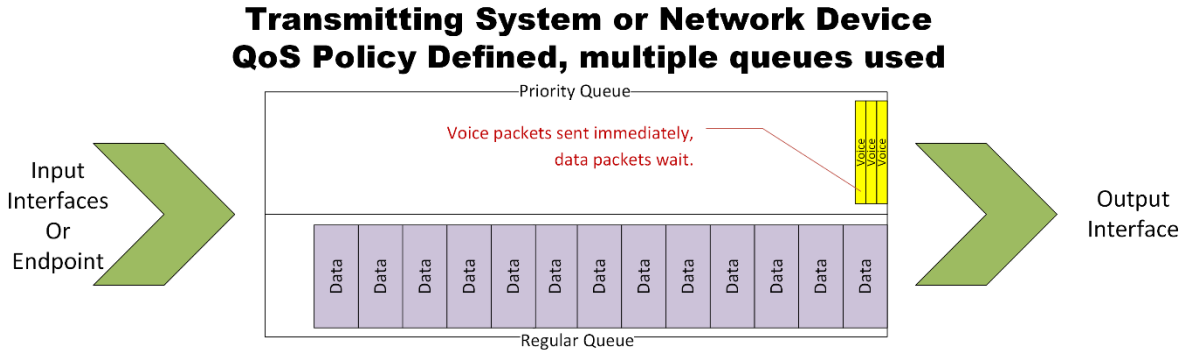
Problem Causes

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 buffered 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 'drop-out'.



A proper QoS policy buffers output traffic using multiple data queues, at least one being a 'priority' hardware queue from which packets are always taken and transmitted in the next available slot. The QoS policy will take data packets which have been classified as voice packets and insert them in the priority queue. Priority traffic will always 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.)*



2. The Wide-Area Network (WAN) link that carries traffic to/from the Internet or between offices can experience 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 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?

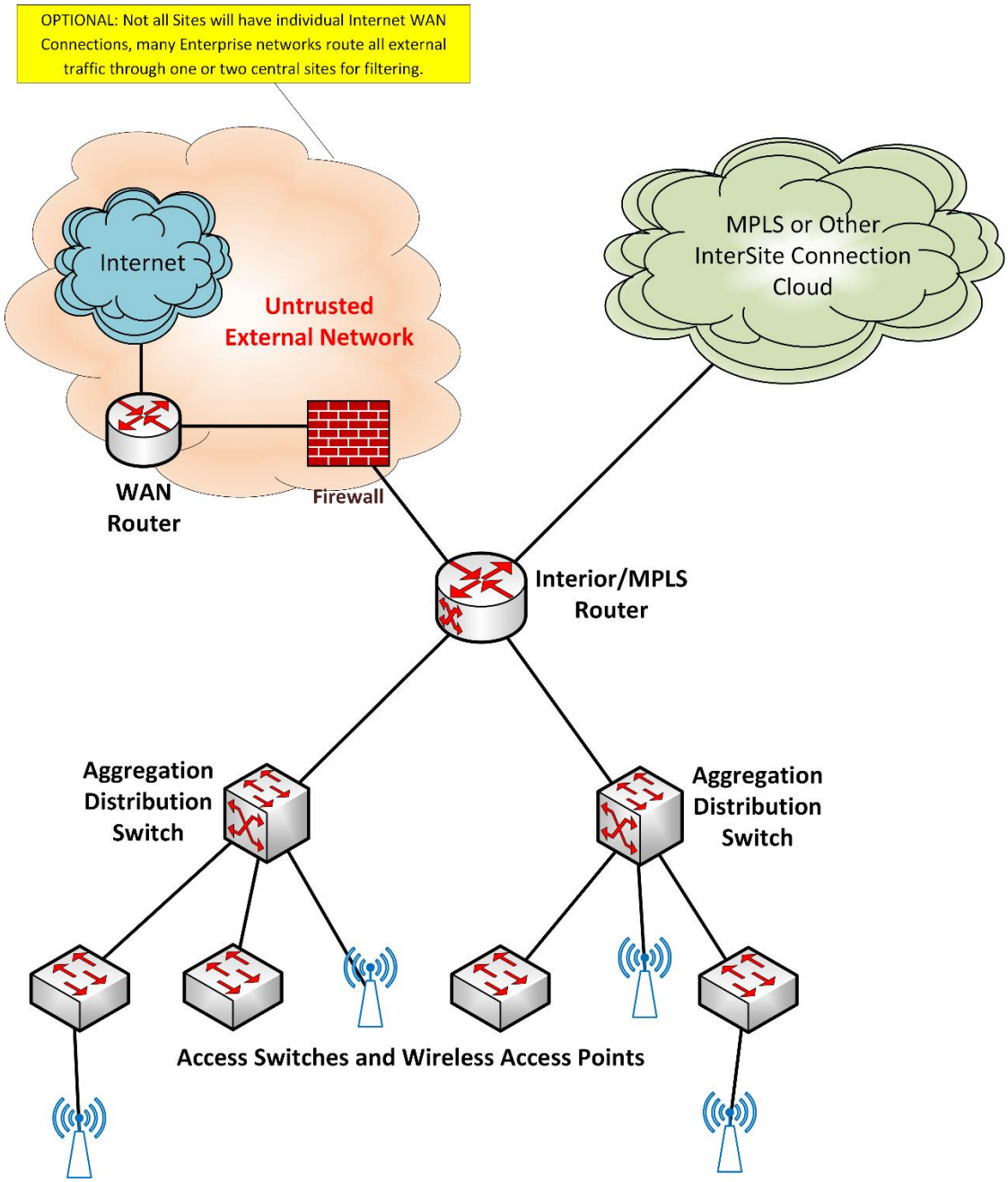
Normal network monitoring tools check traffic levels at large preset intervals, usually 1 minute (60 seconds) or 5 minutes (300 seconds). They also apply algorithms that effectively average the measured traffic flow over relatively long periods of time. A 10 second burst of heavy traffic can result in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

Enterprise Network Topology

An enterprise network absolutely ***must*** have a carefully planned QoS set up 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 or branch offices):

1. ***Endpoint Devices*** – Computers, phones, softphones, video conference devices, etc.

2. ***Access Switches*** – Provide connectivity to computers, phones, and access points.
3. ***Wireless Access Points (WAPs)*** – Provide connectivity to wireless users. They function like an access switch, but have different QoS mechanisms.
4. ***Aggregation / Distribution Switches*** – Aggregates the traffic from multiple access switches and/or WAPs.
5. ***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***.
6. ***Firewalls*** – Provide access control to allow only preapproved traffic flows.
7. ***WAN Routers*** – Provide access to the Internet or private carrier network(s).



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 if needed. (This is particularly critical when you

consider that Microsoft Windows strips out all DSCP markings, changing them to zero and rendering softphone traffic indistinguishable from web traffic.)
2. Police the data input stream so that a misbehaving endpoint cannot 'take over' the network.
3. Prioritize traffic exiting the corporate network to Users / Phones and ensure that Voice traffic is expedited.
4. Inspect the traffic entering the corporate network from Wireless Access Points (WAPs) and re-mark the DSCP tags as needed.
5. Merge traffic from multiple user / phone devices into composite 'trunk' connections that are fed to upstream to Aggregation / Distribution Switches.

The ports on Access Switches generally belong to the following 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 software VoIP phone application in addition to or in lieu of a hardware VoIP phone. Real-time data streams ingressing a User Port should be policed to a maximum of 500Kbps of Real-time audio.
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 may 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 often 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 required. Some Wireless Access Points do not have the capability to alter traffic DSCP tags and will require the upstream switch to perform the re-marking task.
3. Merge traffic from multiple mobile devices and WiFi 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 connected to Access Switches to reduce the complexity 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 trunk ports 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 often 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 Switch*** or a ***Core Router***. Some very large Enterprises have ***Site Switches*** or ***Site Routers*** in addition to Core devices.

Interior Routers that utilize external circuits to extend the customer network to other locations ***must*** also include QoS shaping policies to smooth traffic and ensure that traffic flowing from the router toward the external circuit does not exceed the contracted traffic rates of the circuit.

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. If this is not possible, you must enable QoS and Shaping functionality in the firewall. Please see the Appendices regarding vendor specific firewall QoS configurations for interoperation with Ring Central.

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 and support QoS prioritization. It must also be capable of re-marking the DSCP values of return traffic.

Quality of Service

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 decimal value (0 – 63) with each data packet. This value is called the DSCP value. It can be used by network devices to prioritize packet flow 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

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

DSCP / ToS Tagging

The universally defined and accepted DSCP values / names are shown in the following table:

DSCP Value	Decimal	Name	Drop Probability	IP Precedence
111 000	56	CS7		7
110 000	48	CS6		6
101 110	46	EF	N/A	5
101 000	40	CS5		5
100 110	38	AF43	High	4
100 100	36	AF42	Medium	4
100 010	34	AF41	Low	4
100 000	32	CS4		4
011 110	30	AF33	High	3
011 100	28	AF32	Medium	3
011 010	26	AF31	Low	3
011 000	24	CS3		3
010 110	22	AF23	High	2

DSCP Value	Decimal	Name	Drop Probability	IP Precedence
011 100	20	AF22	Medium	2
010 010	18	AF21	Low	2
010 000	16	CS2		2
001 110	14	AF13	High	1
001 100	12	AF12	Medium	1
001 010	10	AF11	Low	1
001 000	8	CS1		1
000 000	0	BE (Best Effort)	N/A	0

The values normally used for RingCentral communication services are highlighted in yellow.

DSCP EF (46) is normally used to mark real-time voice media. Standard VoIP implementations send one data packet every 20 milliseconds or 50 packets every second – some encoding schemes allow for these parameters to be changed. Most VoIP phones and PBXs use a 'jitter buffer' of 40-100 milliseconds to allow for packets to be variably delayed in transit. Delay of a packet by more than the size of the jitter buffer results in dropped packets which sounds to the end user as gaps in audio or garbled speech. This makes it critical to ensure that these packets all 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 and loss, but not to the same extent as voice traffic.

DSCP AF31 (26) is normally used to mark UDP and TCP SIP traffic used for control, registration, and signaling – call setup and teardown. This traffic is important and must be guaranteed but is relatively insensitive to jitter. (Note: Cisco uses DSCP CS3 [24] for this purpose.)

DSCP AF21 (18) is to mark all other RingCentral traffic. This traffic is not sensitive to jitter.

Traffic Ingress Re-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 packet re-marking.

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

1. Internet connections – Many Internet Service Providers (ISPs) alter the DSCP value to a different value than required for media traffic using in VoIP and video communication, often setting the field to the value of Best Effort traffic (BE). Some firewalls / WAN routers will automatically mark return traffic with the same DSCP value as the outgoing connection. If it doesn't, a QoS policy must examine the data packets, determine their type of traffic, 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).

2. WAP Ports – The status of DSCP markings in WAP traffic is vendor dependent. Some (very few) WAP vendors provide a DSCP re-marking mechanism. You should take great effort to force wireless clients to properly mark traffic as it is generated. The WAP looks at the DSCP value on traffic upon ingress to determine handling rules. Voice traffic that is not marked properly will not be handled correctly and voice quality may be degraded under load.
3. 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 & 10 based computers to enable proper transmission of DSCP values upstream. A sample of such policies is given in Appendix A.

Re-marking ingress policies for certain vendors' switches and routers are given in the Appendices. Please note that many soft clients do not generate the correct markings. It is best to use the Group Policy or NetQosPolicy on Windows computers. If not possible, you should 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.

Please note that DSCP marking of soft client / mobile client traffic in RingCentral applications is disabled by default. You must ask your RingCentral account representative or system engineer to enable it.

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 faster than 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 technique is called *'traffic shaping'*. Traffic Shaping constitutes delaying and/or discarding selected traffic so that the output rate to a carrier never exceeds a set data rate. The selection of traffic to be delayed or discarded should be based upon QoS parameters. Traffic should be shaped to an average value of 95% of the contracted data rate.

Some carriers offer a service whereby a customer can 'burst' to higher data rates at times when bandwidth is available. This type of service should NEVER be used unless the carrier can *guarantee* that DSCP tagged traffic will NOT EVER be dropped. A router or firewall has no way of knowing what traffic level the carrier is willing to accept at any given point in time and can't dynamically alter the shaping bandwidth setting.

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 vendor devices are given in the Appendices.

MPLS & QoS

Many carriers offer MPLS Data connections. This can be thought of as an E-LAN (any to any) Ethernet service but with the carrier's Layer-3 intelligence and control in the middle of the network. This can provide a great deal of flexibility.

MPLS networks are composed of 3 router node categories.

- **'P' nodes** form the backbone of the carrier network. These nodes are generally very high speed MPLS only routers. They connect only to other 'P' nodes or to Provider Edge ('PE') nodes.
- **'PE' nodes** form the interface between the MPLS network and the Customer network.
- **'CE' nodes** connect to the MPLS provider 'PE' nodes. They are part of the end-customer's logical network. Some MPLS providers (AT&T and Verizon) require managed customers utilize carrier provided and managed 'CE node' routers. Some carriers allow for the customer or RingCentral to terminate the MPLS link and provide the 'CE node' service.

MPLS carriers offer a variety of QoS policies. Most policies support four and/or six 'Class of Service' (CoS) subgroupings. The highest priority level (lowest numbered) CoS group is for DSCP EF (Voice Real-time) traffic. The lowest priority level (highest numbered) CoS group is for all otherwise unclassified traffic and is Best-Effort. The carriers have a variety of policy/CoS setups with varying levels of traffic apportioned between CoS groups within the policy. Data Packets are classified based upon several criteria and assigned to a CoS group. The CoS group will be given a minimum of the amount of bandwidth specified for that CoS group. Leftover bandwidth is apportioned between all non-realtime CoS groups.

Traffic exceeding the minimum guaranteed traffic level for its CoS group is either treated as Best-Effort or, in the case of Real-time Audio, ***DISCARDED***. It is critical that the traffic level for the Real-time Audio CoS group be configured correctly.

Most of the MPLS carriers automatically establish the Voice Real-time CoS group and configure it with a minimal (8Kbps) level of traffic. This is the single most frequent cause of voice garble on MPLS circuits. Customers fail to order the correct (or any) CoS profile or they fail to properly specify the bandwidth needed for Voice Real-time CoS. Obviously, the default value of 8Kbps will not even support a single call and most of the voice packets will be discarded.

Beware, providers may have to subcontract circuits from a different provider to reach their destination. One Telus customer had severe voice issues. We finally discovered that their Telus MPLS circuit that fed their Dallas TX USA data center was partially provided by Verizon and there was no CoS profile attached. Look out for similar situations.

Document Updates

The current/updated version of this document and vendor specific Appendices can be obtained from http://www.celab.ringcentral.com at any time.

Appendix A – Microsoft Windows

*Please **Read and Heed** Appendix Z to properly configure RingCentral Meetings.*

*Also, if you are a **LEGACY** Engage customer (from prior to the RingCentral acquisition) you must contact RingCentral Custom Engineering to obtain QoS implementation services.*

Microsoft Windows, by default, resets the DSCP value of all transmitted packets to BestEffort (0). You must take positive action forcing Windows to tag RingCentral traffic with proper DSCP values. Please note that the traffic going TO RingCentral will be marked, but you must implement proper QoS in the remainder of your network to take advantage of the markings and to set the DSCP values on return traffic as it ingresses your network. This is only one element of a proper QoS implementation.

***This is particularly critical if you are using WiFi.** Wireless Access Points depend on the DSCP marking of traffic in order to enable WMM prioritization of voice/video traffic. Without this marking a busy wireless network will not support voice / video traffic effectively.*

There are two categories of Windows QoS. One version is for domain-based deployments where you can define and deploy a domain-wide group policy that is utilized be every machine in the domain. The other version is for standalone Windows machines. The RingCentral Custom Engineering web server at https://www.celab.ringcentral.com/qos/qos.html has a download link that provides a ZIP file containing two PowerShell (.ps1) scripts, one for each version. These scripts will have a name that contains the release date.

Domain Based Implementation

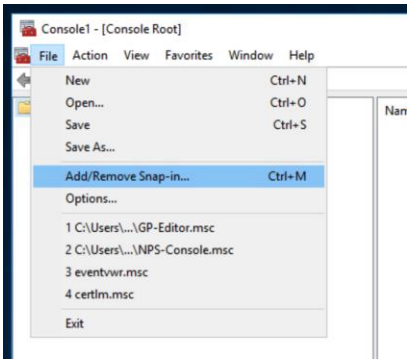
The domain-based QoS script defines a Group Policy Object (GPO) containing the current RingCentral QoS rules. Once created, this GPO must be linked to either the domain or to specific Organization Units (OUs) depending on your target scope. This implementation is much cleaner and easier to maintain than the previous Windows Group Policy QoS implementation which directly edited the 'Default Domain Policy'. I suggest you read about GPO inheritance on the web for further information.

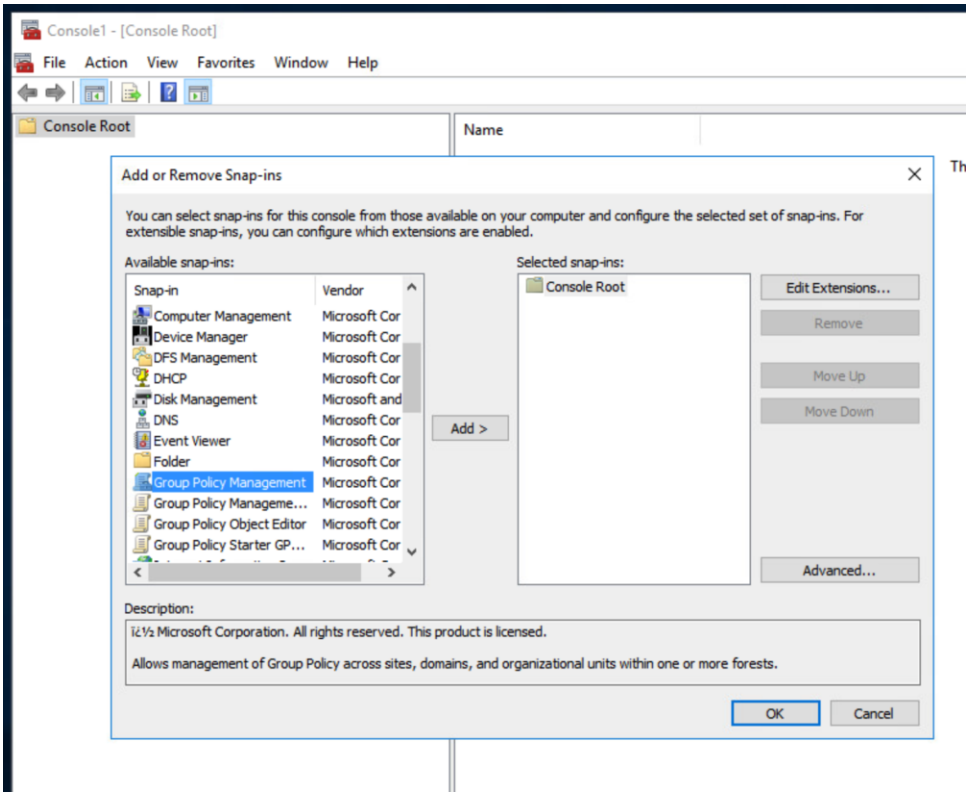
Create RC GPO and link it to the desired domain(s) / OU(s)

1. Download the ZIP file, unzip it, and run the WinGroupPolicy-xxxxx.ps1 script as Administrator. Follow the instructions at the beginning of the script to enable its execution.

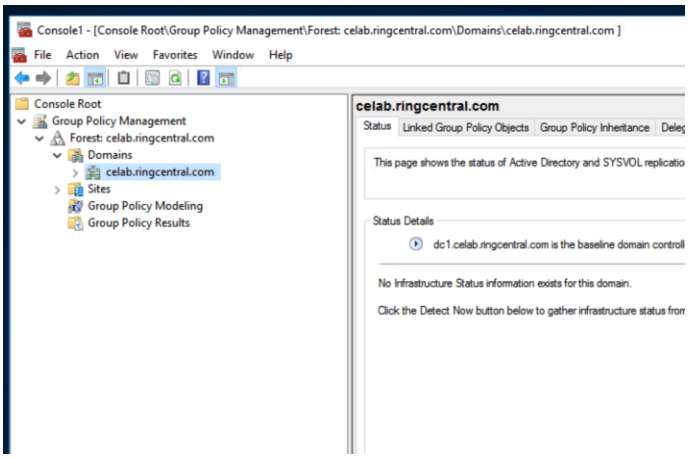
2. Start MMC.exe as Administrator.

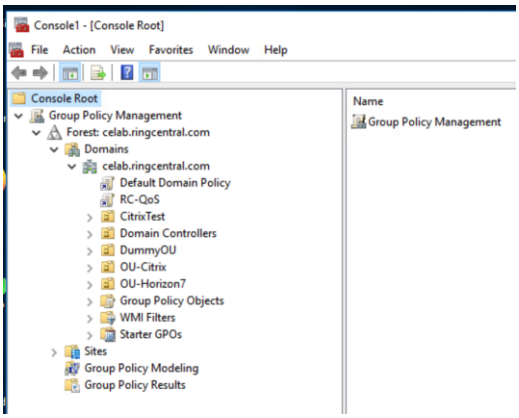
3. Add the 'Group Policy Management' snap-in. Note, **NOT** the 'Group Policy Management Editor'.



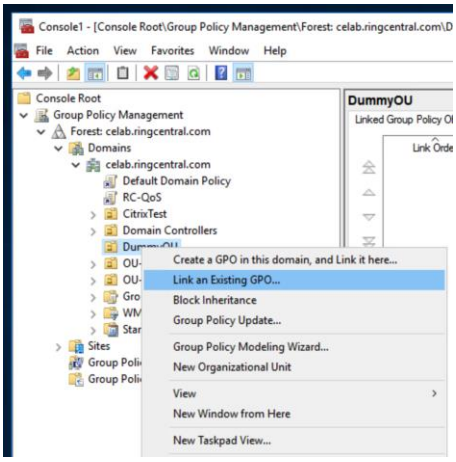


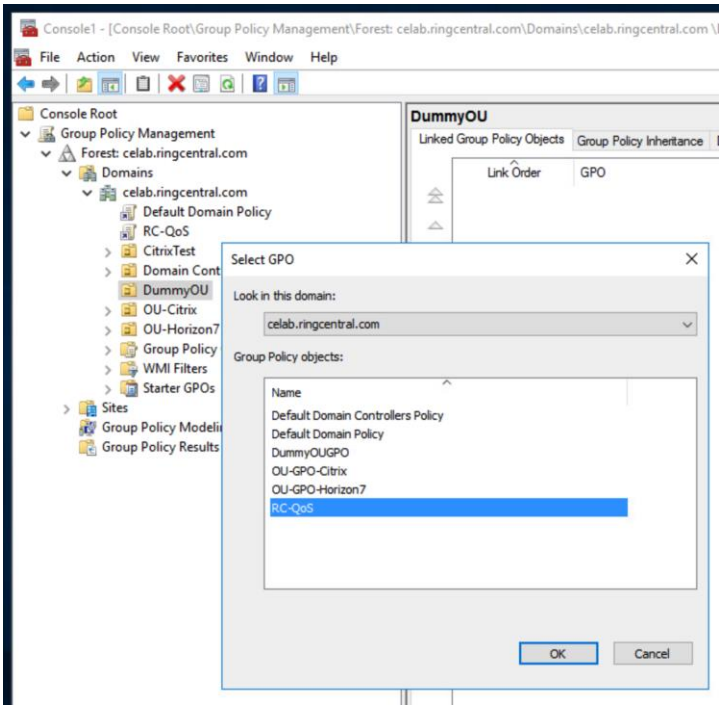
4. Navigate to the domain name and click on it. It will display any objects linked to it and any OUs defined under it.



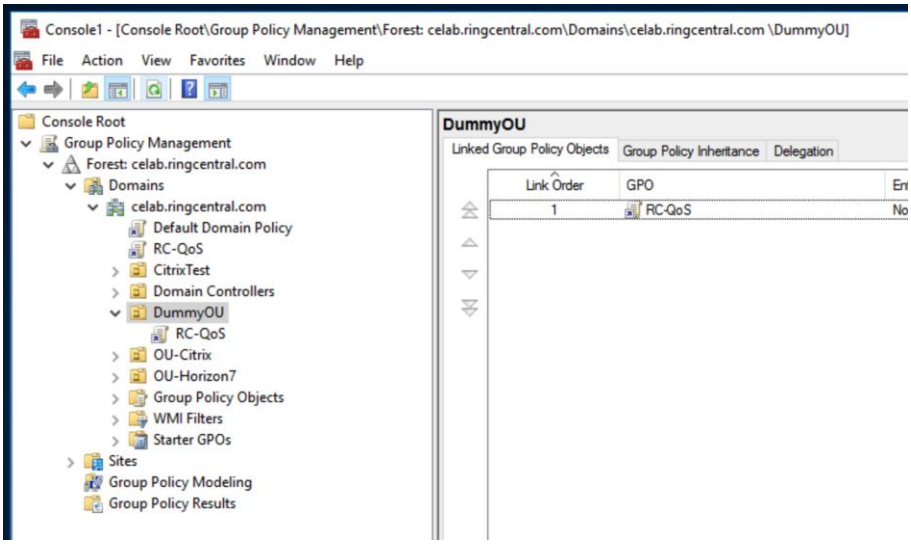


5. Right-click on the domain name or the OU to which you want the RC-QoS GPO attached, then select 'Link an Existing GPO'. Select RC-QoS and click OK.





6. The RC-QoS GPO should now be shown in the 'Linked Group Policy Objects' listing with a Link Order of 1.



7. Repeat for any other domains or OUs that need RC-QoS applied. Please note that if you apply it at the domain name level then all OUs belonging to that domain automatically inherit it.

Standalone Machine Implementation

Download the ZIP file, unzip it, and run the WinNetQosPolicy-xxxxx.ps1 script ***as Administrator***. Follow the instructions at the beginning of the script to enable its execution.

That's all there is to it!

Appendix B – Cisco Equipment

There are several different Cisco families for which we provide sample QoS configurations.

Two policy versions are provided, one for sites where User/AP traffic is already marked with proper DSCP tags; the other for sites where traffic is not marked, or markings cannot be trusted.

This revision of the Cisco configurations removes support for the old Zoom-based RingCentral Meetings product. Support for the RingCentral Video meetings product is included.

Universal Note: ***If at all possible, ensure that user endpoint traffic is marked with proper DSCP markings and utilize the policy-map versions for Trusted ports.***

- Apply Appendix A to all Windows based PCs that run any RingCentral soft-clients using either Group Policy or individual configuration.
- Have your Account Manager go into 'Admin Web' and enable proper QoS marking for non-Windows soft-clients. This is an account-wide setting that can only be made by a RingCentral employee.
- Have your SE apply custom code to ensure that your hard phones are configured to use proper QoS markings.

*Please note that Windows machines which connect via WiFi will pass through a Wireless Access Point (WAP) before any switches are encountered. You **MUST** implement the group policy as defined in Appendix A to have the traffic classified and marked for the WAP to process. WAPs are dependent on the DSCP marking of traffic to enable WMM (Wireless Multimedia) prioritization of voice/video traffic. Without this marking a congested wireless network will not support voice or video traffic effectively under multiuser conditions.*

Please note that the following configurations are for example only. They are specific for certain models and release versions of Cisco firmware. Some alterations may be required for certain models and firmware versions.

1. IOS based Cisco switches
    a. IOS based universal configuration
    b. IOS based MLS switches (2960/3560/3750 families)
    c. IOS based MQC switches (3650/3850/9000 families)
2. IOS based Cisco routers (all families)
3. NX-OS based Cisco switches
    a. NX-OS based MQC switches (Nexus 5xxx)
4. Cisco Zone Based Firewall (ZBF/ZFW) Configuration

5. Cisco ASA firewalls
6. Cisco Wireless Controllers

Naming Conventions

The configurations used in this document are written using some standardized naming conventions. A prefix is used denoting the primary type of the construct. We have found this to be useful in troubleshooting.

```
!=====================================================================
! Note:  The following Prefixes / Acronyms are used in these scripts
!  Prefixes are used in naming each entity to eliminate any possible
!  confusion.
!---------------------------------------------------------------------
!
! PFX – Prefix for Prefix Lists
! ACL - Prefix and/or acronym for Access Control Lists
! CM -  Prefix for Class Map definitions
! PM -  Prefix for Policy Map definitions
!
! 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)
!
! R2E - Used to indicate traffic flow moving FROM RingCentral to EndPoint
! E2R - Used to indicate traffic flow moving TO RingCentral from EndPoint
!
! RC -  Acronym standing for RingCentral
! RTP - Acronym standing for Real Time Protocol
!
```

DSCP Tagging Values

The following are the generally accepted DSCP values used to tag network traffic.

```
!=====================================================================
! 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 {one vendor uses CS3 (24) instead}
! AF21 (18) - All other RC traffic.  Unused for QoS, but good for troubleshooting.
! BE    (0) - Best Effort
!
```

IOS based Cisco switches

Please note that the Nexus product line does not use anything in this section. Go directly to the NX-OS Nexus Based Cisco section.

IOS Universal Configuration Elements Shared by All Cisco IOS Configurations

These elements are the same across all Cisco switches that utilize IOS and should be applied to all Cisco switches. The device specific configurations will, in turn, utilize these configuration elements.

Cleanup

To remove prior QoS configuration attempts first remove all service-policy statements from all interfaces. *{'show run | include interface|service-policy'}* After that you must run the following script. Ignore any errors as not all these constructs must be defined.

```
no policy-map PM-E2R-Trust
no policy-map PM-E2R-TrustNP
no policy-map PM-E2R-User
no policy-map PM-E2R-UserNP
no policy-map PM-R2E-ClassifyInbound
no policy-map PM-ZAP

no class-map match-any CM-E2R-RC-Voice
no class-map match-any CM-R2E-RC-Voice
no class-map match-any CM-E2R-RC-Video
no class-map match-any CM-R2E-RC-Video
no class-map match-any CM-E2R-RC-Other
no class-map match-any CM-R2E-RC-Other
no class-map match-any CM-E2R-RC-Signal
no class-map match-any CM-R2E-RC-Signal
no class-map match-any CM-DSCP-EF
no class-map match-any CM-DSCP-AF41
no class-map match-any CM-DSCP-AF31
no class-map match-any CM-DSCP-AF21

no ip access-list extended ACL-E2R-RC-All
no ip access-list extended ACL-R2E-RC-All
no ip access-list extended ACL-E2R-RC-Signal
no ip access-list extended ACL-R2E-RC-Signal
no ip access-list extended ACL-E2R-RC-Voice
no ip access-list extended ACL-R2E-RC-Voice
no ip access-list extended ACL-E2R-RC-Video
no ip access-list extended ACL-R2E-RC-Video
no ip access-list extended ACL-DSCP-EF
no ip access-list extended ACL-DSCP-AF41
no ip access-list extended ACL-DSCP-AF31
no ip access-list extended ACL-DSCP-AF21

no object-group network NOG-RingCentral
no object-group service SOG-E2R-RC-Signal
no object-group service SOG-R2E-RC-Signal
no object-group service SOG-E2R-RC-RTPMeeting
no object-group service SOG-R2E-RC-RTPMeeting
```

Use the following Packet Matching syntax for IOS versions that support object-groups

Object-groups are used to simplify Cisco Access Lists. Groups of addresses or service ports allow for great simplification of the configuration. *Object-groups are a Cisco feature that was introduced recently and may not be supported in your earlier versions of IOS.*

```
!-------------------------------------------------------------------
! Define Access Lists to Identify and Classify traffic FROM users/WAPs
! going TO RingCentral.  This version uses network object groups.
!-------------------------------------------------------------------
!
! Create lists and objects
!
object-group network NOG-RingCentral
 description All RC Public Networks a/o 20200813
 66.81.240.0 255.255.240.0
 80.81.128.0 255.255.240.0
 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-E2R-RC-Signal
 description RC SIP and Video Signal service identifiers a/o 20220107
 tcp-udp range 5090 5099
 tcp-udp range 5060 5061
 tcp range 8083 8090
 exit
!
object-group service SOG-R2E-RC-Signal
 description RC SIP and Video Signal service identifiers a/o 20220107
 tcp-udp source range 5090 5099
 tcp-udp source range 5060 5061
 tcp source range 8083 8090
 exit
!
object-group service SOG-E2R-RC-RTPMeeting
 description RC Meeting RTP service identifiers a/o 20220107
 tcp-udp range 8801 8802
 udp range 10000 19999
 exit
!
object-group service SOG-R2E-RC-RTPMeeting
 description RC Meeting RTP service identifiers a/o 20220107
 tcp-udp source range 8801 8802
 udp source range 10000 19999
 exit
!
object-group service SOG-E2R-RC-RTPAudio
 description RC Meeting RTP service identifiers a/o 20220107
 udp range 20000 64999
 udp 8803
 exit
!
object-group service SOG-R2E-RC-RTPAudio
 description RC Meeting RTP service identifiers a/o 20220107
 udp source range 20000 64999
 udp source 8803
 exit
!
! All RC network traffic not otherwise marked will be marked as AF21 traffic
!
ip access-list extended ACL-E2R-RC-All
 permit ip any object-group NOG-RingCentral
 exit
!
ip access-list extended ACL-R2E-RC-All
 permit ip object-group NOG-RingCentral any
 exit
```

```
!
! General signaling traffic will be marked AF31 traffic
!
ip access-list extended ACL-E2R-RC-Signal
 permit object-group SOG-E2R-RC-Signal any object-group NOG-RingCentral
 exit
!
ip access-list extended ACL-R2E-RC-Signal
 permit object-group SOG-R2E-RC-Signal object-group NOG-RingCentral any
 exit
!
! Phone / Softphone voice RT traffic will be marked EF traffic
!
ip access-list extended ACL-E2R-RC-Voice
 permit object-group SOG-E2R-RC-RTPAudio any object-group NOG-RingCentral
 exit
!
ip access-list extended ACL-R2E-RC-Voice
 permit object-group SOG-R2E-RC-RTPAudio object-group NOG-RingCentral any exit
 exit

!
! RC Video RT traffic will be marked AF41 traffic
!   -- Peer to peer must be set for ports 8850-8869
!
ip access-list extended ACL-E2R-RC-Video
 permit object-group SOG-E2R-RC-RTPMeeting any object-group NOG-RingCentral
 exit
!
ip access-list extended ACL-R2E-RC-Video
 permit object-group SOG-R2E-RC-RTPMeeting object-group NOG-RingCentral any
 exit
!
```

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.
!-------------------------------------------------------------------------
!
! All RC network traffic will be marked as AF21 traffic
!
ip access-list extended ACL-E2R-RC-All
 permit ip any 66.81.240.0 0.0.15.255
 permit ip any 80.81.128.0 0.0.15.255
 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 199.68.212.0 0.0.3.255
 permit ip any 199.255.120.0 0.0.3.255
 permit ip any 208.87.40.0 0.0.3.255
 exit
!
ip access-list extended ACL-R2E-RC-All
 permit ip 66.81.240.0 0.0.15.255 any
 permit ip 80.81.128.0 0.0.15.255 any
 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 199.68.212.0 0.0.3.255 any
 permit ip 199.255.120.0 0.0.3.255 any
 permit ip 208.87.40.0 0.0.3.255 any
 exit
```

```
!
! General SIP traffic will be marked AF31 traffic
!
ip access-list extended ACL-E2R-RC-Signal
 permit tcp any 66.81.240.0 0.0.15.255 range 5060 5061
 permit tcp any 80.81.128.0 0.0.15.255 range 5060 5061
 permit tcp any 103.44.68.0 0.0.3.255 range 5060 5061
 permit tcp any 104.245.56.0 0.0.7.255 range 5060 5061
 permit tcp any 185.23.248.0 0.0.3.255 range 5060 5061
 permit tcp any 192.209.24.0 0.0.7.255 range 5060 5061
 permit tcp any 199.68.212.0 0.0.3.255 range 5060 5061
 permit tcp any 199.255.120.0 0.0.3.255 range 5060 5061
 permit tcp any 208.87.40.0 0.0.3.255 range 5060 5061
 permit udp any 66.81.240.0 0.0.15.255 range 5060 5061
 permit udp any 80.81.128.0 0.0.15.255 range 5060 5061
 permit udp any 103.44.68.0 0.0.3.255 range 5060 5061
 permit udp any 104.245.56.0 0.0.7.255 range 5060 5061
 permit udp any 185.23.248.0 0.0.3.255 range 5060 5061
 permit udp any 192.209.24.0 0.0.7.255 range 5060 5061
 permit udp any 199.68.212.0 0.0.3.255 range 5060 5061
 permit udp any 199.255.120.0 0.0.3.255 range 5060 5061
 permit udp any 208.87.40.0 0.0.3.255 range 5060 5061
 permit tcp any 66.81.240.0 0.0.15.255 range 5090 5099
 permit tcp any 80.81.128.0 0.0.15.255 range 5090 5099
 permit tcp any 103.44.68.0 0.0.3.255 range 5090 5099
 permit tcp any 104.245.56.0 0.0.7.255 range 5090 5099
 permit tcp any 185.23.248.0 0.0.3.255 range 5090 5099
 permit tcp any 192.209.24.0 0.0.7.255 range 5090 5099
 permit tcp any 199.68.212.0 0.0.3.255 range 5090 5099
 permit tcp any 199.255.120.0 0.0.3.255 range 5090 5099
 permit tcp any 208.87.40.0 0.0.3.255 range 5090 5099
 permit udp any 66.81.240.0 0.0.15.255 range 5090 5099
 permit udp any 80.81.128.0 0.0.15.255 range 5090 5099
 permit udp any 103.44.68.0 0.0.3.255 range 5090 5099
 permit udp any 104.245.56.0 0.0.7.255 range 5090 5099
 permit udp any 185.23.248.0 0.0.3.255 range 5090 5099
 permit udp any 192.209.24.0 0.0.7.255 range 5090 5099
 permit udp any 199.68.212.0 0.0.3.255 range 5090 5099
 permit udp any 199.255.120.0 0.0.3.255 range 5090 5099
 permit udp any 208.87.40.0 0.0.3.255 range 5090 5099
 permit tcp any 66.81.240.0 0.0.15.255 range 8083 8090
 permit tcp any 80.81.128.0 0.0.15.255 range 8083 8090
 permit tcp any 103.44.68.0 0.0.3.255 range 8083 8090
 permit tcp any 104.245.56.0 0.0.7.255 range 8083 8090
 permit tcp any 185.23.248.0 0.0.3.255 range 8083 8090
 permit tcp any 192.209.24.0 0.0.7.255 range 8083 8090
 permit tcp any 199.68.212.0 0.0.3.255 range 8083 8090
 permit tcp any 199.255.120.0 0.0.3.255 range 8083 8090
 permit tcp any 208.87.40.0 0.0.3.255 range 8083 8090
 exit
!
ip access-list extended ACL-R2E-RC-Signal
 permit tcp 66.81.240.0 0.0.15.255 range 5060 5061 any
 permit tcp 80.81.128.0 0.0.15.255 range 5060 5061 any
 permit tcp 103.44.68.0 0.0.3.255 range 5060 5061 any
 permit tcp ay 104.245.56.0 0.0.7.255 range 5060 5061 any
 permit tcp 185.23.248.0 0.0.3.255 range 5060 5061 any
 permit tcp 192.209.24.0 0.0.7.255 range 5060 5061 any
 permit tcp 199.68.212.0 0.0.3.255 range 5060 5061 any
 permit tcp 199.255.120.0 0.0.3.255 range 5060 5061 any
 permit tcp 208.87.40.0 0.0.3.255 range 5060 5061 any
 permit udp 66.81.240.0 0.0.15.255 range 5060 5061 any
 permit udp 80.81.128.0 0.0.15.255 range 5060 5061 any
 permit udp 103.44.68.0 0.0.3.255 range 5060 5061 any
 permit udp 104.245.56.0 0.0.7.255 range 5060 5061 any
 permit udp 185.23.248.0 0.0.3.255 range 5060 5061 any
 permit udp 192.209.24.0 0.0.7.255 range 5060 5061 any
```

```
 permit udp 199.68.212.0 0.0.3.255 range 5060 5061 any
 permit udp 199.255.120.0 0.0.3.255 range 5060 5061 any
 permit udp 208.87.40.0 0.0.3.255 range 5060 5061 any
 permit tcp 66.81.240.0 0.0.15.255 range 5090 5099 any
 permit tcp 80.81.128.0 0.0.15.255 range 5090 5099 any
 permit tcp 103.44.68.0 0.0.3.255 range 5090 5099 any
 permit tcp 104.245.56.0 0.0.7.255 range 5090 5099 any
 permit tcp 185.23.248.0 0.0.3.255 range 5090 5099 any
 permit tcp 192.209.24.0 0.0.7.255 range 5090 5099 any
 permit tcp 199.68.212.0 0.0.3.255 range 5090 5099 any
 permit tcp 199.255.120.0 0.0.3.255 range 5090 5099 any
 permit tcp 208.87.40.0 0.0.3.255 range 5090 5099 any
 permit udp 66.81.240.0 0.0.15.255 range 5090 5099 any
 permit udp 80.81.128.0 0.0.15.255 range 5090 5099 any
 permit udp 103.44.68.0 0.0.3.255 range 5090 5099 any
 permit udp 104.245.56.0 0.0.7.255 range 5090 5099 any
 permit udp 185.23.248.0 0.0.3.255 range 5090 5099 any
 permit udp 192.209.24.0 0.0.7.255 range 5090 5099 any
 permit udp 199.68.212.0 0.0.3.255 range 5090 5099 any
 permit udp 199.255.120.0 0.0.3.255 range 5090 5099 any
 permit udp 208.87.40.0 0.0.3.255 range 5090 5099 any
 permit tcp 66.81.240.0 0.0.15.255 range 8083 8090 any
 permit tcp 80.81.128.0 0.0.15.255 range 8083 8090 any
 permit tcp 103.44.68.0 0.0.3.255 range 8083 8090 any
 permit tcp 104.245.56.0 0.0.7.255 range 8083 8090 any
 permit tcp 185.23.248.0 0.0.3.255 range 8083 8090 any
 permit tcp 192.209.24.0 0.0.7.255 range 8083 8090 any
 permit tcp 199.68.212.0 0.0.3.255 range 8083 8090 any
 permit tcp 199.255.120.0 0.0.3.255 range 8083 8090 any
 permit tcp 208.87.40.0 0.0.3.255 range 8083 8090 any
 exit
!
! Phone / Softphone voice RT traffic will be marked EF traffic
!
ip access-list extended ACL-E2R-RC-Voice
 permit udp any 66.81.240.0 0.0.15.255 range 20000 64999
 permit udp any 80.81.128.0 0.0.15.255 range 20000 64999
 permit udp any 103.44.68.0 0.0.3.255 range 20000 64999
 permit udp any 104.245.56.0 0.0.7.255 range 20000 64999
 permit udp any 185.23.248.0 0.0.3.255 range 20000 64999
 permit udp any 192.209.24.0 0.0.7.255 range 20000 64999
 permit udp any 199.255.120.0 0.0.3.255 range 20000 64999
 permit udp any 199.68.212.0 0.0.3.255 range 20000 64999
 permit udp any 208.87.40.0 0.0.3.255 range 20000 64999
 permit udp any 66.81.240.0 0.0.15.255 eq 8803
 permit udp any 80.81.128.0 0.0.15.255 eq 8803
 permit udp any 103.44.68.0 0.0.3.255 eq 8803
 permit udp any 104.245.56.0 0.0.7.255 eq 8803
 permit udp any 185.23.248.0 0.0.3.255 eq 8803
 permit udp any 192.209.24.0 0.0.7.255 eq 8803
 permit udp any 199.255.120.0 0.0.3.255 eq 8803
 permit udp any 199.68.212.0 0.0.3.255 eq 8803
 permit udp any 208.87.40.0 0.0.3.255 eq 8803
 exit
!
ip access-list extended ACL-R2E-RC-Voice
 permit udp 66.81.240.0 0.0.15.255 range 20000 64999 any
 permit udp 80.81.128.0 0.0.15.255 range 20000 64999 any
 permit udp 103.44.68.0 0.0.3.255 range 20000 64999 any
 permit udp 104.245.56.0 0.0.7.255 range 20000 64999 any
 permit udp 185.23.248.0 0.0.3.255 range 20000 64999 any
 permit udp 192.209.24.0 0.0.7.255 range 20000 64999 any
 permit udp 199.255.120.0 0.0.3.255 range 20000 64999 any
 permit udp 199.68.212.0 0.0.3.255 range 20000 64999 any
 permit udp 208.87.40.0 0.0.3.255 range 20000 64999 any
 permit udp 66.81.240.0 0.0.15.255 eq 8803 any
 permit udp 80.81.128.0 0.0.15.255 eq 8803 any
```

```
 permit udp 103.44.68.0 0.0.3.255 eq 8803 any
 permit udp 104.245.56.0 0.0.7.255 eq 8803 any
 permit udp 185.23.248.0 0.0.3.255 eq 8803 any
 permit udp 192.209.24.0 0.0.7.255 eq 8803 any
 permit udp 199.255.120.0 0.0.3.255 eq 8803 any
 permit udp 199.68.212.0 0.0.3.255 eq 8803 any
 permit udp 208.87.40.0 0.0.3.255 eq 8803 any
 exit
!
! RC Meetings Video RT traffic or premarked AF41/CS4 traffic
!
ip access-list extended ACL-E2R-RC-Video
 permit udp any 66.81.240.0 0.0.15.255 range 8801 8802
 permit udp any 80.81.128.0 0.0.15.255 range 8801 8802
 permit udp any 103.44.68.0 0.0.3.255 range 8801 8802
 permit udp any 104.245.56.0 0.0.7.255 range 8801 8802
 permit udp any 185.23.248.0 0.0.3.255 range 8801 8802
 permit udp any 192.209.24.0 0.0.7.255 range 8801 8802
 permit udp any 199.255.120.0 0.0.3.255 range 8801 8802
 permit udp any 199.68.212.0 0.0.3.255 range 8801 8802
 permit udp any 208.87.40.0 0.0.3.255 range 8801 8802
 permit tcp any 66.81.240.0 0.0.15.255 range 8801 8802
 permit tcp any 80.81.128.0 0.0.15.255 range 8801 8802
 permit tcp any 103.44.68.0 0.0.3.255 range 8801 8802
 permit tcp any 104.245.56.0 0.0.7.255 range 8801 8802
 permit tcp any 185.23.248.0 0.0.3.255 range 8801 8802
 permit tcp any 192.209.24.0 0.0.7.255 range 8801 8802
 permit tcp any 199.255.120.0 0.0.3.255 range 8801 8802
 permit tcp any 199.68.212.0 0.0.3.255 range 8801 8802
 permit tcp any 208.87.40.0 0.0.3.255 range 8801 8802
 permit udp any 66.81.240.0 0.0.15.255 range 10000 19999
 permit udp any 80.81.128.0 0.0.15.255 range 10000 19999
 permit udp any 103.44.68.0 0.0.3.255 range 10000 19999
 permit udp any 104.245.56.0 0.0.7.255 range 10000 19999
 permit udp any 185.23.248.0 0.0.3.255 range 10000 19999
 permit udp any 192.209.24.0 0.0.7.255 range 10000 19999
 permit udp any 199.255.120.0 0.0.3.255 range 10000 19999
 permit udp any 199.68.212.0 0.0.3.255 range 10000 19999
 permit udp any 208.87.40.0 0.0.3.255 range 10000 19999
 exit
!
ip access-list extended ACL-R2E-RC-Video
 permit udp 66.81.240.0 0.0.15.255 range 8801 8802 any
 permit udp 80.81.128.0 0.0.15.255 range 8801 8802 any
 permit udp 103.44.68.0 0.0.3.255 range 8801 8802 any
 permit udp 104.245.56.0 0.0.7.255 range 8801 8802 any
 permit udp 185.23.248.0 0.0.3.255 range 8801 8802 any
 permit udp 192.209.24.0 0.0.7.255 range 8801 8802 any
 permit udp 199.255.120.0 0.0.3.255 range 8801 8802 any
 permit udp 199.68.212.0 0.0.3.255 range 8801 8802 any
 permit udp 208.87.40.0 0.0.3.255 range 8801 8802 any
 permit tcp 66.81.240.0 0.0.15.255 range 8801 8802 any
 permit tcp 80.81.128.0 0.0.15.255 range 8801 8802 any
 permit tcp 103.44.68.0 0.0.3.255 range 8801 8802 any
 permit tcp 104.245.56.0 0.0.7.255 range 8801 8802 any
 permit tcp 185.23.248.0 0.0.3.255 range 8801 8802 any
 permit tcp 192.209.24.0 0.0.7.255 range 8801 8802 any
 permit tcp 199.255.120.0 0.0.3.255 range 8801 8802 any
 permit tcp 199.68.212.0 0.0.3.255 range 8801 8802 any
 permit tcp 208.87.40.0 0.0.3.255 range 8801 8802 any
 permit udp 66.81.240.0 0.0.15.255 range 10000 19999 any
 permit udp 80.81.128.0 0.0.15.255 range 10000 19999 any
 permit udp 103.44.68.0 0.0.3.255 range 10000 19999 any
 permit udp 104.245.56.0 0.0.7.255 range 10000 19999 any
 permit udp 185.23.248.0 0.0.3.255 range 10000 19999 any
 permit udp 192.209.24.0 0.0.7.255 range 10000 19999 any
 permit udp 199.255.120.0 0.0.3.255 range 10000 19999 any
```

```
 permit udp 199.68.212.0 0.0.3.255 range 10000 19999 any
 permit udp 208.87.40.0 0.0.3.255 range 10000 19999 any
 exit
!
```

Class-maps for all IOS versions

```
!-----------------------------------------------------------------
! Establish Class-Maps for matching port ingress traffic
!
class-map match-any CM-E2R-RC-Voice
 match access-group name ACL-E2R-RC-Voice
 exit
!
class-map match-any CM-R2E-RC-Voice
 match access-group name ACL-R2E-RC-Voice
 exit
!
class-map match-any CM-E2R-RC-Video
 match access-group name ACL-E2R-RC-Video
 exit
!
class-map match-any CM-R2E-RC-Video
 match access-group name ACL-R2E-RC-Video
 exit
!
class-map match-any CM-E2R-RC-Other
 match access-group name ACL-E2R-RC-All
 exit
!
class-map match-any CM-R2E-RC-Other
 match access-group name ACL-R2E-RC-All
 exit
!
class-map match-any CM-E2R-RC-Signal
 match access-group name ACL-E2R-RC-Signal
 exit
!
class-map match-any CM-R2E-RC-Signal
 match access-group name ACL-R2E-RC-Signal
 exit
!
```

Access and Aggregation / Distribution Switches (MLS based – 2960/3560/3750 Families)

The Access switch must examine packets as they come in from user and WAP ports and potentially police the priority traffic to prevent a run-away process from harming the network. If the packets are not already marked, the Access switch must determine their proper classification and set the appropriate DSCP value. It has been determined empirically that a 'hard' phone involved in a phone initiated 3-way conference call will require slightly less than 512Kbps of 'real-time' voice capacity in each direction. User voice traffic destined to Ring Central and exceeding 512Kbps will be dropped because it exceeds the specified maximum rate.

Please note that cascading switches and hard phones on a user access port which utilizes a policing service policy may drop valid voice traffic when multiple phones are in use simultaneously and the single port policing limits are exceeded. *Never* cascade users/switches on a single user access port set for policing. Always use a trunk port to feed another Access Switch to maintain a consistent QoS policy across devices.

Please note when troubleshooting that the output from the '`show policy-map interface xx/n/n`' is useless for debugging purposes. ***The counters will show zero values and will not update. This is known behavior – all policy-mapping and packet matching tasks are being done in silicon at line rate without updating the processor. The only way you can be sure your policy-map is working is by mirroring the trunk port to a machine running packet captures and examining the DSCP tags of actual packets.***

Enable MLS

QoS is disabled by default on these models and must be specifically enabled.

```
!-------------------------------------------------------------------
! On switches that are MLS based (2960, 3560, 3750, etc) you must
! enable MLS QoS.  The following code will set things up properly.
!
! Ports that are set to 'mls trust cos' ignore the DSCP value as received
! and set it based upon the received 802.1p COS value (0-7).  The default
! values used by Cisco are not correct.  This command corrects the values.
! Note that we don't normally use this function, but it should be set
! correctly for hybrid configurations to function properly.
mls qos map cos-dscp 0 8 18 26 34 46 48 56
!
! The following commands are used to set the 802.1p layer-2 priority values
! when untagged traffic ingresses the switch.
mls qos map dscp-cos 46 to 5
mls qos map dscp-cos 34 to 4
mls qos map dscp-cos 26 to 3
!
! The following values for srr-queue settings should be tuned for specific
! sites/applications.  The following values have been known to work for
! one large customer and are for example only.
!
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
!
! Activate QoS
!
mls qos
!
```

Policy-maps

```
!================================================================================
! Policy maps are provided for trusted and untrusted user ports with and
! without policing applied.  WAP ports and trunk ports should be set up
! using the policies ending with NP (No Policing).
!
! Please note that ALL interswitch 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.  When in doubt issue the command to so so.
!
! If you have set up your Windows users to force QoS marking as described in
! Appendix A or you are using a MAC or Linux machine you must ensure that
! the user ports are set to trust the DSCP value as it is transmitted or
! it will be reset to Best Effort.
!--------------------------------------------------------------------------------
!
! Class maps to match dscp/prec in the MLS based units need to be done using
! ACLs.  Don't try to use the match dscp clause in the class-map definition.
!
ip access-list extended ACL-DSCP-EF
 permit ip any any dscp ef
 permit ip any any precedence 5
 exit
!
ip access-list extended ACL-DSCP-AF41
 permit ip any any dscp af41
 permit ip any any precedence 4
 exit
!
ip access-list extended ACL-DSCP-AF31
 permit ip any any dscp af31
 permit ip any any precedence 3
 exit
!
ip access-list extended ACL-DSCP-AF21
 permit ip any any dscp af21
 exit
!
class-map match-any CM-DSCP-EF
 match access-group name ACL-DSCP-EF
 exit
!
class-map match-any CM-DSCP-AF41
 match access-group name ACL-DSCP-AF41
 exit
!
class-map match-any CM-DSCP-AF31
 match access-group name ACL-DSCP-AF31
```

```
 exit
!
class-map match-any CM-DSCP-AF21
 match access-group name ACL-DSCP-AF21
 exit
!
!----------------------------------------------------------------
! Create this Inbound QoS Markup/Police Policy for User or WAP
! Ports where classification and marking are needed.
!
! Policing is set to allow 512Kbps of voice RTP traffic (to
! allow for 3-way conferencing from the phone – this has been
! determined empirically to allow for 3-way phone initiated
! conferencing.)
!
! Use the NP (No Policing) version for ports where policing is
! not desired, but classification is needed.  (WAP ports and trunk
! ports coming from devices that do not apply marking.)
!
! Note: Different firmware revision levels may differ in syntax.
! Read the documentation for your level if you encounter a syntax
! error.  This pertains particularly to the 'police' clause.
!
policy-map PM-E2R-User
 class CM-E2R-RC-Voice
  set ip dscp ef
  police 512000 16000 exceed-action drop
  exit
 class CM-E2R-RC-Video
  set ip dscp af41
  police 768000 8000 exceed-action policed-dscp-transmit
  exit
 class CM-E2R-RC-Signal
  set ip dscp af31
  police 32000 8000 exceed-action policed-dscp-transmit
  exit
 class CM-E2R-RC-Other
  set ip dscp af21
  exit
 class class-default
  set ip dscp default
  exit
 exit
!
! Same policy with no policing actions
!
policy-map PM-E2R-UserNP
 class CM-E2R-RC-Voice
  set ip dscp ef
  exit
 class CM-E2R-RC-Video
  set ip dscp af41
  exit
 class CM-E2R-RC-Signal
  set ip dscp af31
  exit
 class CM-E2R-RC-Other
  set ip dscp af21
  exit
 class class-default
  set ip dscp default
  exit
 exit
!
!----------------------------------------------------------------
! Create this Inbound QoS Markup/Police Policy for ports where
! classification and marking are already present.
```

```
!
! PM-E2R-Trust should be used when you want to apply single user police
! action to the port.
!
! Use the NP (No Policing) version for ports where policing is
! not desired.  (WAP ports and trunk ports coming from devices
! that do apply marking.)
!
policy-map PM-E2R-Trust
 class CM-DSCP-EF
  police 512000 16000 exceed-action drop
  trust dscp
  exit
 class CM-DSCP-AF41
  police 768000 8000 exceed-action policed-dscp-transmit
  trust dscp
  exit
 class CM-DSCP-AF31
  police 32000 8000 exceed-action policed-dscp-transmit
  trust dscp
  exit
 class CM-DSCP-AF21
  trust dscp
  exit
 class class-default
  set ip dscp default
  exit
 exit
!
! Same policy with no policing actions.  Other than changing CS5 to EF
! and CS3 to AF31 this policy does nothing other than pass through.
!
policy-map PM-E2R-TrustNP
 class CM-DSCP-EF
  set dscp ef
  exit
 class CM-DSCP-AF41
  set dscp af41
  exit
 class CM-DSCP-AF31
  set dscp af31
  exit
 class CM-DSCP-AF21
  set dscp af21
  exit
 class class-default
  set dscp default
  exit
 exit
!
!-----------------------------------------------------------
! Policy maps for ports that receive inbound RC traffic from an ISP or
! a direct connection.
!
! This is not usually used on an access switch, but in rare cases the Internet
! feed may be present on the switch.  This is usually found on the Internet WAN
! router.
!
policy-map PM-R2E-ClassifyInbound
 class CM-R2E-RC-Voice
  set ip dscp ef
  exit
 class CM-R2E-RC-Video
  set ip dscp af41
  exit
 class CM-R2E-RC-Signal
  set ip dscp af31
```

```
  exit
 class CM-R2E-RC-Other
  set ip dscp af21
  exit
 class class-default
  set ip dscp default
  exit
 exit
!
! Policy map for testing, zero out dscp
!
! Used for testing only!!!!
!
policy-map PM-ZAP
 class class-default
  set dscp default
  exit
 exit
```

Application to Switch Ports

Policy maps must be **applied** to the input of every port to correctly establish QoS. When in doubt, apply a User policy to the port. Trunk ports need only be set to trust DSCP.

```
!==========================================================================
!
! User ports – With Policing Applied
!
!   Use 'mls qos trust dscp' to set port to trusted mode if you are passing
!   in marked traffic.
!
!   Critical Note: You MUST remove the 'mls qos trust device cisco-phone'
!   or 'qos trust device cisco-phone' configuration statement.  If it is
!   present all dscp markings from any device other than a Cisco IP Phone,
!   including your PC, will be completely stripped and set to best-effort.
!   Also *ALL* auto-qos configuration should be totally removed from your
!   configurations or, at the very least, from the port used.
!
!   Ports with devices that do not mark RC traffic and cannot be
!   trusted should be set up like this:
!
interface range Gi1/0/9-10
 no mls qos trust device cisco-phone
 no auto qos voip cisco-phone
 no mls qos trust cos
 no mls qos trust dscp
 priority-queue out
 service-policy input PM-E2R-User
 exit
!
!   Ports with devices that do not mark RC traffic and can be
!   trusted should be set up like this:
!
interface range Gi1/0/11-20
 no mls qos trust device cisco-phone
 no auto qos voip cisco-phone
 no mls qos trust cos
 mls qos trust dscp
 priority-queue out
 service-policy input PM-E2R-UserNP
 exit
!
!   Ports with devices that do mark traffic and can be
!   trusted should be set up like this:
```

```
!
!   Windows machines which have had Appendix A group policy applied fall in
!   this category, as do hard phones with proper QoS settings confirmed.
!
interface range Gi1/0/21-30
 no mls qos trust device cisco-phone
 no auto qos voip cisco-phone
 no mls qos trust cos
 mls qos trust dscp
 priority-queue out
 service-policy input PM-E2R-Trust
 exit
!
!================================================================================
!
! Wireless Access Point ports
!
! If you potentially have wireless clients that are not marking their
! traffic or trunks from switches/devices that do not mark their traffic
! you should mark the traffic on ingress.
!
! (Please note that if wifi clients do NOT mark their traffic natively
! the WAP has no way to identify real-time traffic and voice quality will
! suffer randomly.
!
! Always use the NP (No Policing) policy form.
!
interface Gi1/0/21
 no mls qos trust device cisco-phone
 no auto qos voip cisco-phone
 no mls qos trust cos
 no mls qos trust dscp
 priority-queue out
 service-policy input PM-E2R-UserNP
 exit
!
! Ports with devices that do mark traffic and can be
! trusted should be set up like this:
!
interface Gi1/0/22
 no mls qos trust device cisco-phone
 no auto qos voip cisco-phone
 no mls qos trust cos
 mls qos trust dscp
 priority-queue out
 service-policy input PM-E2R-TrustNP
 exit
!
!================================================================================
!
! Trunk Ports
!   Use 'mls qos trust dscp' to set port to trusted mode.
!
!   All interswitch trunk ports must be set to trust dscp.
!
!   If using LACP based port-channels to aggregate traffic, the qos commands
!   must usually be applied on each member interface and generally cannot
!   be applied to the logical port-channel interface.  Certain IOS versions,
!   however, may require application to the port-channel interface.
!
interface Gi0/49
 no mls qos trust device cisco-phone
 no auto qos voip cisco-phone
 no mls qos trust cos
 mls qos trust dscp
 priority-queue out
 service-policy input PM-E2R-TrustNP
```

```
 exit
!
!=============================================================================
!
! Internet Ports
!
! Please note that these switches CANNOT perform traffic shaping and are
! very poor choices to connect directly to an ISP device.
!
! Use PM-R2E-ClassifyInbound to mark all traffic ingressing your network
! from the Internet or any upstream device that does not mark traffic.
!
interface Gi0/49
 no mls qos trust device cisco-phone
 no auto qos voip cisco-phone
 no mls qos trust cos
 no mls qos trust dscp
 priority-queue out
 service-policy input PM-R2E-ClassifyInbound
 exit
!
! If you trust your upstream provider or device to send you properly marked
! traffic, then do not use an inbound service policy and simply trust dscp.
! This will be VERY RARELY done and only used when subscribing to specialized
! ISP services such as ATT MIS+ that carry DSCP tags end-to-end.
!
interface Gi0/49
 no mls qos trust device cisco-phone
 no auto qos voip cisco-phone
 no mls qos trust cos
 mls qos trust dscp
 priority-queue out
 exit
!
```

Access and Aggregation / Distribution Switches (MQC based – 3650/3850 Families)

This family of switches are frequently used in both Access and Distribution functions. They are quite advanced and feature-rich.

Miscellaneous Configuration Statements

```
!=============================================================================
! DSCP downcheck tables for exceeding or violating policing values.
!
! The DSCP value will be changed to this value when rate is exceeded.
!
table-map TM-Exceed-Map
 default 0
 exit
!
table-map TM-Violate-Map
 default 0
 exit
!
!-----------------------------------------------------------------
! Create DSCP based QoS class matches
!
! Unlike the MLS switches, you may use the 'match dscp' clause in the class-map definitions.
!
class-map match-any CM-DSCP-EF
 match dscp ef
 exit
```

```
!
class-map match-any CM-DSCP-AF41
 match dscp af41
 exit
!
class-map match-any CM-DSCP-AF31
 match dscp af31
 exit
!
class-map match-any CM-DSCP-AF21
 match dscp af21
 exit
!
```

Policy-maps

```
!
!-----------------------------------------------------------------
! Create this Inbound QoS Markup/Police Policy for User or WAP
! Ports where classification and marking are needed.
!
! Policing is set to allow 512Kbps of voice RTP traffic (to
! allow for 3-way conferencing from the phone – this has been
! determined empirically to allow for 3-way phone initiated
! conferencing.)
!
! Use the NP (No Policing) version for ports where policing is
! not desired, but classification is needed.  (WAP ports and trunk
! ports coming from devices that do not apply marking.)
!
! Note: Different firmware revision levels may differ in syntax.
! Read the documentation for your level if you encounter a syntax
! error.  This pertains particularly to the 'police' clause.
!
policy-map PM-E2R-User
 class CM-E2R-RC-Voice
  set dscp ef
  set cos 5
  police cir 512000 bc 16000
   conform-action transmit
   exceed-action drop
   exit
  exit
 class CM-E2R-RC-Video
  set dscp af41
  set cos 4
  police cir 768000 bc 8000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table TM-Exceed-Map
   exit
  exit
 class CM-E2R-RC-Signal
  set dscp af31
  set cos 3
  police cir 32000 bc 8000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table TM-Exceed-Map
   exit
  exit
 class CM-E2R-RC-Other
  set dscp af21
  set cos 2
  exit
 class class-default
  set dscp default
  set cos 0
  exit
 exit
```

```
!
policy-map PM-E2R-UserNP
 class CM-E2R-RC-Voice
  set dscp ef
  set cos 5
  exit
 class CM-E2R-RC-Video
  set dscp af41
  set cos 4
  exit
 class CM-E2R-RC-Signal
  set dscp af31
  set cos 3
  exit
 class CM-E2R-RC-Other
  set dscp af21
  set cos 2
  exit
 class class-default
  set dscp default
  set cos 0
  exit
 exit
!
!-----------------------------------------------------------------
! Create this Inbound QoS Markup/Police Policy for ports where
! classification and marking are already present.
!
! PM-E2R-Trust should be used when you want to apply single user police
! action to the port.
!
! Use the NP (No Policing) version for ports where policing is
! not desired.  (WAP ports and trunk ports coming from devices
! that do apply marking.)
!
policy-map PM-E2R-Trust
 class CM-DSCP-EF
  set cos 5
  police cir 512000 bc 16000
   conform-action transmit
   exceed-action drop
   exit
  exit
 class CM-DSCP-AF41
  set cos 4
  police cir 768000 bc  8000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table TM-Exceed-Map
   exit
  exit
 class CM-DSCP-AF31
  set cos 3
  police cir 32000 bc 8000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table TM-Exceed-Map
   exit
  exit
 class CM-DSCP-AF21
  set cos 2
  exit
 class class-default
  set cos 0
  exit
 exit
!
policy-map PM-E2R-TrustNP
 class CM-DSCP-EF
```

```
  set cos 5
  exit
class CM-DSCP-AF41
  set cos 4
  exit
class CM-DSCP-AF31
  set cos 3
  exit
class CM-DSCP-AF21
  set cos 2
  exit
 class class-default
  set cos 0
  exit
 exit
!
! Policy maps for ports that receive inbound RC traffic from ISP
!
! This is not usually used on an access switch, but in rare cases the Internet
! feed may be present on the switch.  This is usually found on the Internet WAN
! router/firewall.
!
policy-map PM-R2E-ClassifyInbound
 class CM-R2E-RC-Voice
  set ip dscp ef
  set cos 5
  exit
 class CM-R2E-RC-Video
  set ip dscp af41
  set cos 4
  exit
 class CM-R2E-RC-Signal
  set ip dscp af31
  set cos 3
  exit
 class CM-R2E-RC-Other
  set ip dscp af21
  set cos 2
  exit
 class class-default
  set ip dscp default
  set cos 0
  exit
 exit
!
! **ALL** interfaces must have PM-ALL-StdOutbound or a parent policy
!  which references it applied as service-policy outbound.
!
! Please note that the 3850 can shape the outbound traffic on a port.
!
policy-map PM-ALL-StdOutbound
 class CM-DSCP-EF
  priority level 1 percent 20
  exit
 class CM-DSCP-AF41
  priority level 2 percent 40
  exit
 class CM-DSCP-AF31
  bandwidth remaining percent 5
  exit
 class CM-DSCP-AF21
  bandwidth remaining percent 10
  exit
 class class-default
  bandwidth remaining percent 25
  exit
 exit
```

```
!
! A shaping policy can be defined to provide shaped output to a circuit
! with throughput set to less than the physical port speed.  Note that the
! speed is given in bits per second, NOT kilobits or megabits per second.
!
! The 'shape average' should be set to 95% of the contracted circuit data
! rate.
!
policy-map PM-E2R-Shape-5M
 class class-default
  shape average 4700000
  service-policy PM-ALL-StdOutbound
  exit
 exit
!
! Policy map for testing, zero out dscp
!
! Used for testing only!!!!
!
policy-map PM-ZAP
 class class-default
  set dscp default
  exit
 exit
```

Application to Switch Ports

```
!================================================================================
! Normal User ports or trunks – traffic needs to be marked and/or policed
!
interface range Gi1/0/1-2
 service-policy input PM-E2R-User
 service-policy output PM-ALL-StdOutbound
 exit
!
!================================================================================
! Normal User ports or trunks – traffic needs to be marked but not policed
!
interface range Gi1/0/1-2
 service-policy input PM-E2R-UserNP
 service-policy output PM-ALL-StdOutbound
 exit
!
!================================================================================
! Normal User ports or trunks – traffic already marked, no need to police
!
interface range Gi1/0/1-2
 service-policy input PM-E2R-Trust
 service-policy output PM-ALL-StdOutbound
 exit
!
!================================================================================
!
! Trunk Ports coming FROM subsidiary switches or WAPs being aggregated –
! traffic needs to be marked; no policing allowed.
!
!   If using LACP based port-channels to aggregate traffic, these commands
!   must be applied on each component interface and generally cannot
!   be applied to the logical port-channel interface – this may be IOS
!   version dependent.
!
interface Gi1/0/25
 service-policy input PM-E2R-UserNP
 service-policy output PM-ALL-StdOutbound
```

```
 exit
!
!=============================================================================
!
! Trunk Ports coming FROM subsidiary switches or WAPs being aggregated –
! traffic already marked, no policing needed.  Port must be set to trust
! dscp.
!
!   If using LACP based port-channels to aggregate traffic, these commands
!   must be applied on each component interface and generally cannot
!   be applied to the logical port-channel interface.
!
interface Gi1/0/25
 qos trust dscp
 service-policy output PM-ALL-StdOutbound
 exit
!
!=============================================================================
!
! WAN Port – traffic needs to be classified and marked, traffic going
! through another device that will do shaping
!
!
interface Gi1/0/24
 service-policy input PM-R2E-ClassifyInbound
 service-policy output PM-ALL-StdOutbound
 exit
!
!=============================================================================
!
! WAN Port – inbound traffic needs to be classified and marked and
! output shaped to 5Mbps
!
!
interface Gi1/0/24
 service-policy input PM-R2E-ClassifyInbound
 service-policy output PM-E2R-Shape-5M
 exit
!
```

Routers

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

Class-maps and Policy-maps for all IOS versions

```
!
! Define Inbound Class Maps for ISP circuits
!
!-----------------------------------------------------------------
! Create DSCP based QoS class matches
!
!
class-map match-any CM-DSCP-EF
 match dscp ef
 exit
!
class-map match-any CM-DSCP-AF41
 match dscp af41
 exit
!
class-map match-any CM-DSCP-AF31
 match dscp af31
 exit
!
class-map match-any CM-DSCP-AF21
 match dscp af21
 exit
!
!================================================================
!
! 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.
!
! If there is any interface through which unmarked traffic enters
! the router you may utilize the PM-E2R-UserNP policy-map
! to mark the traffic.  Do not do this unless it is needed as it
! presents a large CPU load to the router.
!
!----------------------------------------------------------------
! Standard QoS Policy
!   This policy will apportion bandwidth based upon 20% EF, 15% AF41,
!   5% AF31, 10% AF21.
!
!   Must be the child of a shaping policy if contracted bandwidth is
!   less than the physical interface bandwidth.
!
policy-map PM-ALL-StdOutbound
 class CM-DSCP-EF
  priority percent 20
  set cos 5
  exit
 class CM-DSCP-AF41
  bandwidth percent 15
  set cos 4
  exit
 class CM-DSCP-AF31
  bandwidth percent 5
  set cos 3
  exit
 class CM-DSCP-AF21
```

```
  bandwidth percent 10
  set cos 2
  exit
 class class-default
  set dscp default
  set cos 0
  exit
 exit
!
!-----------------------------------------------------------------
! Outbound QoS Policy to circuit peered with a RingCentral Data Center.
! A peering link to RC will have higher percentages of traffic going to RC.
!
!
!   Must be the child of a shaping policy if contracted bandwidth is
!   less than the physical interface bandwidth.
!
policy-map PM-E2R-RCFeed
 class CM-DSCP-EF
  priority percent 55
  exit
 class CM-DSCP-AF41
  bandwidth percent 30
  exit
 class CM-DSCP-AF31
  bandwidth percent 9
  exit
 class CM-DSCP-AF21
  bandwidth percent 5
  exit
 class class-default
  set dscp default
  exit
 exit
!
! Policy maps for ports that receive inbound RC traffic.  This policy
! is used to restore the proper tags to traffic after it traverses the
! public Internet.
!
policy-map PM-R2E-ClassifyInbound
 class CM-R2E-RC-Voice
  set ip dscp ef
  exit
 class CM-R2E-RC-Video
  set ip dscp af41
  exit
 class CM-R2E-RC-Signal
  set ip dscp af31
  exit
 class CM-R2E-RC-Other
  set ip dscp af21
  exit
class class-default
  set ip dscp default
  exit
 exit
!
! Policy map for testing: zero out dscp
!
! Used for testing only!!!!
!
policy-map PM-ZAP
 class class-default
  set ip dscp default
  exit
 exit
!
```

Applying to Interfaces and Shaping

```
! ********************************************************************
! * CRITICAL - Shaping *MUST* be applied to any circuit operating      *
! * at less than full physical interface/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 to Ring Central 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-E2R-RCFeed-100M
 class class-default
  shape average 95m
  service-policy PM-E2R-RCFeed
  exit
 exit
!
! 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 DataCenter
 bandwidth 100000        ! Use the real number in kbps here, not the 95% number
 priority-queue out      ! may or may not be required or allowed
 service-policy out PM-E2R-RCFeed-100M
 service-policy in PM-R2E-ClassifyInbound
 exit
!
!====================================================================
! Link to ISP
!
! Create shaping parent policy, set shaping average to 95% of the
! contracted UPSTREAM data rate.  You may use g, m, or k in the rate.
!
policy-map PM-E2R-Standard-5M
 class class-default
  shape average 4500k    ! Use the 95% number in kbps here, not the real number
  service-policy PM-ALL-StdOutbound
  exit
 exit
!
! Apply shaping policy as outbound policy to interface.
! Apply standard QoS re-marking policy as inbound policy.
!
interface GigabitEthernet0/1
 description 5M link to an ISP
 bandwidth 5000 ! Use the real number in kbps here, not the 95% number
 priority-queue out      ! may or may not be required or allowed
 service-policy out PM-E2R-Standard-5M
 service-policy in PM-R2E-ClassifyInbound
 exit
!
!====================================================================
! 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      ! may or may not be required or allowed
 service-policy out PM-ALL-StdOutbound
 exit
```

Applying to MetroEthernet (P2MP) and Shaping per Destination

A Metro-Ethernet is essentially an E-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 specific for that site. The standard outbound policy is then applied to that class.

This type of network is problematic with respect to QoS as there is no coordination of bandwidth usage between multiple nodes. For instance, site 1 can be transmitting to site 2 and obeying the traffic shaping rules. Suddenly site 3, which has no way of knowing that site 1 is already sending data to site 2 at the full limit of the link to site 2, decides to send a large file to site 2 and completely overloads the site 2 link. When this happens voice and video quality suddenly drop and become unacceptable. VERY careful planning and consideration of all possible data flows must be undertaken when configuring this form of network.

```
!-------------------------------------------------------------------
! Class Maps to identify individual sites.  There MUST be exactly
! one acl/class-map combination per site.
!
! === 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
 exit
!
class-map match-any CM-Site3
 description Traffic destined for Site3
 match access-group name ACL-Site3
 exit
!
! === 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
 exit
!
class-map match-any CM-Site4
 description Traffic destined for Site4
 match access-group name ACL-Site4
 exit
!
! == 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 its own contracted data rate.
!-------------------------------------------------------------------
!
policy-map PM-R2E-MetroE-Shape
 class CM-Site3
  shape average 9500k
  service-policy PM-ALL-StdOutbound
  exit
 class CM-Site4
  shape average 190m
  service-policy PM-ALL-StdOutbound
  exit
!
! == repeat class, shape, and service-policy for every site
!
 exit
!
!-------------------------------------------------------------------
! 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 MetroEthernet
 ip address 192.168.30.1 255.255.255.0
 priority-queue out      ! may or may not be required or allowed
 service-policy out PM-R2E-MetroE-Shape
 exit
```

Applying to Vlans on a Trunk

A scenario may be established where multiple Vlans are set up with different services delivered per Vlan. Shaping may be applied on both a composite and per vlan basis.

```
!
! Use the following to shape for output to a VLAN trunk.
! Apply outbound to the physical trunk port.
! Modify based on other VLANS in trunk.
! Note that you may need both inbound and outbound versions.
!
class-map CM-Vlan-ISP
 match vlan 999
 exit
!
class-map CM-Vlan31
 match vlan 31
 exit
!
policy-map PM-OUT-MainTrunk
 class CM-Vlan-ISP
  shape average 95m
  service-policy PM-ALL-StdOutbound
  exit
 class CM-Vlan31
  shape average 895m
  service-policy PM-ALL-StdOutbound
  exit
 exit
!
policy-map PM-INB-MainTrunk
 class CM-Vlan-ISP
  service-policy PM-R2E-ClassifyInbound
  exit
 exit
```

```
!
!
interface GigabitEthernet0/0
 service-policy output PM-OUT-MainTrunk
 service-policy input PM-INB-MainTrunk
 no shutdown
 exit
!
```

Zone Based Firewalls (ZBF/ZFW)

Many Cisco IOS devices support the Cisco 'Zone Based Firewall' configuration options. Here are sample configuration snippets used to implement it. The example code defines 3 zones, Inside (LAN), Outside (INTERNET/WAN), and a direct link to RingCentral (only used for Direct Connect customers). The Inside and Outside policies are applied to two VLAN interfaces on the lab router.

The Zone Based Firewall does NOT perform QoS or traffic shaping. That must be implemented using the QoS configurations shown earlier. This is ONLY a security feature and is presented here due to numerous user requests.

Please note: ***These sample configurations utilize the access-list definitions created earlier in this appendix as part of the QoS solution.***

```
!
! Zone Based Firewall (ZBF) Configuration
!
! Define Class-Maps for use in policies
!
class-map type inspect match-all ZCM-R2E-RC-All
 match access-group name ACL-R2E-RC-All
 exit
!
class-map type inspect match-all ZCM-E2R-RC-All
 match access-group name ACL-E2R-RC-All
 exit
!
class-map type inspect match-all ZCM-R2E-RC-Signal
 match access-group name ACL-R2E-RC-Signal
 exit
!
class-map type inspect match-all ZCM-E2R-RC-Signal
 match access-group name ACL-E2R-RC-Signal
 exit
!
class-map type inspect match-all ZCM-R2E-RC-Voice
 match access-group name ACL-R2E-RC-Voice
 exit
!
class-map type inspect match-all ZCM-E2R-RC-Voice
 match access-group name ACL-E2R-RC-Voice
 exit
!
class-map type inspect match-all ZCM-R2E-RC-Video
 match access-group name ACL-R2E-RC-Video
 exit
!
class-map type inspect match-all ZCM-E2R-RC-Video
 match access-group name ACL-E2R-RC-Video
 exit
```

```
!
! This class map represents a user's security portion of the policy.  The class-maps
! defined above should always come FIRST in the policy-map, above all the
! non-RingCentral customer defined classes.
!
class-map type inspect match-any ZCM-RoutineStuff
 match protocol dns
 match protocol http
 match protocol https
 match protocol ntp
 match protocol ssh
 match protocol icmp
 match protocol tcp
 match protocol udp
 exit
!
! A policy-map (used in the zone-pair definition) should be defined for each flow
! direction of each zone-pair.
!

policy-map type inspect PM-Inside-2-Outside
 class type inspect ZCM-E2R-RC-Signal
  pass
  exit
 class type inspect ZCM-E2R-RC-Voice
  pass
  exit
 class type inspect ZCM-E2R-RC-Video
  pass
  exit
 class type inspect ZCM-E2R-RC-All
  pass
  exit
 class type inspect ZCM-RoutineStuff
  inspect
  exit
 class class-default
  drop log
  exit
 exit
!
policy-map type inspect PM-Inside-2-RingCentral
 class type inspect ZCM-E2R-RC-Signal
  pass
  exit
 class type inspect ZCM-E2R-RC-Voice
  pass
  exit
 class type inspect ZCM-E2R-RC-Video
  pass
  exit
 class type inspect ZCM-E2R-RC-All
  pass
  exit
 class class-default
  drop log
  exit
 exit
!
policy-map type inspect PM-Outside-2-Inside
 class type inspect ZCM-R2E-RC-Signal
  pass
  exit
 class type inspect ZCM-R2E-RC-Voice
  pass
  exit
 class type inspect ZCM-R2E-RC-Video
```

```
  pass
  exit
 class type inspect ZCM-R2E-RC-All
  pass
  exit
! insert class-maps to implement incoming customer policies here
! class type inspect xxxxxx
!  inspect
!  exit
 class class-default
  drop log
  exit
 exit
!
policy-map type inspect PM-RingCentral-2-Inside
 class type inspect ZCM-R2E-RC-Signal
  pass
  exit
 class type inspect ZCM-R2E-RC-Voice
  pass
  exit
 class type inspect ZCM-R2E-RC-Video
  pass
  exit
 class type inspect ZCM-R2E-RC-All
  pass
  exit
 class class-default
  drop log
  exit
 exit
!
! Nothing should EVER move from Outside toward RingCentral
!
policy-map type inspect PM-Outside-2-RingCentral
 class class-default
  drop
  exit
 exit
!
! Nothing should EVER move from RingCentral toward Outside
!
policy-map type inspect PM-RingCentral-2-Outside
 class class-default
  drop
  exit
 exiut
```

Now that the policy-maps are defined we need to set up the Zone Based Firewall elements, the zones and the zone-pairs and then apply them to the correct interfaces.

```
zone security ZN-Inside
zone security ZN-Outside
zone security ZN-RingCentral

zone-pair security ZNP-Inside-2-Outside source ZN-Inside destination ZN-Outside
  service-policy type inspect PM-Inside-2-Outside

zone-pair security ZNP-Inside-2-RingCentral source ZN-Inside destination ZN-RingCentral
  service-policy type inspect PM-Inside-2-RingCentral

zone-pair security ZNP-Outside-2-Inside source ZN-Outside destination ZN-Inside
  service-policy type inspect PM-Outside-2-Inside

zone-pair security ZNP-Outside-2-RingCentral source ZN-Outside destination ZN-RingCentral
```

```
  service-policy type inspect PM-Outside-2-RingCentral

zone-pair security ZNP-RingCentral-2-Outside source ZN-RingCentral destination ZN-Outside
  service-policy type inspect PM-RingCentral-2-Outside

zone-pair security ZNP-RingCentral-2-Inside source ZN-RingCentral destination ZN-Inside
  service-policy type inspect PM-RingCentral-2-Inside

! Outside (Internet) Interface is Gi0/0.306
interface Gi0/0.306
  zone-member security ZN-Outside

! Inside (LAN) Interface is Gi0/1.397
interface Gi0/1.397
  zone-member security ZN-Inside
```

The sample configuration shown above will work properly with RingCentral applications and phones.

NX-OS Based Cisco (Nexus)

Access and Aggregation / Distribution Switches (MQC based – Nexus Family)

The Nexus line does NOT use the access-lists/object groups defined in 'IOS Universal Configuration Elements Shared by All Cisco IOS Configurations' at the beginning of this document. You will find them defined in this section with proper syntax for NX-OS.

The Nexus family of switches are generally used in Data Center applications as Aggregation/Distribution Switches. It is assumed that traffic flowing into the Nexus switch from 'downstream' customer switches is already marked with the correct DSCP tag value. If any port is connected to a 'WAN' source that does not provide pre-classified traffic with proper DSCP markings, you must manually classify it.

```
!================================================================================
! Nexus 5548 QoS config - required on all units
! For version 5.2(1)N1(1)
```

Use the following Packet Matching syntax for Nexus 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.  This version uses network object groups.
!--------------------------------------------------------------------
!
! Create lists and objects
!
object-group ip address NOG-RingCentral
 ! description All RC Public Networks a/o 20200813
 66.81.240.0 255.255.240.0
 80.81.128.0 255.255.240.0
 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 ip port SOG-TCP-E2R-RC-Signal
 ! description RC SIP service identifiers a/o 20190529
 range 5090 5099
 range 8083 8090
 range 5060 5061
 exit
!
object-group ip port SOG-TCP-R2E-RC-Signal
 ! description RC SIP service identifiers a/o 20190529
 range 5090 5099
 range 8083 8090
 range 5060 5961
 exit
```

```
!
object-group ip port SOG-UDP-E2R-RC-Signal
 ! description RC SIP service identifiers a/o 20190529
 range 5090 5099
 eq 5060
 exit
!
object-group ip port SOG-UDP-R2E-RC-Signal
 ! description RC SIP service identifiers a/o 20190529
 range 5090 5099
 eq 5060
 exit
!
object-group ip port SOG-TCP-E2R-RC-RTPMeeting
 ! description RC Meeting RTP service identifiers a/o 20190529
 range 8801 8802
 exit
!
object-group ip port SOG-TCP-R2E-RC-RTPMeeting
 ! description RC Meeting RTP service identifiers a/o 20190529
 range 8801 8802
 exit
!
object-group ip port SOG-UDP-E2R-RC-RTPMeeting
 ! description RC Meeting RTP service identifiers a/o 20190529
 range 8801 8802
 range 10000 19999
 exit
!
object-group ip port SOG-UDP-R2E-RC-RTPMeeting
 ! description RC Meeting RTP service identifiers a/o 20190529
 range 8801 8802
 range 10000 19999
 exit
!
object-group ip port SOG-UDP-E2R-RC-RTPAudio
 ! description RC Meeting RTP service identifiers a/o 20190529
 range 20000 64999
 eq 8803
 exit
!
object-group ip port SOG-UDP-R2E-RC-RTPAudio
 ! description RC Meeting RTP service identifiers a/o 20190529
 range 20000 64999
 eq 8803
 exit
!
! All RC network traffic not otherwise marked will be marked as AF21 traffic
!
ip access-list ACL-E2R-RC-All
 permit ip any addrgroup NOG-RingCentral
 exit
!
ip access-list ACL-R2E-RC-All
 permit ip addrgroup NOG-RingCentral any
 exit
!
! General signaling traffic will be marked AF31 traffic
!
ip access-list ACL-E2R-RC-Signal
 permit tcp any addrgroup NOG-RingCentral portgroup SOG-TCP-E2R-RC-Signal
 permit udp any addrgroup NOG-RingCentral portgroup SOG-UDP-E2R-RC-Signal
 exit
!
ip access-list ACL-R2E-RC-Signal
 permit tcp addrgroup NOG-RingCentral portgroup SOG-TCP-E2R-RC-Signal any
 permit udp addrgroup NOG-RingCentral portgroup SOG-UDP-E2R-RC-Signal any
```

```
 exit
!
! Phone / Softphone voice RT traffic will be marked EF traffic
!
ip access-list ACL-E2R-RC-Voice
 permit udp any addrgroup NOG-RingCentral portgroup SOG-UDP-E2R-RC-RTPAudio
 exit
!
ip access-list ACL-R2E-RC-Voice
 permit udp addrgroup NOG-RingCentral portgroup SOG-UDP-E2R-RC-RTPAudio any
 exit
!
! RC Meetings Video RT traffic will be marked AF41 traffic
!
ip access-list ACL-E2R-RC-Video
 permit udp any addrgroup NOG-RingCentral portgroup SOG-UDP-E2R-RC-RTPMeeting
 permit tcp any addrgroup NOG-RingCentral portgroup SOG-TCP-E2R-RC-RTPMeeting
 exit
!
ip access-list ACL-R2E-RC-Video
 permit udp addrgroup NOG-RingCentral portgroup SOG-UDP-E2R-RC-RTPMeeting any
 permit tcp addrgroup NOG-RingCentral portgroup SOG-TCP-E2R-RC-RTPMeeting any
 exit
```

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

```
!--------------------------------------------------------------------
! Define Access Lists to Identify and Classify traffic FROM users/WAPs
! going TO RingCentral.
!--------------------------------------------------------------------
!
! All RC network traffic will be marked as AF21 traffic if not otherwise
! classified
!
no ip access-list ACL-E2R-RC-All
ip access-list ACL-E2R-RC-All
 permit ip any 66.81.240.0 0.0.15.255
 permit ip any 80.81.128.0 0.0.15.255
 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 199.68.212.0 0.0.3.255
 permit ip any 199.255.120.0 0.0.3.255
 permit ip any 208.87.40.0 0.0.3.255
 exit
!
no ip access-list ACL-R2E-RC-All
ip access-list ACL-R2E-RC-All
 permit ip 66.81.240.0 0.0.15.255 any
 permit ip 80.81.128.0 0.0.15.255 any
 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 199.68.212.0 0.0.3.255 any
 permit ip 199.255.120.0 0.0.3.255 any
 permit ip 208.87.40.0 0.0.3.255 any
 exit
!
! General SIP traffic will be marked AF31 traffic
!
no ip access-list ACL-E2R-RC-Signal
ip access-list ACL-E2R-RC-Signal
 permit tcp any 66.81.240.0 0.0.15.255 range 5090 5099
 permit tcp any 80.81.128.0 0.0.15.255 range 5090 5099
```

```
 permit tcp any 103.44.68.0 0.0.3.255 range 5090 5099
 permit tcp any 104.245.56.0 0.0.7.255 range 5090 5099
 permit tcp any 185.23.248.0 0.0.3.255 range 5090 5099
 permit tcp any 192.209.24.0 0.0.7.255 range 5090 5099
 permit tcp any 199.68.212.0 0.0.3.255 range 5090 5099
 permit tcp any 199.255.120.0 0.0.3.255 range 5090 5099
 permit tcp any 208.87.40.0 0.0.3.255 range 5090 5099
 permit udp any 66.81.240.0 0.0.15.255 range 5090 5099
 permit udp any 80.81.128.0 0.0.15.255 range 5090 5099
 permit udp any 103.44.68.0 0.0.3.255 range 5090 5099
 permit udp any 104.245.56.0 0.0.7.255 range 5090 5099
 permit udp any 185.23.248.0 0.0.3.255 range 5090 5099
 permit udp any 192.209.24.0 0.0.7.255 range 5090 5099
 permit udp any 199.68.212.0 0.0.3.255 range 5090 5099
 permit udp any 199.255.120.0 0.0.3.255 range 5090 5099
 permit udp any 208.87.40.0 0.0.3.255 range 5090 5099
 permit tcp any 66.81.240.0 0.0.15.255 range 8083 8090
 permit tcp any 80.81.128.0 0.0.15.255 range 8083 8090
 permit tcp any 103.44.68.0 0.0.3.255 range 8083 8090
 permit tcp any 104.245.56.0 0.0.7.255 range 8083 8090
 permit tcp any 185.23.248.0 0.0.3.255 range 8083 8090
 permit tcp any 192.209.24.0 0.0.7.255 range 8083 8090
 permit tcp any 199.68.212.0 0.0.3.255 range 8083 8090
 permit tcp any 199.255.120.0 0.0.3.255 range 8083 8090
 permit tcp any 208.87.40.0 0.0.3.255 range 8083 8090
 permit tcp any 66.81.240.0 0.0.15.255 range 5060 5061
 permit tcp any 80.81.128.0 0.0.15.255 range 5060 5061
 permit tcp any 103.44.68.0 0.0.3.255 range 5060 5061
 permit tcp any 104.245.56.0 0.0.7.255 range 5060 5061
 permit tcp any 185.23.248.0 0.0.3.255 range 5060 5061
 permit tcp any 192.209.24.0 0.0.7.255 range 5060 5061
 permit tcp any 199.68.212.0 0.0.3.255 range 5060 5061
 permit tcp any 199.255.120.0 0.0.3.255 range 5060 5061
 permit tcp any 208.87.40.0 0.0.3.255 range 5060 5061
 permit udp any 66.81.240.0 0.0.15.255 eq 5060
 permit udp any 80.81.128.0 0.0.15.255 eq 5060
 permit udp any 103.44.68.0 0.0.3.255 eq 5060
 permit udp any 104.245.56.0 0.0.7.255 eq 5060
 permit udp any 185.23.248.0 0.0.3.255 eq 5060
 permit udp any 192.209.24.0 0.0.7.255 eq 5060
 permit udp any 199.68.212.0 0.0.3.255 eq 5060
 permit udp any 199.255.120.0 0.0.3.255 eq 5060
 permit udp any 208.87.40.0 0.0.3.255 eq 5060
 exit
!
no ip access-list ACL-R2E-RC-Signal
ip access-list ACL-R2E-RC-Signal
 permit tcp 66.81.240.0 0.0.15.255 range 5090 5099 any
 permit tcp 80.81.128.0 0.0.15.255 range 5090 5099 any
 permit tcp 103.44.68.0 0.0.3.255 range 5090 5099 any
 permit tcp 104.245.56.0 0.0.7.255 range 5090 5099 any
 permit tcp 185.23.248.0 0.0.3.255 range 5090 5099 any
 permit tcp 192.209.24.0 0.0.7.255 range 5090 5099 any
 permit tcp 199.68.212.0 0.0.3.255 range 5090 5099 any
 permit tcp 199.255.120.0 0.0.3.255 range 5090 5099 any
 permit tcp 208.87.40.0 0.0.3.255 range 5090 5099 any
 permit udp 66.81.240.0 0.0.15.255 range 5090 5099 any
 permit udp 80.81.128.0 0.0.15.255 range 5090 5099 any
 permit udp 103.44.68.0 0.0.3.255 range 5090 5099 any
 permit udp 104.245.56.0 0.0.7.255 range 5090 5099 any
 permit udp 185.23.248.0 0.0.3.255 range 5090 5099 any
 permit udp 192.209.24.0 0.0.7.255 range 5090 5099 any
 permit udp 199.68.212.0 0.0.3.255 range 5090 5099 any
 permit udp 199.255.120.0 0.0.3.255 range 5090 5099 any
 permit udp 208.87.40.0 0.0.3.255 range 5090 5099 any
 permit tcp 66.81.240.0 0.0.15.255 range 8083 8090 any
 permit tcp 80.81.128.0 0.0.15.255 range 8083 8090 any
```

```
 permit tcp 103.44.68.0 0.0.3.255 range 8083 8090 any
 permit tcp 104.245.56.0 0.0.7.255 range 8083 8090 any
 permit tcp 185.23.248.0 0.0.3.255 range 8083 8090 any
 permit tcp 192.209.24.0 0.0.7.255 range 8083 8090 any
 permit tcp 199.68.212.0 0.0.3.255 range 8083 8090 any
 permit tcp 199.255.120.0 0.0.3.255 range 8083 8090 any
 permit tcp 208.87.40.0 0.0.3.255 range 8083 8090 any
 permit tcp 66.81.240.0 0.0.15.255 range 5060 5061 any
 permit tcp 80.81.128.0 0.0.15.255 range 5060 5061 any
 permit tcp 103.44.68.0 0.0.3.255 range 5060 5061 any
 permit tcp 104.245.56.0 0.0.7.255 range 5060 5061 any
 permit tcp 185.23.248.0 0.0.3.255 range 5060 5061 any
 permit tcp 192.209.24.0 0.0.7.255 range 5060 5061 any
 permit tcp 199.68.212.0 0.0.3.255 range 5060 5061 any
 permit tcp 199.255.120.0 0.0.3.255 range 5060 5061 any
 permit tcp 208.87.40.0 0.0.3.255 range 5060 5061 any
 permit udp 66.81.240.0 0.0.15.255 eq 5060 any
 permit udp 80.81.128.0 0.0.15.255 eq 5060 any
 permit udp 103.44.68.0 0.0.3.255 eq 5060 any
 permit udp 104.245.56.0 0.0.7.255 eq 5060 any
 permit udp 185.23.248.0 0.0.3.255 eq 5060 any
 permit udp 192.209.24.0 0.0.7.255 eq 5060 any
 permit udp 199.68.212.0 0.0.3.255 eq 5060 any
 permit udp 199.255.120.0 0.0.3.255 eq 5060 any
 permit udp 208.87.40.0 0.0.3.255 eq 5060 any
 exit
!
! Phone / Softphone voice RT traffic will be marked EF traffic
!
no ip access-list ACL-E2R-RC-Voice
ip access-list ACL-E2R-RC-Voice
 permit udp any 66.81.240.0 0.0.15.255 range 20000 64999
 permit udp any 80.81.128.0 0.0.15.255 range 20000 64999
 permit udp any 103.44.68.0 0.0.3.255 range 20000 64999
 permit udp any 104.245.56.0 0.0.7.255 range 20000 64999
 permit udp any 185.23.248.0 0.0.3.255 range 20000 64999
 permit udp any 192.209.24.0 0.0.7.255 range 20000 64999
 permit udp any 199.255.120.0 0.0.3.255 range 20000 64999
 permit udp any 199.68.212.0 0.0.3.255 range 20000 64999
 permit udp any 208.87.40.0 0.0.3.255 range 20000 64999
 permit udp any 66.81.240.0 0.0.15.255 eq 8803
 permit udp any 80.81.128.0 0.0.15.255 eq 8803
 permit udp any 103.44.68.0 0.0.3.255 eq 8803
 permit udp any 104.245.56.0 0.0.7.255 eq 8803
 permit udp any 185.23.248.0 0.0.3.255 eq 8803
 permit udp any 192.209.24.0 0.0.7.255 eq 8803
 permit udp any 199.255.120.0 0.0.3.255 eq 8803
 permit udp any 199.68.212.0 0.0.3.255 eq 8803
 permit udp any 208.87.40.0 0.0.3.255 eq 8803
 exit
!
no ip access-list ACL-R2E-RC-Voice
ip access-list ACL-R2E-RC-Voice
 permit udp 66.81.240.0 0.0.15.255 range 20000 64999 any
 permit udp 80.81.128.0 0.0.15.255 range 20000 64999 any
 permit udp 103.44.68.0 0.0.3.255 range 20000 64999 any
 permit udp 104.245.56.0 0.0.7.255 range 20000 64999 any
 permit udp 185.23.248.0 0.0.3.255 range 20000 64999 any
 permit udp 192.209.24.0 0.0.7.255 range 20000 64999 any
 permit udp 199.255.120.0 0.0.3.255 range 20000 64999 any
 permit udp 199.68.212.0 0.0.3.255 range 20000 64999 any
 permit udp 208.87.40.0 0.0.3.255 range 20000 64999 any
 permit udp 66.81.240.0 0.0.15.255 eq 8803 any
 permit udp 80.81.128.0 0.0.15.255 eq 8803 any
 permit udp 103.44.68.0 0.0.3.255 eq 8803 any
 permit udp 104.245.56.0 0.0.7.255 eq 8803 any
 permit udp 185.23.248.0 0.0.3.255 eq 8803 any
```

```
 permit udp 192.209.24.0 0.0.7.255 eq 8803 any
 permit udp 199.255.120.0 0.0.3.255 eq 8803 any
 permit udp 199.68.212.0 0.0.3.255 eq 8803 any
 permit udp 208.87.40.0 0.0.3.255 eq 8803 any
 exit
!
! RC Meetings Video RT traffic or premarked AF41/CS4 traffic
!
no ip access-list ACL-E2R-RC-Video
ip access-list ACL-E2R-RC-Video
 permit udp any 66.81.240.0 0.0.15.255 range 8801 8802
 permit udp any 80.81.128.0 0.0.15.255 range 8801 8802
 permit udp any 103.44.68.0 0.0.3.255 range 8801 8802
 permit udp any 104.245.56.0 0.0.7.255 range 8801 8802
 permit udp any 185.23.248.0 0.0.3.255 range 8801 8802
 permit udp any 192.209.24.0 0.0.7.255 range 8801 8802
 permit udp any 199.255.120.0 0.0.3.255 range 8801 8802
 permit udp any 199.68.212.0 0.0.3.255 range 8801 8802
 permit udp any 208.87.40.0 0.0.3.255 range 8801 8802
 permit tcp any 66.81.240.0 0.0.15.255 range 8801 8802
 permit tcp any 80.81.128.0 0.0.15.255 range 8801 8802
 permit tcp any 103.44.68.0 0.0.3.255 range 8801 8802
 permit tcp any 104.245.56.0 0.0.7.255 range 8801 8802
 permit tcp any 185.23.248.0 0.0.3.255 range 8801 8802
 permit tcp any 192.209.24.0 0.0.7.255 range 8801 8802
 permit tcp any 199.68.212.0 0.0.3.255 range 8801 8802
 permit tcp any 199.255.120.0 0.0.3.255 range 8801 8802
 permit tcp any 208.87.40.0 0.0.3.255 range 8801 8802
 permit udp any 66.81.240.0 0.0.15.255 range 10000 19999
 permit udp any 80.81.128.0 0.0.15.255 range 10000 19999
 permit udp any 103.44.68.0 0.0.3.255 range 10000 19999
 permit udp any 104.245.56.0 0.0.7.255 range 10000 19999
 permit udp any 185.23.248.0 0.0.3.255 range 10000 19999
 permit udp any 192.209.24.0 0.0.7.255 range 10000 19999
 permit udp any 199.255.120.0 0.0.3.255 range 10000 19999
 permit udp any 199.68.212.0 0.0.3.255 range 10000 19999
 permit udp any 208.87.40.0 0.0.3.255 range 10000 19999
 exit
!
no ip access-list ACL-R2E-RC-Video
ip access-list ACL-R2E-RC-Video
 permit udp 66.81.240.0 0.0.15.255 range 8801 8802 any
 permit udp 80.81.128.0 0.0.15.255 range 8801 8802 any
 permit udp 103.44.68.0 0.0.3.255 range 8801 8802 any
 permit udp 104.245.56.0 0.0.7.255 range 8801 8802 any
 permit udp 185.23.248.0 0.0.3.255 range 8801 8802 any
 permit udp 192.209.24.0 0.0.7.255 range 8801 8802 any
 permit udp 199.255.120.0 0.0.3.255 range 8801 8802 any
 permit udp 199.68.212.0 0.0.3.255 range 8801 8802 any
 permit udp 208.87.40.0 0.0.3.255 range 8801 8802 any
 permit tcp 66.81.240.0 0.0.15.255 range 8801 8802 any
 permit tcp 80.81.128.0 0.0.15.255 range 8801 8802 any
 permit tcp 103.44.68.0 0.0.3.255 range 8801 8802 any
 permit tcp 104.245.56.0 0.0.7.255 range 8801 8802 any
 permit tcp 185.23.248.0 0.0.3.255 range 8801 8802 any
 permit tcp 192.209.24.0 0.0.7.255 range 8801 8802 any
 permit tcp 199.68.212.0 0.0.3.255 range 8801 8802 any
 permit tcp 199.255.120.0 0.0.3.255 range 8801 8802 any
 permit tcp 208.87.40.0 0.0.3.255 range 8801 8802 any
 permit udp 66.81.240.0 0.0.15.255 range 10000 19999 any
 permit udp 80.81.128.0 0.0.15.255 range 10000 19999 any
 permit udp 103.44.68.0 0.0.3.255 range 10000 19999 any
 permit udp 104.245.56.0 0.0.7.255 range 10000 19999 any
 permit udp 185.23.248.0 0.0.3.255 range 10000 19999 any
 permit udp 192.209.24.0 0.0.7.255 range 10000 19999 any
 permit udp 199.255.120.0 0.0.3.255 range 10000 19999 any
 permit udp 199.68.212.0 0.0.3.255 range 10000 19999 any
```

```
 permit udp 208.87.40.0 0.0.3.255 range 10000 19999 any
 exit
```

Class-maps and Policy-maps for all Nexus versions

```
!-----------------------------------------------------------------
! Establish Class-Maps for matching port ingress traffic traveling
! from RingCentral to the customer endpoint
!
! Classify all Voice RTP traffic
!
class-map type qos CM-R2E-RC-Voice
 match access-group name ACL-R2E-RC-Voice
 exit
!
! Ditto Video RTP
!
class-map type qos CM-R2E-RC-Video
 match access-group name ACL-R2E-RC-Video
 exit
!
! Ditto SIP Control
!
class-map type qos CM-R2E-RC-Signal
 match access-group name ACL-R2E-RC-Signal
 exit
!
! Ditto all other traffic from RC
!
class-map type qos CM-R2E-RC-All
 match access-group name ACL-R2E-RC-All
 exit
!
! Define a policy map that will take traffic coming IN from an Internet/WAN
! connection and set the DSCP markings  (qos-group is used to internally mark
! the packet within the switch for output queuing)
!
policy-map type qos PM-R2E-ClassifyInbound
 class type qos CM-R2E-RC-Voice
  set dscp ef
  set qos-group 5
  exit
 class type qos CM-R2E-RC-Video
  set dscp af41
  set qos-group 4
  exit
 class type qos CM-R2E-RC-Signal
  set dscp af31
  set qos-group 3
  exit
 class type qos CM-R2E-RC-All
  set dscp af21
  set qos-group 2
  exit
 class class-default
  set dscp default
  exit
 exit
!
!================================================================================
! Define queueing rules for traffic ingressing any interface headed from the
! customer endpoint toward RingCentral (DEFAULT INPUT POLICY)
!
! Note that this traffic must have already had DSCP marks applied, either by the
! input policy map or by the access switches that feed this switch.
!
! Inbound Voice RTP
```

```
!
class-map type qos match-any CM-DSCP-EF
 match dscp ef cs5
 exit
!
! Ditto Video RTP
!
class-map type qos match-any CM-DSCP-AF41
 match dscp af41 cs4
 exit
!
! Ditto SIP Signaling
!
class-map type qos match-any CM-DSCP-AF31
 match dscp af31 cs3
 exit
!
! Ditto all other RC traffic
!
class-map type qos match-any CM-DSCP-AF21
 match dscp af21 cs2
 exit
!
! This is the actual inbound qos policy.
!
policy-map type qos PM-IB-Standard
 class type qos CM-DSCP-EF
  set qos-group 5
  exit
 class type qos CM-DSCP-AF41
  set qos-group 4
  exit
 class type qos CM-DSCP-AF31
  set qos-group 3
  exit
 class type qos CM-DSCP-AF21
  set qos-group 2
  exit
 exit
!
!================================================================================
! Define queueing rules for traffic going OUT ANY interface (DEFAULT OUTPUT POLICY)
!
! Note that this traffic should have already had DSCP marks and qos-group
! applied by the input policy map.
!
! Outbound Voice RTP
!
class-map type queuing CM-QG5
 match qos-group 5
 exit
!
! Ditto Video RTP
!
class-map type queuing CM-QG4
 match qos-group 4
 exit
!
! Ditto SIP Signaling
!
class-map type queuing CM-QG3
 match qos-group 3
 exit
!
! Ditto all other RC traffic
!
class-map type queuing CM-QG2
```

```
 match qos-group 2
 exit
!
! This is the actual outbound queueing policy.
! Note that the first two classes must be present in this format.
!
! Any unused capacity is given to other classes proportionally.
!
policy-map type queuing PM-OB-Standard
 class type queuing class-default
  bandwidth percent 10
  exit
 class type queuing CM-QG5
  priority
  exit
 class type queuing CM-QG4
  bandwidth percent 30
  exit
 class type queuing CM-QG3
  bandwidth percent 10
  exit
 class type queuing CM-QG2
  bandwidth percent 10
  exit
 exit
!
! Enable MQC QoS and set the default output and input policies.
!
system qos
 service-policy type queuing output PM-OB-Standard
 service-policy type qos input PM-IB-Standard
 exit
!
!================================================================================
!
! FOR EVERY INTERFACE CONNECTED TO THE OUTSIDE WORLD
!
! Unless traffic has already been classified and had DSCP tags set you *MUST* set up
! the inbound interface(s) to do this.
!
interface ethernet y/x
 service-policy type qos input PM-R2E-ClassifyInbound
 exit
!
! FOR EVERY INTERFACE ON WHICH YOU NEED TO OVERRIDE THE OUTBOUND QUEUEING POLICY
!
! Note that this is only needed if you want to override the default policy.
! All interfaces have a default from the 'system qos' declaration.
!
!interface ethernet y/x
! service-policy type queuing output PM-OB-Standard
! exit
!
! FOR EVERY INTERFACE ON WHICH YOU NEED TO OVERRIDE THE INBOUND CLASSIFICATION POLICY
!
! Note that this is only needed if you want to override the default policy.
! All interfaces have a default from the 'system qos' declaration.
!
!interface ethernet y/x
! service-policy type qos input PM-IB-Standard
! exit
!
!-------------------------------------------------------------------------
! The 5548 does not do shaping, so the firewalls *MUST* implement outbound
! shaping policies.
!-------------------------------------------------------------------------
```

ASA Firewalls

Many RingCentral customers use Cisco ASA series devices as firewalls to protect their networks, establish VPN tunnels, and sometimes to interface with their service provider(s). This paper was written to provide configuration guidance for use with RingCentral services.

It is important to note that the ASA devices only provide one level of prioritization and, as such, are not an optimal device for establishing QoS. The ASA devices cannot apply or change DSCP markings; that must be done in another device. Also note that the -X series (multi-core) cannot provide the critical QoS traffic shaping services; another device must be used to perform shaping.

Bug Work-Around

A program error exists in the ASA software releases prior to and including version 9.6(1). The code below can be used to implement a work-around. Please note that this bug will impact *all* TCP traffic, not just RingCentral's.

```
!================================================================================
! Bug (CSCuq807040 exists in ASA software releases prior to and including 9.6(1)
! The ASA software incorrectly drops connections when the TCP Timestamp value wraps
! around the 2^32 value.  A tcp-map can be used to disable the timestamp option on
! connections.
!
tcp-map TCPM-ClearTsOption
 tcp-options timestamp clear
 exit
!
access-list ACL-TimestampTCP extended permit tcp any any
!
class-map CM-TcpTimestampMap
 match access-list ACL-TimestampTCP
 exit
!
policy-map global_policy
 class CM-TcpTimestampMap
  set connection advanced-options TCPM-ClearTsOption
  exit
 exit
```

Traffic Prioritization / Queuing / Shaping

```
!================================================================================
! Define an object group to identify traffic destined to or originating from
! the RingCentral public address spaces.
!
object-group network NWOG-RC-AllPublic
 description RingCentral Public Addresses a/o 20200813
 network-object 66.81.240.0 255.255.240.0
 network-object 80.81.128.0 255.255.240.0
 network-object 103.44.68.0 255.255.252.0
 network-object 104.245.56.0 255.255.248.0
 network-object 185.23.248.0 255.255.252.0
 network-object 192.209.24.0 255.255.248.0
 network-object 199.255.120.0 255.255.252.0
 network-object 199.68.212.0 255.255.252.0
 network-object 208.87.40.0 255.255.252.0
!
! Use the above defined network object group to create access-list entries
! to identify inbound and outbound RingCentral traffic.  No attempt is made
```

```
! to differentiate types of traffic as the ASA only has one priority level.
! All RingCentral traffic will be identified by these access-lists.
!
access-list ACL-IB-RC-Traffic extended permit ip object-group NWOG-RC-AllPublic any
access-list ACL-OB-RC-Traffic extended permit ip any object-group NWOG-RC-AllPublic
!
! Match rule for traffic that already has DSCP markings.
!
class-map CM-DSCP-Priority
 match dscp ef cs5 af41 cs4 af31 cs3 af21
 exit
!
! Match rule for traffic coming FROM RingCentral to customer.
!
class-map CM-IB-RCPriority
 match access-list ACL-IB-RC-Traffic
 exit
!
! Match rule for traffic going from customer TO RingCentral.
!
class-map CM-OB-RCPriority
 match access-list ACL-OB-RC-Traffic
 exit
!
! Policy map to prioritize Inbound traffic from RingCentral
!
policy-map PM-IB-Priority
 !
 ! Matching based on existing markings is optional and should only
 ! be done if you trust the inbound DSCP markings.  If you have a
 ! switch or router between the ASA and the service provider you
 ! should have it mark the traffic and trust it.
 !
 class CM-DSCP-Priority
  priority
  exit
 !
 ! Matching based upon address flows may be used if you do not have
 ! a switch or router between the ASA and the service provider to
 ! pre-mark the traffic.
 !
 class CM-IB-RCPriority
  priority
  exit
 exit
!
! Policy map to prioritize Outbound traffic to RingCentral
!
policy-map PM-OB-Priority
  !
  ! Matching based on existing markings is preferred and should
  ! be done if you trust the inbound DSCP markings.  You should have a
  ! switch or router between the ASA and the customer LAN that applies
  ! DSCP markings to the traffic.  Remove this class if you do not
  ! have such an arrangement.
  !
 class CM-DSCP-Priority
  priority
  exit
  !
  ! Matching based upon address flows may be used if you do not have
  ! a switch or router between the ASA and the customer network to
  ! pre-mark the traffic.
  !
 class CM-OB-RCPriority
  priority
  exit
```

```
 exit
!
! Policy map to prioritize *AND* shape outbound traffic to RingCentral on a
! 20 Mbps link.  Always set shaping to be no more than 95% of the contracted
! link speed.
!
! Note that the -X multi-core models do not support traffic shaping in any form.
!
! WARNING: Outbound Traffic Shaping is required to implement QoS and must be
! applied prior to handing traffic off to the service provider.  Failure to
! provide traffic shaping will result in intermittent voice quality issues.
!
policy-map PM-OB-Shape-2M
 class class-default
  shape average 19000000
  service-policy PM-OB-RCPriority
  exit
 exit
!
! Apply policy maps to all interfaces as appropriate
!
service-policy PM-IB-RCPriority interface inside
service-policy PM-OB-Shape-2M interface outside
```

SIP ALG Service

SIP Application Layer Gateway should be disabled completely under all conditions. ALG implementations adjust the SIP headers such that all phones have the same ip address in the VIA header. The Session Border Controllers do not allow for multiple instances of the same SIP UserID (DL number) to be associated with a single IP address. This presents a problem since hard phones, PC soft-phones, and mobile phone instances exist on the same network and register using the same SIP UserID.

```
!================================================================================
! The following code can be used to disable the SIP ALG completely.
!
policy-map global_policy
 class inspection_default
  no inspect sip
  exit
 exit
```

Cisco Wireless Controllers

The default settings of Cisco Wireless Controllers (WLCs) do not support voice well. All traffic by default is treated as Best Effort. There are a variety of potential wireless clients that may need to use the wireless system to carry voice traffic – wireless enabled hard phones, wireless PCs running a softphone client, and mobile/cell phones running a mobile phone application. Regardless of the endpoint type, you must ensure the device generating traffic applies proper DSCP markings as follows:

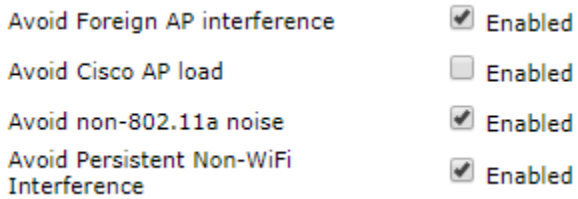
Traffic Type	DSCP Mark
Real-Time Voice Traffic	EF (46)
Real-Time Video Traffic	AF41 (34)
Signaling/Control Traffic	AF31 (26)

RingCentral, by default, does not apply DSCP markings to traffic generated by hard phones, softphone clients, or mobile phone applications. You must request your Account Representative activate the Soft/Mobile Client DSCP markings for your account. You must also request to have Custom Code applied to all your Polycom hard phones so that QoS is properly configured. Other phones will require you to manually configure QoS.

Microsoft Windows (all versions) removes all DSCP markings from applications' IP traffic. The steps in Appendix A must be applied to all Microsoft Windows machines that will generate wireless voice/video traffic.

Once you have ensured that the traffic is marked properly, log into the Wireless Controller and do the following. **Please note that your wireless networks WILL BE DOWN while this is being done.**

1. Select **Wireless -> 802.11a/n/ac -> Network**.
    a. Uncheck the **802.11a Network Status** enable box.
    WARNING – this will turn off your 5GHz network.
    b. Click the **Apply** button on the upper right corner of the web page.
2. Select **Wireless -> 802.11b/g/n -> Network**.
    a. Uncheck the **802.11b/g Network Status** enable box.
    WARNING – this will turn off your 2.4GHz network.
    b. Click the **Apply** button on the upper right corner of the web page.
3. Select **Wireless -> 802.11a/n/ac -> RRM -> DCA**.
    a. Ensure the boxes are checked as shown below:

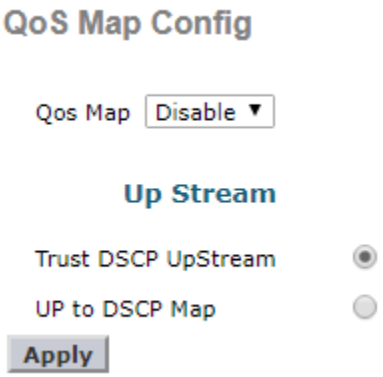


The unchecked box, **Avoid Cisco AP load**, will attempt to keep one AP from getting overloaded, but it depends on the wireless endpoint honoring a message type 17. Cisco

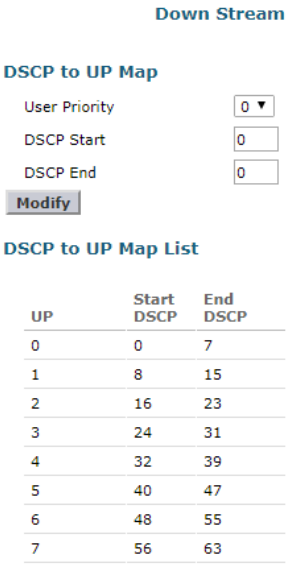
and Apple devices do honor this message type, but other devices may not and will suffer from poor roaming performance.

b. Click the **Apply** button on the upper right corner of the web page.

4. Select **Wireless -> 802.11b/g/n -> RRM -> DCA**.
   a. Ensure the boxes are checked as shown in step 3a.
   b. Click the **Apply** button on the upper right corner of the web page.
5. Select **Wireless -> QoS -> QoS Map**.
   a. In the **Up Stream** section do the following:
      i. Change **Qos Map** to Disable.
      ii. Select the **Trust DSCP UpStream** radio button.

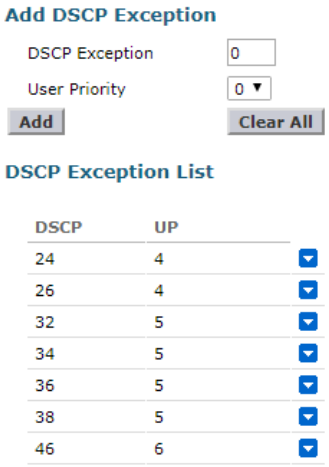


      iii. Click the **Apply** button at the bottom of the **Up Stream** section.
   b. In the **Down Stream** section do the following:
      i. Adjust the **DSCP to UP Map** table so that it reflects the following data:



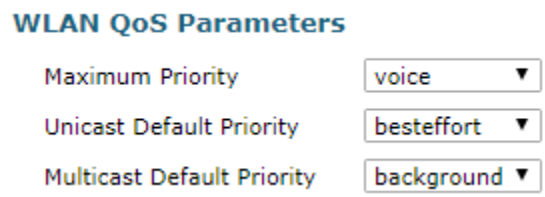
UP	Start DSCP	End DSCP
0	0	7
1	8	15
2	16	23
3	24	31
4	32	39
5	40	47
6	48	55
7	56	63

ii. Clear the **DSCP Exception List** and add the following entries:



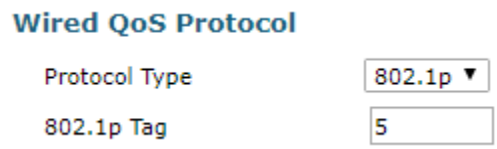
c. Click the **Apply** button on the upper right corner of the web page.

6. Select **Wireless -> QoS -> Profiles**.
   a. Click on **platinum**.
   b. Adjust the **WLAN QoS Parameters** as shown:



Please note: This is CRITICAL. The default settings will mark ALL traffic on the SSID as voice priority, not just the voice packets.

   c. Adjust the **Wired QoS Protocol** as shown:



   d. Click on the **Apply** button on the upper right hand section of the page.

7. Select **WLANs -> WLANs -> WLANs**.
   a. Click on the **WLAN ID** of the SSID you want to enable for Voice.
   b. Under the **QoS** tab
      i. Select *Platinum (voice)* as the **QoS Profile**
      ii. Ensure that **Fastlane** is ***not*** enabled.

iii. Set **WMM Policy** to *Required*.

c. Under the **Security -> Layer2** tab
   i. Set **Fast Transition** to *Enable*
   ii. Ensure that **Over the DS** is ***NOT*** checked.
   iii. Under the **Authentication Key Management** subsection:
      1. If **802.1X** is checked, also check **FT 802.1X** additionally.
      2. If **PSK** is checked, also check **FT PSK** additionally.

d. Under the **Advanced** tab
   i. In the **11k** subsection
      1. Check to enable **Neighbor List**.
      2. Check to enable **Neighbor List Dual Band** only if your endpoints need to roam between 5GHz and 2.4GHz bands.
   ii. In the **11v BSS Transition Support** subsection
      1. Check to enable **BSS Transition**
      2. Check to enable **BSS Max Idle Service**

e. Click the **Apply** button on the upper right corner of the web page.

f. Select the **General** tab
   i. Check the **Status Enabled** box

g. Click the **Apply** button on the upper right corner of the web page.

8. Select **Wireless -> 802.11b/g/n -> Network**.
   a. Check the **802.11b/g Network Status** enable box.
   WARNING – this will reenable your 2.4GHz network.
   b. Click the **Apply** button on the upper right corner of the web page.
9. Select **Wireless -> 802.11a/n/ac -> Network**.
   a. Check the **802.11a Network Status** enable box.
   WARNING – this will reenable your 5GHz network.
   b. Click the **Apply** button on the upper right corner of the web page.

Appendix C – Juniper Equipment

We provide sample configurations for Juniper EX, QFX, and SRX families. Note that interface names, count of interfaces, etc. are model specific and may need to be changed to match the model in use.

Note that this is ONLY a QoS implementation guide. It is NOT a security/firewall configuration guide.

The configuration included supports traffic where packets are already marked with proper DSCP tags as well as packets that are not marked or where markings cannot be trusted.

Universal Note: ***If at all possible, ensure that user endpoint traffic is marked with proper DSCP markings upon ingress to the switch/router/firewall and utilize the policy-maps designated for Trusted ports.***

- Apply **Appendix A** to all Windows based PCs that run any of the soft-clients using either Group Policy or individual configuration.
- Have your Account Manager go into ***'Admin Web'*** and enable proper QoS marking for soft-clients.
- Have your SE apply custom code account-wide to ensure that your hard phones are configured with proper QoS DSCP values.

Juniper QoS processing starts by classifying each packet upon ingress to an interface and assigning it to a particular forwarding class. These forwarding classes are assigned to hardware queue numbers on the egress interface. Schedulers and schedule-maps are used to assign parameters to each forwarding class. Upon egress, packets may be re-marked with a corrected DSCP tag. This will be discussed in more detail later in this document.

Naming Conventions

The configurations used in this document are written using some standardized naming conventions. A prefix is used denoting the primary type of the construct. We have found this to be quite useful in troubleshooting.

```
#=========================================================================
# Note:  The following Prefixes / Acronyms are used in these scripts
#  Prefixes are used in naming each entity to eliminate any possible
#  confusion.
#-------------------------------------------------------------------------
#
# PFX  - Prefix Lists
# FC   - Forwarding Class definitions
# FLTR - Filter definition
# TERM - Term definition within a Filter definition
# TRCP – Traffic Control Profile
# SMAP – Scheduler Map
# SCH  - Scheduler rule
# RWRL – Rewrite Rule
# PLCR - Policer
#
# R2E  - Used to indicate traffic flow moving FROM RingCentral to EndPoint
# E2R  - Used to indicate traffic flow moving TO RingCentral from EndPoint
```

```
#
# RC   - Acronym standing for RingCentral
# RTP  - Acronym standing for Real Time Protocol
#
# L2   - Layer-2 logic (Ethernet)
# L3   - Layer-3 logic (IP)
#
```

DSCP/CoS Tagging Values

The following are the generally accepted DSCP and 802.1p CoS values used by RingCentral to tag network traffic for voice and video purposes. The 802.1p CoS value is displayed between angle brackets such as <3>. DSCP is used to control Layer-3 forwarding while CoS is used to control Layer-2 forwarding.

```
#=====================================================================
# Note:  The following DSCP/CoS values are used in this document and are
# considered to be the default values for their purpose along with the
# mapping to the appropriate Juniper Forwarding Class (FC).
#
# DSCP      CoS
# ========= ===
# EF   (46) <5> - FC-Voice       Voice Real-Time Traffic
# AF41 (34) <4> - FC-Video       Video Real-Time Traffic
# AF31 (26) <3> - FC-Signal      Signaling and Control (All except Cisco)
# CS3  (24) <3> - FC-Signal      Signaling and Control (Cisco default)
# AF21 (18) <2> - FC-Important   All other RC traffic
# BE    (0) <0> - FC-BestEffort  Best Effort
#
```

Syntax

Please note that the basic setup configuration is not impacted by the ELS (New) / Non-ELS (Old) software syntax differences. It is identical for both. Changes ARE found in the actual implementation statements. The only syntax differences for the basic configuration lie in JunOS differences between EX/QFX models vs SRX models.

GREEN highlighted statements should be used only on EX/QFX devices while YELLOW highlighted statements should be used only on SRX devices. Statements that are not highlighted should be used for both models.

Preliminary

If you are doing this on a new system with no installed configuration you may be continually nagged about Auto Image Upgrade. Eliminate this annoyance AND set the root password with the following configuration steps:

```
# In configuration mode!!!!
#
delete chassis auto-image-upgrade
#
# You must set the root password to commit this change.
#
set system root-authentication plain-text-password
P@ssw0rd!
P@ssw0rd!
#
commit
#
```

Basic setup elements

These elements are common to all device models.

RingCentral Network Matching

A prefix list is used to identify all nine (9) the RingCentral public IPv4 blocks. All RingCentral real-time / media services are hosted within these address blocks. ***It is critical to note that the Public IP network address blocks are not regionally divided and that individual subnets of these blocks may, in fact, move between regions or datacenters frequently and without notice due to dynamically changing load conditions.*** Do not make any assumptions about which blocks to allow, you must assume they are all needed.

```
###############################################################################
##                                Network Blocks                             ##
###############################################################################
#
# Identify the RingCentral public network blocks.  All media will go to/from addresses
# within these blocks.
#
edit policy-options prefix-list PFX-RC-Networks
set 66.81.240.0/20
set 80.81.128.0/20
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 / Queues

We must define a set of ***forwarding classes*** and assign them to specific ***queues***. Please note that there are syntax differences between the EX/QFX series and the SRX series. Classifiers examine ingress traffic and assign each packet to one of these forwarding classes. There are usually 8 queues (0-7).

```
###############################################################################
##                              Forwarding Classes                           ##
###############################################################################
#
# Define JunOS forwarding classes and assign them to appropriate queue numbers.
#
# EX and QFX Series
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
#
# SRX Series
edit class-of-service forwarding-classes
set queue 7 FC-Voice priority high
set queue 6 FC-Video priority high
set queue 4 FC-Signal priority low
set queue 2 FC-Important priority low
set queue 0 FC-BestEffort priority low
top
#
```

Behavior Aggregate Classifiers

We define ***Behavior Aggregate classifiers*** to perform basic classification of layer-2 and layer-3 traffic. Note that the layer-2 classifier is not currently used. There is a more complex multi-field filter classifier used to classify untrusted traffic. It is discussed later.

```
###############################################################################
##                          Behavior Aggregate Definitions                   ##
###############################################################################
#
# Layer-3
#
```

```
edit class-of-service classifiers dscp RC-BA-Classifier
set forwarding-class FC-Voice loss-priority low code-points ef
set forwarding-class FC-Video loss-priority low code-points af41
set forwarding-class FC-Signal loss-priority low code-points af31
set forwarding-class FC-Important loss-priority low code-points af21
set forwarding-class FC-BestEffort loss-priority low code-points be
top
#
# Layer-2
#
edit class-of-service classifiers ieee-802.1 RC-BA-L2Classifier
set forwarding-class FC-Voice loss-priority low code-points 101
set forwarding-class FC-Video loss-priority low code-points 100
set forwarding-class FC-Signal loss-priority low code-points 011
set forwarding-class FC-Important loss-priority low code-points 010
top
#
```

Rewrite Rules

We must define a set of ***rewrite rules*** for ***forwarding classes***. These are applied to egress interfaces where they force a rewrite of the DSCP (layer-3) and/or 802.1p CoS (layer-2) values on outbound traffic. Note that the Layer-2 rewrite is version dependent. JunOS versions prior to Release 20.1 R1-S3 may not support both rewrites simultaneously and silently ignore the layer-2 rewrite. Juniper support was unable to identify the actual release number where support was implemented. Packet capture and examination may be required to determine whether your version supports this functionality properly.

```
###############################################################################
##                                Rewrite Rules                              ##
###############################################################################
#
# Establish rewrite rules for all forwarding-class / loss-priority combinations.
#
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-Video loss-priority low code-point af41
set forwarding-class FC-Signal loss-priority low code-point af31
set forwarding-class FC-Important loss-priority low code-point af21
set forwarding-class FC-BestEffort loss-priority low code-point be
top
#
edit class-of-service rewrite-rules ieee-802.1 RWRL-RC-L2ReMark
set forwarding-class FC-Voice loss-priority low code-point 101
set forwarding-class FC-Video loss-priority low code-point 100
set forwarding-class FC-Signal loss-priority low code-point 011
set forwarding-class FC-Important loss-priority low code-point 010
set forwarding-class FC-BestEffort loss-priority low code-point 000
top
#
```

Schedulers and Scheduling Maps

We must define ***schedulers*** and ***scheduler maps*** to control traffic output from the ***forwarding classes***. These are used to guarantee a minimum level of bandwidth and to ensure higher priority traffic is transmitted ahead of lower priority traffic. Note that the SRX devices have multiple hardware levels of priority while EX/QFX devices have only two levels of priority.

```
###############################################################################
##                                Schedulers                                 ##
###############################################################################
#
# Create Schedulers for each forwarding-class.
#
# This is where you set up transmission queues and adjust the amount of guaranteed bandwidth
# for each queue.  Used in concert with scheduler-maps which assigns forwarding classes to
# each transmission queue.  These values should be adjusted to meet customer requirements.
#
# NOTE: These parameters depend upon accurate determination of the output bandwidth.
# The default value will be the physical speed of the interface if not overridden by application
# of a shaping-rate to the interface.
#
# Only the network device directly connected to a WAN circuit should attempt to 'shape' the
# output traffic stream going to an ISP.
#
# Traffic marked as DSCP EF or CoS 5 (Real-Time Voice)
set class-of-service schedulers SCH-EF transmit-rate percent 20
```

```
set class-of-service schedulers SCH-EF buffer-size percent 20
set class-of-service schedulers SCH-EF priority strict-high
#
# Traffic marked as DSCP AF41 or CoS 4 (Real-Time Video)
set class-of-service schedulers SCH-AF41 transmit-rate percent 40
set class-of-service schedulers SCH-AF41 buffer-size percent 40
set class-of-service schedulers SCH-AF41 priority low
set class-of-service schedulers SCH-AF41 priority high
#
# Traffic marked as DSCP AF31 or CoS 3 (Signaling)
set class-of-service schedulers SCH-AF31 transmit-rate percent 10
set class-of-service schedulers SCH-AF31 buffer-size percent 10
set class-of-service schedulers SCH-AF31 priority low
set class-of-service schedulers SCH-AF31 priority medium-high
#
# Traffic marked as DSCP AF21 or CoS 2 (Other RingCentral Traffic)
set class-of-service schedulers SCH-AF21 transmit-rate percent 10
set class-of-service schedulers SCH-AF21 buffer-size percent 10
set class-of-service schedulers SCH-AF21 priority low
#
# All other traffic (Best Effort)
set class-of-service schedulers SCH-BE transmit-rate remainder
set class-of-service schedulers SCH-BE buffer-size remainder
set class-of-service schedulers SCH-BE priority low
#
################################################################################
##                        Forwarding Class to Scheduler Assignments           ##
################################################################################
#
# Assign each forwarding-class to a scheduler.  Special cases may require multiple
# scheduler-maps that are applied to different classes of interfaces.
#
# Scheduler-map for interior (line-rate) interfaces
#
edit class-of-service scheduler-maps SMAP-OB-User
set forwarding-class FC-Voice scheduler SCH-EF
set forwarding-class FC-Video scheduler SCH-AF41
set forwarding-class FC-Signal scheduler SCH-AF31
set forwarding-class FC-Important scheduler SCH-AF21
set forwarding-class FC-BestEffort scheduler SCH-BE
top
#
################################################################################
##                            Clean UP for missing sessions!!!                ##
################################################################################
#
# Generate RSTs for invalid sessions to speed up broken connection detection.
#
#
# Clear out sessions that have experienced an RST
#
set security flow tcp-session rst-invalidate-session
#
```

Traffic Policers

We define ***Policers*** to restrict certain traffic to specific rates on interface ingress. This can be used to prevent run-away machines or deliberate denial of service attacks using high priority markings. Policers must be applied by using a ***MultiField Classifier*** input filter.

```
################################################################################
##                                    Policers                                ##
################################################################################
#
# Create policers to prevent runaway devices from taking over the network. Note that
# policers should ONLY be used on a user port that will only have a single voice
# endpoint.  They should NEVER be applied to a WiFi or trunk port.
#
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
#
```

MultiField Classifiers (Filters)

We define ***MultiField (MF) classifiers*** to identify and assign inbound traffic to specific ***forwarding classes***. These are complex classifiers that can identify RingCentral traffic that arrives with no QoS

markings. Policing policies may be included if desired. If both a ***Behavior Aggregate Classifier*** and a MultiField Classifier are applied to a port, the MultiField Classifier takes precedence.

Always be aware that MF Classifiers occupy multiple physical TCAM slots for each port to which they are applied. TCAM slots are a limited hardware resource on a switching platform and may become exhausted. This is particularly true of older and lower model series equipment.

MF classifiers in this document are defined as follows:

Name	Layer	Policing	Function
FLTR-L2-E2R-User	2	Yes	Identify and classify traffic which is unmarked or whose markings cannot be trusted. When in doubt use these!!!
FLTR-L3-E2R-User	3	Yes	
FLTR-L2-E2R-UserNP	2	No	
FLTR-L3-E2R-UserNP	3	No	
FLTR-L2-E2R-Trust	2	Yes	Classify traffic which is marked prior to delivery. Use the L2 NP version for ethernet trunks or, preferably, just use the Behavior Aggregate Classifier.
FLTR-L3-E2R-Trust	3	Yes	
FLTR-L2-E2R-TrustNP	2	No	
FLTR-L3-E2R-TrustNP	3	No	
FLTR-L2-R2E-ClassifyInbound	2	No	Apply markings to return traffic.
FLTR-L3-R2E-ClassifyInbound	3	No	

Layer-2 MultiField (MF) Classifiers

The following filters act as ***MultiField (MF) Classifiers*** for inbound traffic on layer-2 (family ethernet-switching) interfaces. Please note that the SRX models do not allow matching layer-3 fields on a layer-2 interface whilst the EX and QFX models do allow for it. While the configuration can be entered without any indication of errors on an SRX, the commit stage will always fail.

```
###############################################################################################
##                                                                                           ##
##                        Layer-2 MF (MultiField) Filters                                    ##
##                                                                                           ##
##    DO NOT DEFINE THESE FILTERS ON AN SRX.  THE COMMIT STAGE WILL ALWAYS FAIL              ##
##                                                                                           ##
##                                                                                           ##
###############################################################################################
#
# Create FILTERS to classify traffic and assign it to the correct Forwarding Class.
# The DSCP marks will be rewritten by the re-write rules when the traffic egresses
# a port.  These filter versions are for layer-2 interfaces (family ethernet-switching)
# only.  Do not define these on an SRX, they will fail on commit!!!
#
# It is far more efficient to have traffic already classified with proper DSCP markings
# and CoS tags upon ingress to the switch port.
#
#------------------------------------------------------------------------------
# FLTR-L2-E2R-User
#
# Create the filter to apply to all Layer-2 *USER* (PC/Phone) ports where classification
# is or may be needed.  If the traffic is already classified and properly DSCP marked, you
# should use FLTR-L2-E2R-Trust instead of this filter.  That version will trust inbound
# DSCP markings if they are present.
#
# Clean up any prior definition.
delete firewall family ethernet-switching filter FLTR-L2-E2R-User
edit firewall family ethernet-switching filter FLTR-L2-E2R-User
#---
set term TERM-Phone-RT from protocol udp destination-port 20000-64999 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-RT2 from protocol udp destination-port 8803 destination-prefix-list PFX-RC-Networks
set term TERM-Phone-RT2 then accept forwarding-class FC-Voice loss-priority low policer PLCR-UserVoice
#---
set term TERM-Video-RT from protocol udp destination-port 8801-8802 destination-prefix-list PFX-RC-Networks
set term TERM-Video-RT then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT2 from protocol tcp destination-port 8801-8802 destination-prefix-list PFX-RC-Networks
```

```
set term TERM-Video-RT2 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT4 from protocol udp destination-port 10000-19999 destination-prefix-list PFX-RC-Networks
set term TERM-Video-RT4 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Phone-Signal-udp from protocol udp destination-port 5090-5099 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-tcp from protocol tcp destination-port 5090-5099 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-tcp3 from protocol tcp destination-port 8083-8090 destination-prefix-list PFX-RC-Networks
set term TERM-Phone-Signal-tcp3 then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-Video-Signal-tcp from protocol tcp destination-port 5060-5061 destination-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-tcp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-Video-Signal-udp from protocol udp destination-port 5060 destination-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-udp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-RC-Other from destination-prefix-list PFX-RC-Networks
set term TERM-RC-Other then accept forwarding-class FC-Important loss-priority low
#---
set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
#---
top
#
#-------------------------------------------------------------------------------
# FLTR-L2-E2R-UserNP
#
# This is identical to FLTR-L2-E2R-User with policing removed.
#
# Create the filter to apply to all Layer-2 *USER* (PC/Phone) ports where classification
# is or may be needed.  If the traffic is already classified and properly DSCP marked, you
# should use FLTR-L2-E2R-TrustNP instead of this filter.  That version will trust inbound
# DSCP markings if they are present.
#
# Clean up any prior definition.
delete firewall family ethernet-switching filter FLTR-L2-E2R-UserNP
edit firewall family ethernet-switching filter FLTR-L2-E2R-UserNP
#---
set term TERM-Phone-RT from protocol udp destination-port 20000-64999 destination-prefix-list PFX-RC-Networks
set term TERM-Phone-RT then accept forwarding-class FC-Voice loss-priority low
#---
set term TERM-Phone-RT2 from protocol udp destination-port 8803 destination-prefix-list PFX-RC-Networks
set term TERM-Phone-RT2 then accept forwarding-class FC-Voice loss-priority low policer
#---
set term TERM-Video-RT from protocol udp destination-port 8801-8802 destination-prefix-list PFX-RC-Networks
set term TERM-Video-RT then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT2 from protocol tcp destination-port 8801-8802 destination-prefix-list PFX-RC-Networks
set term TERM-Video-RT2 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT4 from protocol udp destination-port 10000-19999 destination-prefix-list PFX-RC-Networks
set term TERM-Video-RT4 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Phone-Signal-udp from protocol udp destination-port 5090-5099 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-tcp from protocol tcp destination-port 5090-5099 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-tcp3 from protocol tcp destination-port 8083-8090 destination-prefix-list PFX-RC-Networks
set term TERM-Phone-Signal-tcp3 then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-Video-Signal-tcp from protocol tcp destination-port 5060-5061 destination-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-tcp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-Video-Signal-udp from protocol udp destination-port 5060 destination-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-udp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-RC-Other from destination-prefix-list PFX-RC-Networks
set term TERM-RC-Other then accept forwarding-class FC-Important loss-priority low
#---
set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
#---
top
#
#-------------------------------------------------------------------------------
# FLTR-L2-E2R-Trust
#
# Create the filter to apply to all *USER* (PC/Phone) ports where MF classification is
# not needed.  Use only if the traffic is already classified and properly DSCP marked.
# This must be used in cases where you trust the DSCP settings, but still need to police
# the real-time traffic level.
#
# Clean up any prior definition.
delete firewall family ethernet-switching filter FLTR-L2-E2R-Trust
edit firewall family ethernet-switching filter FLTR-L2-E2R-Trust
```

```
#---
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-AF41 from dscp [ af41 cs4 ]
set term TERM-AF41 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT2 from protocol udp destination-port 8850-8869
set term TERM-Video-RT2 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-AF31 from dscp [ af31 cs3 ]
set term TERM-AF31 then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-AF21 from dscp af21
set term TERM-AF21 then accept forwarding-class FC-Important loss-priority low
#---
set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
#---
top
#
#-------------------------------------------------------------------------------
# FLTR-L2-E2R-TrustNP
#
# This is identical to FLTR-L2-E2R-Trust with policing removed.
#
# Create the filter to apply to all *USER* (PC/Phone) ports where MF classification and
# policing are not needed.  Use only if the traffic is already classified and properly
# DSCP marked.  It is preferable to use the BA classifier and NOT use this filter.
#
# This filter or the BA classifier should be used on all Ethernet Trunk interfaces.
# Note that the BA classifier is more efficient.
#
# Clean up any prior definition.
delete firewall family ethernet-switching filter FLTR-L2-E2R-TrustNP
edit firewall family ethernet-switching filter FLTR-L2-E2R-TrustNP
#---
set term TERM-EF from dscp [ ef cs5 ]
set term TERM-EF then accept forwarding-class FC-Voice loss-priority low
#---
set term TERM-AF41 from dscp [ af41 cs4 ]
set term TERM-AF41 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT2 from protocol udp destination-port 8850-8869
set term TERM-Video-RT2 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-AF31 from dscp [ af31 cs3 ]
set term TERM-AF31 then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-AF21 from dscp af21
set term TERM-AF21 then accept forwarding-class FC-Important loss-priority low
#---
set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
#---
top
#
#-------------------------------------------------------------------------------
# FLTR-L2-R2E-ClassifyInbound
#
# This filter is used on a WAN facing port to look at traffic coming FROM RingCentral
# TO the Endpoint and classify it.  This is only needed if your firewall does not
# restore the original DSCP markings on return traffic.
#
# Clean up any prior definition.
delete firewall family ethernet-switching filter FLTR-L2-R2E-ClassifyInbound
edit firewall family ethernet-switching filter FLTR-L2-R2E-ClassifyInbound
#---
set term TERM-Phone-RT from protocol udp source-port 20000-64999 source-prefix-list PFX-RC-Networks
set term TERM-Phone-RT then accept forwarding-class FC-Voice loss-priority low
#---
set term TERM-Phone-RT2 from protocol udp source-port 8803 source-prefix-list PFX-RC-Networks
set term TERM-Phone-RT2 then accept forwarding-class FC-Voice loss-priority low
#---
set term TERM-Video-RT from protocol udp source-port 8801-8802 source-prefix-list PFX-RC-Networks
set term TERM-Video-RT then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT from protocol tcp source-port 8801-8802 source-prefix-list PFX-RC-Networks
set term TERM-Video-RT then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT3 from protocol udp source-port 10000-19999 source-prefix-list PFX-RC-Networks
set term TERM-Video-RT3 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Phone-Signal-udp from protocol udp source-port 5090-5099 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-tcp from protocol tcp source-port 5090-5099 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-tcp3 from protocol tcp source-port 8083-8090 source-prefix-list PFX-RC-Networks
set term TERM-Phone-Signal-tcp3 then accept forwarding-class FC-Signal loss-priority low
```

```
#---
set term TERM-Video-Signal-tcp from protocol tcp source-port 5060-5061 source-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-tcp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-Video-Signal-udp from protocol udp source-port 5060 source-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-udp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
#---
top
#
```

Layer-3 MultiField (MF) Classifiers

The following filters act as ***MultiField (MF) Classifiers*** for inbound traffic on layer-3 (family inet) interfaces. Do not define these filters if you do not have any family inet interfaces on the device or if all markings are trusted.

```
##############################################################################################
##                                                                                          ##
##                        Layer-3 MF (MultiField) Filters                                   ##
##                                                                                          ##
## These filters are needed IF and ONLY IF you have any interfaces that are in              ##
## Layer-3 mode (family inet).  Do not create them if they are not needed!!!                ##
##                                                                                          ##
##############################################################################################
#
# Create FILTERS to classify traffic and assign it to the correct Forwarding Class.
# The DSCP marks will be rewritten by the re-write rules when the traffic egresses
# a port.  These filter versions are for layer-3 interfaces (family inet) only.
#
# It is far more efficient to have traffic already classified with proper DSCP markings
# and CoS tags upon ingress to the switch port.
#
#---------------------------------------------------------------------------------------
# FLTR-L3-E2R-User
#
# Create the filter to apply to all Layer-3 *USER* (PC/Phone) ports where classification
# is or may be needed.  If the traffic is already classified and properly DSCP marked, you
# should use FLTR-L3-E2R-Trust instead of this filter.  That version will trust inbound
# DSCP markings if they are present.
#
# Clean up any prior definition.
delete firewall family inet filter FLTR-L3-E2R-User
edit firewall family inet filter FLTR-L3-E2R-User
#---
set term TERM-Phone-RT from protocol udp destination-port 20000-64999 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-RT2 from protocol udp destination-port 8803 destination-prefix-list PFX-RC-Networks
set term TERM-Phone-RT2 then accept forwarding-class FC-Voice loss-priority low policer PLCR-UserVoice
#---
set term TERM-Video-RT from protocol udp destination-port 8801-8802 destination-prefix-list PFX-RC-Networks
set term TERM-Video-RT then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT2 from protocol tcp destination-port 8801-8802 destination-prefix-list PFX-RC-Networks
set term TERM-Video-RT2 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT4 from protocol udp destination-port 10000-19999 destination-prefix-list PFX-RC-Networks
set term TERM-Video-RT4 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Phone-Signal-udp from protocol udp destination-port 5090-5099 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-tcp from protocol tcp destination-port 5090-5099 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-tcp3 from protocol tcp destination-port 8083-8090 destination-prefix-list PFX-RC-Networks
set term TERM-Phone-Signal-tcp3 then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-Video-Signal-tcp from protocol tcp destination-port 5060-5061 destination-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-tcp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-Video-Signal-udp from protocol udp destination-port 5060 destination-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-udp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-RC-Other from destination-prefix-list PFX-RC-Networks
set term TERM-RC-Other then accept forwarding-class FC-Important loss-priority low
#---
set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
#---
top
#
#---------------------------------------------------------------------------------------
```

```
# FLTR-L3-E2R-UserNP
#
# This is identical to FLTR-L3-E2R-User with policing removed.
#
# Create the filter to apply to all Layer-3 *USER* (PC/Phone) ports where classification
# is or may be needed.  If the traffic is already classified and properly DSCP marked, you
# should use FLTR-L3-E2R-TrustNP instead of this filter.  That version will trust inbound
# DSCP markings if they are present.
#
# Clean up any prior definition.
delete firewall family inet filter FLTR-L3-E2R-UserNP
edit firewall family inet filter FLTR-L3-E2R-UserNP
#---
set term TERM-Phone-RT from protocol udp destination-port 20000-64999 destination-prefix-list PFX-RC-Networks
set term TERM-Phone-RT then accept forwarding-class FC-Voice loss-priority low
#---
set term TERM-Phone-RT2 from protocol udp destination-port 8803 destination-prefix-list PFX-RC-Networks
set term TERM-Phone-RT2 then accept forwarding-class FC-Voice loss-priority low
#---
set term TERM-Video-RT from protocol udp destination-port 8801-8802 destination-prefix-list PFX-RC-Networks
set term TERM-Video-RT then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT2 from protocol tcp destination-port 8801-8802 destination-prefix-list PFX-RC-Networks
set term TERM-Video-RT2 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT4 from protocol udp destination-port 10000-19999 destination-prefix-list PFX-RC-Networks
set term TERM-Video-RT4 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Phone-Signal-udp from protocol udp destination-port 5090-5099 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-tcp from protocol tcp destination-port 5090-5099 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-tcp3 from protocol tcp destination-port 8083-8090 destination-prefix-list PFX-RC-Networks
set term TERM-Phone-Signal-tcp3 then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-Video-Signal-tcp from protocol tcp destination-port 5060-5061 destination-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-tcp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-Video-Signal-udp from protocol udp destination-port 5060-5061 destination-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-udp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-RC-Other from destination-prefix-list PFX-RC-Networks
set term TERM-RC-Other then accept forwarding-class FC-Important loss-priority low
#---
set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
#---
top
#
#-------------------------------------------------------------------------------
# FLTR-L3-E2R-Trust
#
# Create the filter to apply to all *USER* (PC/Phone) ports where MF classification is
# not needed.  Use only if the traffic is already classified and properly DSCP marked.
#
# Clean up any prior definition.
delete firewall family inet filter FLTR-L3-E2R-Trust
edit firewall family inet filter FLTR-L3-E2R-Trust
#---
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-AF41 from dscp [ af41 cs4 ]
set term TERM-AF41 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT2 from protocol udp destination-port 8850-8869
set term TERM-Video-RT2 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-AF31 from dscp [ af31 cs3 ]
set term TERM-AF31 then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-AF21 from dscp af21
set term TERM-AF21 then accept forwarding-class FC-Important loss-priority low
#---
set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
#---
top
#
#-------------------------------------------------------------------------------
# FLTR-L3-E2R-TrustNP
#
# This is identical to FLTR-L3-E2R-Trust with policing removed.
#
# Create the filter to apply to all *USER* (PC/Phone) ports where MF classification is
# not needed.  Use only if the traffic is already classified and properly DSCP marked.
#
# Clean up any prior definition.
delete firewall family inet filter FLTR-L3-E2R-TrustNP
```

```
edit firewall family inet filter FLTR-L3-E2R-TrustNP
#---
set term TERM-EF from dscp [ ef cs5 ]
set term TERM-EF then accept forwarding-class FC-Voice loss-priority low
#---
set term TERM-AF41 from dscp [ af41 cs4 ]
set term TERM-AF41 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT2 from protocol udp destination-port 8850-8869
set term TERM-Video-RT2 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-AF31 from dscp [ af31 cs3 ]
set term TERM-AF31 then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-AF21 from dscp af21
set term TERM-AF21 then accept forwarding-class FC-Important loss-priority low
#---
set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
#---
top
#
#-------------------------------------------------------------------------------
# FLTR-L3-R2E-ClassifyInbound
#
# This filter is used on a WAN facing port to look at traffic coming FROM RingCentral
# TO the Endpoint and classify it.  This is only needed if your firewall does not
# restore the original DSCP markings on return traffic.
#
# Clean up any prior definition.
delete firewall family inet filter FLTR-L3-R2E-ClassifyInbound
edit firewall family inet filter FLTR-L3-R2E-ClassifyInbound
#---
set term TERM-Phone-RT from protocol udp source-port 20000-64999 source-prefix-list PFX-RC-Networks
set term TERM-Phone-RT then accept forwarding-class FC-Voice loss-priority low
#---
set term TERM-Phone-RT2 from protocol udp source-port 8803 source-prefix-list PFX-RC-Networks
set term TERM-Phone-RT2 then accept forwarding-class FC-Voice loss-priority low
#---
set term TERM-Video-RT from protocol udp source-port 8801-8802 source-prefix-list PFX-RC-Networks
set term TERM-Video-RT then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT from protocol tcp source-port 8801-8802 source-prefix-list PFX-RC-Networks
set term TERM-Video-RT then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Video-RT3 from protocol udp source-port 10000-19999 source-prefix-list PFX-RC-Networks
set term TERM-Video-RT3 then accept forwarding-class FC-Video loss-priority low
#---
set term TERM-Phone-Signal-udp from protocol udp source-port 5090-5099 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-tcp from protocol tcp source-port 5090-5099 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-tcp3 from protocol tcp source-port 8083-8090 source-prefix-list PFX-RC-Networks
set term TERM-Phone-Signal-tcp3 then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-Video-Signal-tcp from protocol tcp source-port 5060-5061 source-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-tcp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-Video-Signal-udp from protocol udp source-port 5060-5061 source-prefix-list PFX-RC-Networks
set term TERM-Video-Signal-udp then accept forwarding-class FC-Signal loss-priority low
#---
set term TERM-BE then accept forwarding-class FC-BestEffort loss-priority high
#---
top
#
commit
#
```

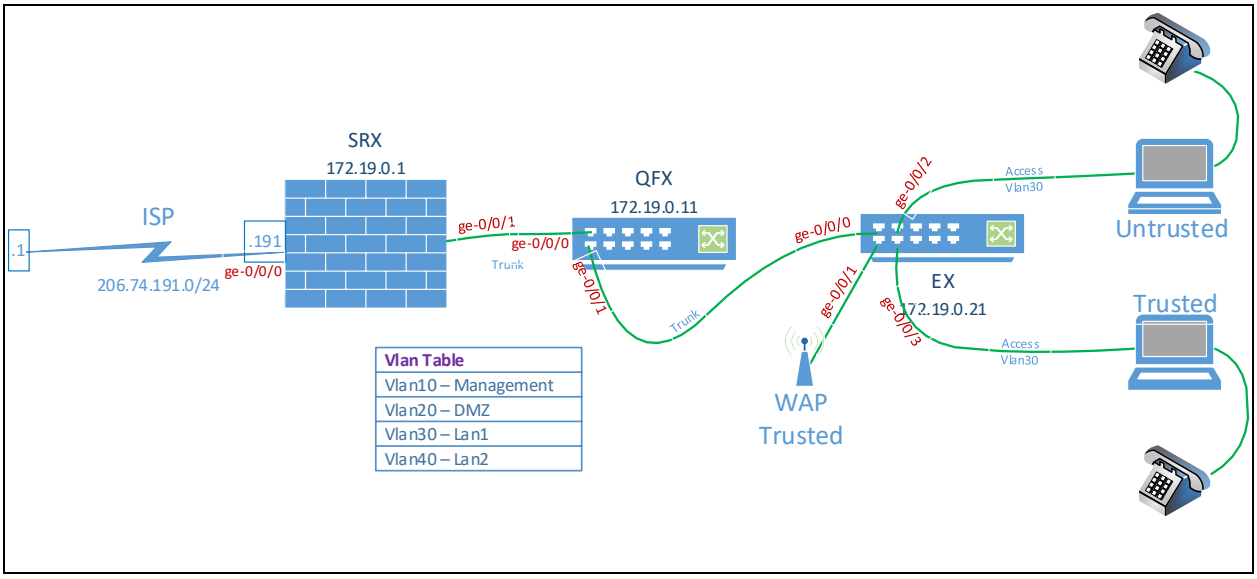
New (ELS) vs Old (Pre-ELS) Syntax Differences

Juniper implemented Uniform Enhanced Layer 2 Software (ELS) for hardware when they transitioned from the Marvell chipset to the Broadcom chipset. It provides a uniform CLI syntax for Layer-2 configuration across multiple product lines (MX, EX, SRX, QFX).

You may easily test to see whether your device requires ELS syntax by going into configuration mode and typing '`set ?`'. If you see '`ethernet-switching-options`' as a valid next choice you do NOT have ELS support on this device. Text and highlighting embedded in the configuration statements will make clear where these differences occur.

Implementation

This diagram details the simplistic test/lab setup used in these examples:



The following are configuration examples based upon the above diagram. It is assumed that the standard definitions given in the previous section have been loaded and committed on each network device. GREEN highlighted statements should be used only on ELS syntax based devices while YELLOW highlighted statements should be used only on older, non-ELS syntax based devices. Statements with no highlighting are common to both syntaxes.

These configurations assume a device that has been factory reset. A minimal level of non-QoS configuration is included; sufficient to configure a minimally working device.

EX and QFX Devices

Please take note that all interfaces are assumed to be operating at full line rate. If an interface must traverse a carrier link that has a CIR less than the line rate you must define a traffic-control-profile and a custom scheduler-map with which it must be associated. That scheduler-map must then be applied specifically to the port in question.

```
###############################################################################################
##                                  Implementation and Usage                                 ##
##   Sample Only – Interface names, ranges, etc will be different depending upon   ##
##   switch line, model, and optional installed interface modules.                 ##
###############################################################################################
#
# NOTE: Vlans and interfaces mentioned below are examples only.
#
###############################################################################################
##                  Sample Vlans and Management Address for examples                 ##
###############################################################################################
#
# Remove vlan 0 management logic and replace with vlan 10 as the management
# network/interface.
#
# → CHANGE MANAGEMENT ADDRESS AS NEEDED FOR YOUR NETWORK ←
#
# vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
# ELS Version
delete vlans default l3-interface irb.0
delete interfaces irb unit 0 family inet
```

```
set vlans Vlan-Mgmt vlan-id 10 l3-interface irb.10
set interfaces irb unit 10 family inet address 172.19.0.11/24
# -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
# Old Non-ELS Version
delete vlans default l3-interface vlan.0
delete interfaces vlan unit 0 family inet
set vlans Vlan-Mgmt vlan-id 10 l3-interface vlan.10
set interfaces vlan unit 10 family inet address 172.19.0.11/24
# ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
#
# Add default route via management vlan.   You will probably want to adjust this to only
# route internal traffic via this interface and have normal production traffic egress
# through a production interface/route or, preferably, move the management network into
# a management only VRF / routing instance.  This has nothing to do with QoS and will not
# be covered in this document.
#
set routing-options static route 0.0.0.0/0 next-hop 172.19.0.1
#
# Create non-management (DATA) vlans
#
set vlans Vlan-Lan1 vlan-id 30
set vlans Vlan-Lan2 vlan-id 40
#
# Adjust the count of AE (trunk/LACP) devices required (ONE TIME TASK).
# This example sets it to 8, creating LACP ports ae0 – ae7
#
set chassis aggregated-devices ethernet device-count 8
#
# Enable SSH logins
#
set system services ssh
set system login user testadmin class super-user
#
# After issuing the next command you will be prompted to enter a password twice.
#
set system login user testadmin authentication plain-text-password
P@ssw0rd!
P@ssw0rd!
#
# Set up ports ge-0/0/[0,1] as trunk ports and ports ge-0/0/[2-3] as access ports on Vlan-Lan1
# Port ge-0/0/2 will be set up as a port where incoming DSCP markings are NOT trusted.
# Port ge-0/0/3 will be set up as a port where incoming DSCP markings ARE trusted.
#
################################################################################
# vvvvvvvvvvvvvvvvvvvvvvvvvvvvvv  QFX ONLY  vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
#
#
# WARNING – The QFX differs from the EX in that the default interfaces are created as
# unit 0 in family inet rather than family ethernet-switching.  To use this
# configuration, which is based upon a standard ethernet switching type aggregation
# switch, the interfaces must be converted by deleting and recreating unit 0.
#
wildcard range delete interfaces ge-0/0/[0-3] unit 0 family inet
wildcard range set interfaces ge-0/0/[0-3] unit 0 family ethernet-switching
#
wildcard range delete interfaces xe-0/0/[0-3] unit 0 family inet
wildcard range set interfaces xe-0/0/[0-3] unit 0 family ethernet-switching
#
# ^^^^^^^^^^^^^^^^^^^^^^^^^^ End of QFX Only ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
################################################################################
#
#
# All interfaces must have re-mark rules, DSCP classifier, and scheduler-map applied
# Do NOT apply the ieee-802.1 classifier – it will cause major issues.
#
set class-of-service interfaces ge-0/0/* scheduler-map SMAP-OB-User
set class-of-service interfaces ge-0/0/* unit 0 classifiers dscp RC-BA-Classifier
set class-of-service interfaces ge-0/0/* unit 0 rewrite-rules dscp RWRL-RC-ReMark
set class-of-service interfaces ge-0/0/* unit 0 rewrite-rules ieee-802.1 RWRL-RC-L2ReMark
#
################################################################################
# vvvvvvvvvvvvvvvvvvvvvvvvvvvvvv  QFX ONLY  vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
set class-of-service interfaces xe-0/0/* scheduler-map SMAP-OB-User
set class-of-service interfaces xe-0/0/* unit 0 classifiers dscp RC-BA-Classifier
set class-of-service interfaces xe-0/0/* unit 0 rewrite-rules dscp RWRL-RC-ReMark
set class-of-service interfaces xe-0/0/* unit 0 rewrite-rules ieee-802.1 RWRL-RC-L2ReMark
# ^^^^^^^^^^^^^^^^^^^^^^^^^^ End of QFX Only ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
################################################################################
#
set class-of-service interfaces ae* scheduler-map SMAP-OB-User
set class-of-service interfaces ae* unit 0 classifiers dscp RC-BA-Classifier
set class-of-service interfaces ae* unit 0 rewrite-rules dscp RWRL-RC-ReMark
set class-of-service interfaces ae* unit 0 rewrite-rules ieee-802.1 RWRL-RC-L2ReMark
#
################################################################################
#
# Set up interfaces
#
#
```

```
# Note that when interfaces are run at line-rate you should use the default scheduler-map
# SMAP-OB-User which is NOT associated with a traffic-control-profile. If an interface
# needs to be bandwidth limited (ie a layer-2 vpls link between locations with a limited
# cir) you will need to associate a separate scheduler-map with a traffic-control-profile
# like the SMAP-OB-User-WAN1 and override the scheduler-map definition on the interface.
#---------------------------------
#
# Interface ge-0/0/0 is a multi-vlan trunk from an upstream WAN device that connects
# to RingCentral but cannot correctly mark DSCP on return traffic.  The layer-2
# MF filter FLTR-L2-R2E-ClassifyInbound is used to classify the traffic, rewrite rules
# update the packets on egress to have the correct DSCP values.
#
set interfaces ge-0/0/0 description UplinkTrunkWanDevice
edit interfaces ge-0/0/0 unit 0 family ethernet-switching
#
# ELS Version
set interface-mode trunk
#
# Old Non-ELS Version
set port-mode trunk
#
set vlan members [ Vlan-Lan1 Vlan-Lan2 Vlan-Mgmt ]
set filter input FLTR-L2-R2E-ClassifyInbound
top
#
#---------------------------------
#
# Interface ge-0/0/1 is a multi-vlan trunk to a wireless access point.  It is set up
# assumeing all traffic in both directions is correctly marked.  It depends on the
# DSCP BA classifier.  This connection MUST NOT police traffic.
#
set interfaces ge-0/0/1 description UplinkTrunkToWAP
edit interfaces ge-0/0/1 unit 0 family ethernet-switching
#
# ELS Version
set interface-mode trunk
#
# Old Non-ELS Version
set port-mode trunk
#
set vlan members [ Vlan-Lan1 Vlan-Lan2 Vlan-Mgmt ]
top
#
#
#   Traffic coming into the interface is NOT trusted, Force remarking of input
#
#---------------------------------
#
# Interface ge-0/0/2 is an access port on Vlan-Lan1.  It assumes the traffic's
# DSCP markings are missing or untrusted.  The layer-2 MF filter FLTR-L2-E2R-User
# is used to classify the traffic, rewrite rules update the packets on egress
# to have the correct DSCP values.  This connection will be policed for a single
# user.
#
set interfaces ge-0/0/2 description UntrustedUser
edit interfaces ge-0/0/2 unit 0 family ethernet-switching
#
# ELS Version
set interface-mode access
#
# Old Non-ELS Version
set port-mode access
#
set vlan members [ Vlan-Lan1 ]
set filter input FLTR-L2-E2R-User
top
#
#---------------------------------
#
# Interface ge-0/0/2 is an access port on Vlan-Lan1.  It assumes the traffic's
# DSCP markings are correct and present on all traffic.  The MF filter FLTR-L2-E2R-Trust
# classifier is used to classify the traffic rather than using the DSCP BA classifier so
# that the traffic will be policed for a single user.
#
set interfaces ge-0/0/3 description TrustedUser
edit interfaces ge-0/0/3 unit 0 family ethernet-switching
#
# ELS Version
set interface-mode access
#
# Old Non-ELS Version
set port-mode access
#
set vlan members [ Vlan-Lan1 ]
set filter input FLTR-L2-E2R-Trust
top
#
```

SRX Devices

```
##############################################################################################
##                                Implementation and Usage                                  ##
##   Sample Only – Interface names, ranges, etc will be different depending upon            ##
##   switch line, model, and optional installed interface modules.                          ##
##############################################################################################
#
# NOTE: Vlans and interfaces mentioned below are examples only.
#
##############################################################################################
##                    Sample Vlans and Management Address for examples                      ##
##############################################################################################
#
# Remove vlan 0 management logic
# ELS Version
delete system services dhcp-local-server group jdhcp-group interface irb.0
delete security zones security-zone trust interfaces irb.0
delete interfaces irb unit 0 family inet address 192.168.2.1/24
delete vlans vlan-trust l3-interface irb.0
#
delete access address-assignment pool junosDHCPPool1
delete access address-assignment pool junosDHCPPool2
#
#
# Add l3-interface for management vlan 10.
#
set vlans Vlan-Mgmt vlan-id 10 l3-interface irb.10
set vlans Vlan-Lan1 vlan-id 30 l3-interface irb.30
set vlans Vlan-Lan2 vlan-id 40 l3-interface irb.40
#
# Assign address to Management Vlan - CHANGE ADDRESS AS NEEDED FOR YOUR NETWORK
#
set interfaces irb unit 10 family inet address 172.19.0.1/24
set interfaces irb unit 30 family inet address 172.19.11.1/24
set interfaces irb unit 40 family inet address 172.19.12.1/24
#
set security zones security-zone trust interfaces irb.10
#
delete system services dhcp-local-server group jdhcp-group
#
edit system services dhcp-local-server
set group group1 interface fxp0.0
set group group1 interface irb.10
set group group1 interface irb.30
set group group1 interface irb.40
top
#
# Old Non-ELS Version
delete system services dhcp propagate-settings ge-0/0/0.0
delete system services dhcp router 192.168.1.1
delete system services dhcp pool 192.168.1.0/24
delete system services web-management http interface vlan.0
delete system services web-management https interface vlan.0
delete security zones security-zone trust interfaces vlan.0
delete security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic system-services dhcp
delete security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic system-services tftp
wildcard range delete interfaces ge-0/0/[1-15] unit 0 family ethernet-switching vlan members vlan-trust
delete vlans vlan-trust l3-interface vlan.0
delete interfaces vlan unit 0 family inet address 192.168.1.1/24
delete vlans vlan-trust vlan-id 3
delete vlans vlan-trust
delete interfaces vlan unit 0
#
#
# Add l3-interface for management vlan 10.
#
set vlans Vlan-Mgmt vlan-id 10 l3-interface vlan.10
set vlans Vlan-Lan1 vlan-id 30 l3-interface vlan.30
set vlans Vlan-Lan2 vlan-id 40 l3-interface vlan.40
#
# Assign address to Management Vlan - CHANGE ADDRESS AS NEEDED FOR YOUR NETWORK
#
set interfaces vlan unit 10 family inet address 172.19.0.1/24
set interfaces vlan unit 30 family inet address 172.19.11.1/24
set interfaces vlan unit 40 family inet address 172.19.12.1/24
#
edit system services dhcp-local-server
set group group1 interface vlan.10
set group group1 interface vlan.30
set group group1 interface vlan.40
top
#
set security zones security-zone trust interfaces vlan.10
set security zones security-zone trust interfaces vlan.30
set security zones security-zone trust interfaces vlan.40
```

```
#
# Enable SSH logins
#
set system services ssh
set system login user testadmin class super-user
#
# Change P@ssw0rd! below to your desired password
set system login user testadmin authentication plain-text-password
P@ssw0rd!
P@ssw0rd!
#
# Set up DHCP Servers for the vlans
#
set access address-assignment pool POOL-Vlan10 family inet network 172.19.0.0/24
set access address-assignment pool POOL-Vlan10 family inet range r1 low 172.19.0.25
set access address-assignment pool POOL-Vlan10 family inet range r1 high 172.19.0.249
set access address-assignment pool POOL-Vlan10 family inet dhcp-attributes router 172.19.0.1
set access address-assignment pool POOL-Vlan10 family inet dhcp-attributes domain-name example.com
set access address-assignment pool POOL-Vlan10 family inet dhcp-attributes name-server 8.8.8.8
set access address-assignment pool POOL-Vlan10 family inet dhcp-attributes name-server 8.8.4.4
#
set access address-assignment pool POOL-Vlan30 family inet network 172.19.11.0/24
set access address-assignment pool POOL-Vlan30 family inet range r1 low 172.19.11.25
set access address-assignment pool POOL-Vlan30 family inet range r1 high 172.19.11.249
set access address-assignment pool POOL-Vlan30 family inet dhcp-attributes router 172.19.11.1
set access address-assignment pool POOL-Vlan30 family inet dhcp-attributes domain-name example.com
set access address-assignment pool POOL-Vlan30 family inet dhcp-attributes name-server 8.8.8.8
set access address-assignment pool POOL-Vlan30 family inet dhcp-attributes name-server 8.8.4.4
#
set access address-assignment pool POOL-Vlan40 family inet network 172.19.12.0/24
set access address-assignment pool POOL-Vlan40 family inet range r1 low 172.19.12.25
set access address-assignment pool POOL-Vlan40 family inet range r1 high 172.19.12.249
set access address-assignment pool POOL-Vlan40 family inet dhcp-attributes router 172.19.12.1
set access address-assignment pool POOL-Vlan40 family inet dhcp-attributes domain-name example.com
set access address-assignment pool POOL-Vlan40 family inet dhcp-attributes name-server 8.8.8.8
set access address-assignment pool POOL-Vlan40 family inet dhcp-attributes name-server 8.8.4.4
#
# Adjust the count of AE (trunk/LACP) devices required (ONE TIME TASK).
# This example sets it to 8, creating LACP ports ae0 – ae7
#
set chassis aggregated-devices ethernet device-count 8
#
# All interfaces must have re-mark rule, classifiers, and scheduler-map applied
#
set class-of-service interfaces ge-0/0/* scheduler-map SMAP-OB-User
set class-of-service interfaces ge-0/0/* unit 0 classifiers dscp RC-BA-Classifier
set class-of-service interfaces ge-0/0/* unit 0 rewrite-rules dscp RWRL-RC-ReMark
set class-of-service interfaces ge-0/0/* unit 0 rewrite-rules ieee-802.1 RWRL-RC-L2ReMark
#
set class-of-service interfaces ae* scheduler-map SMAP-OB-User
set class-of-service interfaces ae* unit 0 classifiers dscp RC-BA-Classifier
set class-of-service interfaces ae* unit 0 rewrite-rules dscp RWRL-RC-ReMark
set class-of-service interfaces ae* unit 0 rewrite-rules ieee-802.1 RWRL-RC-L2ReMark
#
# ELS Version
set class-of-service interfaces irb unit * rewrite-rules dscp RWRL-RC-ReMark
set class-of-service interfaces irb unit * rewrite-rules ieee-802.1 RWRL-RC-L2ReMark
#
# Old Non-ELS Version
set class-of-service interfaces vlan unit * rewrite-rules dscp RWRL-RC-ReMark
set class-of-service interfaces vlan unit * rewrite-rules ieee-802.1 RWRL-RC-L2ReMark
#
##############################################################################
#
# Note that when interfaces are run at line-rate you should use the default scheduler-map
# SMAP-OB-User which is NOT associated with a traffic-control-profile. If an interface
# needs to be bandwidth limited (ie a layer-2 vpls link between locations with a limited
# cir or an ISP link with limited uplink speed) you will need to associate a separate
# scheduler-map with a traffic-control-profile like the SMAP-OB-User-WAN1 and override
# the scheduler-map definition on the interface.
#
delete interfaces ge-0/0/0 unit 0 family inet
#
set interfaces ge-0/0/0 unit 0 family inet address 206.74.191.179/24
set interfaces ge-0/0/0 unit 0 family inet filter input FLTR-L3-R2E-ClassifyInbound
#
set routing-options static route 0.0.0.0/0 next-hop 206.74.191.1
#
# Set up port ge-0/0/0 as a 100mbps uuplink WAN port which requires using a shaping-rate rule.
#
set class-of-service interfaces ge-0/0/* shaping-rate 100m
#
# ========================================================================= #
#                                                                           #
# Note that some older Junos SRX implementations require the following:    #
#                                                                           #
#  set class-of-service interfaces ge-0/0/0 per-unit-scheduler             #
#  set class-of-service interfaces ge-0/0/0 unit 0 shaping-rate 100m       #
```

```
# ========================================================================== #
#
################################################################################
#
#
# Set up ports ge-0/0/[1-2] as trunk ports
#
#
delete interfaces ge-0/0/1 unit 0 family ethernet-switching
edit interfaces ge-0/0/1 unit 0 family ethernet-switching
#
# ELS Version
set interface-mode trunk
#
# Old Non-ELS Version
set port-mode trunk
set vlan members [ Vlan-Lan1 Vlan-Lan2 Vlan-Mgmt ]
top
#
delete interfaces ge-0/0/2 unit 0 family ethernet-switching
edit interfaces ge-0/0/2 unit 0 family ethernet-switching
#
# ELS Version
set interface-mode trunk
#
# Old Non-ELS Version
set port-mode trunk
set vlan members [ Vlan-Lan1 Vlan-Lan2 Vlan-Mgmt ]
top
#
################################################################################
#
#
# Set up ports ge-0/0/[3-15] as access ports on Vlan-Lan1
#
# Note that different models will have different port names/numbers and may have a
# completely different default configuration.  You must adjust as needed.
#
#
# ELS Version
wildcard range delete interfaces ge-0/0/[3-14] unit 0 family ethernet-switching
delete security zones security-zone untrust interfaces ge-0/0/15.0
delete interfaces ge-0/0/15 unit 0 family inet
#
wildcard range set interfaces ge-0/0/[3-15] unit 0 family ethernet-switching vlan members Vlan-Lan1
#
```

Appendix D –Fortinet Equipment

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 recreate them. It will also allow you to simplify the configuration as you won't have to replicate rules for each interface that is part of the Zone. Deleting and reentering most of your configuration just to move the LAN interface from port 5 to port 6 due to port hardware failure is quite painful and is disruptive to production traffic. Changing the membership of the LAN zone from port 5 to port 6 takes only seconds and is not disruptive.
    - Note that you can create a dummy loopback interface to act as a placeholder in a Zone. This allows you to create Zones in anticipation of a future need.
- Likewise, ***create Address Groups to use in lieu of individual address elements*** and ***Service Groups to be used in lieu of individual service elements***.
    - Note that you can create a 'DUMMY' address using an address from the 169.254.0.0/16 reserved space to place in an Address Group so that you can keep the group in the configuration even without any real addresses in it.
- Traffic should be marked with appropriate DSCP values at the earliest possible opportunity. DSCP values should be trusted and passed along throughout the network.

*Please note that Windows machines which connect via WiFi will pass through a Wireless Access Point (WAP) before any switches, routers, or firewalls are encountered. You **MUST** implement the group policy as defined in Appendix A so that the traffic classified and marked for the WAP to process. WAPs are dependent on the DSCP marking of traffic to enable WMM (Wireless Multimedia) prioritization of voice/video traffic. Without this marking a congested wireless network will not support Windows voice / video traffic effectively under multiuser conditions.*

RingCentral Specific Notes

Do not enable the SIP ALG (Application Layer Gateway / Proxy) or apply any Voice Profiles for any RingCentral traffic. Doing so can result in strange and difficult to diagnose issues.

SIP ALG/Proxy (and Voice Profiles) implementations adjust the SIP VIA headers such that all phones have the same (external) source ip address. RingCentral depends upon the VIA header reflecting the original ***interior*** source ip address. The Session Border Controllers do not allow for multiple instances of the same SIP UserID (DL number) to be associated with a single IP address. This presents a problem since hard phones, PC soft-phones, and mobile phone instances exist on the same network.

SIP ALG does not normally present a problem as the built-in configuration expects SIP traffic to be on ports 5060-5061 and RingCentral does not use these ports, but it is far safer to specifically disable it unless you are also using a product such as Microsoft Teams that requires it. Do not 'fix' the ALG to use the RingCentral ports.

Below are the steps involved in disabling the SIP session helper:

1) Remove the session helper.

Run the show command under system session-helper:

```
config system session-helper
show
```

Among the displayed settings may be one with a name of 'sip' and a protocol of 17, similar to the following example:

```
edit 13
    set name sip
    set protocol 17
    set port 5060
next
```

Here entry 13 is the one which points to SIP traffic which uses UDP port 5060 for signaling. In this example, the next commands to remove the corresponding entry would be:

```
delete 13
end
```

Note: It is not necessary for the SIP entry to be 13, so crosscheck which entry has the sip helper settings.

2) Change the default–voip–alg-mode.

By default, the default-voip-alg-mode is set to proxy-based.

For FortiOS versions prior to 6.2.2 run the following commands:

```
config system settings
    set default-voip-alg-mode kernel-helper-based
    set sip-helper disable
    set sip-nat-trace disable
end
```

For FortiOS versions 6.2.2 and later run the following commands:

```
config system settings
    set default-voip-alg-mode kernel-helper-based
    set sip-expectation disable
    set sip-nat-trace disable
end
```

Standalone Fortigate Configuration

This configuration guide describes full QoS support to an existing configured firewall. It does NOT discuss setting up advanced security features.

Please note that the website https://www.celab.ringcentral.com describes a complex 'meshed' configuration implementing seamless failover and, for some FortiOS versions, automated error correction using FEC.

Example Configuration Assumptions

The configuration steps detailed in this guide have been exhaustively tested using a virtual instance of FortiOS 6.2.3 running on vmWare ESXi 6.7 and on a Fortigate 60E hardware appliance. The firewall has the following working basic configuration prior to application of the contents of this guide.

- Interfaces
  - Zone ZN_Mgmt
    - port1 – Management vlan
  - Zone ZN_Outside
    - port2 – WAN circuit 1 (173.95.7.198/27) <secondary Internet pathway>
    - port3 – WAN circuit 2 (12.31.117.9/27) <primary Internet pathway>
  - Zone ZN_Lan
    - port4 – LAN circuit (192.168.130.1/24, DHCP Server)
- Static Routes
  - 0.0.0.0/0 via 173.95.76.193, distance 20 (secondary Internet gateway)
  - 0.0.0.0/0 via 12.31.117.1, distance 10 (primary Internet gateway)
- IPv4 Policies
  - ZN_LAN → ZN_Mgmt, Allow all, no NAT
  - ZN_Mgmt → ZN_LAN, Allow all, no NAT
  - ZN_Lan → ZN_Outside, Allow all, NAT using Outgoing Interface Address
  - ZN_Mgmt → ZN_Outside, Allow all, NAT using Outgoing Interface Address

The bandwidth values used in the example configurations are only examples and must be adjusted to reflect actual customer network architecture and needs. RingCentral account/system engineers can work with you to determine the correct values for your implementation.

RingCentral Traffic Handling Configurations

Step 1: Use CLI to set up the Fortigate to utilize DSCP, establish queue priorities, and set up address/service definitions.

```
# Housekeeping and general global settings
#
config system global
    #
    # Use DSCP features for traffic priority processing
    set traffic-priority dscp
    #
```

```
    # Set default packet priority to LOW instead of default MEDIUM
    set traffic-priority-level low
    #
    # On receipt of TCP packet with no defined tcp session return a reset.
    # This speed up phone resets in the event of a WAN failure.
    #
    set reset-sessionless-tcp enable
    #
end
#
# Set up DSCP priorities and assign packets with certain DSCP priorities
# to specific priority queues.
#
config system dscp-based-priority
    # Real-time audio
    edit 46
        # DSCP EF
        set ds 46
        set priority high
    next
    # Real-time video
    edit 34
        # DSCP AF41
        set ds 34
        set priority medium
    next
    # Signaling / Control
    edit 26
        # DSCP AF31
        set ds 26
        set priority medium
    next
end
#
# Most communication with RingCentral occurs to a set of predefined public IP
# addresses.  These are defined and placed in a convenient Address Groups.
#
# Do NOT associate with any individual interface or zone.
#
config firewall address
    edit "ADR_RC_1"
        set subnet 103.44.68.0 255.255.252.0
    next
    edit "ADR_RC_2"
        set subnet 104.245.56.0 255.255.248.0
    next
    edit "ADR_RC_3"
        set subnet 185.23.248.0 255.255.252.0
    next
    edit "ADR_RC_4"
        set subnet 192.209.24.0 255.255.248.0
    next
    edit "ADR_RC_5"
        set subnet 199.255.120.0 255.255.252.0
    next
    edit "ADR_RC_6"
        set subnet 199.68.212.0 255.255.252.0
    next
    edit "ADR_RC_7"
        set subnet 208.87.40.0 255.255.252.0
    next
    edit "ADR_RC_8"
        set subnet 80.81.128.0 255.255.240.0
    next
    edit "ADR_RC_9"
        set subnet 66.81.240.0 255.255.240.0
```

```
        next
        edit "ADR_RC_11"
             set type fqdn
             set fqdn "ringcentral.com"
        next
        edit "ADR_RC_Prov_1"
             set type fqdn
             set fqdn "pp.ringcentral.com"
        next
        edit "ADR_RC_Prov_2"
             set type fqdn
             set fqdn "cp.ringcentral.com"
        next
        edit "ADR_RC_Prov_3"
             set type fqdn
             set fqdn "yp.ringcentral.com"
        next
        edit "ADR_RC_FwUp_1"
             set type fqdn
             set fqdn "pp.s3.ringcentral.com"
        next
        edit "ADR_RC_API_1"
             set type fqdn
             set fqdn "platform.ringcentral.com"
        next
        edit "ADR_RC_API_2"
             set type fqdn
             set fqdn "platform.devtest.ringcentral.com"
        next
    end
    #
    # Define Address Groups for convenience and simplified configuration.
    #
    config firewall addrgrp
        edit "AG_RingCentral"
            set member "ADR_RC_1" "ADR_RC_2" "ADR_RC_3" "ADR_RC_4" "ADR_RC_5" "ADR_RC_6" "ADR_RC_7"
    "ADR_RC_8" "ADR_RC_9"
        next
        edit "AG_RC_Prov"
            set member "ADR_RC_Prov_1" "ADR_RC_Prov_2" "ADR_RC_Prov_3"
        next
        edit "AG_RC_FwUp"
            set member "ADR_RC_FwUp_1"
        next
        edit "AG_RC_API"
            set member "ADR_RC_API_1" "ADR_RC_API_2"
        next
    end
    #
    # Define service ports for RingCentral
    #
    config firewall service custom
        edit "SVC_RC_SIP"
            set category "VoIP, Messaging & Other Applications"
            set tcp-portrange 5090-5099 8083-8090 5060-5061
            set udp-portrange 5090-5099 5060
        next
        edit "SVC_RC_RTP"
            set category "VoIP, Messaging & Other Applications"
            set udp-portrange 20000-64999 8803
        next
        edit "SVC_RC_Video"
            set category "VoIP, Messaging & Other Applications"
            set tcp-portrange 8801-8802
            set udp-portrange 8801-8802 10000-19999
        next
```

```
    edit "SVC_RC_Prov"
        set category "VoIP, Messaging & Other Applications"
        set tcp-portrange 443
    next
    edit "SVC_RC_FwUp"
        set category "VoIP, Messaging & Other Applications"
        set tcp-portrange 443
    next
    edit "SVC_RC_Pres"
        set category "VoIP, Messaging & Other Applications"
        set tcp-portrange 80 443
    next
    edit "SVC_RC_API"
        set category "VoIP, Messaging & Other Applications"
        set tcp-portrange 443
    next
end
```

Step 2: **CRITICAL** - Set outbound bandwidth on circuits **DIRECTLY** connected to WAN providers. **Do NOT** set outbound bandwidth on circuits if they feed WAN routers or other devices that are set to perform traffic shaping.

```
#
# Set the outbound bandwidth on *EACH* WAN interface to 95% of the contracted
# data rate.  For instance, a 100Mbps connection should be set to 95Mbps.
# Specify the value in kilobits per second.  The example shows 5.5Mbps
# (5.225Mbps) and 100Mbps (95Mbps).  This will ensure that slightly different
# clock rates will NOT result in data transmission exceeding the carriers'
# rate limits.
#
# Note that these settings are ONLY available via the CLI.  The speeds
# displayed on the GUI for WAN circuits are for a different purpose and
# will not set these values.
#
# Be sure to get this correct as the Fortigate will NOT transmit traffic
# faster than this setting.  Anything faster will be DISCARDED. On the
# other hand, setting the value faster than the contracted data rate will
# result in your carrier randomly discarding excess traffic.
#
config sys interface
    edit "port2"
        # Cable ISP with 5.5Mbps up limit; ADJUST AS NEEDED
        set outbandwidth 5225
   next
   edit "port3"
        # Corporate DIA with 100Mbps; ADJUST AS NEEDED
        set outbandwidth 95000
   next
end
```

Step 3: Establish traffic shapers for traffic marked as DSCP EF (46), AF41 (34), and AF31 (26). Guaranteed bandwidth is the minimum bandwidth that will be provided for the classification, maximum bandwidth allows extra to be used up to this limit. The values are given in kbps. The **sum** of the guaranteed bandwidths ***MUST NOT EXCEED*** the total bandwidth set on the WAN circuit in the previous step.

```
config firewall shaper traffic-shaper
    #
    # Voice Real-time traffic (800kbps); ADJUST AS NEEDED
    #
```

```
    edit "TS_DSCP_EF"
        set guaranteed-bandwidth 800
        set maximum-bandwidth 800
        set priority high
    next
    #
    # Video traffic (800kbps, 1000kbps if available); ADJUST AS NEEDED
    #
    edit "TS_DSCP_AF41"
        set guaranteed-bandwidth 800
        set maximum-bandwidth 1000
        set priority medium
    next
    #
    # SIP Signaling traffic (64kbps, 128kbps if available); ADJUST AS NEEDED
    #
    edit "TS_DSCP_AF31"
        set guaranteed-bandwidth 64
        set maximum-bandwidth 128
        set priority high
    next
end
```

Step 4: Establish traffic shaping policy rules to push traffic into the traffic shapers just defined and to force the Fortigate unit to restore the proper DSCP tags onto returned traffic. (Most ISPs remove or alter the DSCP values on traffic as it passes through their networks.)

Step 4a: The following code is used when outbound traffic is already marked with the proper DSCP tags. It keeps track of the connection session and applies the indicated DSCP tag to the return packets.

> WARNING: There is a Fortigate bug that has yet to be addressed which prevents you from backing up and restoring these DSCP matching policies without editing the backup file prior to the restore. The backup procedure outputs the '**`set tos`**' clause before it outputs the '**`set tos-mask`**' clause. On restore, the '**`set tos-mask`**' clause MUST be issued prior to the '**`set tos`**' clause or the '**`set tos`**' clause is silently ignored and the policies will **NOT** function as designed!

```
config firewall shaping-policy
    edit 0
        # DSCP EF Realtime Traffic – Already Marked
        set name "TSP_DSCP_EF"
        set tos-mask 0xfc
        set tos 0xb8
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        set dstintf "ZN_Outside"
        set traffic-shaper "TS_DSCP_EF"
        set traffic-shaper-reverse "TS_DSCP_EF"
        set diffserv-reverse enable
        set diffservcode-rev 101110
    next
    edit 0
        # DSCP AF41 Video Realtime Traffic – Already Marked
        set name "TSP_DSCP_AF41"
        set tos-mask 0xfc
        set tos 0x88
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        set dstintf "ZN_Outside"
        set traffic-shaper "TS_DSCP_AF41"
```

```
            set traffic-shaper-reverse "TS_DSCP_AF41"
            set diffserv-reverse enable
            set diffservcode-rev 100010
        next
        edit 0
            # DSCP AF31 Signaling Traffic – Already Marked
            set name "TSP_DSCP_AF31"
            set tos-mask 0xfc
            set tos 0x68
            set srcaddr "all"
            set dstaddr "all"
            set service "ALL"
            set dstintf "ZN_Outside"
            set traffic-shaper "TS_DSCP_AF31"
            set traffic-shaper-reverse "TS_DSCP_AF31"
            set diffserv-reverse enable
            set diffservcode-rev 011010
        next
        edit 0
            # DSCP AF21 Other Traffic – Already Marked
            set name "TSP_DSCP_AF21"
            set tos-mask 0xfc
            set tos 0x48
            set srcaddr "all"
            set dstaddr "all"
            set service "ALL"
            set dstintf "ZN_Outside"
            set diffserv-reverse enable
            set diffservcode-rev 010010
        next
    end
```

Step 4b: The following code is used when outbound traffic is NOT marked with the proper DSCP tags. It keeps track of the connection session and applies the indicated DSCP tag to the return packets. These policies are order dependent!

```
    config firewall shaping-policy
        edit 0
            # Voice Real-Time Traffic
            set name "TSP_RC_RTVoice"
            set service "SVC_RC_RTP"
            set dstintf "ZN_Outside"
            set traffic-shaper "TS_DSCP_EF"
            set traffic-shaper-reverse "TS_DSCP_EF"
            set diffserv-forward enable
            set diffserv-reverse enable
            set srcaddr "all"
            set dstaddr "AG_RingCentral"
            set diffservcode-forward 101110
            set diffservcode-rev 101110
        next
        edit 0
            # Video Traffic
            set name "TSP_RC_RTVideo"
            set service "SVC_RC_Video"
            set dstintf "ZN_Outside"
            set traffic-shaper "TS_DSCP_AF41"
            set traffic-shaper-reverse "TS_DSCP_AF41"
            set diffserv-forward enable
            set diffserv-reverse enable
            set srcaddr "all"
            set dstaddr "AG_RingCentral"
            set diffservcode-forward 100010
            set diffservcode-rev 100010
```

```
        next
        edit 0
            # Normal SIP Signaling
            set name "TSP_RC_Signal"
            set service "SVC_RC_SIP"
            set dstintf "ZN_Outside"
            set traffic-shaper "TS_DSCP_AF31"
            set traffic-shaper-reverse "TS_DSCP_AF31"
            set diffserv-forward enable
            set diffserv-reverse enable
            set srcaddr "all"
            set dstaddr "AG_RingCentral"
            set diffservcode-forward 011010
            set diffservcode-rev 011010
        next
        edit 0
            # Other RC Traffic
            set name "TSP_RC_Other"
            set service "ALL"
            set dstintf "ZN_Outside"
            set traffic-shaper "TS_DSCP_AF31"
            set traffic-shaper-reverse "TS_DSCP_AF31"
            set diffserv-forward enable
            set diffserv-reverse enable
            set srcaddr "all"
            set dstaddr "AG_RingCentral"
            set diffservcode-forward 011010
            set diffservcode-rev 011010
        next
    end
```

Monitor links and fail-over on link failure

Strictly speaking, this is not part of QoS classification and marking, but I am frequently asked about how to handle failover between two WAN interfaces.

Please note that this 'brute-force' failover results in assignment of a new source address by NAT. All current phone calls will be dropped, phone registrations must time-out, and the phones must re-register before they become active once more.

Step 1: Use the CLI to set up the Fortigate to have static routes out **EACH** desired WAN interface with the distances set as shown.

```
    #
    # REPEAT FOR EACH PHYSICAL WAN INTERFACE/VLAN, NOT ZONE BASED
    #
    # Create static routes to all RingCentral supernets.
    #
    # Adjust administrative distance from the default value of 10
    # to control order of use between interfaces.  Smaller numbers
    # are used first.
    #
    # The following code will preferentially send RingCentral traffic
    # out via port3 through gateway 12.31.117.1.  Use actual port names
    # and not Zone names.
    #
    # A secondary route will be provided out via port2 through gateway
    # 173.95.76.193.  A distance of 11 ensures that it is only used if the
    # primary routes with a distance of 10 are withdrawn.
    #
    # A test applied in step 2 will ping a target address using the
    # primary port and, upon failure, automatically invalidate any static
```

```
# routes defined using that port.  This will result in the traffic using
# the more distant routes or using the last-ditch default route.
#
# Note that we only show 2 outbound pathways here.  Some customers have a
# primary and secondary pathways across dedicated circuits to RingCentral
# along with multiple Internet links. Please note that normal route
# selection rules apply:
#     1. smallest enclosing network takes priority over longer networks
#     2. smallest distance when routes are identical
#
config router static
    #
    # Define Primary Routes over primary WAN link for each of the 9 RingCentral
    # address blocks.  An administrative distance of 10 is used for primary
    # routes.
    #
    edit 0
      set dst 66.81.240.0/20
      set gateway 12.31.117.1
      set device "port3"
      set distance 10
    next
    edit 0
      set dst 80.81.128.0/20
      set gateway 12.31.117.1
      set device "port3"
      set distance 10
    next
    edit 0
      set dst 103.44.68.0/22
      set gateway 12.31.117.1
      set device "port3"
      set distance 10
    next
    edit 0
      set dst 104.245.56.0/21
      set gateway 12.31.117.1
      set device "port3"
      set distance 10
    next
    edit 0
      set dst 185.123.248.0/22
      set gateway 12.31.117.1
      set device "port3"
      set distance 10
    next
    edit 0
      set dst 192.209.29.0/21
      set gateway 12.31.117.1
      set device "port3"
      set distance 10
    next
    edit 0
      set dst 199.255.120.0/22
      set gateway 12.31.117.1
      set device "port3"
      set distance 10
    next
    edit 0
      set dst 199.68.212.0/22
      set gateway 12.31.117.1
      set device "port3"
      set distance 10
    next
    edit 0
      set dst 208.87.40.0/22
```

```
        set gateway 12.31.117.1
        set device "port3"
        set distance 10
      next
      #
      # Define Backup Routes over secondary WAN link for each of the 8
      # RingCentral address blocks.  An administrative distance of 11 is used for
      # backup routes..
      #
      edit 0
        set dst 66.81.240.0/20
        set gateway 173.95.76.193
        set device "port2"
        set distance 11
      next
      edit 0
        set dst 80.81.128.0/20
        set gateway 173.95.76.193
        set device "port2"
        set distance 11
      next
      edit 0
        set dst 103.44.68.0/22
        set gateway 173.95.76.193
        set device "port2"
        set distance 11
      next
      edit 0
        set dst 104.245.56.0/21
        set gateway 173.95.76.193
        set device "port2"
        set distance 11
      next
      edit 0
        set dst 185.123.248.0/22
        set gateway 173.95.76.193
        set device "port2"
        set distance 11
      next
      edit 0
        set dst 192.209.29.0/21
        set gateway 173.95.76.193
        set device "port2"
        set distance 11
      next
      edit 0
        set dst 199.255.120.0/22
        set gateway 173.95.76.193
        set device "port2"
        set distance 11
      next
      edit 0
        set dst 199.68.212.0/22
        set gateway 173.95.76.193
        set device "port2"
        set distance 11
      next
      edit 0
        set dst 208.87.40.0/22
        set gateway 173.95.76.193
        set device "port2"
        set distance 11
      next
end
```

Step 2: Use the CLI to set up the Fortigate link health monitoring to shut down all static routes established through the failed primary WAN pathway. **Use actual interface names, not zones.** All pathways except the highest cost / last-ditch pathway should be monitored.

```
config system link-monitor
    edit 0
      set srcintf "port3"
      set server "199.255.120.129"
      set failtime 3
      set recoverytime 2
      set update-static-route enable
      set interval 10000
    next
end
```

Appendix E –Palo Alto Firewalls

Best Practices for Palo Alto Configurations

- Never use a single Address or Service reference in a policy; always create Address Groups and Service Groups to use in lieu of individual address/service elements. This allows you to change the contents of the service/address group without having to delete/add all the policy elements that reference them.

Implementing QoS

This document assumes that the customer has a known working Palo Alto configuration with the WAN/ISP/Internet interface located in zone L3-untrust. The security rules will properly apply DSCP markings on traffic flowing *toward* RingCentral. Traffic flowing from the L3-untrust zone into the company LAN will be prioritized within the Palo Alto, but the Palo Alto will not rewrite the DSCP tags to the correct values. A separate device will be required to rewrite those tags.

Use SSH to log into an administrative account on the Palo Alto and issue the following commands to create the required data structures and to disable the SIP ALG subsystem: (please note the green line-break characters… you must paste the entire line as a single line, the Palo Alto will not accept line continuations)

```
set cli scripting-mode on
set cli terminal width 500
configure
!
set shared alg-override application sip alg-disabled yes
!
! Define services for E2R direction (Endpoint to RingCentral)
!
set service SVC-RC-E2R-SIGNALING-UDP protocol udp port 5090-5099,5060
set service SVC-RC-E2R-SIGNALING-TCP protocol tcp port 5090-5099,8083-8090,5060-5061
set service-group SG-RC-E2R-SIGNALING members [ SVC-RC-E2R-SIGNALING-TCP -
        SVC-RC-E2R-SIGNALING-UDP ]
set service SVC-RC-E2R-VOICE protocol udp port 20000-64999,8803
set service-group SG-RC-E2R-VOICE members [ SVC-RC-E2R-VOICE ]
set service SVC-RC-E2R-Video-UDP protocol udp port 8801-8802,10000-19999
set service SVC-RC-E2R-Video-TCP protocol tcp port 8801-8802
set service-group SG-RC-E2R-Video members [ SVC-RC-E2R-Video-UDP SVC-RC-E2R-Video-TCP ]
!
! Define services for R2E direction (RingCentral to Endpoint)
!
set service SVC-RC-R2E-SIGNALING-UDP protocol udp source-port 5090-5099,5060 port 0-65535
set service SVC-RC-R2E-SIGNALING-TCP protocol tcp source-port 5090-5099,8083-8090,5060-5061 -
        port 0-65535
set service-group SG-RC-R2E-SIGNALING members [ SVC-RC-R2E-SIGNALING-TCP -
        SVC-RC-R2E-SIGNALING-UDP ]
set service SVC-RC-R2E-VOICE protocol udp source-port 20000-64999,8803 port 0-65535
set service-group SG-RC-R2E-VOICE members [ SVC-RC-R2E-VOICE ]
set service SVC-RC-R2E-Video-UDP protocol udp source-port 8801-8802,10000-19999 port 0-65535
set service SVC-RC-R2E-Video-TCP protocol tcp source-port 8801-8802 port 0-65535
set service-group SG-RC-R2E-Video members [ SVC-RC-R2E-Video-UDP SVC-RC-R2E-Video-TCP ]
!
! Set up Address Group for all RingCentral space
!
set address ADR-RC-1 ip-netmask 103.44.68.0/22
```

```
set address ADR-RC-2 ip-netmask 104.245.56.0/21
set address ADR-RC-3 ip-netmask 185.23.248.0/22
set address ADR-RC-4 ip-netmask 192.209.24.0/21
set address ADR-RC-5 ip-netmask 199.255.120.0/22
set address ADR-RC-6 ip-netmask 199.68.212.0/22
set address ADR-RC-7 ip-netmask 208.87.40.0/22
set address ADR-RC-8 ip-netmask 80.81.128.0/20
set address ADR-RC-9 ip-netmask 66.81.240.0/20
set address-group AG-RingCentral static [ ADR-RC-1 ADR-RC-2 ADR-RC-3 ADR-RC-4 -
        ADR-RC-5 ADR-RC-6 ADR-RC-7 ADR-RC-8 ADR-RC-9 ]
set address-group AG-RingCentral description "All RingCentral Public Address Space"
!
! Define security policy rules for E2R traffic.  These rules will also rewrite
! the DSCP value in the packet headers to the correct value.
!
! NOTE: This only works in the E2R (toward RingCentral) direction.
!
set rulebase security rules RC-E2R-VIDEO to any
set rulebase security rules RC-E2R-VIDEO from any
set rulebase security rules RC-E2R-VIDEO source any
set rulebase security rules RC-E2R-VIDEO destination AG-RingCentral
set rulebase security rules RC-E2R-VIDEO source-user any
set rulebase security rules RC-E2R-VIDEO category any
set rulebase security rules RC-E2R-VIDEO application any
set rulebase security rules RC-E2R-VIDEO service SG-RC-E2R-Video
set rulebase security rules RC-E2R-VIDEO hip-profiles any
set rulebase security rules RC-E2R-VIDEO action allow
set rulebase security rules RC-E2R-VIDEO rule-type interzone
set rulebase security rules RC-E2R-VIDEO qos marking ip-dscp af41
!
set rulebase security rules RC-E2R-SIGNALING to any
set rulebase security rules RC-E2R-SIGNALING from any
set rulebase security rules RC-E2R-SIGNALING source any
set rulebase security rules RC-E2R-SIGNALING destination AG-RingCentral
set rulebase security rules RC-E2R-SIGNALING source-user any
set rulebase security rules RC-E2R-SIGNALING category any
set rulebase security rules RC-E2R-SIGNALING application any
set rulebase security rules RC-E2R-SIGNALING service SG-RC-E2R-SIGNALING
set rulebase security rules RC-E2R-SIGNALING hip-profiles any
set rulebase security rules RC-E2R-SIGNALING action allow
set rulebase security rules RC-E2R-SIGNALING rule-type interzone
set rulebase security rules RC-E2R-SIGNALING qos marking ip-dscp af31
!
set rulebase security rules RC-E2R-VOICE to any
set rulebase security rules RC-E2R-VOICE from any
set rulebase security rules RC-E2R-VOICE source any
set rulebase security rules RC-E2R-VOICE destination AG-RingCentral
set rulebase security rules RC-E2R-VOICE source-user any
set rulebase security rules RC-E2R-VOICE category any
set rulebase security rules RC-E2R-VOICE application any
set rulebase security rules RC-E2R-VOICE service SG-RC-E2R-VOICE
set rulebase security rules RC-E2R-VOICE hip-profiles any
set rulebase security rules RC-E2R-VOICE action allow
set rulebase security rules RC-E2R-VOICE rule-type interzone
set rulebase security rules RC-E2R-VOICE qos marking ip-dscp ef
!
set rulebase security rules RC-E2R-Other to any
set rulebase security rules RC-E2R-Other from any
set rulebase security rules RC-E2R-Other source any
set rulebase security rules RC-E2R-Other destination AG-RingCentral
set rulebase security rules RC-E2R-Other source-user any
set rulebase security rules RC-E2R-Other category any
set rulebase security rules RC-E2R-Other application any
set rulebase security rules RC-E2R-Other service any
set rulebase security rules RC-E2R-Other hip-profiles any
set rulebase security rules RC-E2R-Other action allow
set rulebase security rules RC-E2R-Other rule-type interzone
```

```
set rulebase security rules RC-E2R-Other qos marking ip-dscp af21
move rulebase security rules RC-E2R-Other top
move rulebase security rules RC-E2R-VOICE top
move rulebase security rules RC-E2R-SIGNALING top
move rulebase security rules RC-E2R-VIDEO top
!
! Define QoS Policy rules.  These rules are automatically applied to all traffic
! and serve to assign the traffic internally to QoS 'classes' which are used in
! network qos policies.
!
! Unfortunately they do not provide the capability to rewrite the DSCP
! tag in the packet.
!
set rulebase qos rules POL-QOS-EF dscp-tos any
set rulebase qos rules POL-QOS-EF from any
set rulebase qos rules POL-QOS-EF to L3-untrust
set rulebase qos rules POL-QOS-EF source any
set rulebase qos rules POL-QOS-EF destination AG-RingCentral
set rulebase qos rules POL-QOS-EF source-user any
set rulebase qos rules POL-QOS-EF category any
set rulebase qos rules POL-QOS-EF application any
set rulebase qos rules POL-QOS-EF service SG-RC-E2R-VOICE
set rulebase qos rules POL-QOS-EF action class 1
!
set rulebase qos rules POL-QOS-AF41 dscp-tos any
set rulebase qos rules POL-QOS-AF41 from any
set rulebase qos rules POL-QOS-AF41 to L3-untrust
set rulebase qos rules POL-QOS-AF41 source any
set rulebase qos rules POL-QOS-AF41 destination AG-RingCentral
set rulebase qos rules POL-QOS-AF41 source-user any
set rulebase qos rules POL-QOS-AF41 category any
set rulebase qos rules POL-QOS-AF41 application any
set rulebase qos rules POL-QOS-AF41 service SG-RC-E2R-Video
set rulebase qos rules POL-QOS-AF41 action class 2
!
set rulebase qos rules POL-QOS-AF31 dscp-tos any
set rulebase qos rules POL-QOS-AF31 from any
set rulebase qos rules POL-QOS-AF31 to L3-untrust
set rulebase qos rules POL-QOS-AF31 source any
set rulebase qos rules POL-QOS-AF31 destination AG-RingCentral
set rulebase qos rules POL-QOS-AF31 source-user any
set rulebase qos rules POL-QOS-AF31 category any
set rulebase qos rules POL-QOS-AF31 application any
set rulebase qos rules POL-QOS-AF31 service SG-RC-E2R-SIGNALING
set rulebase qos rules POL-QOS-AF31 action class 3
!
set rulebase qos rules POL-QOS-AF21 dscp-tos any
set rulebase qos rules POL-QOS-AF21 from any
set rulebase qos rules POL-QOS-AF21 to L3-untrust
set rulebase qos rules POL-QOS-AF21 source any
set rulebase qos rules POL-QOS-AF21 destination AG-RingCentral
set rulebase qos rules POL-QOS-AF21 source-user any
set rulebase qos rules POL-QOS-AF21 category any
set rulebase qos rules POL-QOS-AF21 application any
set rulebase qos rules POL-QOS-AF21 service any
set rulebase qos rules POL-QOS-AF21 action class 4
!
set rulebase qos rules POL-QOS-BE dscp-tos any
set rulebase qos rules POL-QOS-BE from any
set rulebase qos rules POL-QOS-BE to L3-untrust
set rulebase qos rules POL-QOS-BE source any
set rulebase qos rules POL-QOS-BE destination any
set rulebase qos rules POL-QOS-BE source-user any
set rulebase qos rules POL-QOS-BE category any
set rulebase qos rules POL-QOS-BE application any
set rulebase qos rules POL-QOS-BE service any
set rulebase qos rules POL-QOS-BE action class 8
```

```
!
set rulebase qos rules POL-QOS-EF-INB dscp-tos any
set rulebase qos rules POL-QOS-EF-INB from L3-untrust
set rulebase qos rules POL-QOS-EF-INB to any
set rulebase qos rules POL-QOS-EF-INB source AG-RingCentral
set rulebase qos rules POL-QOS-EF-INB destination any
set rulebase qos rules POL-QOS-EF-INB source-user any
set rulebase qos rules POL-QOS-EF-INB category any
set rulebase qos rules POL-QOS-EF-INB application any
set rulebase qos rules POL-QOS-EF-INB service SG-RC-R2E-VOICE
set rulebase qos rules POL-QOS-EF-INB action class 1
!
set rulebase qos rules POL-QOS-AF41-INB dscp-tos any
set rulebase qos rules POL-QOS-AF41-INB from L3-untrust
set rulebase qos rules POL-QOS-AF41-INB to any
set rulebase qos rules POL-QOS-AF41-INB source AG-RingCentral
set rulebase qos rules POL-QOS-AF41-INB destination any
set rulebase qos rules POL-QOS-AF41-INB source-user any
set rulebase qos rules POL-QOS-AF41-INB category any
set rulebase qos rules POL-QOS-AF41-INB application any
set rulebase qos rules POL-QOS-AF41-INB service SG-RC-R2E-Video
set rulebase qos rules POL-QOS-AF41-INB action class 2
!
set rulebase qos rules POL-QOS-AF31-INB dscp-tos any
set rulebase qos rules POL-QOS-AF31-INB from L3-untrust
set rulebase qos rules POL-QOS-AF31-INB to any
set rulebase qos rules POL-QOS-AF31-INB source AG-RingCentral
set rulebase qos rules POL-QOS-AF31-INB destination any
set rulebase qos rules POL-QOS-AF31-INB source-user any
set rulebase qos rules POL-QOS-AF31-INB category any
set rulebase qos rules POL-QOS-AF31-INB application any
set rulebase qos rules POL-QOS-AF31-INB service SG-RC-R2E-SIGNALING
set rulebase qos rules POL-QOS-AF31-INB action class 3
!
set rulebase qos rules POL-QOS-AF21-INB dscp-tos any
set rulebase qos rules POL-QOS-AF21-INB from L3-untrust
set rulebase qos rules POL-QOS-AF21-INB to any
set rulebase qos rules POL-QOS-AF21-INB source AG-RingCentral
set rulebase qos rules POL-QOS-AF21-INB destination any
set rulebase qos rules POL-QOS-AF21-INB source-user any
set rulebase qos rules POL-QOS-AF21-INB category any
set rulebase qos rules POL-QOS-AF21-INB application any
set rulebase qos rules POL-QOS-AF21-INB service any
set rulebase qos rules POL-QOS-AF21-INB action class 4
!
set rulebase qos rules POL-QOS-BE-INB dscp-tos any
set rulebase qos rules POL-QOS-BE-INB from L3-untrust
set rulebase qos rules POL-QOS-BE-INB to any
set rulebase qos rules POL-QOS-BE-INB source any
set rulebase qos rules POL-QOS-BE-INB destination any
set rulebase qos rules POL-QOS-BE-INB source-user any
set rulebase qos rules POL-QOS-BE-INB category any
set rulebase qos rules POL-QOS-BE-INB application any
set rulebase qos rules POL-QOS-BE-INB service any
set rulebase qos rules POL-QOS-BE-INB action class 8
!
set rulebase application-override rules POL-AO-RingCentral-SIP-TCP from any
set rulebase application-override rules POL-AO-RingCentral-SIP-TCP to any
set rulebase application-override rules POL-AO-RingCentral-SIP-TCP source any
set rulebase application-override rules POL-AO-RingCentral-SIP-TCP destination -
        AG-RingCentral
set rulebase application-override rules POL-AO-RingCentral-SIP-TCP port 5090-5099, -
        8083-8090,5060-5061
set rulebase application-override rules POL-AO-RingCentral-SIP-TCP protocol tcp
set rulebase application-override rules POL-AO-RingCentral-SIP-TCP application sip
!
set rulebase application-override rules POL-AO-RingCentral-SIP-UDP from any
```

```
set rulebase application-override rules POL-AO-RingCentral-SIP-UDP to any
set rulebase application-override rules POL-AO-RingCentral-SIP-UDP source any
set rulebase application-override rules POL-AO-RingCentral-SIP-UDP destination -
        AG-RingCentral
set rulebase application-override rules POL-AO-RingCentral-SIP-UDP port 5090-5091,5060
set rulebase application-override rules POL-AO-RingCentral-SIP-UDP protocol udp
set rulebase application-override rules POL-AO-RingCentral-SIP-UDP application sip
!
! Set the internal qos 'classes' to the correct priority levels in the default
! network qos profile.
!
set network qos profile default class class1 priority real-time
set network qos profile default class class2 priority high
set network qos profile default class class3 priority high
set network qos profile default class class4 priority medium
set network qos profile default class class5 priority medium
set network qos profile default class class6 priority low
set network qos profile default class class7 priority low
set network qos profile default class class8 priority low

commit
```

Now you create at least two (or more) different QoS Profiles, one for the WAN egress and one for the LAN side egress. Some networks may have multiple interfaces serving these functions, each should have their own QoS Profile. In this example, we show two profiles, one for the WAN circuit and one for the LAN circuit. Please note that for the WAN profile you *must* know the supported/contracted upstream bandwidth. We assume that we can utilize 95% of that bandwidth. The WAN link in this example is assumed to be 100Mbps and the LAN is assumed to be 1Gbps. There are two bandwidth functions shown here, egress-max and egress-guaranteed. The egress-guaranteed is used to guarantee that traffic in this classification will ***always*** have ***at least*** this much bandwidth available for immediate use. The egress-max is an absolute maximum; anything over that rate is discarded. The values are specified in Megabits per second. You should use reasonable values for guarantees in the LAN policy. Insure that there is sufficient bandwidth for the number of concurrent phone/video calls. Adjust the rates and input the configuration as follows:

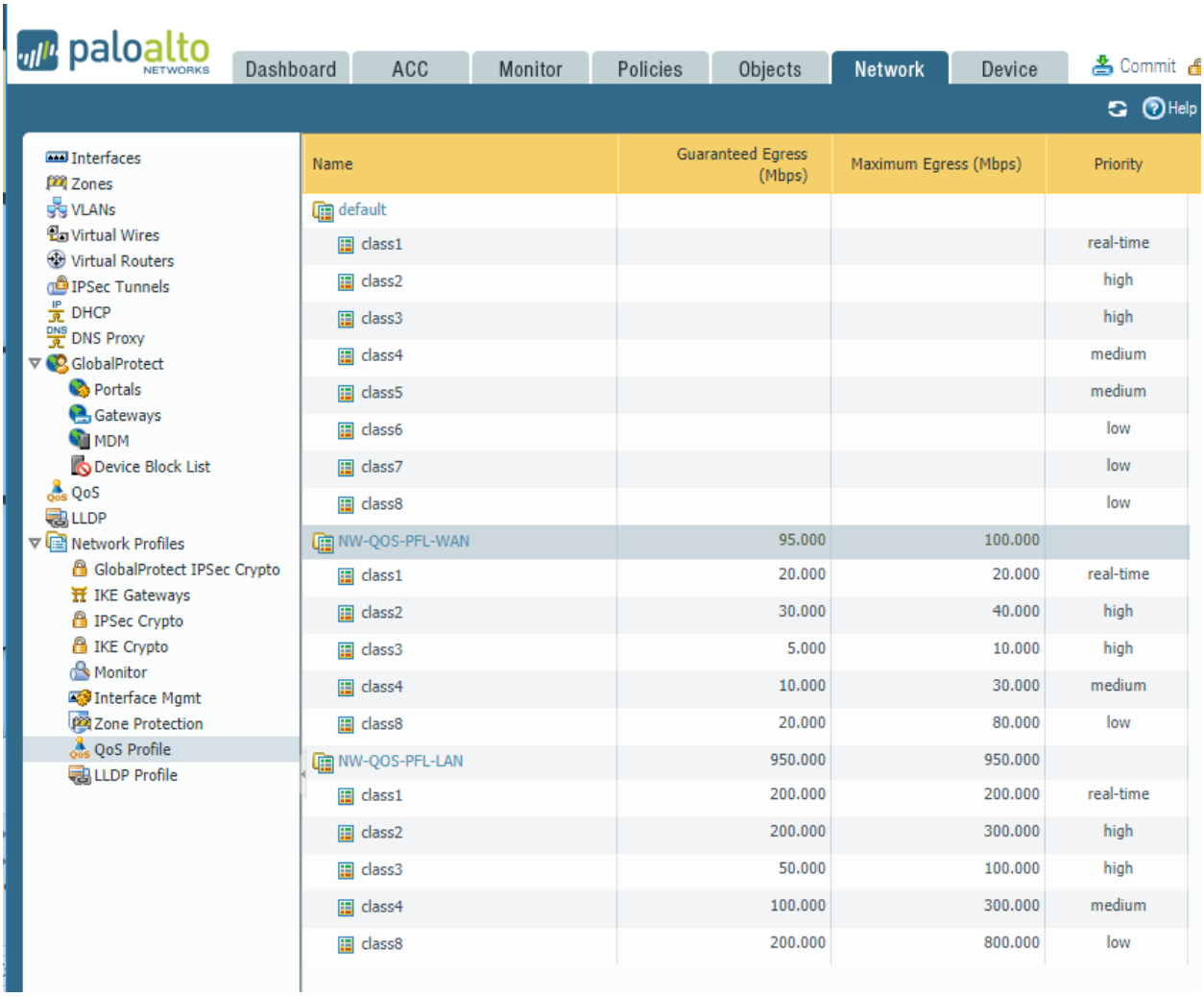
```
set network qos profile NW-QOS-PFL-WAN class class1 class-bandwidth egress-max 20
set network qos profile NW-QOS-PFL-WAN class class1 class-bandwidth egress-guaranteed 20
set network qos profile NW-QOS-PFL-WAN class class1 priority real-time
set network qos profile NW-QOS-PFL-WAN class class2 class-bandwidth egress-max 40
set network qos profile NW-QOS-PFL-WAN class class2 class-bandwidth egress-guaranteed 30
set network qos profile NW-QOS-PFL-WAN class class2 priority high
set network qos profile NW-QOS-PFL-WAN class class3 class-bandwidth egress-max 10
set network qos profile NW-QOS-PFL-WAN class class3 class-bandwidth egress-guaranteed 5
set network qos profile NW-QOS-PFL-WAN class class3 priority high
set network qos profile NW-QOS-PFL-WAN class class4 class-bandwidth egress-max 30
set network qos profile NW-QOS-PFL-WAN class class4 class-bandwidth egress-guaranteed 10
set network qos profile NW-QOS-PFL-WAN class class4 priority medium
set network qos profile NW-QOS-PFL-WAN class class8 class-bandwidth egress-max 80
set network qos profile NW-QOS-PFL-WAN class class8 class-bandwidth egress-guaranteed 20
set network qos profile NW-QOS-PFL-WAN class class8 priority low
set network qos profile NW-QOS-PFL-WAN aggregate-bandwidth egress-max 95
set network qos profile NW-QOS-PFL-WAN aggregate-bandwidth egress-guaranteed 95

set network qos profile NW-QOS-PFL-LAN class class1 class-bandwidth egress-max 200
set network qos profile NW-QOS-PFL-LAN class class1 class-bandwidth egress-guaranteed 200
set network qos profile NW-QOS-PFL-LAN class class1 priority real-time
set network qos profile NW-QOS-PFL-LAN class class2 class-bandwidth egress-max 300
set network qos profile NW-QOS-PFL-LAN class class2 class-bandwidth egress-guaranteed 300
set network qos profile NW-QOS-PFL-LAN class class2 priority high
```

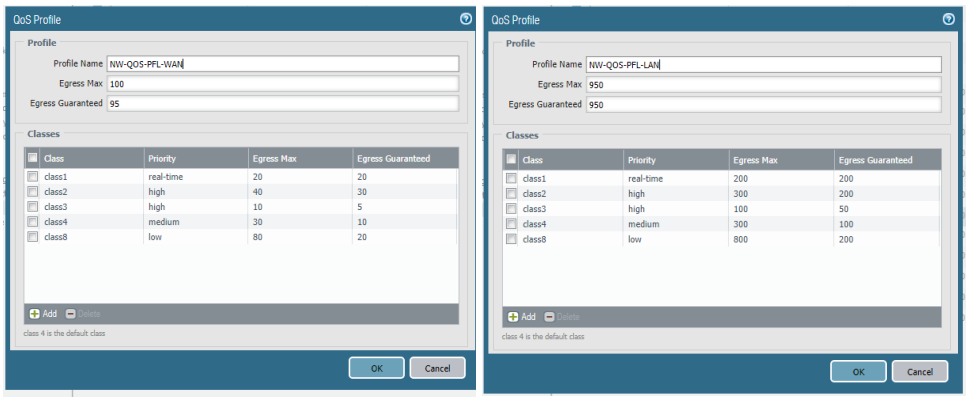
```
set network qos profile NW-QOS-PFL-LAN class class3 class-bandwidth egress-max 100
set network qos profile NW-QOS-PFL-LAN class class3 class-bandwidth egress-guaranteed 50
set network qos profile NW-QOS-PFL-LAN class class3 priority high
set network qos profile NW-QOS-PFL-LAN class class4 class-bandwidth egress-max 300
set network qos profile NW-QOS-PFL-LAN class class4 class-bandwidth egress-guaranteed 100
set network qos profile NW-QOS-PFL-LAN class class4 priority medium
set network qos profile NW-QOS-PFL-LAN class class8 class-bandwidth egress-max 800
set network qos profile NW-QOS-PFL-LAN class class8 class-bandwidth egress-guaranteed 200
set network qos profile NW-QOS-PFL-LAN class class8 priority low
set network qos profile NW-QOS-PFL-LAN aggregate-bandwidth egress-max 950
set network qos profile NW-QOS-PFL-LAN aggregate-bandwidth egress-guaranteed 950

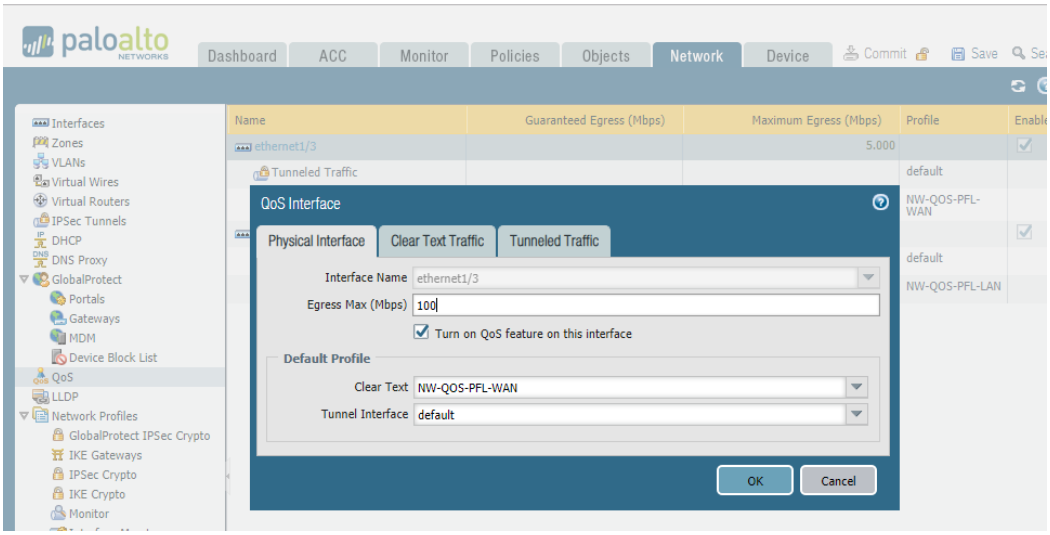
commit
```

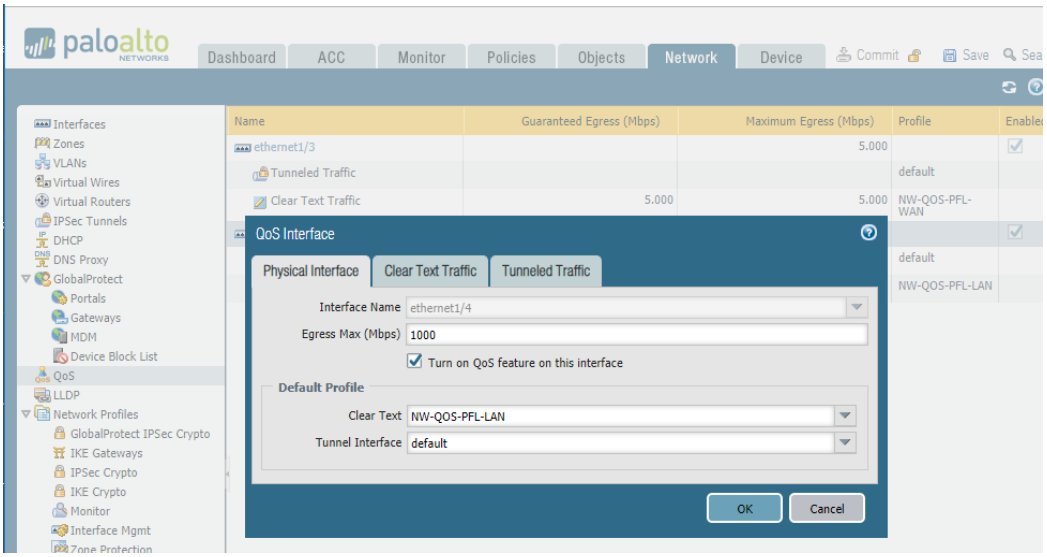
It may be more convenient to use the GUI to create and adjust these values. You also need to use the GUI to apply the QoS Profiles to the interfaces and enable QoS on them. Please note that you *must* apply an appropriate QoS profile to *each* interface and if the interface is running at less than the interface speed you must set the physical interface Egress-max parameter to 95% of the contracted circuit speed.



Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Priority
default			
class1			real-time
class2			high
class3			high
class4			medium
class5			medium
class6			low
class7			low
class8			low
NW-QOS-PFL-WAN	95.000	100.000	
class1	20.000	20.000	real-time
class2	30.000	40.000	high
class3	5.000	10.000	high
class4	10.000	30.000	medium
class8	20.000	80.000	low
NW-QOS-PFL-LAN	950.000	950.000	
class1	200.000	200.000	real-time
class2	200.000	300.000	high
class3	50.000	100.000	high
class4	100.000	300.000	medium
class8	200.000	800.000	low


QoS Profile
Profile
Profile Name NW-QOS-PFL-WAN
Egress Max 100
Egress Guaranteed 95
Classes
Class Priority Egress Max Egress Guaranteed
class1 real-time 20 20
class2 high 40 30
class3 high 10 5
class4 medium 30 10
class8 low 80 20
Add Delete
class 4 is the default class
OK Cancel
QoS Profile
Profile
Profile Name NW-QOS-PFL-LAN
Egress Max 950
Egress Guaranteed 950
Classes
Class Priority Egress Max Egress Guaranteed
class1 real-time 200 200
class2 high 300 200
class3 high 100 50
class4 medium 300 100
class8 low 800 200
Add Delete
class 4 is the default class
OK Cancel


paloalto NETWORKS
Dashboard ACC Monitor Policies Objects Network Device Commit Save
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Device Block List
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Name Guaranteed Egress (Mbps) Maximum Egress (Mbps) Profile
ethernet1/3 5.000
Tunneled Traffic default
NW-QOS-PFL-WAN
default
NW-QOS-PFL-LAN
QoS Interface
Physical Interface Clear Text Traffic Tunneled Traffic
Interface Name ethernet1/3
Egress Max (Mbps) 100
Turn on QoS feature on this interface
Default Profile
Clear Text NW-QOS-PFL-WAN
Tunnel Interface default
OK Cancel


paloalto NETWORKS
Dashboard ACC Monitor Policies Objects Network Device Commit Save
Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Device Block List
QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypto
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
Name Guaranteed Egress (Mbps) Maximum Egress (Mbps) Profile
ethernet1/3 5.000
Tunneled Traffic default
Clear Text Traffic 5.000 5.000 NW-QOS-PFL-WAN
default
NW-QOS-PFL-LAN
QoS Interface
Physical Interface Clear Text Traffic Tunneled Traffic
Interface Name ethernet1/4
Egress Max (Mbps) 1000
Turn on QoS feature on this interface
Default Profile
Clear Text NW-QOS-PFL-LAN
Tunnel Interface default
OK Cancel

When you set the Egress Max value under Physical Interface tab, you should also set the max and guaranteed bandwidth values under the Clear Text Traffic tab.

Remember to COMMIT and SAVE your configuration.

Appendix H – HP/Aruba Switches

There are two different switches against which we tested sample QoS configurations, the Procurve 5412z (J8698A) and the Procurve 2920 (J9728A).

Note: ***If at all possible, ensure that user endpoint traffic is marked with proper DSCP markings before it ingresses network switches. This depends upon proper configuration of the WAN router/firewall device and the access endpoints.***

- Apply Appendix A to all Windows based PCs that run any of the soft-clients using either Group Policy or individual configuration to force proper marking of output traffic.
- Have your Account Manager go into RingCentral's "AI" account database and enable proper QoS marking for software clients and mobile clients.
- Have your SE apply custom code, again using the "AI" account database, to ensure that your hard phones are configured to use proper QoS/CoS markings.
- Ensure that the WAN router/firewall device is applying proper DSCP markings to traffic on the return path. (Upstream carriers frequently strip/alter DSCP markings. DSCP markings on traffic from the public Internet cannot be trusted.)

Please note that the following configurations are for example only. They have been tested only against certain models and release versions of HP/Aruba firmware. Some alterations may be required for certain models and firmware versions.

DSCP Tagging Values

The following are the generally accepted DSCP values used to tag network traffic by RingCentral. Note that while RingCentral uses the generally accepted value of AF31 (26) to mark SIP control traffic, Cisco utilizes the value of CS3 (24). This example prioritizes both DSCP marking values to allow for co-existence.

Value	Name	Purpose
46	EF	Voice Real-Time Traffic
34	AF41	Video Real-Time Traffic
26	AF31	SIP Signaling Traffic (RingCentral)
24	CS3	SIP Signaling Traffic (Cisco)
18	AF21	All other RingCentral Traffic
0	BE	Default Best Effort Marking

HP/Aruba Interface Egress Queues

The HP/Aruba switches may be established with from 1 to 8 interface egress queues. This setting is switch-wide in scope. We utilize 8 queues to provide maximum flexibility and granularity of control.

```
CELAB-HP-ASW01(config)# qos queue-config ?
 2-queues              Set the number of egress queues for each port.
 4-queues              Set the number of egress queues for each port.
 8-queues              Set the number of egress queues for each port.
CELAB-HP-ASW01(config)# qos queue-config 8-queues
```

```
!!!!! Reboot of switch !!!!!

CELAB-HP-ASW01(config)# show qos queue-config

 Egress Queue Configuration

  Number of Queues : 8

          802.1p
  Queue   Priorities
  -----   ----------
    1     1
    2     2
    3     0
    4     3
    5     4
    6     5
    7     6
    8     7
```

Traffic is placed in an egress queue based upon its 802.1p CoS tag value. Queue numbers start with one while 802.1p CoS tag values start with zero. The following table details 802.1p ➔ Queue Number assignments.

802.1p CoS Value	Queue Assignments		
	8 Queue	4 Queue	2 Queue
0	3	2	1
1	1	1	1
2	2	1	1
3	4	2	1
4	5	3	2
5	6	3	2
6	7	4	2
7	8	4	2

Configuration

Mapping Ingress Packets to Specific CoS / Egress Queue

The dscp-map table is used as packets ingress the switch interfaces to alter the 802.1p CoS packet tag based upon the packet's ingress DSCP value. The 802.1p CoS tag is then used to control traffic shaping by directing the packet to a specific egress queue. We want to make *sure* that only those packets which are of interest to us are prioritized. All other packets will be marked as default with priority 0 and mapped to the default traffic queue (queue 3).

You may make alterations to this scheme to add-in support for any existing or planned QoS scheme.

```
qos dscp-map 0 priority 0 name cs0
qos dscp-map 1 priority 0
qos dscp-map 2 priority 0
qos dscp-map 3 priority 0
qos dscp-map 4 priority 0
qos dscp-map 5 priority 0
qos dscp-map 6 priority 0
```

```
qos dscp-map 7 priority 0
qos dscp-map 8 priority 0 name cs1
qos dscp-map 9 priority 0
qos dscp-map 10 priority 0 name af11
qos dscp-map 11 priority 0
qos dscp-map 12 priority 0 name af12
qos dscp-map 13 priority 0
qos dscp-map 14 priority 0 name af13
qos dscp-map 15 priority 0
qos dscp-map 16 priority 0 name cs2
qos dscp-map 17 priority 0
qos dscp-map 18 priority 2 name af21
qos dscp-map 19 priority 0
qos dscp-map 20 priority 0 name af22
qos dscp-map 21 priority 0
qos dscp-map 22 priority 0 name af23
qos dscp-map 23 priority 0
qos dscp-map 24 priority 3 name cs3
qos dscp-map 25 priority 0
qos dscp-map 26 priority 3 name af31
qos dscp-map 27 priority 0
qos dscp-map 28 priority 0 name af32
qos dscp-map 29 priority 0
qos dscp-map 30 priority 0 name af33
qos dscp-map 31 priority 0
qos dscp-map 32 priority 0 name cs4
qos dscp-map 33 priority 0
qos dscp-map 34 priority 4 name af41
qos dscp-map 35 priority 0
qos dscp-map 36 priority 0 name af42
qos dscp-map 37 priority 0
qos dscp-map 38 priority 0 name af43
qos dscp-map 39 priority 0
qos dscp-map 40 priority 0 name cs5
qos dscp-map 41 priority 0
qos dscp-map 42 priority 0
qos dscp-map 43 priority 0
qos dscp-map 44 priority 0
qos dscp-map 45 priority 0
qos dscp-map 46 priority 5 name ef
qos dscp-map 47 priority 0
qos dscp-map 48 priority 6 name cs6
qos dscp-map 49 priority 0
qos dscp-map 50 priority 0
qos dscp-map 51 priority 0
qos dscp-map 52 priority 0
qos dscp-map 53 priority 0
qos dscp-map 54 priority 0
qos dscp-map 55 priority 0
qos dscp-map 56 priority 7 name cs7
qos dscp-map 57 priority 0
qos dscp-map 58 priority 0
qos dscp-map 59 priority 0
qos dscp-map 60 priority 0
qos dscp-map 61 priority 0
qos dscp-map 62 priority 0
qos dscp-map 63 priority 0
```

We must now enable DSCP QoS so that the dscp-map will take effect.

```
qos type-of-service diff-services
```

Now we must assign minimum bandwidth percentages for each of the 8 queues on a per port basis. We are using the following values for trunks and access ports in our example code. Please note that any unused bandwidth is automatically reallocated to other queues – no available bandwidth is wasted.

Queue Number	Trunk Link	Access Link	Traffic Type
1	1%	1%	unassigned in this example
2	5%	2%	RingCentral Traffic not otherwise classified
3	20%	50%	Default Traffic to the world
4	5%	5%	RingCentral SIP Signaling traffic
5	30%	10%	RingCentral Video Real-Time traffic
6	30%	10%	RingCentral Audio Real-Time traffic
7	5%	1%	Reserved for Routing Protocols
8	4%	1%	Reserved for Network Control

```
interface B1
   name "Trunk1"
   bandwidth-min output 1 5 20 5 30 30 5 4
   exit
interface B2
   name "Trunk2"
   bandwidth-min output 1 5 20 5 30 30 5 4
   exit
interface C1
   name "19JA21 Desk"
   bandwidth-min output 1 2 50 5 10 10 1 1
   exit
interface C2
   name "19JA22 Desk"
   bandwidth-min output 1 2 50 5 10 10 1 1
   exit
```

Marking Ingress Traffic If Needed

The following configuration elements, Classes and QoS Policies, may be used to alter the DSCP marking when proper marking upstream is not available. You may selectively apply QoS Policies to only those ports that need them, thus reducing switch processing overhead.

First, we must define 'classes' which are used to match categories of traffic.

```
class ipv4 "CL-RC-E2R-VoiceRTP"
 01 remark "RingCentral Voice – Endpoint to RingCentral"
 05 match udp any 66.81.240.0/20 range 20000 64999
 10 match udp any 80.81.128.0/20 range 20000 64999
 20 match udp any 103.44.68.0/22 range 20000 64999
 30 match udp any 104.245.56.0/21 range 20000 64999
 40 match udp any 185.23.248.0/22 range 20000 64999
 50 match udp any 192.209.24.0/21 range 20000 64999
 60 match udp any 199.68.212.0/22 range 20000 64999
 70 match udp any 199.255.120.0/22 range 20000 64999
 80 match udp any 208.87.40.0/22 range 20000 64999
 85 match udp any 66.81.240.0/20 eq 8803
 90 match udp any 80.81.128.0/20 eq 8803
 100 match udp any 103.44.68.0/22 eq 8803
 110 match udp any 104.245.56.0/21 eq 8803
 120 match udp any 185.23.248.0/22 eq 8803
 130 match udp any 192.209.24.0/21 eq 8803
 140 match udp any 199.68.212.0/22 eq 8803
```

```
 150 match udp any 199.255.120.0/22 eq 8803
 160 match udp any 208.87.40.0/22 eq 8803
 exit

class ipv4 "CL-RC-R2E-VoiceRTP"
 01 remark "RingCentral Voice – RingCentral to Endpoint"
 05 match udp 66.81.240.0/20 range 20000 64999 any
 10 match udp 80.81.128.0/20 range 20000 64999 any
 20 match udp 103.44.68.0/22 range 20000 64999 any
 30 match udp 104.245.56.0/21 range 20000 64999 any
 40 match udp 185.23.248.0/22 range 20000 64999 any
 50 match udp 192.209.24.0/21 range 20000 64999 any
 60 match udp 199.68.212.0/22 range 20000 64999 any
 70 match udp 199.255.120.0/22 range 20000 64999 any
 80 match udp 208.87.40.0/22 range 20000 64999 any
 85 match udp 66.81.240.0/20 eq 8803 any
 90 match udp 80.81.128.0/20 eq 8803 any
 100 match udp 103.44.68.0/22 eq 8803 any
 110 match udp 104.245.56.0/21 eq 8803 any
 120 match udp 185.23.248.0/22 eq 8803 any
 130 match udp 192.209.24.0/21 eq 8803 any
 140 match udp 199.68.212.0/22 eq 8803 any
 150 match udp 199.255.120.0/22 eq 8803 any
 160 match udp 208.87.40.0/22 eq 8803 any
 exit

class ipv4 "CL-RC-E2R-SIP"
 01 remark "RingCentral SIP – Endpoint to RingCentral"
 05 match udp any 66.81.240.0/20 range 5090 5099
 10 match udp any 80.81.128.0/20 range 5090 5099
 20 match udp any 103.44.68.0/22 range 5090 5099
 30 match udp any 104.245.56.0/21 range 5090 5099
 40 match udp any 185.23.248.0/22 range 5090 5099
 50 match udp any 192.209.24.0/21 range 5090 5099
 60 match udp any 199.68.212.0/22 range 5090 5099
 70 match udp any 199.255.120.0/22 range 5090 5099
 80 match udp any 208.87.40.0/22 range 5090 5099
 85 match tcp any 66.81.240.0/20 range 5090 5099
 90 match tcp any 80.81.128.0/20 range 5090 5099
 100 match tcp any 103.44.68.0/22 range 5090 5099
 110 match tcp any 104.245.56.0/21 range 5090 5099
 120 match tcp any 185.23.248.0/22 range 5090 5099
 130 match tcp any 192.209.24.0/21 range 5090 5099
 140 match tcp any 199.68.212.0/22 range 5090 5099
 150 match tcp any 199.255.120.0/22 range 5090 5099
 160 match tcp any 208.87.40.0/22 range 5090 5099
 165 match tcp any 66.81.240.0/20 range 8083 8090
 170 match tcp any 80.81.128.0/20 range 8083 8090
 180 match tcp any 103.44.68.0/22 range 8083 8090
 190 match tcp any 104.245.56.0/21 range 8083 8090
 200 match tcp any 185.23.248.0/22 range 8083 8090
 210 match tcp any 192.209.24.0/21 range 8083 8090
 220 match tcp any 199.68.212.0/22 range 8083 8090
 230 match tcp any 199.255.120.0/22 range 8083 8090
 240 match tcp any 208.87.40.0/22 range 8083 8090
 250 match tcp any 66.81.240.0/20 range 5060 5061
 260 match tcp any 80.81.128.0/20 range 5060 5061
 270 match tcp any 103.44.68.0/22 range 5060 5061
 280 match tcp any 104.245.56.0/21 range 5060 5061
 290 match tcp any 185.23.248.0/22 range 5060 5061
 300 match tcp any 192.209.24.0/21 range 5060 5061
 310 match tcp any 199.68.212.0/22 range 5060 5061
 320 match tcp any 199.255.120.0/22 range 5060 5061
 330 match tcp any 208.87.40.0/22 range 5060 5061
 340 match udp any 66.81.240.0/20 eq 5060
 350 match udp any 80.81.128.0/20 eq 5060
 360 match udp any 103.44.68.0/22 eq 5060
```

```
 370 match udp any 104.245.56.0/21 eq 5060
 380 match udp any 185.23.248.0/22 eq 5060
 390 match udp any 192.209.24.0/21 eq 5060
 400 match udp any 199.68.212.0/22 eq 5060
 410 match udp any 199.255.120.0/22 eq 5060
 420 match udp any 208.87.40.0/22 eq 5060
exit

class ipv4 "CL-RC-R2E-SIP"
 01 remark "RingCentral SIP – RingCentral to Endpoint"
 05 match udp 66.81.240.0/20 range 5090 5099 any
 10 match udp 80.81.128.0/20 range 5090 5099 any
 20 match udp 103.44.68.0/22 range 5090 5099 any
 30 match udp 104.245.56.0/21 range 5090 5099 any
 40 match udp 185.23.248.0/22 range 5090 5099 any
 50 match udp 192.209.24.0/21 range 5090 5099 any
 60 match udp 199.68.212.0/22 range 5090 5099 any
 70 match udp 199.255.120.0/22 range 5090 5099 any
 80 match udp 208.87.40.0/22 range 5090 5099 any
 85 match tcp 66.81.240.0/20 range 5090 5099 any
 90 match tcp 80.81.128.0/20 range 5090 5099 any
 100 match tcp 103.44.68.0/22 range 5090 5099 any
 110 match tcp 104.245.56.0/21 range 5090 5099 any
 120 match tcp 185.23.248.0/22 range 5090 5099 any
 130 match tcp 192.209.24.0/21 range 5090 5099 any
 140 match tcp 199.68.212.0/22 range 5090 5099 any
 150 match tcp 199.255.120.0/22 range 5090 5099 any
 160 match tcp 208.87.40.0/22 range 5090 5099 any
 165 match tcp 66.81.240.0/20 range 8083 8090 any
 170 match tcp 80.81.128.0/20 range 8083 8090 any
 180 match tcp 103.44.68.0/22 range 8083 8090 any
 190 match tcp 104.245.56.0/21 range 8083 8090 any
 200 match tcp 185.23.248.0/22 range 8083 8090 any
 210 match tcp 192.209.24.0/21 range 8083 8090 any
 220 match tcp 199.68.212.0/22 range 8083 8090 any
 230 match tcp 199.255.120.0/22 range 8083 8090 any
 240 match tcp 208.87.40.0/22 range 8083 8090 any
 250 match tcp 66.81.240.0/20 range 5060 5061 any
 260 match tcp 80.81.128.0/20 range 5060 5061 any
 270 match tcp 103.44.68.0/22 range 5060 5061 any
 280 match tcp 104.245.56.0/21 range 5060 5061 any
 290 match tcp 185.23.248.0/22 range 5060 5061 any
 300 match tcp 192.209.24.0/21 range 5060 5061 any
 310 match tcp 199.68.212.0/22 range 5060 5061 any
 320 match tcp 199.255.120.0/22 range 5060 5061 any
 330 match tcp 208.87.40.0/22 range 5060 5061 any
 340 match udp 66.81.240.0/20 eq 5060 any
 350 match udp 80.81.128.0/20 eq 5060 any
 360 match udp 103.44.68.0/22 eq 5060 any
 370 match udp 104.245.56.0/21 eq 5060 any
 380 match udp 185.23.248.0/22 eq 5060 any
 390 match udp 192.209.24.0/21 eq 5060 any
 400 match udp 199.68.212.0/22 eq 5060 any
 410 match udp 199.255.120.0/22 eq 5060 any
 420 match udp 208.87.40.0/22 eq 5060 any
exit

class ipv4 "CL-RC-E2R-Video"
 01 remark "RingCentral Video – Endpoint to RingCentral"
 05 match tcp any 66.81.240.0/20 range 8801 8802
 10 match tcp any 80.81.128.0/20 range 8801 8802
 20 match tcp any 103.44.68.0/22 range 8801 8802
 30 match tcp any 104.245.56.0/21 range 8801 8802
 40 match tcp any 185.23.248.0/22 range 8801 8802
 50 match tcp any 192.209.24.0/21 range 8801 8802
 60 match tcp any 199.68.212.0/22 range 8801 8802
 70 match tcp any 199.255.120.0/22 range 8801 8802
```

```
 80 match tcp any 208.87.40.0/22 range 8801 8802
 85 match udp any 66.81.240.0/20 range 8801 8802
 90 match udp any 80.81.128.0/20 range 8801 8802
 100 match udp any 103.44.68.0/22 range 8801 8802
 110 match udp any 104.245.56.0/21 range 8801 8802
 120 match udp any 185.23.248.0/22 range 8801 8802
 130 match udp any 192.209.24.0/21 range 8801 8802
 140 match udp any 199.68.212.0/22 range 8801 8802
 150 match udp any 199.255.120.0/22 range 8801 8802
 160 match udp any 208.87.40.0/22 range 8801 8802
 245 match udp any 66.81.240.0/20 range 10000 19999
 250 match udp any 80.81.128.0/20 range 10000 19999
 260 match udp any 103.44.68.0/22 range 10000 19999
 270 match udp any 104.245.56.0/21 range 10000 19999
 280 match udp any 185.23.248.0/22 range 10000 19999
 290 match udp any 192.209.24.0/21 range 10000 19999
 300 match udp any 199.68.212.0/22 range 10000 19999
 310 match udp any 199.255.120.0/22 range 10000 19999
 320 match udp any 208.87.40.0/22 range 10000 19999
 exit

class ipv4 "CL-RC-R2E-Video"
 01 remark "RingCentral Video – RingCentral to Endpoint"
 05 match tcp 66.81.240.0/20 range 8801 8802 any
 10 match tcp 80.81.128.0/20 range 8801 8802 any
 20 match tcp 103.44.68.0/22 range 8801 8802 any
 30 match tcp 104.245.56.0/21 range 8801 8802 any
 40 match tcp 185.23.248.0/22 range 8801 8802 any
 50 match tcp 192.209.24.0/21 range 8801 8802 any
 60 match tcp 199.68.212.0/22 range 8801 8802 any
 70 match tcp 199.255.120.0/22 range 8801 8802 any
 80 match tcp 208.87.40.0/22 range 8801 8802 any
 85 match udp 66.81.240.0/20 range 8801 8802 any
 90 match udp 80.81.128.0/20 range 8801 8802 any
 100 match udp 103.44.68.0/22 range 8801 8802 any
 110 match udp 104.245.56.0/21 range 8801 8802 any
 120 match udp 185.23.248.0/22 range 8801 8802 any
 130 match udp 192.209.24.0/21 range 8801 8802 any
 140 match udp 199.68.212.0/22 range 8801 8802 any
 150 match udp 199.255.120.0/22 range 8801 8802 any
 160 match udp 208.87.40.0/22 range 8801 8802 any
 245 match udp 66.81.240.0/20 range 10000 19999 any
 250 match udp 80.81.128.0/20 range 10000 19999 any
 260 match udp 103.44.68.0/22 range 10000 19999 any
 270 match udp 104.245.56.0/21 range 10000 19999 any
 280 match udp 185.23.248.0/22 range 10000 19999 any
 290 match udp 192.209.24.0/21 range 10000 19999 any
 300 match udp 199.68.212.0/22 range 10000 19999 any
 310 match udp 199.255.120.0/22 range 10000 19999 any
 320 match udp 208.87.40.0/22 range 10000 19999 any
 exit

class ipv4 "CL-RC-E2R-All"
 01 remark "RingCentral Other – Endpoint to RingCentral"
 05 match ip any 66.81.240.0/20
 10 match ip any 80.81.128.0/20
 20 match ip any 103.44.68.0/22
 30 match ip any 104.245.56.0/21
 40 match ip any 185.23.248.0/22
 50 match ip any 192.209.24.0/21
 60 match ip any 199.68.212.0/22
 70 match ip any 199.255.120.0/22
 80 match ip any 208.87.40.0/22
 exit

class ipv4 "CL-RC-R2E-All"
 01 remark "RingCentral Other – RingCentral to Endpoint"
```

```
 05 match ip 66.81.240.0/20 any
 10 match ip 80.81.128.0/20 any
 20 match ip 103.44.68.0/22 any
 30 match ip 104.245.56.0/21 any
 40 match ip 185.23.248.0/22 any
 50 match ip 192.209.24.0/21 any
 60 match ip 199.68.212.0/22 any
 70 match ip 199.255.120.0/22 any
 80 match ip 208.87.40.0/22 any
 exit
```

Next, we create QoS Policies based upon these classes. These QoS Policies may be applied to ports to properly classify ingressing traffic. Note that these policies are ONLY required if the traffic is NOT properly marked with DSCP values.

Policy QP-RC-E2R can be used on trunk links, access point links, and other trusted connections. It does not perform any rate policing actions.

```
policy qos "QP-RC-E2R"
     10 class ipv4 "CL-RC-E2R-VoiceRTP" action dscp ef action priority 5
     20 class ipv4 "CL-RC-E2R-Video" action dscp af41 action priority 4
     30 class ipv4 "CL-RC-E2R-SIP" action dscp af31 action priority 3
     40 class ipv4 "CL-RC-E2R-All" action dscp af21 action priority 2
   default-class action dscp default action priority 0
   exit
```

Policy QP-RC-E2R-User can be used on an access port to which a single user connects. It is identical to QP-RC-E2R but includes rate policing limits which prevent a runaway machine from destroying your network with high priority traffic. Note that the value of 512kbps for Voice RTP is required to support a single phone that initiates phone mediated 3-way conference calling. This was determined empirically.

```
policy qos "QP-RC-E2R-User"
      10 class ipv4 "CL-RC-E2R-VoiceRTP" action dscp ef action priority 5 action rate-limit kbps 512
      20 class ipv4 "CL-RC-E2R-Video" action dscp af41 action priority 4 action rate-limit kbps 750
      30 class ipv4 "CL-RC-E2R-SIP" action dscp af31 action priority 3 action rate-limit kbps 32
      40 class ipv4 "CL-RC-E2R-All" action dscp af21 action priority 2
    default-class action dscp default action priority 0
    exit
```

Policy QP-RC-R2E can be used on WAN links where the WAN router/firewall cannot properly restore the DSCP markings on return traffic.

```
policy qos "QP-RC-R2E"
     10 class ipv4 "CL-RC-R2E-VoiceRTP" action dscp ef action priority 5
     20 class ipv4 "CL-RC-R2E-Video" action dscp af41 action priority 4
     30 class ipv4 "CL-RC-R2E-SIP" action dscp af31 action priority 3
     40 class ipv4 "CL-RC-R2E-All" action dscp af21 action priority 2
   default-class action dscp default action priority 0
   exit
```

Finally, we apply these QoS Policies to ports where needed to classify ingressing traffic. Note that these policies are ONLY required if the traffic is NOT properly marked with DSCP values.

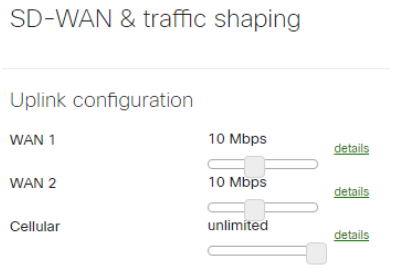
```
interface B1
   name "Trunk1"
   service-policy QP-RC-E2R in
   exit
interface B2
   name "Trunk2"
   service-policy QP-RC-E2R in
```

```
   exit
interface C1
   name "19JA21 Desk"
   service-policy QP-RC-E2R-User in
   exit
interface C2
   name "19JA22 Desk"
   service-policy QP-RC-E2R-User in
   exit
interface C3
   name "WAN IN"
   service-policy QP-RC-R2E in
   exit
```

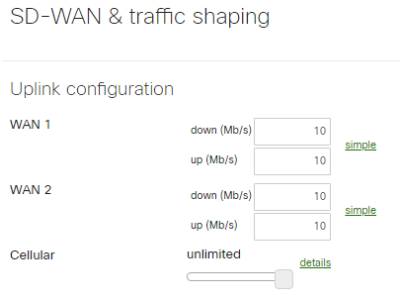
Appendix K –Meraki Devices

Set WAN Speeds

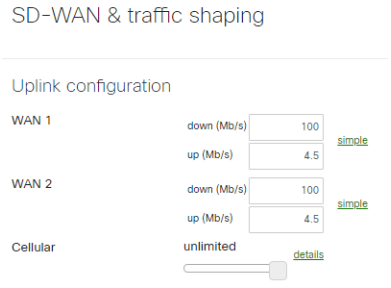
Log into your Meraki management portal account. Select 'Security & SD-WAN/SD-WAN & traffic shaping' from the left side menu bar. You will see the following screen:



Click on the words 'details' to allow textual entry of separate up and down speeds for the active WAN circuits:



Enter the correct values and click on Save Changes.



Now add traffic shaping rules (select bandwidth limit to suit your environment):

Set '**Default Rules**' to a value of 'Disable default traffic shaping rules', then add the following explicit traffic shaping rules:

Rule 1: (Real-time Audio)

Definition:

```
net/port 66.81.240.0/20:20000-64999
net/port 80.81.128.0/20:20000-64999
```

```
net/port 103.44.68.0/22:20000-64999
net/port 104.245.56.0/21:20000-64999
net/port 185.23.248.0/22:20000-64999
net/port 192.209.24.0/21:20000-64999
net/port 199.255.120.0/22:20000-64999
net/port 199.68.212.0/22:20000-64999
net/port 208.87.40.0/22:20000-64999

net/port 66.81.240.0/20:8803
net/port 80.81.128.0/20:8803
net/port 103.44.68.0/22:8803
net/port 104.245.56.0/21:8803
net/port 185.23.248.0/22:8803
net/port 192.209.24.0/21:8803
net/port 199.255.120.0/22:8803
net/port 199.68.212.0/22:8803
net/port 208.87.40.0/22:8803
```

Bandwidth limit: Ignore network per-client limit (unlimited)
Priority: High
DSCP Tagging: 46 (EF – Expedited Forwarding)

Rule 2: (Real-time Video)

Definition:

```
net/port 66.81.240.0/20:10000-19999
net/port 80.81.128.0/20:10000-19999
net/port 103.44.68.0/22:10000-19999
net/port 104.245.56.0/21:10000-19999
net/port 185.23.248.0/22:10000-19999
net/port 192.209.24.0/21:10000-19999
net/port 199.255.120.0/22:10000-19999
net/port 199.68.212.0/22:10000-19999
net/port 208.87.40.0/22:10000-19999

net/port 66.81.240.0/20:8801-8802
net/port 80.81.128.0/20:8801-8802
net/port 103.44.68.0/22:8801-8802
net/port 104.245.56.0/21:8801-8802
net/port 185.23.248.0/22:8801-8802
net/port 192.209.24.0/21:8801-8802
net/port 199.255.120.0/22:8801-8802
net/port 199.68.212.0/22:8801-8802
net/port 208.87.40.0/22:8801-8802
```

Bandwidth limit: Ignore network per-client limit (unlimited)
Priority: Normal
DSCP Tagging: 34 (AF41 – Multimedia Conferencing, Low Drop)

Rule 3: (Signaling)

Definition:

```
net/port 66.81.240.0/20:5090-5099
net/port 80.81.128.0/20:5090-5099
net/port 103.44.68.0/22:5090-5099
net/port 104.245.56.0/21:5090-5099
net/port 185.23.248.0/22:5090-5099
net/port 192.209.24.0/21:5090-5099
net/port 199.255.120.0/22:5090-5099
net/port 199.68.212.0/22:5090-5099
net/port 208.87.40.0/22:5090-5099
```

```
net/port 66.81.240.0/20:8083-8090
net/port 80.81.128.0/20:8083-8090
net/port 103.44.68.0/22:8083-8090
net/port 104.245.56.0/21:8083-8090
net/port 185.23.248.0/22:8083-8090
net/port 192.209.24.0/21:8083-8090
net/port 199.255.120.0/22:8083-8090
net/port 199.68.212.0/22:8083-8090
net/port 208.87.40.0/22:5060-5061
net/port 66.81.240.0/20:5060-5061
net/port 80.81.128.0/20:5060-5061
net/port 103.44.68.0/22:5060-5061
net/port 104.245.56.0/21:5060-5061
net/port 185.23.248.0/22:5060-5061
net/port 192.209.24.0/21:5060-5061
net/port 199.255.120.0/22:5060-5061
net/port 199.68.212.0/22:5060-5061
net/port 208.87.40.0/22:5060-5061
```

Bandwidth limit: Ignore network per-client limit (unlimited)
Priority: Normal
DSCP Tagging: 26 (AF31 – Multimedia Streaming, Low Drop)

Rule 4: (Other, RingCentral)

Definition:

```
net 66.81.240.0/20
net 80.81.128.0/20
net 103.44.68.0/22
net 104.245.56.0/21
net 185.23.248.0/22
net 192.209.24.0/21
net 199.255.120.0/22
net 199.68.212.0/22
net 208.87.40.0/22
```

Bandwidth limit: Ignore network per-client limit (unlimited)
Priority: Low
DSCP Tagging: 18 (AF21 – Low latency data, Low Drop)

Rule 5: (Other, non-RingCentral)

Definition:

```
net 0.0.0.0/0
```

Bandwidth limit: Ignore network per-client limit (unlimited)
Priority: Low
DSCP Tagging: 0 (BE – Best Effort)

Group Policies for MR Devices

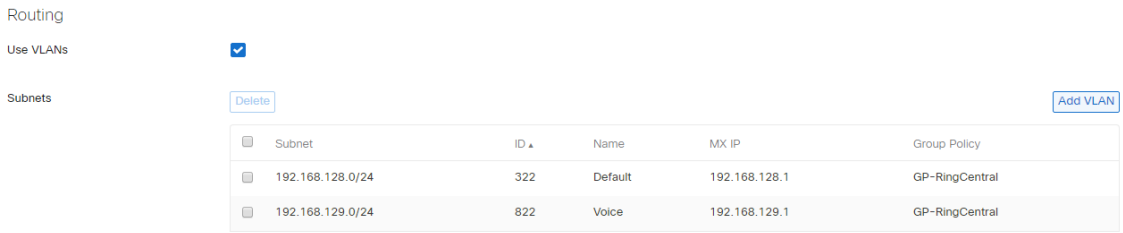
Select 'Network-wide/Group policies' from the left side menu bar. Click on 'Add a group'. Set the name to 'GP-RingCentral' and change the 'Firewall and traffic shaping' pulldown to read 'Custom network firewall & shaping rules'. Add the following new shaping rules:

1. PCP/DSCP Tagging = 4 / 34. Definitions:
    a. 8801-8802 (ports only)
    b. 66.81.240.0/20:10000-19999
    c. 80.81.128.0/20:10000-19999

        d. 103.44.68.0/22:10000-19999
        e. 104.245.56.0/21:10000-19999
        f. 185.23.248.0/22:10000-19999
        g. 192.209.24.0/21:10000-19999
        h. 199.68.212.0/22:10000-19999
        i. 199.255.120.0/22:10000-19999
        j. 208.87.40.0/22:10000-19999
        k. 6182
    2. PCP/DSCP Tagging = 3 / 26. Definitions:
        a. 8083-8090
        b. 5090-5099
        c. 5060-5061
    3. PCP/DSCP Tagging = 7 / 46. Definitions:
        a. 66.81.240.0/20:20000-64999
        b. 80.81.128.0/20:20000-64999
        c. 103.44.68.0/22:20000-64999
        d. 104.245.56.0/21:20000-64999
        e. 185.23.248.0/22:20000-64999
        f. 192.209.24.0/21:20000-64999
        g. 199.68.212.0/22:20000-64999
        h. 199.255.120.0/22:20000-64999
        i. 208.87.40.0/22:20000-64999
        j. 8803 (port only)
    4. PCP/DSCP Tagging = 2 / 18. Definitions:
        a. 66.81.240.0/20
        b. 80.81.128.0/20
        c. 103.44.68.0/22
        d. 104.245.56.0/21
        e. 185.23.248.0/22
        f. 192.209.24.0/21
        g. 199.68.212.0/22
        h. 199.255.120.0/22
        i. 208.87.40.0/22

Save the Group policy.

Select 'Security & SD-WAN/Addressing & VLANs' from the left side menu bar. Go to the Routing section and set **all** of your LAN subnets to use the Group policy GP-RingCentral as shown below:



Switches

Select 'Switch/Switch Settings' from the left side menu bar. Set up the following values in the Quality of Service section and then click on Save Changes.

VLAN	Protocol	Source port	Destination port	Action	Value
ANY	TCP	ANY	8801-8802	Set DSCP to	34 (AF41)
ANY	UDP	ANY	8801-8802	Set DSCP to	34 (AF41)
ANY	UDP	ANY	10000-19999	Set DSCP to	34 (AF41)
ANY	TCP	ANY	5090-5099	Set DSCP to	26 (AF31)

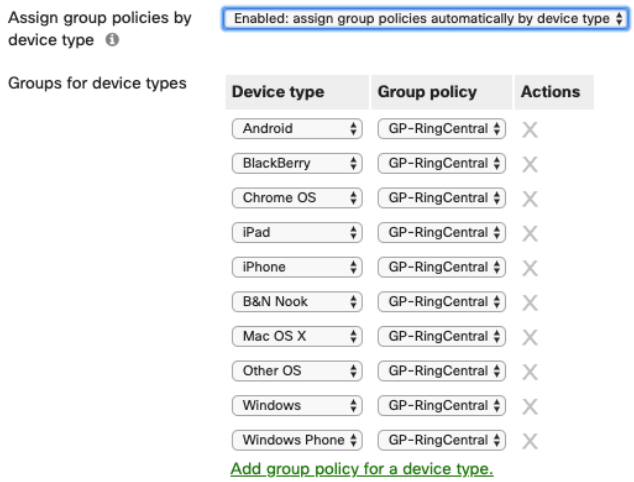
ANY	TCP	ANY	5060-5061	Set DSCP to	26 (AF31)
ANY	UDP	ANY	5090-5099	Set DSCP to	26 (AF31)
ANY	UDP	ANY	5060	Set DSCP to	26 (AF31)
ANY	TCP	ANY	8083-8090	Set DSCP to	26 (AF31)
ANY	UDP	ANY	20000-64999	Set DSCP to	46 (EF voice)
ANY	UDP	ANY	8803	Set DSCP to	46 (EF voice)

Wireless

Select 'Wireless/Firewall & traffic shaping'. Make sure the settings for 'Shape traffic' and 'Default Rules' match what is shown below:



Select 'Wireless/Access control'. For best roaming performance it is suggested that you set '802.11r' to a value of 'Adaptive'. The bottom of the page deals with group policies and should be set as follows:



Appendix M – Mikrotik Devices

Mikrotik Routers Overview

Mikrotik was founded in 1996 to develop router software and wireless ISP systems. It is headquartered in Riga, Latvia. Mikrotik began developing and selling hardware devices optimized for their software in 2002.

Devices based on Mikrotik Router-OS are filled with many advanced features and are quite inexpensive. They are frequently found in educational settings and in many foreign countries.

Connection/Packet Classification

The first task you should undertake is to classify all connections and mark all resulting packets. This is done in the ip/firewall/mangle subsystem. As each new connection starts, we apply a mark to that connection that will be associated with that connection until it terminates or times out. We utilize 4 connection marks for RingCentral traffic. This connection mark is used to process every RingCentral packet that flows through the router. Each packet is given a packet mark (PM-QoS1 thru PM-QoS4) based upon the connection mark. The DSCP value and the 802.11p CoS value are also set. If you are not using Vlans, the 802.11p CoS value setting is ignored.

The packet mark is used by a Hierarchical Token Bucket (HBT) queueing system to ensure that voice traffic has priority and to shape the output data stream to conform with the contracted data rate.

Destination Addresses

Media and signaling traffic to/from RingCentral are based upon a set of known public IPv4 address blocks. Separate address-lists (prefix-lists) are created for the two traffic categories.

Paste the following code into a terminal session:

```
###############################################################################
#
# Create an address list that contains all RingCentral owned Address Space
#
/ip firewall address-list
add address=66.81.240.0/20 list=PFX-RC-All
add address=80.81.128.0/20 list=PFX-RC-All
add address=103.44.68.0/22 list=PFX-RC-All
add address=104.245.56.0/21 list=PFX-RC-All
add address=185.23.248.0/22 list=PFX-RC-All
add address=192.209.24.0/21 list=PFX-RC-All
add address=199.255.120.0/22 list=PFX-RC-All
add address=199.68.212.0/22 list=PFX-RC-All
add address=208.87.40.0/22 list=PFX-RC-All
#
```

Mangle Filter Ruleset

The 'mangle' ruleset is used to examine every packet that traverses the device and classify/mark it appropriately. This ruleset takes no action other than classification/marking.

The first group of rules must be created at the top of the IP/FIREWALL/MANGLE chain. The location of the other rules is of no concern so long as they are in the order as given. No matter what other MANGLE

rules you may need, you must keep these first RC and ENG rules at the top of the chain. These rules will look at every packet and process it if it is going to or coming from RingCentral. If they represent a new connection, it will be categorized (visible as connection mark in the ip/firewall/connections screen). Once the connection session is marked, every packet that belongs to that connection will have the DSCP value and 802.1p CoS value set appropriately and a packet-mark attached to it.

Paste the following code into a terminal session:

```
/ip firewall mangle
#
# Create MANGLE rules.  The first 3 rules defined MUST be at the top of the ruleset.
#
# Create a 'dummy' static rule with a known comment value (one which is complete
# nonsensical garbage) that insures there is at least one static rule so that the
# find clause will work properly!!  It will be deleted after inserting our rules.
#
add chain=prerouting action=passthrough comment="DFLHD38947qpoinc marker" disabled=yes
#
#-- Support for normal RingCentral products.  This is comprised of Rules 0, 1, and 2.
# Rule #2
add chain=prerouting action=jump \
    comment="Check all traffic coming FROM RC address space." \
    jump-target=MGL-FromRC src-address-list=PFX-RC-All \
    place-before=([find where dynamic=no]->0)
# Rule #1
add chain=prerouting action=jump comment=\
    "Check all traffic going TO RingCentral address space." dst-address-list=PFX-RC-All \
    jump-target=MGL-ToRC place-before=([find where dynamic=no]->0)
# Rule #0
add chain=prerouting action=passthrough disabled=yes comment=\
    "===> Process traffic to/from RingCentral apps <===" \
    place-before=([find where dynamic=no]->0)
#
# Remove the dummy rule as it is no longer needed.
remove [find comment="DFLHD38947qpoinc marker"]
#
#== ============================================================================
#
#-- The remainder of the rules are not position dependent and may be simply appended
#-- to the bottom of the ruleset.
#
#== ============================================================================
#-- Subroutines to process traffic going TO RingCentral.
```

```
#
#-- If this is a NEW connection you must classify it and set up a connection-mark
#-- so that subsequent packets can be handled properly.  It should only need to be
#-- classified once.  Note that the MGL-NewToRC subroutine must return so that the
#-- remaining code can be executed to take the action required based upon the selected
#-- classification.
#
add chain=MGL-ToRC action=jump comment="If NEW connection classify it." \
    connection-state=new jump-target=MGL-NewToRC passthrough=yes
#
#-- Once classified, the connection-mark is used to control packet marking.
#
#-- Apply packet marks as appropriate for connections marked as QoS class 1
add chain=MGL-ToRC action=jump comment="Process QoS1" connection-mark=CMK-QoS-1 \
    jump-target=MGL-SetQoS1
#-- Apply packet marks as appropriate for connections marked as QoS class 2
add chain=MGL-ToRC action=jump comment="Process QoS2" connection-mark=CMK-QoS-2 \
    jump-target=MGL-SetQoS2
#-- Apply packet marks as appropriate for connections marked as QoS class 3
add chain=MGL-ToRC action=jump comment="Process QoS3" connection-mark=CMK-QoS-3 \
    jump-target=MGL-SetQoS3
#-- Apply packet marks as appropriate for connections marked as QoS class 4
add chain=MGL-ToRC action=jump comment="Process QoS4" connection-mark=CMK-QoS-4 \
    jump-target=MGL-SetQoS4
#
#-- Any traffic without connection marks simply falls off the end and is processed
#-- as Best Effort traffic.
#
#== ============================================================================
#-- Subroutines to process traffic coming FROM RingCentral.
#
#-- All connections are initiated by the user, so there will be no classification
#-- required on the FROM RC direction.  Classification of the session will have
#-- already occurred.
#
#-- Apply packet marks as appropriate for connections marked as QoS class 1
add chain=MGL-FromRC action=jump comment="Process QoS1" connection-mark=CMK-QoS-1 \
    jump-target=MGL-SetQoS1
#-- Apply packet marks as appropriate for connections marked as QoS class 2
add chain=MGL-FromRC action=jump comment="Process QoS2" connection-mark=CMK-QoS-2 \
    jump-target=MGL-SetQoS2
#-- Apply packet marks as appropriate for connections marked as QoS class 3
add chain=MGL-FromRC action=jump comment="Process QoS3" connection-mark=CMK-QoS-3 \
    jump-target=MGL-SetQoS3
#-- Apply packet marks as appropriate for connections marked as QoS class 4
add chain=MGL-FromRC action=jump comment="Process QoS4" connection-mark=CMK-QoS-4 \
    jump-target=MGL-SetQoS4
#
#-- Any traffic without connection marks simply falls off the end and is processed
#-- as Best Effort traffic.
#
#== ============================================================================
#-- Subroutines to classify new connections going to RingCentral.  Note that any packet
#-- reaching this point is guaranteed to be bound for the RingCentral public address
#-- space.  There is no non-RingCentral traffic reaching this point.
#
#-- QoS class 1 – audio real-time traffic
add chain=MGL-NewToRC action=jump comment="Mark RTP traffic" jump-target=MGL-MarkQoS1 \
    dst-port=20000-64999,8803 protocol=udp
add chain=MGL-NewToRC action=return connection-mark=!no-mark
#
#-- QoS class 2 – video real-time traffic
add chain=MGL-NewToRC action=jump comment="Mark Video RT" jump-target=MGL-MarkQoS2 \
    port=8801-8802,10000-19999 protocol=udp
add chain=MGL-NewToRC action=return connection-mark=!no-mark
add chain=MGL-NewToRC action=jump comment="Mark Video RT" jump-target=MGL-MarkQoS2 \
    port=8801-8802 protocol=tcp
```

```
add chain=MGL-NewToRC action=return connection-mark=!no-mark
#
#-- QoS class 3 – signaling traffic
add chain=MGL-NewToRC action=jump comment="Mark SIP control traffic (tcp)" \
    dst-port=5090-5099,8083-8090,5060-5061 jump-target=MGL-MarkQoS3 protocol=tcp
add chain=MGL-NewToRC action=return connection-mark=!no-mark
add chain=MGL-NewToRC action=jump comment="Mark SIP control traffic (udp)" \
    jump-target=MGL-MarkQoS3 dst-port=5090-5099,5060 protocol=udp
add chain=MGL-NewToRC action=return connection-mark=!no-mark
#
#-- QoS class 4 – all other traffic to/from RC
add chain=MGL-NewToRC action=jump comment="Default to QoS4" jump-target=MGL-MarkQoS4
add chain=MGL-NewToRC action=return
#
#== ============================================================================
#-- Subroutines to apply connection-marks to new connections.  The RETURN is required
#-- so that the newly classified connection can continue to be processed in the parent
#-- routine!
#
#-- Apply connection mark for QoS class 1
add chain=MGL-MarkQoS1 action=passthrough comment="Mark Connection as EF (QoS-1)"
add chain=MGL-MarkQoS1 action=mark-connection new-connection-mark=CMK-QoS-1 \
    passthrough=yes
add chain=MGL-MarkQoS1 action=return
#
#-- Apply connection mark for QoS class 2
add action=passthrough chain=MGL-MarkQoS2 comment="Mark Connection as AF41 (QoS-2)"
add action=mark-connection chain=MGL-MarkQoS2 new-connection-mark=CMK-QoS-2 \
    passthrough=yes
add chain=MGL-MarkQoS2 action=return
#
#-- Apply connection mark for QoS class 3
add action=passthrough chain=MGL-MarkQoS3 comment="Mark Connection as AF31 (QoS-3)"
add action=mark-connection chain=MGL-MarkQoS3 new-connection-mark=CMK-QoS-3 \
    passthrough=yes
add chain=MGL-MarkQoS3 action=return
#
#-- Apply connection mark for QoS class 4
add action=passthrough chain=MGL-MarkQoS4 comment="Mark Connection as AF21 (QoS-4)"
add action=mark-connection chain=MGL-MarkQoS4 new-connection-mark=CMK-QoS-4 \
    passthrough=yes
add chain=MGL-MarkQoS4 action=return
#
#== ============================================================================
#-- Subroutines to physically mark packet flows.
#
#-- Apply DSCP, CoS, and packet mark for QoS class 1 (DSCP EF, CoS 5)
add action=change-dscp chain=MGL-SetQoS1 comment="Set QoS1's packets DSCP to EF" \
    new-dscp=46 passthrough=yes
add action=set-priority chain=MGL-SetQoS1 new-priority=5 passthrough=yes
add action=mark-packet chain=MGL-SetQoS1 new-packet-mark=PM-QoS1 passthrough=no
#
#-- Apply DSCP, CoS, and packet mark for QoS class 2 (DSCP AF41, CoS 4)
add action=change-dscp chain=MGL-SetQoS2 comment="Set QoS2's packets DSCP to AF41" \
    new-dscp=34 passthrough=yes
add action=set-priority chain=MGL-SetQoS2 new-priority=4 passthrough=yes
add action=mark-packet chain=MGL-SetQoS2 new-packet-mark=PM-QoS2 passthrough=no
#
#-- Apply DSCP, CoS, and packet mark for QoS class 3 (DSCP AF31, CoS 3)
add action=change-dscp chain=MGL-SetQoS3 comment="Set QoS3's packets DSCP to AF31" \
    new-dscp=26 passthrough=yes
add action=set-priority chain=MGL-SetQoS3 new-priority=3 passthrough=yes
add action=mark-packet chain=MGL-SetQoS3 new-packet-mark=PM-QoS3 passthrough=no
#
#-- Apply DSCP, CoS, and packet mark for QoS class 4 (DSCP AF21, CoS 2)
add action=change-dscp chain=MGL-SetQoS4 comment="Set QoS4's packets DSCP to AF21" \
    new-dscp=18 passthrough=yes
```

```
add action=set-priority chain=MGL-SetQoS4 new-priority=2 passthrough=yes
add action=mark-packet chain=MGL-SetQoS4 new-packet-mark=PM-QoS4 passthrough=no
#
```

Now that the packets are marked, you must set up the queuing and traffic shaping so that voice has priority over other traffic.

Queuing (Hierarchical Token Bucket) and Traffic Shaping Setup

Mikrotik Router OS uses the Hierarchical Token Bucket system to perform traffic shaping and queueing. You must establish traffic shaping values for each WAN port based upon a speed of approximately 95% of the contracted data rate. If you do not determine the outbound bandwidth correctly you will not obtain good QoS.

The code in the Mangle firewall rules apply a marking value to each packet traveling to/from RingCentral address space. This mark will classify the packet as being in one of four QoS classes or it will be unclassified if it is not RingCentral traffic. You must determine the amount of bandwidth guaranteed for each of the QoS classes and how much it will be allowed to additionally use if available. QoS Class 1 (Audio Real-Time) **must have the maximum and guaranteed bandwidth values equal**. This must be done for EACH WAN link. It is most convenient to express the numbers in Kbps.

	WAN Link Example	**WAN Link 1**	**WAN Link 2**	**WAN Link 3**
Interface Name	Outside			
Contracted/measured data rate	5000 Kbps			
Usage Factor	95%			
Usable data rate	4750 Kbps			
Guaranteed bandwidth	**(Each Value must be less than the corresponding Maximum value.)**			
-- QoS Class 1 (audio)	800 Kbps			
-- QoS Class 2 (video)	1000 Kbps			
-- QoS Class 3 (signaling)	100 Kbps			
-- QoS Class 4 (RC Other)	500 Kbps			
-- QoS RC Total	2400 Kbps			
Maximum bandwidth				
-- QoS Class 1 (audio)	800 Kbps			
-- QoS Class 2 (video)	2000 Kbps			
-- QoS Class 3 (signaling)	100 Kbps			
-- QoS Class 4 (RC Other)	1000 Kbps			
-- QoS RC Total	3900 Kbps			
REMEMBER TO LEAVE SOME BANDWIDTH FOR NON-RC TRAFFIC. Also remember that any unused bandwidth will be apportioned to all other Classes, up to the Maximum bandwidth setting and to the unclassified traffic.				

Paste the following code into a terminal session:

```
#
# Repeat this section for each WAN link, substituting the correct values.
#
# The yellow highlight indicates the WAN link interface name.
#
# The first queue tree in this example is for the WAN link on port br301.
#
/queue tree
add comment="Outbound to WAN1 vlan" limit-at=4750K max-limit=4750K name=Outbound-WAN1 \
    parent=Outside queue=ethernet-default
add limit-at=800K max-limit=800K name=OB-WAN-QoS1 packet-mark=PM-QoS1 \
    parent=Outbound-WAN priority=1 queue=ethernet-default
add limit-at=1000K max-limit=2000K name=OB-WAN-QoS2 packet-mark=PM-QoS2 \
    parent=Outbound-WAN priority=2 queue=ethernet-default
add limit-at=200k max-limit=200k name=OB-WAN-QoS3 packet-mark=PM-QoS3 \
    parent=Outbound-WAN priority=3 queue=ethernet-default
add limit-at=250k max-limit=3000k name=OB-WAN-QoS4 packet-mark=PM-QoS4 \
    parent=Outbound-WAN priority=4 queue=ethernet-default
add limit-at=500k max-limit=5000k name=OB-WAN-default packet-mark=no-mark \
    parent=Outbound-WAN queue=ethernet-default
#
# This section assumes full wire speed on the LAN port, so only the priority is needed.
#
add comment="Outbound to LAN vlan" name=Outbound-LAN parent=Lan queue=ethernet-default
add name=OB-LAN-QoS1 packet-mark=PM-QoS1 parent=Outbound-LAN priority=1 \
    queue=ethernet-default
add name=OB-LAN-QoS2 packet-mark=PM-QoS2 parent=Outbound-LAN priority=2 \
    queue=ethernet-default
add name=OB-LAN-QoS3 packet-mark=PM-QoS3 parent=Outbound-LAN priority=3 \
    queue=ethernet-default
add name=OB-LAN-QoS4 packet-mark=PM-QoS4 parent=Outbound-LAN priority=4 \
    queue=ethernet-default
add name=OB-LAN-default packet-mark=no-mark parent=Outbound-LAN queue=ethernet-default
```

Please note that the yellow and cyan highlighted values must be changed to meet your setup. In my lab environment 'Lan' is a bridge that contains the LAN VLAN interface. *(Always create bridge devices to which you can refer rather than use physical devices. That way if you must change the physical device you only have the change it in the bridge port member section rather than all through the configuration.)* Change the value to match your environment. Likewise, 'Outside' is a bridge that contains the WAN VLAN interface.

The values highlighted in cyan are used to adjust traffic shaping. The values for limit-at and max-limit in rule 'Outbound-WAN' should be set to a value that is approximately 95% of your contracted upstream bandwidth. This sets the upper bound of bandwidth available for any of the subsidiary elements to use. The value of 'limit-at' should be considered as the *guaranteed* bandwidth available to an element. The value of 'max-limit' is the amount of bandwidth an element ***may*** grow to consume if no other element needs it. The value of 'limit-at' MUST be less than or equal to the value of 'max-limit'. The values shown are used for a lab cable circuit with 5.5mbps allowed upstream.

In this example the following shaping parameters are applied:

QoS Mark	DSCP	Comment	Guaranteed Bandwidth	Maximum Bandwidth
QoS1	EF (46)	Real-Time Voice Traffic	1mbps	1mbps
QoS2	AF41 (34)	Real-Time Video Traffic	2mbps	4mbps

QoS3	AF31 (26)	Signaling and Control (SIP)	200kbps	200kbps
QoS4	AF21 (18)	All other RingCentral traffic (GLIP,Prov,etc)	250kbps	3Mbps
none	no change	All other traffic	500kbps	5Mbps

You should allow for 100kbps per simultaneous phone call and the values for 'max-limit' should be equal to those for 'limit-at' for QoS Class 1. The total of all guaranteed bandwidth numbers must be less than or equal to the value given on the parent element.

Other

You must disable the SIP Application Layer Gateway. Paste the following code into a terminal session:

```
/ip firewall service-port
set sip disabled=yes
```

Appendix S – SonicWall Firewalls

For the purposes of this document, we are assuming you have a 'virgin' SonicWall unit running firmware load 6.5.4.5-53n, using interface X0 as the LAN interface, and using interface X1 as a single WAN interface connected to a 100Mbps statically addressed ISP link. SSH must be enabled on the X0(LAN) interface. This simple configuration will provide for clients connected to the X0(LAN) interface to obtain addresses via DHCP and apply S-NAT/PAT to their outbound traffic over the X1(WAN) interface so that clients on the X0(LAN) interface can freely browse the Internet and connect to RingCentral.

Setting up a 'Virgin' SonicWall Unit

Connect a pc to the X0(LAN) interface, address the PC interface to 192.168.168.167 with a netmask of 255.255.255.0, power up the Sonicwall unit, then use a web browser to connect to https://192.168.168.168. Launch the Setup Guide in manual mode.

The screen should come up in MANAGE | Appliance | Base Settings. Set firewall name, domain name, and the password for the admin account. To implement better security, you should scroll down to Web Management and set the HTTPS port number to something other than 443. You will need to use this port number for all web connections in the future. In this example I will use port 8443. Likewise, scroll further down to SSH Management Settings and change the SSH Port number to a value other than 22. In this example I will use port 8022. Click on ACCEPT at the bottom of the screen. You will have to reconnect to the SonicWall unit using the new port number in the URL as https://192.168.168.168:8443. You will have to login using the new password.

Next navigate to MANAGE | System Setup | Network | Interfaces.

I normally remove the defaulted PortShield definitions as they are easily forgotten and cause issues. The lab unit, a 250, has interfaces X3 and X4 bridged via PortShield to port X0(LAN) as part of the factory default. Click SHOW PORTSHIELD INTERFACES. For each interface that is part of the PortShield group, click on the Configure icon and change the Zone to unassigned. This should automatically change the Mode to unassigned as well. Click on ACCEPT at the bottom of the screen.

Click on the configure icon for the X1(WAN) interface. Set the correct values and click on OK.

Click on the configure icon for the X0(LAN) interface. Change the device address and netmask to the desired values. Leave the gateway address all zeros. Check the box for SSH management. Click on OK at the bottom of the screen. Change your PC interface to DHCP client mode. The system will attempt link you to the new address, but it may take longer than the system allows to make the address changes. You may need to wait a minute or so and force a reconnection to the new address. Remember to use the new https management port number as part of the URL!!!! Note that you may need to 'preempt' the administrator as your old session may not have timed out yet.

Further non-RingCentral customization actions, such as adding administrators, setting up VPNs, adding DMZs, etc are left to you as they are highly site specific and should be done after completing the rest of this document.

RingCentral QoS Setup

Follow these directions to enable proper RingCentral QoS setup on your SonicWall unit.

Enable Bandwidth Management and Configure Uplink Port Speeds

Enable Bandwidth Management in the Global mode and establish guaranteed and maximum allocation bandwidth for each priority queue.

Queue	Description
0	Realtime – This is for transport of the actual voice. It has ultimate priority. The maximum value should be equal to the guaranteed value. The value required will vary based upon the type of endpoints and your usage patterns. Consult with your RingCentral Solutions Engineer to determine the correct value. Err on the high side as any unused bandwidth will be reallocated to the other queues. This queue is guaranteed 30% of the WAN bandwidth in this example configuration.
1	Highest (Video) – This is for Video-Conference traffic. You may set the maximum value slightly higher than the guaranteed value, but we recommend no more than 10-15% higher. Consult with your RingCentral Solutions Engineer to determine the correct value. Err on the high side as any unused bandwidth will be reallocated to the other queues. This queue is guaranteed 40% of the WAN bandwidth in this example configuration.
2	High (SIP) – This is for the signaling/control traffic. Five percent (5%) is usually a good number for this class for both guaranteed and minimum. This queue is guaranteed 5% of the WAN bandwidth in this example configuration.
3	Medium-High – All other traffic to/from RingCentral owned addresses get put in this queue. This is low volume. This queue is guaranteed 5% of the WAN bandwidth in this example configuration.
4	Medium – Default for all other traffic. This queue is guaranteed 20% of the WAN bandwidth in this example configuration.

SSH to the SonicWall (remember to use the ssh port number you set) and enter configuration mode.

```
configure
(You may be asked to preempt your web session here… if so, answer yes)
bandwidth-management
  type global
  priority realtime guaranteed 30 maximum 30
  priority highest guaranteed 40 maximum 60
  priority high guaranteed 5 maximum 10
  priority medium-high guaranteed 5 maximum 100
  priority medium guaranteed 20 maximum 100
  priority medium-low guaranteed 0 maximum 100
  priority low guaranteed 0 maximum 100
  priority lowest guaranteed 0 maximum 100
  exit
commit
```

We must enable bandwidth management on the egress (outbound) side of the WAN interface. The speed of the UPLINK side of your WAN connection should be multiplied by 0.95 (95%), converted to Kbps, then used in the following script. Adjust interface names as needed based upon your firewall

model. Note that I am enabling 802.1p by default. It does nothing if you are not using Vlans on the interface, but it will be there and enabled if you do decide to use vlans.

SSH to the SonicWall (remember to use the ssh port number you set) and enter configuration mode.

```
configure
(You may be asked to preempt your web session here… if so, answer yes)
interface X0
  cos-8021p
  no bandwidth-management egress
  no bandwidth-management ingress
  comment "LAN port – no bandwidth limit"
  exit
interface X1
  cos-8021p
  bandwidth-management egress 95000.0
  no bandwidth-management ingress
  comment "WAN interface – 100MBps x .095 = 95Mbps = 95000Kbps bandwidth limit"
  exit
interface X2
  cos-8021p
  no bandwidth-management egress
  no bandwidth-management ingress
  exit
interface X3
  cos-8021p
  no bandwidth-management egress
  no bandwidth-management ingress
  exit
interface X4
  cos-8021p
  no bandwidth-management egress
  no bandwidth-management ingress
  exit
commit
```

Configure QoS DSCP/802.1p Mapping

Set up CoS / DSCP mapping to proper values.

SSH to the SonicWall (remember to use the ssh port number you set) and enter configuration mode.

```
configure
(You may be asked to preempt your web session here… if so, answer yes)
qos-mapping cos 2 to-dscp 18 from-dscp 16 23
qos-mapping cos 3 to-dscp 26 from-dscp 24 31
qos-mapping cos 4 to-dscp 34 from-dscp 32 39
qos-mapping cos 5 to-dscp 46 from-dscp 40 47
commit
```

Configure Special Phone Options

These options should always be configured . Traffic to/from an invalid/closed/discarded TCP session should result in a notification being returned to the originator so that a new session can be immediately initiated rather than waiting for a session timeout – potentially many minutes. Additionally, ***RTSP Transformations*** should be disabled.

SSH to the SonicWall (remember to use the ssh port number you set) and enter configuration mode.

```
configure
(You may be asked to preempt your web session here… if so, answer yes)
firewall
  no rtsp-transformations
  issue-rst-for-outgoing-discards
  exit
commit
```

Configure RingCentral Addresses and Address Group

These addresses, address groups, services, and service groups are used to simplify the creation of access rules (policies) in the next section.

SSH to the SonicWall (remember to use the ssh port number you set) and enter configuration mode.

```
configure
(You may be asked to preempt your web session here… if so, answer yes)
address-object ipv4 ADR-RC-1
    zone WAN
    network 80.81.128.0 255.255.240.0
    exit
address-object ipv4 ADR-RC-2
    zone WAN
    network 103.44.68.0 255.255.252.0
    exit
address-object ipv4 ADR-RC-3
    zone WAN
    network 104.245.56.0 255.255.248.0
    exit
address-object ipv4 ADR-RC-4
    zone WAN
    network 185.23.248.0 255.255.252.0
    exit
address-object ipv4 ADR-RC-5
    zone WAN
    network 192.209.24.0 255.255.248.0
    exit
address-object ipv4 ADR-RC-6
    zone WAN
    network 199.255.120.0 255.255.252.0
    exit
address-object ipv4 ADR-RC-7
    zone WAN
    network 199.68.212.0 255.255.252.0
    exit
address-object ipv4 ADR-RC-8
    zone WAN
    network 208.87.40.0 255.255.252.0
```

```
    exit
address-object ipv4 ADR-RC-9
    zone WAN
    network 66.81.240.0 255.255.240.0
    exit
address-object ipv4 ADR-RC-Prov-1
    zone WAN
    host 104.245.57.85
    exit
address-object ipv4 ADR-RC-Prov-2
    zone WAN
    host 104.245.57.60
    exit
address-object ipv4 ADR-RC-Prov-3
    zone WAN
    host 104.245.57.61
    exit
address-object ipv4 ADR-RC-Prov-4
    zone WAN
    host 199.255.120.237
    exit
address-object ipv4 ADR-RC-Prov-5
    zone WAN
    host 199.255.120.239
    exit
address-object ipv4 ADR-RC-Prov-6
    zone WAN
    host 199.255.120.234
    exit
address-object fqdn ADR-RC-Pres-1
    zone WAN
    domain *.pubnub.com
    no dns-ttl
    exit
address-object fqdn ADR-RC-Pres-2
    zone WAN
    domain *.pubnub.net
    no dns-ttl
    exit
address-object fqdn ADR-RC-Pres-3
    zone WAN
    domain *.pndsn.com
    no dns-ttl
    exit
commit

address-group ipv4 AG-RC-ALL
    address-object ipv4 ADR-RC-9
    address-object ipv4 ADR-RC-8
    address-object ipv4 ADR-RC-7
    address-object ipv4 ADR-RC-6
    address-object ipv4 ADR-RC-5
    address-object ipv4 ADR-RC-4
    address-object ipv4 ADR-RC-3
    address-object ipv4 ADR-RC-2
    address-object ipv4 ADR-RC-1
    exit
address-group ipv4 AG-RC-Provisioning
    address-object ipv4 ADR-RC-Prov-6
    address-object ipv4 ADR-RC-Prov-5
    address-object ipv4 ADR-RC-Prov-4
```

```
    address-object ipv4 ADR-RC-Prov-3
    address-object ipv4 ADR-RC-Prov-2
    address-object ipv4 ADR-RC-Prov-1
    exit
address-group ipv4 AG-RC-Pres
    address-object fqdn ADR-RC-Pres-3
    address-object fqdn ADR-RC-Pres-2
    address-object fqdn ADR-RC-Pres-1
    exit
commit

service-object SVC-RC-Video-1 UDP 8801 8802
service-object SVC-RC-Video-2 UDP 10000 19999
service-object SVC-RC-Video-3 TCP 8801 8802
service-object SVC-RC-VoiceMedia-1 UDP 20000 64999
service-object SVC-RC-VoiceMedia-2 UDP 8803 8803
service-object SVC-RC-SIP-TCP-1 TCP 5090 5099
service-object SVC-RC-SIP-TCP-2 TCP 8083 8090
service-object SVC-RC-SIP-TCP-3 TCP 5060 5061
service-object SVC-RC-SIP-UDP-1 UDP 5090 5090
service-object SVC-RC-SIP-UDP-2 UDP 5060 5060
service-object SVC-RC-Directory-1 TCP 636 636
service-object SVC-RC-Directory-2 TCP 3269 3269
service-object SVC-RC-Presence-1 TCP 6182 6182
commit

service-group SG-RC-Voice-RT
    service-object SVC-RC-VoiceMedia-1
    service-object SVC-RC-VoiceMedia-2
    exit
service-group SG-RC-Video-RT
    service-object SVC-RC-Video-3
    service-object SVC-RC-Video-2
    service-object SVC-RC-Video-1
    exit
service-group SG-RC-Video-PTP
    service-object SVC-RC-Meeting-PTP-1
    exit
service-group SG-RC-Signaling
    service-object SVC-RC-SIP-TCP-3
    service-object SVC-RC-SIP-TCP-2
    service-object SVC-RC-SIP-TCP-1
    service-object SVC-RC-SIP-UDP-2
    service-object SVC-RC-SIP-UDP-1
    exit
service-group SG-RC-Directory
    service-object SVC-RC-Directory-2
    service-object SVC-RC-Directory-1
    exit
service-group SG-RC-Presence
    service-object SVC-RC-Presence-1
    exit
commit
```

Configure Access / QoS Rules

Access rules (policies) are responsible for categorizing traffic and assigning it to a traffic queue for transmission out the WAN interface.

You must create all these policies for each inter-zone traffic flow. Normally this will be LAN ➔ WAN. If you are using other zones that must talk to RingCentral, such as DMZ ➔ WAN, you should duplicate this section for each 'from' zone. The TO zone will always be WAN unless you are doing strange, advanced configurations.

SSH to the SonicWall (remember to use the ssh port number you set) and enter configuration mode.

```
configure
(You may be asked to preempt your web session here… if so, answer yes)

access-rule from LAN to WAN action allow service group SG-RC-Voice-RT
destination address group AG-RC-ALL
    name POL-RC-Voice-RT
    logging
    max-connections 100
    priority manual 1
    no dpi
    quality-of-service dscp explicit 46
    quality-of-service class-of-service explicit video
    bandwidth-management
        egress priority realtime
        no ingress
        exit
    exit

access-rule from LAN to WAN action allow service group SG-RC-Video-RT
destination address group AG-RC-ALL
    name POL-RC-Video-RT
    logging
    priority manual 3
    no dpi
    quality-of-service dscp explicit 34
    quality-of-service class-of-service explicit controlled-load
    bandwidth-management
        egress priority highest
        no ingress
        exit
    exit

access-rule from LAN to WAN action allow service group SG-RC-Video-PTP
    name POL-RC-Video-PTP
    logging
    priority manual 4
    no dpi
    quality-of-service dscp explicit 34
    quality-of-service class-of-service explicit controlled-load
    bandwidth-management
        egress priority highest
        no ingress
        exit
    exit

access-rule from LAN to WAN action allow service group SG-RC-Signaling
destination address group AG-RC-ALL
    name POL-RC-Signaling
    logging
    priority manual 5
    no dpi
    quality-of-service dscp explicit 26
```

```
        quality-of-service class-of-service explicit excellent-effort
        bandwidth-management
            egress priority high
            no ingress
            exit
        exit

    access-rule from LAN to WAN action allow service name HTTPS destination address
    group AG-RC-Provisioning
        name POL-RC-Provisioning
        logging
        priority manual 7
        no dpi
        quality-of-service dscp explicit 18
        quality-of-service class-of-service explicit spare
        bandwidth-management
            egress priority medium-high
            no ingress
            exit
        exit

    access-rule from LAN to WAN action allow service group SG-RC-Directory
        name POL-RC-Directory
        logging
        priority manual 8
        dpi
        quality-of-service dscp explicit 18
        quality-of-service class-of-service explicit spare
        bandwidth-management
            egress priority medium-high
            no ingress
            exit
        exit

    access-rule from LAN to WAN action allow service group SG-RC-Presence
        name POL-RC-Presence
        logging
        priority manual 9
        dpi
        quality-of-service dscp explicit 18
        quality-of-service class-of-service explicit spare
        bandwidth-management
            egress priority medium-high
            no ingress
            exit
        exit

    access-rule from LAN to WAN action allow destination address group AG-RC-ALL
        name POL-RC-Other
        logging
        priority manual 10
        dpi
        quality-of-service dscp explicit 18
        quality-of-service class-of-service explicit spare
        bandwidth-management
            egress priority medium-high
            no ingress
            exit
        exit

    commit
```

Appendix U – Ubiquiti EdgeMax Switches

Ubiquiti switches (EdgeMax Series) have severe hardware limitations that prevent using them to classify RingCentral traffic. Provided the traffic has already been tagged with proper DSCP markings, these switches can ensure that RingCentral traffic receives a guaranteed portion of bandwidth to prevent loss of critical traffic.

The switch has 8 hardware queues, used as shown in the chart shown below. Queues 3 – 6 have been set with a guaranteed minimum percent of outbound bandwidth and applied globally to all ports.

Queue Number	Use	Guaranteed B/W Portion (%)
7	Switch Internal Use Only (Stack)	
6	Real-time voice traffic (DSCP 46 - EF)	30
5	Real-time video traffic (DSCP 34 – AF41)	30
4	Signaling and Control (DSCP 26 – AF31)	5
3	RingCentral other traffic (DSCP 18 – AF21) Also by default, DSCP 48 - 63	10
2	By default, DSCP 32 – 33, 35 – 45, and 47	
1	By default, DSCP 0 – 7 24 – 25, 27 - 31	
0	By default, DSCP 8 – 17, and 19 – 23	

Use SSH to log into the switch, enter *enable* mode, then enter the following:

```
configure

class-map match-all CL-EF ipv4
 match ip dscp 46
 exit

class-map match-all CL-AF41 ipv4
 match ip dscp 34
 exit

class-map match-all CL-AF31 ipv4
 match ip dscp 26
 exit

class-map match-all CL-AF21 ipv4
 match ip dscp 18
 exit

class-map match-all CL-Default ipv4
 match any
 exit

policy-map PL-Inb-All in
 class CL-EF
  assign-queue 6
 exit

 class CL-AF41
  assign-queue 5
```

```
 exit

 class CL-AF31
  assign-queue 4
 exit

 class CL-AF21
  assign-queue 3
 exit

 class CL-Default
  assign-queue 1
 exit

exit

classofservice trust ip-dscp
classofservice ip-dscp-mapping 18 3
classofservice ip-dscp-mapping 26 4
classofservice ip-dscp-mapping 34 5
classofservice ip-dscp-mapping 46 6
cos-queue min-bandwidth 0 0 0 0 5 30 30 0
cos-queue strict 4 5 6

interface 0/1-48
 service-policy in PL-Inb-All
exit

end
```

Critical Notes:

All traffic must have DSCP markings properly assigned ***before*** the traffic reaches the switch.

Microsoft soft clients – Refer to Appendix A of this document.

Other soft clients and mobile clients – Special settings must be enabled by your account representative in a tool called Admin Web.

Polycom Hard Phones – The following custom code snippet must be applied account-wide to all Polycom phone models.

```
<PHONE_CONFIG>
<qos
qos.ethernet.callControl.user_priority="3"
qos.ethernet.other.user_priority="2"
qos.ethernet.rtp.user_priority="5"
qos.ethernet.rtp.video.user_priority="4"
qos.ethernet.tcpQosEnabled="1"
qos.ip.callControl.dscp="AF31"
qos.ip.rtp.dscp="EF"
qos.ip.rtp.video.dscp="AF41"
/>
</PHONE_CONFIG>
```

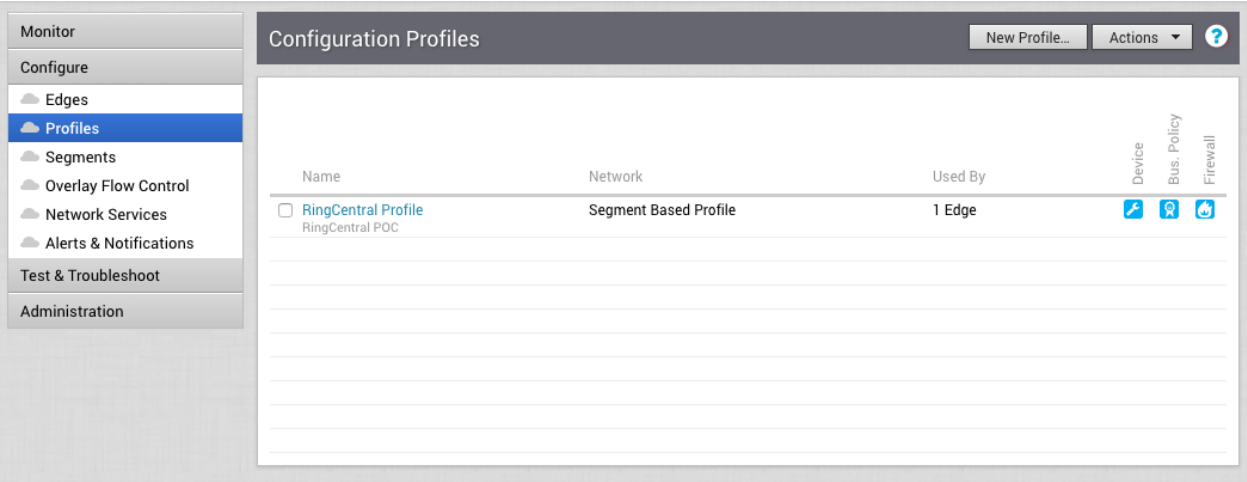
Other Hard Phones – Manual setup of QoS required based upon the following table

Traffic Type	IP DSCP Value	Ethernet CoS Value
Real-Time Voice (RTP)	EF (46)	5
Real-Time Video (RTP) [only if present]	AF41 (34)	4
Signaling / Control / SIP	AF31 (26)	3

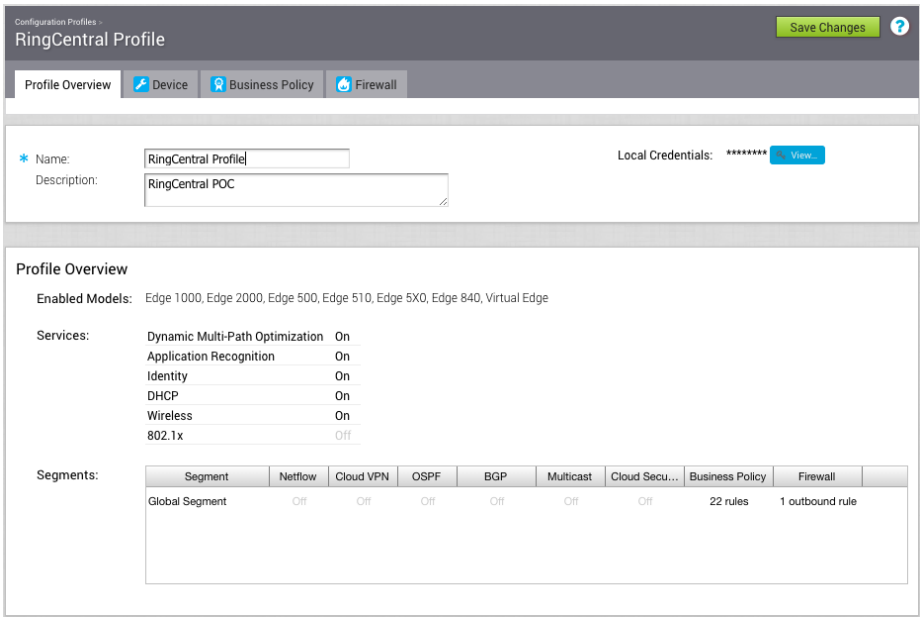
Appendix V –VeloCloud SD-WAN devices

The VeloCloud SD-WAN device implements SD-WAN based upon a central 'Orchestrator' that provides configuration information to all edge devices and gateway devices. It has a very extensive suite of QoS features and includes packet loss remediation using packet duplication. **It is important for bandwidth planning purposes to note that phone calls and video calls will require twice the normal bandwidth in both directions.**

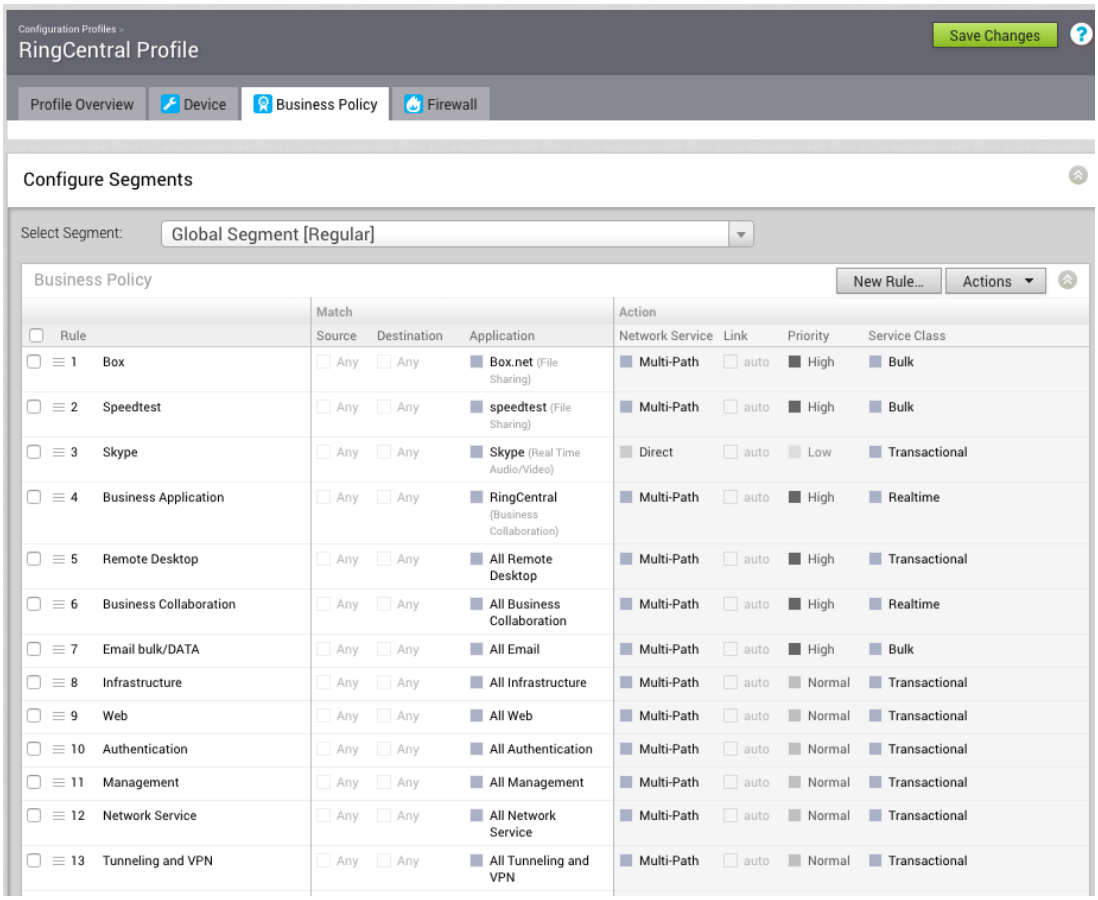
VeloCloud maintains an internal Internet service that has gateway devices in many large, well connected data centers around the globe. Customer VeloCloud edge devices should be set up to identify RingCentral traffic and route it through the VeloCloud gateways using packet loss remediation. This should be set up by logging into your account on the VeloCloud Orchestrator and navigating to Configure / Profiles.



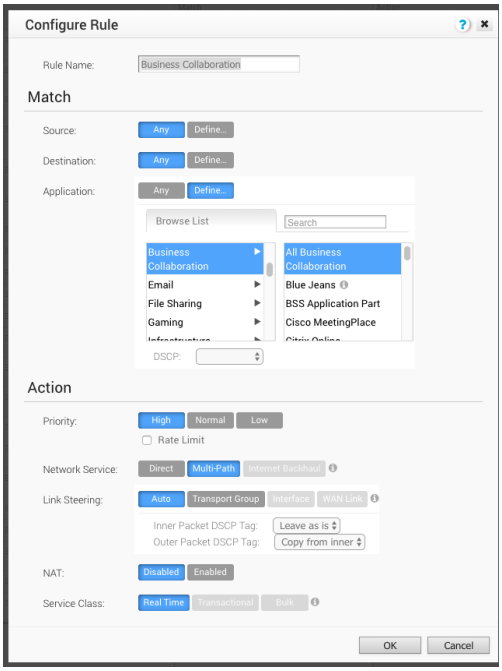
Click on the Profile Name.



Click on the Business Policy tab.



Click on 'Business Collaboration'.



Duplicate the settings in the Business Collaboration rule as shown above. Make sure that 'All Business Collaboration' is selected on the right-side listing. You should scroll down in the right-side listing to ensure that RingCentral is listed.

Click OK to save the rule.

Any VeloCloud edge device that is set to use this profile will now optimize RingCentral traffic and apply packet loss remediation to it. Lab tests show that this rule can compensate for up to 15% packet loss on both of dual circuits simultaneously and maintain toll grade voice quality.

The VeloCloud devices do not, by default, change the DSCP marking of any traffic. It is essential that full QoS marking be implemented on all other network devices to do so.

Appendix W –Watchguard Devices

This example configures a Watchguard Firebox T15 from scratch to support RingCentral including QoS and Traffic Shaping. The lab device was forced to do a factory default reset using the console cable.

Initial configuration

1. Use a browser to log into the device at ***https://10.0.1.1:8080*** using the admin account (default password is ***readwrite***).

2. Select ***Create a new configuration for your Firebox***, acknowledge the license agreement, and click on **NEXT.**

3. Configure your external interface as appropriate.

4. Configure your Trusted (internal) interface as appropriate. In this case we are leaving it set to the default values.

5. Set the passwords on the predefined accounts as desired.

6. If you want to be able to manage the device from an external address, configure that option and click **NEXT**.

7. Adjust the Contact settings as desired and click **NEXT**.

8. Set the Time Zone as desired and click **NEXT**.

9. Configure your subscription services and *WebBlocker* settings as desired.

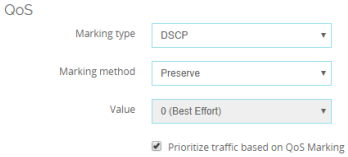
10. Log back in to the admin account and then reboot the device.

The device is now functional at a basic level.

RingCentral Follow-on Configuration

1. Log back in to the admin account and select ***FIREWALL → Traffic Management***. Check the box to Enable Traffic Management. Select the Interfaces tab, then select the table column for the External Interface. Set the bandwidth for 95% of the OUTBOUND (site toward Internet) Contracted data rate, which is usually less than or equal to the INBOUND (Internet toward site) data rate. Click on **SAVE**. *Please note that it is **CRITICAL** that this value be set correctly.*

2. Select ***NETWORK -> Interfaces***. Select the table entry for your External Interface and click **EDIT**. Select the Advanced tab. Under QoS select the following:



   Then click on **SAVE**.

3. Perform step 2 for each interface you plan to use. Once completed, all of your interfaces will be set up to honor DSCP QoS markings and pass them through transparently.

4. Select ***FIREWALL → Traffic Management***. Under Traffic Management Actions, click on ADD.

   The user must determine how much bandwidth to Guarantee and how much bandwidth is allowed for each category of RingCentral traffic.

   Create the following policies:

   Name: TMP-RingCentral-Voice-RTP
   Description: Real-Time Voice (80Kbps per concurrent call)
   Type: All Policies
   Maximum Bandwidth: 1024 Kbps (Adjust to fit need)
   Guaranteed Bandwidth: 1024 Kbps (Adjust to fit need)

   Name: TMP-RingCentral-Video-RTP
   Description: Real-Time Video
   Type: All Policies
   Maximum Bandwidth: 3076 Kbps (Adjust to fit need)
   Guaranteed Bandwidth: 1024 Kbps (Adjust to fit need)

   Name: TMP-RingCentral-Signal
   Description: Voice/Video Signaling
   Type: All Policies
   Maximum Bandwidth: 512 Kbps (Adjust to fit need)
   Guaranteed Bandwidth: 256 Kbps (Adjust to fit need)

   Name: TMP-RingCentral-Other
   Description: Other RingCentral Functions
   Type: All Policies
   Maximum Bandwidth: 2048 Kbps (Adjust to fit need)
   Guaranteed Bandwidth: 128 Kbps (Adjust to fit need)

5. Select ***FIREWALL → Aliases***. Click on ADD. Name the Alias '***AG-RingCentral***' and add the following Alias Members: (All are of member type '***Network IPv4***'.)

```
66.81.240.0 255.255.240.0    (/20)
80.81.128.0 255.255.240.0    (/20)
103.44.68.0 255.255.252.0    (/22)
104.245.56.0 255.255.248.0   (/21)
185.23.248.0 255.255.252.0   (/22)
192.209.24.0 255.255.248.0   (/21)
199.255.120.0 255.255.252.0  (/22)
199.68.212.0 255.255.252.0   (/22)
208.87.40.0 255.255.252.0    (/22)
```

   Click on **SAVE**.

6. Select ***FIREWALL→ Firewall Policies***. Click on **ADD POLICY**. Set policy type to Custom and click **ADD** to add a policy template. Set the name to PT-Voice-RTP. Enable the Specify custom idle timeout box and set the value to 300. Click the **ADD** button to add the following protocols:

   Type: Port Range
   Protocol: UDP
   Ports: 20000-64999

   Type: Single Port
   Protocol: UDP
   Ports: 8803-8803

   Click on **SAVE**, then click on **ADD POLICY**. On the following screen in the TO block, highlight the Any-External entry and click **REMOVE**, then click **ADD** to add alias AG-RingCentral to the box. Check the Specify Custom idle timeout box and set it to 300 seconds. Select the Traffic Management tab and set both Forward and Reverse Actions to '***TMP-RingCentral-Voice-RTP***'. Select the Advanced tab and under QoS check the Override per-interface settings box. Set Marking Type to DSCP, Marking method to Assign, Value to 46 (EF), Prioritize traffic based on Custom Value, Value 5. Click on **SAVE**.

7. Click on **ADD POLICY**. Set policy type to Custom and click **ADD** to add a policy template. Set the name to PT-RingCentral-Video-RTP. Enable the Specify custom idle timeout box and set the value to 300. Click the **ADD** button to add the following protocols:

   Type: Port Range
   Protocol: UDP
   Ports: 8801-8802

   Type: Port Range
   Protocol: TCP

Ports: 8801-8802

Type: Port Range
Protocol: UDP
Ports: 10000-19999

Click on **SAVE**, then click on **ADD POLICY**. On the following screen in the TO block, highlight the Any-External entry and click **REMOVE**, then click **ADD** to add alias AG-RingCentral to the box. Check the Specify Custom idle timeout box and set it to 300 seconds. Select the Traffic Management tab and set both Forward and Reverse Actions to 'TMP-RingCentral-Video-RTP'. Select the Advanced tab and under QoS check the Override per-interface settings box. Set Marking Type to DSCP, Marking method to Assign, Value to 34 (AF41), Prioritize traffic based on Custom Value, Value 4. Click on **SAVE**.

8. Click on **ADD POLICY**. Set policy type to Custom and click **ADD** to add a policy template. Set the name to PT-RingCentral-Signal. Enable the Specify custom idle timeout box and set the value to 300. Click the **ADD** button to add the following protocols:

   Type: Port Range
   Protocol: TCP
   Ports: 5090-5099

   Type: Port Range
   Protocol: UDP
   Ports: 5090-5099

   Type: Port Range
   Protocol: TCP
   Ports: 8083-8090

   Type: Port Range
   Protocol: TCP
   Ports: 5060-5061

   Type: Single Port
   Protocol: UDP
   Ports: 5060

   Click on **SAVE**, then click on **ADD POLICY**. On the following screen in the TO block, highlight the Any-External entry and click **REMOVE**, then click **ADD** to add alias AG-RingCentral to the box. Check the Specify Custom idle timeout box and set it to 300 seconds. Select the Traffic Management tab and set both Forward and Reverse Actions to 'TMP-RingCentral-Signal'. Select the Advanced tab and under QoS check the Override per-interface settings box. Set Marking

Type to DSCP, Marking method to Assign, Value to 26 (AF31), Prioritize traffic based on Custom Value, Value 3. Click on **SAVE**.

9. Click on **ADD POLICY**. Set policy type to Custom and click **ADD** to add a policy template. Set the name to PT-RingCentral-Other. Enable the Specify custom idle timeout box and set the value to 300. Click the **ADD** button to add the following protocols:

   Type: Single Port
   Protocol: Any

   Click on **SAVE**, then click on **ADD POLICY**. On the following screen in the TO block, highlight the Any-External entry and click **REMOVE**, then click **ADD** to add alias AG-RingCentral to the box. Check the Specify Custom idle timeout box and set it to 300 seconds. Select the Traffic Management tab and set both Forward and Reverse Actions to 'TMP-RingCentral-Other. Select the Advanced tab and under QoS check the Override per-interface settings box. Set Marking Type to DSCP, Marking method to Assign, Value to 18 (AF21), Prioritize traffic based on Custom Value, Value 2. Click on **SAVE**.

10. Select ***FIREWALL → Firewall Policies***. Click on **DISABLE POLICY AUTO-ORDER MODE** and answer YES. Drag the RingCentral Policies to the top. Policy numbers should be in this order:

    1 PT-RingCentral-Voice-RTP
    2 PT-RingCentral-Video-RTP
    3 PT-RingCentral-Signal
    4 PT-RingCentral-Other

    Click on **SAVE POLICY ORDER**.

Completed!! Save your work by backing up your configuration file.