



Avaya Solution & Interoperability Test Lab

Application Notes for Kentrox Q-1300 QoS Appliance connected to an Avaya IP Office - Issue 1.0

Abstract

These Application Notes describe the configuration of a Voice over IP (VoIP) solution using the Kentrox Q1300 QoS Appliance and Avaya IP Office to verify voice quality in a small office scenario. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a Voice over IP (VoIP) solution using Quality of Service (QoS) on the Kentrox Q1300 QoS Appliance connected to an Avaya IP Office to verify voice quality in a small office scenario. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

Compliance testing emphasis was placed on verifying voice quality in a small office scenario using low bandwidth serial T-1 links for the private IP WAN network. QoS based on Layer 3 Differentiated Services was implemented across the network to prioritize voice traffic over the WAN. Compliance testing included throughput, Direct Media and codec's G.711 and G.729.

Kentrox Q-Series Q1300 QoS Appliance

The Q1300 QoS Appliance combines the features of a QoS appliance and Ethernet switch into one easy-to use network access device. Graphical reporting also helps ensure that QoS is performing in the network.

The configuration in **Figure 1** shows a corporate site connected to a remote office site.

For the compliance testing the DHCP server function on Avaya IP Office was disabled and instead a centralized corporate DHCP server was put in place to handle both the corporate and remote sites. To better manage the different traffic types at each site, the voice and data traffic were separated onto different VLANs.

Corporate site

The corporate site consists of an Avaya IP Office 406V2 connected to the Extreme Summit 300 Switch with two Avaya IP Telephones and one Avaya digital phone, which in turn is connected to the WAN. The corporate site provides a DHCP server for assigning IP network parameters to the Avaya IP Telephones.

Remote office site

The remote office site consists of two Avaya C364T-PWR switches, Kentrox Q1300 QoS appliance, two Avaya 4600 Series IP Telephones and a PC running Avaya IP Office Phone Manager Pro. The Q1300 is rate limiting the fast Ethernet connection to the Avaya C364T-PWR port to 1.54 Bps to not exceed the WAN bandwidth limitations. The telephones and the PC running Avaya Phone ManagerPro are registering to the IP Office at the corporate site.

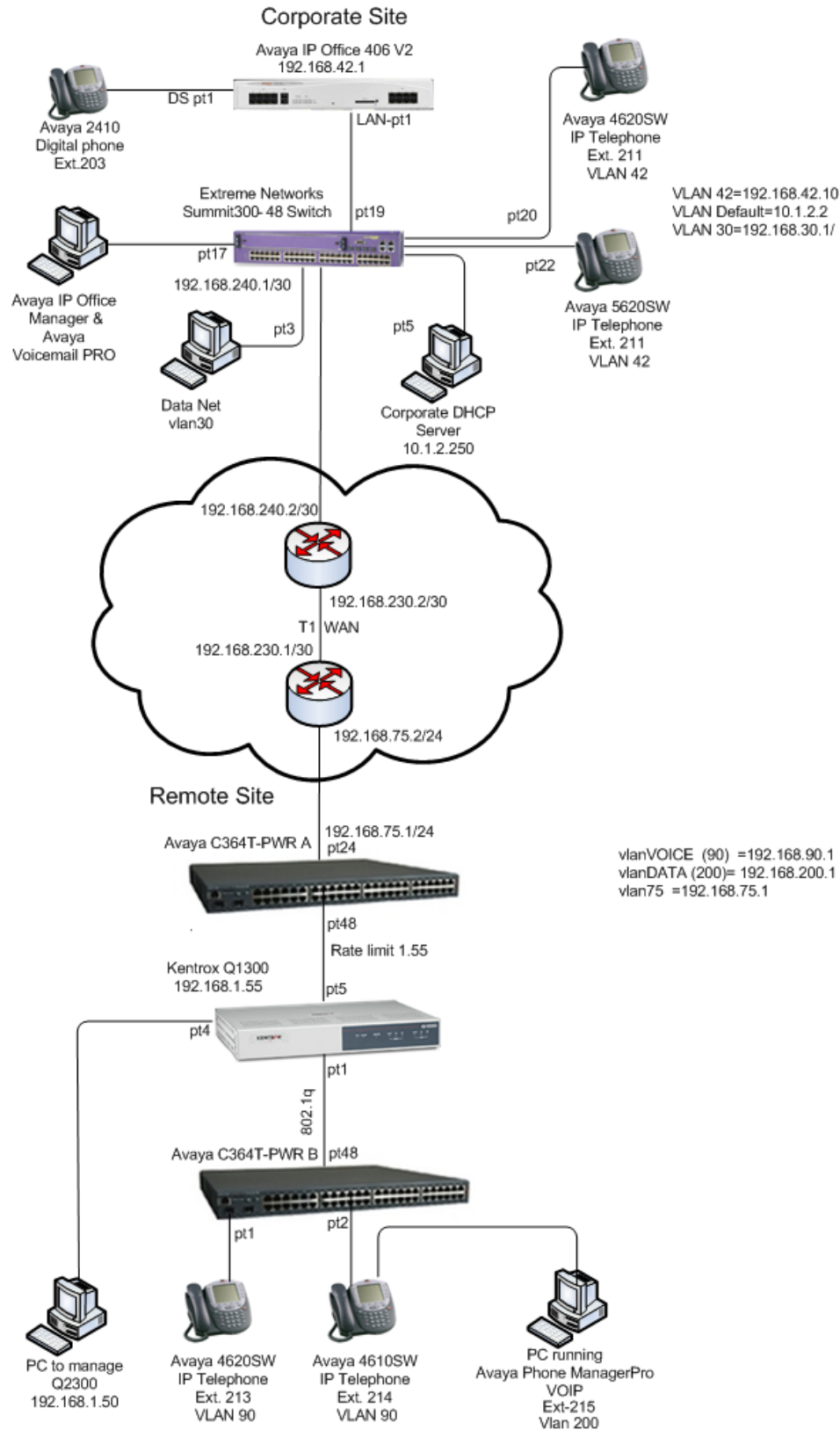


Figure 1: Network Configuration

2. Equipment and Software Validated

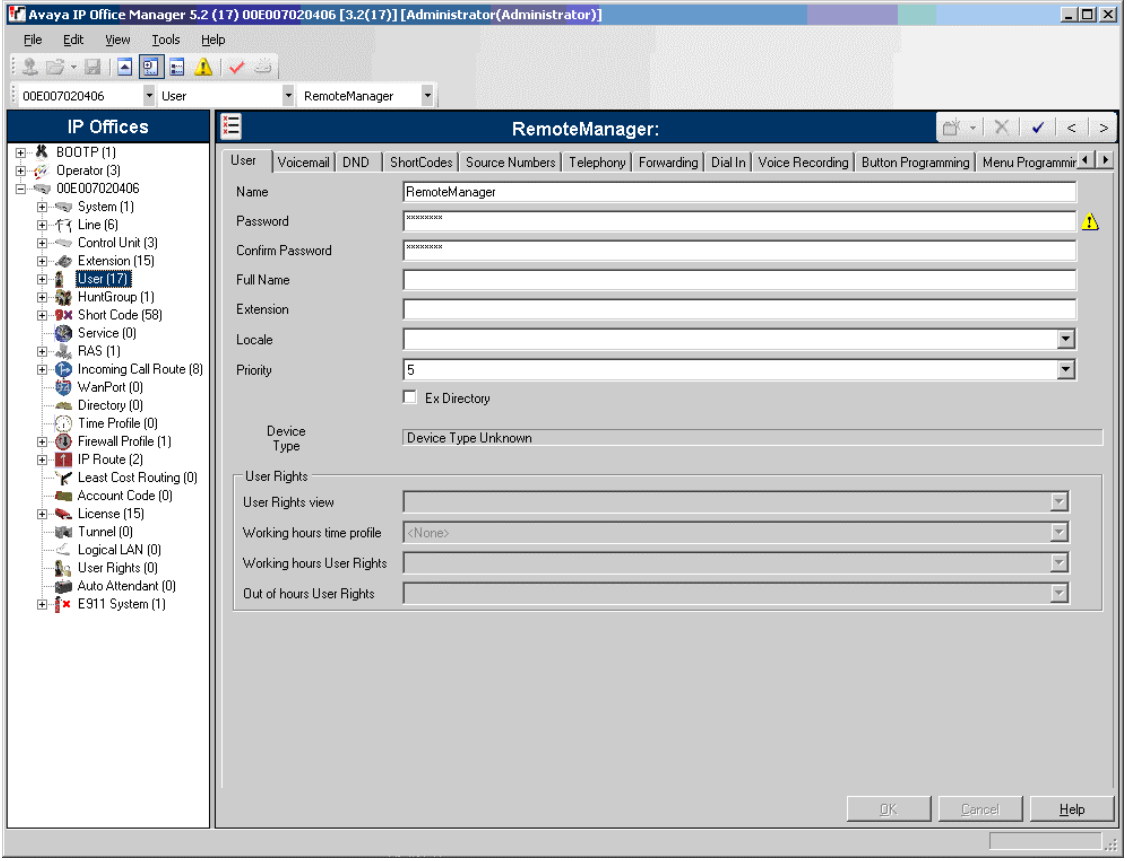
The following equipment and software/firmware were used for the sample configuration provided:

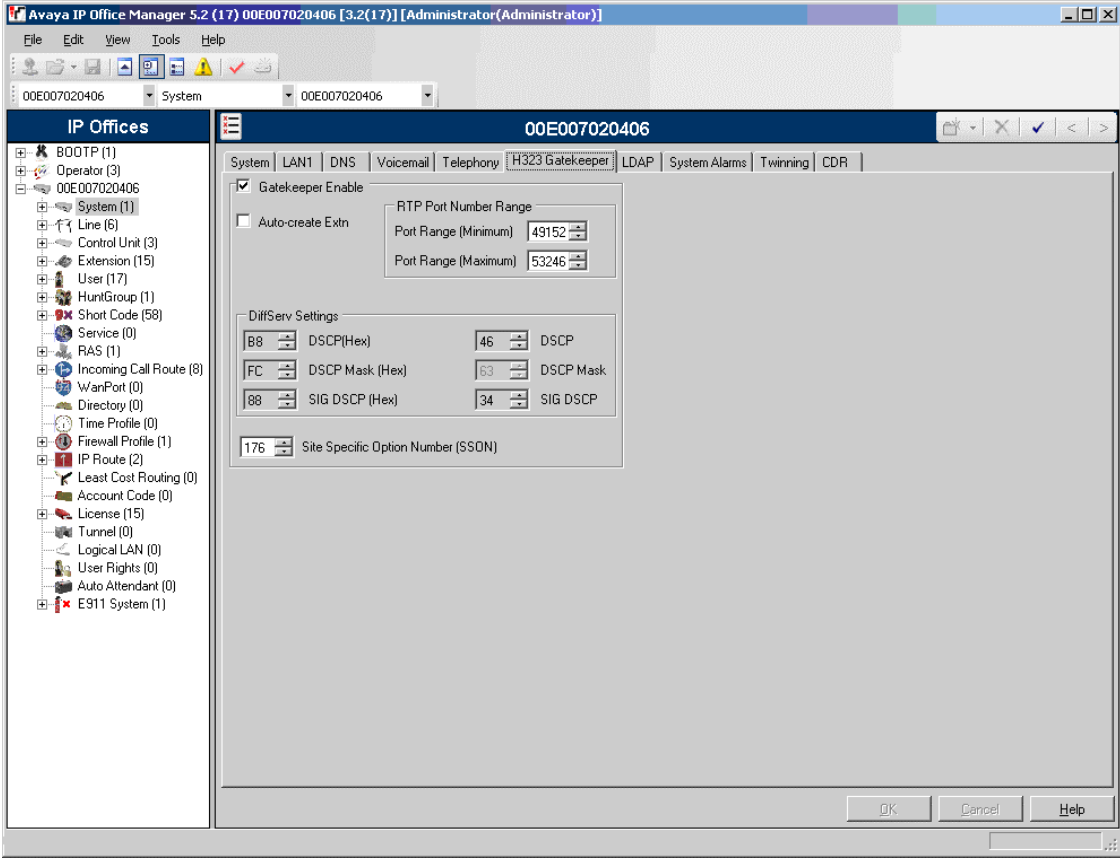
Equipment	Software/Firmware
Avaya IP Office IP406V2	3.2(17)
Avaya 4620 IP Telephones	2.6
Avaya 4610 IP Telephones	2.6
Avaya 5620 Telephones	2.6
Avaya 2410 Digital Telephone	N/A
Avaya IP Office Manager	3.2(17)
Avaya IP Office Phone Manager Pro	3.2.15
Avaya C364T-PWR	4.5.14
Kentrox Q1300 QoS Appliance	1.01
Extreme Networks Summit 300-48 Switch	ExtremeWare 7.4e.1.5

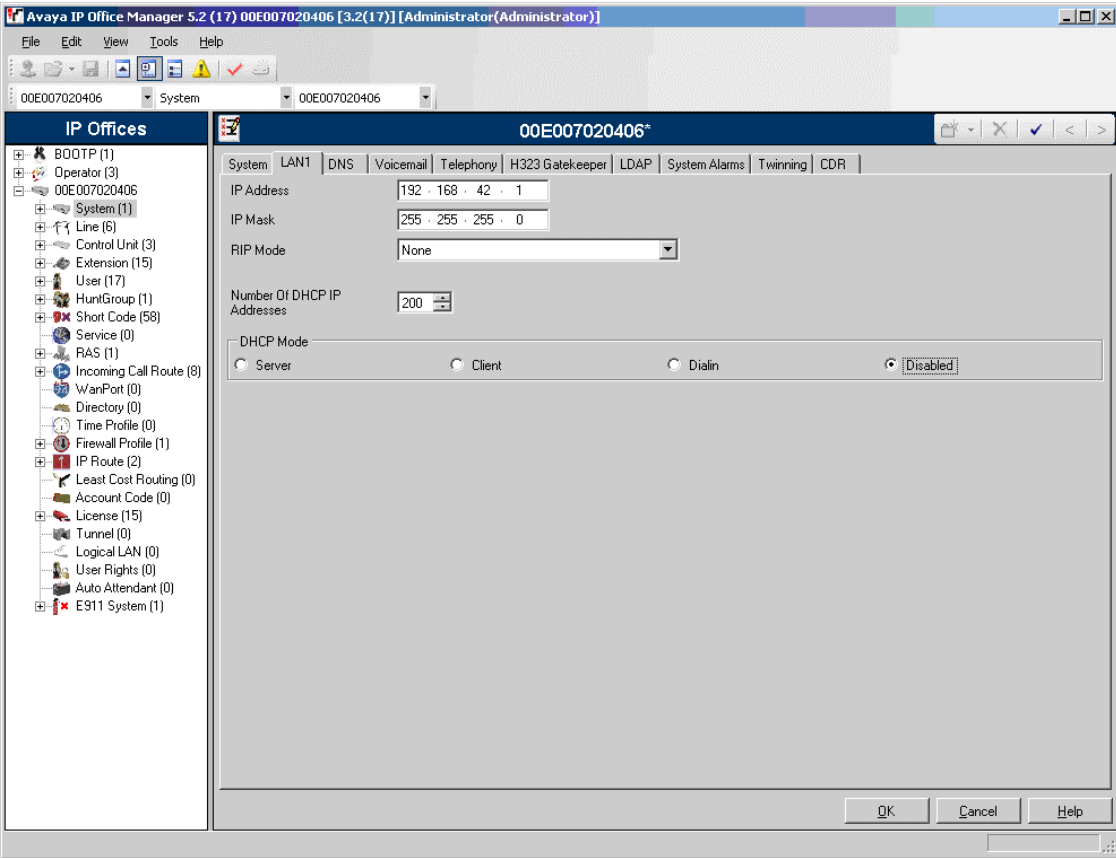
3. Avaya IP Office settings

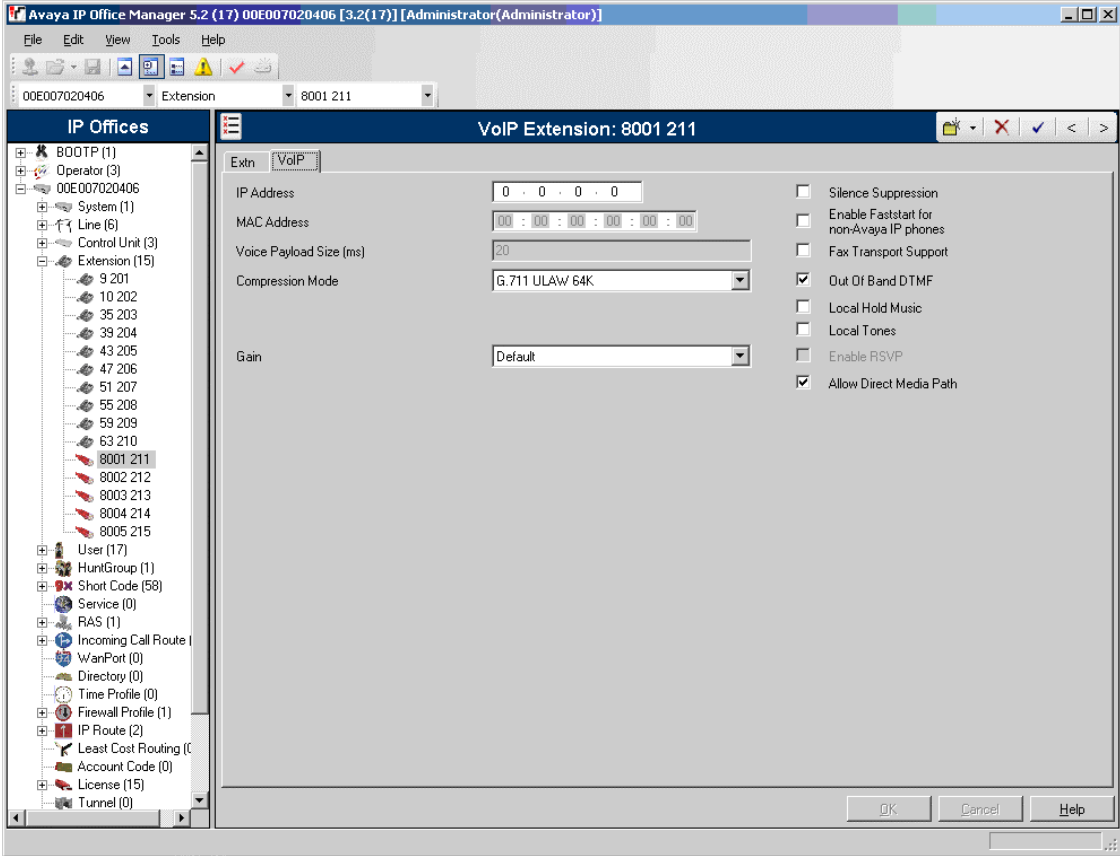
No Kentrox specific configuration is required on Avaya IP Office to support this solution. Except where stated the parameters in all steps are the default settings and are supplied for reference. For all other provisioning information such as provisioning of the trunks, call coverage, and extensions, please refer to the Avaya IP Office product documentation.

Log into the PC running IP Office Manager and go to **Start** → **Programs** → **IP Office** → **Manager** to launch the Manager application. Log into the Manager application using the appropriate credentials. In the Manager window that appears, select **File** → **Open** to search for IP Offices in the network.

Step	Description
1.	<p>IP Office Manager window. The main IP Office Manager window appears.</p> 

Step	Description
2.	<p>Verify Gatekeeper information and IP phone QoS settings</p> <p>In the Manager window, click System. Select the H.323 Gatekeeper Tab. Verify the Diffserv Settings for DSCP and SIG DSCP.</p> 

Step	Description
3.	<p>Disable DHCP server on Avaya IP Office.</p> <p>Select the LAN1 Tab. Set the DHCP Mode to Disabled. Press OK to continue.</p>  <p>The screenshot shows the Avaya IP Office Manager interface. On the left is a tree view of system components. The main window displays the configuration for the 'LAN1' tab. The 'DHCP Mode' is set to 'Disabled'.</p>

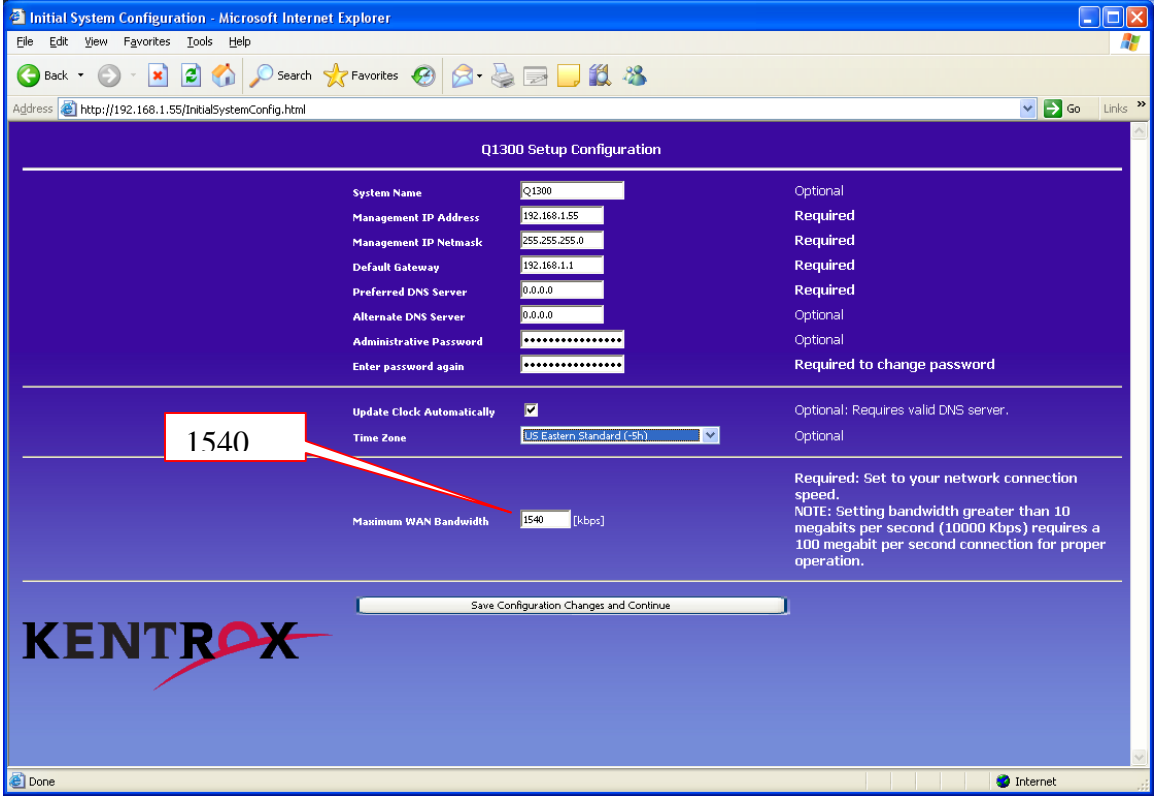
Step	Description
4.	<p>Verify Direct Media Path. Select Extensions. Double-click on the IP telephone extension to check. Select the VoIP tab. Verify that the Allow Direct Media Path box is checked. Press OK to continue</p>  <p>The screenshot shows the Avaya IP Office Manager 5.2 interface. On the left, a tree view under 'IP Offices' shows 'Extension (15)' expanded, with '8001 211' selected. The main pane displays the 'VoIP Extension: 8001 211' configuration. The 'VoIP' tab is active. Fields include IP Address (0.0.0.0), MAC Address (00:00:00:00:00:00), Voice Payload Size (20 ms), Compression Mode (G.711 ULAW/64K), and Gain (Default). On the right, a list of checkboxes shows 'Out Of Band DTMF' and 'Allow Direct Media Path' checked, while others like 'Silence Suppression' and 'Enable Faststart' are unchecked. 'OK', 'Cancel', and 'Help' buttons are at the bottom right.</p>

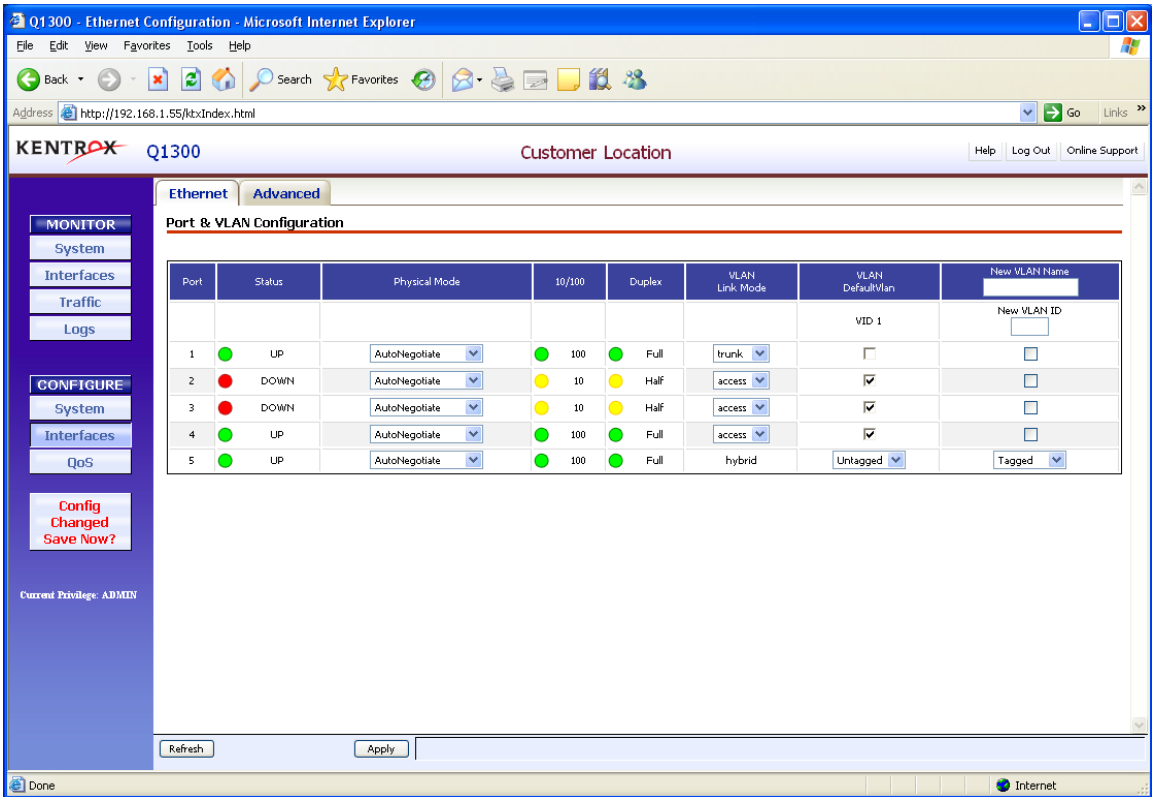
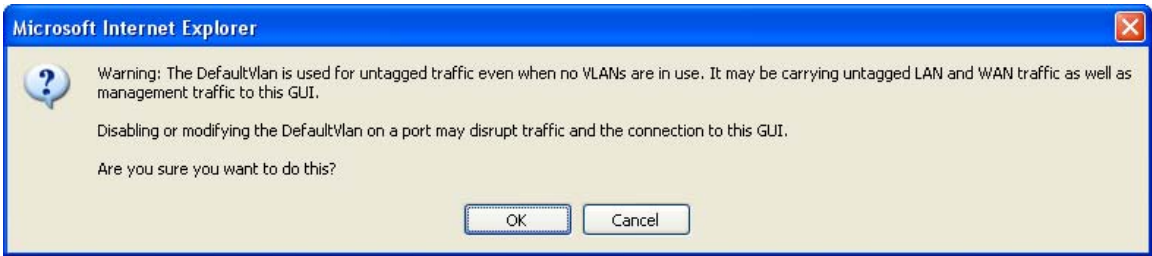
4. Configure the Kentrox Q1300 QoS Appliance

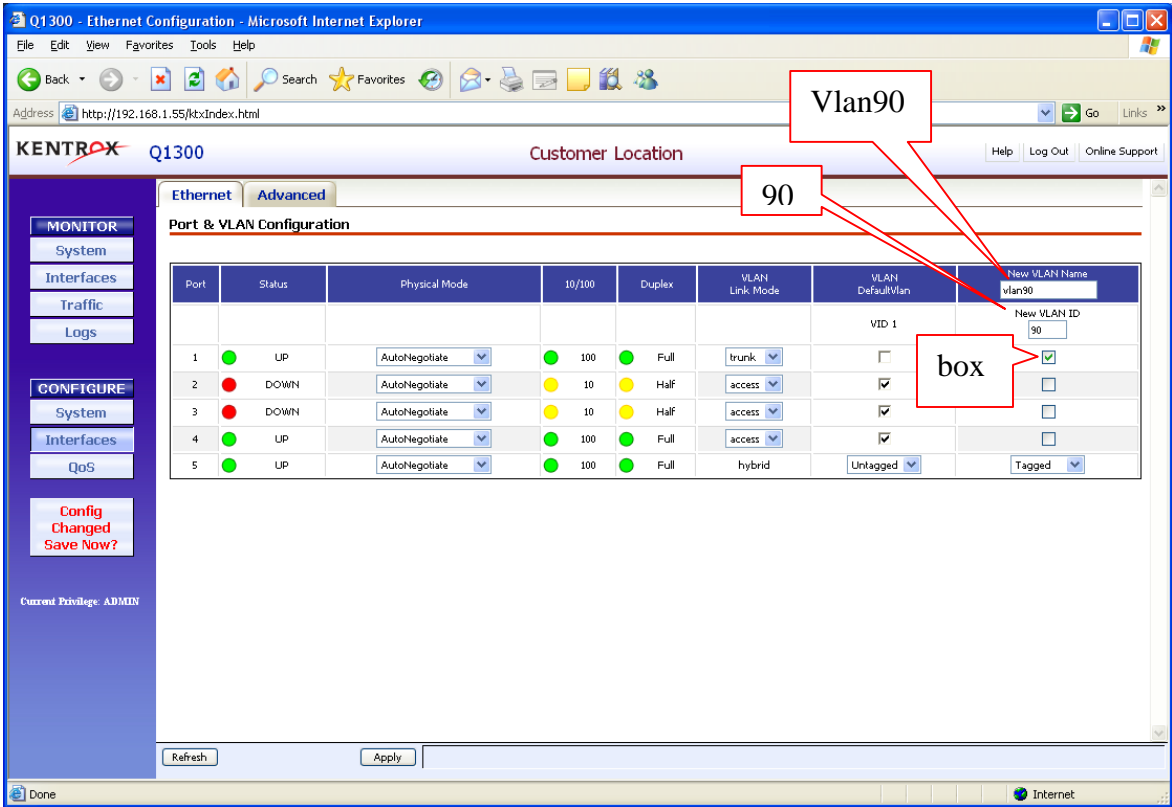
This section addresses configuring the Kentrox Q1300 QoS Appliance access device. Except where stated the parameters in all steps are the default settings and are supplied for reference. All required fields on the screens are indicated by a red asterisk (*).

Note: For this compliance testing Port 4 was used for managing the Q1300.

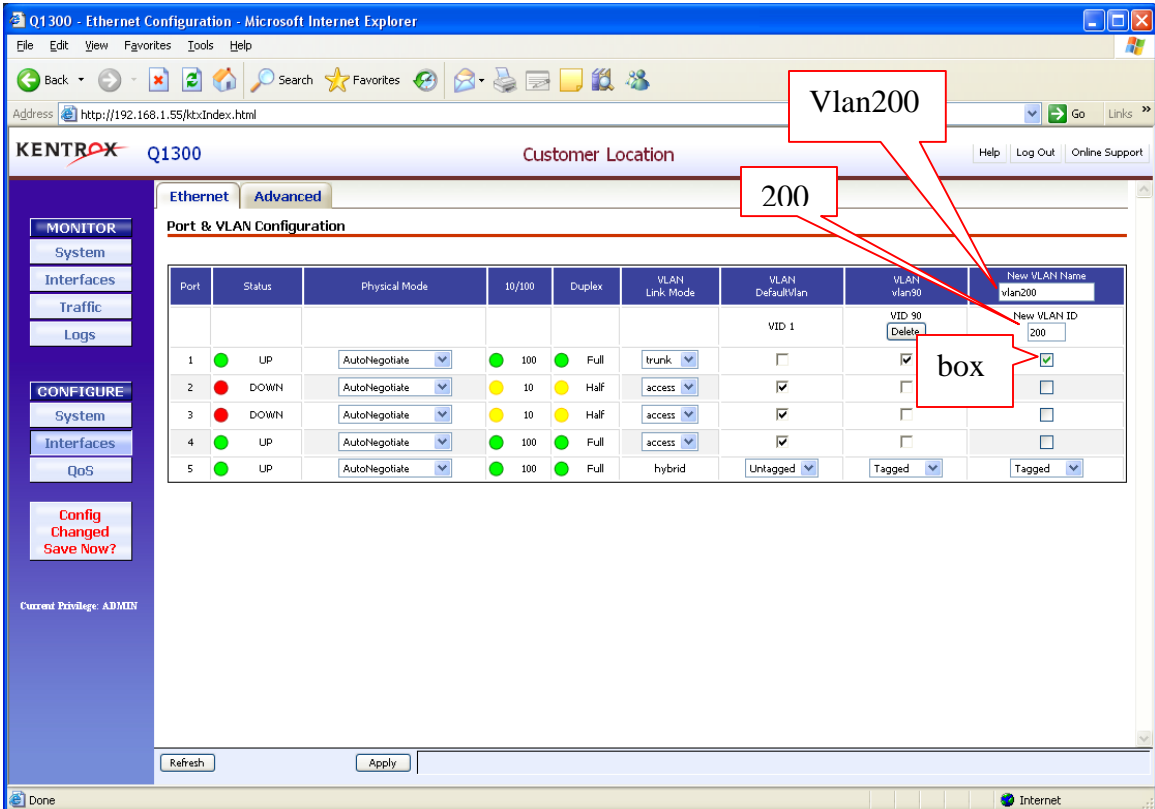
Step	Description
1.	Configure a PC to Manage the Q1300. Configure the PC to use IP address 192.168.1.10/24 with a default gateway of 192.168.1.1 . The Kentrox Q1300 IP Address is 192.168.1.55. Connect the PC to port 4 and then use Windows Internet Explorer to browse to the IP address of the Q1300 Administration web page. Log into the Q1300 using the appropriate credentials. When the Q1300 authentication window appears press OK .
2.	The following box will appear. Change the Maximum WAN Bandwidth to 1540 Kbps (WAN speed) and Change the Time Zone to user preference. Press Save Configuration Changes and Continue to continue. The screen in Step 3 is presented.



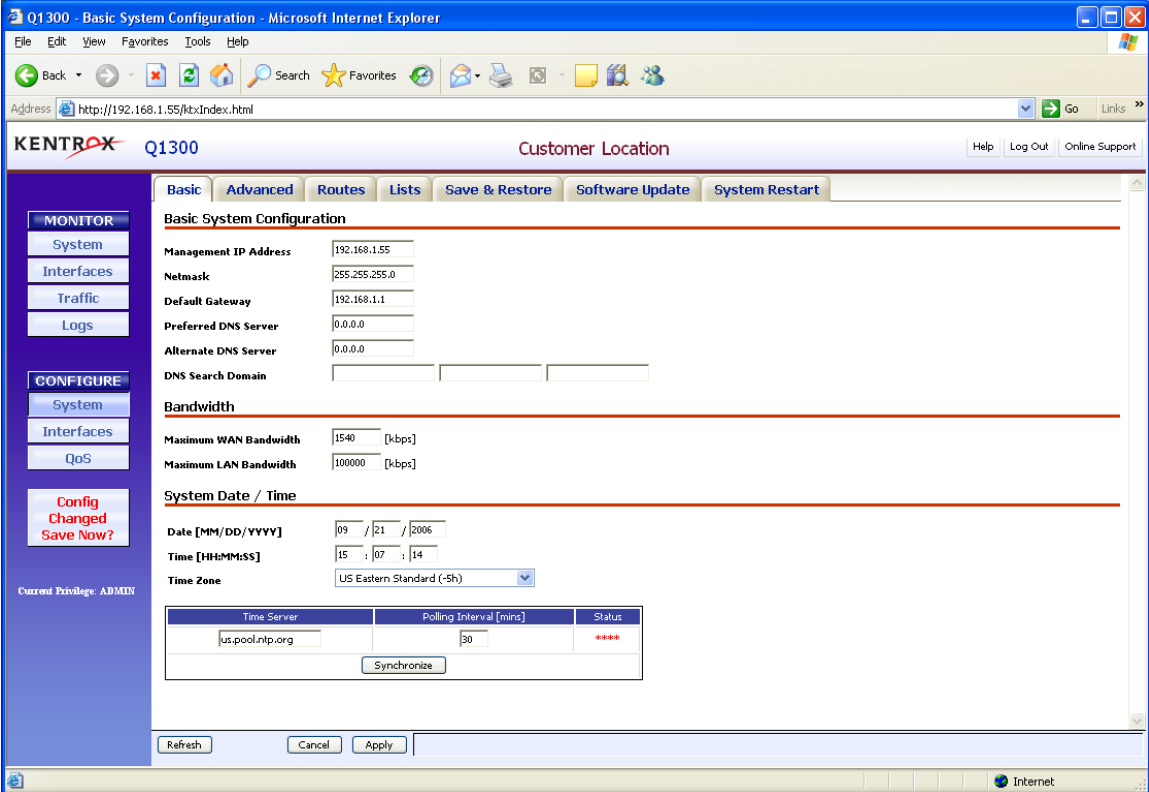
Step	Description
3.	<p>Configure dot1Q trunk to the Avaya C64T-PWR B switch. Select Configure → Interfaces and click the VLAN Link Mode drop down list for Port 1. Select trunk and un-check VLAN DefaultVlan box for port 1. Press Apply to continue.</p> 
4.	<p>The following information screen appears. Press OK to continue</p> 

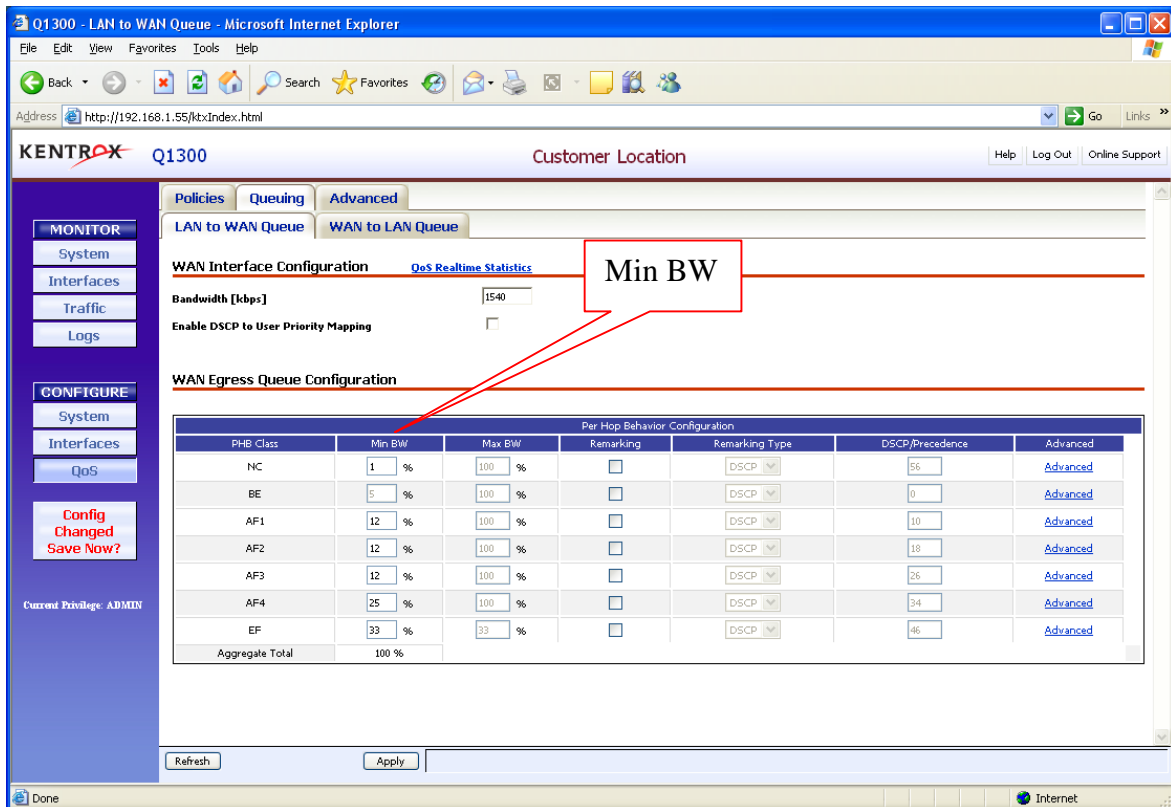
Step	Description
5.	<p>Configure Voice VLAN. Select Configure → Interfaces. Configure a unique Vlan name and Vlan ID under New VLAN Name and New VLAN ID. Check the box to add the VLAN to the trunk on Port 1. Press Apply to continue.</p> 

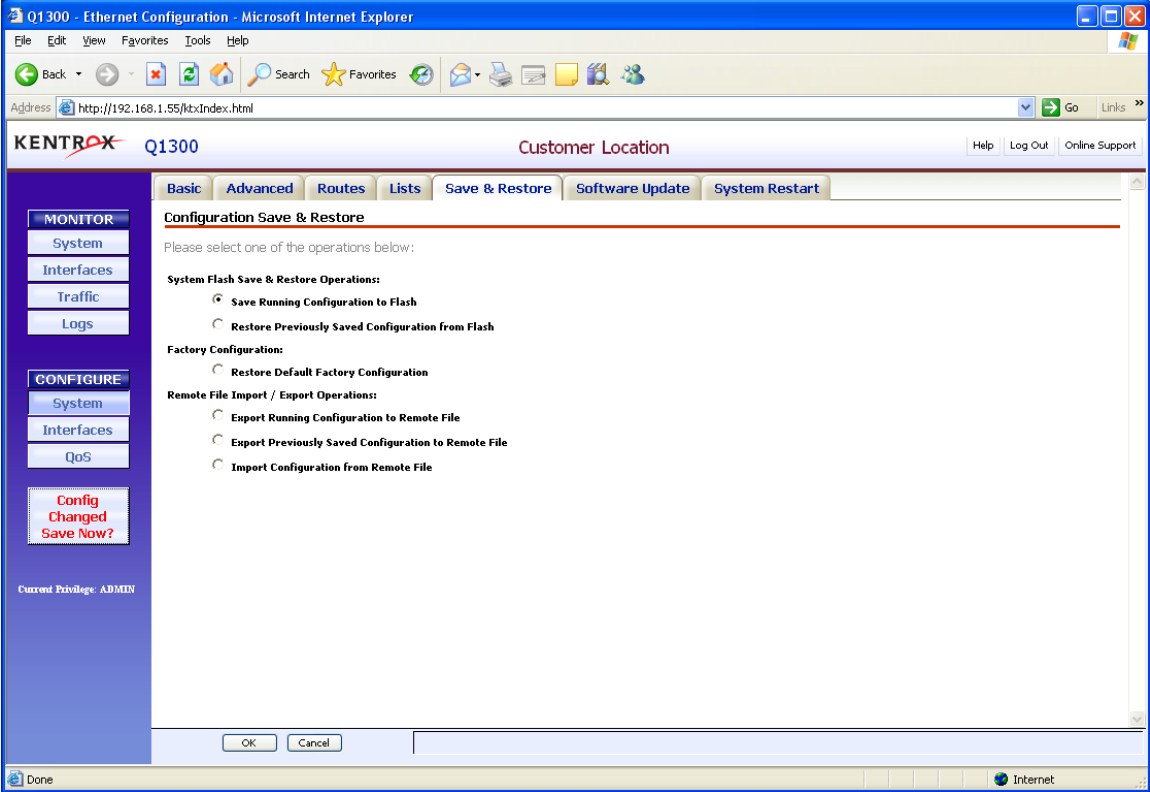
Step	Description
6.	<p>Configure Data VLAN.</p> <p>Select Configure → Interfaces. Configure a unique Vlan name and Vlan ID under New VLAN Name and New VLAN ID. Check the box to add the VLAN to the trunk on Port 1. Press Apply to continue.</p>



Port	Status	Physical Mode	10/100	Duplex	VLAN Link Mode	VLAN DefaultVlan	VLAN Vlan90	New VLAN Name	New VLAN ID	Add to Trunk
1	UP	AutoNegotiate	100	Full	trunk	VID 1	<input checked="" type="checkbox"/>	Vlan200	200	<input checked="" type="checkbox"/>
2	DOWN	AutoNegotiate	10	Half	access	<input checked="" type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>
3	DOWN	AutoNegotiate	10	Half	access	<input checked="" type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>
4	UP	AutoNegotiate	100	Full	access	<input checked="" type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>
5	UP	AutoNegotiate	100	Full	hybrid	Untagged	Tagged			Tagged

Step	Description
7.	<p>Set the time and date. Select Configure → System Date / Time → Basic. Press Apply and then OK to continue.</p> 

Step	Description																																																															
8.	<p>Verify bandwidth and QoS settings for the LAN to WAN Queue. For compliance testing the default values for QoS were used. Changes to the % value in the Min BW fields will alter the LAN to WAN QoS. Refer to section 10 for more information.</p> <p>Configure → QoS → Queuing</p>  <p>The screenshot shows the KENTROX Q1300 configuration interface. The 'WAN Interface Configuration' section has a 'Bandwidth [kbps]' field set to 1540. The 'WAN Egress Queue Configuration' table is as follows:</p> <table><tr><th>PHB Class</th><th>Min BW</th><th>Max BW</th><th>Remarking</th><th>Remarking Type</th><th>DSCP/precedence</th><th>Advanced</th></tr><tr><td>HC</td><td>1 %</td><td>100 %</td><td><input type="checkbox"/></td><td>DSCP</td><td>56</td><td>Advanced</td></tr><tr><td>BE</td><td>5 %</td><td>100 %</td><td><input type="checkbox"/></td><td>DSCP</td><td>0</td><td>Advanced</td></tr><tr><td>AF1</td><td>12 %</td><td>100 %</td><td><input type="checkbox"/></td><td>DSCP</td><td>10</td><td>Advanced</td></tr><tr><td>AF2</td><td>12 %</td><td>100 %</td><td><input type="checkbox"/></td><td>DSCP</td><td>18</td><td>Advanced</td></tr><tr><td>AF3</td><td>12 %</td><td>100 %</td><td><input type="checkbox"/></td><td>DSCP</td><td>26</td><td>Advanced</td></tr><tr><td>AF4</td><td>25 %</td><td>100 %</td><td><input type="checkbox"/></td><td>DSCP</td><td>34</td><td>Advanced</td></tr><tr><td>EF</td><td>33 %</td><td>33 %</td><td><input type="checkbox"/></td><td>DSCP</td><td>46</td><td>Advanced</td></tr><tr><td>Aggregate Total</td><td>100 %</td><td></td><td></td><td></td><td></td><td></td></tr></table>	PHB Class	Min BW	Max BW	Remarking	Remarking Type	DSCP/precedence	Advanced	HC	1 %	100 %	<input type="checkbox"/>	DSCP	56	Advanced	BE	5 %	100 %	<input type="checkbox"/>	DSCP	0	Advanced	AF1	12 %	100 %	<input type="checkbox"/>	DSCP	10	Advanced	AF2	12 %	100 %	<input type="checkbox"/>	DSCP	18	Advanced	AF3	12 %	100 %	<input type="checkbox"/>	DSCP	26	Advanced	AF4	25 %	100 %	<input type="checkbox"/>	DSCP	34	Advanced	EF	33 %	33 %	<input type="checkbox"/>	DSCP	46	Advanced	Aggregate Total	100 %					
PHB Class	Min BW	Max BW	Remarking	Remarking Type	DSCP/precedence	Advanced																																																										
HC	1 %	100 %	<input type="checkbox"/>	DSCP	56	Advanced																																																										
BE	5 %	100 %	<input type="checkbox"/>	DSCP	0	Advanced																																																										
AF1	12 %	100 %	<input type="checkbox"/>	DSCP	10	Advanced																																																										
AF2	12 %	100 %	<input type="checkbox"/>	DSCP	18	Advanced																																																										
AF3	12 %	100 %	<input type="checkbox"/>	DSCP	26	Advanced																																																										
AF4	25 %	100 %	<input type="checkbox"/>	DSCP	34	Advanced																																																										
EF	33 %	33 %	<input type="checkbox"/>	DSCP	46	Advanced																																																										
Aggregate Total	100 %																																																															

Step	Description
9.	<p>Save the configuration.</p> <p>Once the configuration changes are complete, save the configuration to Flash. Click on the “Config Changes Save Now?” button or Select Configure → System → Config Save / Restore and choose the most appropriate action. The default selection is Save Running Configuration to Flash. Press OK.</p> 

5. Configure the Avaya C364T-PWR switch A at Remote site

Step	Description
1.	Connect to the Avaya C364T-PWR A switch. Log in using the appropriate Login ID and Password . Login: Password: C360-1(super)#
2.	Enter routing module C360-1(super)# session router
3.	Enable DHCP Relay Router-1(super)# ip bootp-dhcp relay
4.	Create VLAN vlan75 Router-1(super)# set vlan 75 name vlan75
5.	Create vlan75 interface (port is assigned in step 10) Router-1(super)# interface vlan75 Router-1(super-if:90)# ip address 192.168.75.1 255.255.255.0 Router-1(super-if:90)# ip vlan name 75
6.	Create VLAN vlanVOICE Router-1(super)# set vlan 90 name vlanVOICE
7.	Create vlanVOICE interface (virtual interface) Router-1(super)# interface vlanVOICE Router-1(super-if:90)# ip address 192.168.90.1 255.255.255.0 Router-1(super-if:90)# ip vlan name 90 Router-1(super-if:90)# ip bootp-dhcp server 10.1.2.250 Router-1(super-if:90)# ip bootp-dhcp network 192.168.90.0

8.	Create VLAN vlanDATA Router-1(super)# set vlan 200 name vlanDATA
9.	Create vlanDATA interface (virtual interface) Router-1(super)# interface vlanDATA Router-1(super-if:200)# ip address 192.168.200.1 255.255.255.0 Router-1(super-if:200)# ip vlan name 200 Router-1(super-if:200)# ip bootp-dhcp server 10.1.2.250 Router-1(super-if:200)# ip bootp-dhcp network 192.168.200.0
10.	Assign vlan75 to port 1/24 Router-1(super)# session switch C360-1(super)# set port vlan 75 1/24
11.	Set trunking on port 1/48. C360-1(configure)# set trunk 1/48 dot1q
12.	Set port binding to port 1/48 to allow all VLAN traffic on the port. C360-1(configure)# set port vlan-binding-mode 1/48 bind-to-all

6. Configure the Avaya C364T-PWR switch B

This section shows the necessary steps in configuring the Avaya C364T-PWR switch as shown in the sample network.

Step	Description
1.	Connect to the Avaya C364T-PWR switch. Log in using the appropriate Login ID and Password . Login: Password: C360-1(super)#
2.	Create VLANS VlanVOICE and VlanDATA . C360-1(super)# set vlan 90 name vlanVOICE C360-1(super)# set vlan 200 name vlanDATA
3.	Set trunking on ports 1/2 and 1/48 C360-1(super)# set trunk 1/2 dot1q C360-1(super)# set trunk 1/48 dot1q
4.	Set port binding to port 1/48 to allow all VLAN traffic on the port. C360-1(super)# set port vlan-binding-mode 1/48 bind-to-all
5.	Assign VLANS to ports 1/1 and 1/2 . C360-1(super)# set port vlan 90 1/1 C360-1(super)# set port vlan 200 1/2
6.	Assign Static VLAN to port 1/2 . C360-1(super)# set port static-vlan 1/2 90

7. Configure the Extreme Summit 300-48 Switch

This section shows the necessary steps in configuring the Summit 300-48 as shown in the sample network.

Step	Description
1.	Connect to the Summit 300-48. Log in using the appropriate Login ID and Password . Login: Password: Summit300-48:1 #
2.	Ensure the ports are not already configured. Use the show port <port> info detail command to check the current configuration for the port. Make sure the port is not assigned to a VLAN. Summit300-48:1 # show port 1:3 info detail Repeat for ports 1:4,1:5,1:17,1:19,1:20,1:22,1:48
3.	Create the Voice VLAN and interface . QoS profile QP7 is a pre-defined profile. Summit300-48:31 # create vlan vlan42 Summit300-48:32 # configure vlan42 tag 42 Summit300-48:34 # configure vlan42 qosprofile QP7 Summit300-48:34 # configure vlan42 priority 7
4.	Add an IP address for the Voice VLAN , and enable IP forwarding. Note: subnets/VLANs will not route unless IP forwarding is enabled for that VLAN. Summit300-48:34 # configure vlan42 ipaddress 192.168.42.254/24 Summit300-48:34 # enable ipforwarding vlan42
5.	Remove the default vlan for the ports. Summit300-48:1# configure vlan default delete ports 1:4,1:5, 1:17,1:19,1:20,1:22,1:48
6.	Assign ports to the Voice VLAN for the IP Phones. Summit300-48:34 # configure vlan42 add ports 1:20,1:22 tagged

Step	Description
7.	Assign ports to the Voice VLAN for Avaya IP Office and PC . Port 1:19 will be used for the Avaya IP Office. Summit300-48:34 # configure vlan42 add ports 1:17,1:19
8.	Assign Voice VLAN to the trunk port. Summit300-48:34 # configure vlan42 add ports 1:48 tagged
9.	Assign Port 1:19 to qosprofile QP7 . QoS profile QP7 is a pre-defined profile. Summit300-48:34 # configure ports 1:19 qosprofile QP7
10.	Enable DiffServ examination on port 1:19. Summit300-48:34 # enable diffserv examination ports 1:19
11.	Set all ingress traffic on port 1:19 to priority 6 . Summit300-48:34 # create access-mask port19pri6 port Summit300-48:34 # create access-list pri19 access-mask port19pri6 port 1:19 permit set dot1p 6
12.	Create the Data VLAN . Summit300-48:31 # create vlan vlan30 Summit300-48:32 # configure vlan30 tag 30 Summit300-48:34 # configure vlan30 qosprofile QP1 Summit300-48:34 # configure vlan30 priority 1
13.	Add the IP address for the Data VLAN , and enable IP forwarding. Note: subnets/VLANs will not Route unless to enable IP forwarding for that vlan Summit300-48:34 # configure vlan30 ipaddress 192.168.30.1/24 Summit300-48:34 # enable ipforwarding vlan30
14.	Assign ports to the Data VLAN Summit300-48:34 # configure vlan30 add ports 1:4

Step	Description
15	<p>Create WAN VLAN</p> <p>Summit300-48:31 # create vlan vlan240 Summit300-48:32 # configure vlan240 tag 240 Summit300-48:34 # configure vlan240 qosprofile QP7 Summit300-48:34 # configure vlan240 priority 7</p>
16	<p>Add the IP address for the WAN VLAN, and enable IP forwarding</p> <p>Note: subnets/VLANs will not Route unless to enable IP forwarding for that vlan</p> <p>Summit300-48:34 # configure vlan240 ipaddress 192.168.240.1/30 Summit300-48:34 # enable ipforwarding vlan240</p>
17	<p>Assign ports to the WAN VLAN</p> <p>Summit300-48:34 # configure vlan240 add ports 1:24</p>
18	<p>Add static routes for the local corporate networks going to the remote site.</p> <p>Summit300-48:34 # configure iproute add 192.168.230.0 255.255.255.0 192.168.240.2 1 Summit300-48:34 # configure iproute add 192.168.75.0 255.255.255.0 192.168.240.2 1 Summit300-48:34 # configure iproute add 192.168.90.0 255.255.255.0 192.168.240.2 1 Summit300-48:34 # configure iproute add 192.168.200.0 255.255.255.0 192.168.240.2 1</p>
19	<p>Create 10 VLAN</p> <p>Summit300-48:31 # create vlan vlan10 Summit300-48:32 # configure vlan10 tag 10</p>
20	<p>Add the IP address for the 10 VLAN, and enable IP forwarding</p> <p>Note: subnets/VLANs will not Route unless IP forwarding is enabled for that vlan</p> <p>Summit300-48:34 # configure vlan10 ipaddress 10.1.2.2 Summit300-48:34 # enable ipforwarding vlan10</p>
21	<p>Assign ports to the 10 VLAN</p> <p>Summit300-48:34 # configure vlan10 add ports 1:5</p>

8. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality, serviceability, and performance testing.

Feature functionality testing focused on the QoS and VLAN implementation in the Avaya/Kentrox configuration. Specifically, compliance testing verified that VoIP media and signaling traffic could be carried together with low priority data traffic on a low bandwidth link while still achieving good voice quality. Prioritization of voice traffic was achieved by implementing DiffServ-based QoS. Voice and data traffic were segmented in the enterprise network using VLANs.

Performance testing was conducted by generating voice calls with a bulk call generator and data traffic with a data traffic generator to simulate a converged network for a prolonged period of time. At the end of the performance test, it was verified that the network devices continued to operate successfully for small office scenarios.

Serviceability testing was conducted to verify the ability of the Avaya/Kentrox VoIP solutions to recover from adverse conditions, such as power cycling network devices and disconnecting cables between the LAN and WAN interfaces. In all cases, the ability to recover after the network has been normalized was verified.

8.1. General Test Approach

All feature functionality test cases were performed manually. The general test approach entailed verifying the following:

- LAN/WAN connectivity between the Avaya and Kentrox products,
- Registration of Avaya IP Telephones with the Avaya IP Office,
- VoIP calls between the corporate and the remote office sites,
- Inter-office calls using G.711 mu-law and G.729 codec sets, and conferencing, and
- Sending low priority data traffic over the WAN links and verifying that QoS directed the voice signaling and voice media to the higher priority egress queue based on the packets' DSCP value.

The performance tests were performed by generating low priority data traffic for small office scenarios over the WAN interface, and verifying that good voice quality was achieved when calls are routed over the WAN interface

8.2. Test Results

All feature functionality, serviceability, and performance test cases passed. The Q-Series QoS implementation yielded good voice quality and no lost calls. The stability of the Avaya/Kentrox solution was successfully verified through performance and serviceability testing.

9. Verification Steps

This section provides the steps for verifying end-to-end network connectivity and QoS in the field from the perspective of the Q1300 QoS Appliance. In general, the verification steps include:

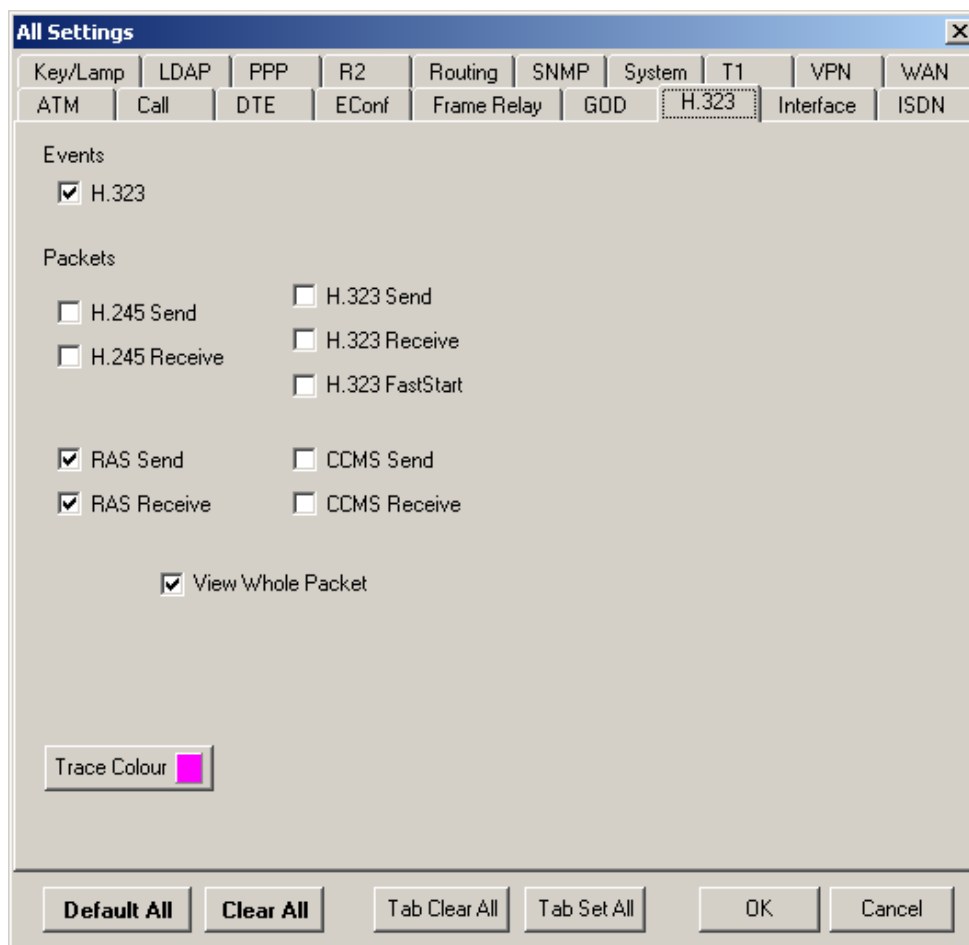
1. Verify IP communication to the following network devices and interfaces by using the **ping** command.
 - Ping the Avaya IP Office.
 - Ping the Avaya IP telephones registered to the Avaya IP Office.
 - Ping the DHCP server
2. Check that the Avaya IP Telephones have successfully registered using the IP Office **System Monitor**. See section 8.1.
3. Place internal and external calls between the Digital telephone and IP telephones at each site.

10. Troubleshooting

10.1. Avaya IP Office Troubleshooting

Troubleshooting can be done on the IP Office via the IP Office System Monitor application. Log into the IP Office Monitor PC and select **Start** → **Programs** → **IP Office** → **Monitor** to launch the IP Office System Monitor application. Log into the application using the appropriate credentials.

To see the registration messages going to and from IP Office, select **Trace Options** under the **Filters** Menu. Select the **H.323** tab and configure as illustrated below.



10.2. Miscellaneous Troubleshooting

1. If the voice quality is poor, check the QoS configuration in the Q1300 browser interface in section 3.8.
2. If a Q1300 QoS Appliance is unable to communicate with any of the aforementioned IP devices and interfaces, check the routing and status of the Ethernet interfaces through the Q1300 browser interface in section 3.6.

11. Support

For technical support on the Kentrox Q-Series routers, contact Kentrox Technical Support using any of the following options:

- Toll-free: (800) 733-5511
- Direct: (503) 643-1681
- Email: care@kentrox.com

12. Conclusion

These Application Notes describe the configuration steps required for integrating the Kentrox Q1300 QoS Appliance into a small office and/or low traffic/bandwidth Avaya IP Office infrastructure. For the configuration described in these Application Notes, the Q1300 QoS Appliance was responsible for enforcing QoS using Differentiated Services. The Avaya IP Offices delivered the voice traffic to the routers for transmission over the WAN together with data traffic. Good voice quality was successfully achieved in the Avaya/Kentrox configuration described herein.

13. Additional References

This section references the Avaya and Kentrox product documentation that are relevant to these Application Notes.

The Avaya product documentation can be found at:

<http://marketingtools.avaya.com/knowledgebase/>

The Kentrox product documentation can be found at:

<http://www.kentrox.com/products/Q1300/>

©2006 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DeveloperConnection Program at devconnect@avaya.com.