Avaya Solution & Interoperability Test Lab

Application Notes for Kentrox Q-2300 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 Q-Series Q2300 access router and Avaya IP Office. The Kentrox Q-Series Q2300 was compliance-tested with an Avaya IP Office. Emphasis was placed on verifying 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 Q-Series Q2300 Router connected to an Avaya IP Office. The Kentrox Q-Series Q2300 Access Router was compliance-tested with an Avaya IP Office.

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 711 and 729.

Kentrox Q-Series Q2300 Access Route
The Q2300 router combines the features of an IP router, QoS appliance, IPSec VPN appliance, firewall, and Ethernet switch into one easy-to-use network access device.

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 and Q2300 were 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 a Kentrox Q2300 router, two Avaya 4600 and 5600 IP Telephones and a PC running Avaya IP Office Phone Manager Pro. The Q2300 is rate limiting the WAN port to 1.54 Megs to not exceed the WAN bandwidth limitations and is providing DHCP relay functions so that a centralized DHCP server can be used. The Phones and the PC running Avaya Phone ManagerPro are registering to the IP Office at the corporate site.

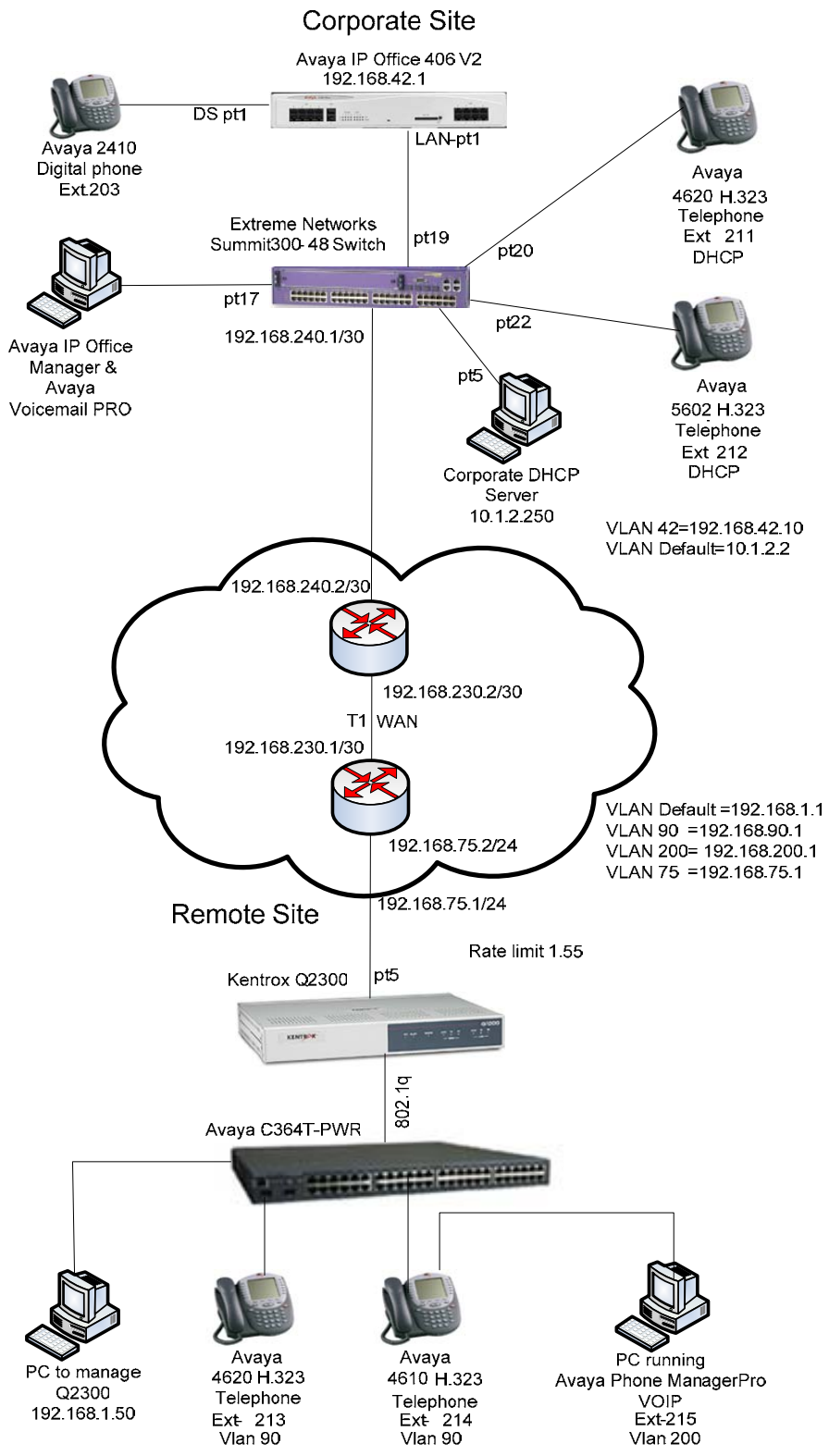


Figure 1: Network Configuration

2. Equipment and Software Validated

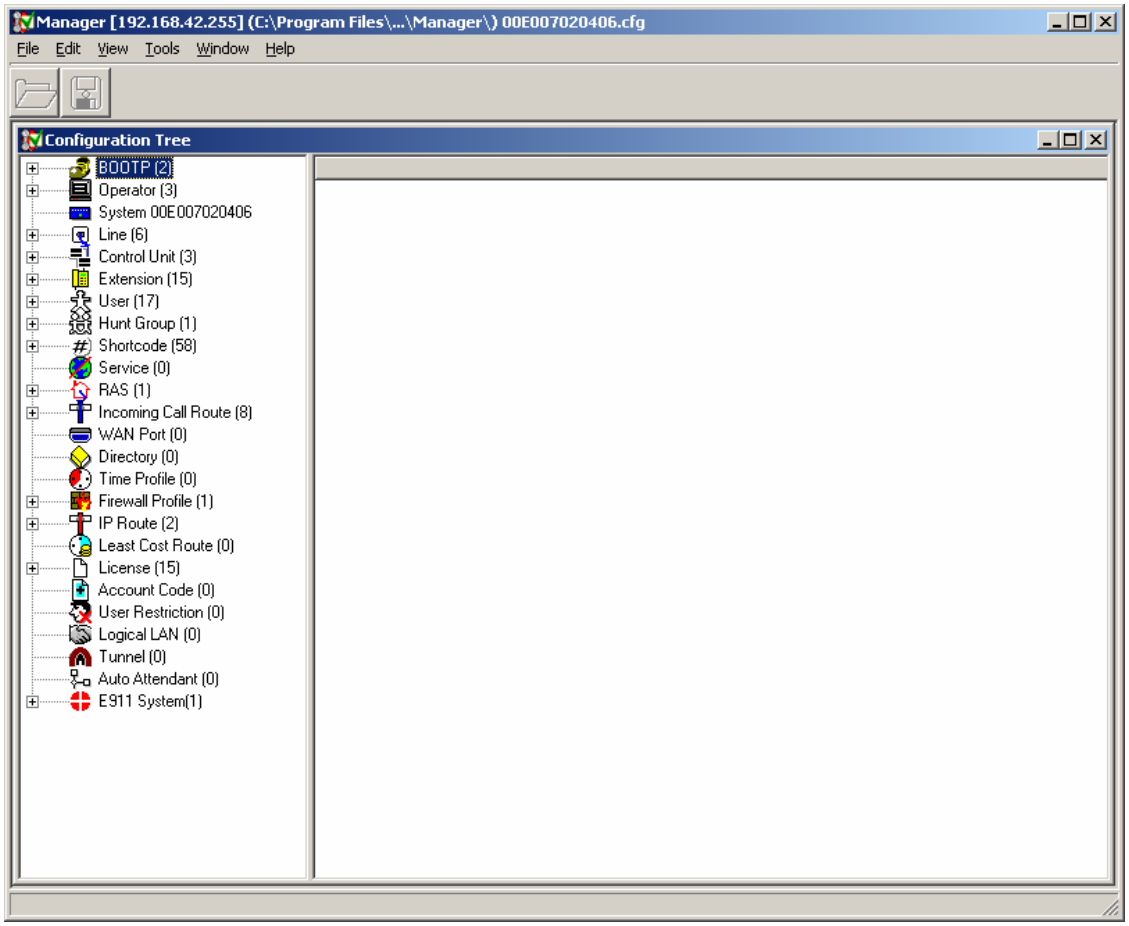
The following equipment and software/firmware were used for the sample configuration provided:

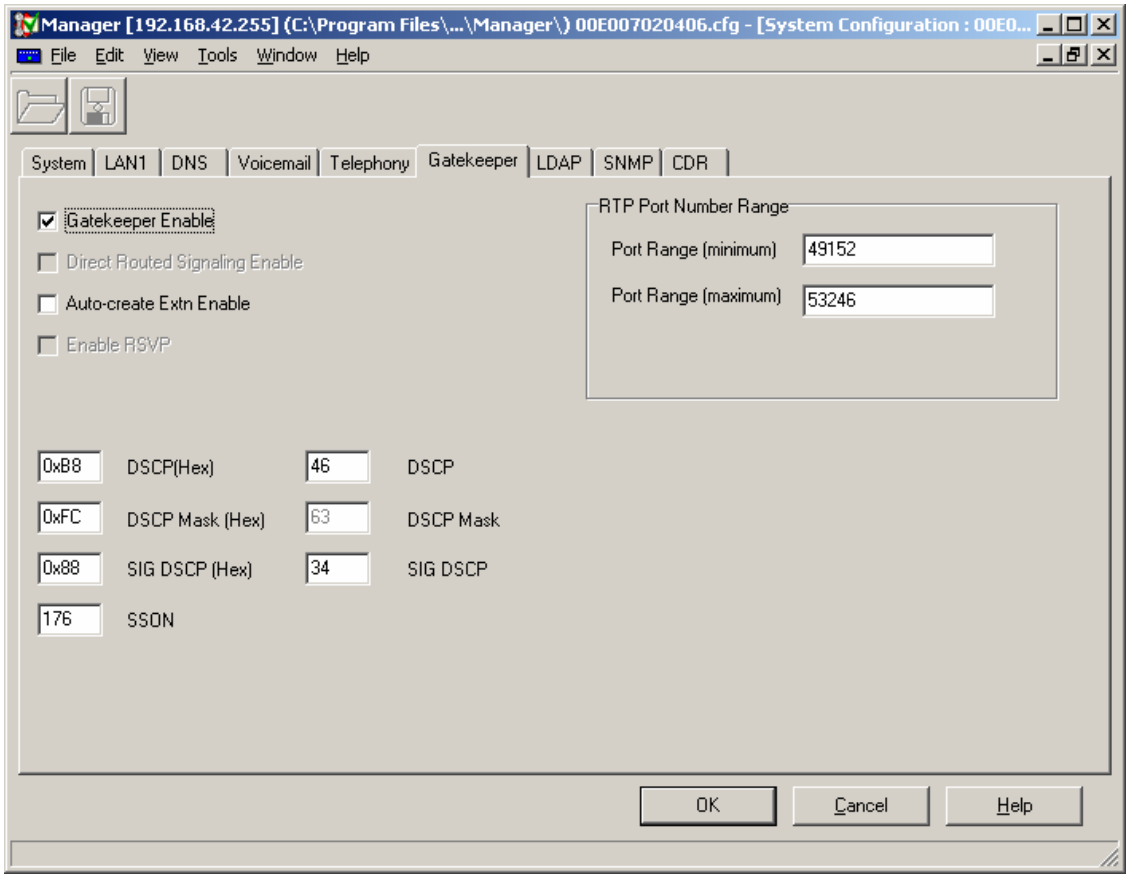
Equipment	Software/Firmware
Avaya IP Office IP406V2	3.1(65)
Avaya 4620 IP Telephones	2.3
Avaya 5602 Telephones	2.3
Avaya 2410 Digital Telephone	N/A
Avaya IP Office Manager	3.1(65)
Avaya IP Office System Monitor	3.1(65)
Avaya IP Office Phone Manager Pro	3.1.15
Kentrox Q-Series Q2300	1.35
Extreme Networks Summit 300-48 Switch	ExtremeWare 7.4e.1.5

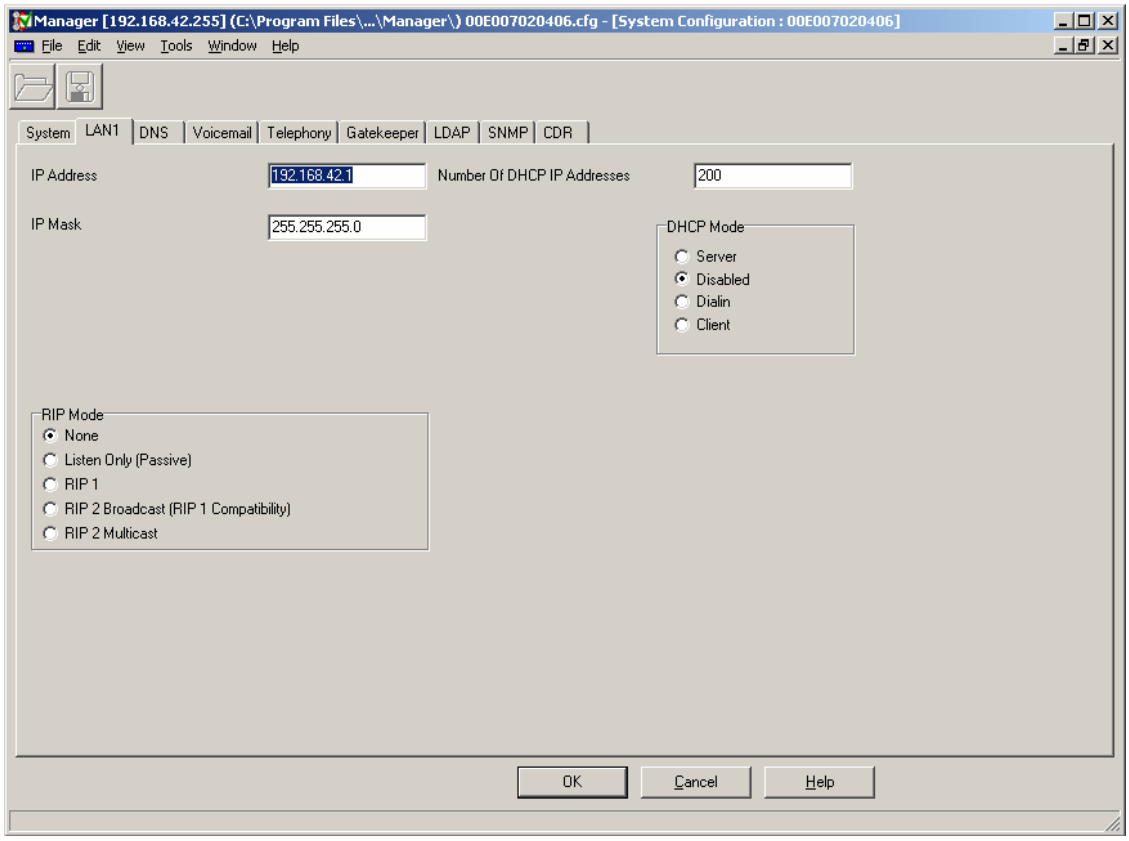
3. Avaya IP Office settings

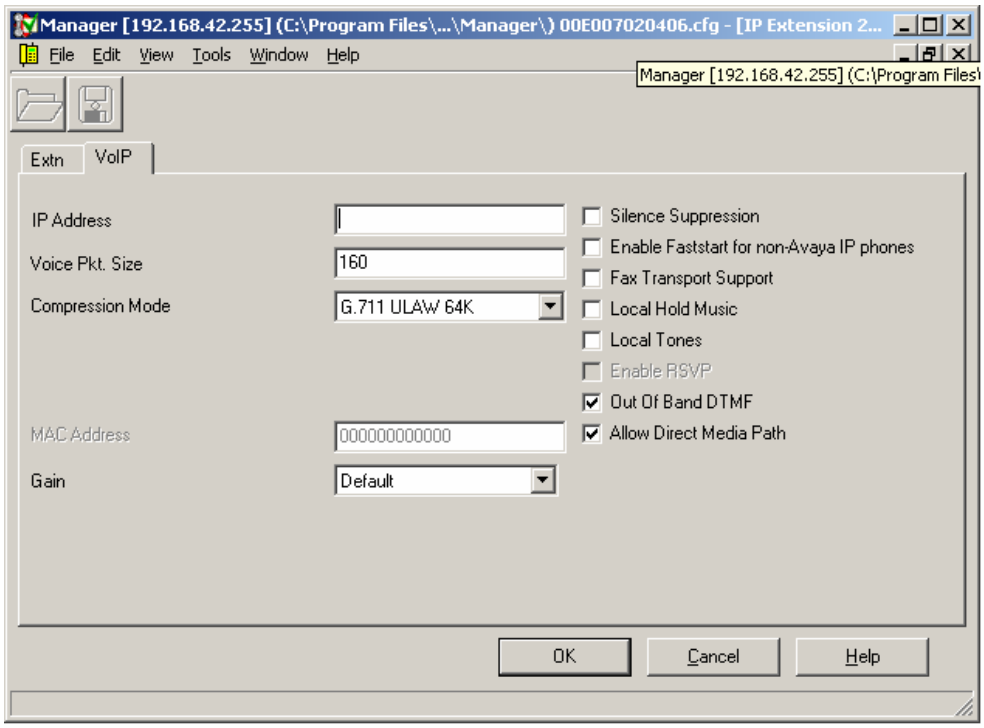
No Kentrox specific configuration is required on Avaya IP Office to support this solution. Except where stated the parameters in all steps are the default settings and are supplied for reference. For all other provisioning information such as provisioning of the trunks, call coverage, and extensions, 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.	IP Office Manager window. The main IP Office Manager window appears. It is from the Configuration Tree to the left that all of the following steps are referring to. 

Step	Description
2.	Verify Gatekeeper information. In the Manager window, go to the Configuration Tree and double-click **System**. Select the **Gatekeeper** Tab. Verify the DSCP setting for **DSCP** and **SIG DSCP**. 

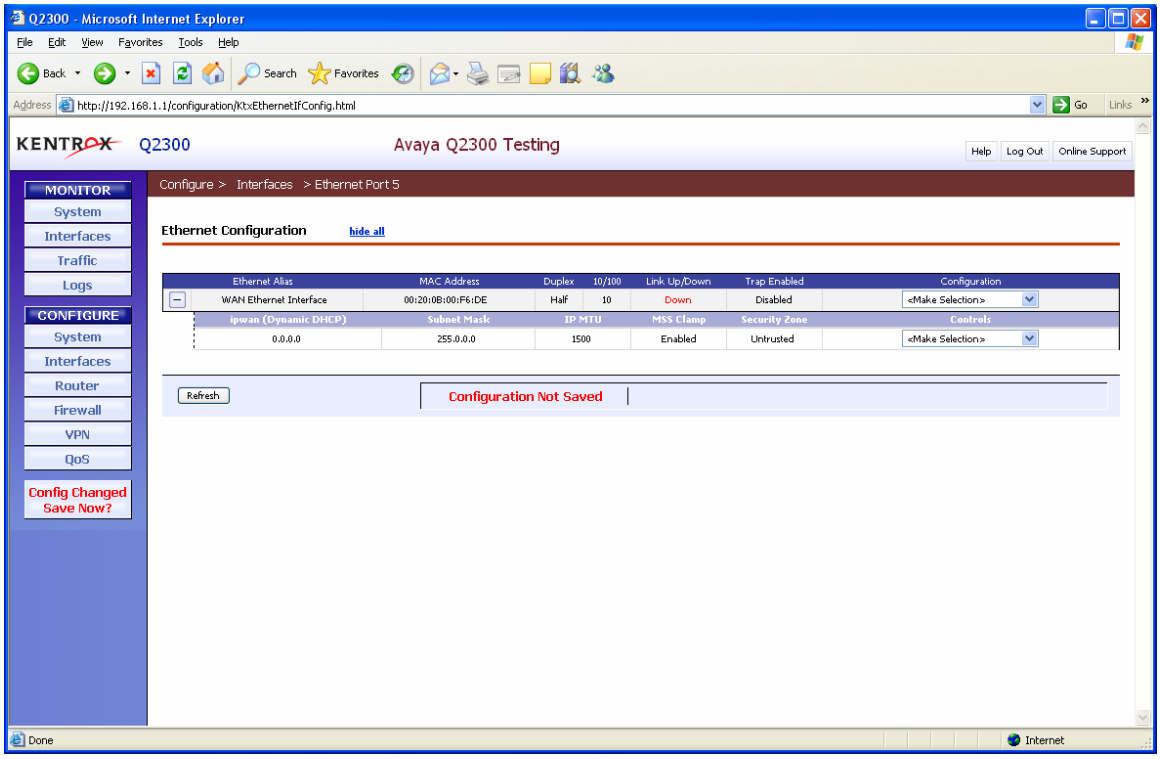
Step	Description
3.	Disable DHCP server on Avaya IP Office. From the Configuration Tree double-click **System**. Select the **LAN1** Tab. Set the **DHCP Mode** to **Disabled**. Press **OK** to continue. 

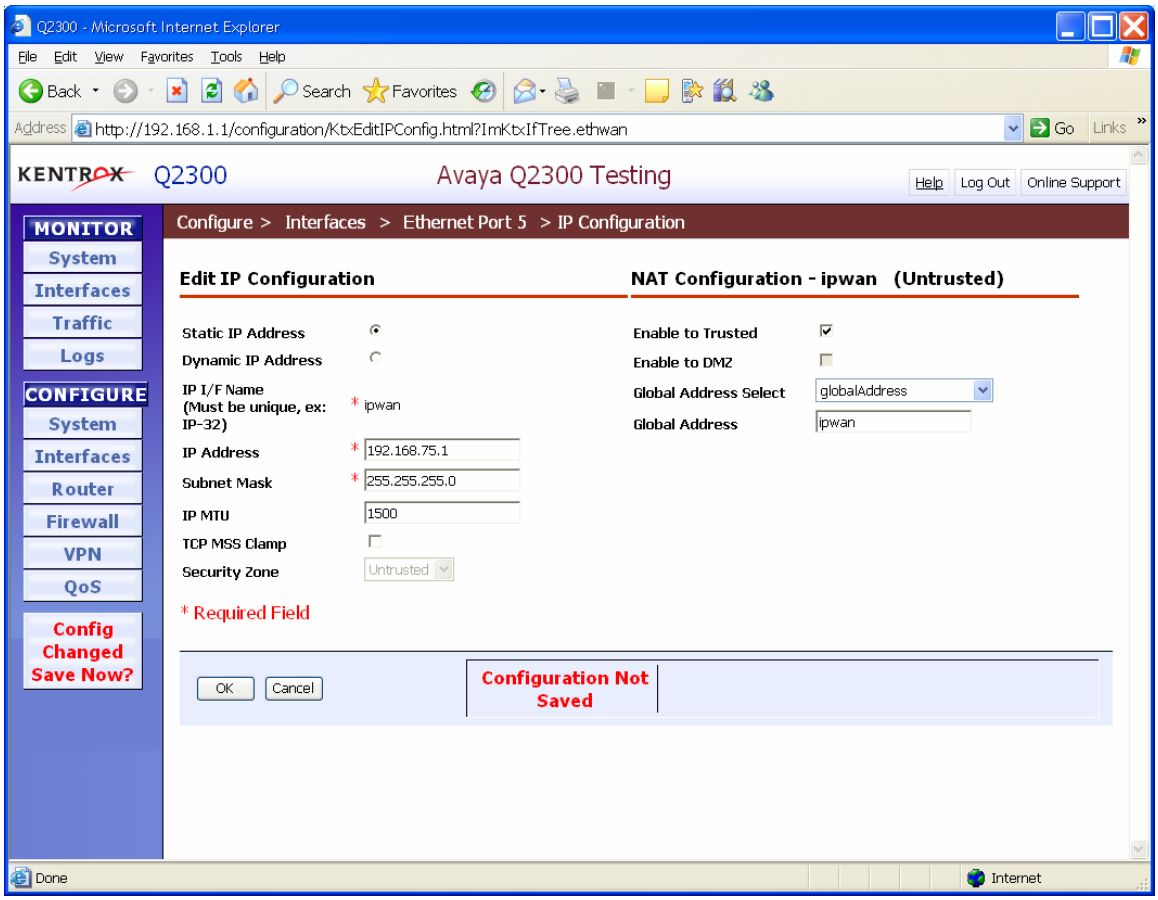
Step	Description
4.	Verify Direct Media Path. From the Configuration Tree select **Extensions**. Double-click on the IP telephone extension to check. Select the **VoIP** tab. Verify that the **Allow Direct Media box** is checked. Press **OK** to continue 

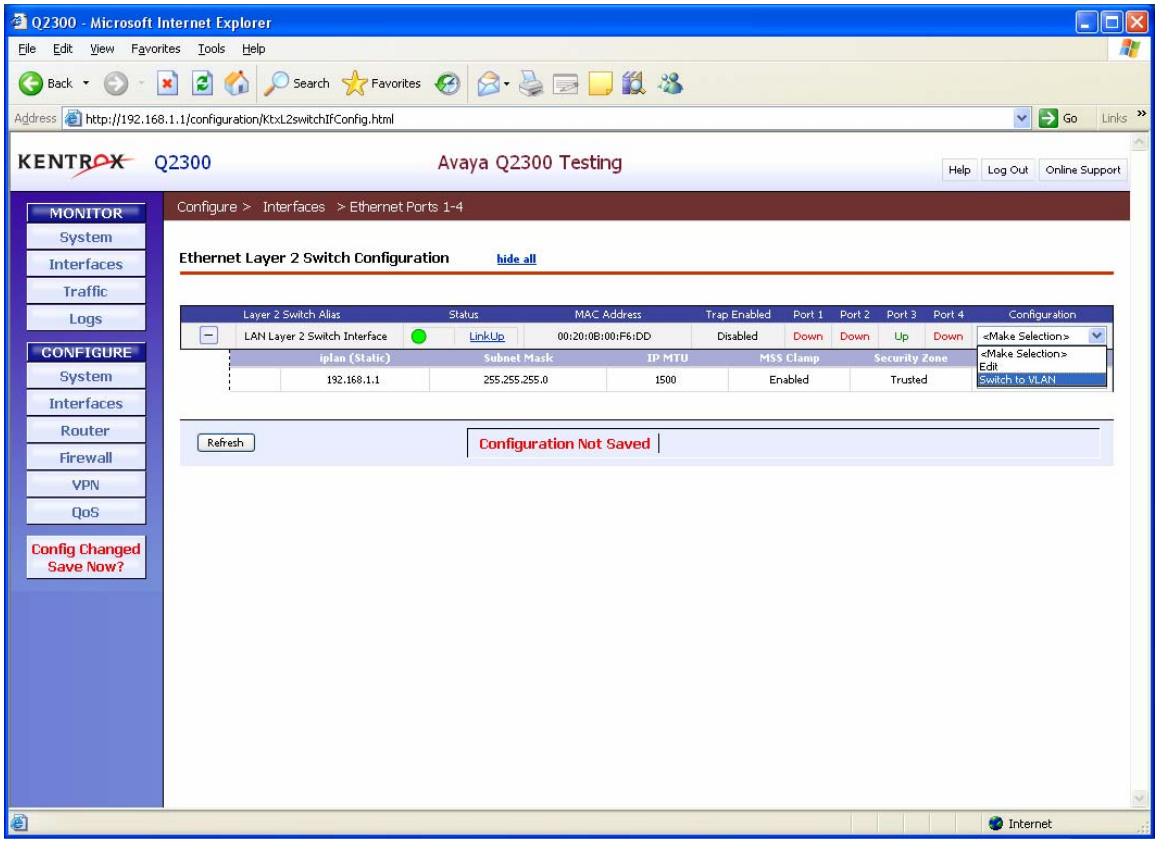
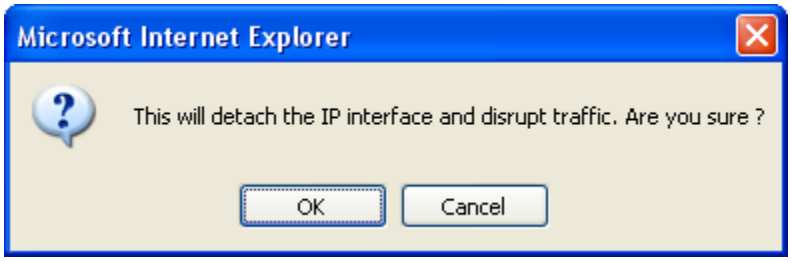
4. Configure the Kentrox Q-Series Access Router

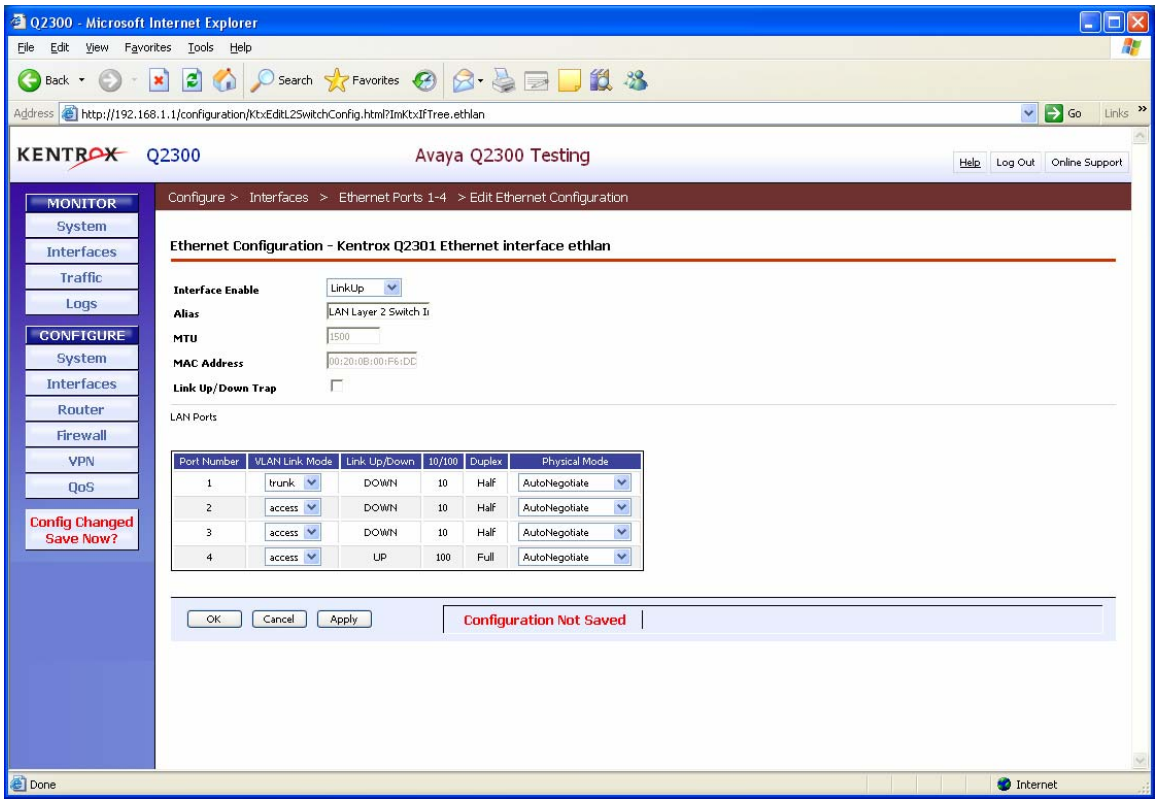
This section addresses configuring the Kentrox Q-Series Q2300 Access Router to route to the corporate site and the Avaya IP Office. Except where stated the parameters in all steps are the default settings and are supplied for reference. All required fields on the screens are indicated by a red asterisk (*).

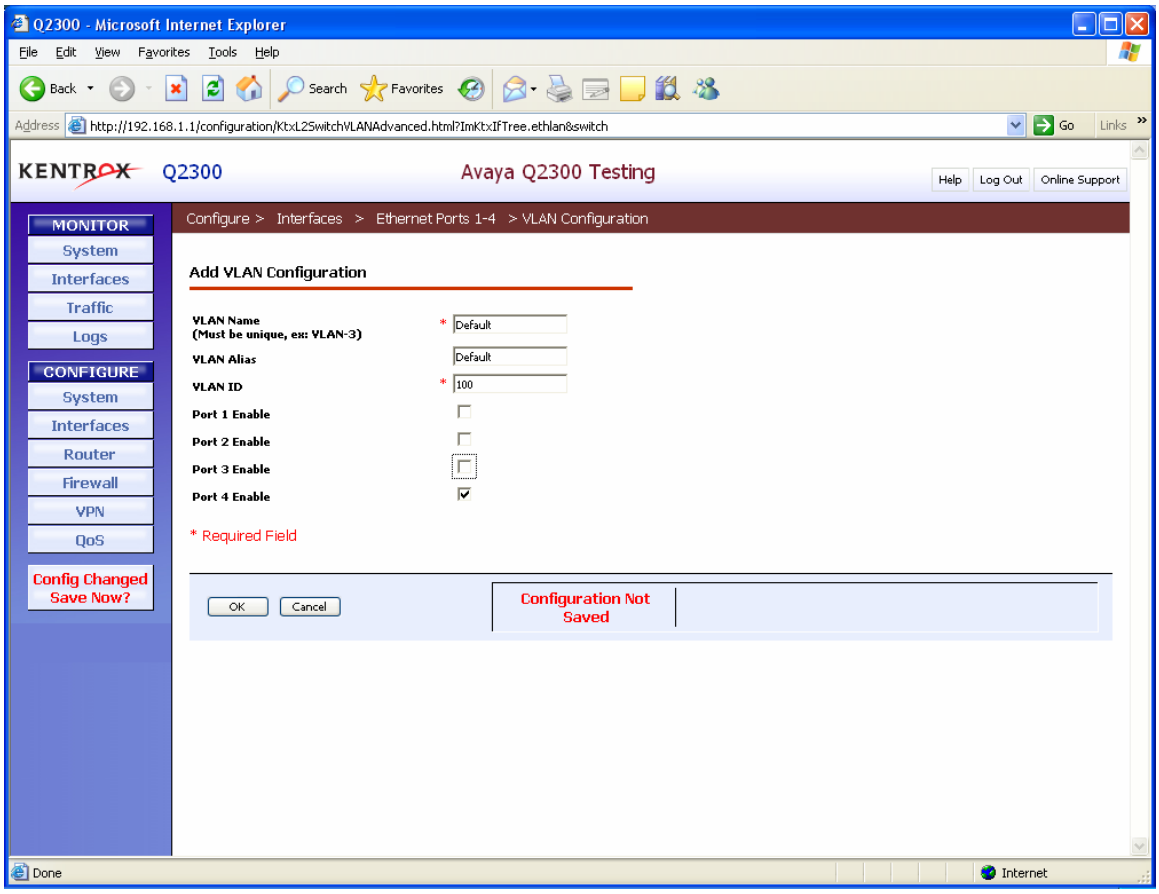
Note: For this compliance testing Port 4 was used for managing the Q2300.

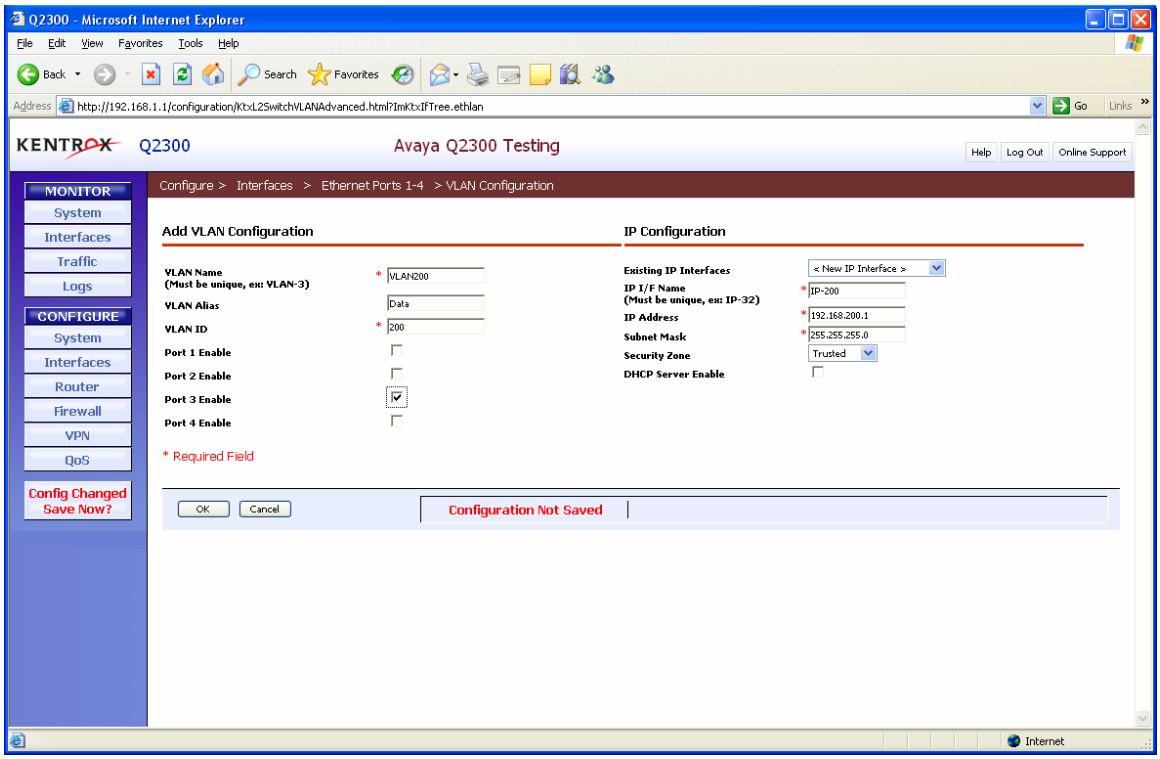
Step	Description
1.	Configure a PC to Manage the Q2300. Configure the PC to use IP address **192.168.1.50/24** with a default gateway of **192.168.1.1**, which is the Kentrox Q2300 IP Address. Connect the PC to port 4 and then use Windows Internet Explorer to browse to the IP address of the Q2300 router Administration web page. Log into the Q2300 using the appropriate credentials. When the Q2300 authentication window appears. Press **OK.**
2.	Configure the WAN interface. Port 5 is the WAN interface port on the Q2300. To configure the port select **Configure → Interfaces → Ethernet Port 5**. Click on the **Configuration** drop down list and select **Edit IP**. The interface box will automatically open. 

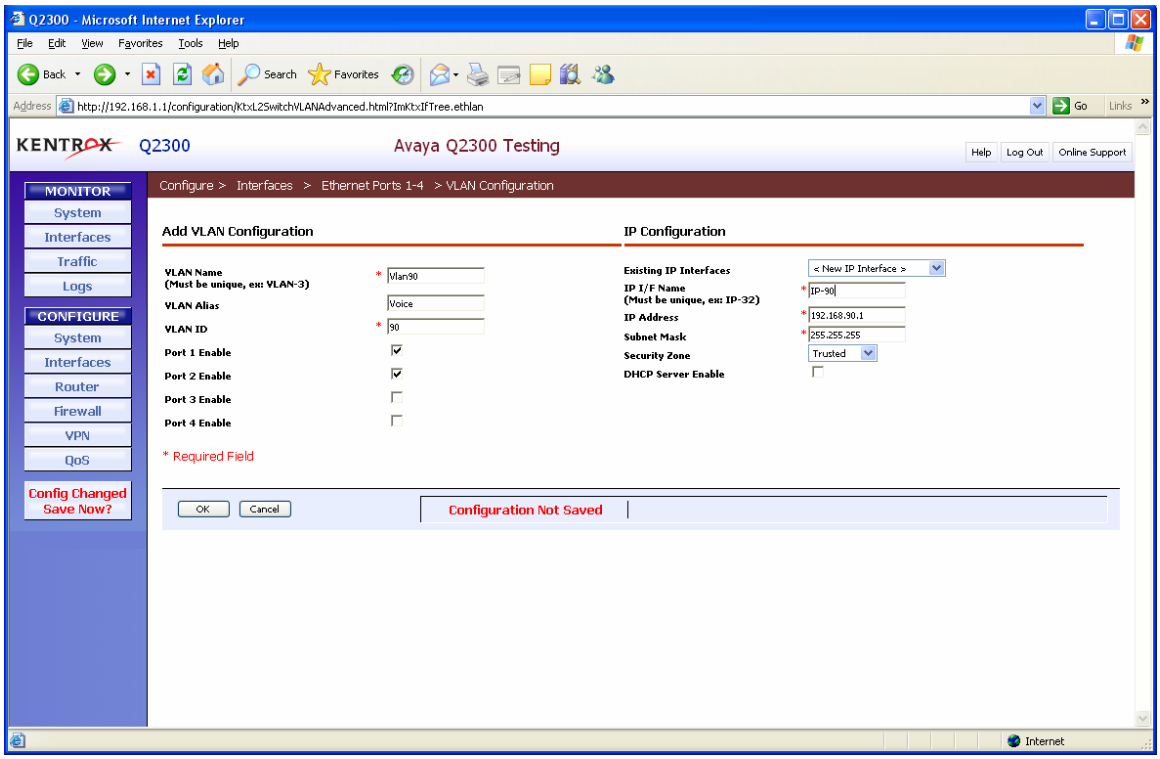
Step	Description
3.	Configure WAN IP address. Select **Static IP Address**, this will enable the **IP Address** and **Subnet Mask** fields for data entry. Enter the IP address **192.168.75.1** and Subnet Mask **255.255.255.0** Press **OK** to continue. 

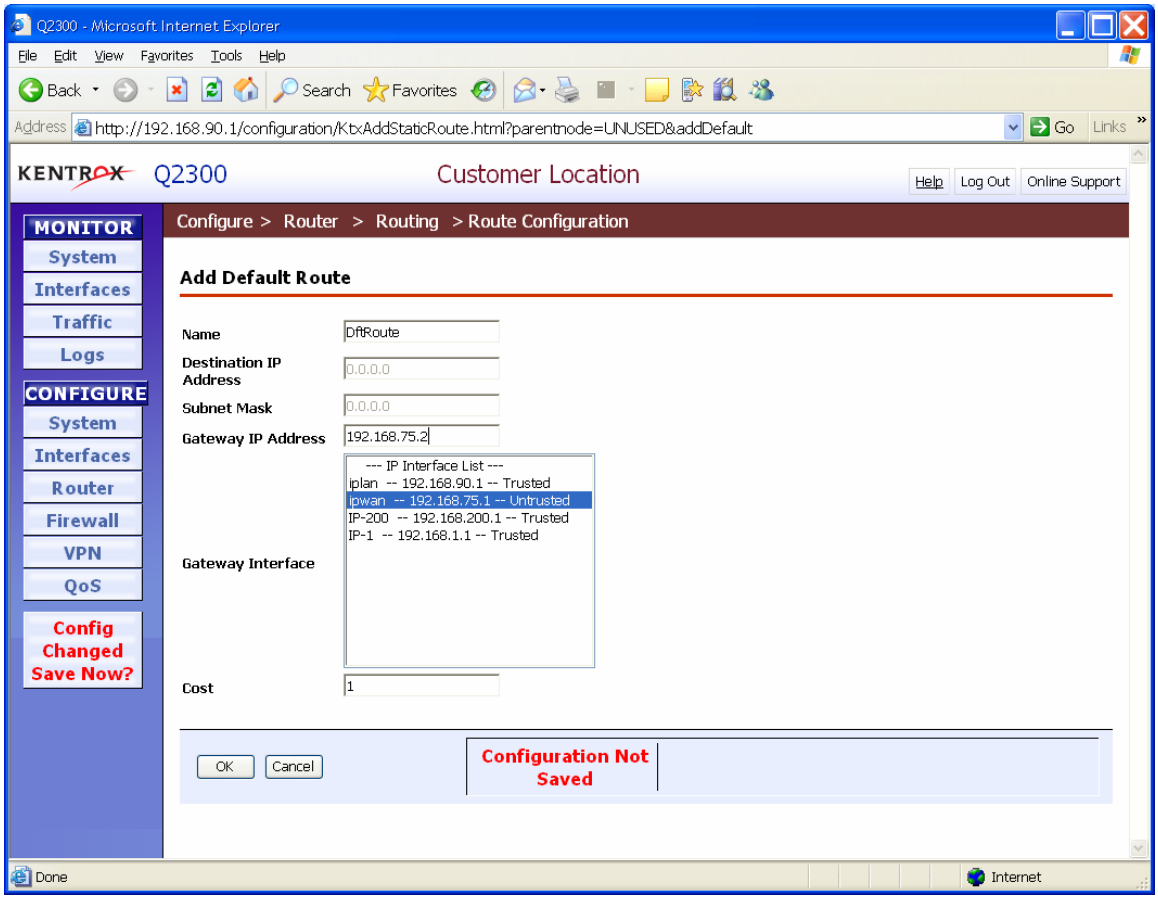
Step	Description
4.	Configure the Q2300 for VLANs. Select **Configure → Interfaces → Ethernet Ports 1-4** and click the **Configuration** drop down list for the LAN Layer-2 switch. Select **Switch to VLAN**. 
5.	The following information box will appear. Press **OK** to continue. 

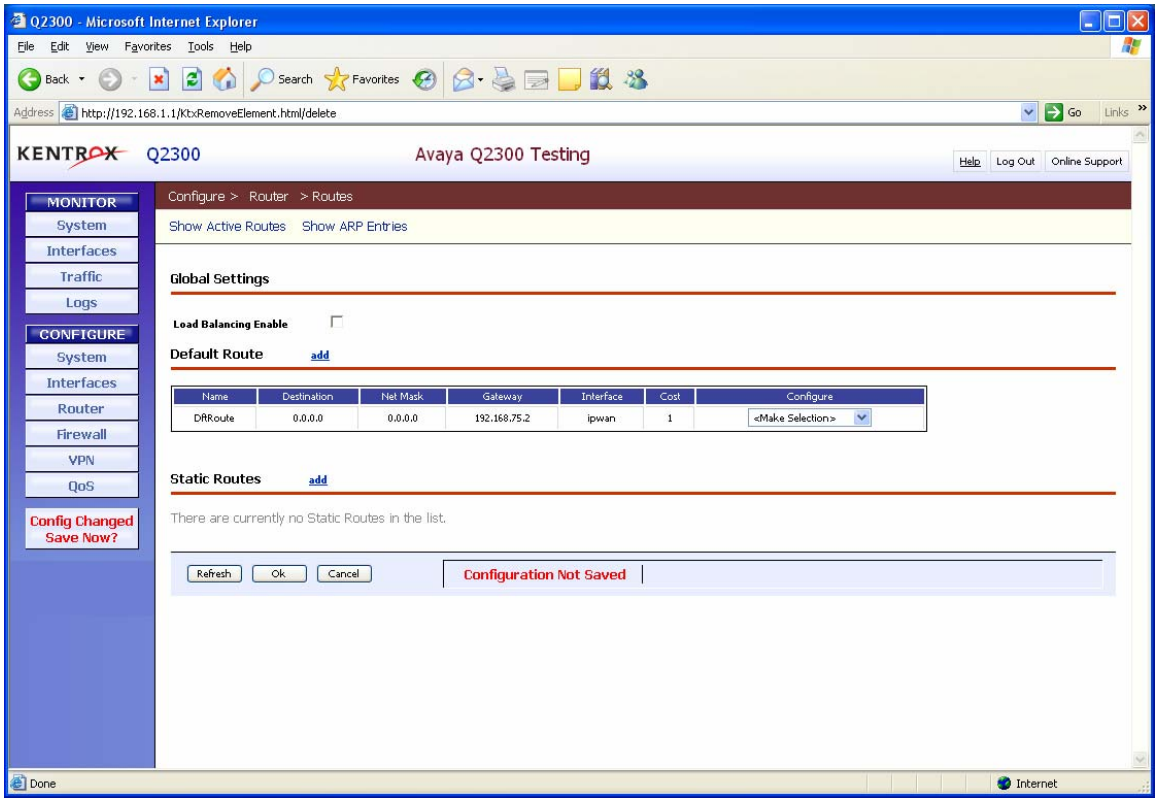
Step	Description
6.	Configure dot1Q trunk. Select **Configure → Interfaces → Ethernet Ports 1-4** and click the **Configuration** drop down list for the LAN Layer-2 switch. Select **Edit**. Select the **VLAN Link Mode** drop down list for port and select **trunk** 

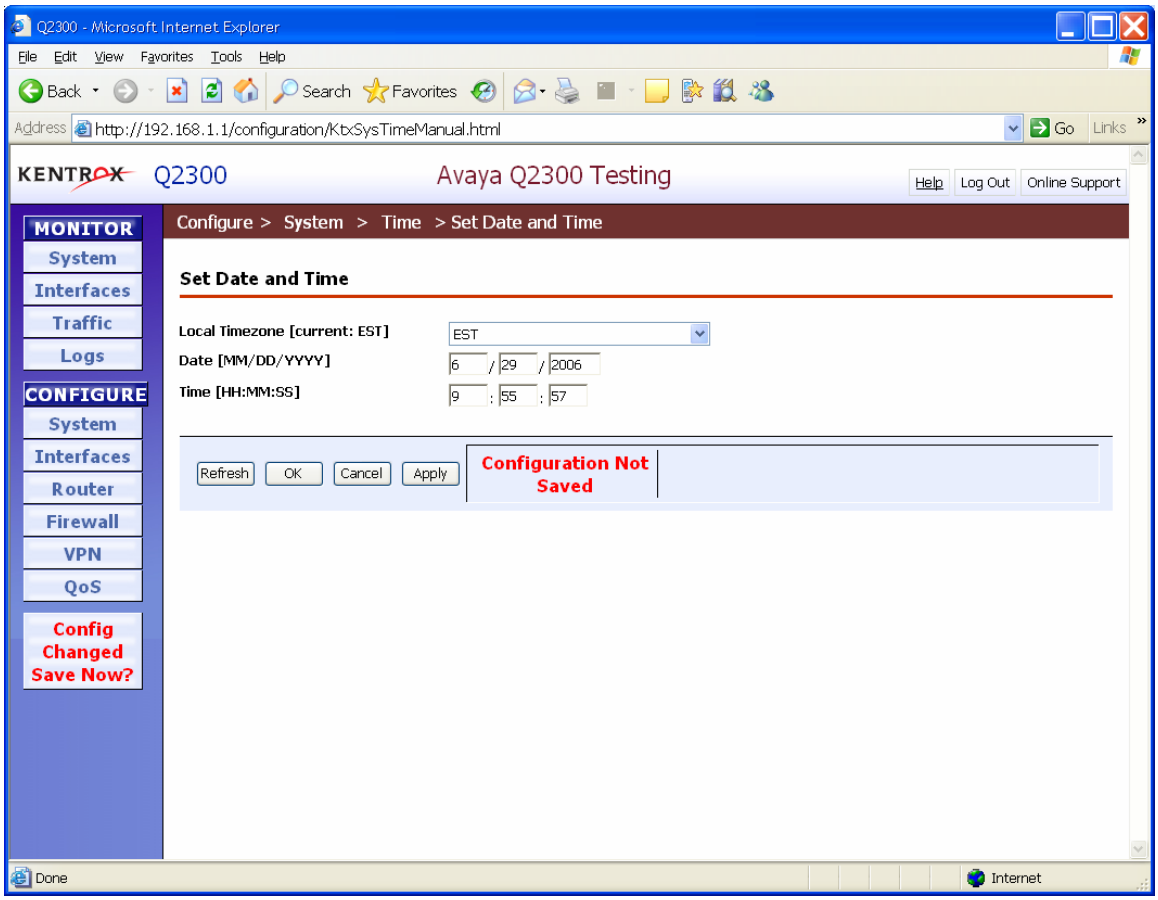
Step	Description
7.	Configure the Default VLAN. Enter information for **VLAN Name**, **VLAN Alias**, and **VLAN ID.** De-select ports **1, 2, and 3**. Press **OK** to continue. Enter a unique string for the **VLAN Name** and **VLAN Alias** as well as a unique **VLAN ID** number. Press **OK** to continue. 

Step	Description
8.	Configure Data VLAN. Select **Configure → Interfaces → Ethernet Ports 1-4** and click on the **Configuration** drop down list for the LAN Layer 2 switch. Select **Add VLAN**. Configure a unique **VLAN Name** and **VLAN Alias** as well as the unique **VLAN ID**. Enter the **IP I/F Name**, **IP Address,** and **Subnet Mask**. Check the **Port 3 Enable** box. Disable the DHCP server on this VLAN by removing the check in the **DHCP Server Enable** option. Press **OK** to continue. 

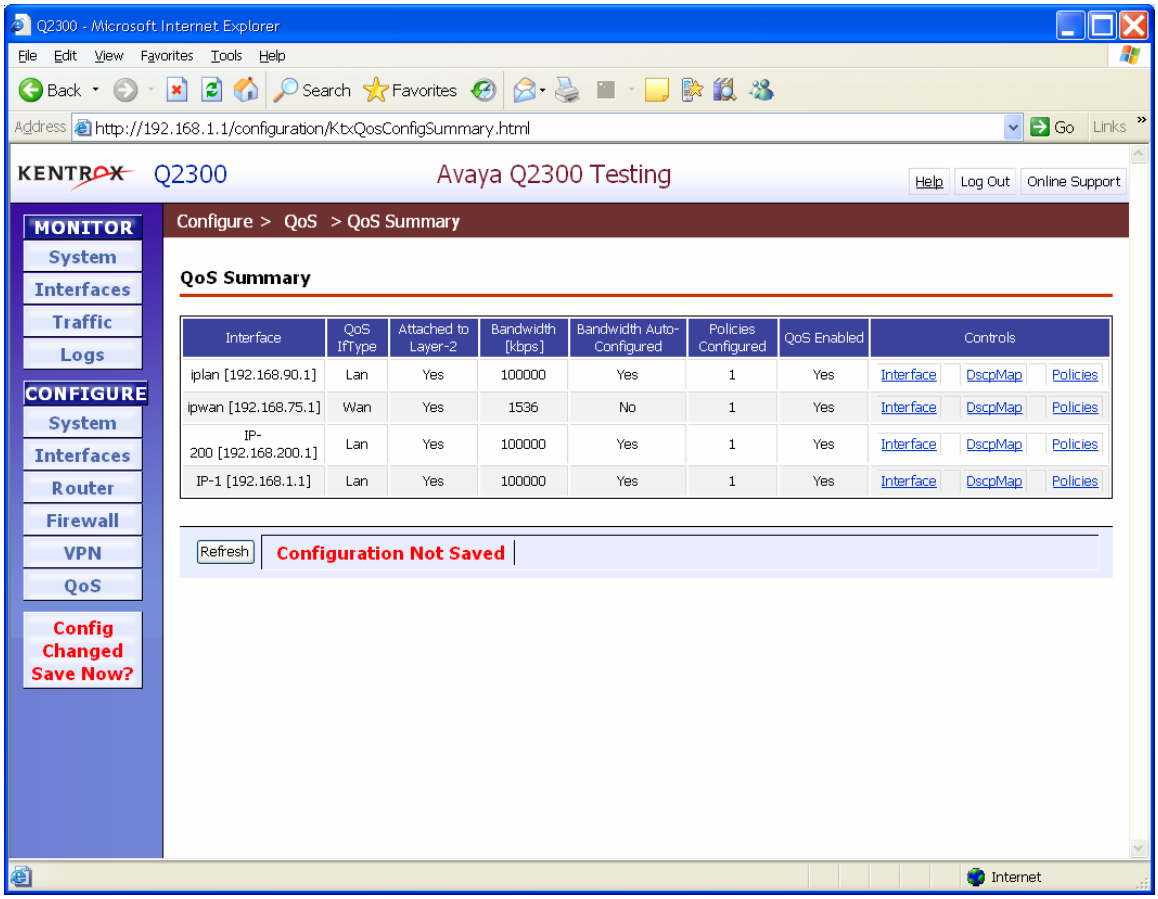
Step	Description
9.	Configure Voice VLAN. Select **Configure → Interfaces → Ethernet Ports 1-4** and click on the **Configuration** pull down menu for the LAN Layer 2 switch and Select **Add VLAN**. Configure a unique **VLAN Name** and **VLAN Alias** as well as the unique **VLAN ID**. Enter the **IP I/F Name**, **IP Address,** and **Subnet Mask**. Check the **Port 1 Enable and Port 2 Enable** boxes. Disable the DHCP server on this VLAN by removing the check in the **DHCP Server Enable** option. Press **OK** to continue. 

Step	Description
10.	Set the default gateway. Select **Configure → Router → Routes** and select the **Add** hyperlink next to the "Default Route" title. Provide a valid **Name** and enter the gateway IP address in the **Gateway IP address** field. Select the **ipwan** port in the **IP Interface** list. Press **OK** to continue. 

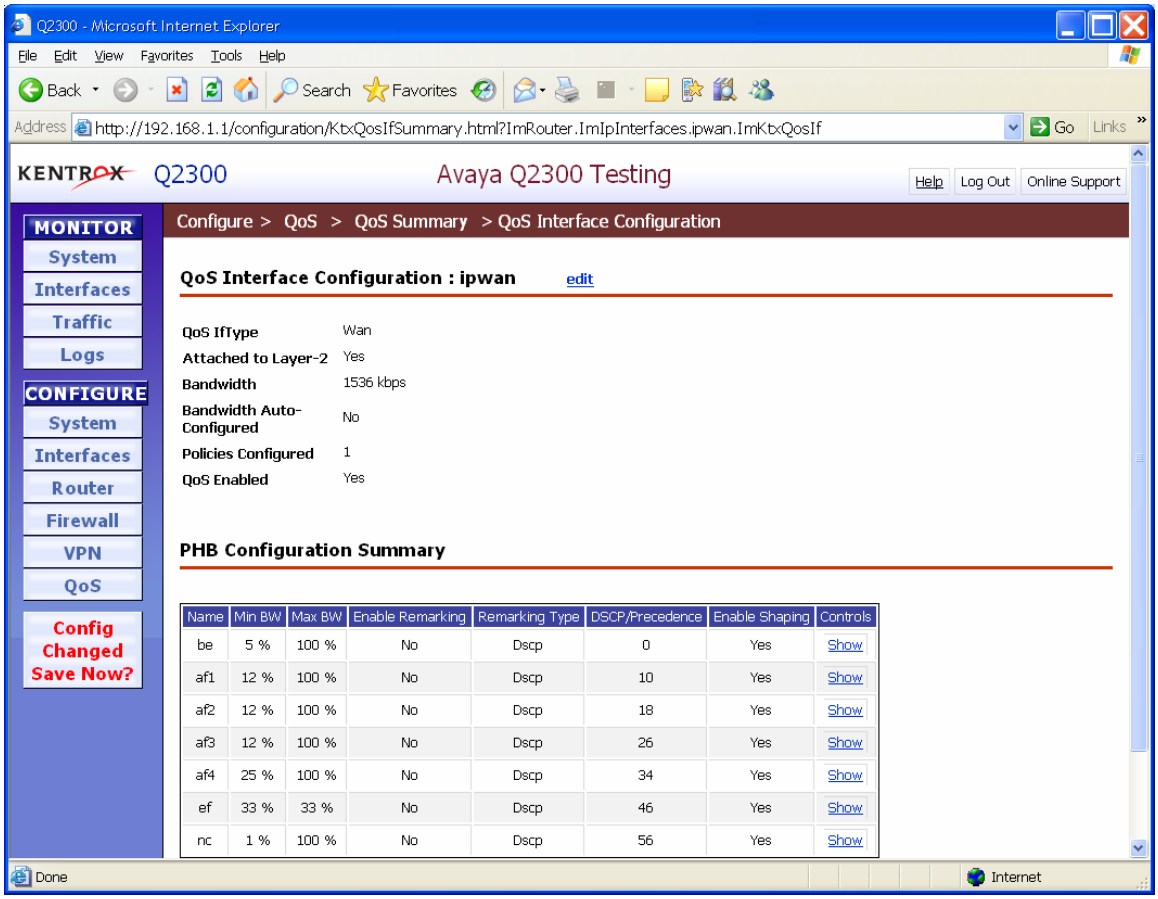
Step	Description
11.	Verify the default IP route has been added. To display static routes, select **Configure → Router → Routes.** Press **Cancel** to continue. 

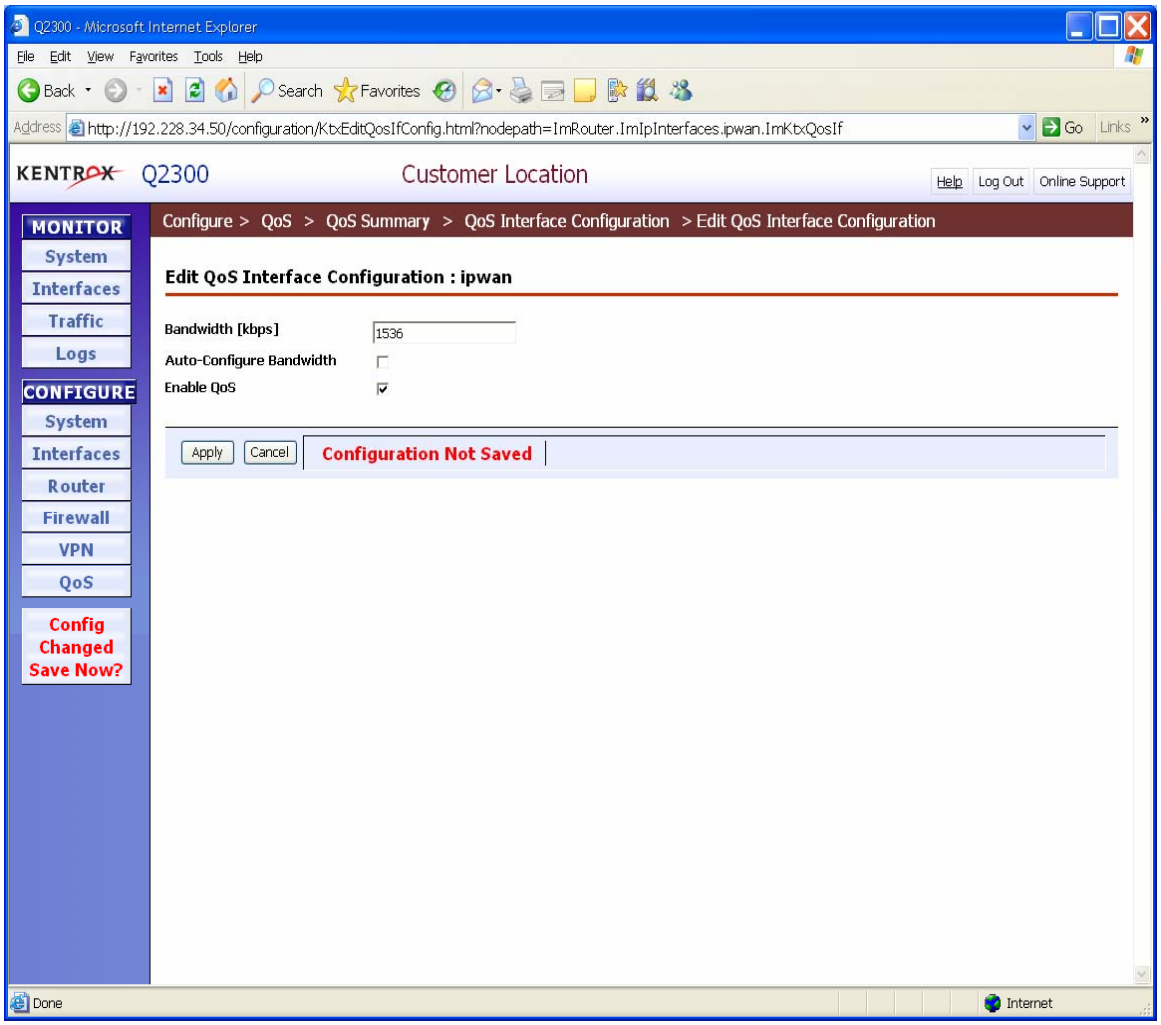
Step	Description
12.	Set the time and date. Select **Configure → System → Time → Set Time and Date**. If needed, the SNTP server can be selected. Follow the instructions for setting the time and date. Press **Apply** and then **OK** to continue. 

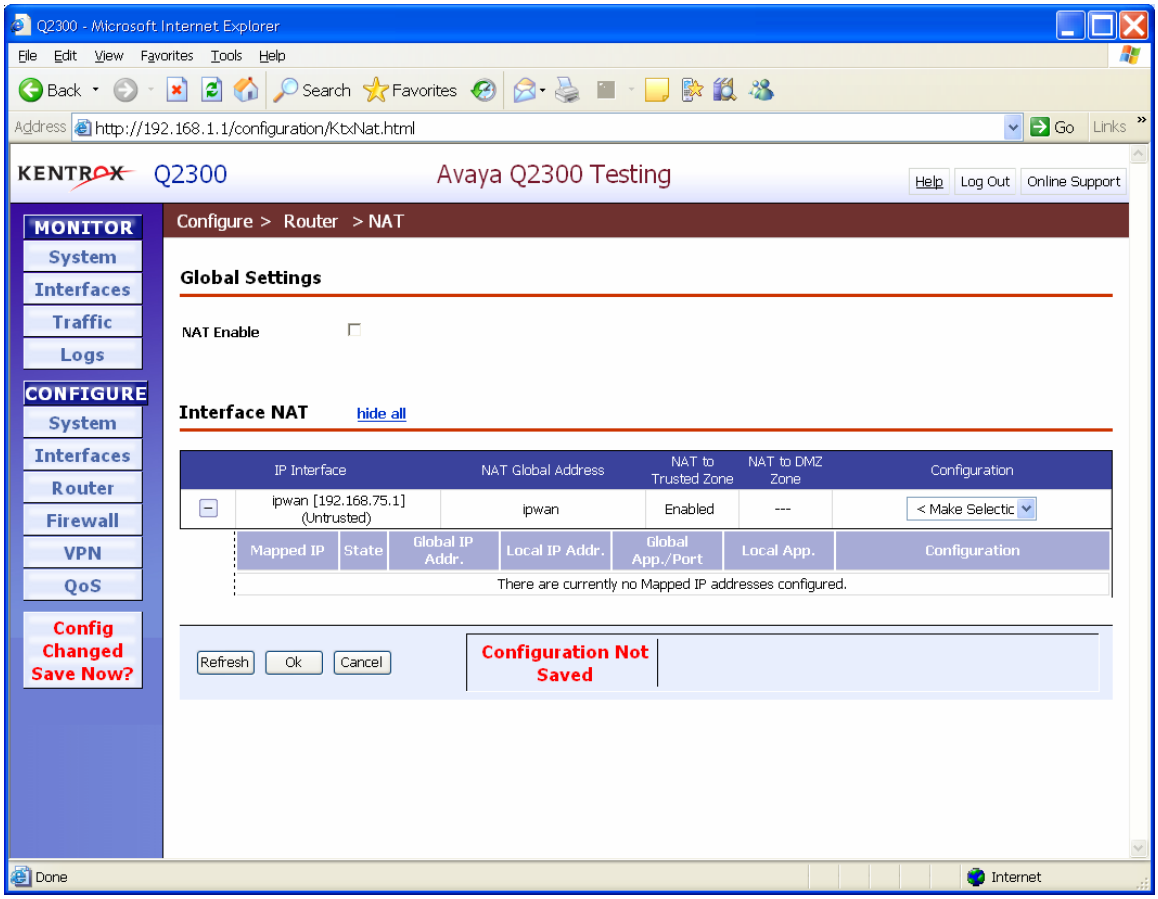
Step	Description
13.	Configure the QoS Parameters. Select **Configure → QoS → QoS Summary.** QoS is typically performed on the outbound side of the router, so click on the interface hyperlink for the **ipwan Interface.**

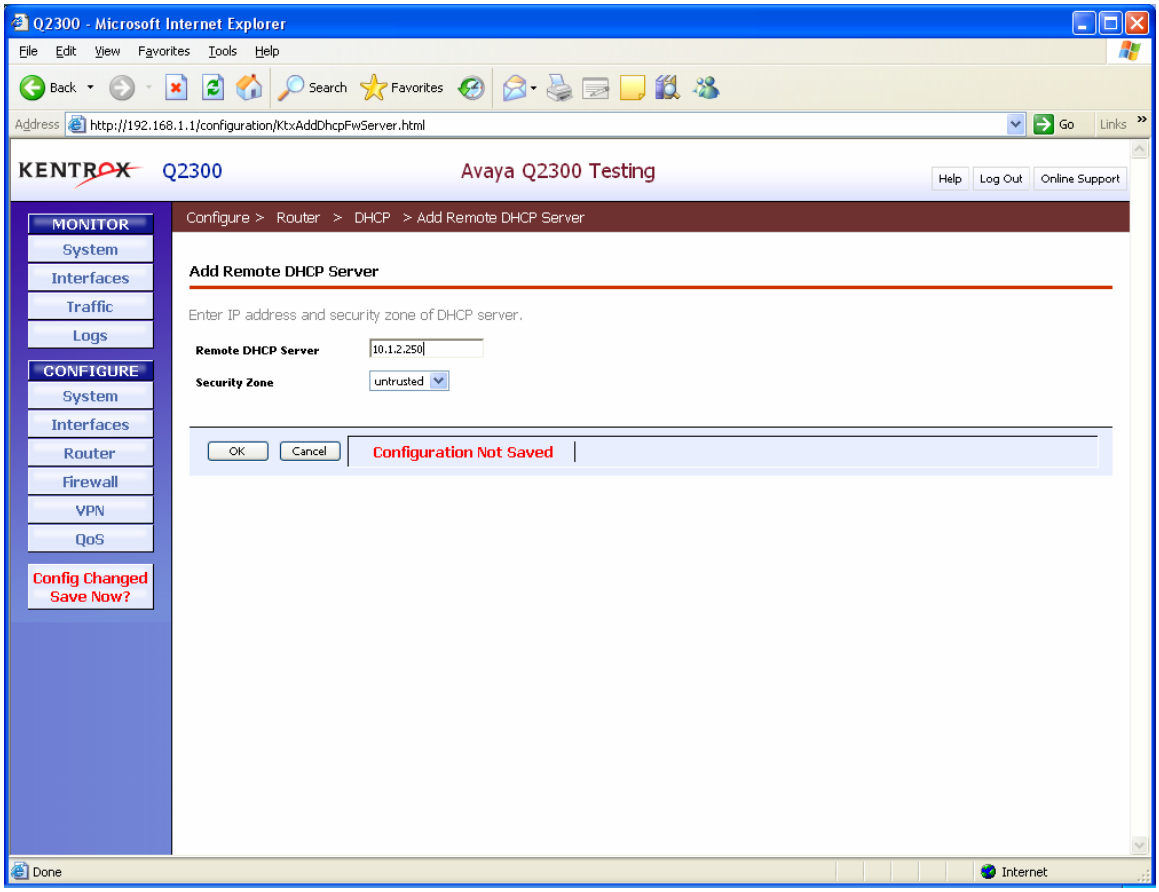


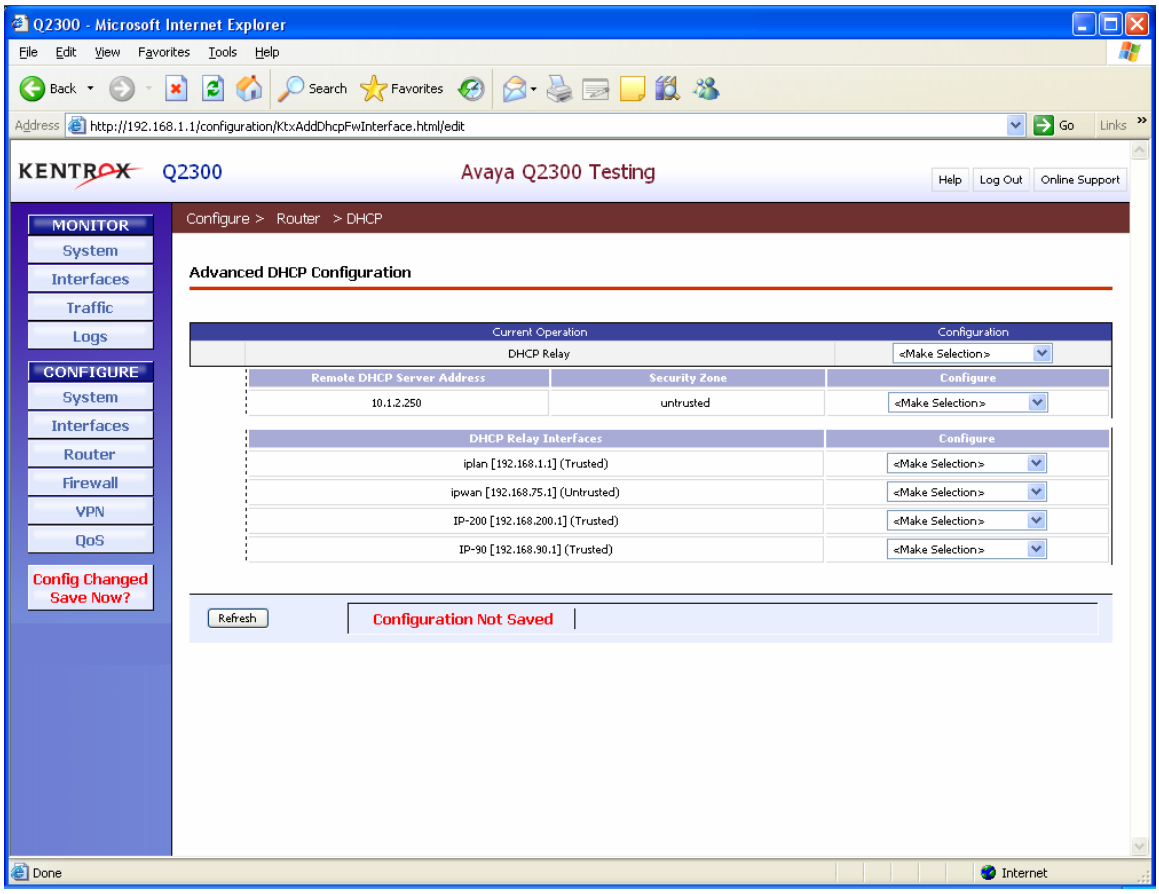
Step	Description
14.	Verify bandwidth settings for the **ipwan** Interface. For compliance testing the default values were used. Refer to the Kentrox support page to change these settings . **Configure → QoS → QoS Summary → Controls** and select the Interface hyperlink for the **ipwan Interface** and then **edit**

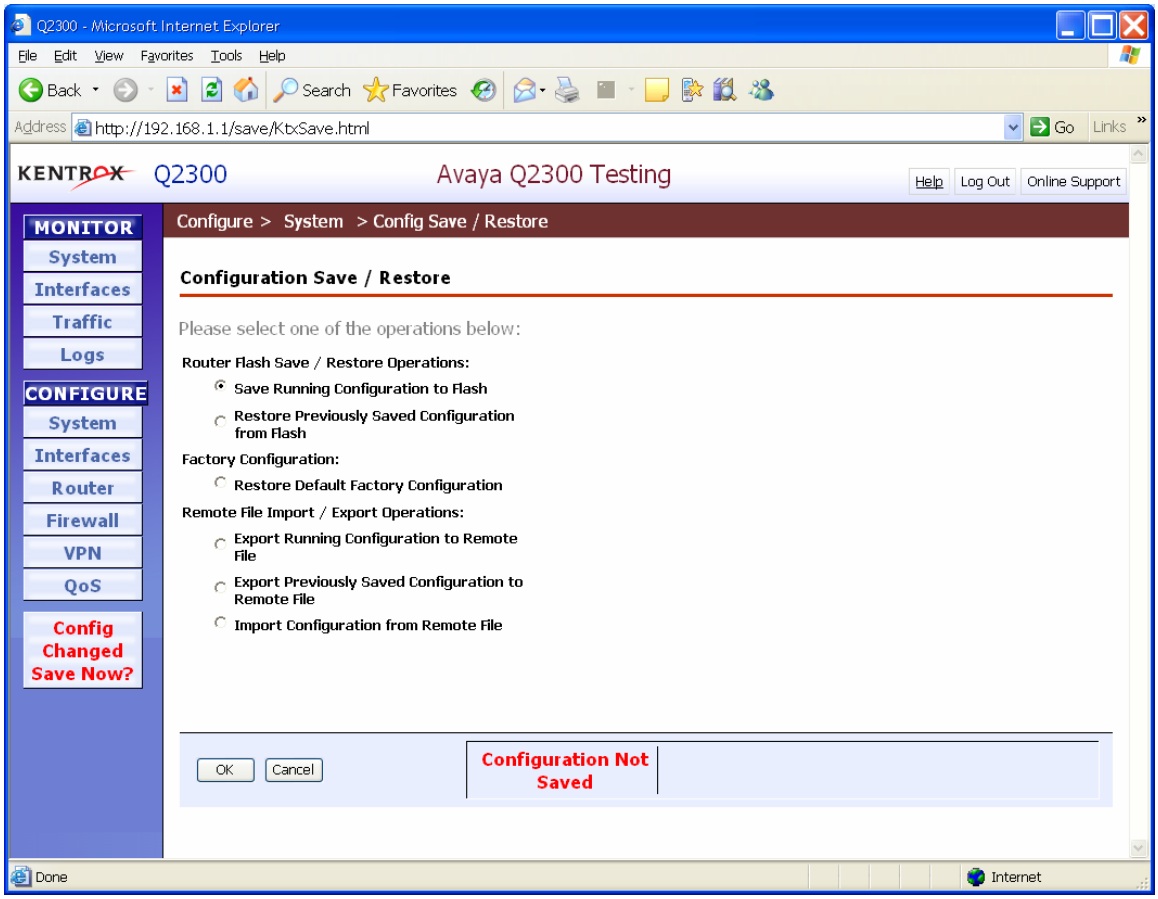


Step	Description
15.	Verify QoS rate limit setting. Select **Configure → QoS → QoS Summary** and select the Interface hyperlink for the **ipwan Interface** and then **edit** next to the ipwan title. Press **Apply** to continue. The default setting of 1536 kbps was used for the compliance testing. 

Step	Description
16.	Disable NAT. Select **Configure → Router → NAT** and de-select the **NAT Enable** check box. Press **OK** to continue. 

Step	Description
17.	Disable the DHCP server function and enable DHCP Relay functionality. Select **Configure → Router → DHCP** and click on the **Configuration** drop down list. Select **Enable DHCP Relay**. Once in DHCP Relay Mode, click on the **Configuration** drop down list and select **Add Remote DHCP Server**. Enter the IP address of the remote DHCP server **10.1.2.250.** Click OK to continue. 

Step	Description
18.	Add DHCP Relay Interfaces. Select **Configure → Router → DHCP** and click on the **Configuration** drop down list. Select **Add DHCP Relay Interface.** Add interfaces for **192.168.90.1 (Voice) and 192.168.200.1 (Data).** 

Step	Description
19.	Save the configuration. Once the configuration changes are complete, save the configuration to Flash. Click on the RED "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**. 

5. Configure the Avaya C364T-PWR switch

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 #**
2.	Enter **Configure** mode. C360-1# **configure** C360-1(configure)#
3.	Create VLANS **VlanVOICE** and **VlanDATA.** C360-1(configure)# **set vlan 90 name vlanVOICE** C360-1(configure)# **set vlan 200 name vlanDATA**
4.	Set trunking on ports **1/2** and **1/48.** C360-1(configure)# **set trunk 1/48 dot1q** C360-1(configure)# **set trunk 1/2 dot1q**
5.	Set port binding to port **1/48.** C360-1(configure)# **set port vlan-binding-mode 1/48 bind-to-all**
6.	Assign VLANS to ports **1/1** and **1/2.** C360-1(configure)# **set port vlan 90 1/1** C360-1(configure)# **set port vlan 200 1/2**
7.	Assign Static VLAN to port **1/2.** C360-1(configure)# **set port static-vlan 1/2 90**

6. 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. Summit300-48:1 # **show port 1:3 info detail** Repeat for ports 1:4,1:5,1:17,1:18,1:19,1:20,1:21,1:22,1:24
3.	Create the **Voice VLAN and interface**. 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 1:3,1:5,1:17,1:19,1:20** Summit300-48:1# **configure vlan default delete ports 1:22, 1:24**
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 1:17,1:19,1:48**
8.	Assign Port 1:19 to **qosprofile QP7.** Summit300-48:34 # **configure ports 1:19 qosprofile QP7**
9.	Enable **DiffServ** examination on port 1:19. Summit300-48:34 # **enable diffserv examination ports 1:19**
10.	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**
11.	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**
12.	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**
13.	Assign ports to the **Data VLAN** Summit300-48:34 # **configure vlan30 add ports 1:3,1:4**
14.	Create **WAN VLAN** 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**

Step	Description
15.	Add the IP address for the **WAN VLAN,** and enable IP forwarding **Note:** subnets/VLANs will not Route unless to enable IP forwarding for that vlan Summit300-48:34 # **configure vlan240 ipaddress 192.168.240.1/30** Summit300-48:34 # **enable ipforwarding vlan240**
16.	Assign ports to the **WAN VLAN** Summit300-48:34 # **configure vlan240 add ports 1:24**
17.	Add **static routes** for the local corporate networks going to the remote site. 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**
18.	Create **10 VLAN** Summit300-48:31 # **create vlan vlan10** Summit300-48:32 # **configure vlan10 tag 10**
19.	Add the IP address for the **10 VLAN,** and enable IP forwarding **Note:** subnets/VLANs will not Route unless IP forwarding is enabled for that vlan Summit300-48:34 # **configure vlan10 ipaddress 10.1.2.2** Summit300-48:34 # **enable ipforwarding vlan10**
20.	Assign ports to the **10 VLAN** Summit300-48:34 # **configure vlan10 add ports 1:5**

7. 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.

7.1. 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,
- Verification of the DHCP relay configuration,
- 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

7.2. 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.

8. Verification Steps

This section provides the steps for verifying end-to-end network connectivity and QoS in the field from the perspective of the Q2300 router. 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. Verify DHCP relay on the Q-Series is functioning by confirming that the IP Telephones on the Q2300 side of the network receive their IP addresses from the DHCP server on the corporate side of the network

3. Check that the Avaya IP Telephones have successfully registered using the IP Office **System Monitor**. See section 9.1.

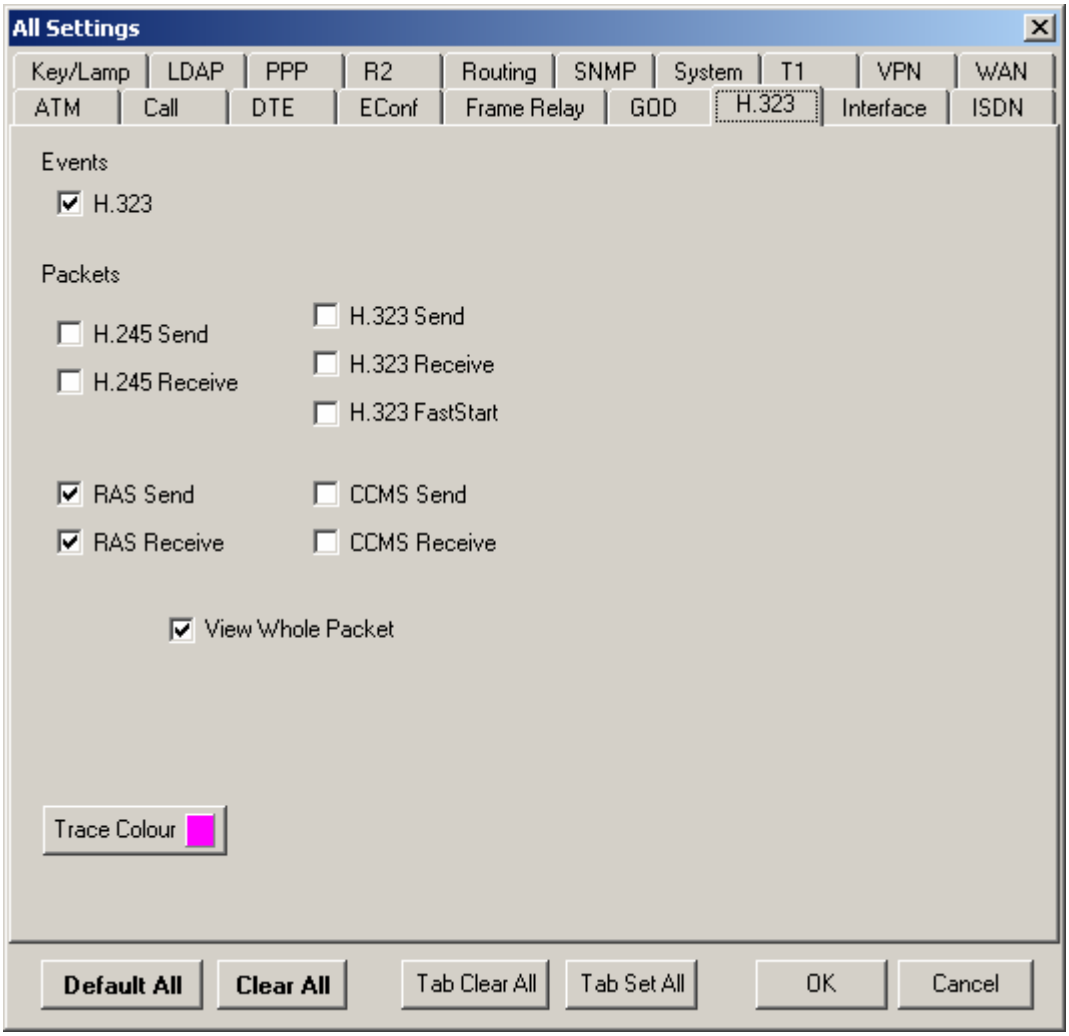
4. Place internal and external calls between the Digital telephone and IP telephones at each site.

9. Troubleshooting

9.1. 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.



9.2. Miscellaneous Troubleshooting

1. If the voice quality is poor, check the QoS configuration in the Q2300 browser interface in section 4.13.

2. If a Q2300 router is unable to communicate with any of the aforementioned IP devices and interfaces, check the routing and status of the Ethernet and WAN interfaces through the Q2300 browser interface in section 4.3.

10. 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

11. Conclusion

These Application Notes describe the configuration steps required for integrating the Kentrox Q-Series Q2300 Router into a small office and/or low traffic/bandwidth Avaya IP Office infrastructure. For the configuration described in these Application Notes, the Q-Series router 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.

12. 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/Q2300/

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 Developer*Connection* Program at devconnect@avaya.com.