



Avaya Solution & Interoperability Test Lab

Application Notes for VoIP over a PPP Link with Quality of Service using Kentrox Q-Series Routers with Avaya IP Office - Issue 1.0

Abstract

These Application Notes describe a configuration for supporting Voice over IP (VoIP) over a PPP link with Quality of Service (QoS) on Kentrox Q-Series Routers connected to an Avaya IP Telephony infrastructure intended for small office scenarios. The Kentrox Q-Series Q2400 and Q2200 Routers were compliance-tested with Avaya IP Office. Emphasis was placed on verifying voice quality in a small office scenario in a converged network. QoS based on Layer 3 Differentiated Services was implemented across the network to prioritize voice traffic over the WAN. 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 configuration for supporting Voice over IP (VoIP) over a private line PPP link with Quality of Service (QoS) on Kentrox Q-Series Routers connected to an Avaya IP Telephony infrastructure. The Kentrox Q-Series Q2400 and Q2200 Routers were compliance-tested with an Avaya IP Office.

Q-Series Q2200 T1 QoS Access Router

The Q-Series Q2200 Access Router provides VPN functionality and supports QoS based on DiffServ over its WAN link. The Q2200 supports PPP and Frame Relay encapsulation.

Q-Series Q2400 QoS Access Router

The Q-Series Q2400 QoS Access Router is a multi-port router with two T1 ports and one Ethernet WAN port. It provides the same functionality as the Q2200.

Compliance testing emphasis was placed on verifying voice quality in a small office scenario. QoS based on Layer 3 Differentiated Services was implemented across the network to prioritize voice traffic over the WAN.

The configuration in **Figure 1** shows a corporate site connected to a branch office site via a private line PPP link. The corporate site consists of an Avaya IP Office 412 connected to the Kentrox Q2400 router, which in turn is connected to the WAN. The branch office site consists of an Avaya IP Office 403 and it is also connected to the WAN via a Kentrox Q2200 router. Each site contains a Layer-2 managed Ethernet switch to connect the Avaya IP Telephones and the Avaya IP Office. The corporate site also provides a DHCP server for functions including assigning IP network parameters and VLAN information, and serving Option 176 settings to the Avaya IP Telephones. DHCP was used to exercise DHCP relay on the Kentrox router at the branch office. The voice and data traffic were separated onto different VLANs.

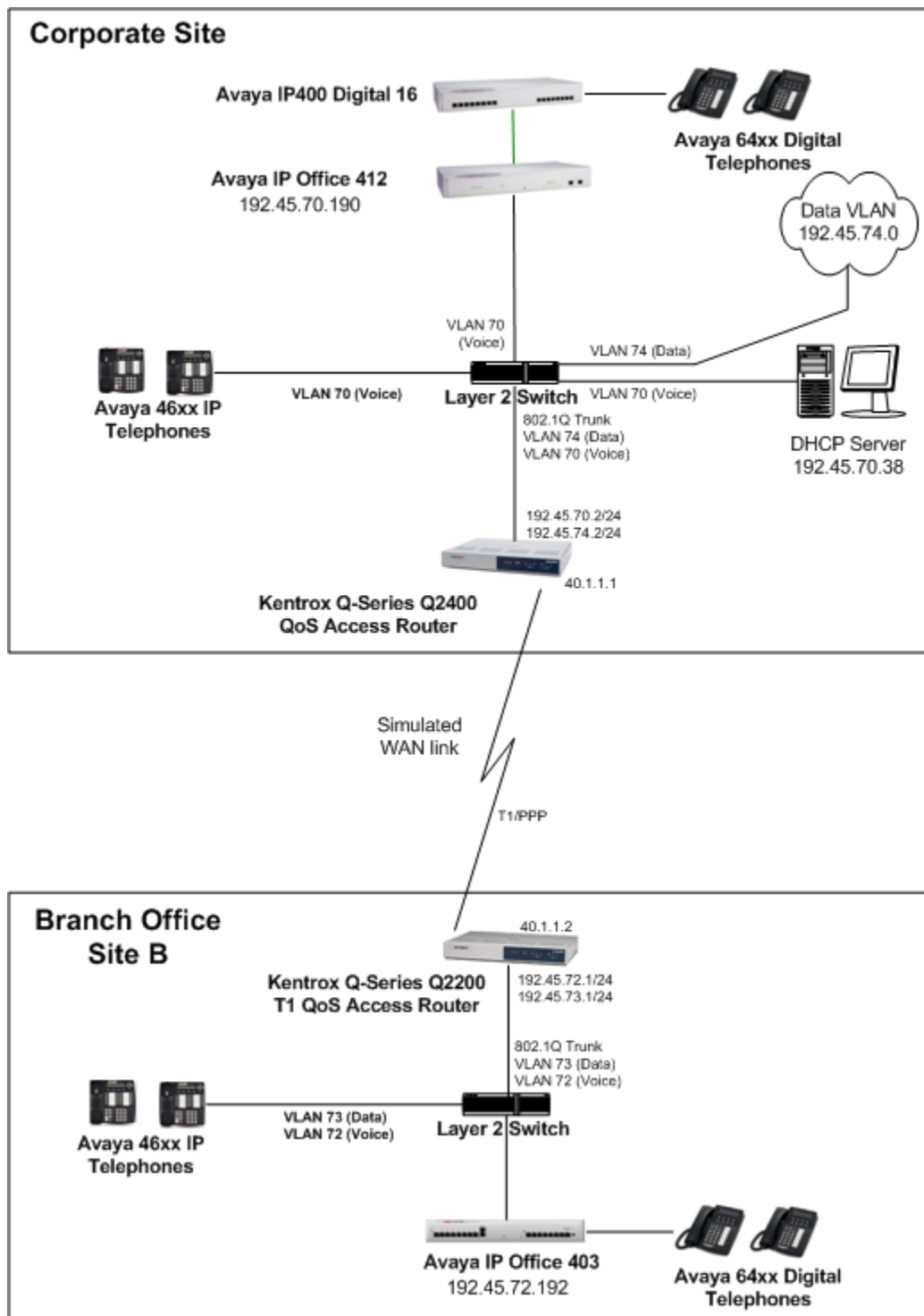


Figure 1: Network Configuration

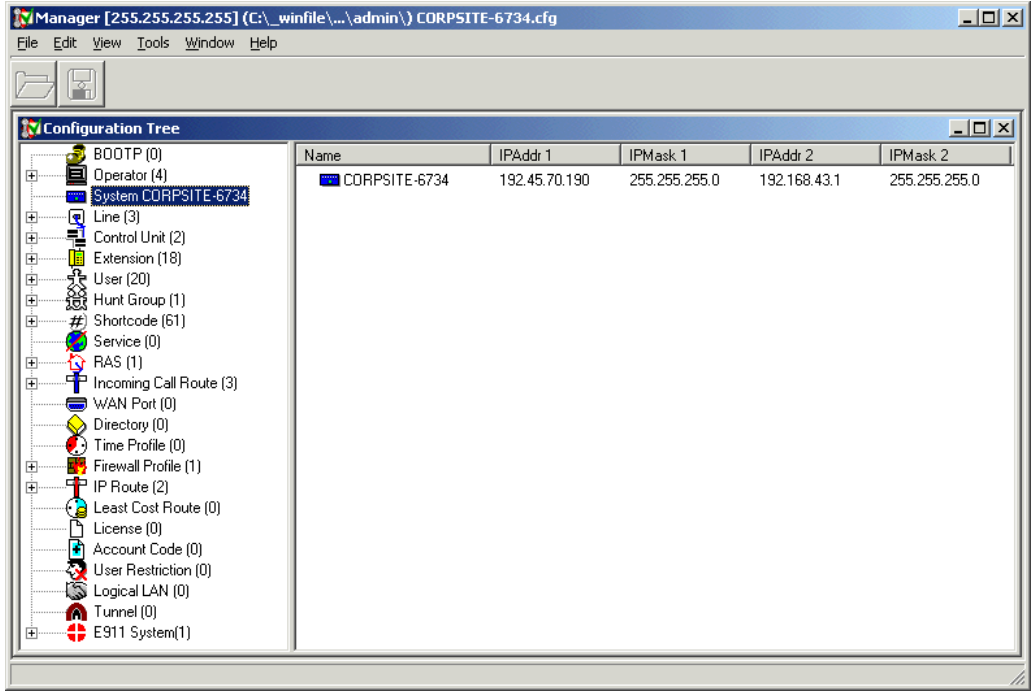
2. Equipment and Software Validated

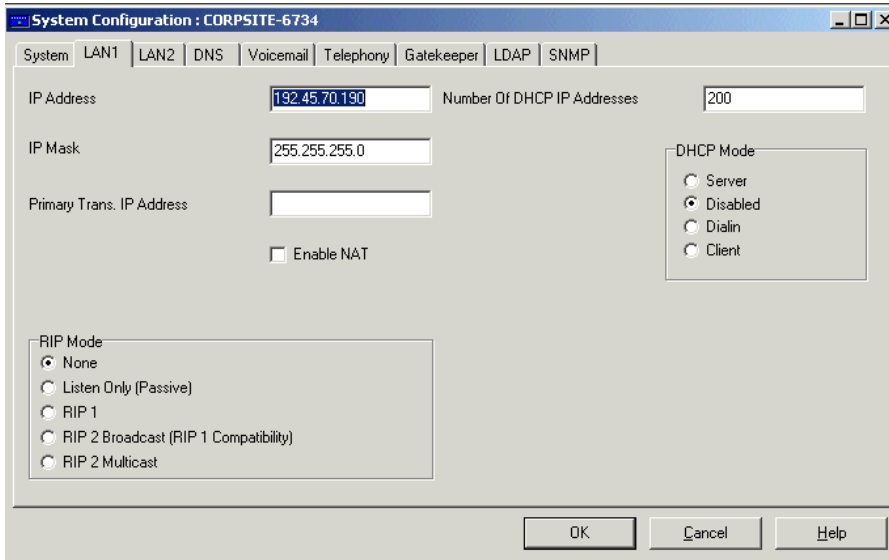
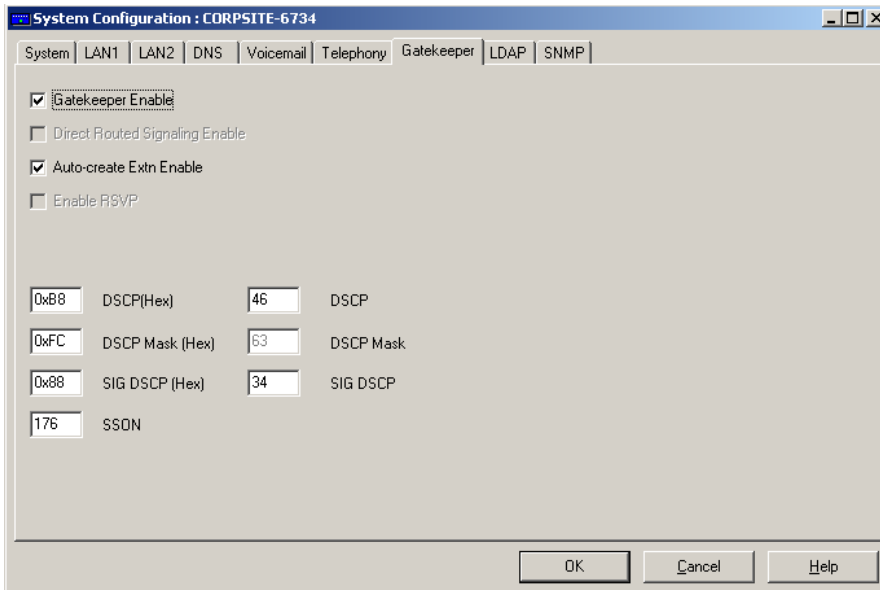
The following equipment and software were used for the sample configuration provided:

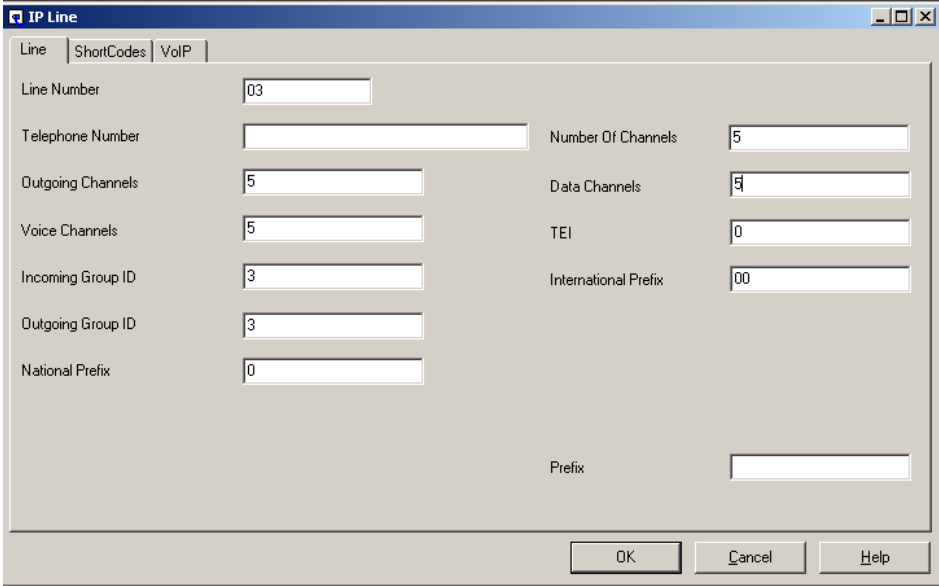
Equipment	Software
Avaya IP403 Office	2.1(27)
Avaya IP403 Office	2.1(27)
Avaya 4612, 4624 IP Telephones	1.81
Avaya 6400 Series Digital Telephones	--
Kentrox Q-Series Q2400 QoS Access Router	1.3
Kentrox Q-Series Q2200 T1 QoS Access Router	1.3

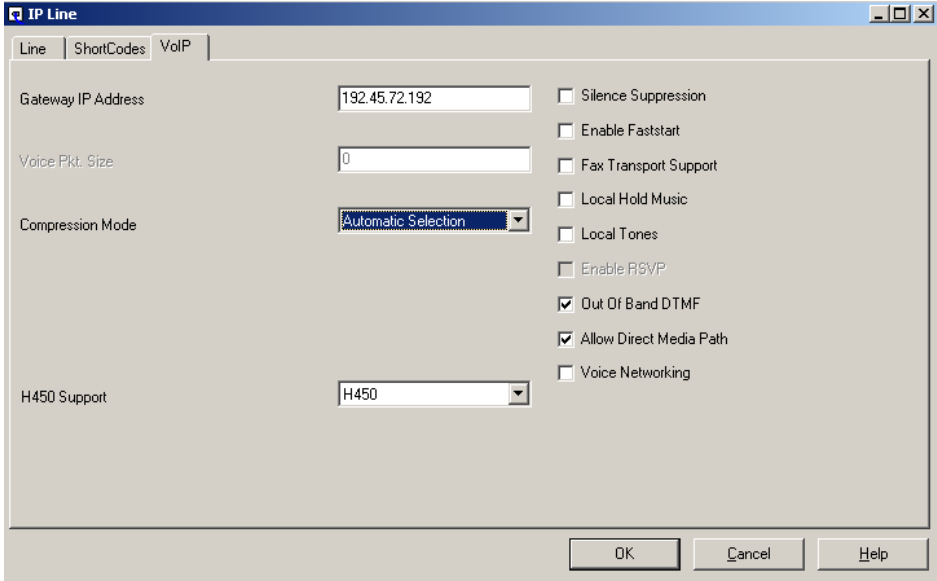
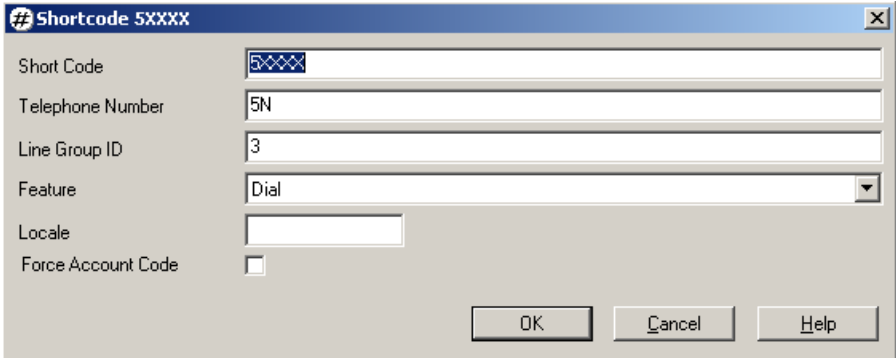
3. Configure the Avaya IP Office 412

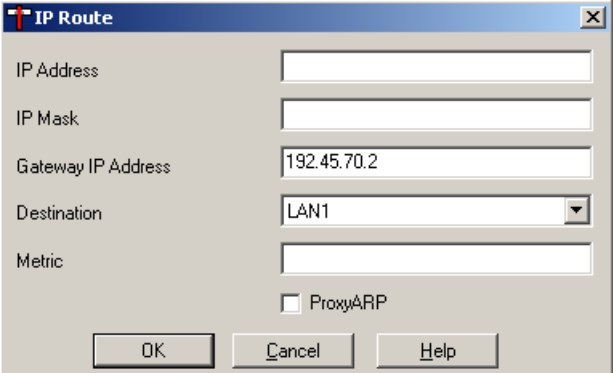
This section describes the configuration steps for providing the Avaya IP Office with an IP configuration, DSCP values for VoIP traffic, IP trunks to the branch site, short codes for routing VoIP calls, and a default route. The IP Office was configured using the **Avaya IP Office Manager** application.

Step	Description
1.	<p>To configure the Avaya IP Office, open the Manager application from a PC connected to the IP Office via IP. By default, the IP Office is assigned IP address 192.168.42.1 with a subnet mask of 255.255.255.0. The Manager main window is displayed. All of the configuration options are selected from the tree view of the Manager window.</p> 

Step	Description
2.	<p>To configure an IP address on the IP Office, select the System option. In the LAN1 tab, set the IP Address and IP Mask to values that correspond to the customer's network and select Disabled for DHCP Mode.</p>  <p>The screenshot shows the 'System Configuration : CORPSITE-6734' window with the 'LAN1' tab selected. The 'IP Address' field is set to '192.45.70.190' and the 'IP Mask' is '255.255.255.0'. The 'Number Of DHCP IP Addresses' is set to '200'. The 'DHCP Mode' is set to 'Disabled'. The 'RIP Mode' is set to 'None'. The 'Enable NAT' checkbox is unchecked. The 'Primary Trans. IP Address' field is empty. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.</p>
3.	<p>In the Gatekeeper tab, verify that the DSCP values for VoIP media and signaling traffic are set to 46 and 34, respectively. These same DiffServ code points are used by the IP Telephones for the media and signaling respectively in the compliance-tested configuration.</p>  <p>The screenshot shows the 'System Configuration : CORPSITE-6734' window with the 'Gatekeeper' tab selected. The 'Gatekeeper Enable' checkbox is checked. The 'Direct Routed Signaling Enable' checkbox is unchecked. The 'Auto-create Extn Enable' checkbox is checked. The 'Enable RSVP' checkbox is unchecked. The 'DSCP(Hex)' field is set to '46', the 'DSCP Mask (Hex)' is '63', the 'SIG DSCP (Hex)' is '34', and the 'SSON' is '176'. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.</p>

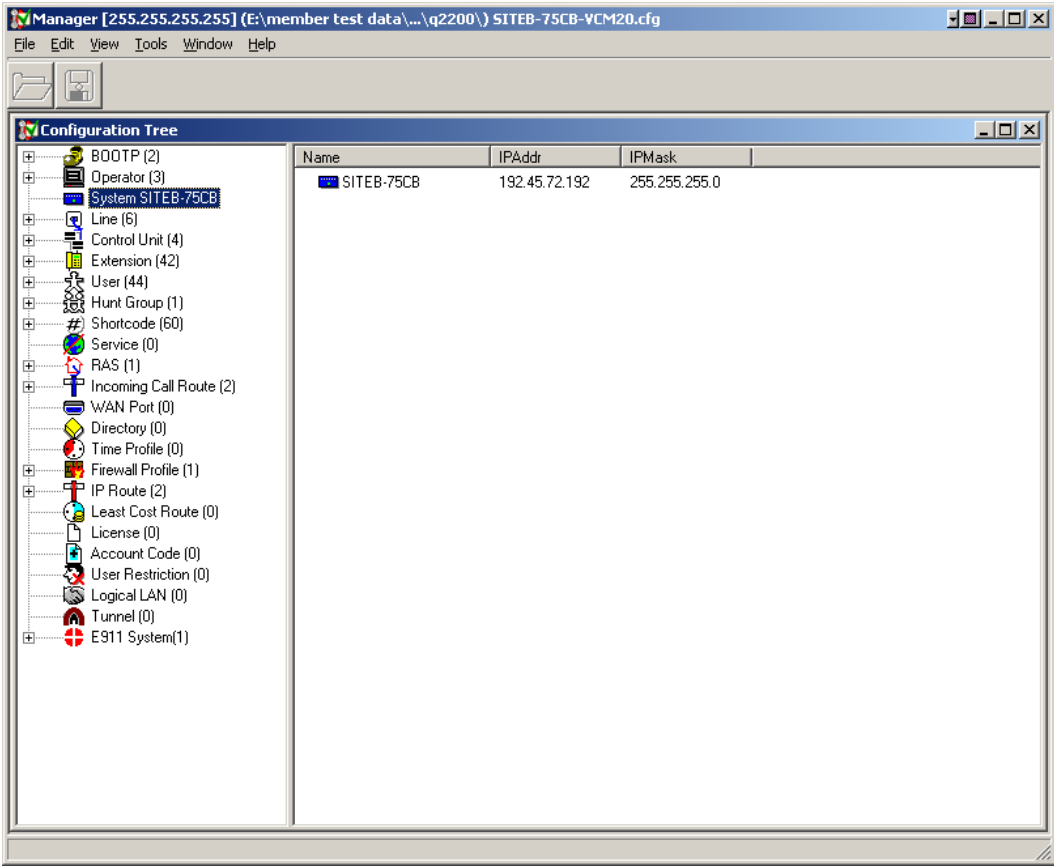
Step	Description
4.	<p>Next, create an IP trunk to the Avaya IP Office 403 at the branch site. Select the Line option from the Manager tree view and add an IP Line. Specify the Line Number, the number of Outgoing Channels and Voice Channels in this IP line, and the Incoming and Outgoing Group ID. The Outgoing Group ID is specified in the short code that routes outgoing calls to the branch site.</p>  <p>NOTE: The number of channels defined for the IP trunk was based on the IP Office VCM 5 module used in the test configuration. If a higher number of channels were to be used, then the default Kentrox bandwidth allocation discussed in Step 39 of Section 5.1 may require modification.</p>

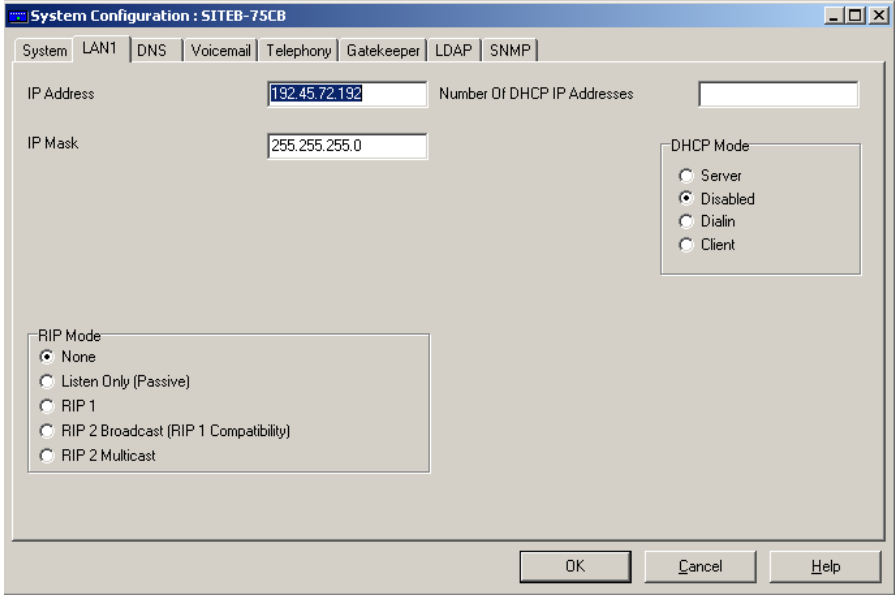
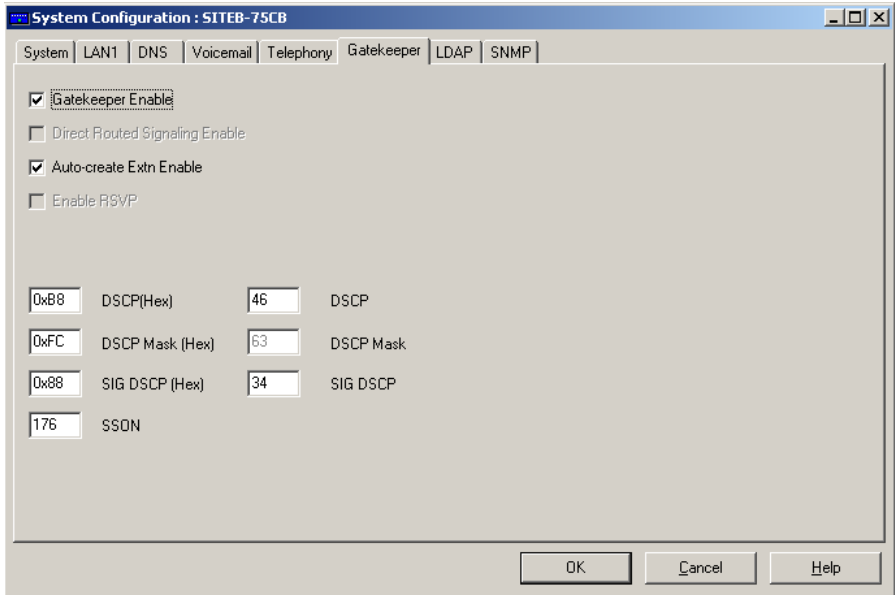
Step	Description
5.	<p>Under the VoIP tab of the IP Line form, set the Gateway IP Address to the IP address of the Avaya IP Office 403 at the branch site. The Compression Mode can be set to Automatic Selection. During the course of testing, the compression mode was altered to allow testing of both G.711 and G.729.</p> 
6.	<p>To route calls to the IP telephones at the branch site, create a short code by selecting the Shortcode option from the Manager tree view. The extensions at the branch site begin with the digit '5' and are 5-digits in length. In this example, the short code specifies that calls with dialed digits in the format 5xxxx, where 'x' denotes a wildcard, will be routed over Line Group ID 3 configured in Step 4. The Telephone Number field was set to 5N, which means that the 5xxxx digits dialed are sent over the IP trunk.</p> 

Step	Description
7.	<p>Next, select the IP Route option from the left panel of the Manager Main Window to add a default route. The IP Route form specifies the Q2400 at the corporate office as the default gateway. IP address 192.45.70.2 belongs to the Ethernet port on the Q2400 router associated with the voice VLAN (VLAN ID 70). This route is used to route VoIP media and signaling packets to the branch site.</p> 
8.	<p>Add IP Extensions and Users for the IP telephones that will register with the IP Office. The reader should consult the Avaya IP Office documentation listed in Section 10 for instructions on adding IP stations.</p>
9.	<p>In the Manager window, select File → Save to save the configuration to the IP Office system and wait for the system to update.</p>

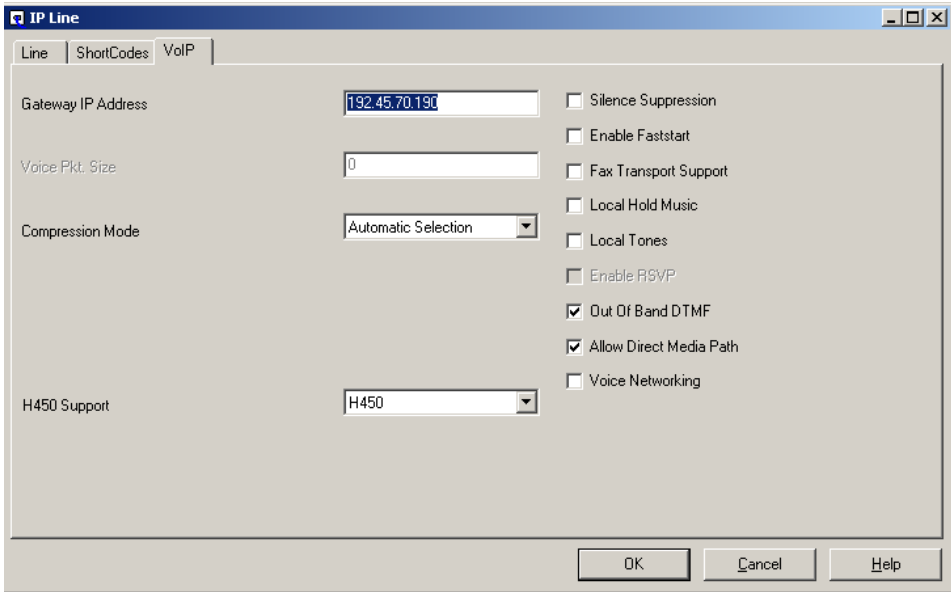
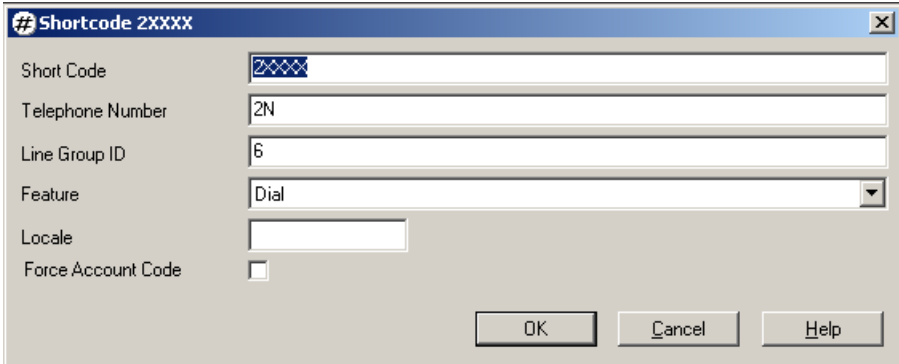
4. Configure the Avaya IP Office 403

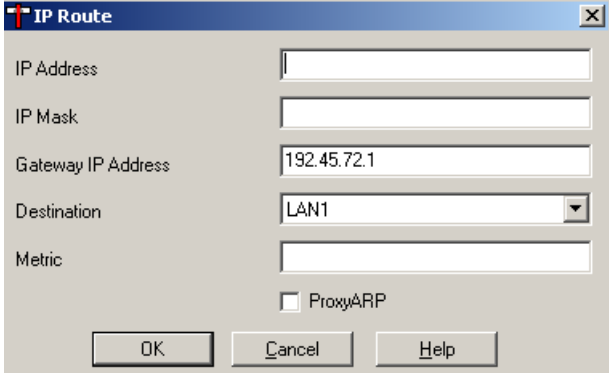
This section describes the configuration steps for providing the Avaya IP Office with an IP configuration, DSCP values for VoIP traffic, IP trunks to the corporate site, short codes for routing VoIP calls, and a default route. The IP Office was configured using the **Avaya IP Office Manager** application.

Step	Description
1.	<p>To configure the Avaya IP Office, open the Manager application from a PC connected to the IP Office via IP. By default, the IP Office is assigned IP address 192.168.42.1 with a subnet mask of 255.255.255.0. The Manager main window is displayed. All of the configuration options are selected from the tree view of the Manager window.</p> 

Step	Description
2.	<p>To configure an IP address on the IP Office, select the System option. In the LAN1 tab, set the IP Address and IP Mask. In the field, specify the IP configuration that corresponds to the customer's network. Select Disabled for DHCP Mode. Although the integrated DHCP server in the IP Office could have been used, DHCP relay to the corporate site was used for illustrative purposes.</p> 
3.	<p>In the Gatekeeper tab, verify that the DSCP values for VoIP media and signaling traffic are set to 46 and 34, respectively. These same DiffServ code points are used by the IP Telephones for the media and signaling respectively in the compliance-tested configuration.</p> 

Step	Description
4.	<p>Next, create an IP trunk to the Avaya IP Office at the corporate site. Select the Line option from the Manager tree view and add an IP Line. Specify the Line Number, the number of Outgoing Channels and Voice Channels in this IP line, and the Incoming and Outgoing Group ID. The Outgoing Group ID is specified in the short code that routes outgoing calls to the corporate site.</p> <div data-bbox="402 457 1346 1041"> </div> <p>NOTE: The number of channels defined for the IP trunk was based on the IP Office VCM 5 module used in the test configuration. If a higher number of channels were to be used, then the default Kentrox bandwidth allocation discussed in Step 39 of Section 5.1 may require modification.</p>

Step	Description
5.	<p>Under the VoIP tab of the IP Line form, set the Gateway IP Address to the IP address of the Avaya IP Office at the corporate site. The Compression Mode can be set to Automatic Selection. During the course of testing, the compression mode was altered to allow testing of both G.711 and G.729.</p> 
6.	<p>To route calls to the IP telephones at the corporate site, create a short code by selecting the Shortcode option from the Manager tree view. The extensions at the corporate site begin with the digit '2' and are 5-digits in length. In this example, the short code specifies that calls with dialed digits in the format 2xxxx, where 'x' denotes a wildcard, be routed over Line Group ID 6 that was configured in Step 4. The Telephone Number field was set to 2N, which means that the 2xxxx digits dialed are sent over the IP trunk.</p> 

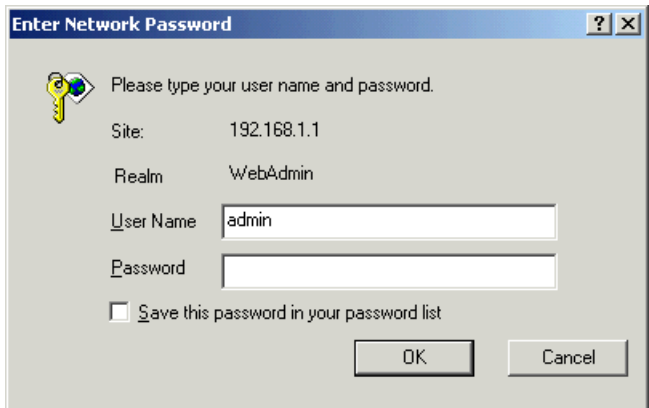
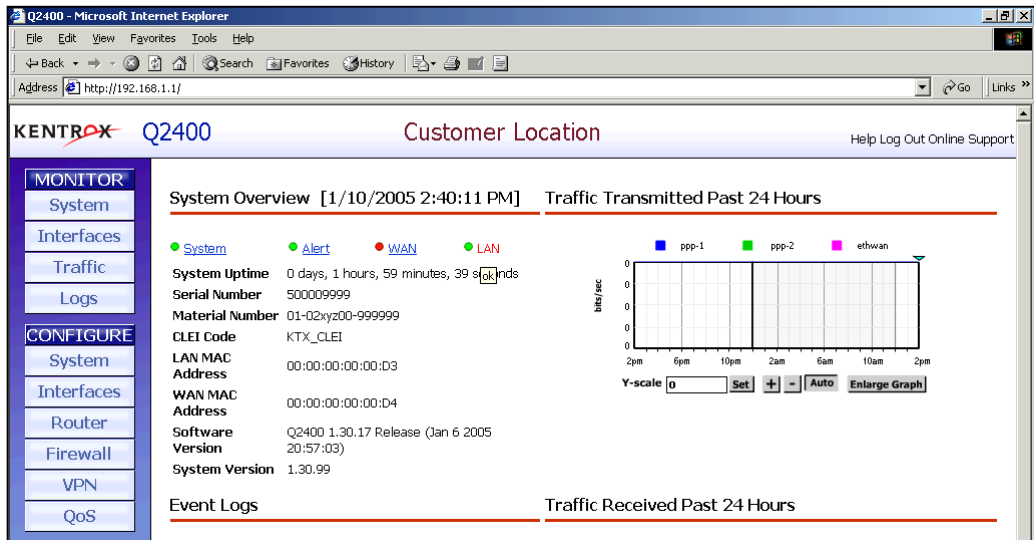
Step	Description
7.	<p>Next, select the IP Route option from the left panel of the Manager Main Window to add a default route. The IP Route form specifies the Q2200 at the branch office as the default gateway. IP address 192.45.72.1 belongs to the Ethernet port on the Q2200 router associated with the voice VLAN (VLAN ID 72). This route is used to route VoIP media and signaling packets to the corporate site.</p> 
8.	Add IP Extensions and Users for the IP telephones that will register with the IP Office. The reader should consult the Avaya IP Office documentation listed in Section 10 for instructions on adding IP stations.
9.	In the Manager window, select File → Save to save the configuration to the IP Office system and wait for the system to update.

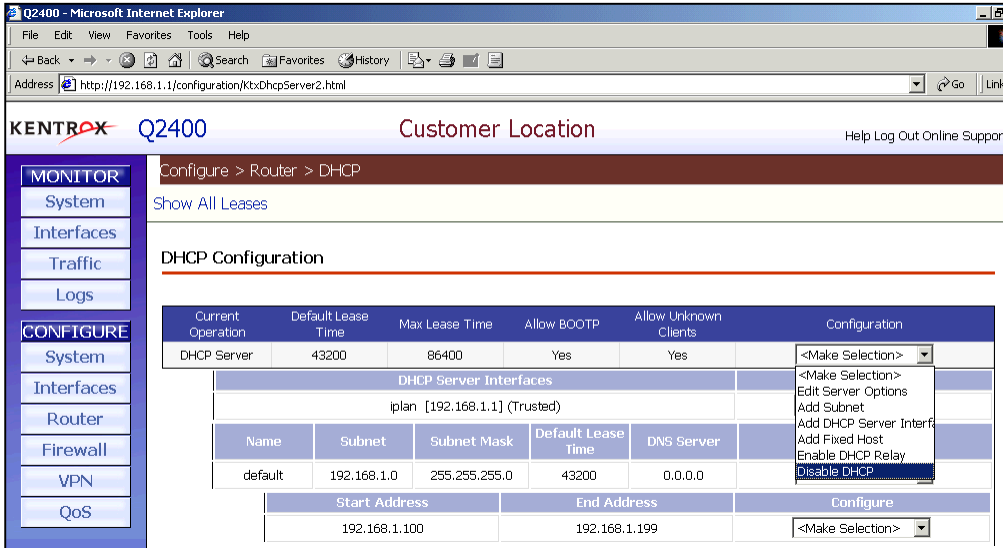
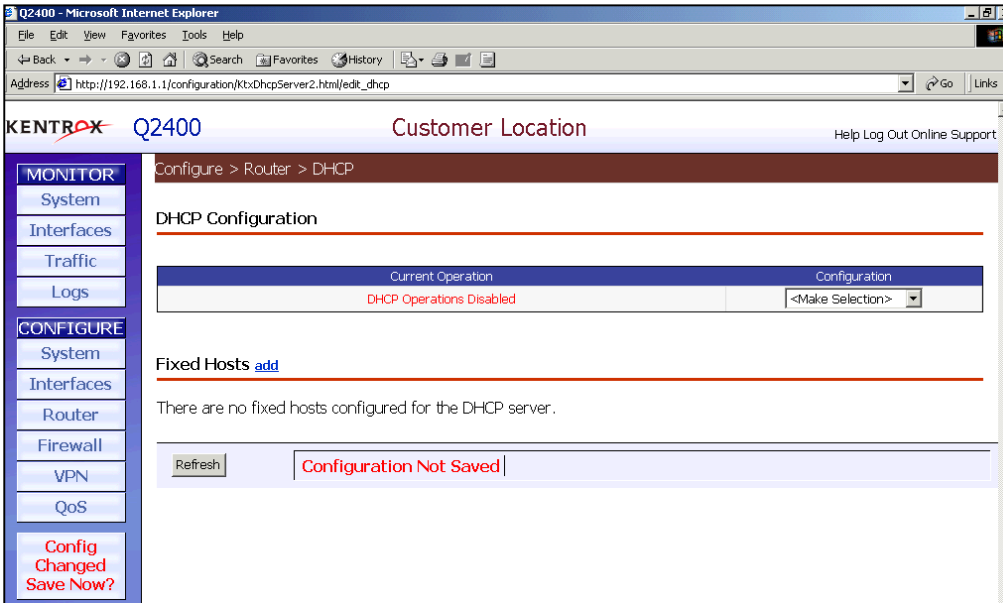
5. Configure the Kentrox Q-Series Routers for T1/PPP

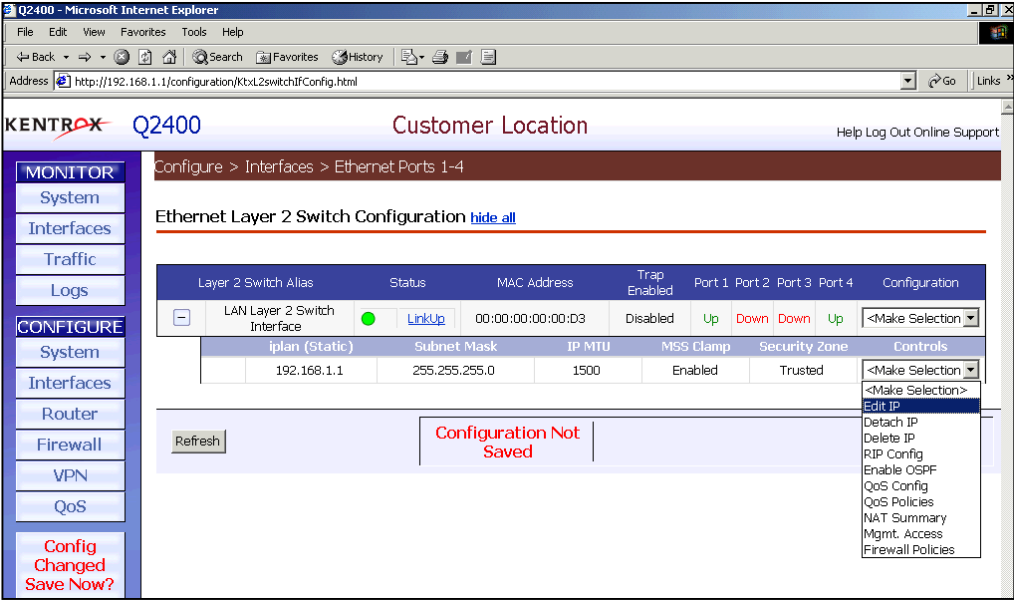
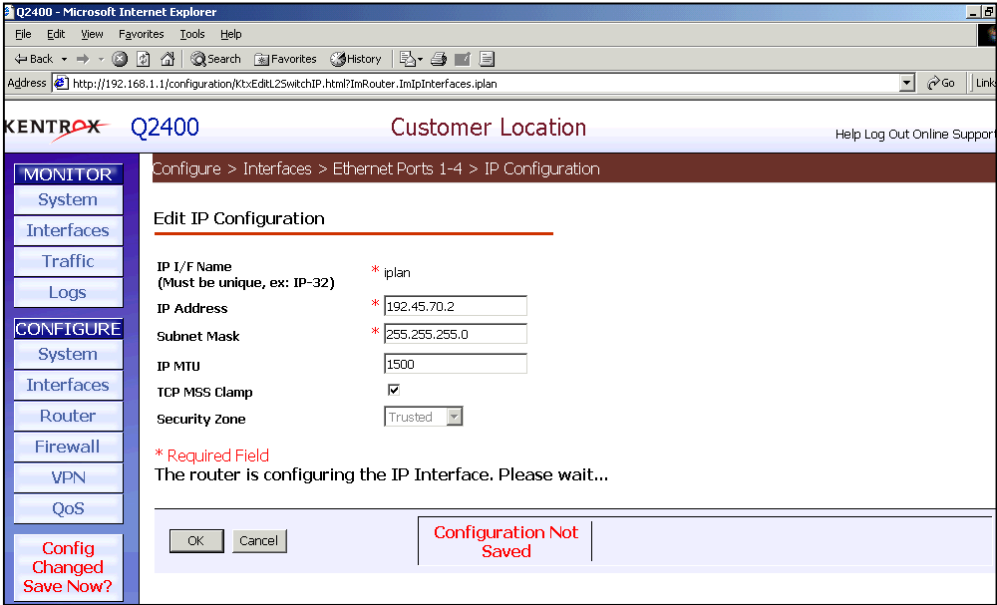
The Kentrox Q-Series routers provide WAN connectivity for the corporate and branch office sites using PPP links. The Q2400 at the corporate site and the Q2200 at the branch site both connect to the private line.

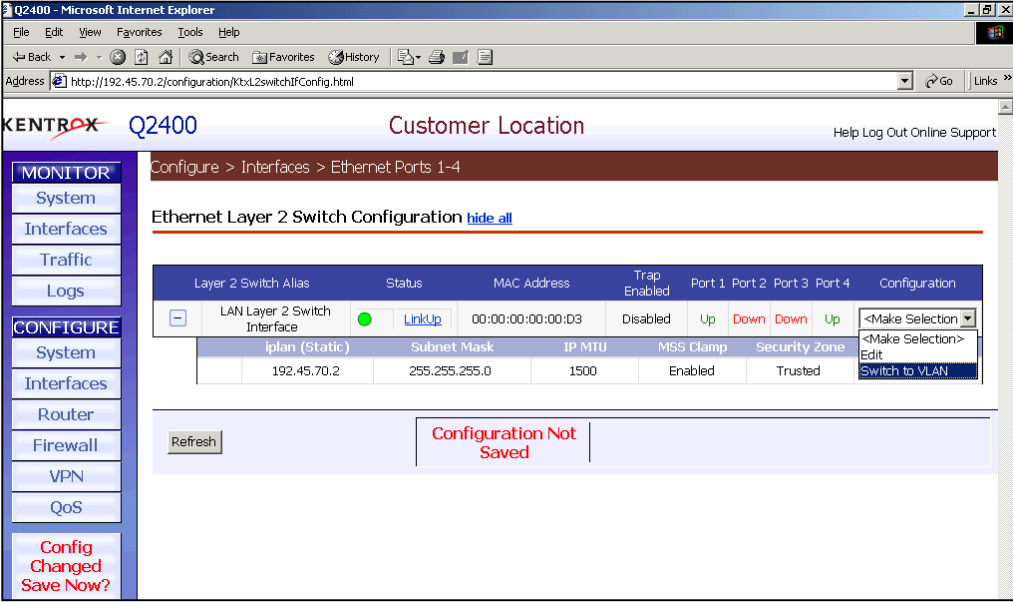
5.1. Kentrox Q2400 in the Corporate Site

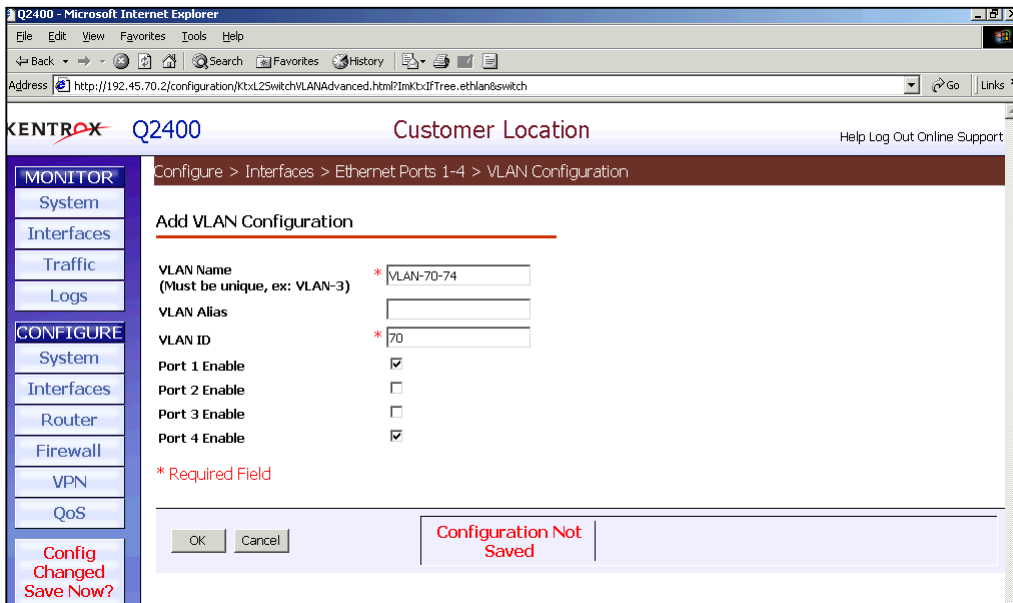
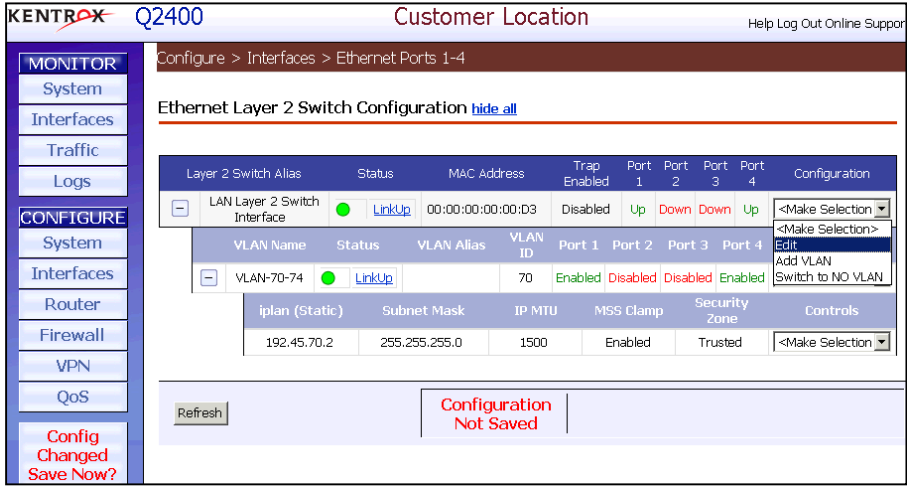
This section provides the configuration of the Q2400 in the corporate site. The Q2400 connects to the Avaya IP Office 412 via a Layer-2 switch.

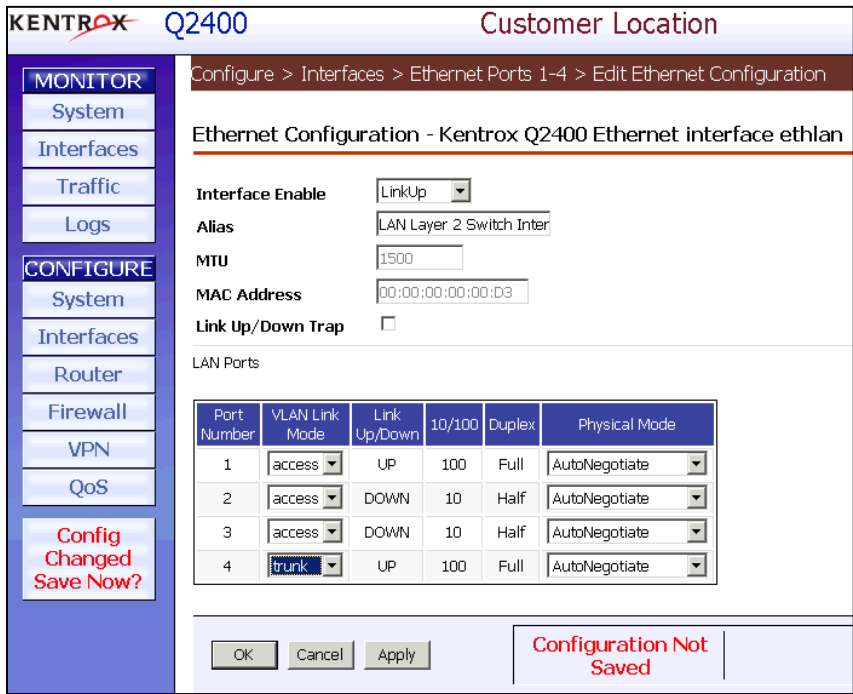
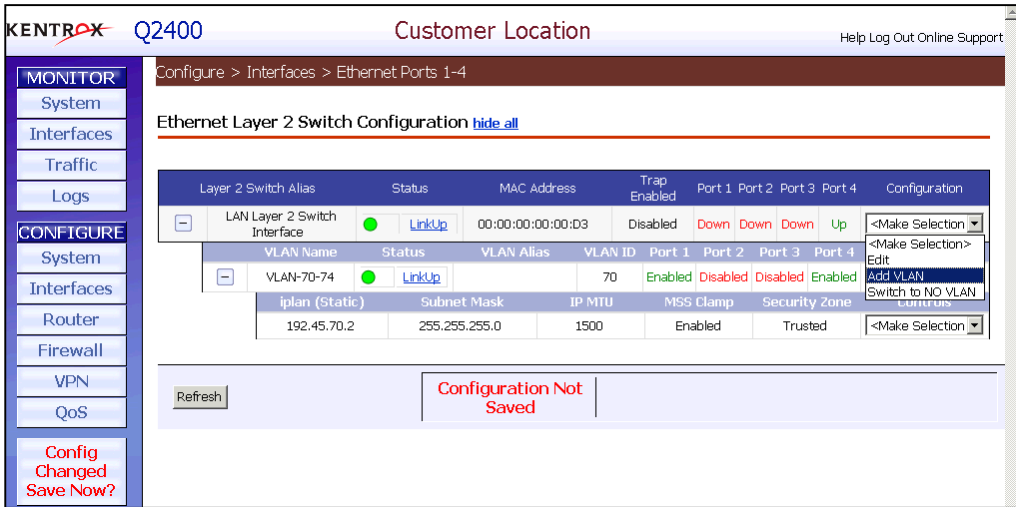
Step	Description
1.	<p>To configure the Kentrox Q2400, launch Internet Explorer from a PC directly connected to the Q2400. By default, the Q2400 is assigned an IP address 192.168.1.1 with a subnet mask of 255.255.255.0. Log into the Q2400 using the appropriate credentials when the Q2400 authentication window appears.</p>  <p>NOTE: In the configuration used for these Application Notes, the PC used to initially configure the Q2400 was directly connected to Port 1 and the Layer 2 switch connected to the Q2400 was connected to Port 4.</p>
2.	<p>Once successfully logged in, the Q2400 main window is displayed. All of the configuration options are selected from the tree view on the left side of the Q2400 main window.</p> 

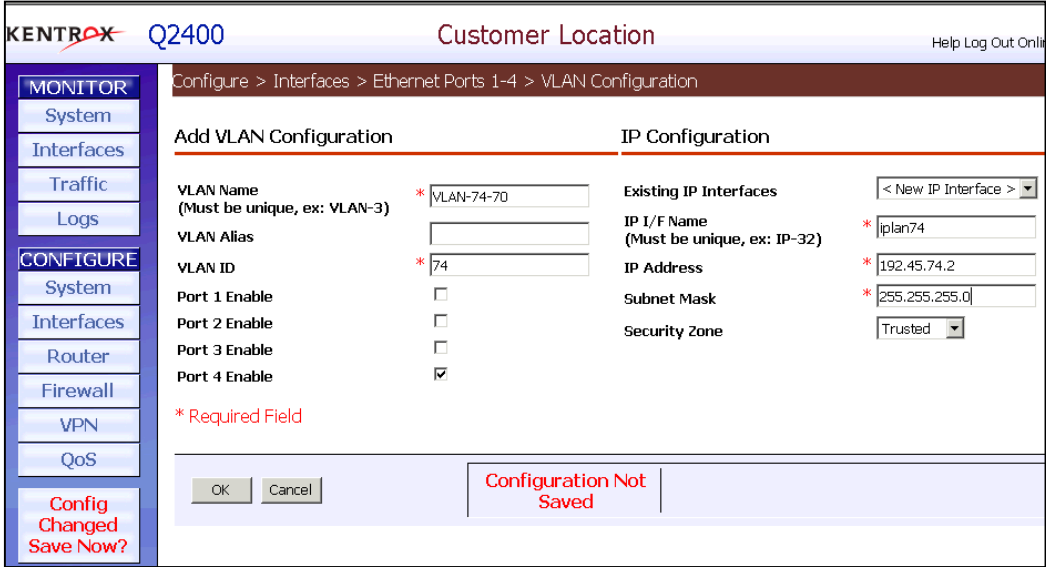
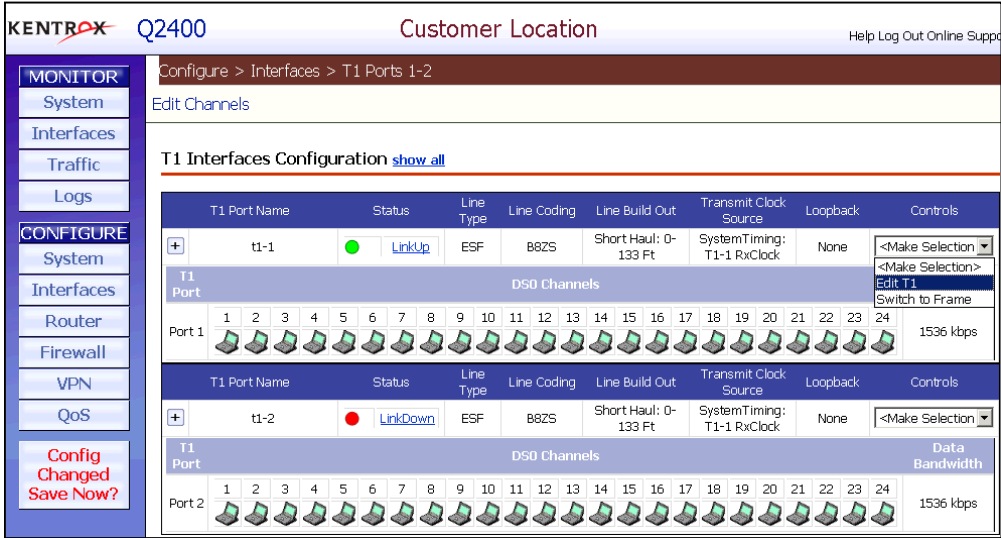
Step	Description
3.	<p>To disable the Q2400 DHCP Server, select Router → DHCP under CONFIGURE in the tree view. In the Configure > Router > DHCP page that appears, select Disable DHCP from the Configuration pull-down menu for the DHCP Server.</p>  <p>The screenshot shows the Q2400 web interface in Microsoft Internet Explorer. The address bar shows 'http://192.168.1.1/configuration/ktxDhcpServer2.html'. The left sidebar has 'CONFIGURE' selected, with 'Router' and 'DHCP' in the tree view. The main content area is titled 'DHCP Configuration'. It contains a table with columns: Current Operation, Default Lease Time, Max Lease Time, Allow BOOTP, Allow Unknown Clients, and Configuration. The 'Configuration' dropdown menu is open, showing options: '<Make Selection>', 'Edit Server Options', 'Add Subnet', 'Add DHCP Server Interface', 'Add Fixed Host', 'Enable DHCP Relay', and 'Disable DHCP'. 'Disable DHCP' is highlighted.</p>
4.	Click OK at the ‘This will disable DHCP. Are you sure?’ popup that appears.
5.	<p>The message ‘DHCP Operations Disabled’ now appears for the DHCP Configuration.</p>  <p>The screenshot shows the Q2400 web interface after disabling DHCP. The address bar shows 'http://192.168.1.1/configuration/ktxDhcpServer2.html/edit_dhcp'. The left sidebar has 'CONFIGURE' selected, with 'Router' and 'DHCP' in the tree view. The main content area is titled 'DHCP Configuration'. It contains a table with columns: Current Operation and Configuration. The 'Current Operation' is 'DHCP Operations Disabled'. Below the table, there is a section for 'Fixed Hosts' with a message: 'There are no fixed hosts configured for the DHCP server.' At the bottom, there is a 'Refresh' button and a red message: 'Configuration Not Saved'.</p>

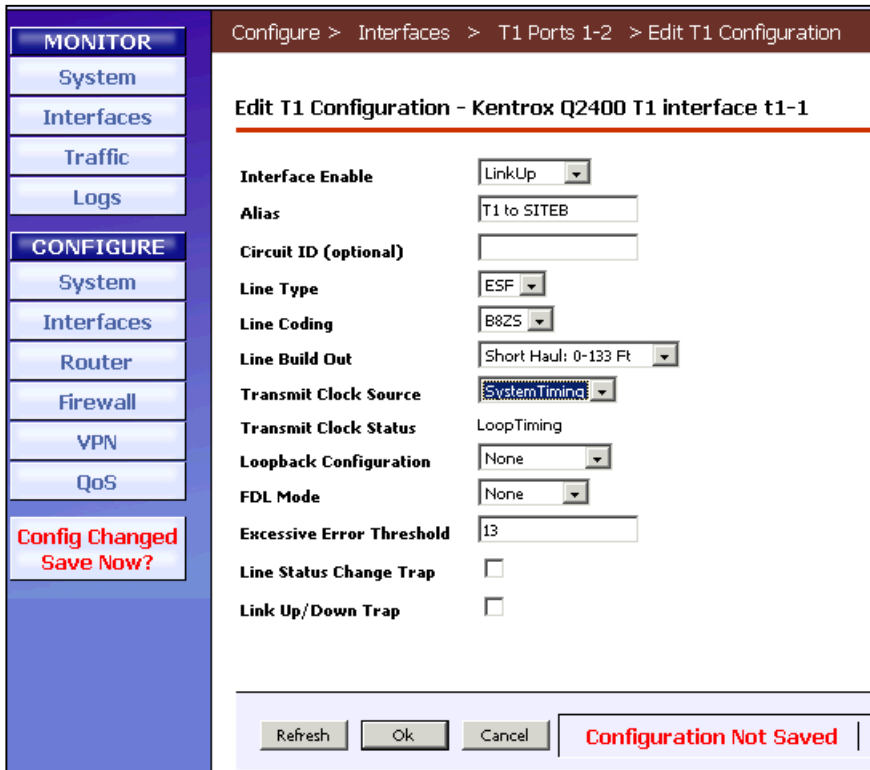
Step	Description
6.	<p>To configure the IP address on the Q2400, select Interfaces → Ethernet Ports 1-4 under CONFIGURE in the tree view. In the Configure > Interfaces > Ethernet Ports 1-4 page that appears, select Edit IP in the Controls pull-down menu for IP address 192.168.1.1.</p> 
7.	<p>In the Configure > Interfaces > Ethernet Ports 1-4 > IP Configuration page that appears, set <i>IP Address</i> to 192.45.70.2, <i>Subnet Mask</i> to 255.255.255.0 and click OK.</p> 

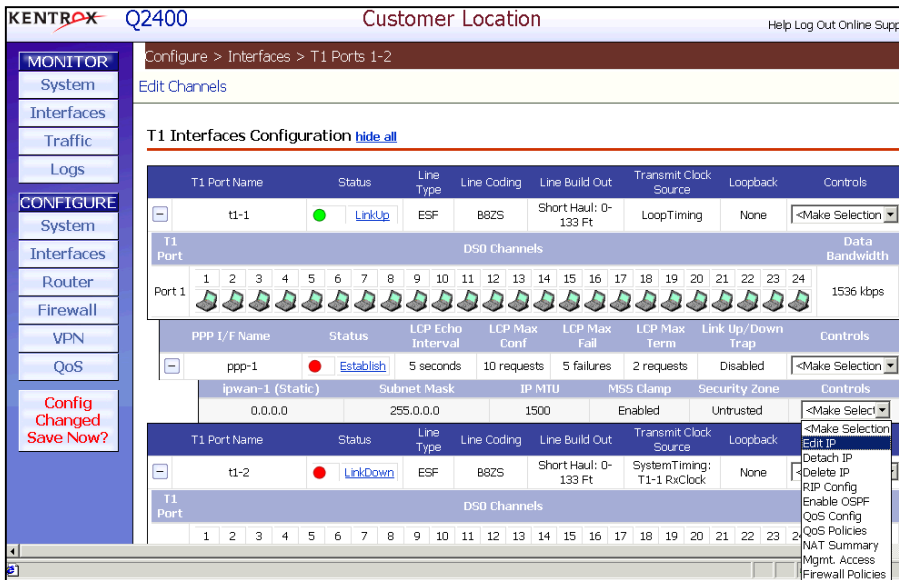
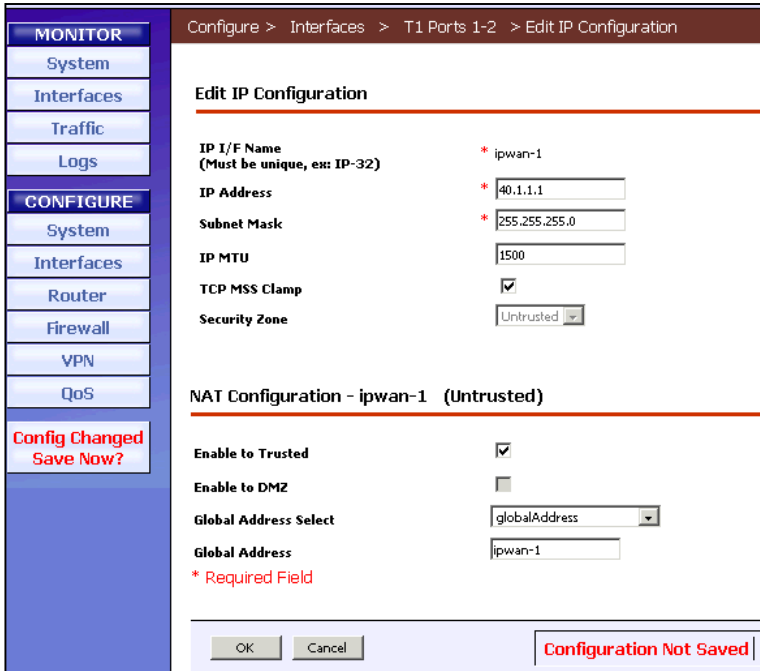
Step	Description
8.	Change the IP address of the PC directly connected to the Q2400, browse to 192.45.70.2 and log into the Q2400.
9.	<p>Select Interfaces → Ethernet Ports 1-4 under CONFIGURE in the tree view. In the Configure > Interfaces > Ethernet Ports 1-4 page that appears, select Switch to VLAN in the Configuration pull-down menu for LAN Layer 2 Switch Interface.</p> 
10.	Click OK at the ‘This will detach the IP interface and disrupt traffic. Are you sure?’ popup that appears.

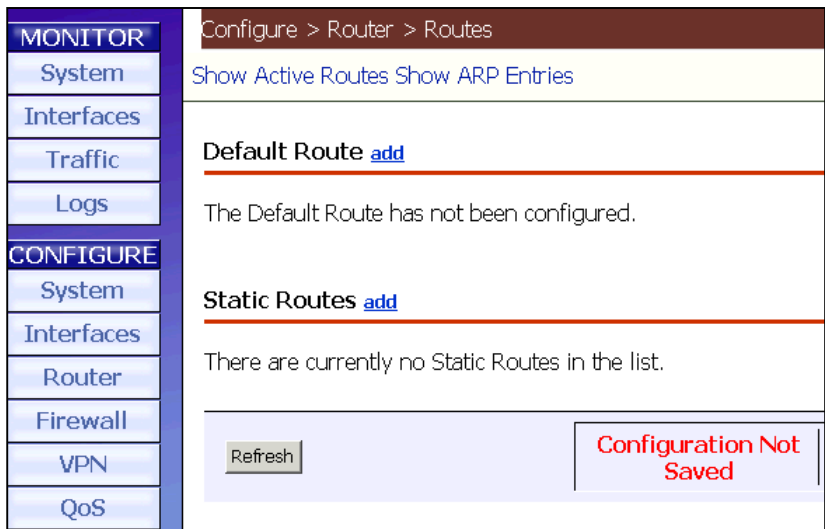
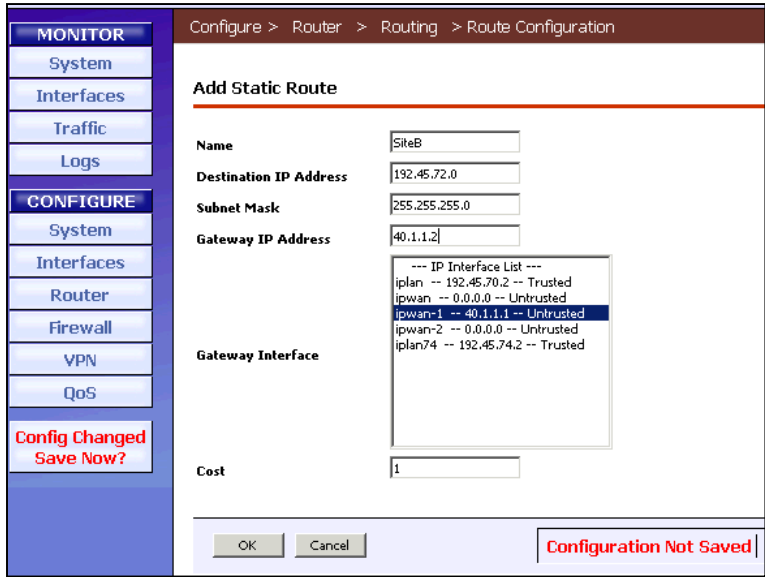
Step	Description
11.	<p>Configure VLAN 70 in the Configure > Interfaces > Ethernet Ports 1-4 > VLAN Configuration page that appears. Set <i>VLAN Name</i> to VLAN-70-74, <i>VLAN ID</i> to 70, check Port 1 Enable, check Port 4 Enable, and click OK.</p> 
12.	<p>This change causes the connection to the browser to drop. Browse to 192.45.70.2 and log into the Q2400.</p>
13.	<p>Select Interfaces → Ethernet Ports 1-4 under CONFIGURE in the tree view. In the Configure > Interfaces > Ethernet Ports 1-4 page that appears, select Edit in the Configuration pull-down menu for LAN Layer 2 Switch Interface.</p> 

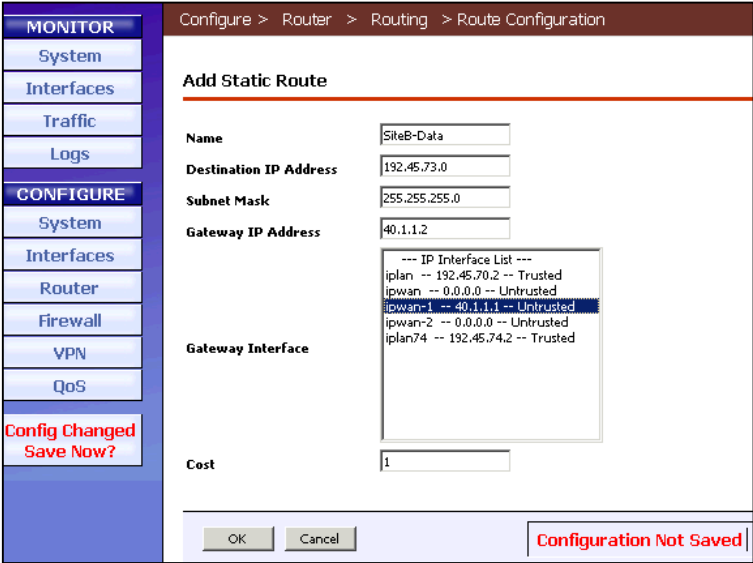
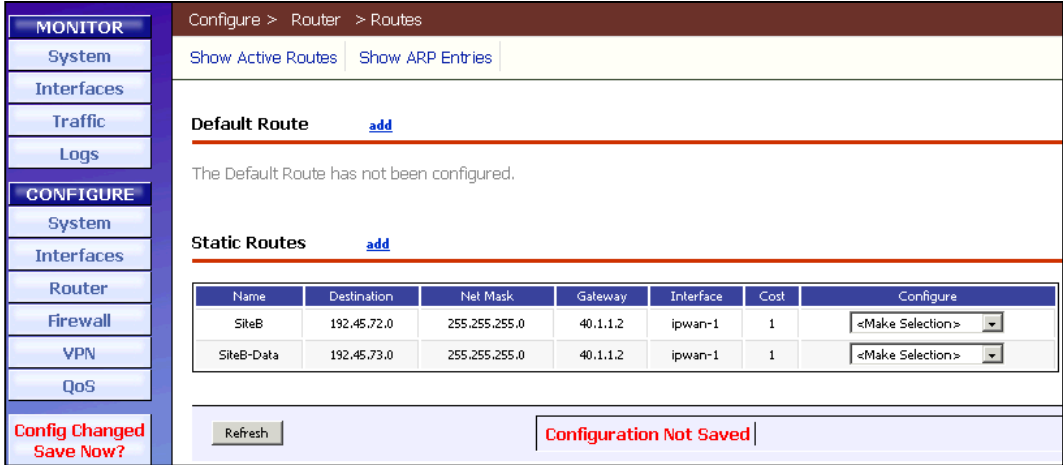
Step	Description
14.	<p>In the Configure > Interfaces > Ethernet Ports 1-4 > Edit Ethernet Configuration page that appears, set Port 4 <i>VLAN Link Mode</i> to trunk and click OK.</p>  <p>NOTE: The port on the Layer-2 switch connecting to port 4 on the Q2400 was configured for 802.1q (VLAN) mode. This allows VLAN header information to be exchanged between the switch at the corporate site and the Q2400. The corporate site contains voice VLAN 70 and data VLAN 74.</p>
15.	<p>In the Configure > Interfaces > Ethernet Ports 1-4 page that appears, select Add VLAN in the Configuration pull-down menu for LAN Layer 2 Switch Interface.</p> 

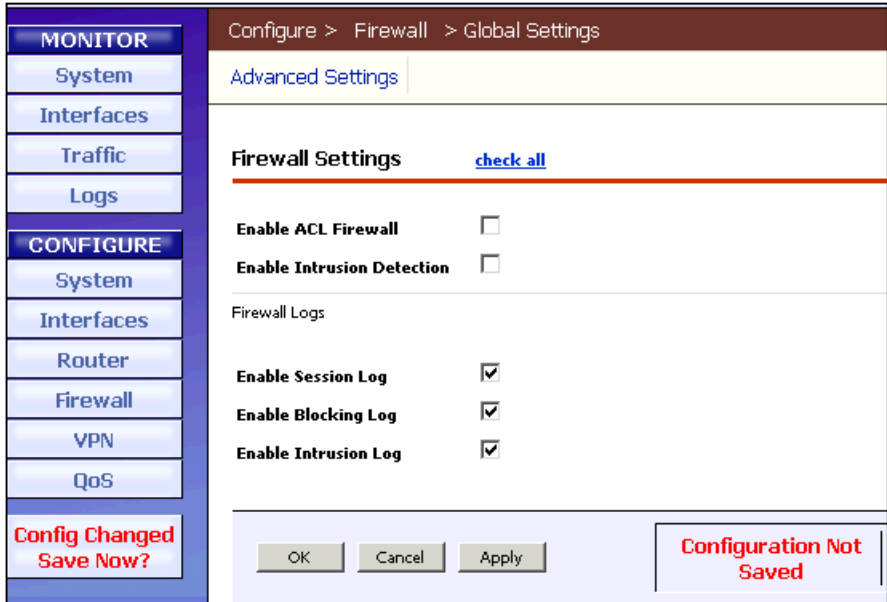
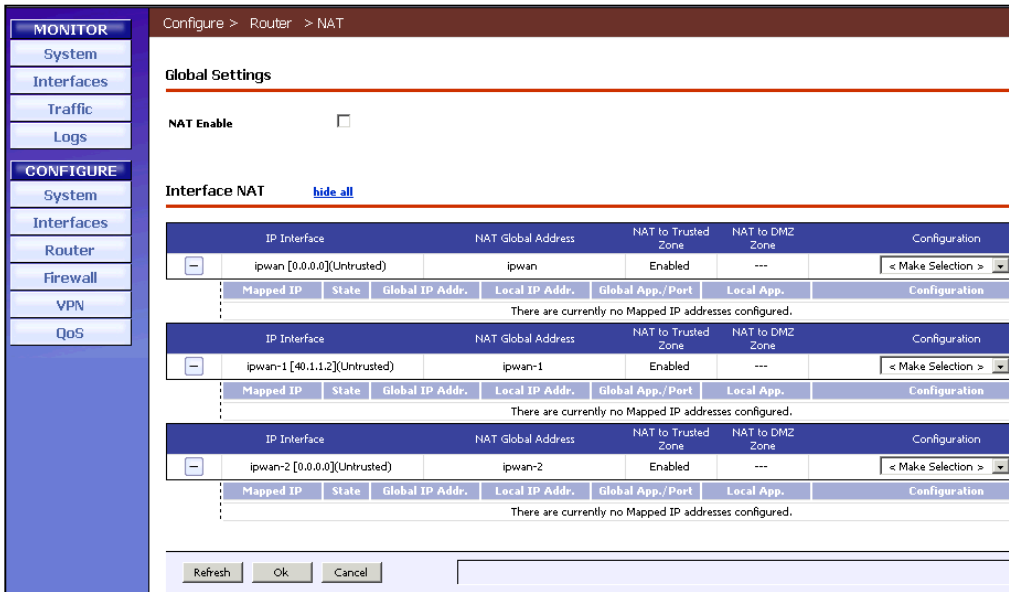
Step	Description
16.	<p>Configure VLAN 74 in the Configure > Interfaces > Ethernet Ports 1-4 > VLAN Configuration page that appears. Set VLAN Name to VLAN-74-70, VLAN ID to 74, check Port 4 Enable, IP I/F Name to iplan74, IP Address to 192.45.74.2, Subnet Mask to 255.255.255.0, and click OK.</p> 
17.	<p>Select Interfaces → T1 Ports 1-2 under CONFIGURE in the tree view. In the Configure > Interfaces > T1 Ports 1-2 page that appears, select Edit T1 in the Controls pull-down menu for T1 Port Name t1-1.</p> 

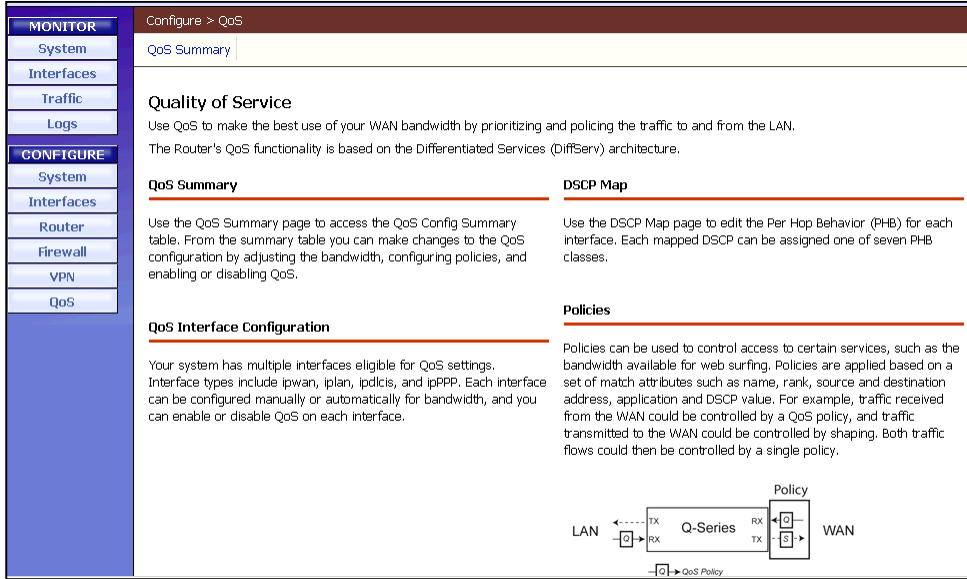
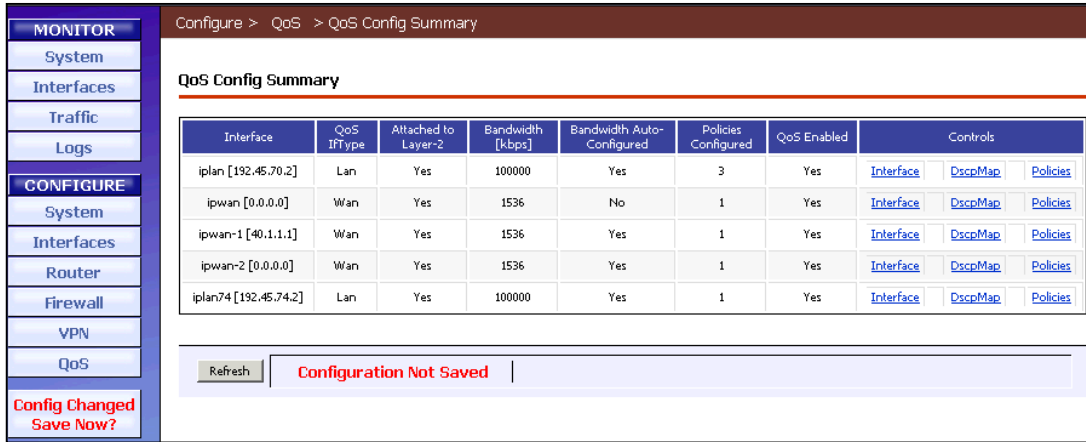
Step	Description
18.	<p>In the Configure > Interfaces > T1 Ports 1-2 > Edit T1 Configuration page that appears, configure the line settings needed to connect the T1 to the network and click OK.</p> 

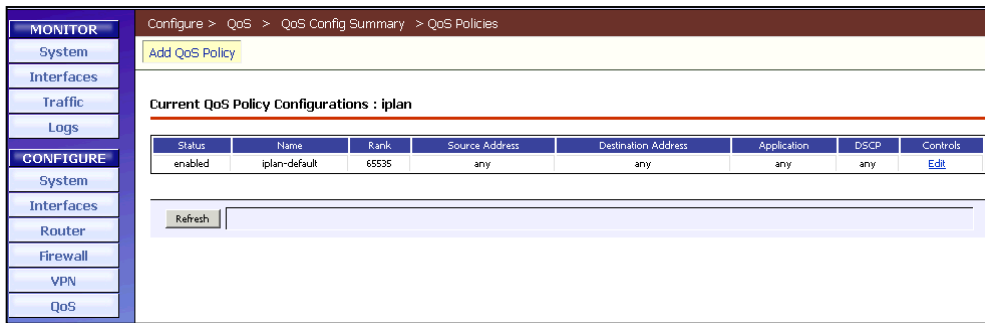
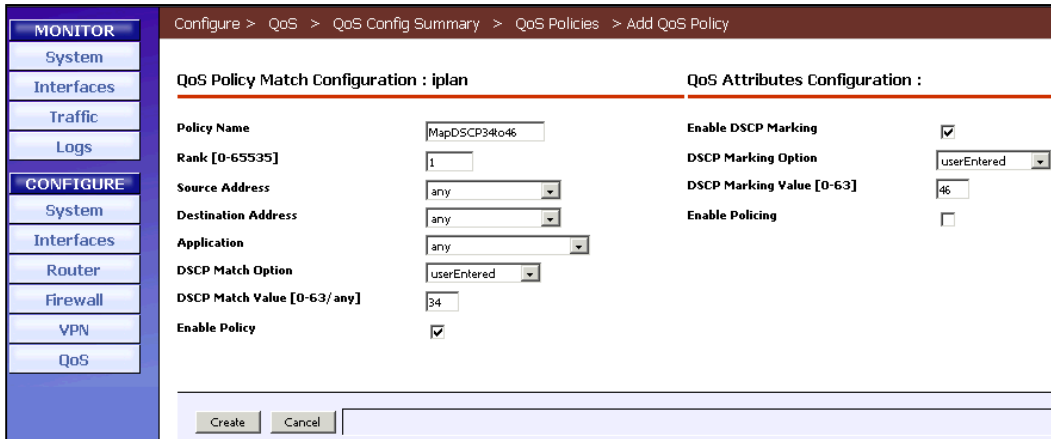
Step	Description
19.	<p>In the Configure > Interfaces > T1 Ports 1-2 page that appears, select Edit IP in the Controls pull-down menu for PPP I/F Name ppp-1.</p> 
20.	<p>In the Configure > Interfaces > T1 Ports 1-2 > Edit IP Configuration page that appears, set <i>IP Address</i> to 40.1.1.1, <i>Subnet Mask</i> to 255.255.255.0 and click OK.</p> 

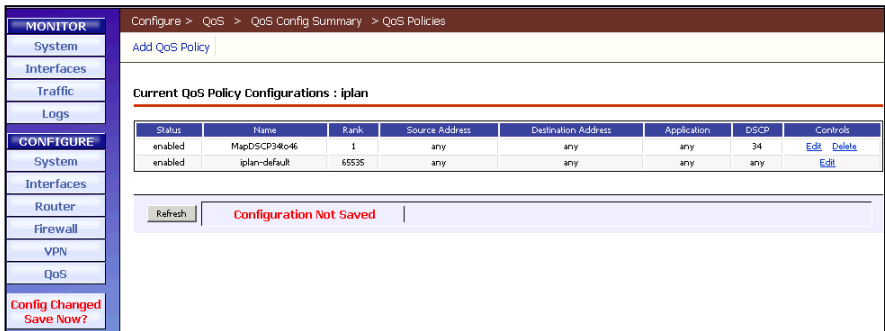
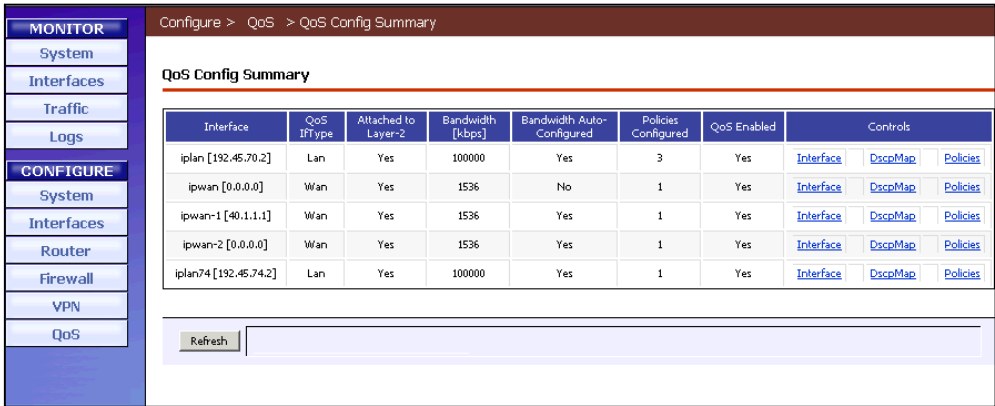
Step	Description
21.	<p>Select Router → Routes under CONFIGURE in the tree view. In the Configure > Router > Routes page that appears, click Add for Static Routes.</p> 
22.	<p>In the Configure > Router > Routing > Route Configuration page that appears, set <i>Name</i> to SiteB, <i>Destination IP Address</i> to 192.45.72.0, <i>Subnet Mask</i> to 255.255.255.0, <i>Gateway IP Address</i> to 40.1.1.2, select ipwan-1 in the <i>Gateway Interface</i> list and click OK.</p> 
23.	<p>In the Configure > Router > Routes page that appears again, click Add for Static Routes.</p>

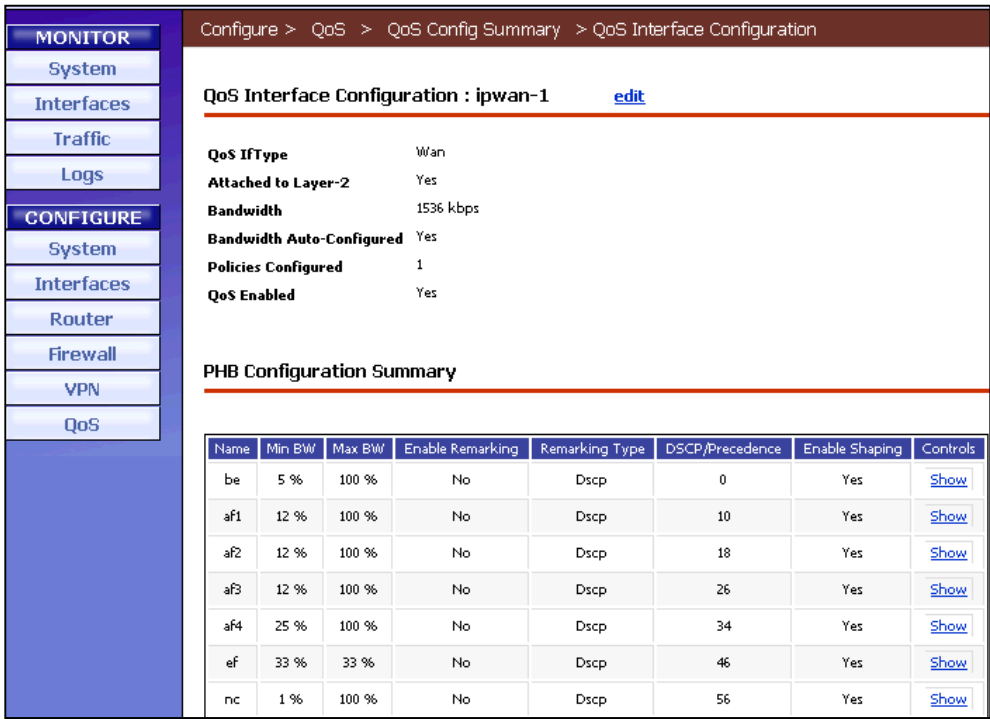
Step	Description
24.	<p>In the Configure > Router > Routing > Route Configuration page that appears, set <i>Name</i> to SiteB-Data, <i>Destination IP Address</i> to 192.45.73.0, <i>Subnet Mask</i> to 255.255.255.0, <i>Gateway IP Address</i> to 40.1.1.2, select ipwan-1 in the <i>Gateway Interface</i> list and click OK.</p> 
25.	<p>In the Configure > Router > Routes pages that appears, the newly defined static routes are listed.</p> 

Step	Description
26.	<p>Select Firewall → Global Settings under CONFIGURE in the tree view. In the Configure > Firewall > Global Settings page that appears, uncheck Enable ACL Firewall, uncheck Enable Intrusion Detection and click OK. These Application Notes do not address firewall configuration.</p> 
27.	<p>Click OK at the ‘Disabling the Firewall leaves the LAN and the Router unprotected.’ popup that appears.</p>
28.	<p>Select Router → NAT under CONFIGURE in the tree view. In the Configure > Router > NAT page that appears, uncheck NAT and click OK.</p> 

Step	Description
29.	Click OK at the ‘Changing the NAT configuration will terminate the session. Do you want to continue?’ popup that appears.
30.	If logged in remotely, the previous step may cause the connection to drop. If so, browse to 192.45.70.2 and log into the Q2400.
31.	Select QoS under CONFIGURE in the tree view. In the Configure > QoS page that appears, click QoS Summary .
	
32.	In the Configure > QoS > QoS Config Summary page that appears, click Policies for the Interface iplan [192.45.70.2] .
	

Step	Description
33.	<p>In the Configure > QoS > QoS Config Summary > QoS Policies page that appears, click Add QoS Policy.</p> 
34.	<p>In the Configure > QoS > QoS Config Summary > QoS Policies > Add QoS Policy page that appears, set <i>Policy Name</i> to MapDSCP34to46, <i>Rank</i> to 1, <i>Source Address</i> to any, <i>Destination Address</i> to any, <i>Application</i> to any, <i>DSCP Match Option</i> to userEntered, <i>DSCP Match Value</i> to 34, <i>DSCP Marking Option</i> to userEntered, <i>DSCP Marking Value</i> to 46, check Enable Policy, check Enable DSCP Marking and click Create.</p>  <p>NOTE: The Q-Series routers keep traffic marked with DSCP 46 (EF) in its own priority queue. However, DSCP 34 (AF4) marked traffic is kept in a Weighted Fair Queue (WFQ) with all other DSCP values. High traffic scenarios negatively impact call-signaling traffic when it is kept in the WFQ. To ensure highest priority for both signaling and audio, a policy was created to map DSCP 34 to 46 at both the corporate and branch site Q-series routers. This ensures that signaling and audio packets are transmitted using the priority queue, instead of the WFQ.</p>

Step	Description
35.	<p>In the Configure > QoS > QoS Config Summary > QoS Policies page that appears, the newly added policy is listed.</p> 
36.	<p>Select System → Save Config under CONFIGURE in the tree view to save the configuration.</p>
37.	<p>This change causes the connection to the browser to drop. Browse to 192.45.70.2 and log into the Q2400.</p>
38.	<p>Select QoS → QoS Summary under CONFIGURE in the tree view. In the Configure > QoS > QoS Config Summary page that appears, click Interface for the Interface ipwan-1 [40.1.1.1].</p> 

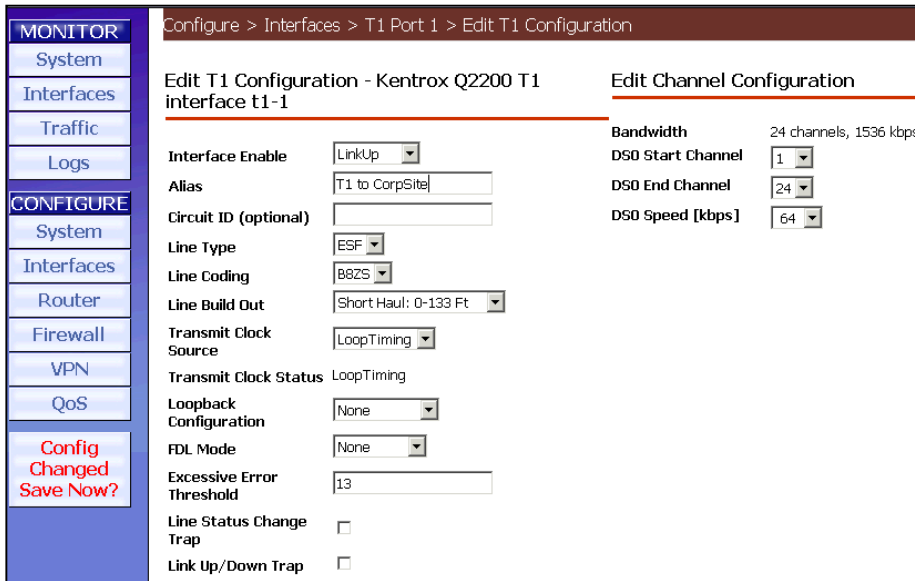
Step	Description
39.	<p>In the Configure > QoS > QoS Config Summary > QoS Interface Configuration page that appears, the QoS configuration for the ipwan-1 interface is listed. Modify the Bandwidth for the link and/or each DSCP value as necessary.</p>  <p>NOTE: By default, the Q-Series routers perform traffic shaping on the traffic going through the WAN interface. Expedited forwarding traffic is limited to 33% of the bandwidth shown at the top of the screen. These default settings are optimal for the targeted small office and/or low bandwidth configurations for which the products are intended. These values can be configured.</p>

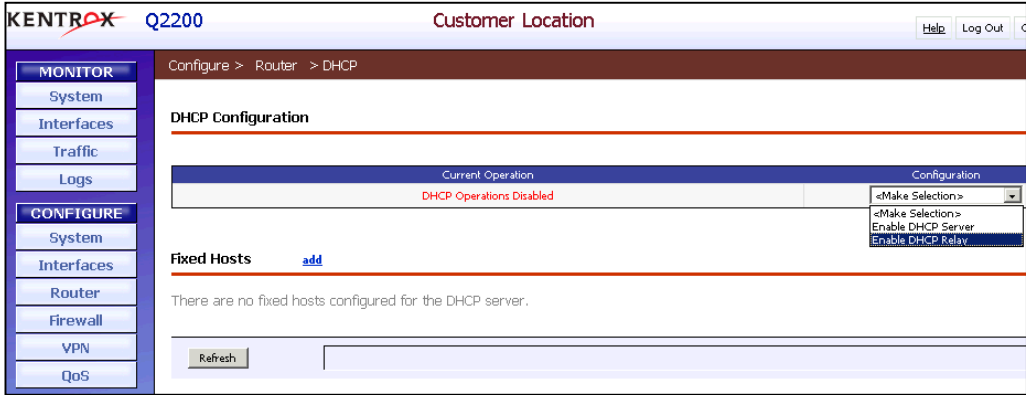
5.2. Kentrox Q2200 in Branch Office Site

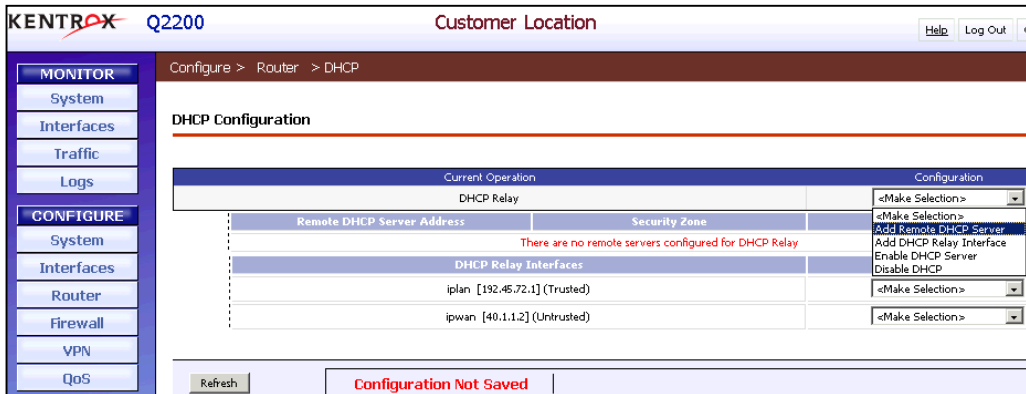
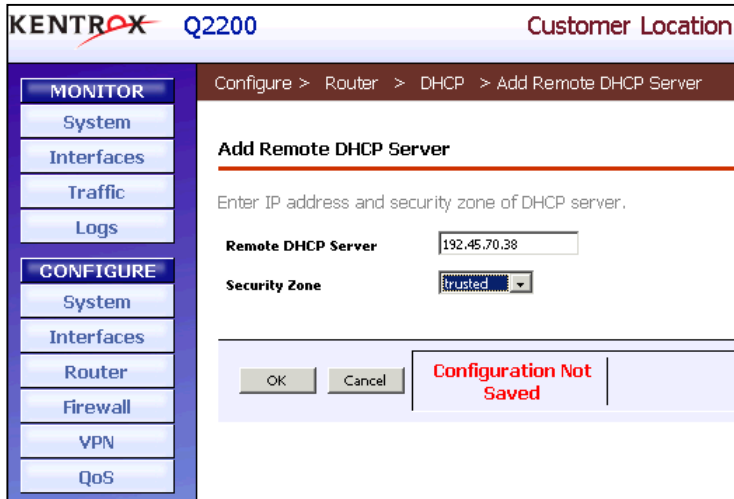
This section provides the configuration of the Q2200 in the Branch Office Site. The Q2400 browser based administrative interface is the same for the Q2200. Therefore, screenshots have been omitted for most steps in this section.

Step	Description
1.	<p>To configure the Kentrox Q2200, launch Internet Explorer from a PC directly connected to the Q2200. Initially, the Q2200 is assigned an IP address 192.168.1.1 with a subnet mask of 255.255.255.0. Log into the Q2200 using the appropriate credentials when the Q2200 authentication window appears. NOTE: In the configuration used for these Application Notes, the PC used to initially configure the Q2200 was directly connected to Port 1 and the Layer 2 switch connected to the Q2200</p>

Step	Description
	was connected to Port 4.
2.	Once successfully logged in, the Q2200 main window is displayed. All of the configuration options are selected from the tree view on the left side of the Q2200 main window.
3.	To disable the Q2200 DHCP Server, select Router → DHCP under CONFIGURE in the tree view. In the Configure > Router > DHCP page that appears, select Disable DHCP from the Configuration pull-down menu for the DHCP Server.
4.	Click OK at the ‘This will disable DHCP. Are you sure?’ popup that appears.
5.	In the Configure > Router > DHCP page that appears, the message ‘ DHCP Operations Disabled ’ now appears for the DHCP Configuration.
6.	To configure the IP address on the Q2200, select Interfaces → Ethernet Ports 1-4 under CONFIGURE in the tree view. In the Configure > Interfaces > Ethernet Ports 1-4 page that appears, select Edit IP in the Controls pull-down menu for IP address 192.168.1.1.
7.	In the Configure > Interfaces > Ethernet Ports 1-4 > IP Configuration page that appears, set <i>IP Address</i> to 192.45.72.1 , <i>Subnet Mask</i> to 255.255.255.0 and click OK .
8.	Change the IP address of the PC directly connected to the Q2200, browse to 192.45.72.1 and log into the Q2200.
9.	Select Interfaces → Ethernet Ports 1-4 under CONFIGURE in the tree view. In the Configure > Interfaces > Ethernet Ports 1-4 page that appears, select Switch to VLAN in the Configuration pull-down menu for LAN Layer 2 Switch Interface.
10.	Click OK at the ‘This will detach the IP interface and disrupt traffic. Are you sure?’ popup that appears.
11.	Configure VLAN 72 in the Configure > Interfaces > Ethernet Ports 1-4 > VLAN Configuration page that appears. Set <i>VLAN Name</i> to VLAN-72-73 , <i>VLAN ID</i> to 72 , check Port 1 Enable , check Port 4 Enable , and click OK .
12.	This change causes the connection to the browser to drop. Browse to 192.45.72.1 and log into the Q2200.
13.	Select Interfaces → Ethernet Ports 1-4 under CONFIGURE in the tree view. In the Configure > Interfaces > Ethernet Ports 1-4 page that appears, select Edit in the Configuration pull-down menu for LAN Layer 2 Switch Interface.
14.	In the Configure > Interfaces > Ethernet Ports 1-4 > Edit Ethernet Configuration page that appears, set Port 4 <i>VLAN Link Mode</i> to trunk and click OK . NOTE: The port on the Layer-2 switch connecting to port 4 on the Q2200 was configured for 802.1q (VLAN) mode. This allows VLAN header information to be exchanged between the switch at the branch site and the Q2200. The branch site contains voice VLAN 72 and data VLAN 73.
15.	In the Configure > Interfaces > Ethernet Ports 1-4 page that appears, select Add VLAN in the Configuration pull-down menu for LAN Layer 2 Switch Interface.
16.	Configure VLAN 73 in the Configure > Interfaces > Ethernet Ports 1-4 > VLAN Configuration page that appears. Set <i>VLAN Name</i> to VLAN-73-72 , <i>VLAN ID</i> to 73 , check Port 4 Enable , <i>IP I/F Name</i> to iplan73 , <i>IP Address</i> to 192.45.73.1 , <i>Subnet Mask</i> to 255.255.255.0 , and click OK .

Step	Description
17.	Select Interfaces → T1 Port 1 under CONFIGURE in the tree view. In the Configure > Interfaces > T1 Port 1 page that appears, select Edit T1 in the Controls pull-down menu for T1 Port Name t1-1 .
18.	<p>In the Configure > Interfaces > T1 Port 1 > Edit T1 Configuration page that appears, configure the line settings needed to connect the T1 to the network and click OK.</p> 
19.	In the Configure > Interfaces > T1 Port 1 page that appears, select Edit IP in the Controls pull-down menu for PPP I/F Name ppp-1 .
20.	In the Configure > Interfaces > T1 Port 1 > Edit IP Configuration page that appears, set <i>IP Address</i> to 40.1.1.2 , <i>Subnet Mask</i> to 255.255.255.0 and click OK .
21.	Select Router → Routes under CONFIGURE in the tree view. In the Configure > Router > Routes page that appears, click Add for Default Route.
22.	In the Configure > Router > Routing > Route Configuration page that appears, set <i>Name</i> to DefRoute , <i>Gateway IP Address</i> to 40.1.1.1 , select ipwan in the <i>Gateway Interface</i> list and click OK .
23.	Select Firewall → Global Settings under CONFIGURE in the tree view. In the Configure > Firewall > Global Settings page that appears, uncheck Enable ACL Firewall , uncheck Enable Intrusion Detection and click OK . These Application Notes do not address firewall configuration.
24.	Click OK at the ‘Disabling the Firewall leaves the LAN and the Router unprotected.’ popup that appears.
25.	Select Router → NAT under CONFIGURE in the tree view. In the Configure > Router > NAT page that appears, uncheck NAT and click OK .
26.	Click OK at the ‘Changing the NAT configuration will terminate the session. Do you want to continue?’ popup that appears.
27.	If logged in remotely, the previous step may cause the connection to drop. If so, browse to 192.45.72.1 and log into the Q2200.

Step	Description
28.	Select QoS under CONFIGURE in the tree view. In the Configure > QoS page that appears, click QoS Summary .
29.	In the Configure > QoS > QoS Config Summary page that appears, click Policies for the Interface iplan [192.45.72.1] .
30.	In the Configure > QoS > QoS Config Summary > QoS Policies page that appears, click Add QoS Policy .
31.	<p>In the Configure > QoS > QoS Config Summary > QoS Policies > Add QoS Policy page that appears, set <i>Policy Name</i> to MapDSCP34to46, <i>Rank</i> to 1, <i>Source Address</i> to any, <i>Destination Address</i> to any, <i>Application</i> to any, <i>DSCP Match Option</i> to userEntered, <i>DSCP Match Value</i> to 34, <i>DSCP Marking Option</i> to userEntered, <i>DSCP Marking Value</i> to 46, check Enable Policy, check Enable DSCP Marking and click Create.</p> <p>NOTE: The Q-Series routers keep traffic marked with DSCP 46 (EF) in its own priority queue. However, DSCP 34 (AF4) marked traffic is kept in a Weighted Fair Queue (WFQ) with all other DSCP values. High traffic scenarios negatively impact call-signaling traffic when it is kept in the WFQ. To ensure highest priority for both signaling and audio, a policy was created to map DSCP 34 to 46 at both the corporate and branch site Q-series routers. This ensures that signaling and audio packets are transmitted using the priority queue, instead of the WFQ.</p>
32.	In the Configure > QoS > QoS Config Summary > QoS Policies page that appears, the newly added policy is listed.
33.	<p>Select Router → DHCP under CONFIGURE in the tree view. In the Configure > Router > DHCP page that appears, the message 'DHCP Operations Disabled' now appears for the DHCP Configuration. Select Enable DHCP Relay from the Configuration pull-down menu.</p> 
34.	Click OK at the 'This will clear all DHCP configuration. Are you sure?' popup that appears.

Step	Description
35.	<p>In the Configure > Router > DHCP page that appears, the message ‘There are no remote servers configured for DHCP Relay’ now appears for the DHCP Configuration. Select Add Remote DHCP Server from the Configuration pull-down menu.</p> 
36.	<p>In the Configure > Router > DHCP > Add Remote DHCP Server page that appears, set <i>Remote DHCP Server</i> to 192.45.70.38 and click OK.</p> 
37.	<p>Select System → System Restart under CONFIGURE in the tree view. In the Configure > System > System Restart page that appears, click OK to save the configuration and restart the Q2200.</p>
38.	<p>This change causes the connection to the browser to drop. Browse to 192.45.72.1 and log into the Q2200.</p>
39.	<p>Select QoS → QoS Summary under CONFIGURE in the tree view. In the Configure > QoS > QoS Config Summary page that appears, click Interface for the Interface ipwan [40.1.1.2].</p>

Step	Description
40.	<p>In the Configure > QoS > QoS Config Summary > QoS Interface Configuration page that appears, the QoS configuration for the ipwan interface is listed. Modify the Bandwidth for the link and/or each DSCP value as necessary.</p> <p>NOTE: By default, the Q-Series routers perform traffic shaping on the traffic going through the WAN interface. Expedited forwarding traffic is limited to 33% of the bandwidth shown at the top of the screen. These default settings are optimal for the targeted small and/or low bandwidth configurations for which the products are intended. These values can be configured.</p>

6. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality 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 T-1 link while still achieving good voice quality. Prioritization of voice traffic was achieved by implementing DiffServ-based QoS on a PPP link. 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. The bulk call generator was also used to quantify the speech quality of the VoIP calls. At the end of the performance test, it was verified that the network devices continued to operate successfully.

6.1. 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 branch office sites using IP trunks between the sites,
- Inter-office calls using G.711mu-law and G.729 codec sets, and conferencing,
- 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 with a bulk call generator and data traffic generator running simultaneously. The most important verification step was checking voice quality while transmitting low priority data traffic for small office scenarios.

6.2. Test Results

All feature functionality and performance test cases passed. The Q-Series QoS implementation (including the signaling packet DSCP remarking) over a PPP link yielded good voice quality. The stability of the Avaya/Kentrox solution was successfully verified through performance tests.

7. Verification Steps

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

1. Verify IP communication from the WAN router 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**.
3. If a Q-Series 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 Q-Series browser interface.
4. Place calls between the DCP and IP telephones at each site. If the call cannot be established, check the activity of the IP trunks using the IP Office **System Monitor**.
5. If the voice quality is poor, check the QoS configuration in the Q-Series routers.
6. Use the Kentrox tools to ensure the traffic is going in the intended queues.

8. 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 option 3
- Direct: (503) 643-1681 option 3
- Email: care@kentrox.com

9. Conclusion

These Application Notes describe the configuration steps required for integrating the Kentrox Q-Series Q2400 and Q2200 Routers into a small office and/or low traffic/bandwidth Avaya IP Office infrastructure. For the configuration described in these Application Notes, the Q-Series routers were responsible for enforcing QoS using DiffServ. The Avaya IP Office 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.

10. 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://support.avaya.com> and the Kentrox product documentation can be found at <http://www.kentrox.com>.

[1] Avaya IP Office 2.1 Manager, Issue 15c, May 2004.

[2] Kentrox QoS Access Router User's Guide, Software Release 1.3, Document #650-00319-03.

©2005 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 Developer*Connection* Program at devconnect@avaya.com.