



Application Notes for Radware LinkProof Multi-WAN Switch connected to Avaya Distributed Office in a Converged VoIP and Data Network - Issue 1.0

Abstract

These Application Notes describe the configuration of a Voice over IP (VoIP) solution using Radware LinkProof Multi-WAN Switch connected to an Avaya Distributed Office in an Avaya IP Telephony Environment. The Radware LinkProof Multi-WAN Switch was compliance-tested with Avaya Distributed Office with emphasis was placed on bandwidth management and traffic shaping in a converged VoIP and data network scenario.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration of a Voice over IP (VoIP) solution using Radware LinkProof Multi-WAN 3020 Switches connected to an Avaya Distributed Office in an Avaya IP Telephony Environment. Compliance testing emphasis was placed on maintaining the prioritization of VoIP traffic through bandwidth management and traffic shaping on the LinkProof Multi-WAN Switch in a converged VoIP and Data network scenario. Quality of Service (QoS) based on Layer 2 Priority (802.1p) and Layer 3 Differentiated Services (Diffserv) was implemented across the network to prioritize voice traffic over the LAN. The Avaya IP Telephones get QoS priority settings from Avaya Distributed Office and are enforced in the network by the LinkProof Switches. To verify VoIP traffic was give priority over data traffic, tests were performed by over subscribing the LAN interfaces with low priority data traffic and verifying that acceptable voice quality was achieved when calls were routed over all of the LAN interfaces. Compliance testing included verifying Switch failover, QoS, throughput, Multi-WAN connections, load balancing.

1.1. Radware LinkProof 3020 Switch

LinkProof optimizes and routes traffic across Internet links, moderating bandwidth loads to ensure connection fault tolerance and scalability. Utilizing compression, TCP session handling and caching, LinkProof accelerates application responsiveness. Securing all enterprise entry points and cleansing all link traffic, LinkProof delivers Denial of Service protection and intrusion prevention to insulate distributed applications, resources and users against attack.

2. Hardware Configuration

The configuration in **Figure 1** shows a multi site converged VoIP and data network with load balancing, Layer2/Layer3 QoS and Redundancy.

For compliance testing, a centralized corporate DHCP server was used. To better manage the different traffic types, the voice and data traffic were separated onto different VLANs.

2.1. Control Room

The Main Site consisted of two Radware LinkProof Multi-WAN 3020 Switches, Avaya Distributed Office, one Avaya 9630 IP, one Avaya 9620 IP and one Corporate DHCP/File Server. The corporate site provided a DHCP/File server for assigning IP network parameters and to download settings to the Avaya IP telephones. The LinkProof 3020 switches were configured to support load balancing, Layer2/Layer3 QoS and Redundancy.

2.2. Branch site

Lab-A consisted of a Radware LinkProof Multi-WAN 3020 Switch, one Avaya 9630 IP Telephone, one Avaya 9620 IP and one PC on Datavlan2. The LinkProof 3020 switch was configured to support Layer2 and Layer3 QoS.

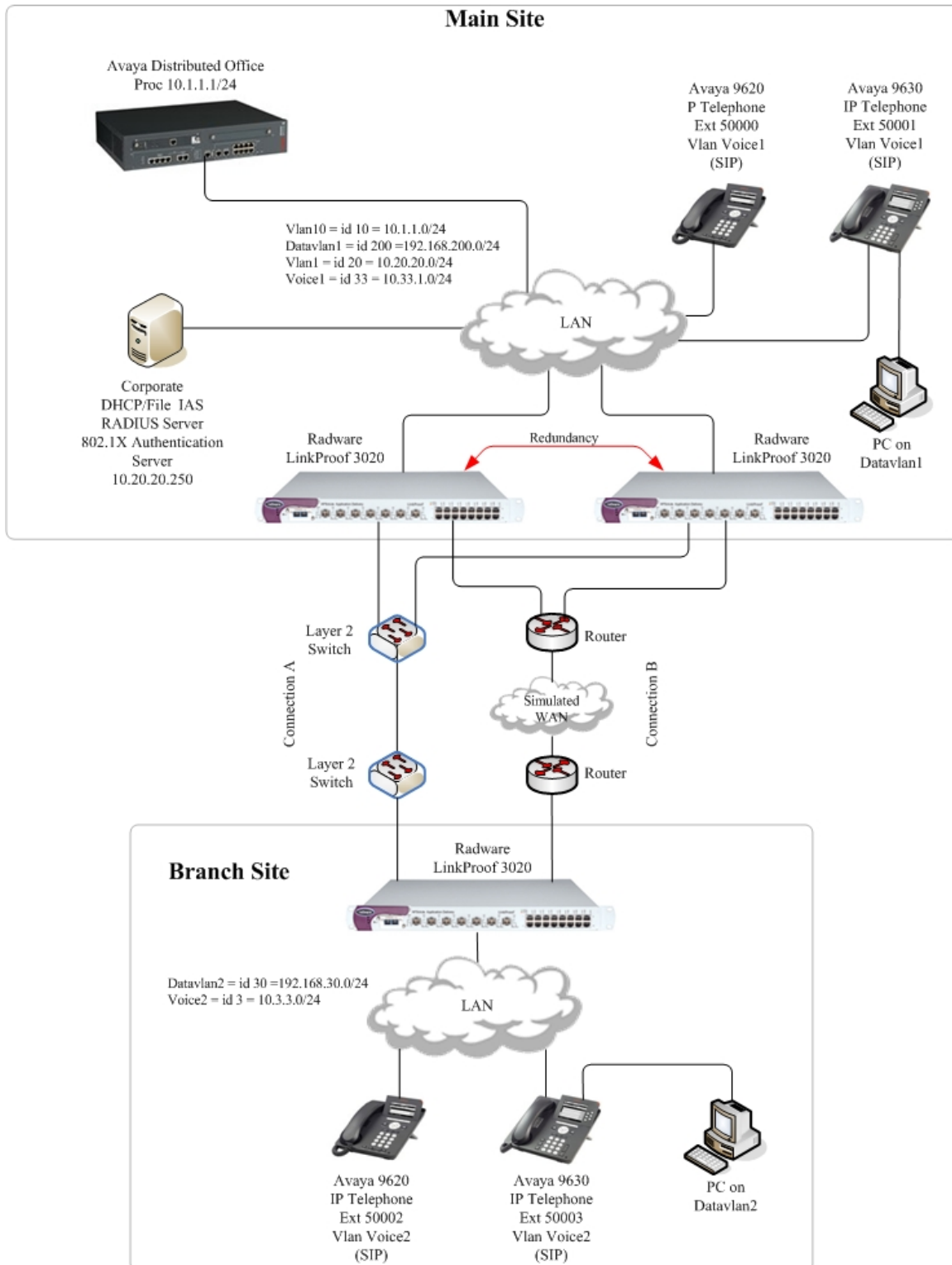


Figure 1: Network Configuration

3. Equipment and Software Validated

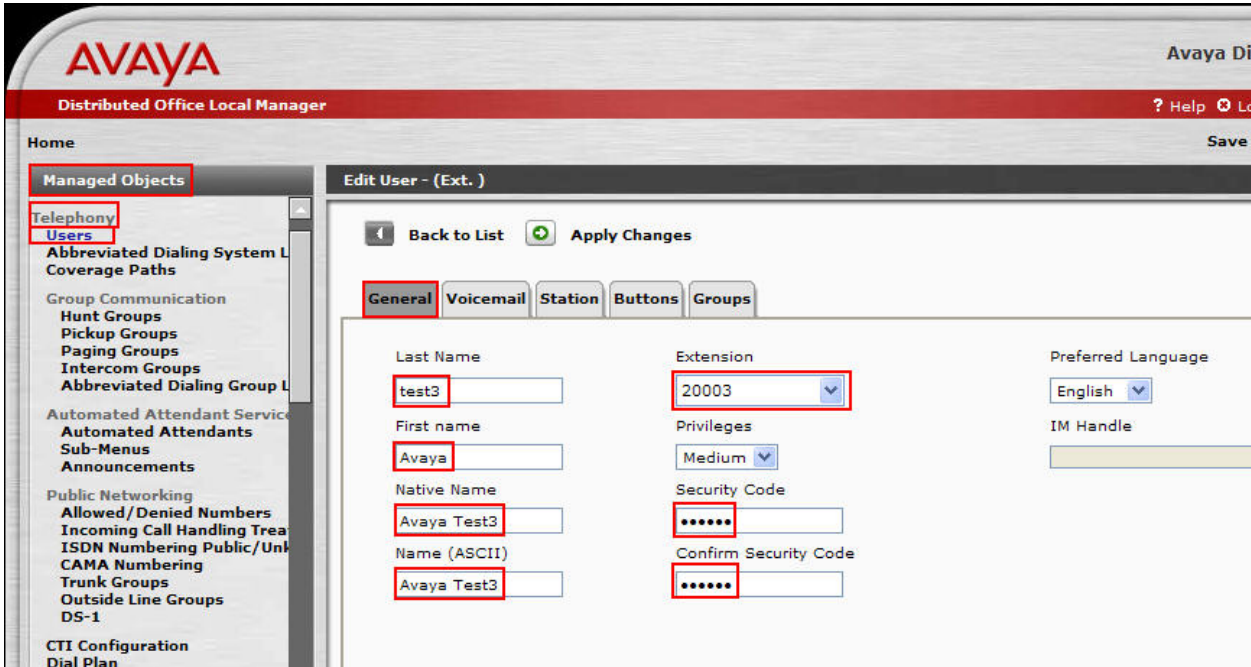
The following equipment and software/firmware were used for the sample configuration provided:

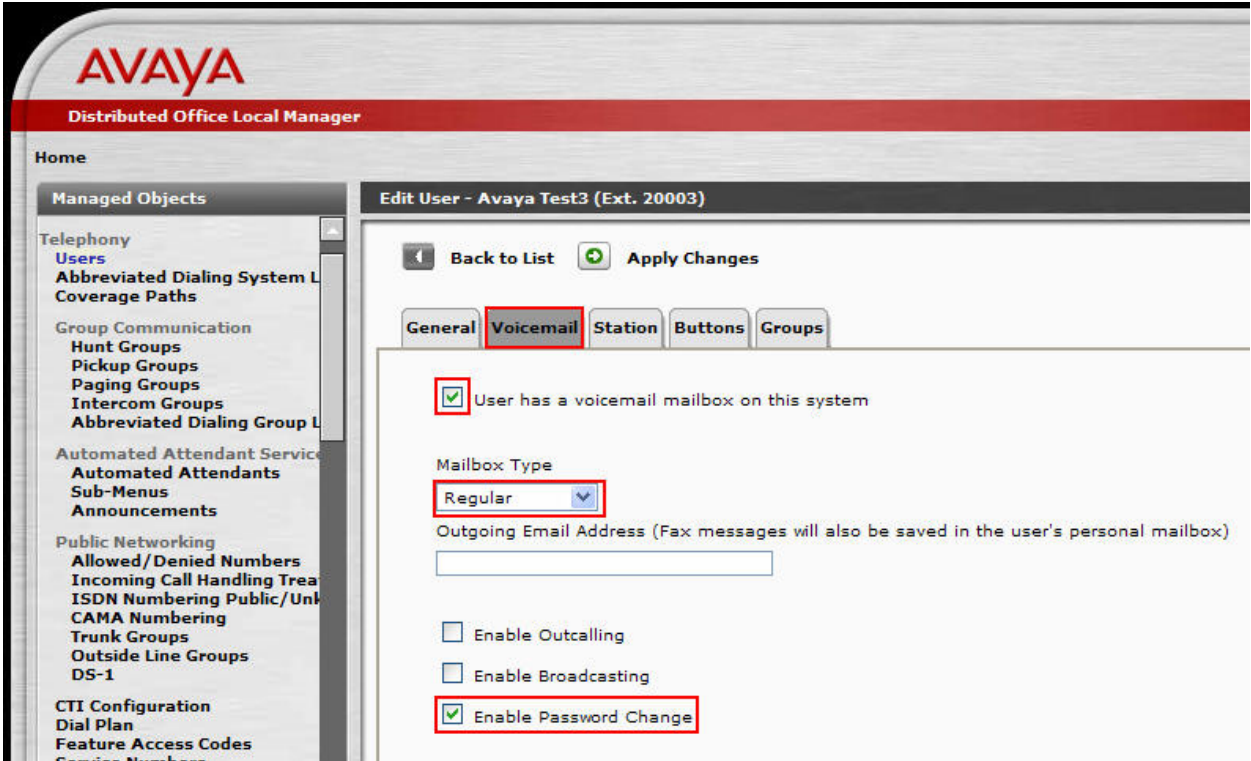
Equipment	Software/Firmware
Avaya Distributed Office i120 with Avaya Distributed Office AM110 card	I120 sw.27.17.1 DO AM110 1.1.1_41.03
Avaya 9600 Series IP Telephones	Avaya one-X™ Deskphone SIP 1.5 (SIP)
Radware LinkProof Multi-WAN 3020 Switch	FW-K.12.22

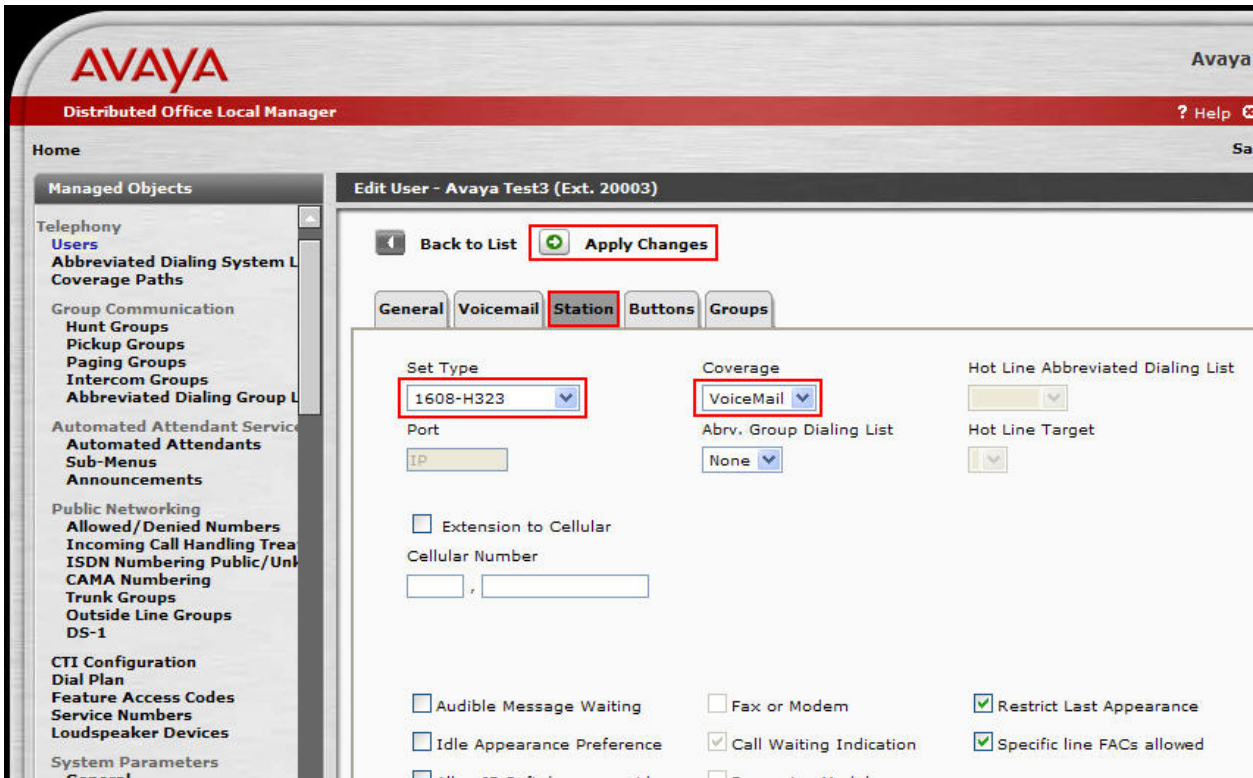
Note: This testing is also applicable to the same version of the Avaya Distributed Office i40.

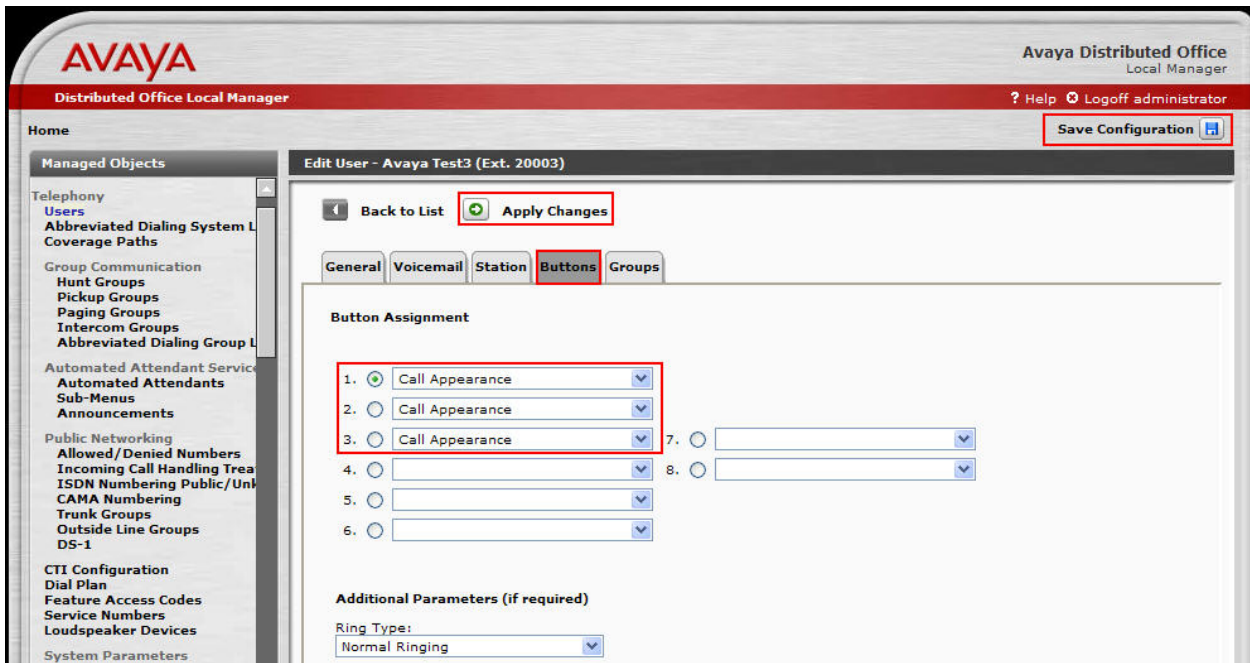
4. Avaya Distributed Office Configuration

Avaya Distributed Office is administered via a web interface. In the sample network the Avaya Distributed Office was assigned the IP address 10.1.1.1 and the URL <http://10.1.1.1> was used to access the administration interface. For information on how to access and setup a factory default system, refer to [1].

Step	Description
1.	<p>Navigate to the Edit User window by clicking Managed Object→Telephony→Users. Enter the values displayed below and then click Apply Changes. Last Name, First name and Native Name can be any descriptive text that identifies this user. Name (ASCII) may be populated with the same information that is entered in Native Name. Security Code and Confirm Security code. Use the drop-down list for Extension and select any available extension. The remaining parameters were left at the default values.</p> 

Step	Description
2.	<p>Navigate to the Voicemail tab by clicking Voicemail. Check the User has a voicemail mailbox on this system and Enable Password Change check boxes. Use the drop-down list for Mailbox Type to select “Regular”. Press the Station tab to continue.</p>  <p>The screenshot shows the Avaya Distributed Office Local Manager interface. The main title is 'AVAYA Distributed Office Local Manager'. The left sidebar contains a 'Managed Objects' tree with categories like Telephony, Group Communication, Automated Attendant Services, Public Networking, and CTI Configuration. The 'Voicemail' tab is selected in the top navigation bar. The 'Edit User - Avaya Test3 (Ext. 20003)' page is displayed, showing a 'General' tab and a 'Voicemail' tab. The 'Voicemail' tab contains the following settings: a checked checkbox for 'User has a voicemail mailbox on this system', a 'Mailbox Type' dropdown menu set to 'Regular', an 'Outgoing Email Address' field, and three checkboxes: 'Enable Outcalling' (unchecked), 'Enable Broadcasting' (unchecked), and 'Enable Password Change' (checked). The 'Station' tab is highlighted in the left sidebar.</p>

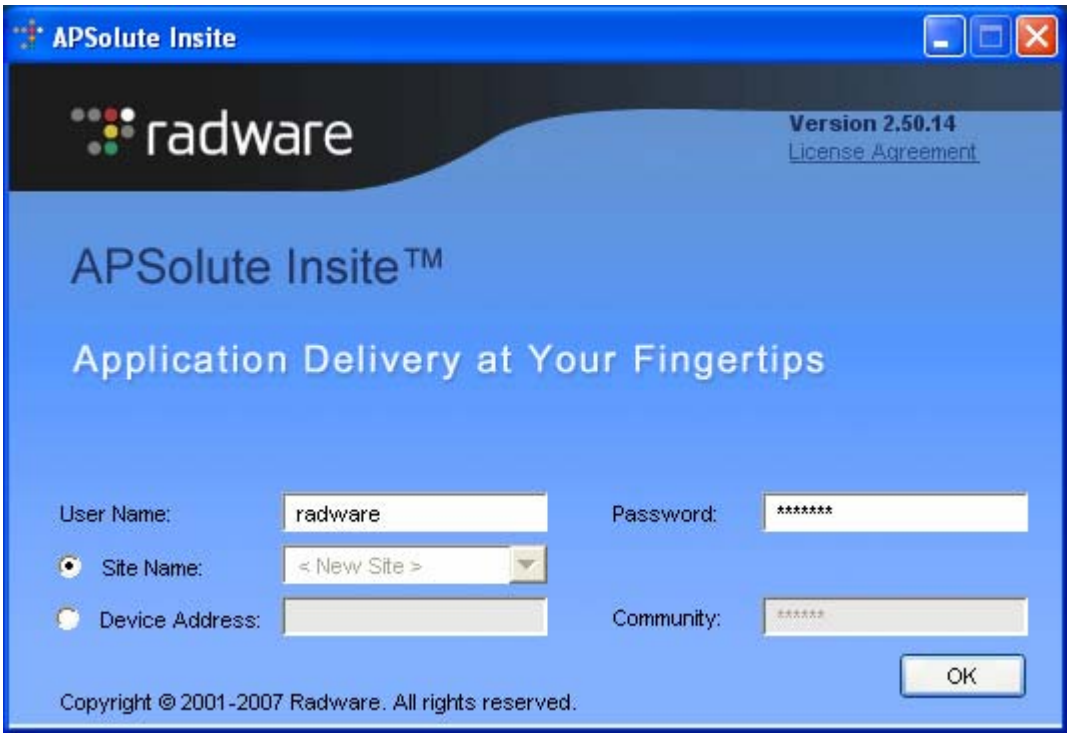
Step	Description
3.	<p>Navigate to the Station tab by clicking Station. Use the drop-down list for Set Type to select “1608-H323” and use the drop-down list for Coverage to select “VoiceMail”. The remaining parameters were left at the default values. Press the Buttons tab to continue.</p>  <p>The screenshot shows the Avaya Distributed Office Local Manager interface. The left sidebar contains a 'Managed Objects' tree with categories like Telephony, Group Communication, Automated Attendant Services, Public Networking, and CTI Configuration. The main area is titled 'Edit User - Avaya Test3 (Ext. 20003)'. It has tabs for General, Voicemail, Station, Buttons, and Groups. The 'Station' tab is active. In this tab, there are three main sections: 'Set Type' with a dropdown menu showing '1608-H323', 'Coverage' with a dropdown menu showing 'VoiceMail', and 'Hot Line Abbreviated Dialing List' with a dropdown menu. Below these are fields for 'Port' (set to 'IP'), 'Abrv. Group Dialing List' (set to 'None'), and 'Hot Line Target'. There are also checkboxes for 'Extension to Cellular', 'Audible Message Waiting', 'Idle Appearance Preference', 'Fax or Modem', 'Call Waiting Indication', 'Restrict Last Appearance', and 'Specific line FACs allowed'. The 'Apply Changes' button is highlighted with a red box.</p>

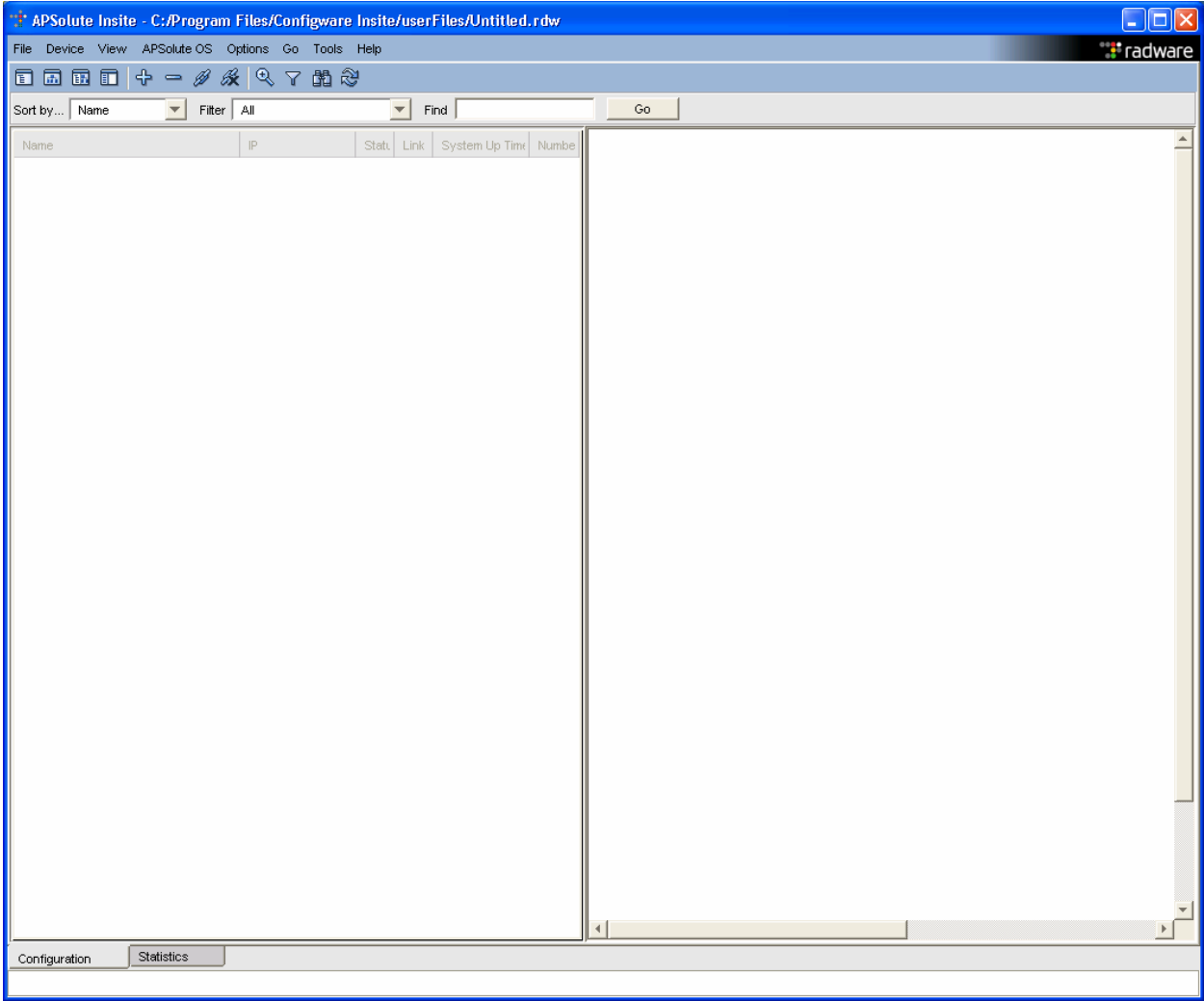
Step	Description
4.	<p>Navigate to the Buttons tab by clicking Buttons. Use the drop list for Button Assignment 1 – 3 and select “Call Appearance”. The remaining parameters were left at the default values. Click Apply Changes and then click Save Configuration.</p> <p>Note the user may receive a message indicating the system is busy if Save Configuration is clicked immediately after Apply Changes. If that occurs, simply click Save Configuration after one or two minutes.</p> 
5.	Repeat Steps 1 thru 4 for each Avaya IP Telephone. Click Apply Changes

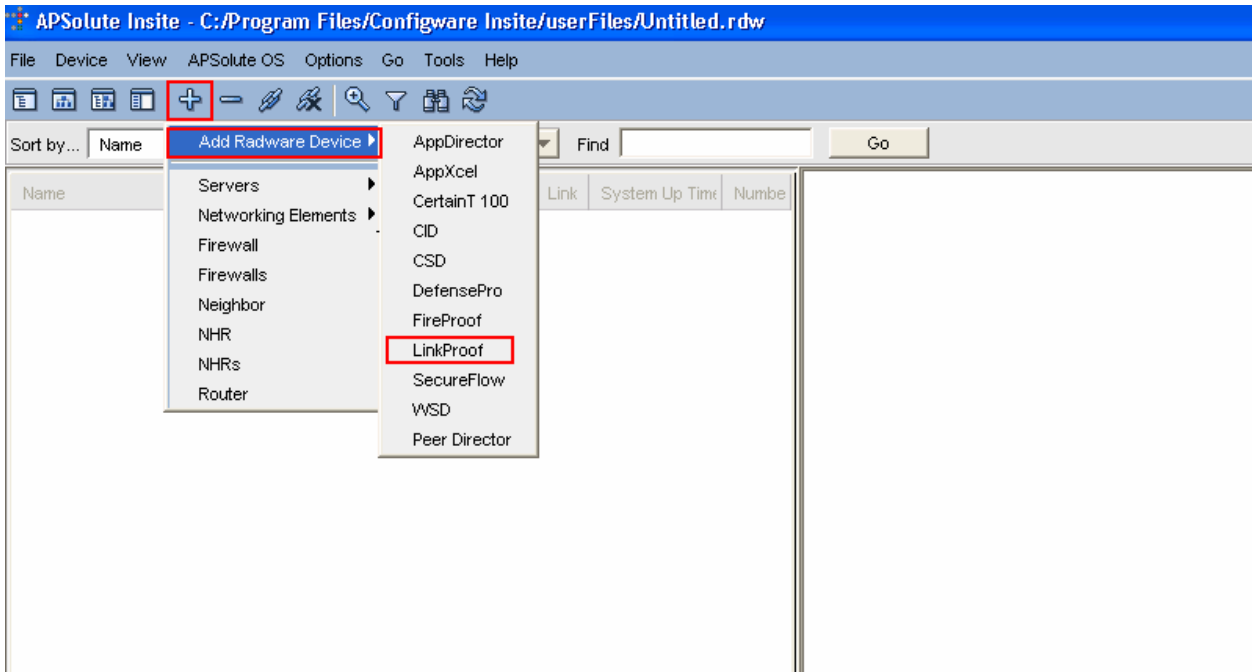
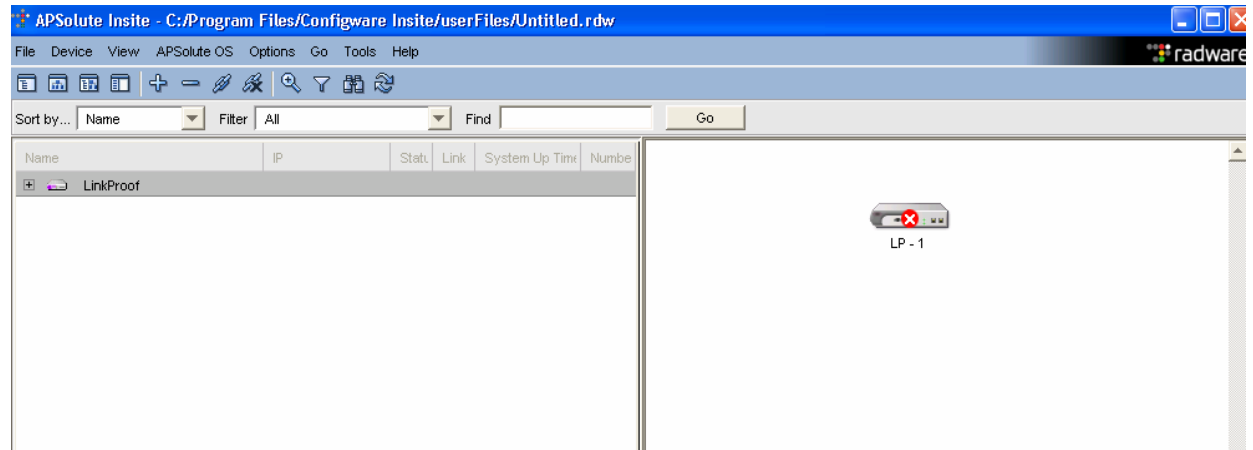
5. Configuration Radware LinkProof Multi-WAN 3020 Switch

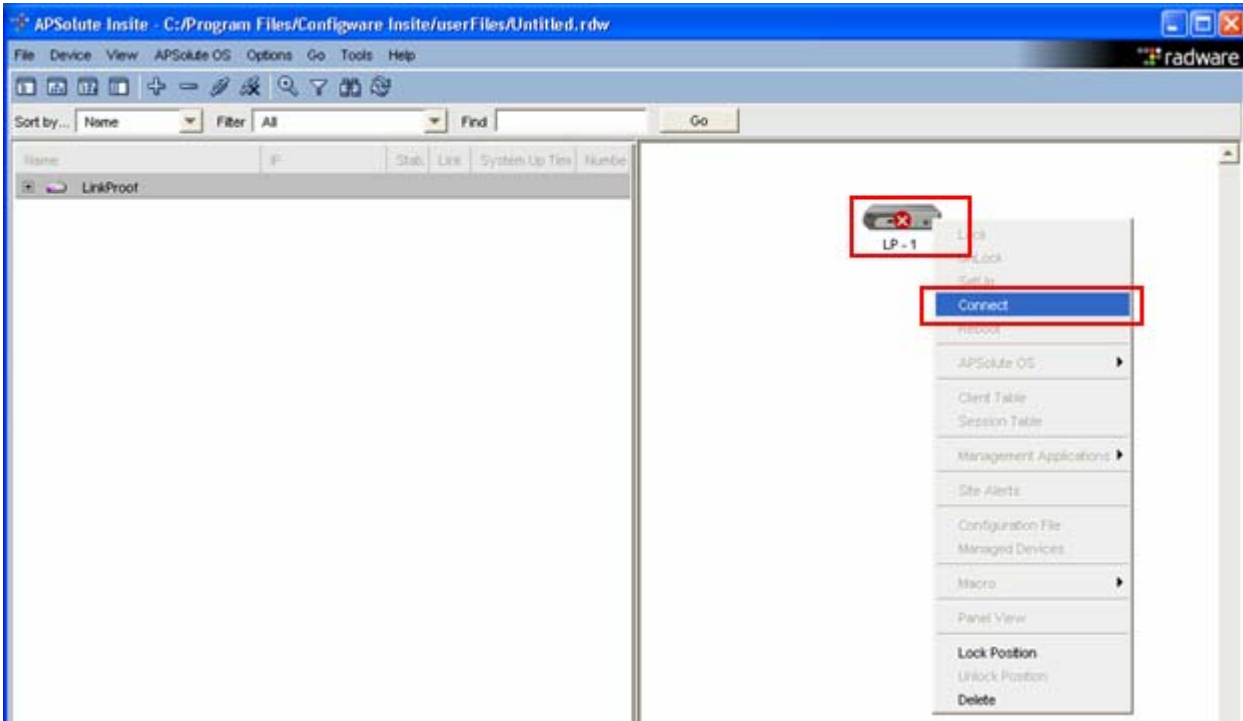
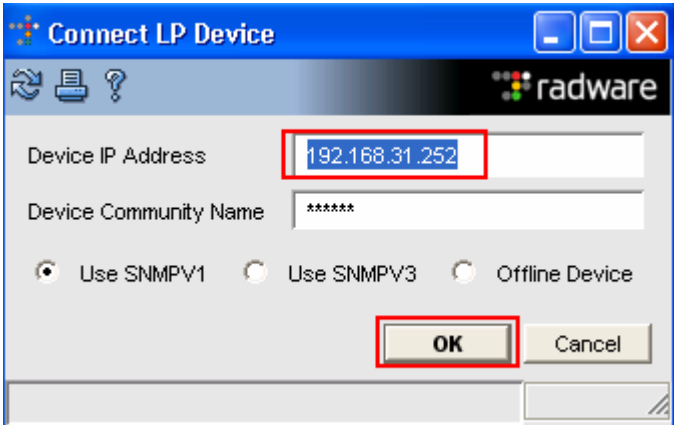
This section addresses how to configure the Radware LinkProof Multi-WAN 3020 Switches. Please refer to section [6] for basic setup and installation of the LinkProof Switch and the APSolute Insite software. This section will pertain to the configuration tested. Redundancy testing of a second LinkProof Switch, **Figure 1**, was compliance tested but the configuration of the second LinkProof switch will not be covered in the document.

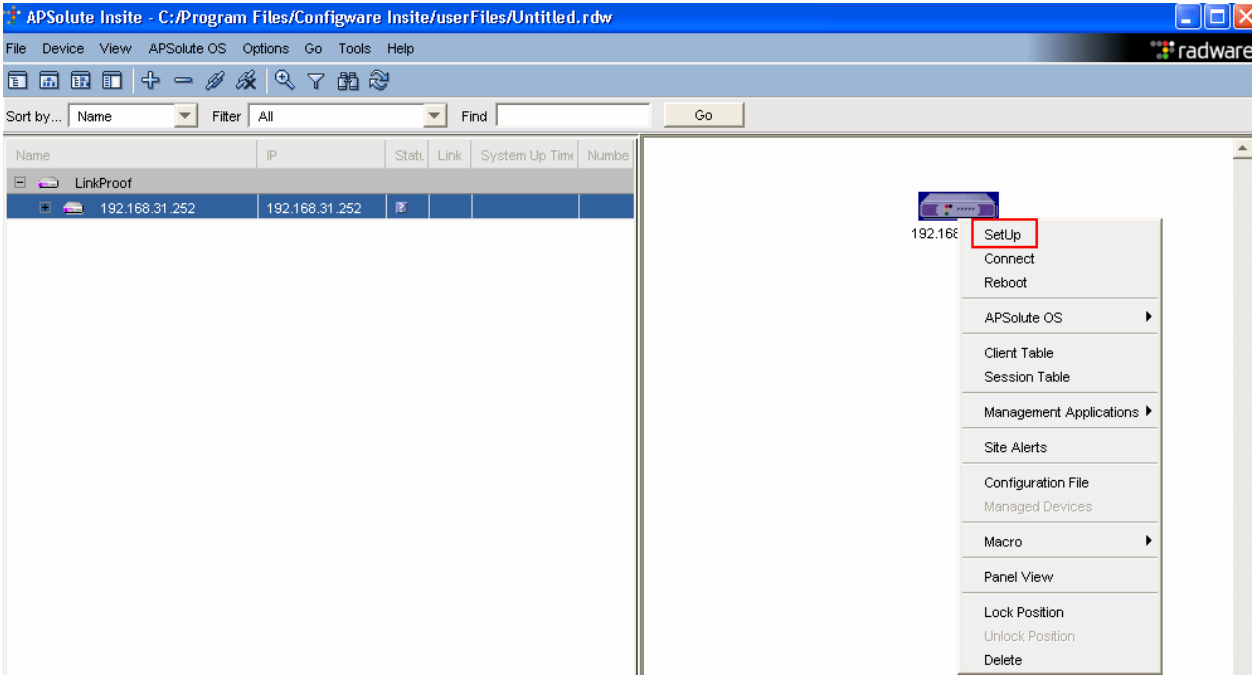
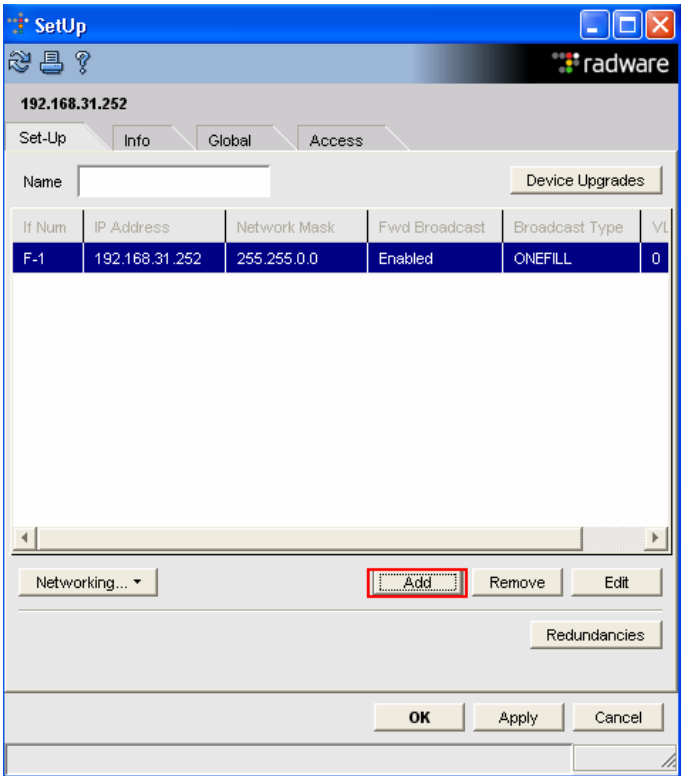
For this configuration different priorities were used for each route based on the speeds of the links. The following configuration uses the switched interface as the primary route with the routed interface as a standby which will only be used if the “main” route fails. If the routed interface on the LinkProof switch is configured to **Mode regular**, the interfaces will load balance between the two routes.

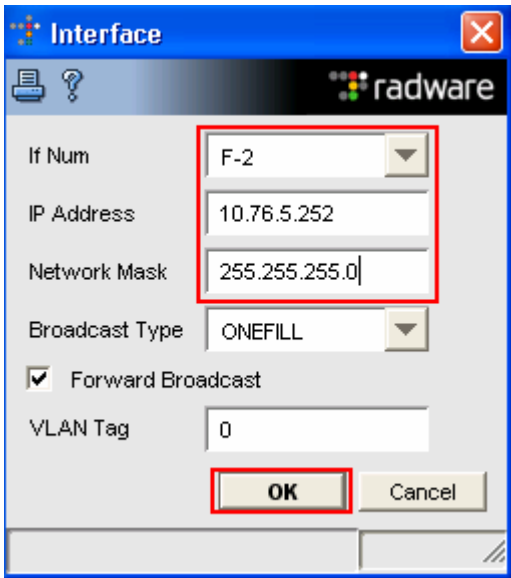
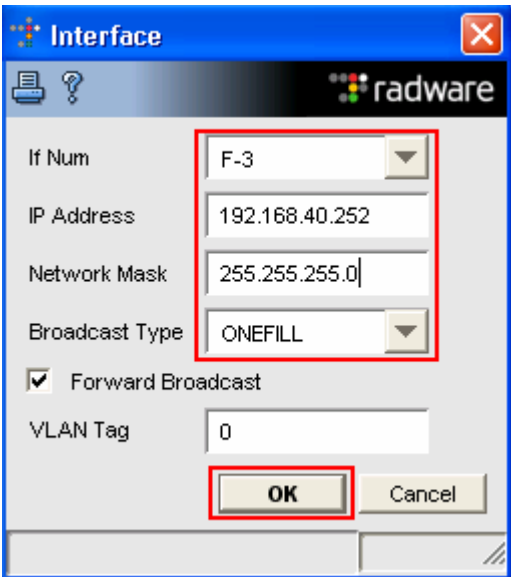
Step	Description
1.	<p>Log into the APSolute using the default credentials which can be obtained from the Radware LinkProof documentation.</p> 

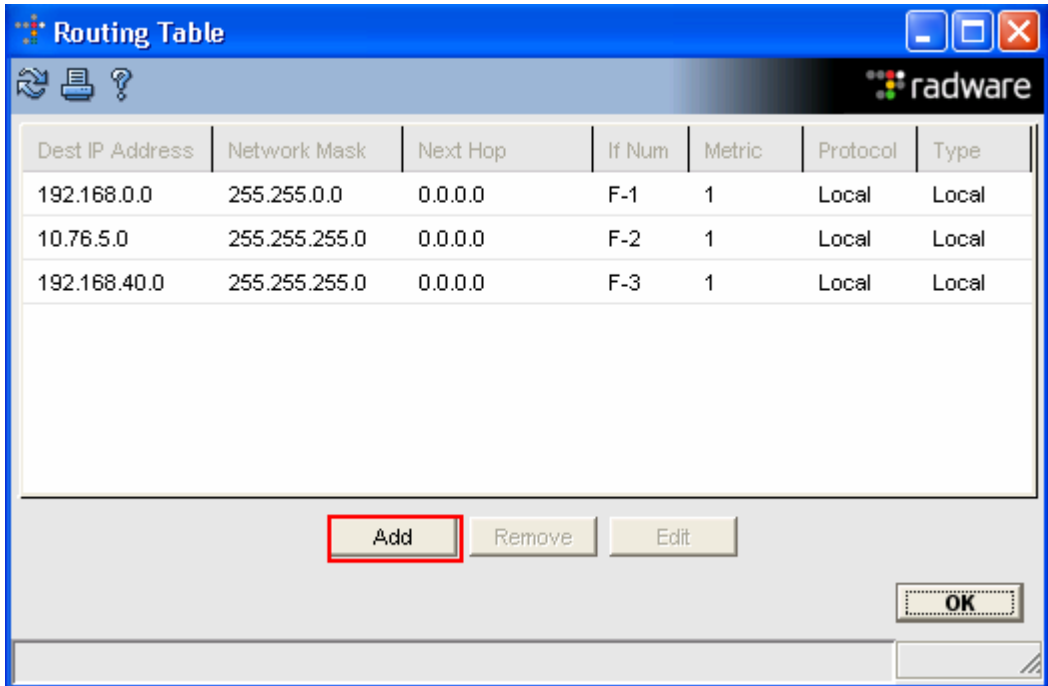
Step	Description
2.	<p>The following APSolute Insite main screen is displayed.</p> 

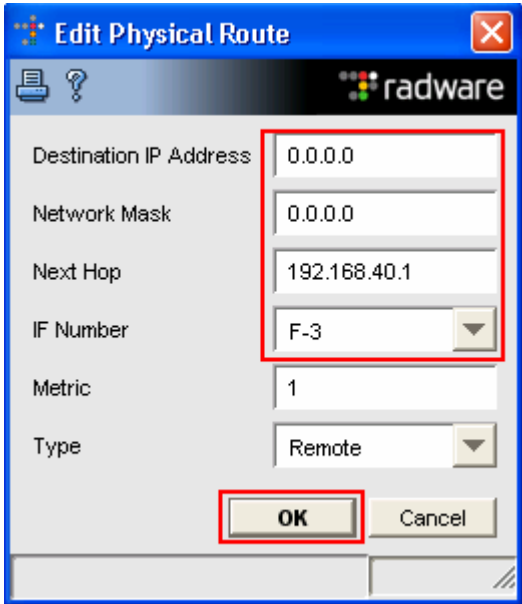
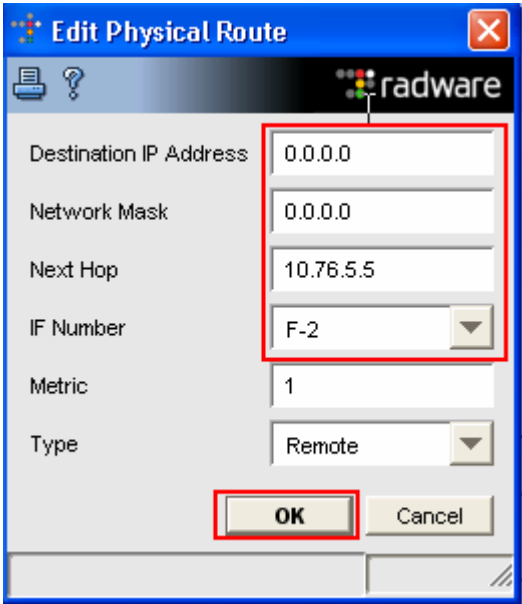
Step	Description
3.	<p>Add LinkProof device for the Main site, Select Device → Add Radware Device → LinkProof</p>  <p>The LinkProof Icon for the Main site appears</p> 

Step	Description
4.	Right click on the Main site LinkProof icon, Select Connect to the device.
	 <p>The screenshot shows the APSolute Insite application window. On the left, a tree view contains a 'LinkProof' icon. On the right, a context menu is open, listing various actions. The 'Connect' option is highlighted with a red rectangle. Other options include 'Lock', 'Unlock', 'APSSuite OS', 'Client Table', 'Session Table', 'Management Applications', 'Site Alerts', 'Configuration File', 'Managed Devices', 'Macro', 'Panel View', 'Lock Position', 'Unlock Position', and 'Delete'.</p>
	<p>The Connect LP Device box appears, enter the IP address of the Main site LinkProof device, select OK to continue.</p>  <p>The screenshot shows the 'Connect LP Device' dialog box. It has a title bar with the Radware logo. Inside, there are two text input fields: 'Device IP Address' containing '192.168.31.252' and 'Device Community Name' containing '*****'. Below these are three radio buttons: 'Use SNMPV1' (selected), 'Use SNMPV3', and 'Offline Device'. At the bottom right are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a red rectangle.</p>

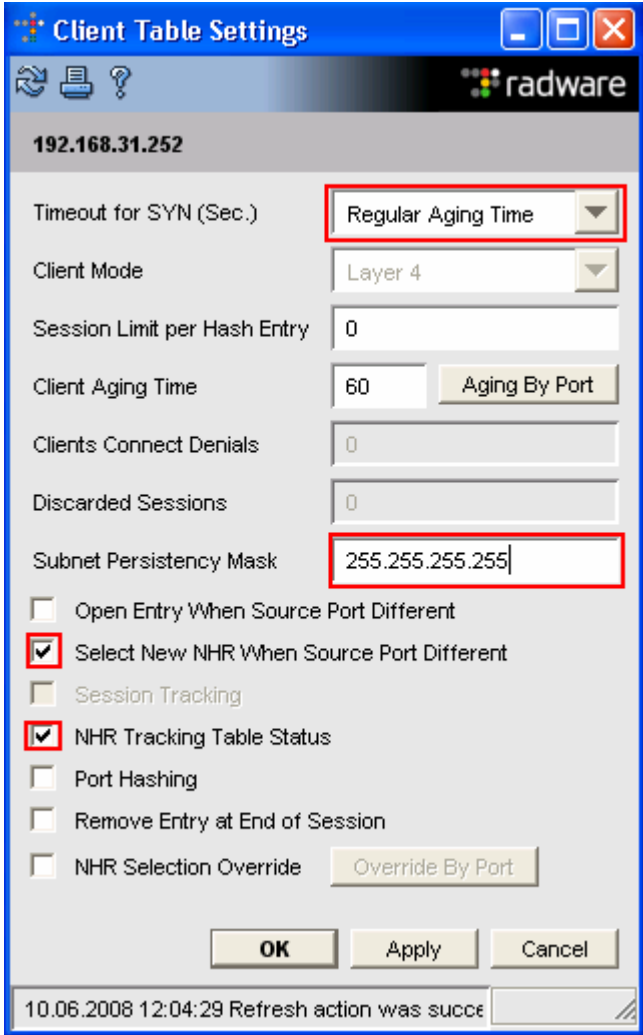
Step	Description
5.	<p>Create interfaces F-2 and F-3, Right mouse click on the LinkProof device. Select Setup.</p>  <p>The SetUp box appears, select Add</p> 

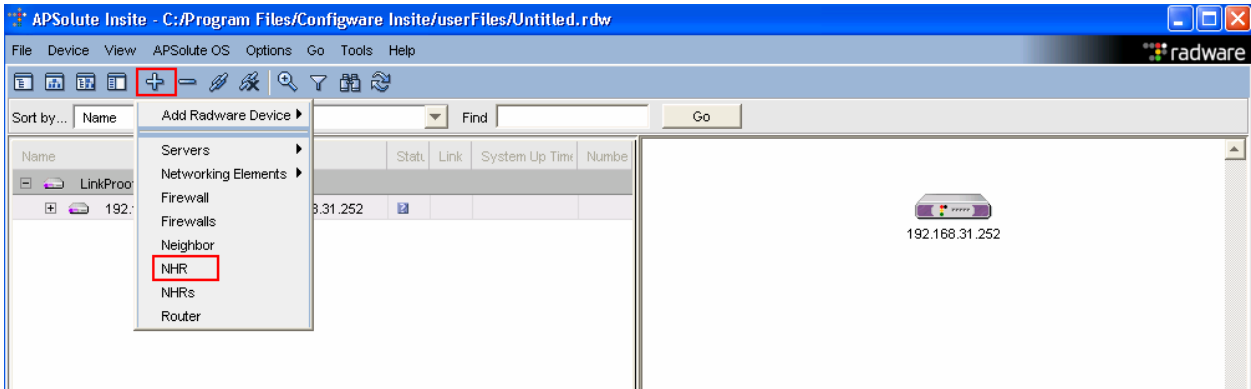
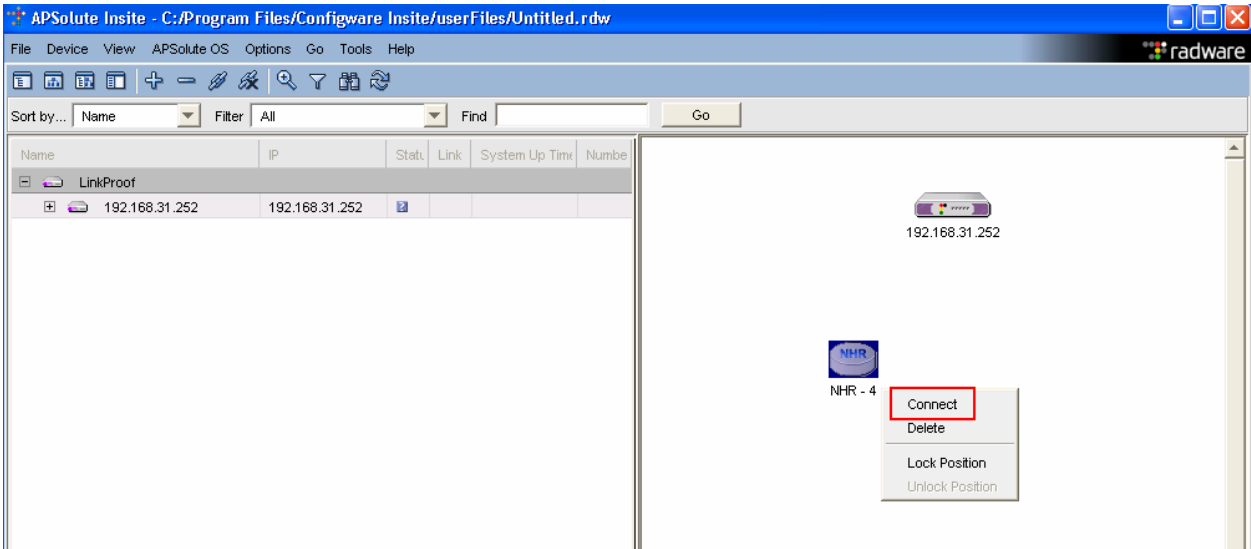
Step	Description
6.	<p>The Interface box appears, click on the pull down tab for If Num, select F-2. Enter the IP Address and Network Mask, select OK to continue.</p> 
7.	<p>Repeat Step 5 to create Interface F-3. Select OK to continue.</p> 

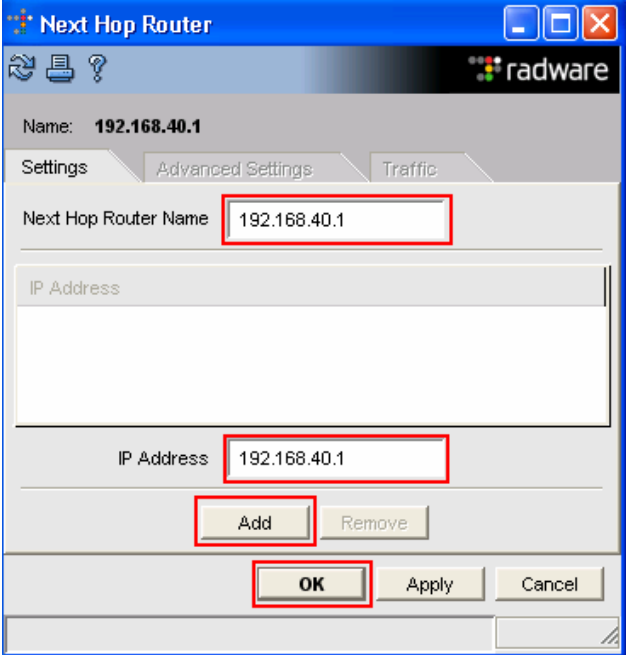
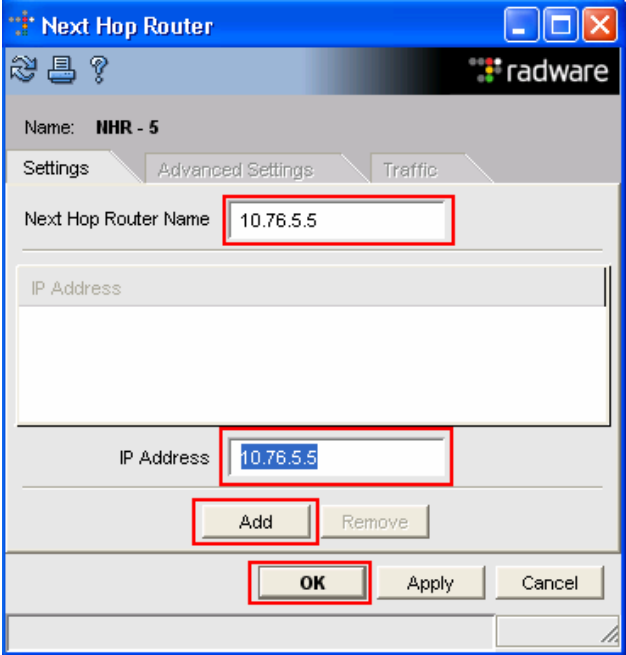
Step	Description																												
8.	<p>Add routes to the routing table.</p> <p>Right mouse click on the LinkProof device. Select Setup, click the pull down tab for Networking, select Routing Table. The Routing Table box appears, add the follow routes, select Add.</p>  <table><thead><tr><th>Dest IP Address</th><th>Network Mask</th><th>Next Hop</th><th>If Num</th><th>Metric</th><th>Protocol</th><th>Type</th></tr></thead><tbody><tr><td>192.168.0.0</td><td>255.255.0.0</td><td>0.0.0.0</td><td>F-1</td><td>1</td><td>Local</td><td>Local</td></tr><tr><td>10.76.5.0</td><td>255.255.255.0</td><td>0.0.0.0</td><td>F-2</td><td>1</td><td>Local</td><td>Local</td></tr><tr><td>192.168.40.0</td><td>255.255.255.0</td><td>0.0.0.0</td><td>F-3</td><td>1</td><td>Local</td><td>Local</td></tr></tbody></table>	Dest IP Address	Network Mask	Next Hop	If Num	Metric	Protocol	Type	192.168.0.0	255.255.0.0	0.0.0.0	F-1	1	Local	Local	10.76.5.0	255.255.255.0	0.0.0.0	F-2	1	Local	Local	192.168.40.0	255.255.255.0	0.0.0.0	F-3	1	Local	Local
Dest IP Address	Network Mask	Next Hop	If Num	Metric	Protocol	Type																							
192.168.0.0	255.255.0.0	0.0.0.0	F-1	1	Local	Local																							
10.76.5.0	255.255.255.0	0.0.0.0	F-2	1	Local	Local																							
192.168.40.0	255.255.255.0	0.0.0.0	F-3	1	Local	Local																							

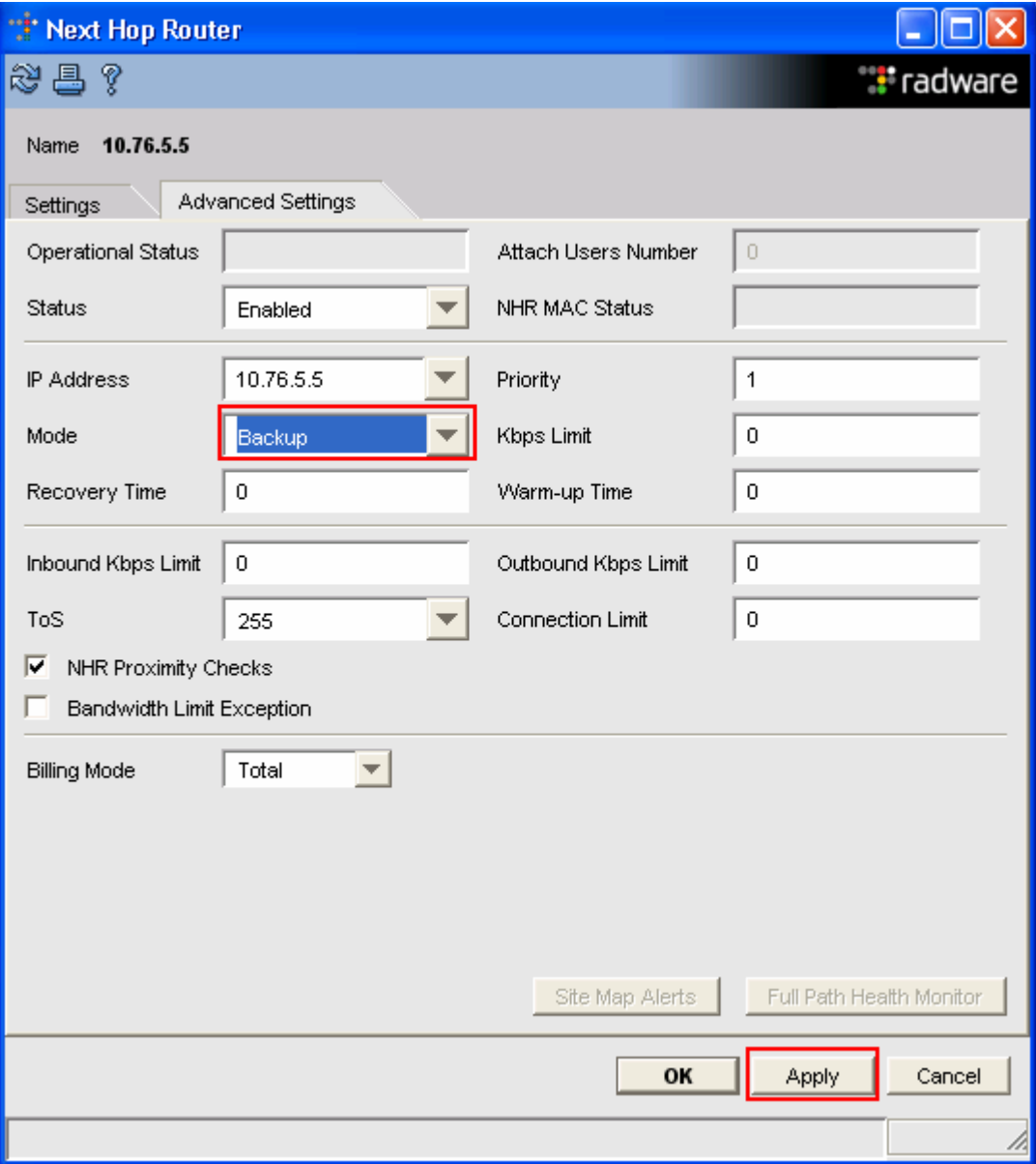
Step	Description
9.	<p>Add the following Default Routes, Add Destination IP Address, Mask Next Hop, IF Number. Click OK to continue.</p> <div data-bbox="371 340 889 940">  </div> <div data-bbox="911 340 1429 940">  </div>

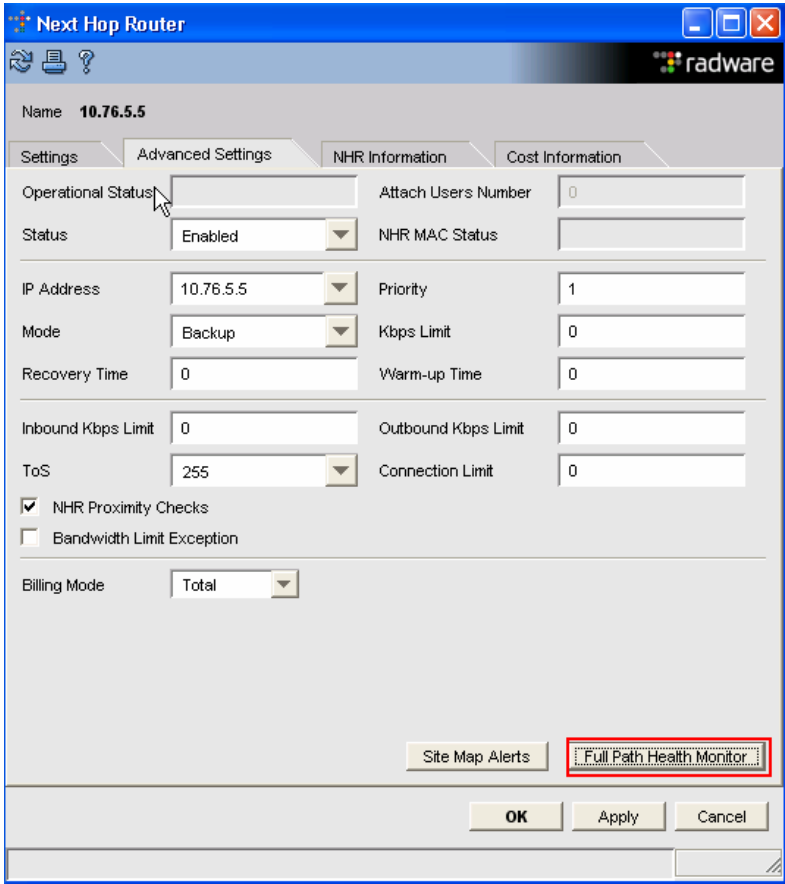
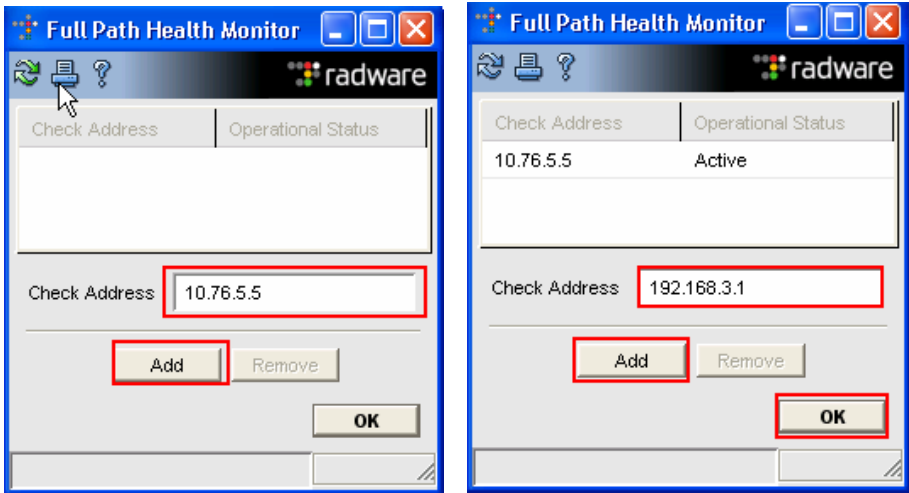
Step	Description
10.	<p>Add the following Local Routes, Add Destination IP Address, Mask Next Hop, IF Number. Click OK to continue.</p> <div data-bbox="375 342 889 940"> </div> <div data-bbox="914 342 1427 940"> </div> <div data-bbox="643 974 1157 1575"> </div>

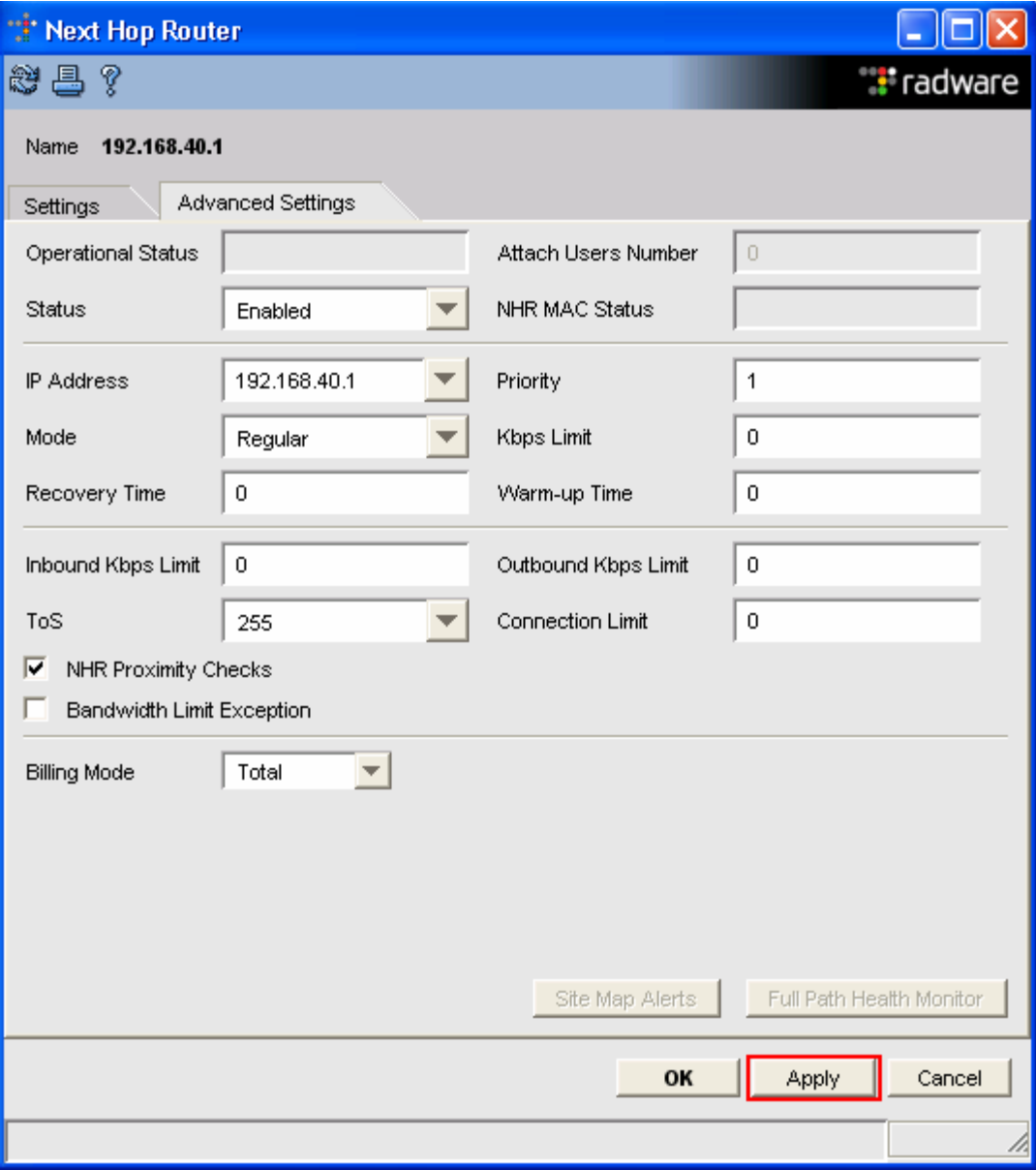
Step	Description
11.	<p>Configure the Client Table Settings on the LinkProof device.</p> <p>Right mouse click on the LinkProof device, select Setup, after the Setup box appears, select the Global tab, select Client Table Settings, then Edit Settings.</p> <p>Set the Following:</p> <ol style="list-style-type: none"> Timeout for SYN (SEC) to Regular Aging Time Subnet Persistency Mask to 255.255.255.255 Check Select New NHR When Source Port Different Check NHR Tracking Table Status  <p>The screenshot shows the 'Client Table Settings' window for IP address 192.168.31.252. The settings are as follows:</p> <ul style="list-style-type: none"> Timeout for SYN (Sec.): Regular Aging Time (selected) Client Mode: Layer 4 Session Limit per Hash Entry: 0 Client Aging Time: 60 (Aging By Port button is active) Clients Connect Denials: 0 Discarded Sessions: 0 Subnet Persistency Mask: 255.255.255.255 <input type="checkbox"/> Open Entry When Source Port Different <input checked="" type="checkbox"/> Select New NHR When Source Port Different <input type="checkbox"/> Session Tracking <input checked="" type="checkbox"/> NHR Tracking Table Status <input type="checkbox"/> Port Hashing <input type="checkbox"/> Remove Entry at End of Session <input type="checkbox"/> NHR Selection Override (Override By Port button is active) <p>Buttons at the bottom: OK, Apply, Cancel.</p> <p>Status bar: 10.06.2008 12:04:29 Refresh action was succe...</p>

Step	Description
12.	<p>Create the following Next Hop Router (NHR) entries. Click + → NHR</p>  <p>A NHR icon appears, right mouse click on the NHR icon and select Connect.</p> 

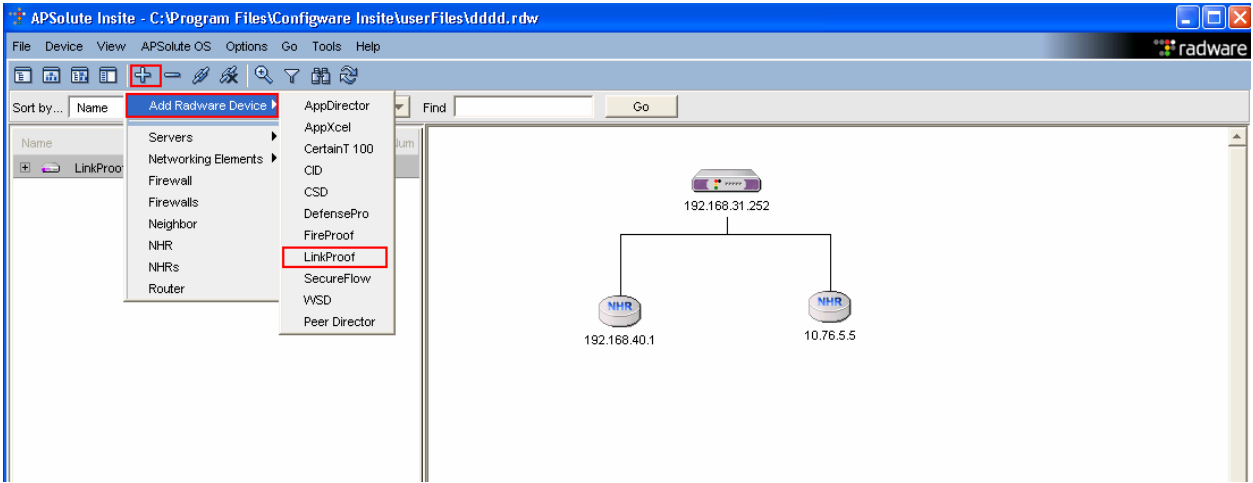
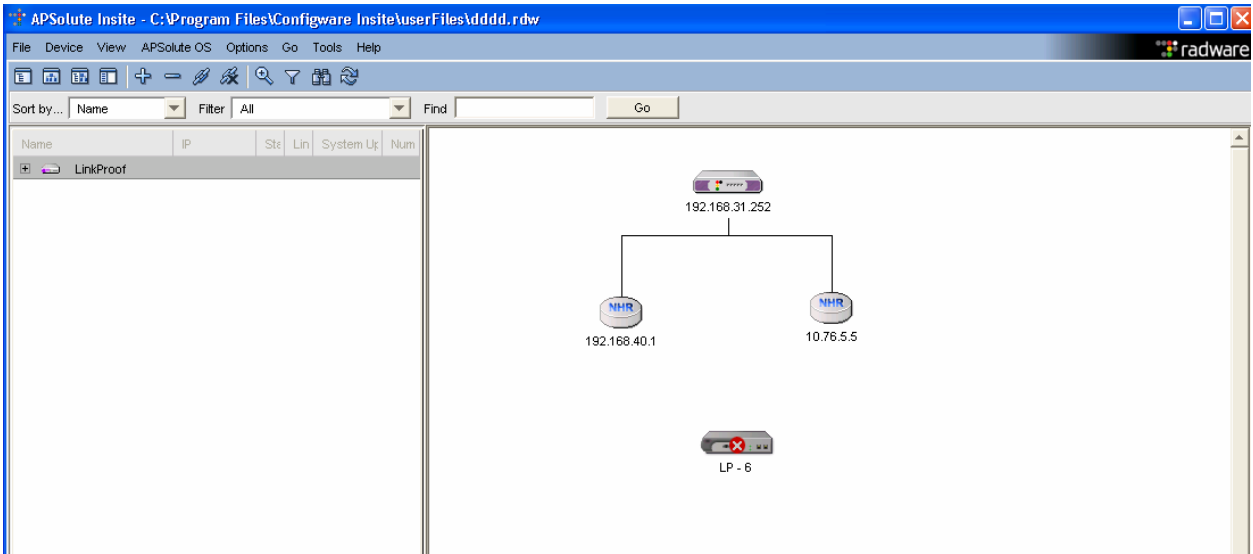
Step	Description
13.	<p>The Next Hop Router box appears, add the following information:</p> <ul style="list-style-type: none"> • Next Hop Router Name to 192.168.40.1 • IP Address to 192.168.40.1 <p>Select Add then OK to continue.</p>  <p>Repeat Step 12 to create the 2nd Next hop Router.</p> 

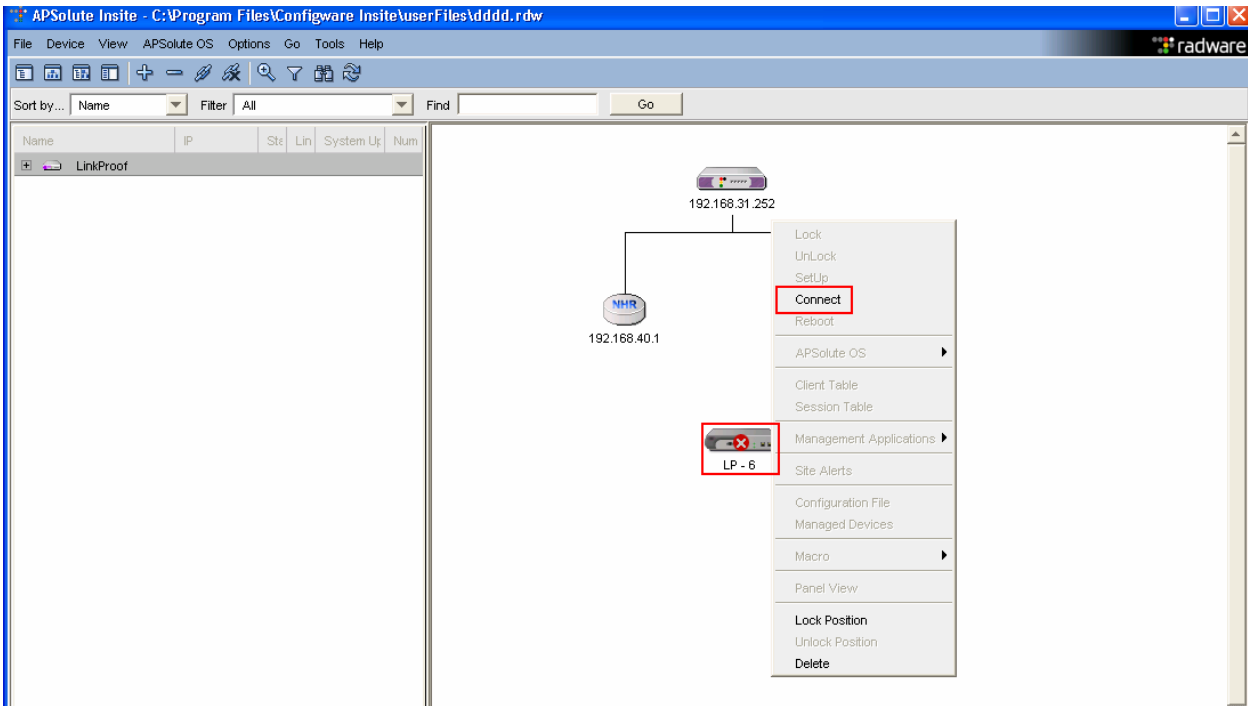

Step	Description
14.	<p data-bbox="277 237 927 268">Link the LinkProof and the two Next Hop Routers.</p> <p data-bbox="277 310 1529 415">Holding down the left mouse button, sweep it over the LinkProof and the two Next Hop Routers, then ctrl-L. After the Next Hop Router boxes appear (2), starting with interface 10.76.5.5, click on the pull down tab for Mode and select Backup, Press Apply to continue.</p> 

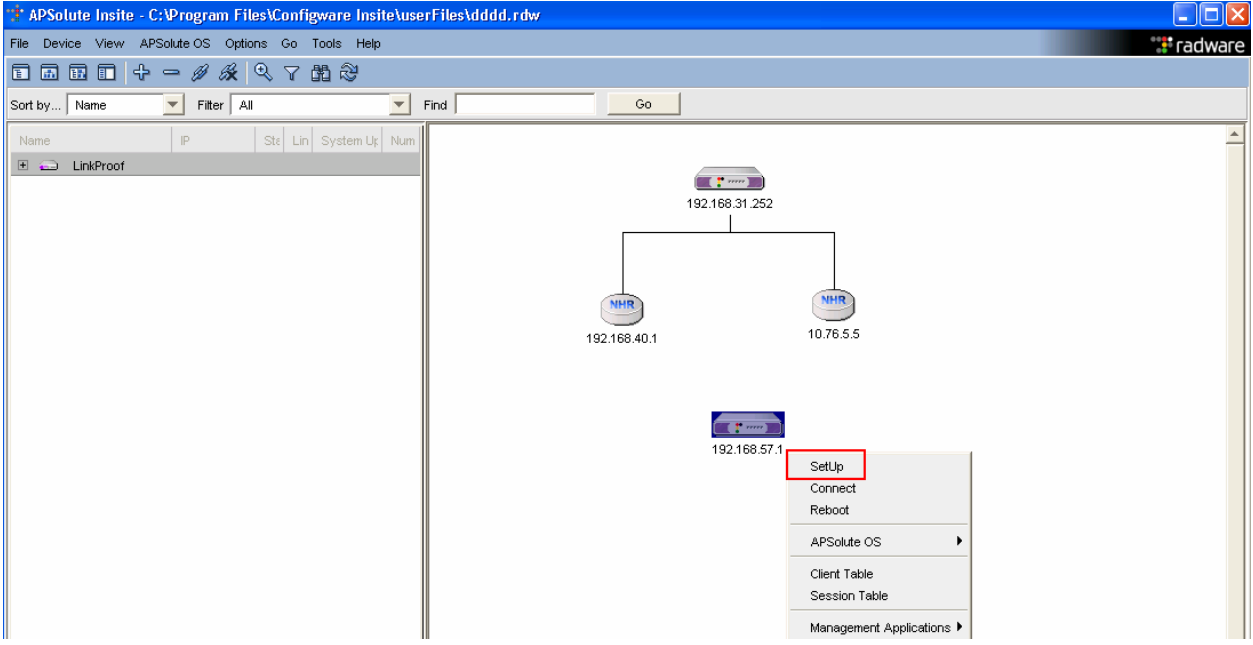
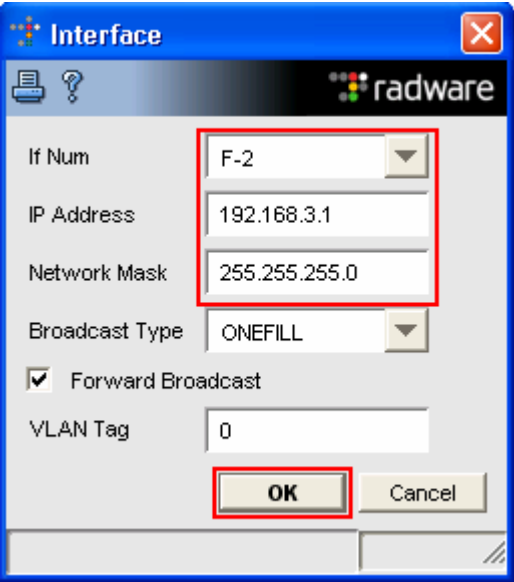
Step	Description
15.	<p data-bbox="277 237 1406 306">Another Next Hop Router box appears for interface 10.75.5.5. Select Full Path Health Monitor</p> <div data-bbox="511 340 1291 1218">  <p>The screenshot shows the 'Next Hop Router' configuration window for interface 10.76.5.5. The 'Full Path Health Monitor' button is highlighted with a red box. The window includes tabs for Settings, Advanced Settings, NHR Information, and Cost Information. The 'Status' is set to 'Enabled'. The 'IP Address' is 10.76.5.5. The 'Mode' is 'Backup'. The 'Recovery Time' is 0. The 'Inbound Kbps Limit' is 0. The 'Outbound Kbps Limit' is 0. The 'ToS' is 255. The 'Connection Limit' is 0. The 'Billing Mode' is 'Total'. The 'NHR Proximity Checks' checkbox is checked. The 'Bandwidth Limit Exception' checkbox is unchecked. The 'Site Map Alerts' button is also visible.</p> </div> <p data-bbox="277 1255 1508 1325">Add the IP address of the routers. Refer to Figure1 for the IP addresses. Enter the IP address to the Check Address box, click Add, Repeat fort the second router address Click OK to continue.</p> <div data-bbox="448 1362 1352 1852">  <p>The first screenshot shows the 'Full Path Health Monitor' window with the 'Check Address' field containing '10.76.5.5' and the 'Add' button highlighted with a red box. The second screenshot shows the same window with the 'Check Address' field containing '192.168.3.1' and the 'Add' button highlighted with a red box. The 'Operational Status' is 'Active'.</p> </div>

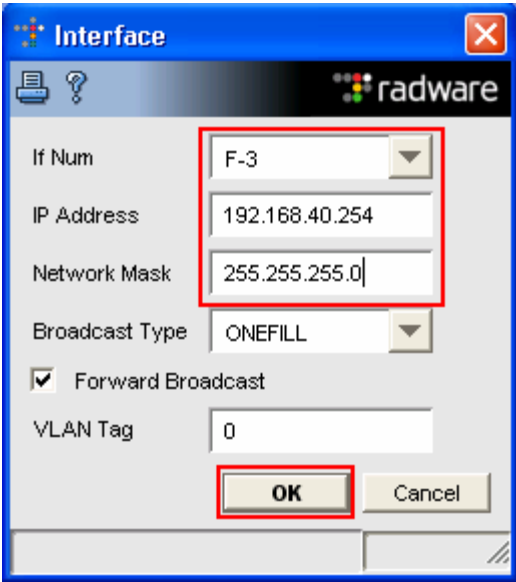
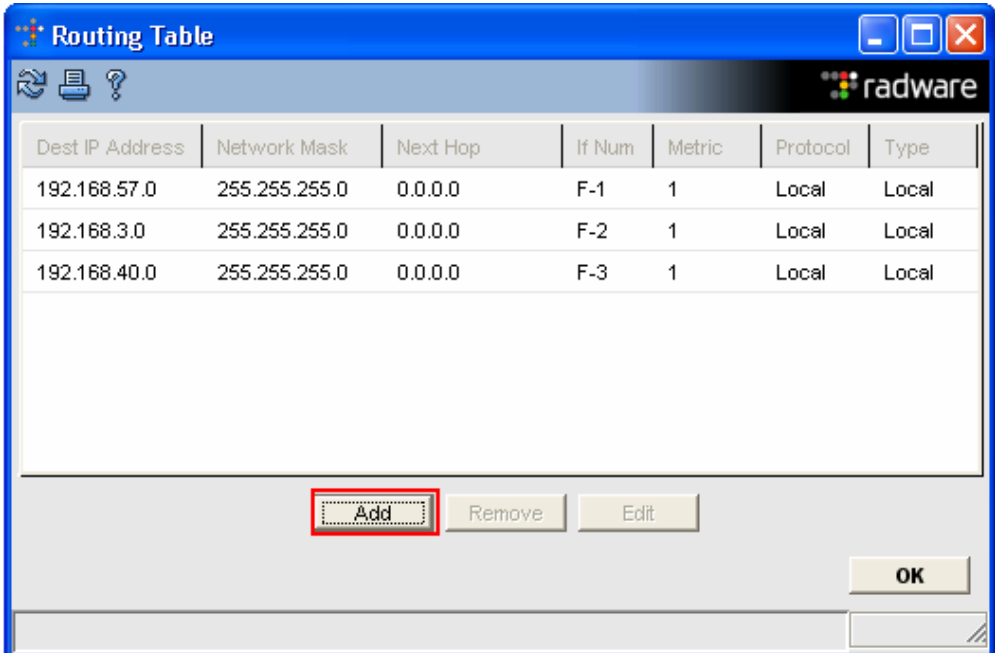
Step	Description
16.	<p>Interface 192.162.40.1, Press Apply to continue.</p> 

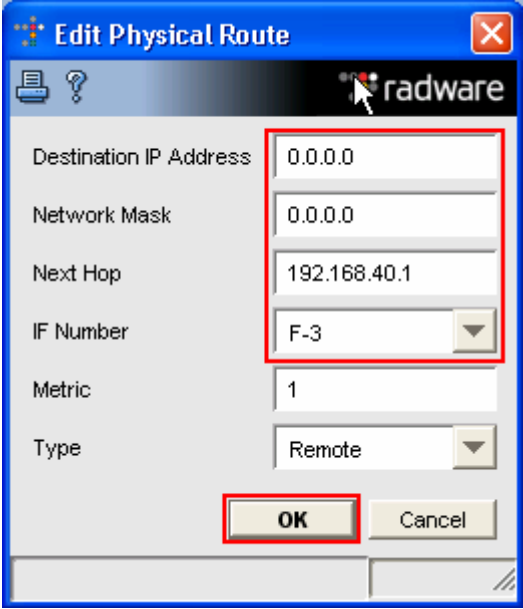
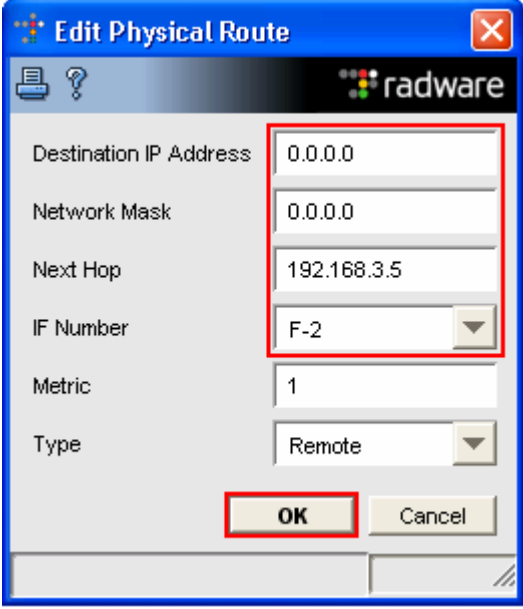
Step	Description
17.	<p data-bbox="277 237 1455 306">Another Next Hop Router box appears for interface 192.162.40.1. Select Full Path Health Monitor.</p> <div data-bbox="513 342 1289 1215" data-label="Image"> </div> <p data-bbox="277 1255 1495 1325">Add the IP address of the router. Refer to Figure1 for the IP addresses. Enter the IP address to the Check Address box, click Add, click OK to continue.</p> <div data-bbox="682 1360 1120 1850" data-label="Image"> </div>

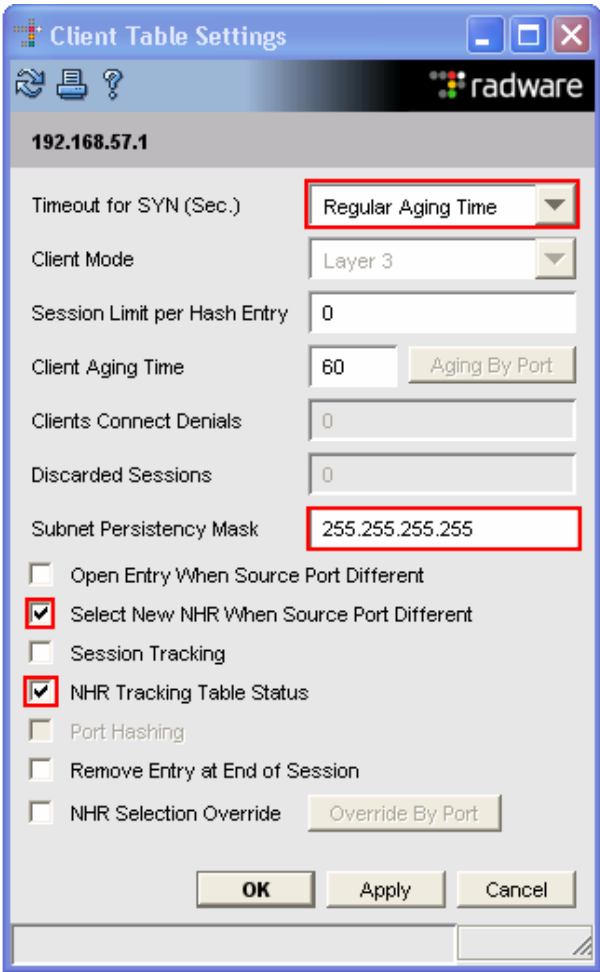
Step	Description
18.	<p>Add LinkProof device for the Branch site, Select Device → Add Radware Device → LinkProof.</p>  <p>The LinkProof icon for the Branch site should appear.</p> 

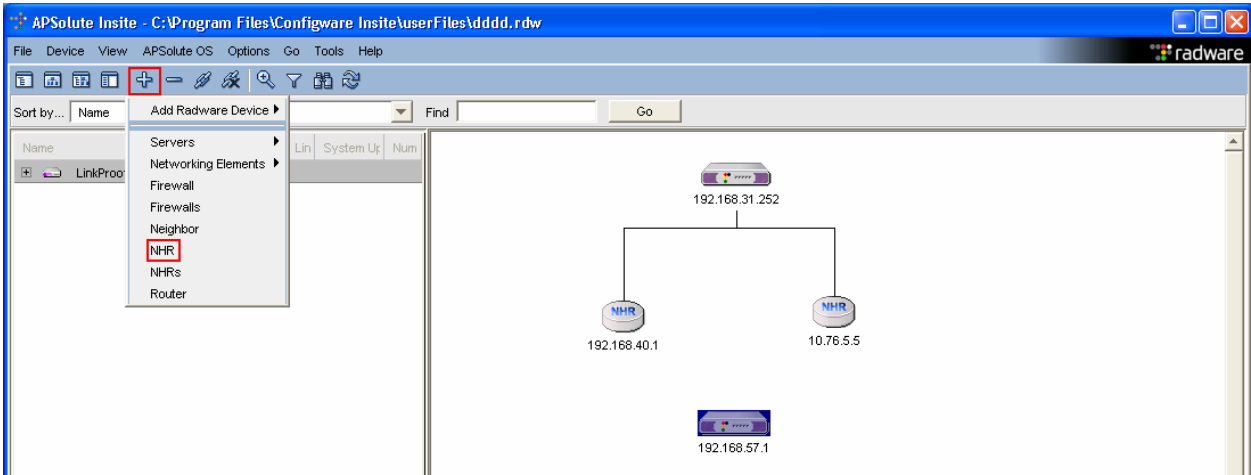
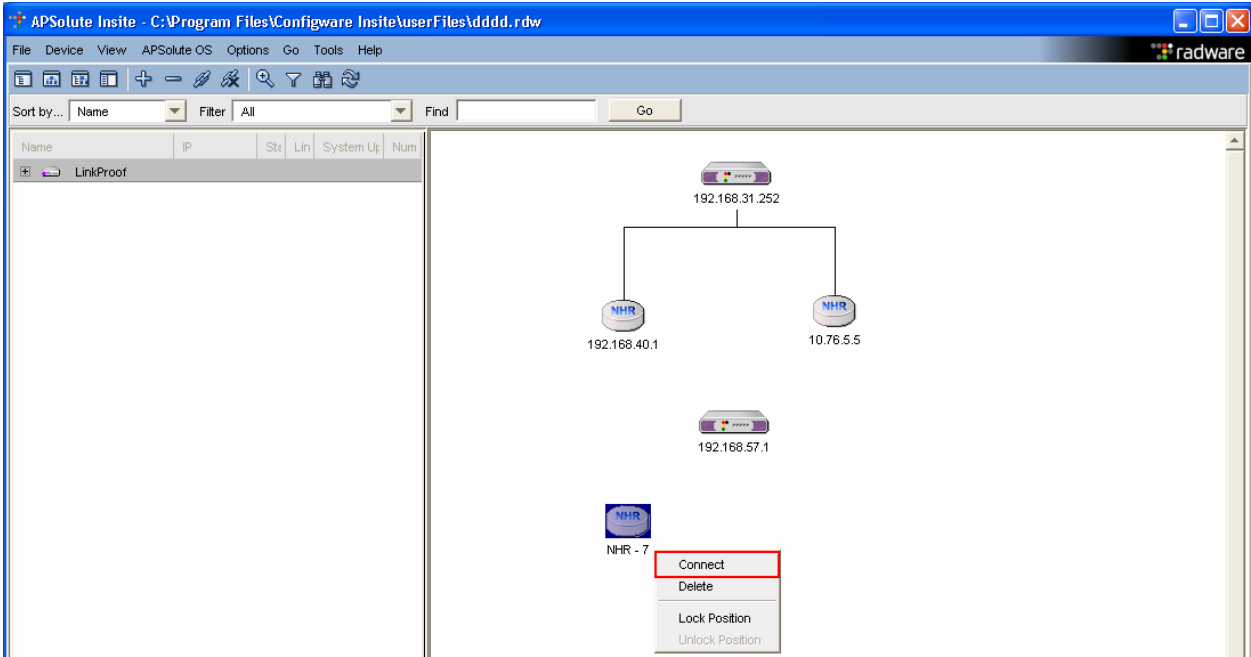
Step	Description
19.	<p>Right click on the Branch LinkProof icon, Select Connect to the device.</p>  <p>The Connect LP Device box appears, enter the IP address of the Branch LinkProof device, select OK to continue.</p> 

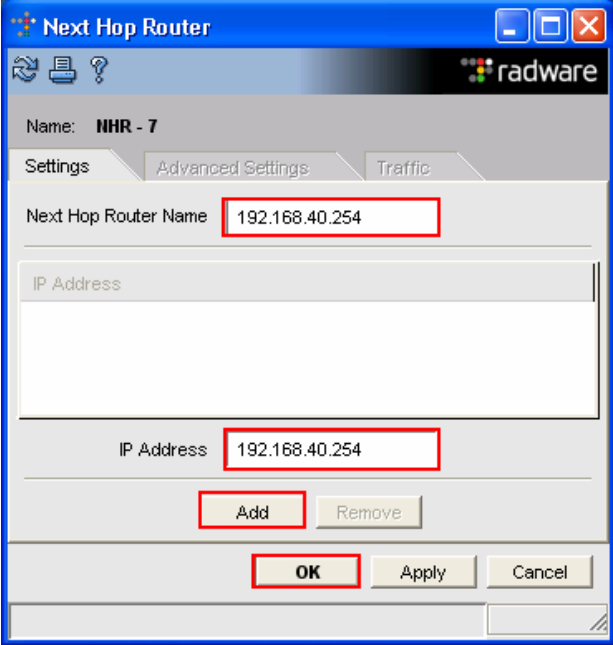
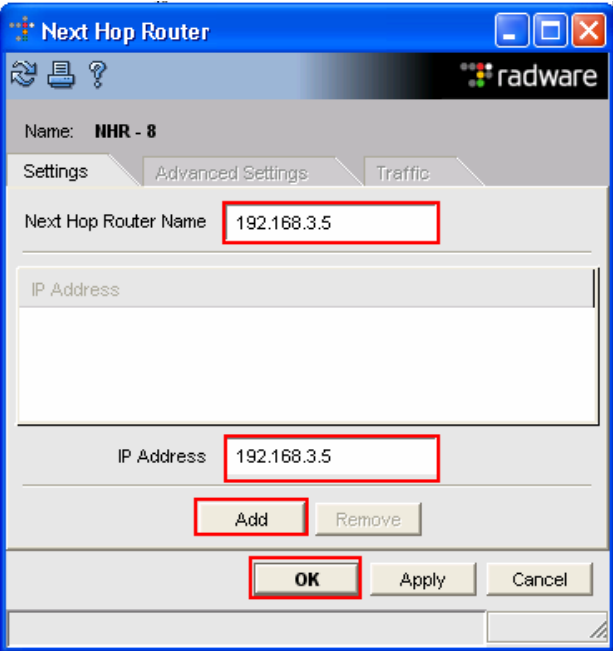
Step	Description
20.	<p>Create interfaces F-2 and F-3, Right mouse click on the Branch LinkProof device. Select Setup.</p> 
21.	<p>The Interface box appears, click on the pull down tab for If Num, and select F-2. Enter the IP Address and Network Mask, select OK to continue.</p> 

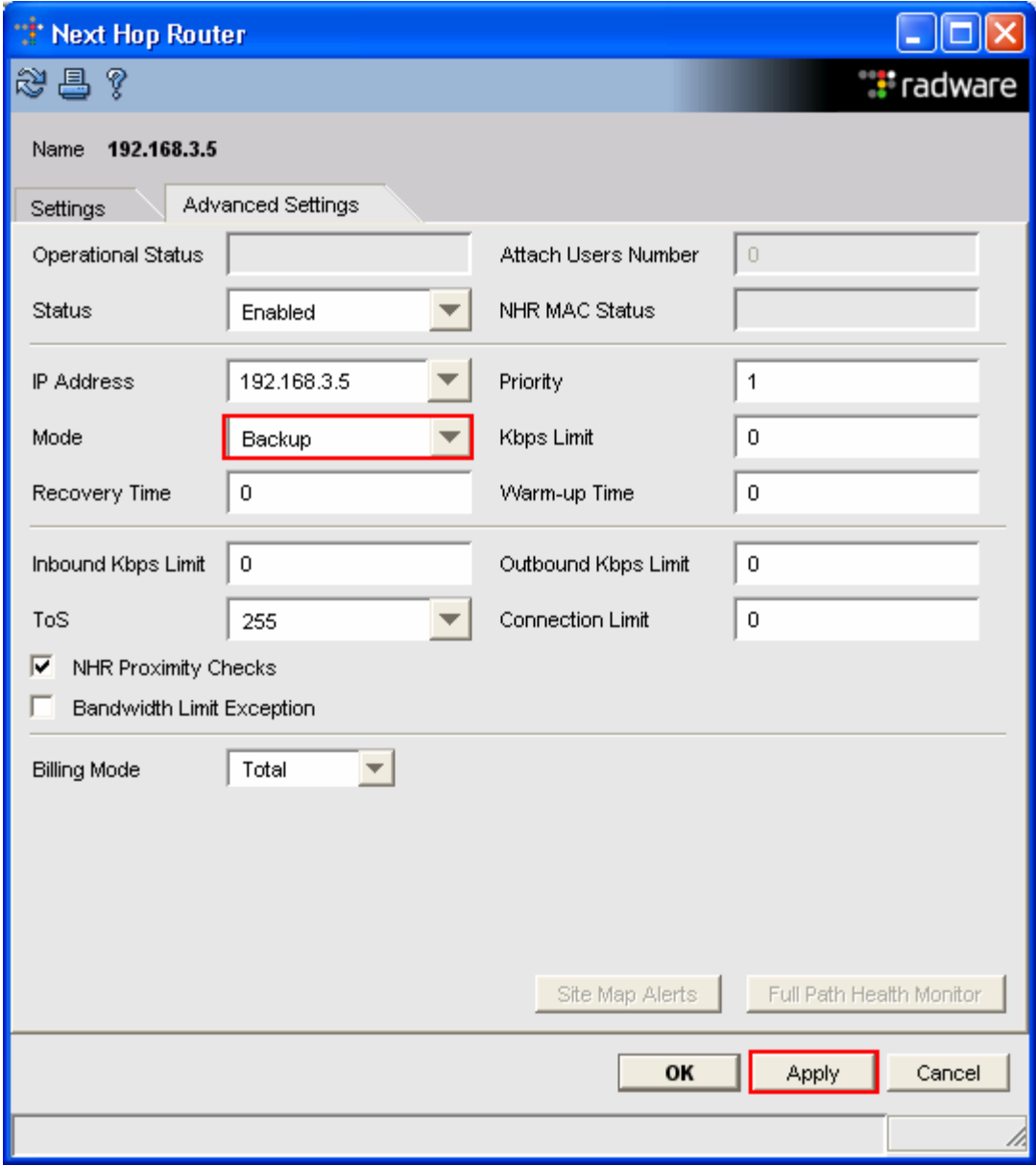
Step	Description
22.	<p>Repeat Step 5 to create Interface F-3. Select OK to continue.</p> <div></div>
23.	<p>Add routes to the routing table.</p> <p>Right mouse click on the LinkProof device. Select Setup, click the pull down tab for Networking, select Routing Table. The Routing Table box appears, add the following routes, select Add.</p> <div></div>

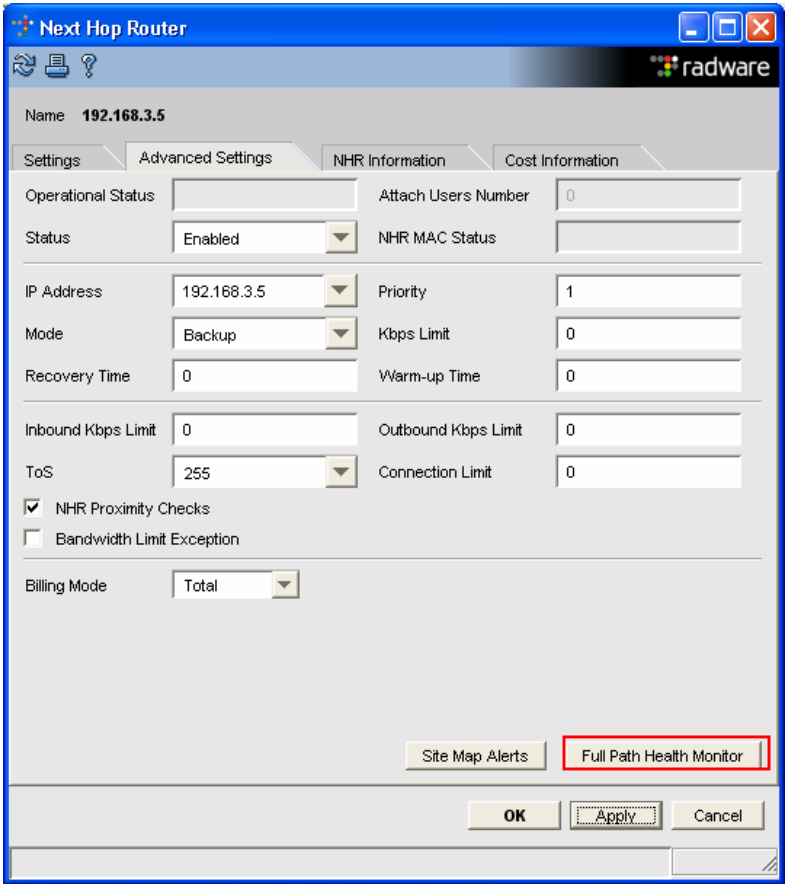
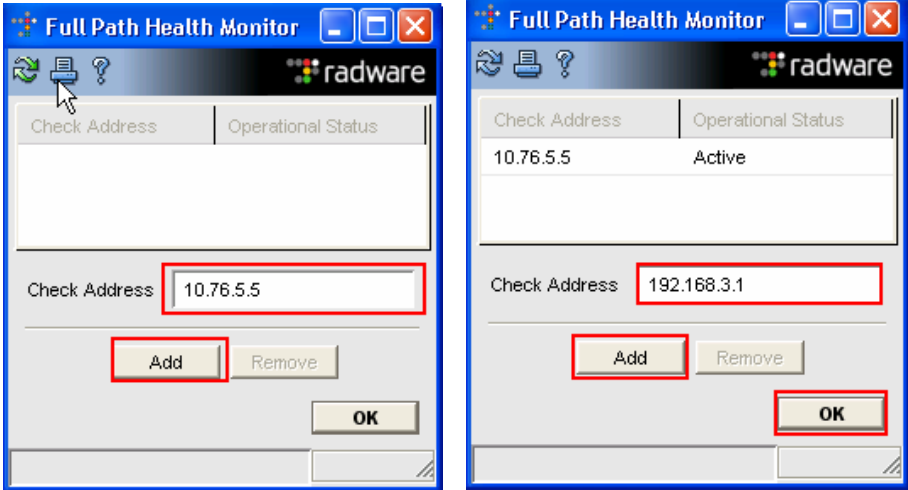
Step	Description
24.	<p>Add the following Default Routes, Add Destination IP Address, Mask Next Hop, IF Number.</p> <div data-bbox="370 310 889 915">  </div> <div data-bbox="911 310 1430 915">  </div>

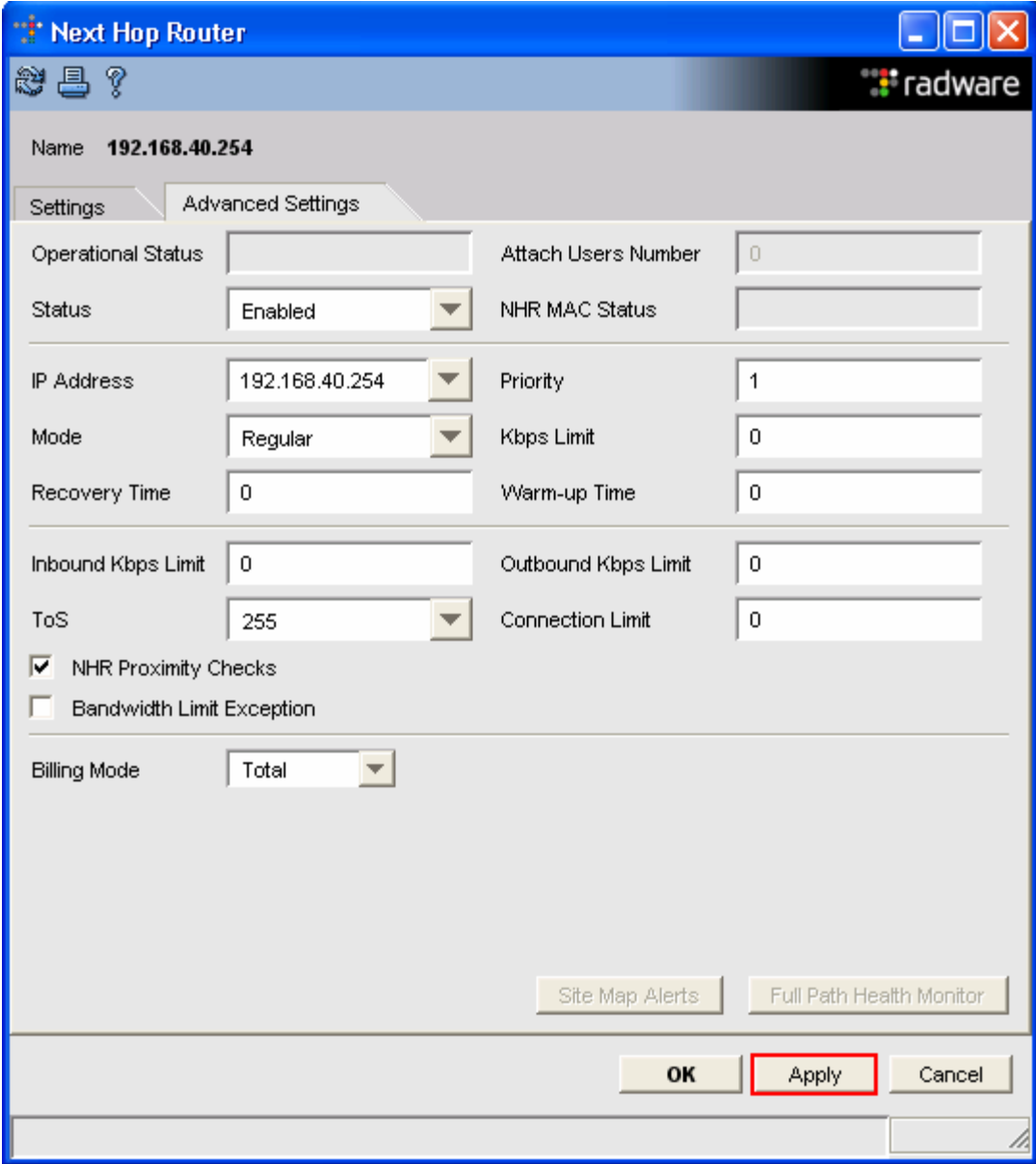
Step	Description
25.	<p>Configure the Client Table selections on the Branch LinkProof device.</p> <p>Right mouse click on the Branch LinkProof device, select Setup, after the Setup box appears, select the Global tab, select Client Table Settings, then Edit Settings.</p> <p>Set the Following:</p> <ul style="list-style-type: none"> • Timeout for SYN (SEC) to Regular Aging Time • Subnet Persistency Mask to 255.255.255.255 • Check Select New NHR When Source Port Different • Check NHR Tracking Table Status 

Step	Description
26.	<p>Create the following Next Hop Router (NHR) entries on the Branch LinkProof device. Click + → NHR</p>  <p>A NHR icon appears, right mouse click on the NHR icon and select Connect.</p> 

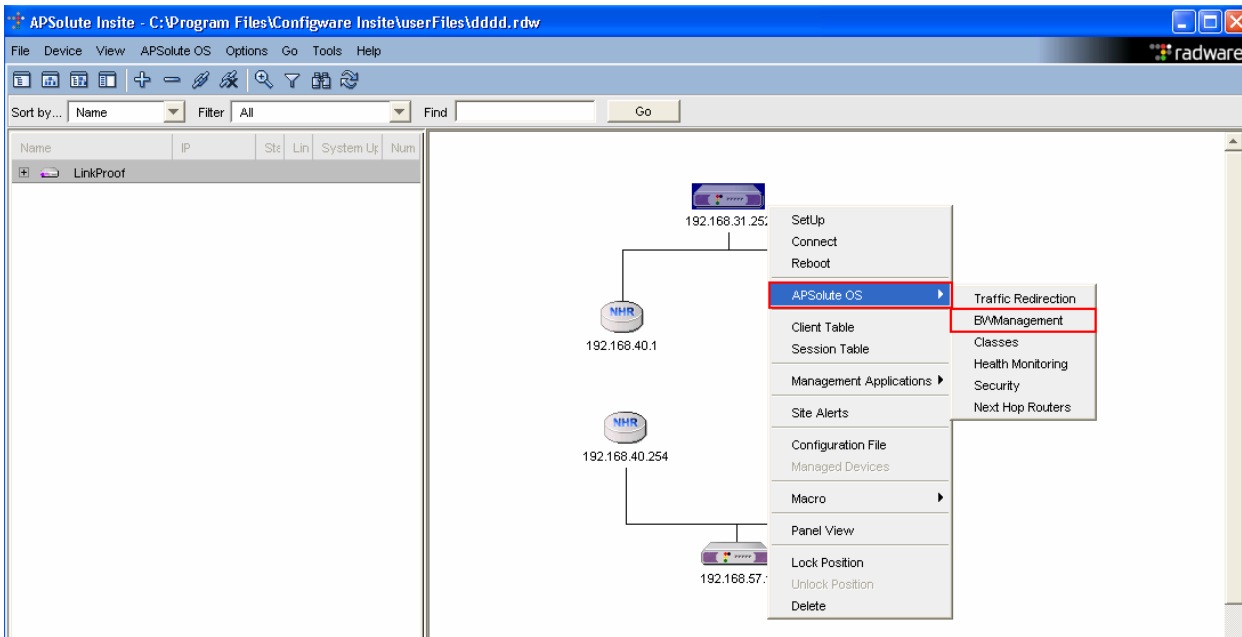
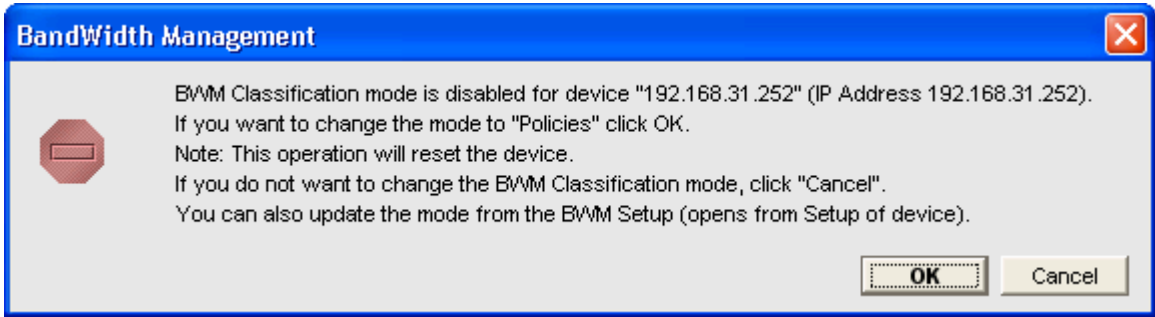
Step	Description
27.	<p>The Next Hop Router box appears, add the following information:</p> <ul style="list-style-type: none"> • Next Hop Router Name to 192.168.40.254 • IP Address to 192.168.40.254 <p>Select Add then OK to continue.</p>  <p>Repeat Step 27 to create the 2nd Next hop Router.</p> 

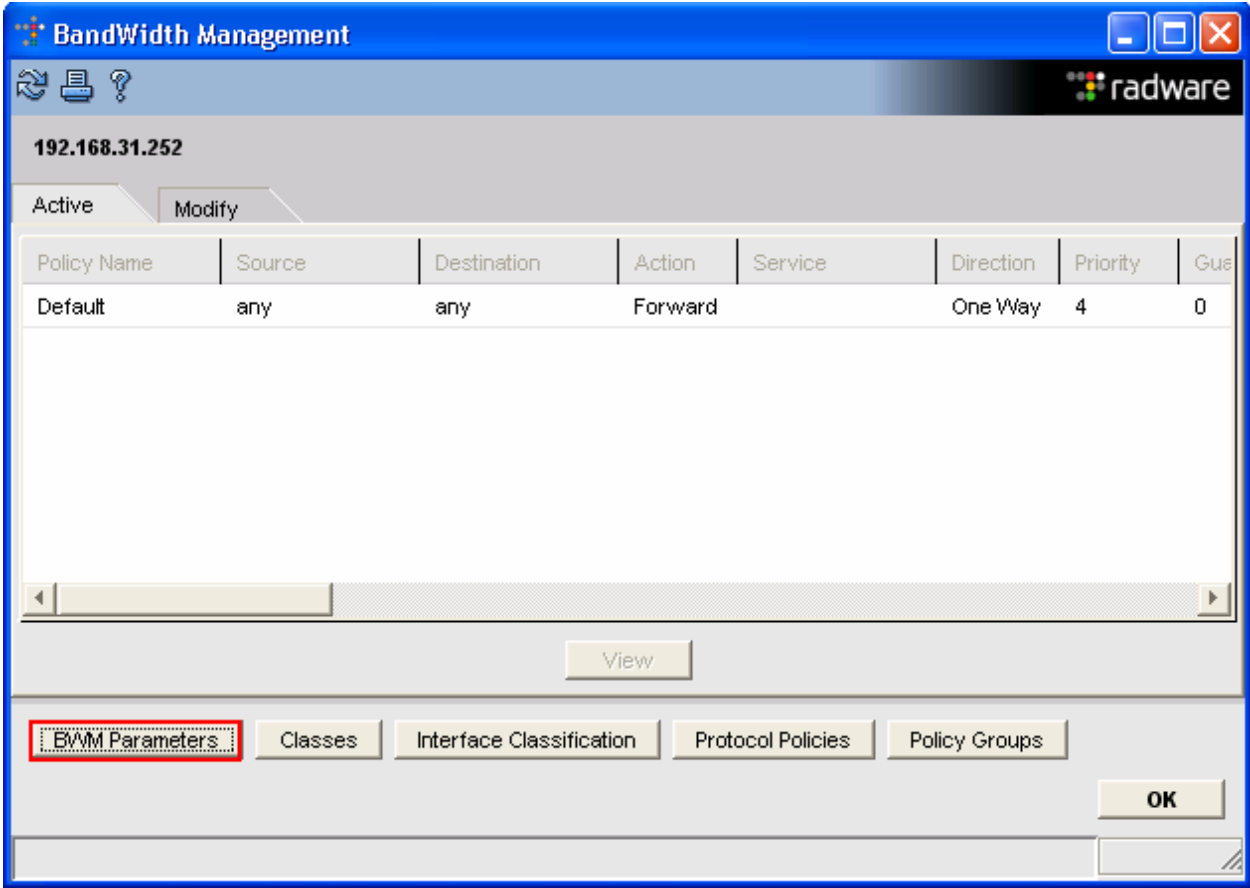
Step	Description
28.	<p data-bbox="277 243 1143 275">Link the Branch LinkProof and the two Branch Next Hop Routers.</p> <p data-bbox="277 310 1484 453">Holding down the left mouse button, sweep it over the Branch LinkProof and the two Branch Next Hop Routers, then ctrl-L. After the Next Hop Router boxes appear, starting with interface 192.168.3.5, click on the pull down tab for Mode and select Backup, Press Apply to continue.</p> 

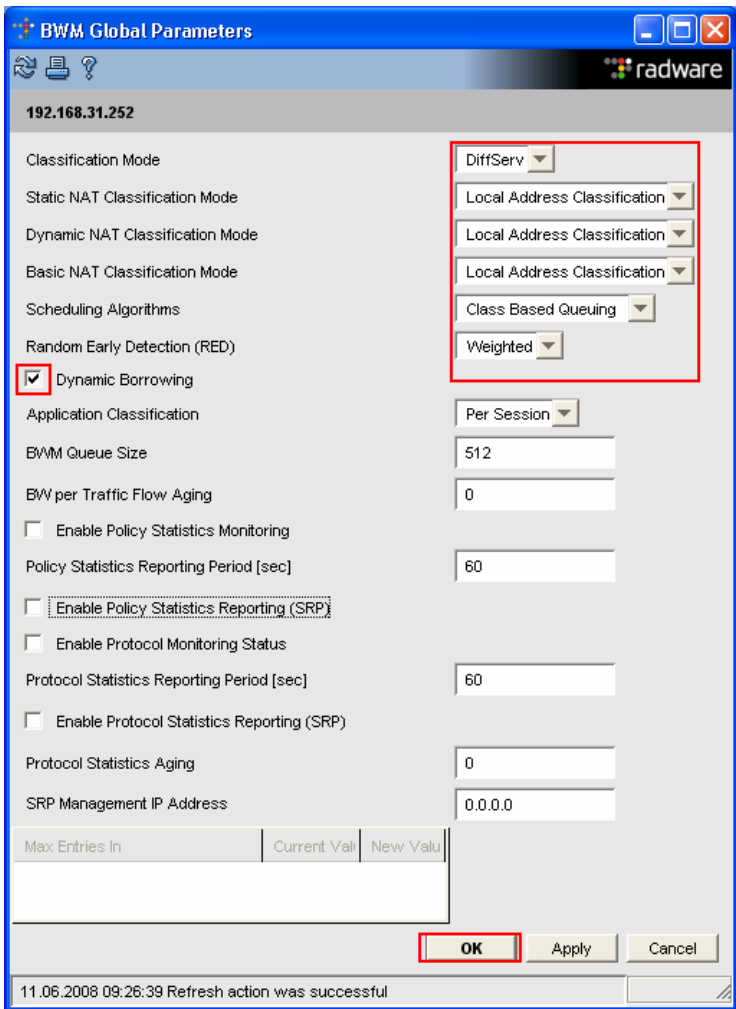
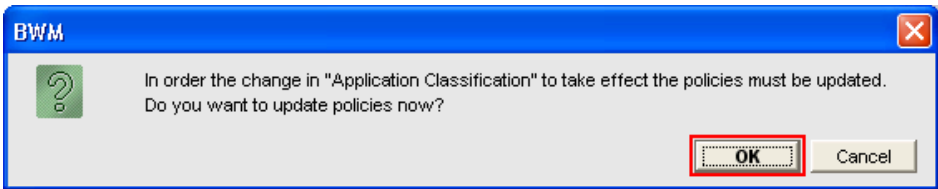
Step	Description
29.	<p>Another Next Hop Router box appears for interface 192.168.3.5. Select Full Path Health Monitor</p>  <p>Add the IP address of the routers. Refer to Figure1 for the IP addresses. Enter the IP address to the Check Address box, click add, Repeat for the second router address Click OK to continue.</p> 

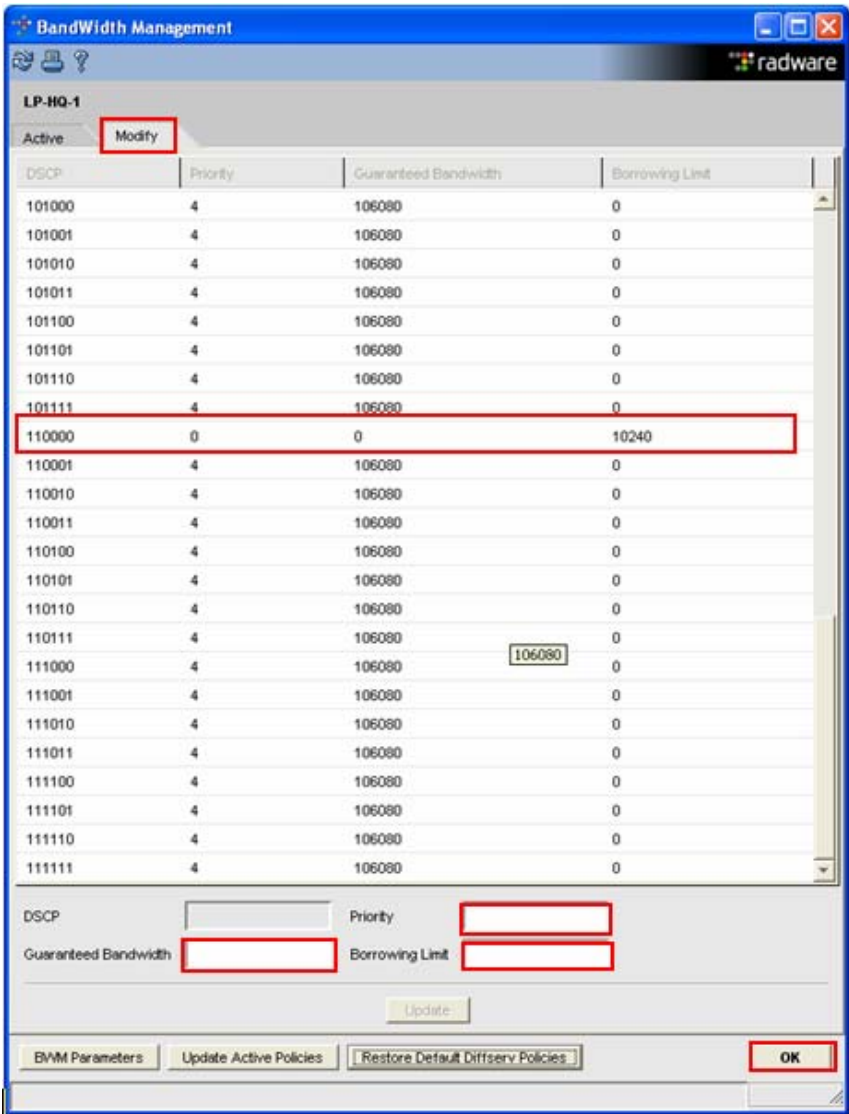
Step	Description
30.	<p data-bbox="277 237 932 275">Interface 192.162.40.254, Press Apply to continue.</p> 

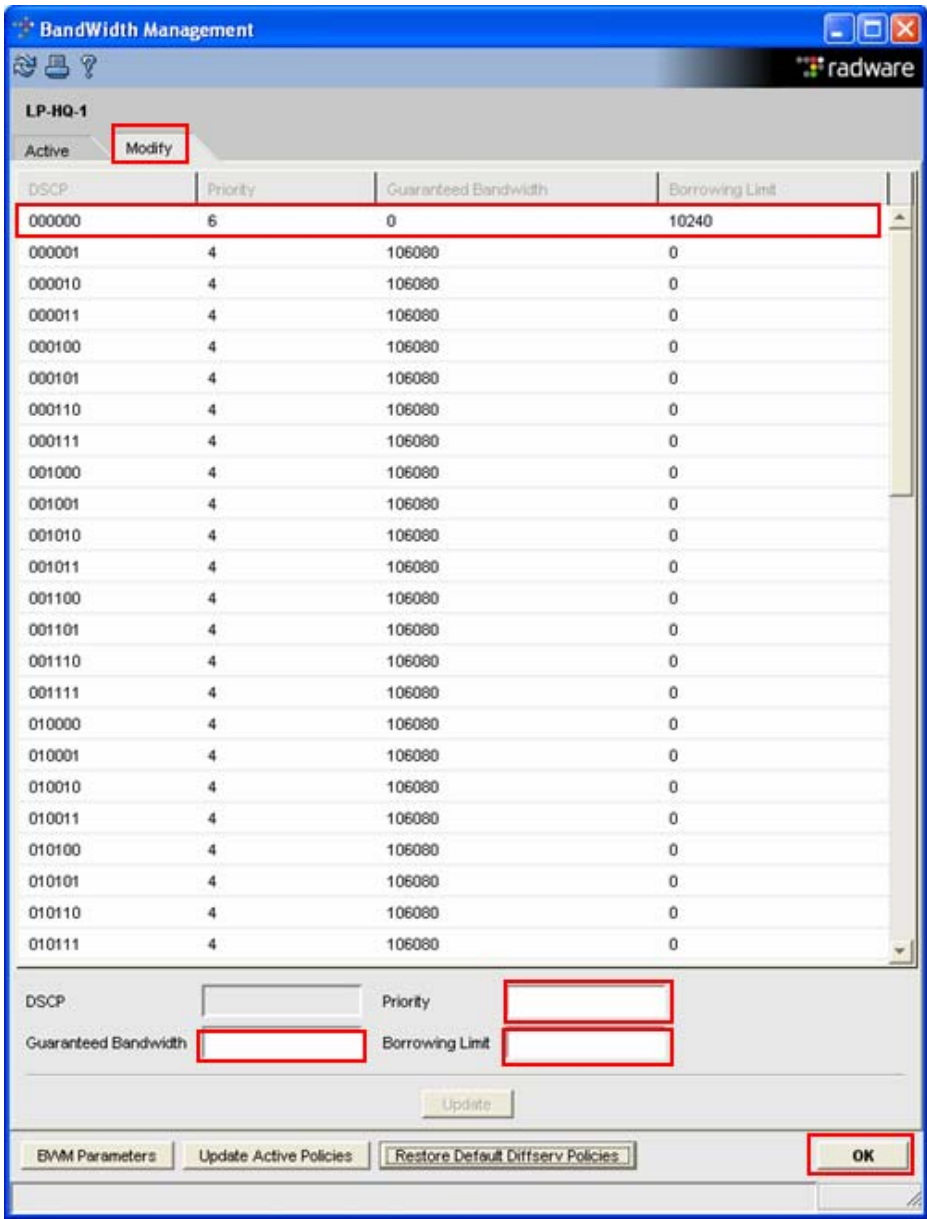
Step	Description
31.	<p>Another Next Hop Router box appears for interface 192.162.40.1. Select Full Path Health Monitor.</p> <div data-bbox="511 338 1291 1213" data-label="Image"> </div> <p>Add the IP address of the router. Refer to Figure1 for the IP addresses. Enter the IP address to the Check Address box, click Add, click OK to continue.</p> <div data-bbox="678 1360 1120 1852" data-label="Image"> </div>

Step	Description
32.	<p>Configure Bandwidth. Right click on the Main site LinkProof device, select APolute → BWManagement</p>  <p>The BWM dialog box appears, Select OK to enable BWM. Reboot LinkProof as requested.</p> 

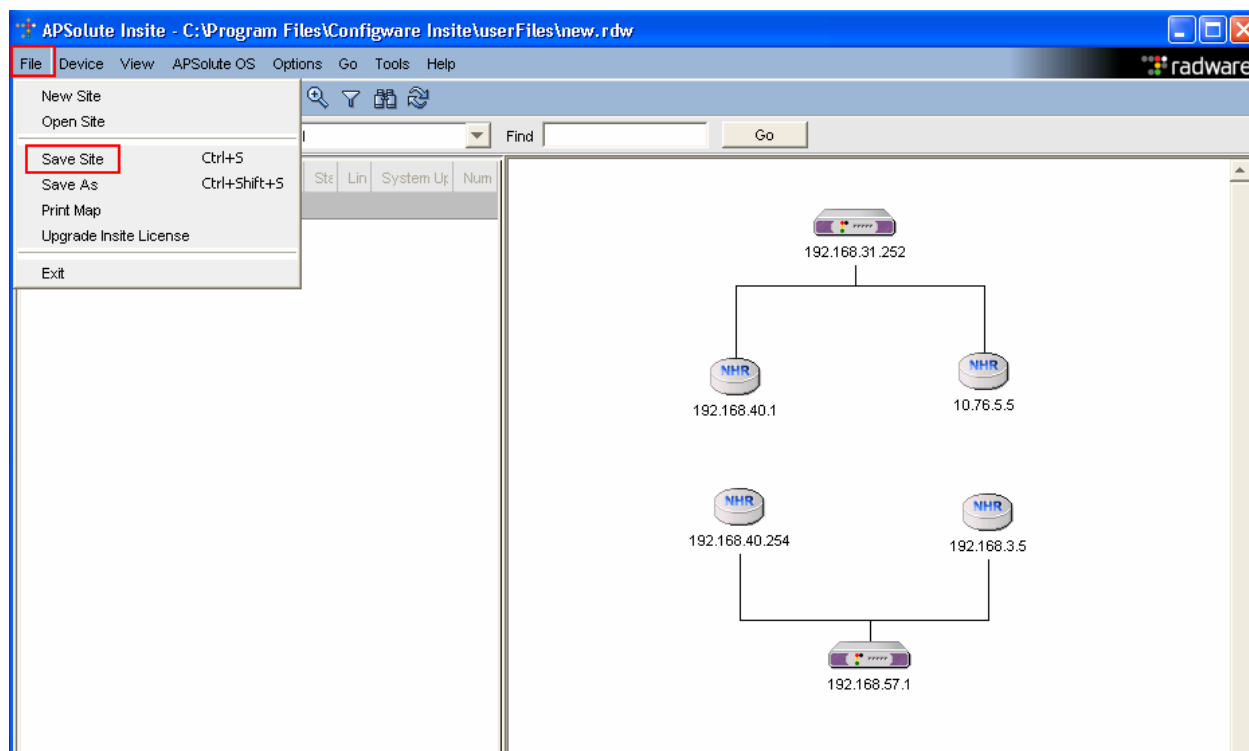
Step	Description
33.	<p>Once the LinkProof finishes rebooting the BandWidth Management box appears. Select BWM Parameters to continue.</p> 

Step	Description
34.	<p>Set BWM Global Parameters, click the pull down tab for the following:</p> <ul style="list-style-type: none"> • Classification Mode to DiffServ. • Static NAT Classification Mode to Local address Classification • Dynamic NAT Classification Mode to Local address Classification • Basic NAT Classification Mode to Local address Classification • Scheduling Algorithms to Class Based Queuing <p>Check Dynamic Borrowing, Press OK to continue.</p>  <p>The BWM dialogue box appears, select OK to continue.</p> 
TMA; Reviewed: SPOC 7/24/2008	<p>Solution & Interoperability Test Lab Application Notes ©2008 Avaya Inc. All Rights Reserved.</p>
	<p>39 of 46 Radware-ADO</p>

Step	Description
35.	<p>Configure QoS for voice traffic.</p> <p>Voice is using a DiffServ Code Point of 48, (110000), and is give a priority of 0. Click Modify → DSCP 110000. Set the following:</p> <ul style="list-style-type: none"> • Priority to 0 • Guaranteed Bandwidth to 0 • Borrowing Limit to 10240 <p>Note: The default priority value is 4 with a guaranteed bandwidth of 106080 kbps. Values run from 0 thru 7, with 7 being the lowest priority.</p> <p>Select OK to continue.</p> 

Step	Description
36.	<p>For devices that are not set to use DiffServ, set the priority to 6 and bandwidth limit them to 10240 kbps.</p> <p>Best effort data is using a DiffServ Code Point of 0, (000000), and is give a priority of 6. Click Modify → DSCP 000000. Set the following:</p> <ul style="list-style-type: none"> • Priority to 6 • Guaranteed Bandwidth to 0 • Borrowing Limit to 10240 <p>Select OK to continue.</p> 

Step	Description
37.	Repeat steps 33 thru 37 on the Branch LinkProof.
38.	Save the Site configuration. Click File → Save Site



6. Interoperability Compliance Testing

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

Feature functionality testing focused on the QoS and VLAN implementation in the Avaya/Radware configuration. Specifically, compliance testing verified Redundancy and that when the Radware Switch interfaces are over subscribed with low priority data traffic, the higher priority VoIP media and signaling traffic still got through and achieved good voice quality. Prioritization of voice traffic was achieved by implementing Layer 3 DiffServ-based QoS and Layer 2 priority (801.p). Voice and data traffic were segmented in the enterprise network using VLANs.

QoS was verified by making voice calls while a traffic generator generated low priority data traffic to simulate a converged network. It was verified that the voice traffic was given priority over the lower priority data traffic and continued to operate successfully.

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

6.1. General Test Approach

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

- Failover of the primary Radware LinkProof Multi-WAN 3020 Switch to the backup
- LAN connectivity between the Avaya and Radware products
- Registration of Avaya H.323 IP Telephones with Avaya Communication Manager
- Registration of Avaya SIP IP Telephones with Avaya SIP Enablement Services
- Verification of the DHCP relay configuration
- VoIP calls over Layer 2 and Layer 3 connections
- Inter-office calls using G.711 mu-law & G.729 codecs, conferencing, and sending low priority data traffic over the LAN.
- Verifying that QoS directed the voice signaling and voice media to the higher priority egress queue based on the packets' DSCP value.
- Verifying that Avaya Modular Messaging voicemail and MWI work properly.

The load tests were performed by over subscribing the lines with low priority data and verifying that the prioritization of VoIP traffic and voice was achieved when calls are routed over all of the LAN interfaces.

6.2. Test Results

All feature functionality, serviceability, and load test cases passed. The Radware LinkProof Multi-WAN 3020 Switch implementation did prioritization of VoIP traffic, failed over to the

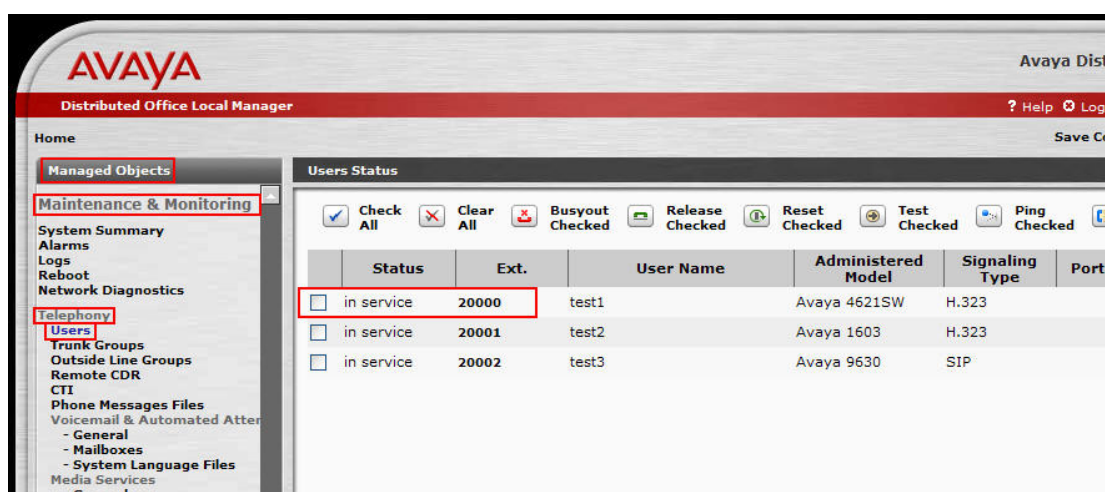
backup Radware LinkProof Multi-WAN 3020 Switch and yielded good voice quality with no calls being lost. The stability of the Avaya/Radware solution was successfully verified through load and serviceability testing.

7. Verification Steps

This section provides the steps for verifying end-to-end network connectivity and QoS, verification steps include:

Verify the DHCP relay is functioning by confirming that the all Avaya IP telephones from all locations receive their IP addresses from the DHCP server

- Place calls between sites for each Avaya IP Telephone.
- Check that the Avaya IP telephones have successfully registered with Avaya Distributed Office. Log into Avaya Distributed Office using the appropriate credentials, select **Managed Objects** → **Maintenance & Monitoring** → **Telephony** → **Users**, look for **in service**.



8. Conclusion

These Application Notes describe the configuration steps required for integrating Radware LinkProof Multi-WAN 3020 Switches with an Avaya telephony infrastructure. For the configuration described in these Application Notes, the Radware LinkProof Multi-WAN 3020 Switch were responsible for enforcing, QoS using Layer 3 Differentiated Services and Layer 2 (802.1p) as well as link aggregation, rapid spanning tree and load balancing and Redundancy. The Avaya Distributed Office delivered the voice traffic to the routers for transmission over the LAN together with data traffic. Prioritization of VoIP traffic and good voice quality was successfully achieved in the Avaya/ProCurve configuration described herein.

9. Additional References

The documents referenced below were used for additional support and configuration information.

The following Avaya product documentation can be found at <http://support.avaya.com>.

- [1] *Avaya Distributed Office i20 Installation Quick Start*, May 2007 Issue 1, Document Number 03-602289
- [2] *Command Reference Release*, Document Number: 882-10034 Rev 1
- [3] *Configuration Guide*, Document Number: 882-20034 Rev 2
- [4] *Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Installation and Maintenance Guide Release 1*, Doc # 16-601438
- [5] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Installation and Maintenance Guide Release 1.0*

The Radware product documentation can be found at: <http://www.radware.com/>.

- [6] *Register at the Radware web site to obtain configuration guides.*

©2008 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 DevConnect Program at devconnect@avaya.com.