



Avaya Solution & Interoperability Test Lab

Application Notes for Radware LinkProof Multi-WAN Switch connected to an Avaya Communication Manager and Avaya SIP Enablement Services 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 Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging in an Avaya IP Telephony Environment. Radware LinkProof Multi-WAN Switch was compliance-tested with Avaya Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging. Emphasis was placed on bandwidth management and traffic shaping.

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 Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging 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 Communication Manager 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 QoS, throughput, Multi-WAN connections, load balancing, Direct IP Media connectivity and the G.711 and G.729 codecs.

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 Communication Manager running on an Avaya S8300 Server with an Avaya G700 Media Gateway, one SIP Enablement Services Server, one Avaya Modular Messaging, one Avaya 2400 Series Digital Telephone, one Avaya 9630 IP Telephone running Avaya one-X Deskphone Edition, one Avaya 9620 IP Telephone running Avaya one-X Deskphone SIP 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 running Avaya one-X Deskphone Edition and one Avaya 9620 IP Telephone running Avaya one-X Deskphone SIP and one PC on Datavlan2. The LinkProof 3020 switches were configured to support load balancing, Layer2/Layer3 QoS and Redundancy.

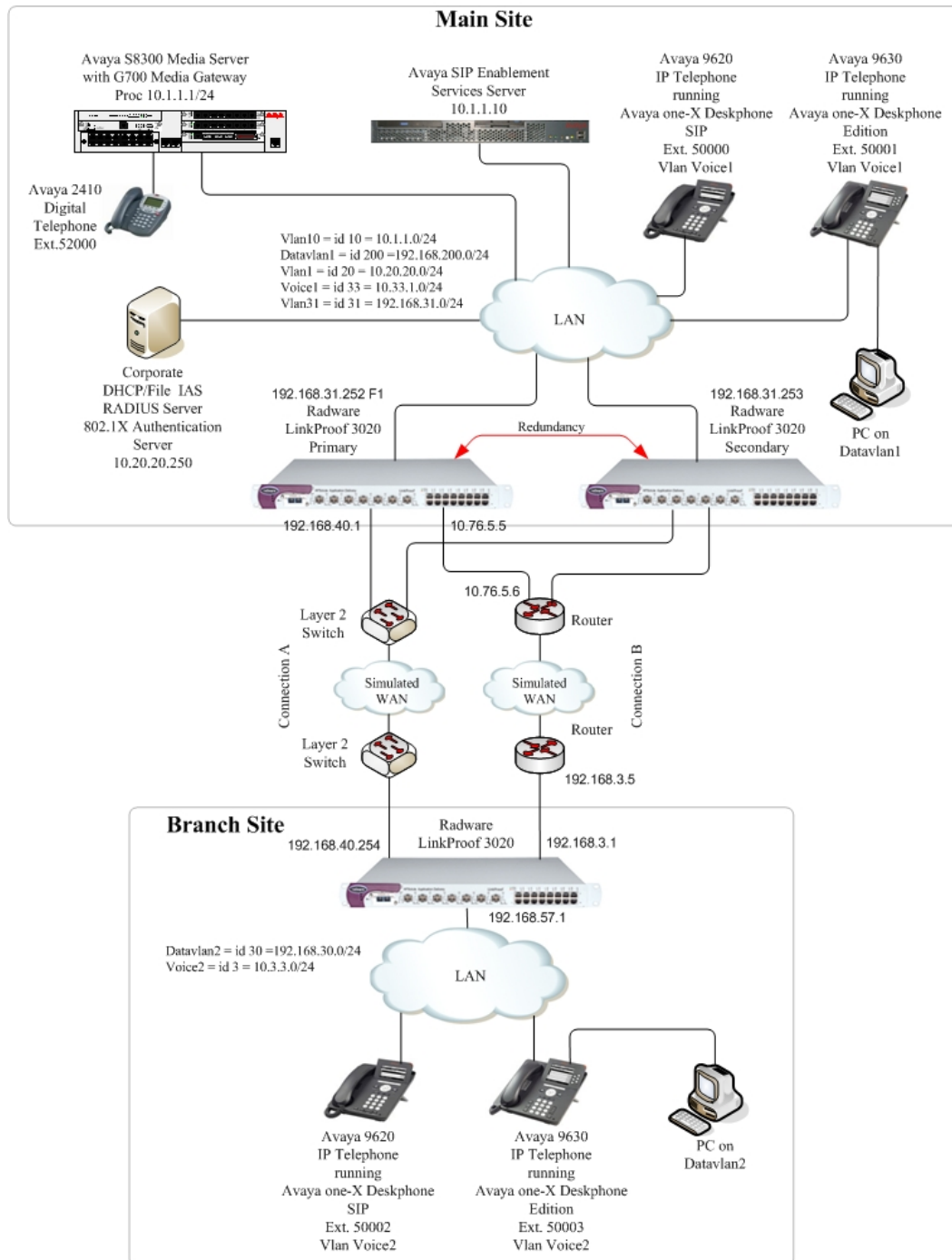


Figure 1: Network Configuration

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Server	Avaya Communication Manager 4x.00.1.731.2
Avaya G700 Media Gateway with MM712 DCP Media Module 8	26.31.0 FW 008
Avaya Modular Messaging Server	3.1
Avaya SIP Enabled Services (SES) Server	SES-4.0.0.0-033.6
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone SIP 1.5 (SIP)
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone Edition 1.2 (H.323)
Avaya 2410 Digital Telephone	4.0
Radware LinkProof Multi-WAN 3020 Switch	FW-K.12.22

4. Configure Avaya Communication Manager

This section shows the steps used to configure Avaya Communication Manager. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, refer to [1].

4.1. Configure QoS on Avaya Communication Manager

IP networks were originally designed to carry data on a best-effort delivery basis, which meant that all traffic had equal priority and an equal chance of being delivered in a timely manner. As a result, all traffic had an equal chance of being dropped when congestion occurred. QoS is utilized and should be implemented throughout the entire network.

In order to achieve prioritization of VoIP traffic, the VoIP traffic must be classified. The Avaya S8300 Server, Avaya G700 Media Gateway, Avaya SIP Enablement Services and Avaya IP Telephones support both Layer 2 802.1p/Q priority and Layer 3 DiffServ.

All network components are in network region 1 for this sample configuration. The DiffServ and 802.1p/Q values configured here will be downloaded to the Avaya H.323 IP Telephones via Avaya Communication Manager. Avaya SIP IP Telephones will get QoS setting by downloading the 46xxsetting file from the HTTP server. For more information on QoS settings please refer to [1].

Use the **change ip-network-region 1** command to change the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS settings configured in Avaya Communication Manager.

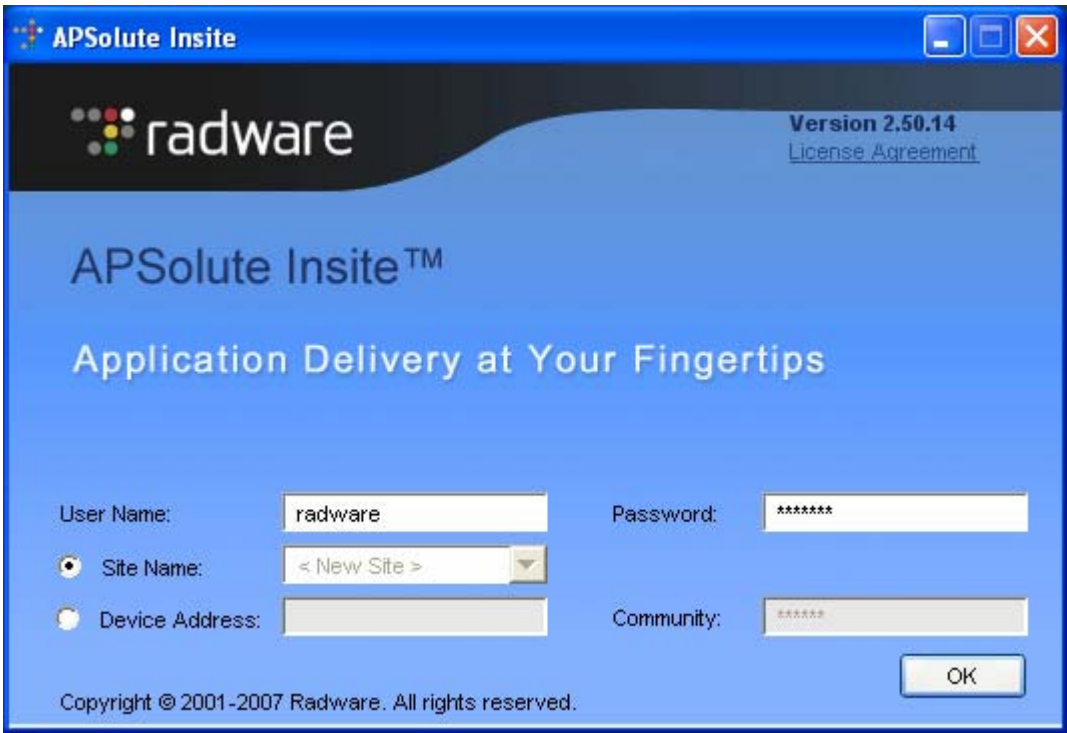
```
change ip-network-region 1                               Page 1 of 19
                                     IP NETWORK REGION
  Region: 1
  Location:      Authoritative Domain: devcon.com
    Name:
MEDIA PARAMETERS                                     Intra-region IP-IP Direct Audio: yes
  Codec Set: 1                                       Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048                                IP Audio Hairpinning? y
  UDP Port Max: 3027
DIFFSERV/TOS PARAMETERS                               RTCP Reporting Enabled? y
  Call Control PHB Value: 46                         RTCP MONITOR SERVER PARAMETERS
  Audio PHB Value: 46                               Use Default Server Parameters? y
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5                         AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
```

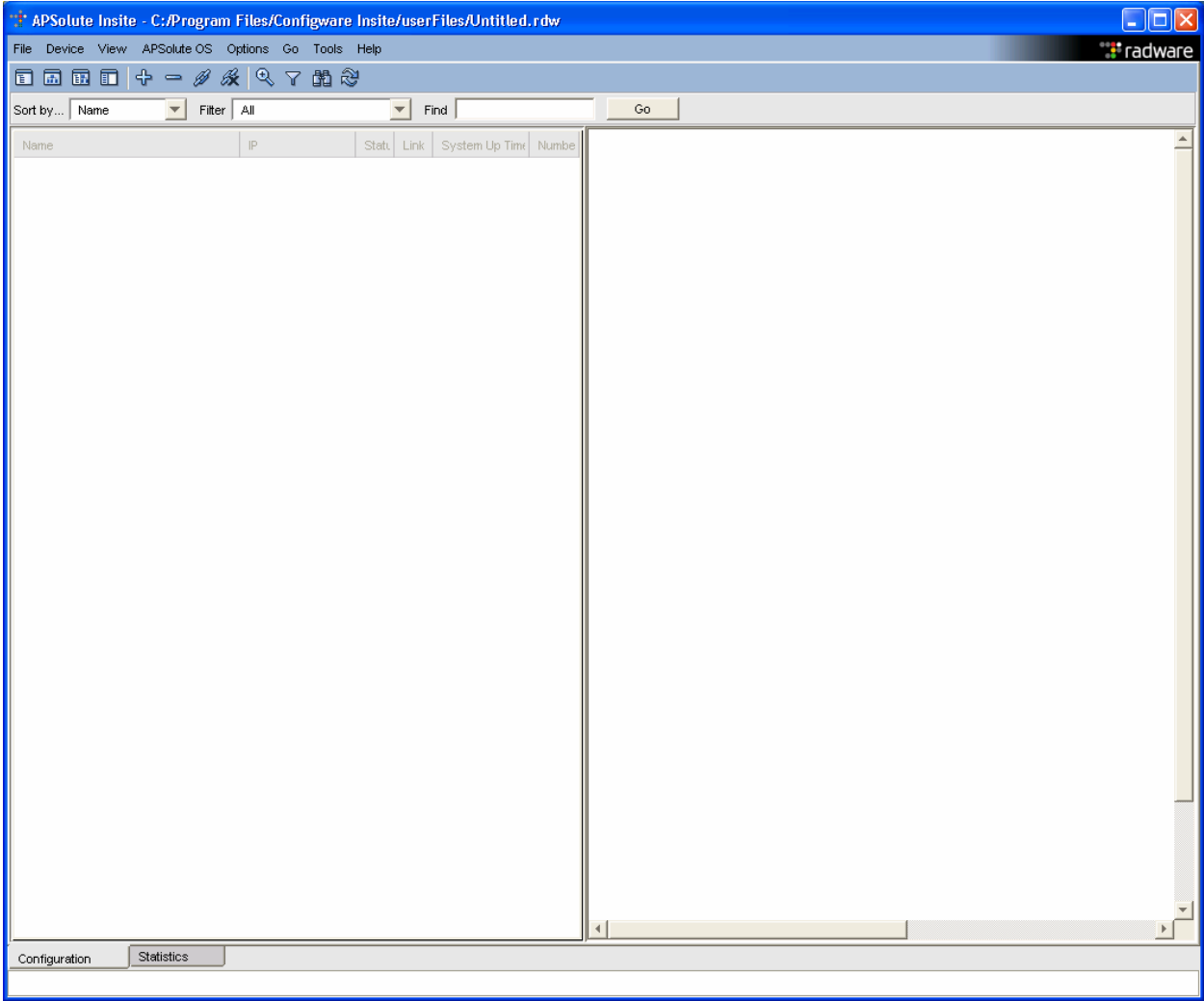
The Differentiated Services Code Point (DSCP) value of 46 will be used for both **PHB Values**. DSCP 46 represents the Traffic Class of Premium and the Traffic Type Voice. Set the **Call Control PHB Value to 46** and the **Audio PHB Value to 46**. The **Call Control 802.1p** and **Audio 802.1p** priority are set to **6**.

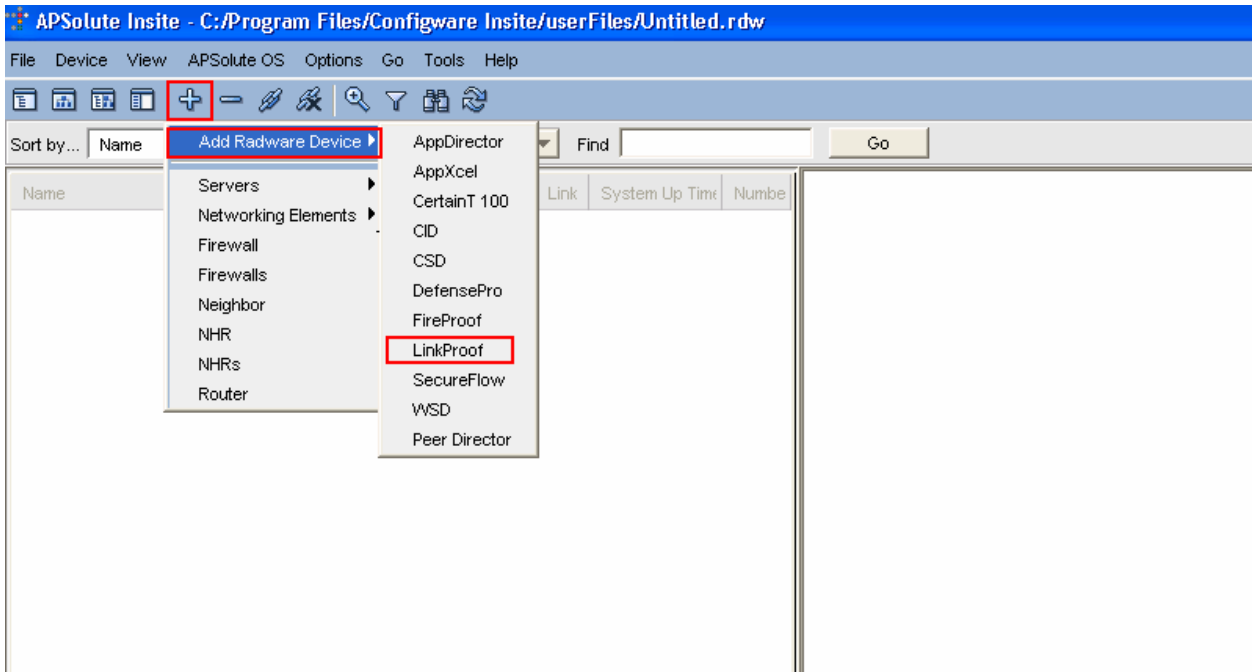
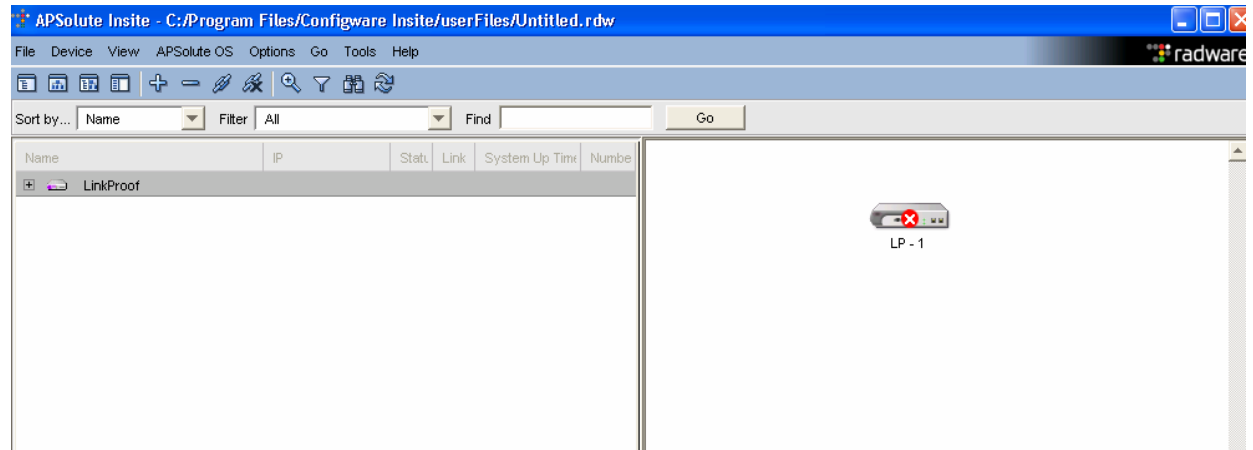
5. Configuration Radware LinkProof Multi-WAN 3020 Switch

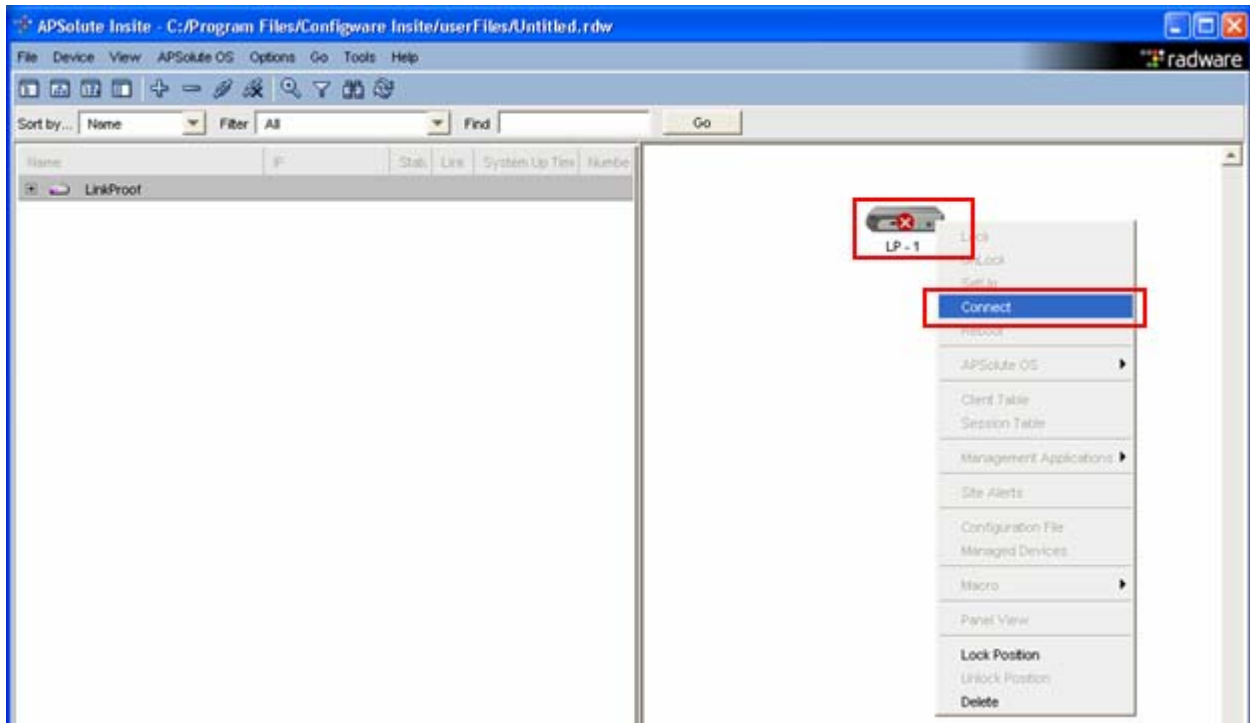
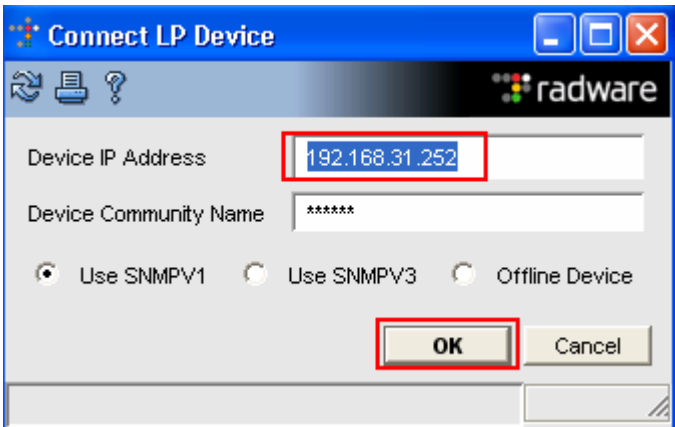
This section addresses how to configure the Radware LinkProof Multi-WAN 3020 Switches. Please refer to [5] for basic setup and installation of the LinkProof Switch and the APSolute Insite software. This section will pertain to the configuration tested. Redundancy testing of a second LinkProof Switch, **Figure1**, was compliance tested but the configuration of the second LinkProof switch will not be covered in the document.

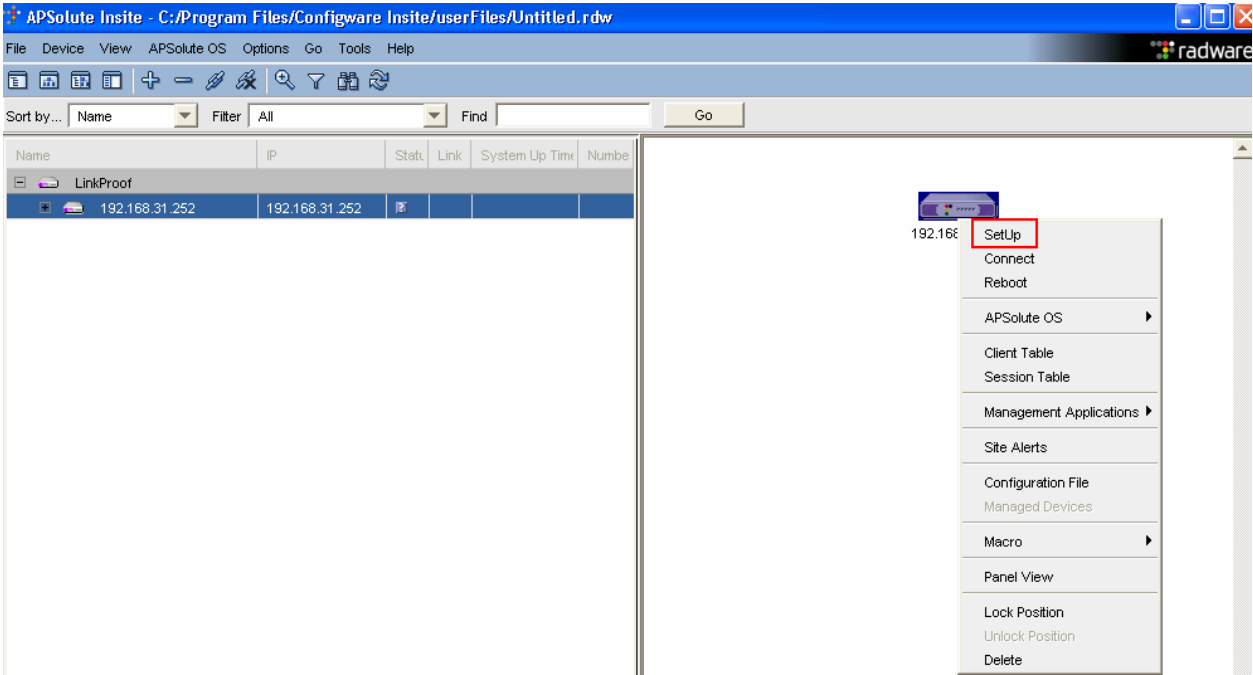
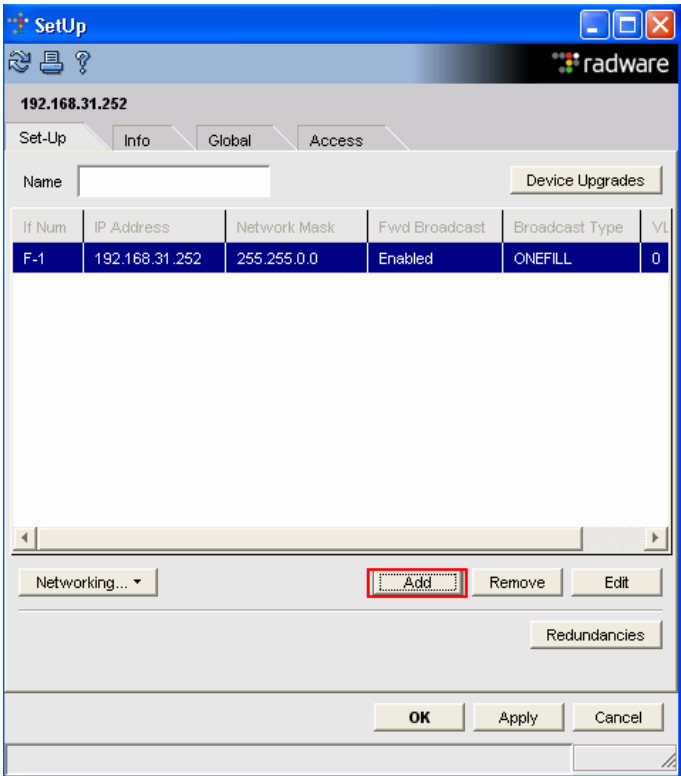
For this configuration different priorities were used for each route based on the speeds of the links. The following configuration uses the switched interface as the primary route with the routed interface as a standby which will only be used if the “main” route fails. If the routed interface on the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

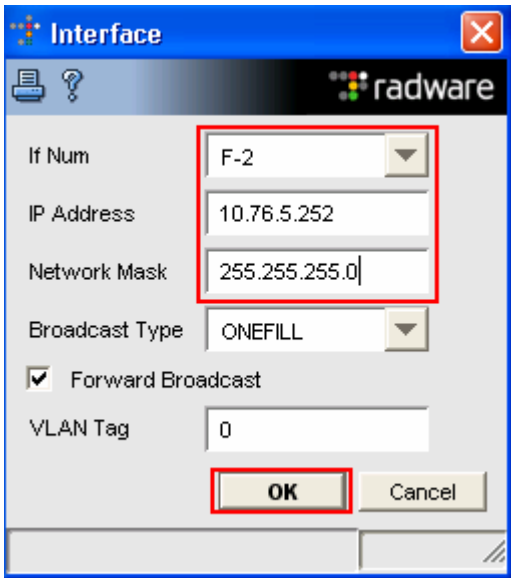
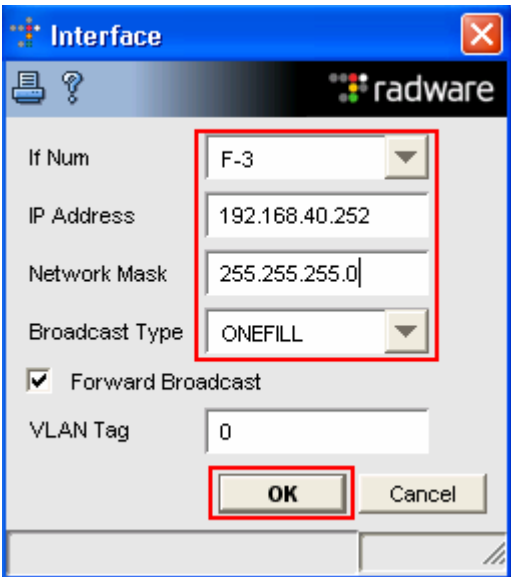
Step	Description
1.	<p>Log into the APSolute using the default credentials which can be obtained from the Radware LinkProof documentation.</p> 

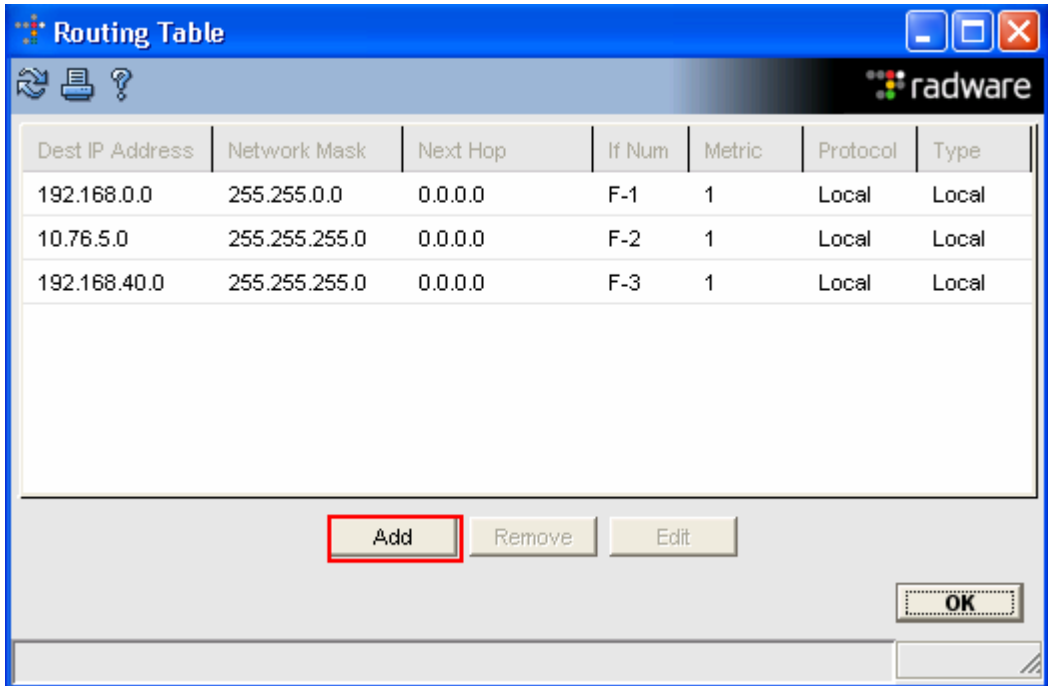
Step	Description
2.	<p>The following APSolute Insite main screen is displayed.</p> 

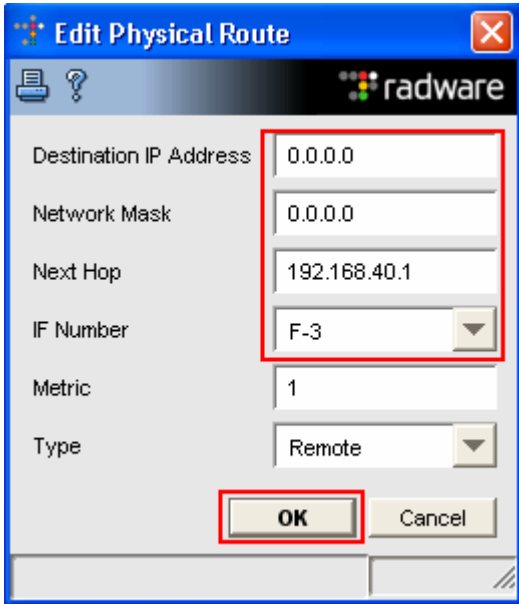
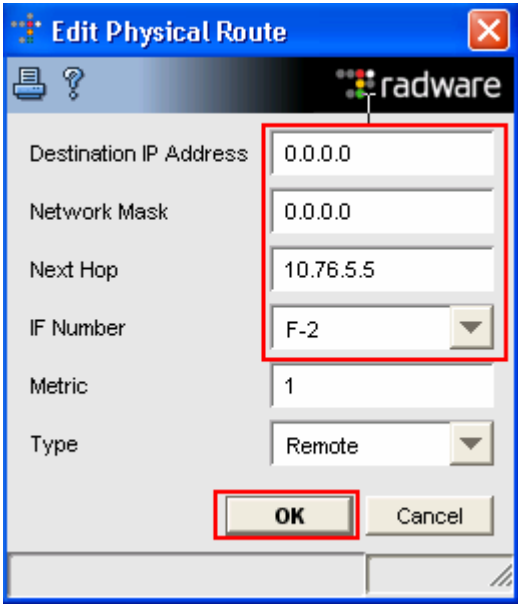
Step	Description
3.	<p>Add LinkProof device for the Main site, Select Device → Add Radware Device → LinkProof</p>  <p>The LinkProof Icon for the Main site appears</p> 

Step	Description
4.	<p data-bbox="277 237 1227 268">Right click on the Main site LinkProof icon, Select Connect to the device.</p>  <p data-bbox="277 1058 1471 1129">The Connect LP Device box appears, enter the IP address of the Main site LinkProof device, select OK to continue.</p> 

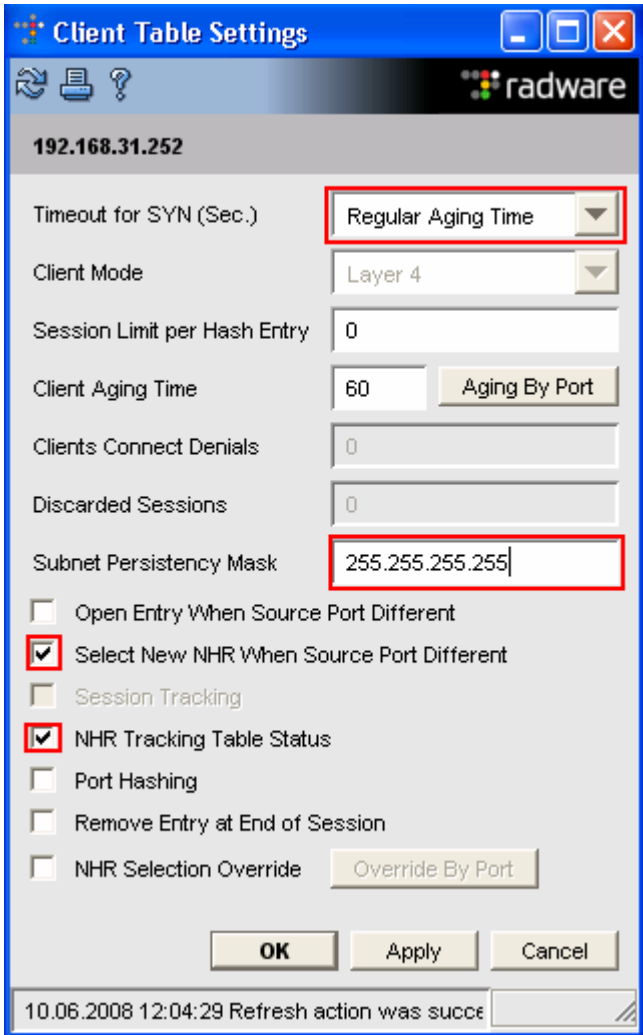
Step	Description
5.	<p>Create interfaces F-2 and F-3. Right mouse click on the LinkProof device. Select Setup.</p>  <p>The SetUp box appears, select Add</p> 

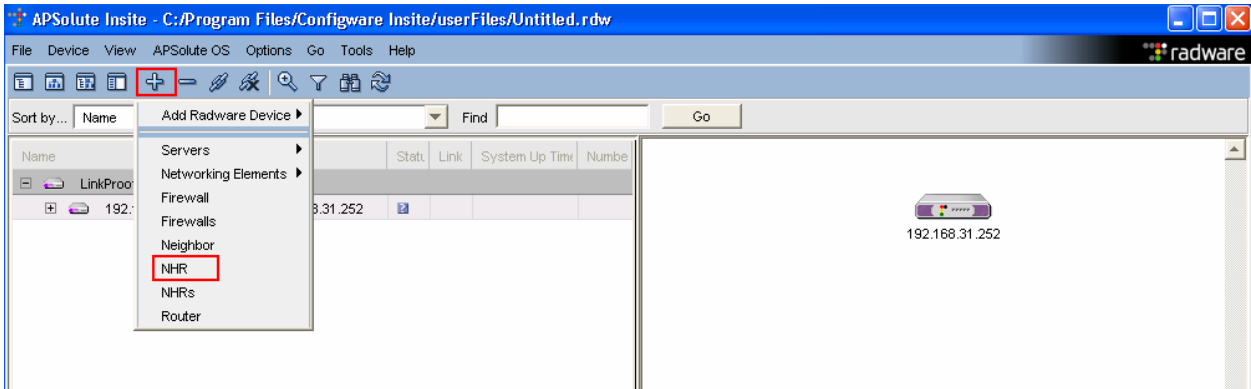
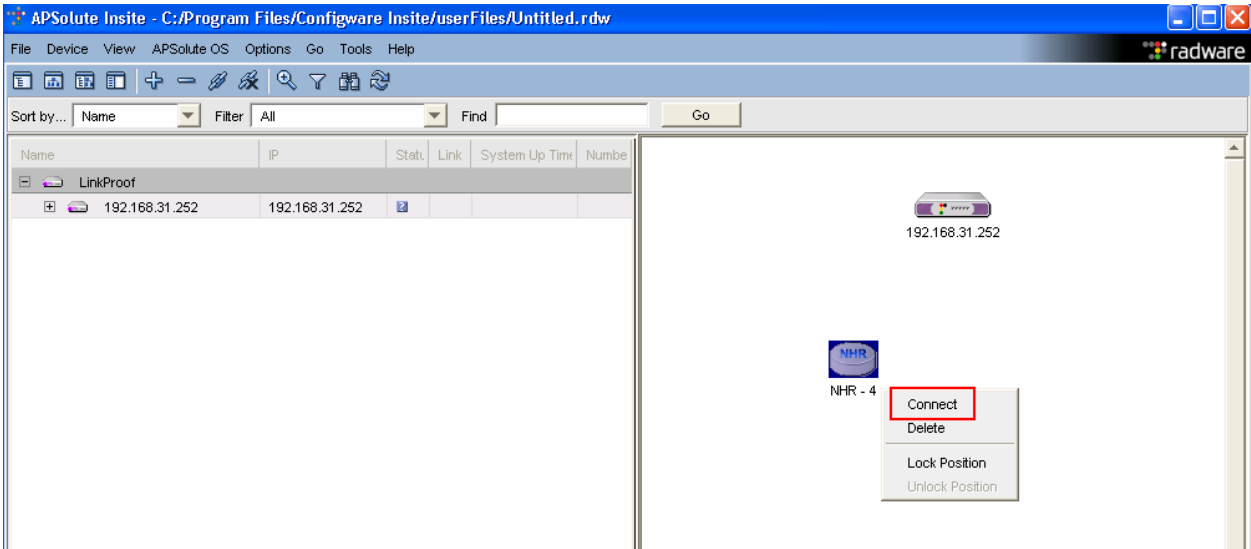
Step	Description
6.	<p>The Interface box appears, click on the pull down tab for If Num, select F-2. Enter the IP Address and Network Mask, select OK to continue.</p> 
7.	<p>Repeat Step 5 to create Interface F-3. Select OK to continue.</p> 

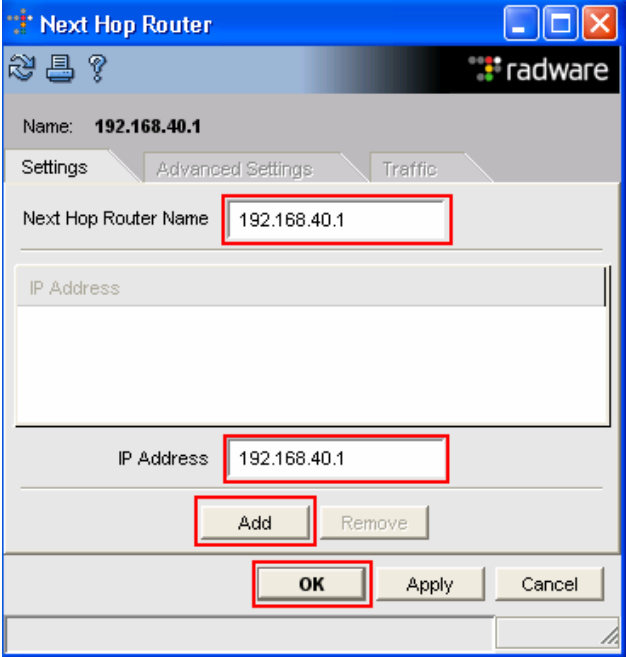
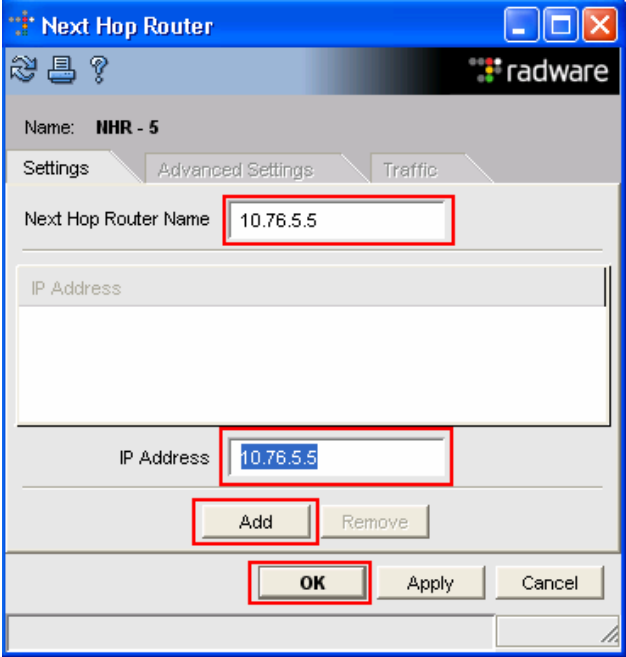
Step	Description																												
8.	<p>Add routes to the routing table.</p> <p>Right mouse click on the LinkProof device. Select Setup, click the pull down tab for Networking, select Routing Table. The Routing Table box appears, add the follow routes, select Add.</p>  <table><thead><tr><th>Dest 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																							

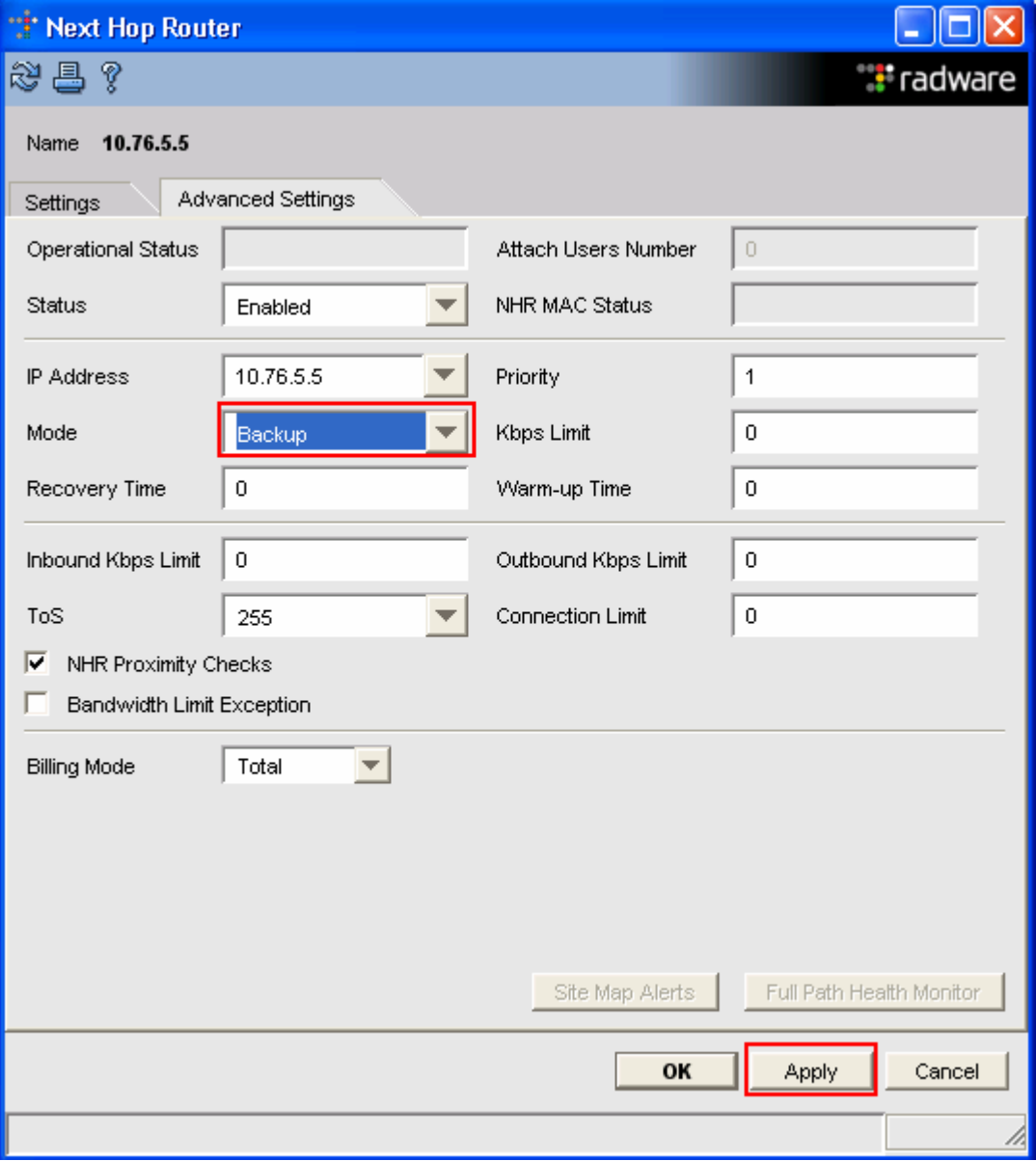
Step	Description
9.	<p>Add the following Default Routes, Add Destination IP Address, Mask Next Hop, IF Number. Click OK to continue.</p> <div data-bbox="371 340 886 940">  </div> <div data-bbox="911 340 1425 940">  </div>

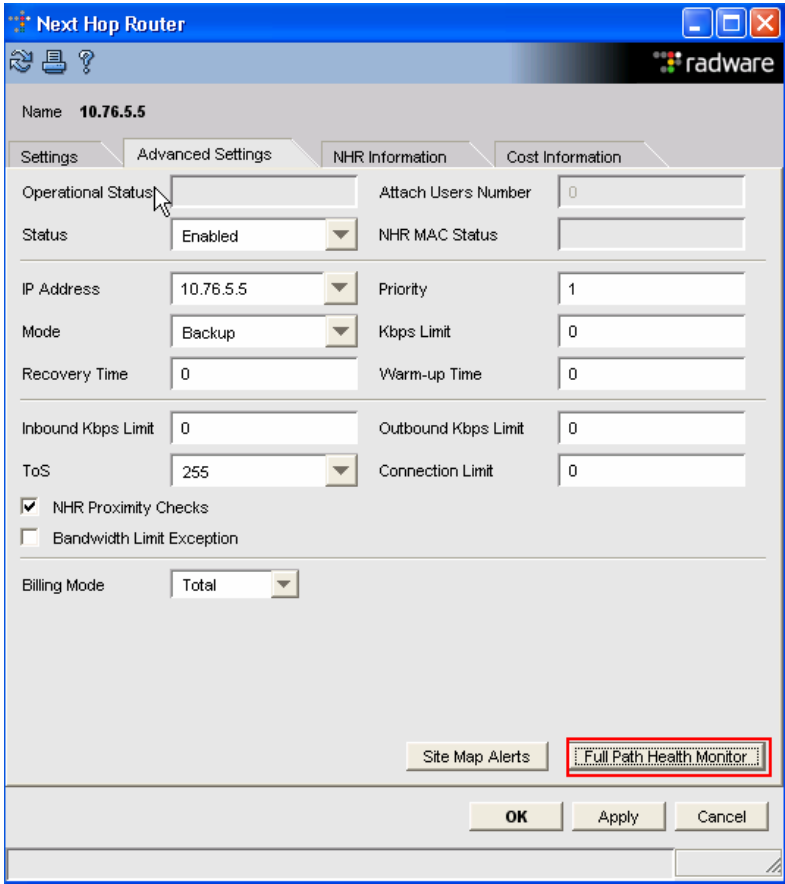
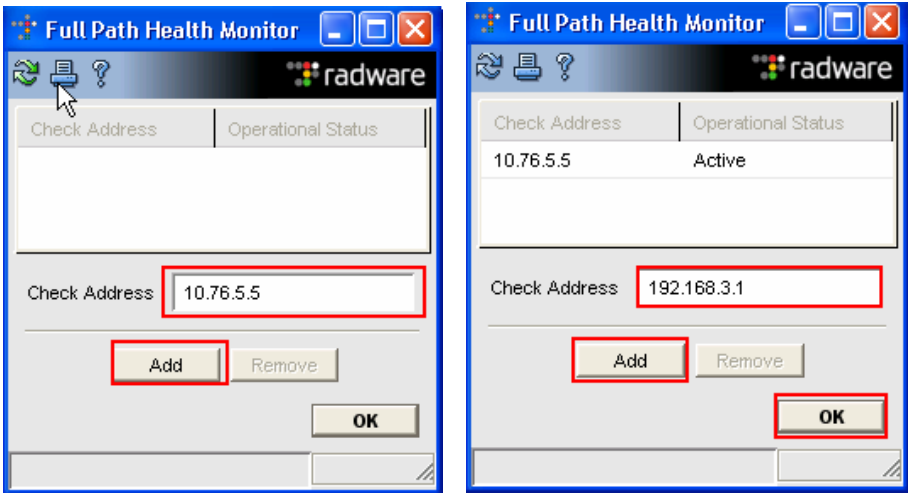
Step	Description
10.	<p>Add the following Local Routes, Add Destination IP Address, Mask Next Hop, IF Number. Click OK to continue.</p> <div data-bbox="375 342 889 940"> </div> <div data-bbox="915 342 1427 940"> </div> <div data-bbox="643 976 1157 1575"> </div>

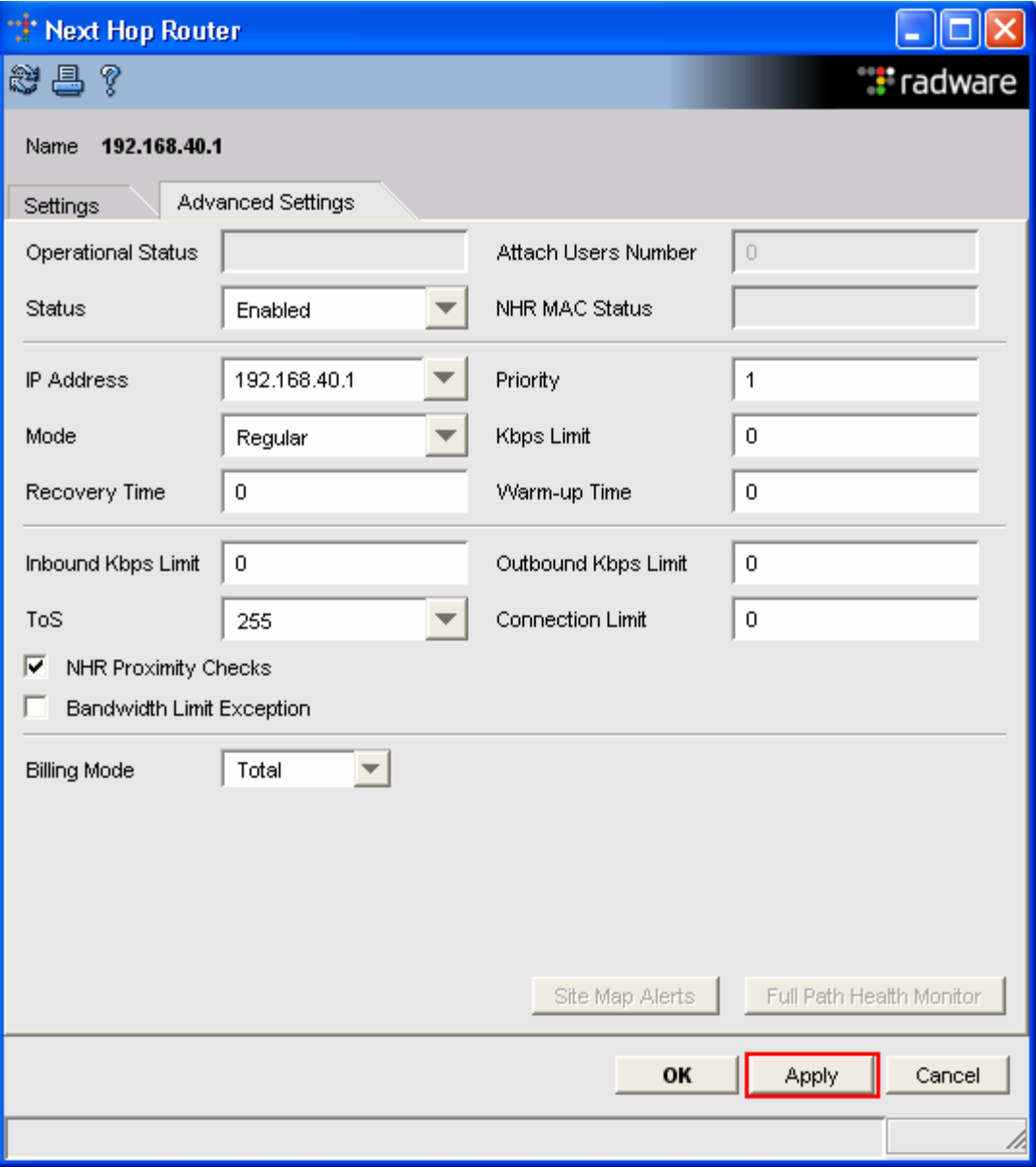
Step	Description
11.	<p>Configure the Client Table Settings on the LinkProof device.</p> <p>Right mouse click on the LinkProof device, select Setup, after the Setup box appears, select the Global tab, select Client Table Settings, then Edit Settings.</p> <p>Set the Following:</p> <ul style="list-style-type: 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 

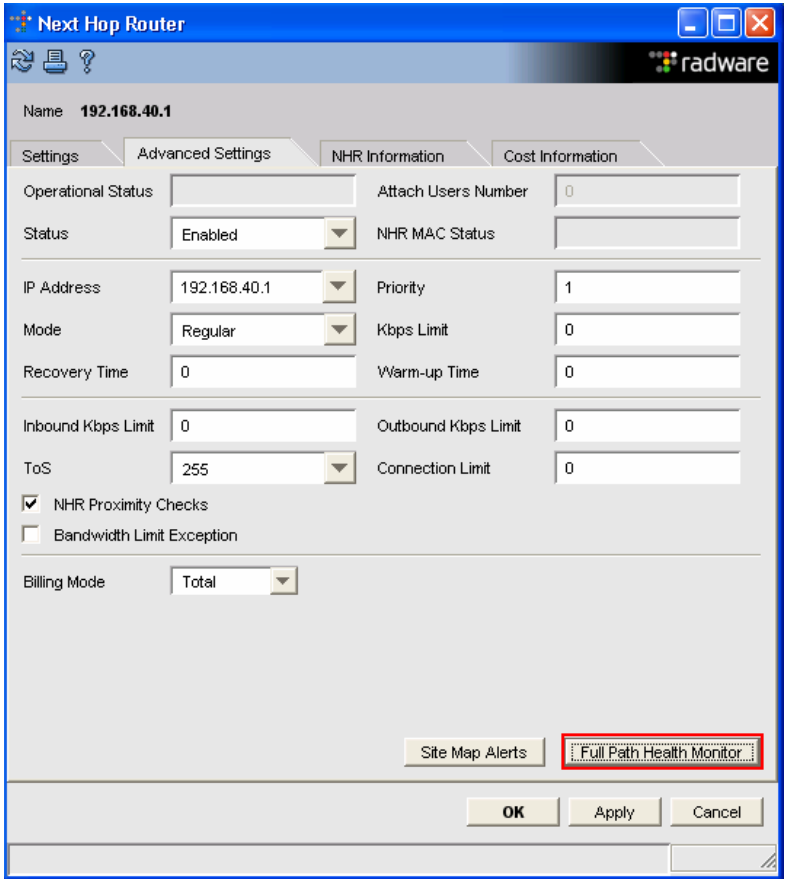
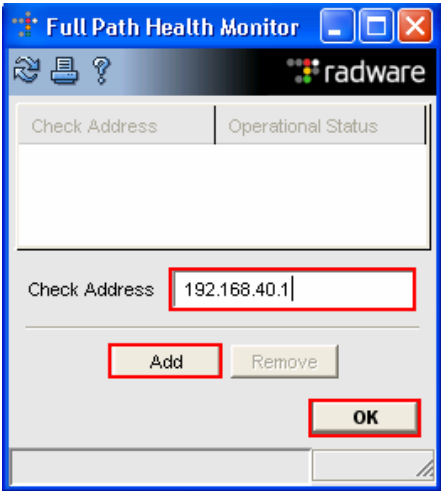
Step	Description
12.	<p>Create the following Next Hop Router (NHR) entries. Click + → NHR</p>  <p>A NHR icon appears, right mouse click on the NHR icon and select Connect.</p> 

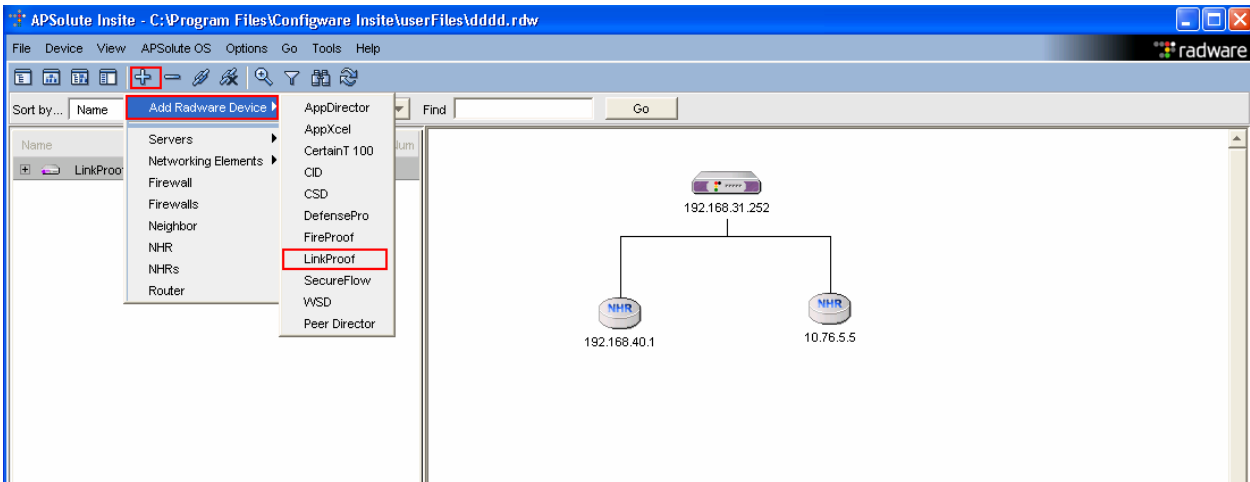
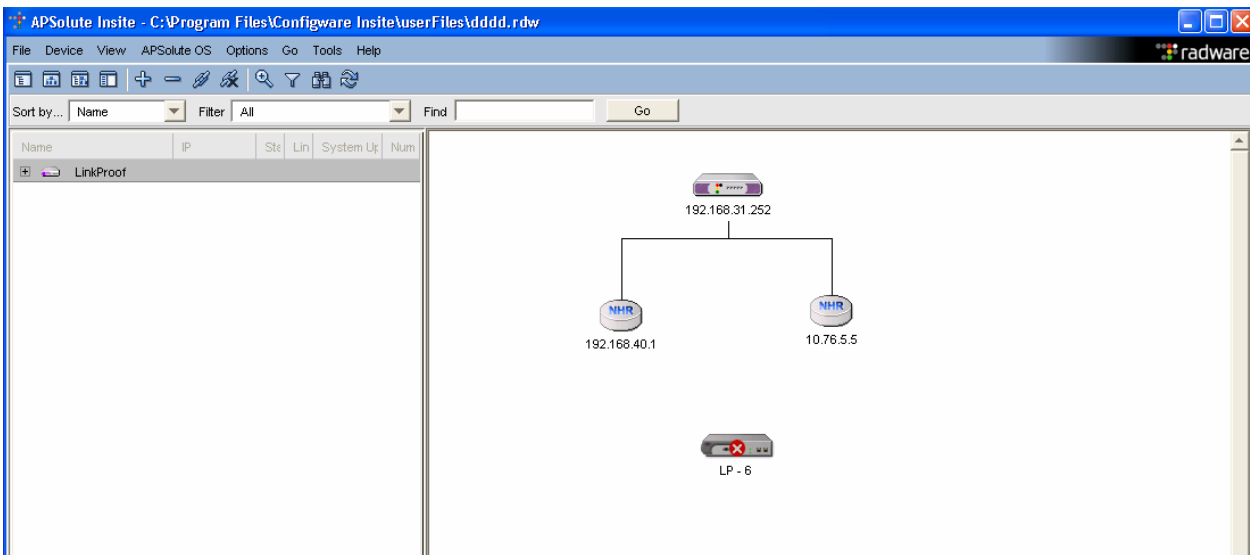
Step	Description
13.	<p>The Next Hop Router box appears, add the following information:</p> <ul style="list-style-type: none"> • Next Hop Router Name to 192.168.40.1 • IP Address to 192.168.40.1 <p>Select Add then OK to continue.</p>  <p>Repeat Step 12 to create the 2nd Next hop Router.</p> 

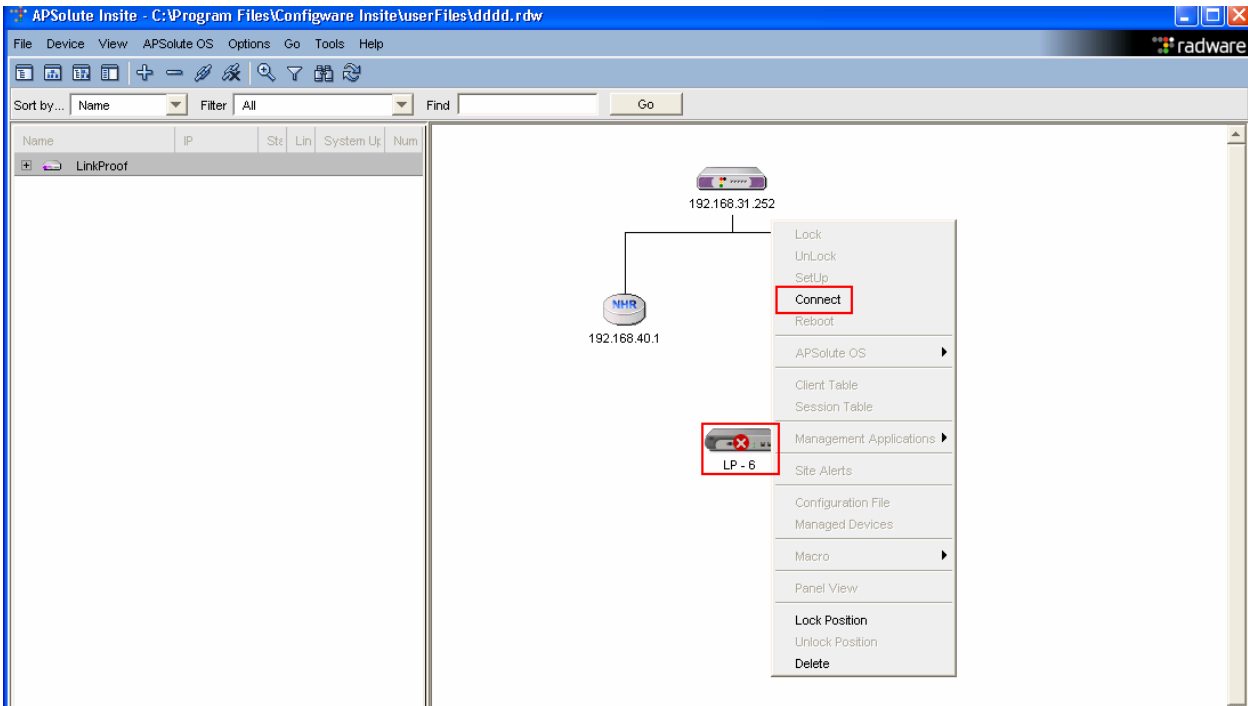

Step	Description
14.	<p data-bbox="277 243 927 275">Link the LinkProof and the two Next Hop Routers.</p> <p data-bbox="277 310 1531 422">Holding down the left mouse button, sweep it over the LinkProof and the two Next Hop Routers, then ctrl-L. After the Next Hop Router boxes appear (2), starting with interface 10.76.5.5, click on the pull down tab for Mode and select Backup, Press Apply to continue.</p> 

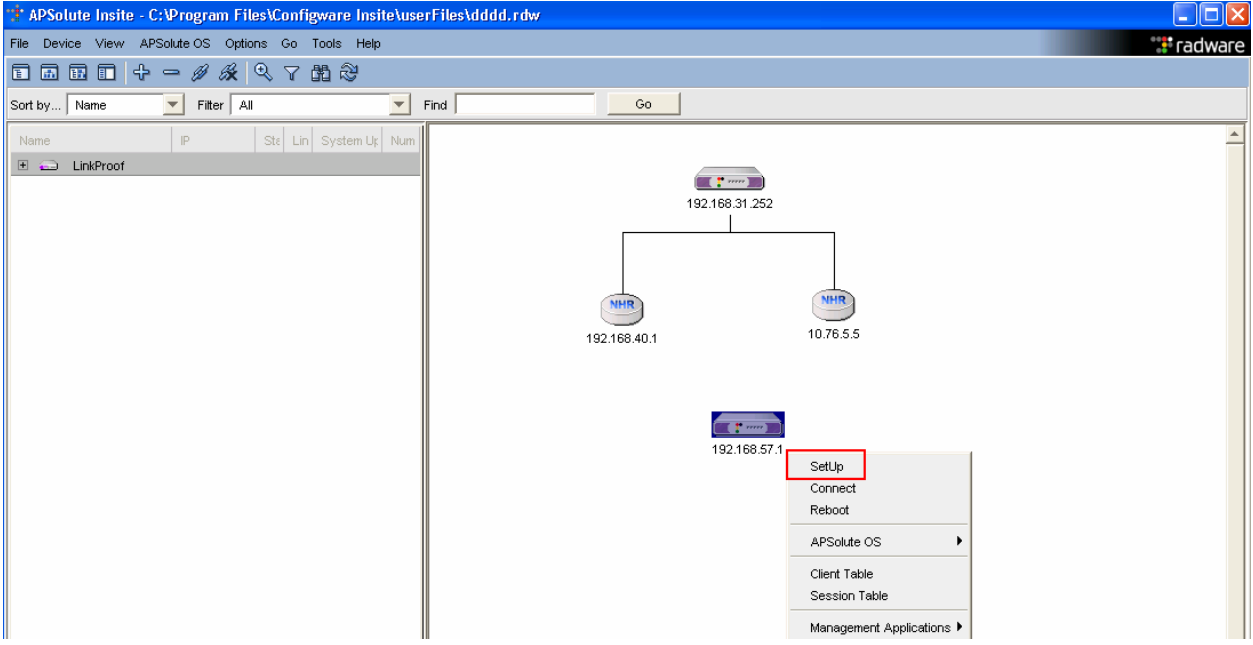
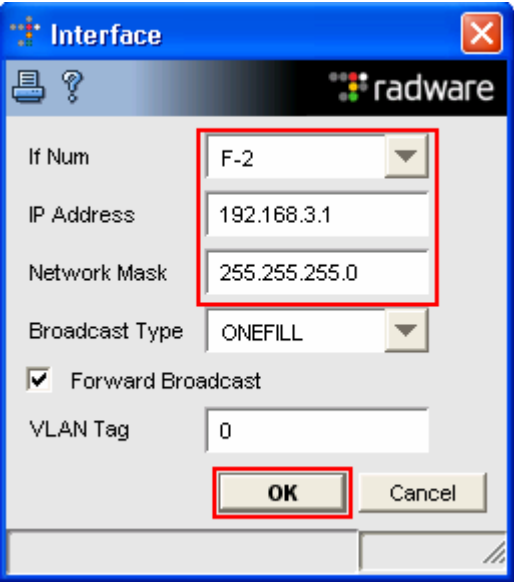
Step	Description
15.	<p>Another Next Hop Router box appears for interface 10.75.5.5. Select Full Path Health Monitor</p>  <p>Add the IP address of the routers. Refer to Figure1 for the IP addresses. Enter the IP address to the Check Address box, click Add, Repeat fort the second router address Click OK to continue.</p> 

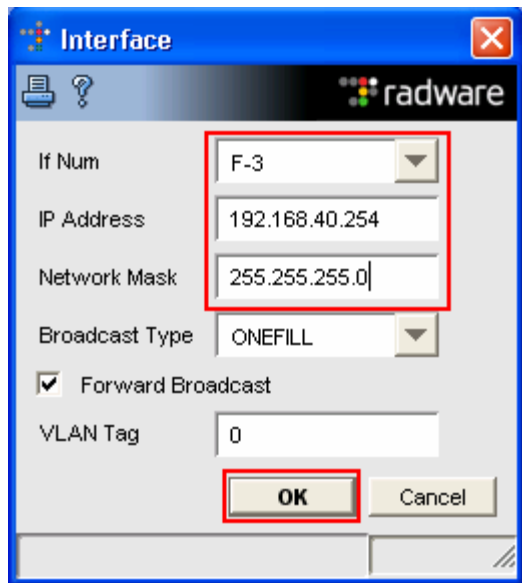
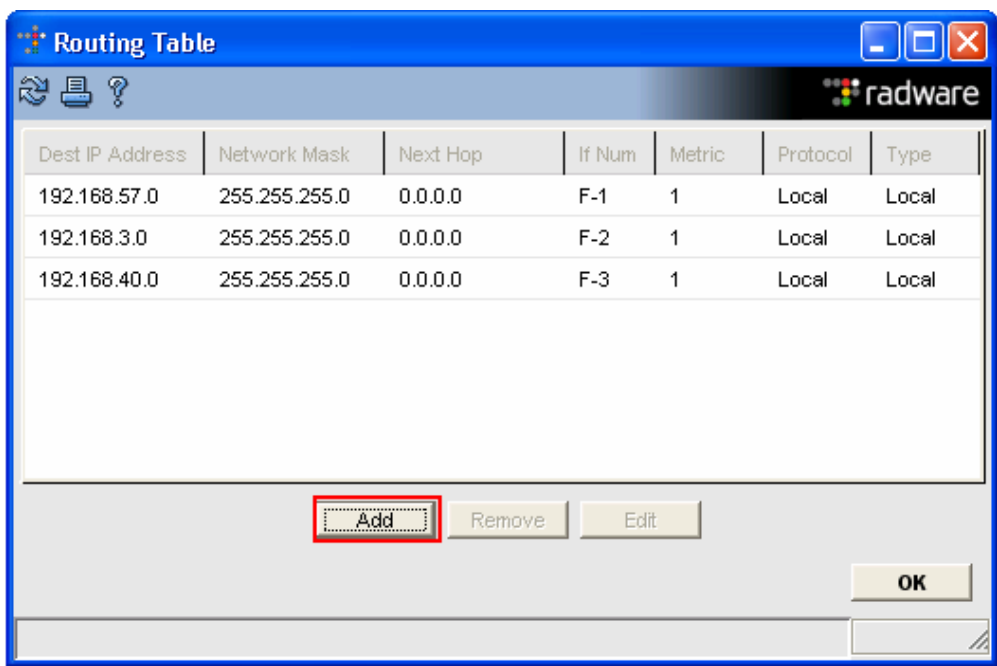
Step	Description
16.	<p>Interface 192.168.40.1, Press Apply to continue.</p> 

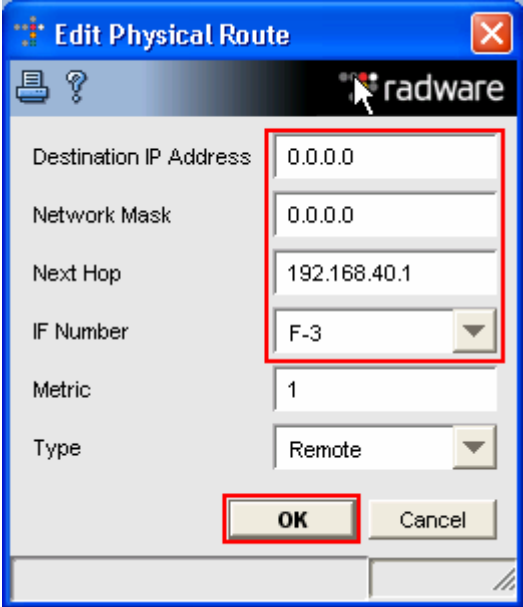
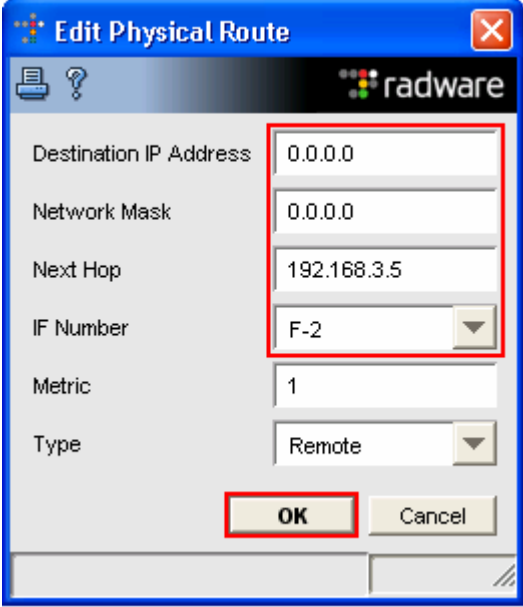
Step	Description
17.	<p>Another Next Hop Router box appears for interface 192.162.40.1. Select Full Path Health Monitor.</p>  <p>Add the IP address of the router. Refer to Figure1 for the IP addresses. Enter the IP address to the Check Address box, click Add, click OK to continue.</p> 

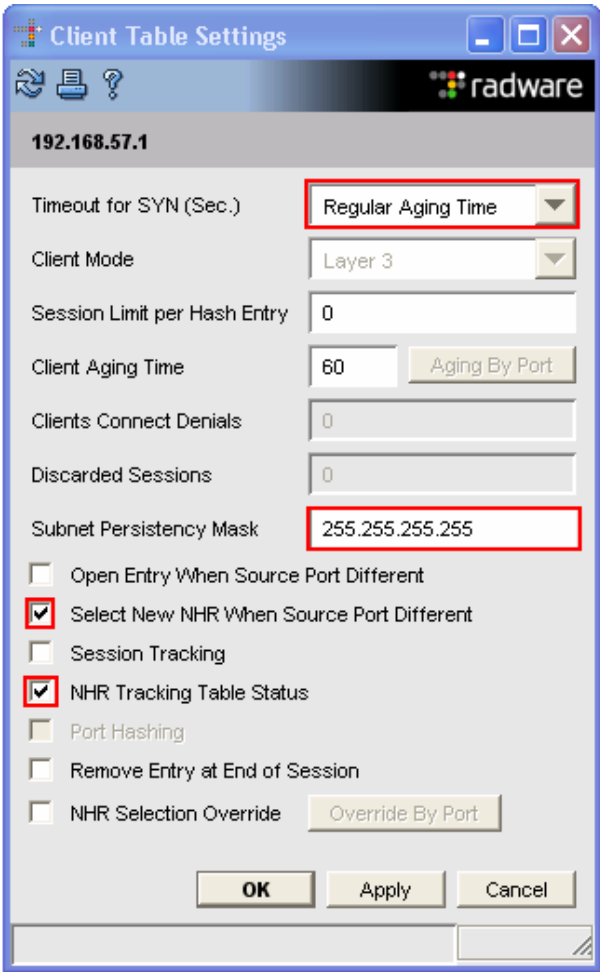
Step	Description
18.	<p>Add LinkProof device for the Branch site, Select Device → Add Radware Device → LinkProof.</p>  <p>The LinkProof icon for the Branch site should appear.</p> 

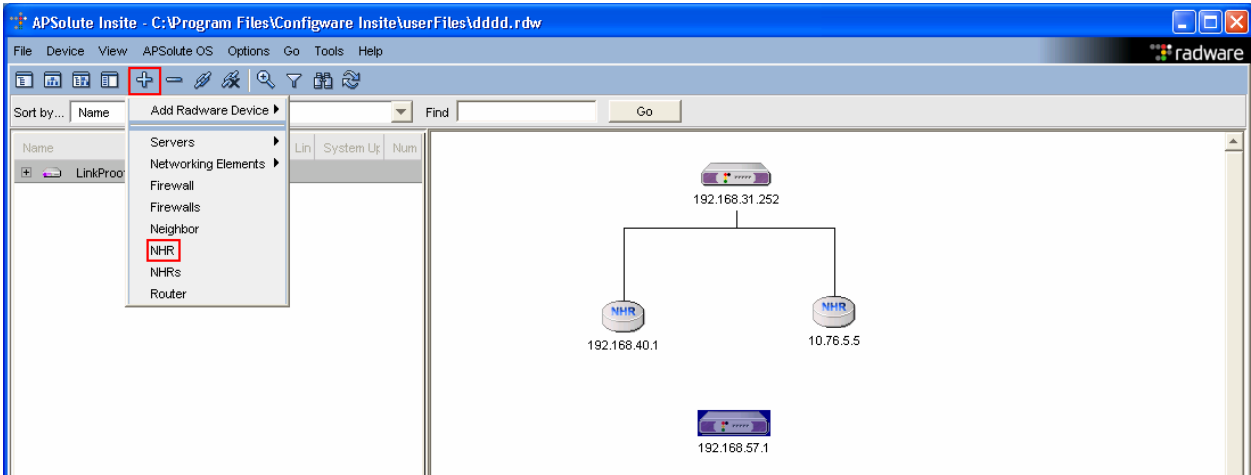
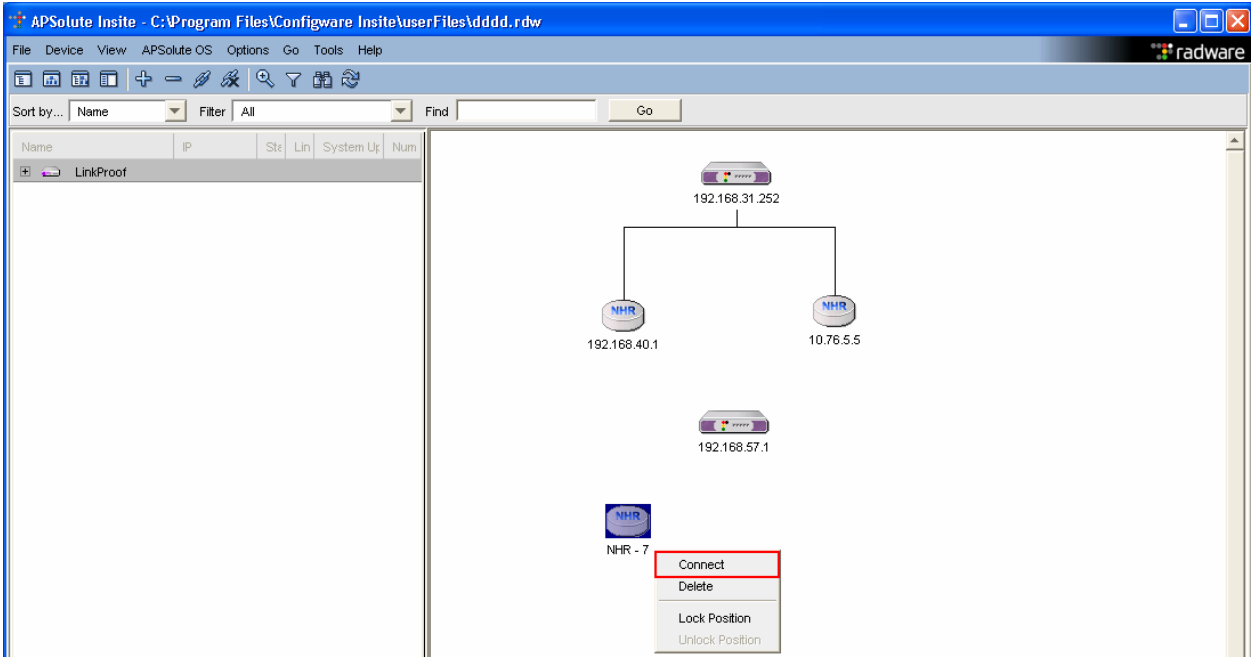
Step	Description
19.	<p data-bbox="277 237 1203 275">Right click on the Branch LinkProof icon, Select Connect to the device.</p>  <p data-bbox="277 1041 1528 1115">The Connect LP Device box appears, enter the IP address of the Branch LinkProof device, select OK to continue.</p> 

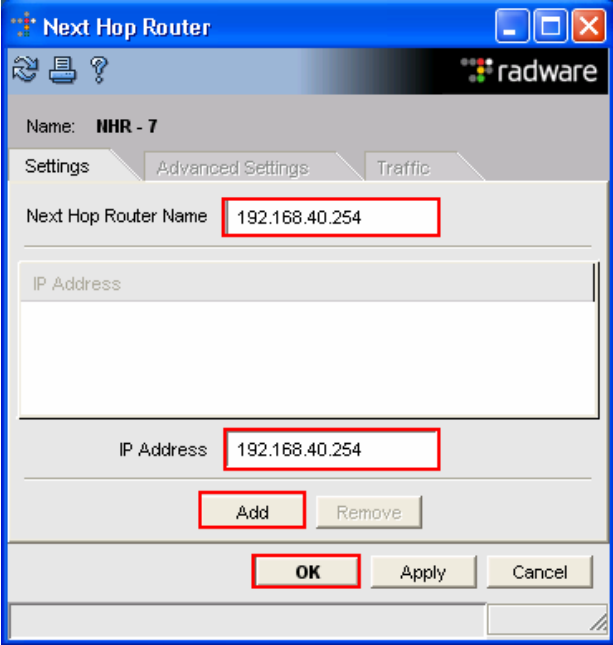
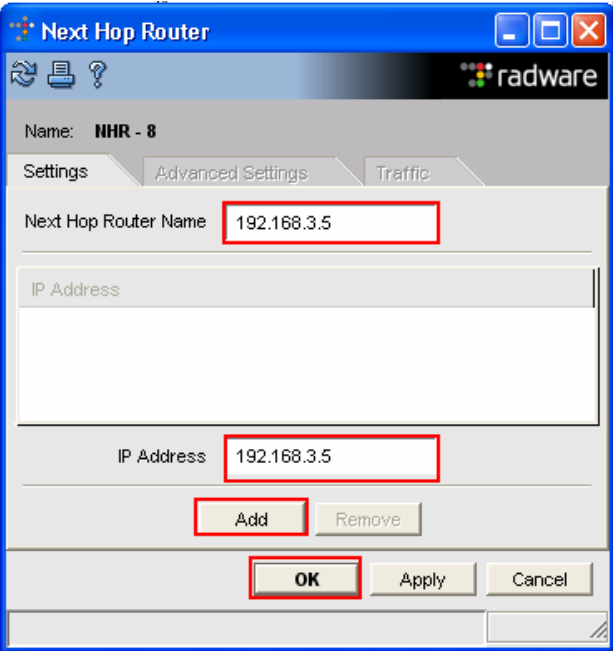
Step	Description
20.	<p>Create interfaces F-2 and F-3, Right mouse click on the Branch LinkProof device. Select Setup.</p> 
21.	<p>The Interface box appears, click on the pull down tab for If Num, and select F-2. Enter the IP Address and Network Mask, select OK to continue.</p> 

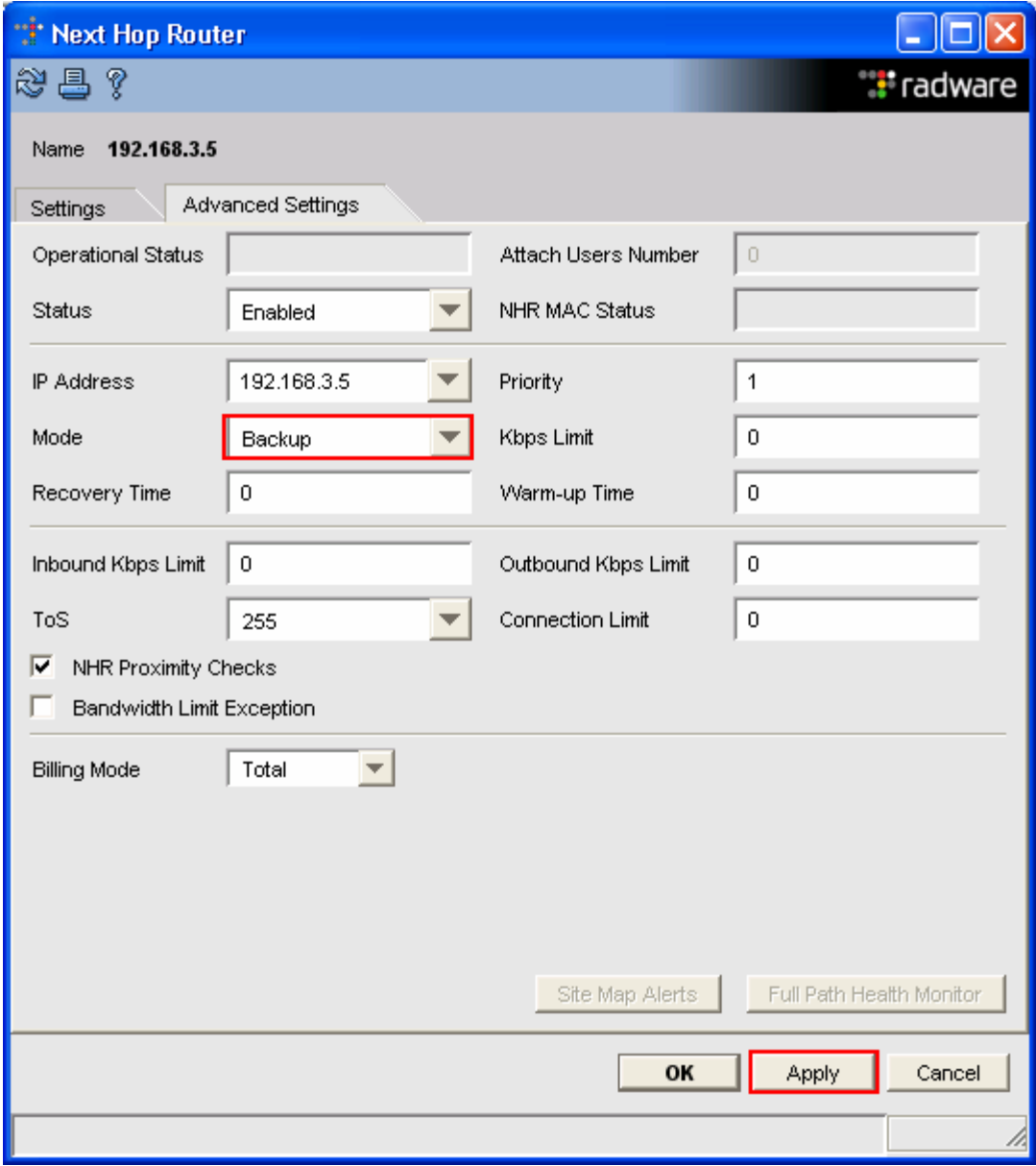
Step	Description																												
22.	<p>Repeat Step 5 to create Interface F-3. Select OK to continue.</p> 																												
23.	<p>Add routes to the routing table.</p> <p>Right mouse click on the LinkProof device. Select Setup, click the pull down tab for Networking, select Routing Table. The Routing Table box appears, add the following routes, select Add.</p>  <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>192.168.57.0</td><td>255.255.255.0</td><td>0.0.0.0</td><td>F-1</td><td>1</td><td>Local</td><td>Local</td></tr><tr><td>192.168.3.0</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	192.168.57.0	255.255.255.0	0.0.0.0	F-1	1	Local	Local	192.168.3.0	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																							
192.168.57.0	255.255.255.0	0.0.0.0	F-1	1	Local	Local																							
192.168.3.0	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																							

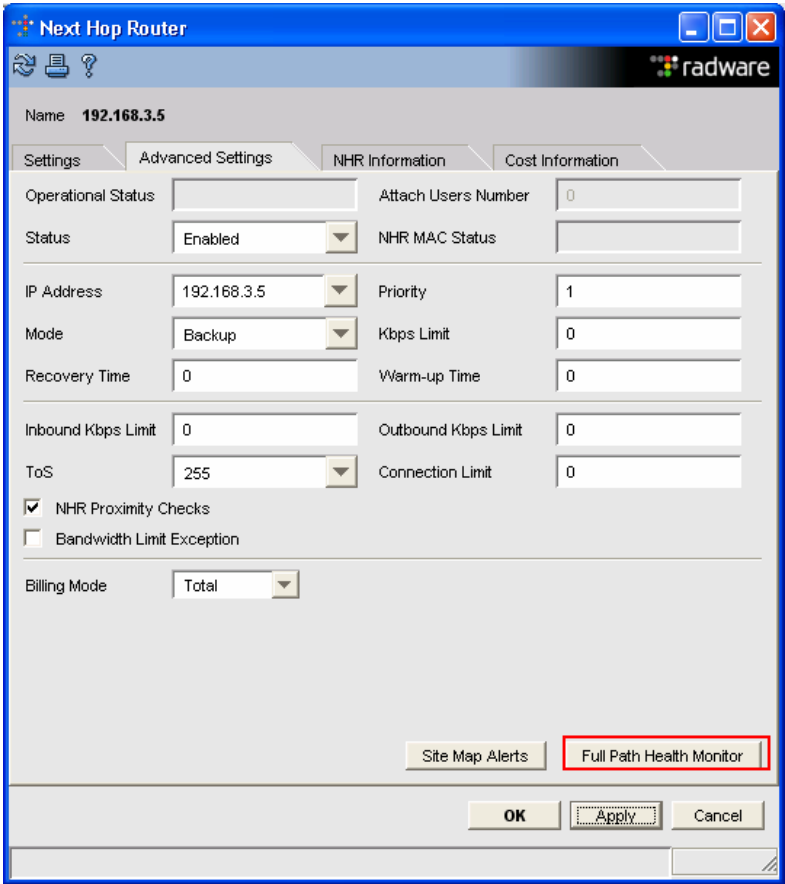
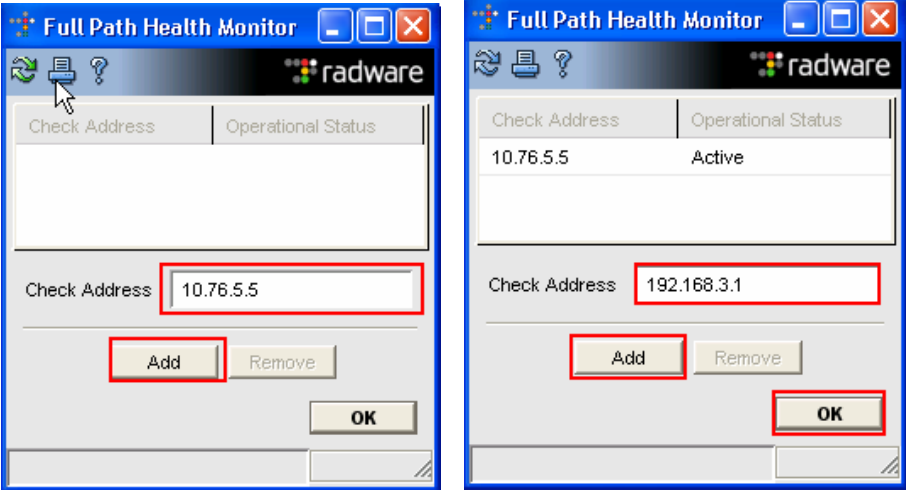
Step	Description
24.	<p>Add the following Default Routes, Add Destination IP Address, Mask Next Hop, IF Number.</p> <div data-bbox="370 310 889 913">  </div> <div data-bbox="911 310 1430 913">  </div>

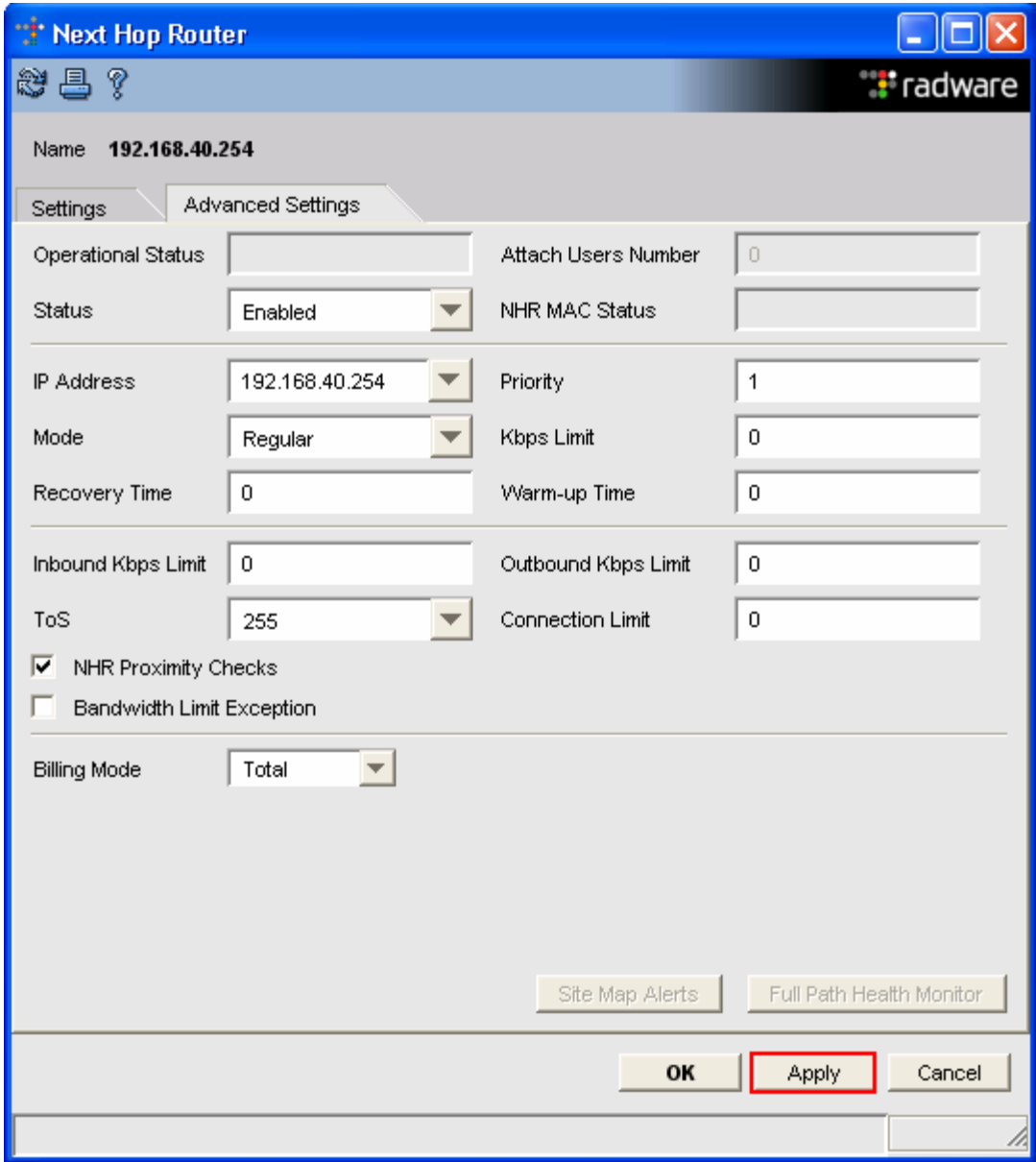
Step	Description
25.	<p>Configure the Client Table selections on the Branch LinkProof device.</p> <p>Right mouse click on the Branch LinkProof device, select Setup, after the Setup box appears, select the Global tab, select Client Table Settings, then Edit Settings.</p> <p>Set the Following:</p> <ul 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> 

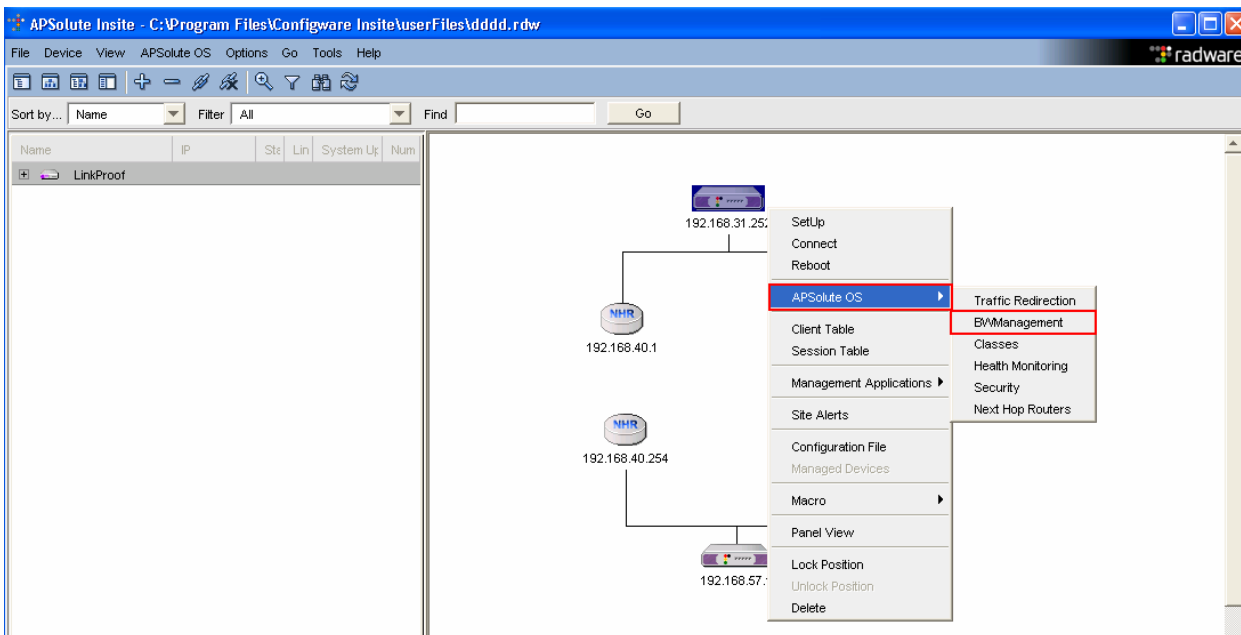
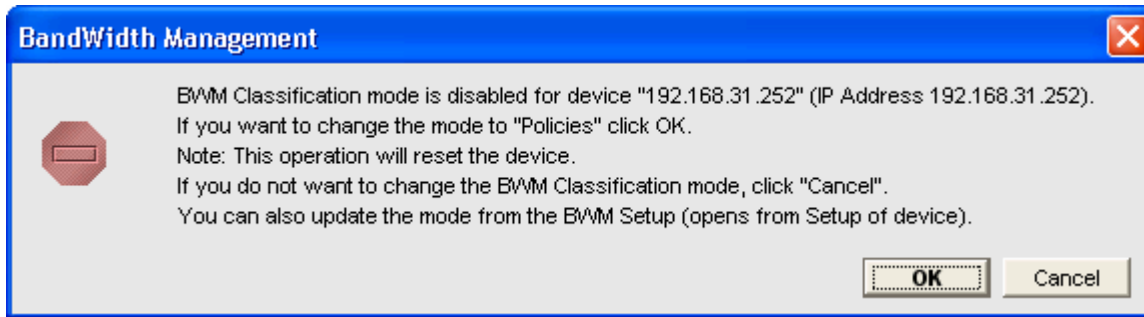
Step	Description
27.	<p>The Next Hop Router box appears, add the following information:</p> <ul style="list-style-type: none"> • Next Hop Router Name to 192.168.40.254 • IP Address to 192.168.40.254 <p>Select Add then OK to continue.</p>  <p>Repeat Step 27 to create the 2nd Next hop Router.</p> 

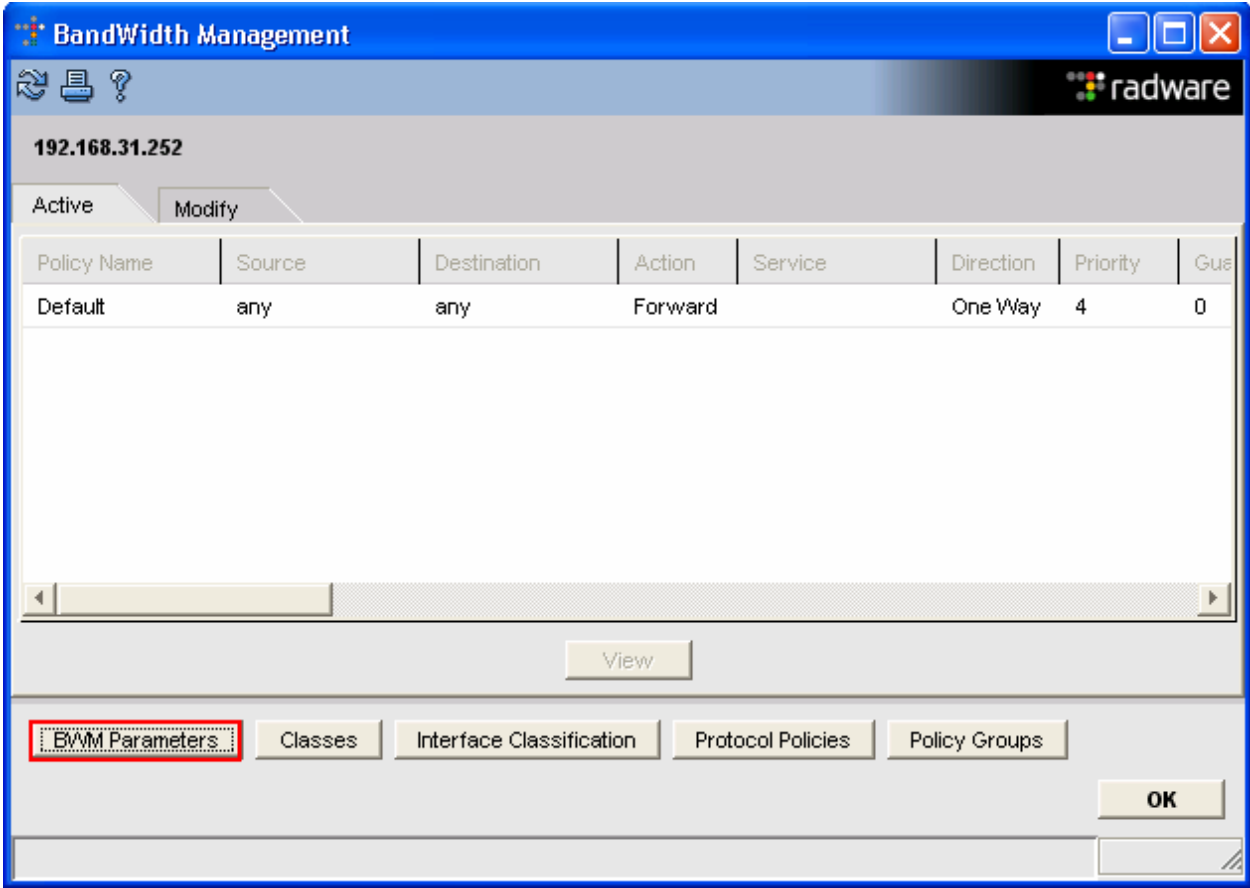
Step	Description
28.	<p data-bbox="277 237 1143 273">Link the Branch LinkProof and the two Branch Next Hop Routers.</p> <p data-bbox="277 310 1484 451">Holding down the left mouse button, sweep it over the Branch LinkProof and the two Branch Next Hop Routers, then ctrl-L. After the Next Hop Router boxes appear, starting with interface 192.168.3.5, click on the pull down tab for Mode and select Backup, Press Apply to continue.</p> 

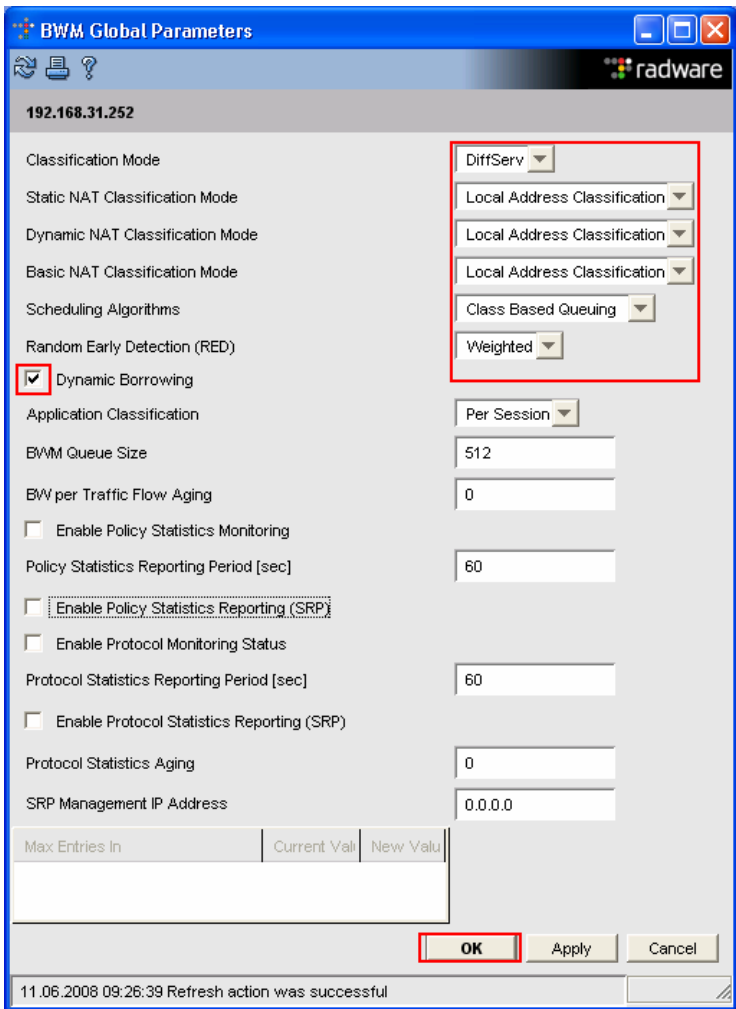
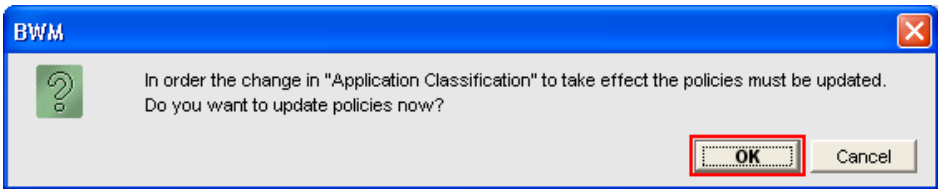
Step	Description
29.	<p>Another Next Hop Router box appears for interface 192.168.3.5. Select Full Path Health Monitor</p>  <p>Add the IP address of the routers. Refer to Figure1 for the IP addresses. Enter the IP address to the Check Address box, click Add, Repeat for the second router address Click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

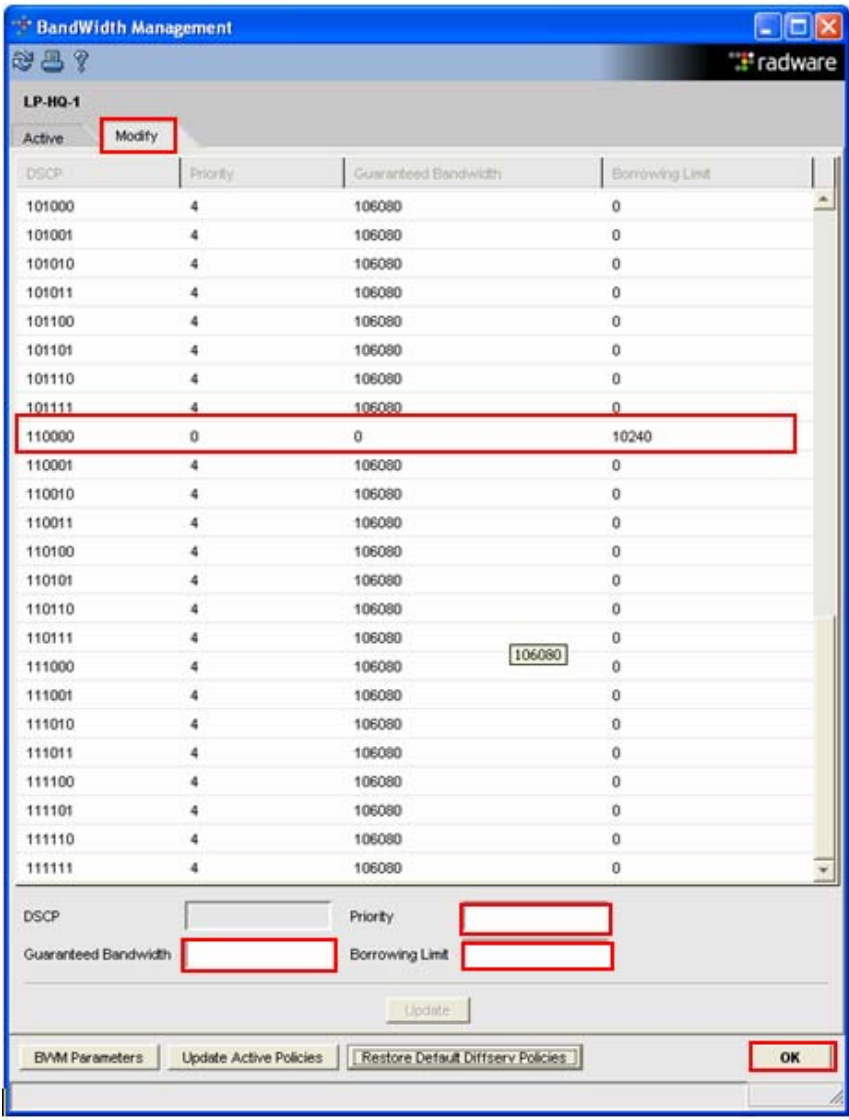
Step	Description
30.	<p>Interface 192.162.40.254, Press Apply to continue.</p>  <p>The screenshot shows the 'Next Hop Router' configuration window for the interface 192.168.40.254. The window has a blue title bar and a Radware logo. It contains two tabs: 'Settings' and 'Advanced Settings'. The 'Advanced Settings' tab is active, showing various configuration fields. The 'Operational Status' is set to 'Enabled'. The 'IP Address' is 192.168.40.254. The 'Mode' is 'Regular'. The 'Billing Mode' is 'Total'. The 'Apply' button is highlighted with a red box.</p>

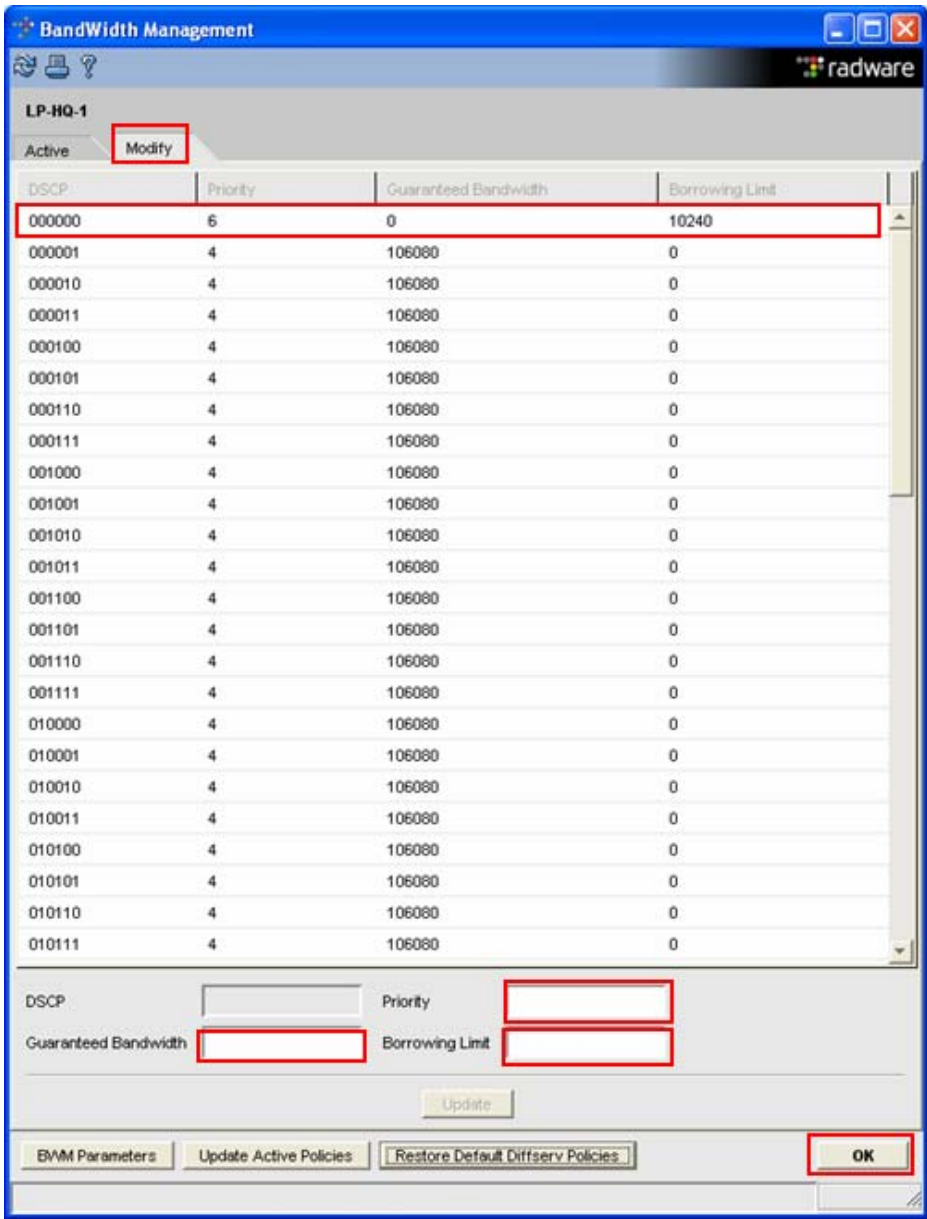
Step	Description
31.	<p>Another Next Hop Router box appears for interface 192.162.40.1. Select Full Path Health Monitor.</p> <div data-bbox="511 340 1289 1213" data-label="Image"> </div> <p>Add the IP address of the router. Refer to Figure1 for the IP addresses. Enter the IP address to the Check Address 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> 

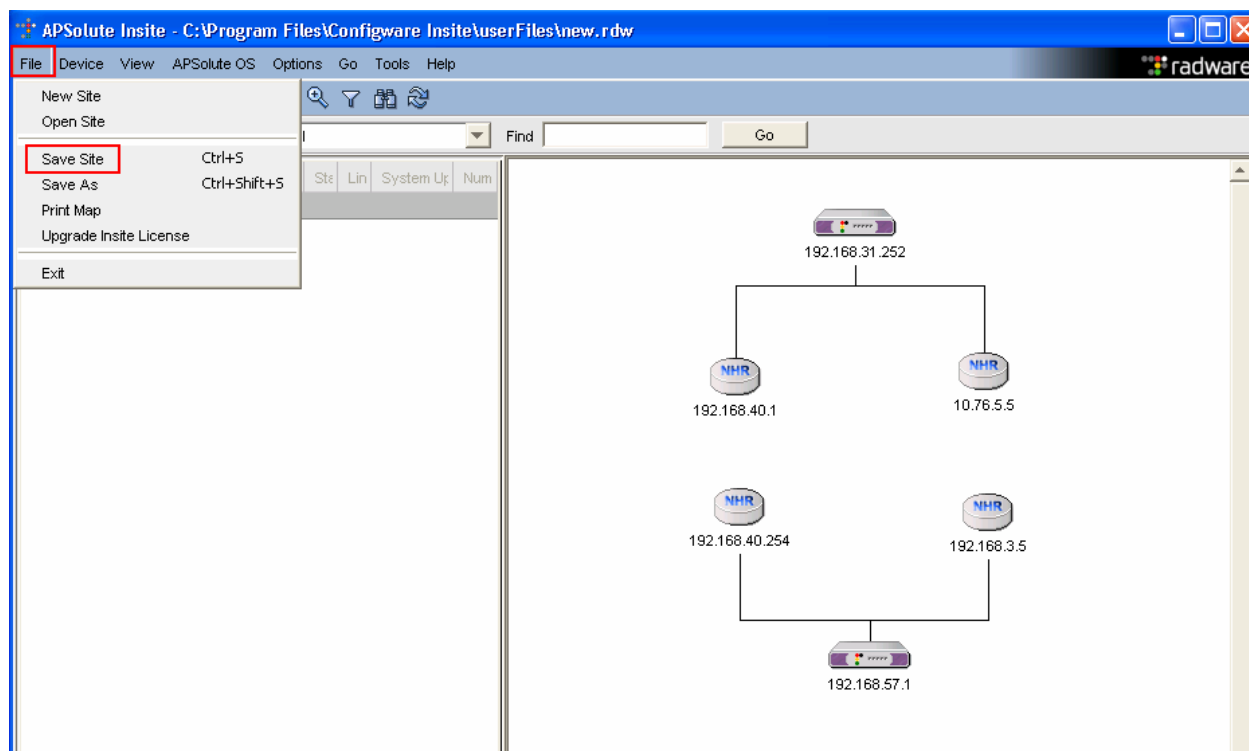
Step	Description
33.	<p>Once the LinkProof finishes rebooting the BandWidth Management box appears. Select BWM Parameters to continue.</p> 

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> 

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>  <p>The screenshot shows the 'BandWidth Management' window for device 'LP-HQ-1'. The 'Modify' tab is selected. A table lists DSCP values and their corresponding settings. The first row, DSCP 000000, is highlighted with a red box, showing a Priority of 6, Guaranteed Bandwidth of 0, and a Borrowing Limit of 10240. Below the table, there are input fields for DSCP, Priority, Guaranteed Bandwidth, and Borrowing Limit, each with a red box around it. At the bottom right, the 'OK' button is highlighted with a red box.</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 in the field from the perspective of the Radware LinkProof Multi-WAN 3020 Switch. In general, the verification steps include:

1. Verify the DHCP relay on the Radware LinkProof Multi-WAN 3020 Switch is functioning by confirming that the IP Telephones receive their IP addresses from the DHCP server connected to the Radware LinkProof Multi-WAN 3020 Switch.
2. Check that the Avaya IP telephones have successfully registered with Avaya Communication Manager by the **list registered-station**
3. Place internal and external calls between the digital telephone and IP telephones at each site.

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 Communication Manager 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] *Administrator Guide for Avaya Communication Manager*, February 2007, Issue 3.1, Document Number 03-300509
- [2] *Installing and Administering SIP Enablement Services*, March 2007, Issue 2.1, Document Number 03-600768
- [3] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide*
- [4] *Messaging Application Server (MAS) Administration Guide Release 3.1*, February 2007

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

- [5] *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.