



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Talari Networks Adaptive Private Networking Solution with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya IP Telephones in a Multi-Site Converged VoIP and Data Network - Issue 1.0

Abstract

These Application Notes describe procedures for configuring the Talari Networks Adaptive Private Networking Solution with an Avaya Aura® Telephony Infrastructure including Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya IP Telephones in a Multi-Site Converged VoIP and Data Network

The Talari T730 provides the enterprise with multiple connections to the WAN for redundancy and provides traffic redirection on the WAN links. In addition, the T730 provides load balancing, Layer2/Layer3 Quality of Service, bandwidth management and traffic shaping. The compliance testing focused on how these feature sets provide improved access of remote site IP telephony users to the telephony applications at the main enterprise site in light of heavy link utilization and failures.

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 document how to configure the Talari Networks Adaptive Private Networking Solution with an Avaya Aura® Telephony Infrastructure including Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya IP Telephones in a Multi-Site Converged VoIP and Data Network

The Talari T730 provides the enterprise with multiple connections to the WAN for redundancy and provides traffic redirection on the WAN links. In addition, the T730 provides load balancing, Layer2/Layer3 Quality of Service (Qos), bandwidth management and traffic shaping. The compliance testing focused on how these feature sets provide improved access of remote site IP telephony users to the telephony applications at the main enterprise site in light of heavy link utilization and failures.

2. General Test Approach and Test Results

The general test approach was to configure a Multi-Site Voice over IP (VoIP) Solution using the Talari Networks Adaptive Private Networking Solution with Aura® Communication Manager, Avaya Aura® Session Manager and Avaya IP Telephones with emphasis placed on voice quality while the Talari enforced load balancing, Layer2/Layer3 Quality of Service, and traffic shaping policies. The configuration, (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered, feature functionality, serviceability, and performance testing. Compliance testing emphasis was placed on verifying voice quality in a multi-site converged VoIP and data network scenario. Specifically, compliance testing verified that the Avaya IP telephones retain good voice quality between the corporate and branch sites while the Talari T730 enforced, load balancing, Layer2/Layer3 Quality of Service, and traffic shaping policies.

Feature functionality tested:

- Enforce Layer2/Layer3 Quality of Service
- VLANs
- Best path link with traffic
- Link Failover
- Traffic shaping

Telephony features verified to operate correctly included:

- Attended/Unattended transfer
- Conference call add/drop/participation
- Multiple call appearances
- Caller ID operation
- Call forwarding
- Call Park/Call pick-up
- Bridged call appearances
- Voicemail using Communication Manager Messaging and Avaya Modular Messaging
- Message Waiting Indicator (MWI)
- Hold/Return from hold
- Direct IP Media (Shuffling)
- G.711 and G.729 codecs

Serviceability testing:

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

2.2. Test Results

The Talari Networks Adaptive Private Networking Solution with Aura® Communication Manager, Avaya Aura® Session Manager and Avaya IP Telephones passed compliance testing.

2.3. Support

Technical support for Talari can be obtained through the following:

- Phone: +1 408 689 0400
- Web support: <http://www.talari.com/support>
- Email: support@talari.com

3. Reference Configuration

The network diagram shown in Figure 1 illustrates the network environment used for the compliance test. The Talari Networks Adaptive Private Networking Solution provides network connectivity for the voice and data traffic between the Corporate and Remote Sites.

The Avaya and Talari components used to create the corporate site included:

- Avaya S8300D Server running Avaya Aura® Communication Manager & Avaya Aura® Communication Manager Messaging
- Avaya S8800 Server running Avaya Aura® Session Manager
- Avaya S8800 Server running Avaya Aura® System Manager
- Avaya G450 Media Gateway
- Avaya Modular Messaging Server (MAS) and (MSS)
- Avaya 9600-Series IP telephone (H.323)
- Avaya 9600-Series IP telephone (SIP)
- Avaya 2410 digital telephone
- Talari Networks T730 Appliance
- LAN router/switch
- DHCP/HTTP/TFTP Server

The Avaya and Talari components used to create the remote site included:

- Avaya 9600-Series IP telephone (H.323)
- Avaya 9600-Series IP telephone (SIP)
- Talari Networks T730 Appliance
- LAN router/switch

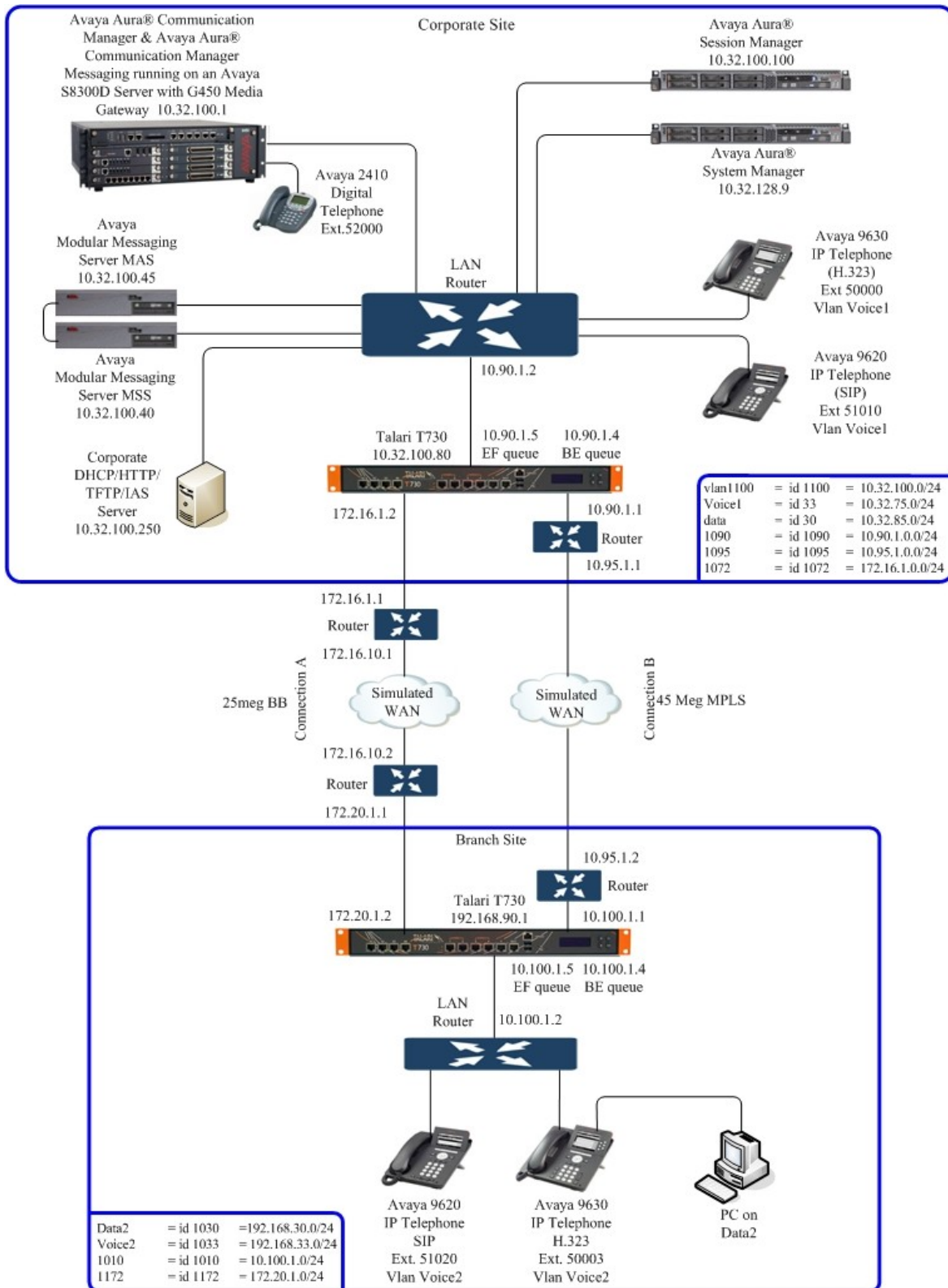


Figure 1: Avaya IP Telephony Network traversing Talari Networks Adaptive Private Networking Solution

4. Equipment and Software Validated

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

Equipment	Software/Firmware
<i>Avaya PBX Products</i>	
Avaya S8300D Server running Avaya Aura® Communication Manager	Avaya Aura® Communication Manager 6.0
Avaya G450 Media Gateway (Corporate Site) MGP MM712 DCP Media Module	30.13.2 HW9
<i>Avaya Aura® Session Manager</i>	
Avaya Aura® Session Manager	6.0
Avaya Aura® System Manager	6.0
<i>Avaya Messaging (Voice Mail) Products</i>	
Avaya Modular Messaging - Messaging Application Server (MAS)	5.2
Avaya Modular Messaging - Message Storage Server (MSS)	5.2
Avaya Aura® Communication Manager Messaging (CMM)	6.0
<i>Avaya Telephony Sets</i>	
Avaya 9600 Series IP Telephones	(H.323 3.1.1) and (SIP 2.6.4)
Avaya 2410 Digital Telephone	5.0
<i>Talari Network Products</i>	
Talari T730	2.1 GA_P1
<i>MS Products</i>	
DHCP/HTTP/TFTP/IAS Server	Microsoft Windows 2003 Server

Table 1: Equipment and Software Tested

The specific equipment above was used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager.

5. Avaya Aura® Communication Manager

There is no Talari specific configuration required on Avaya Aura® Communication Manager and Avaya Aura® Session Manager to support this solution. It is assumed that all Aura® Telephony components and appropriate licenses and authentication files have been configured already, e.g., trunks, dial plans, etc, and will not be covered in this document. For detailed information on the installation, maintenance, and configuration of Communication Manager and Session Manager, please reference **Section 9**. **Sections 5.1** and **5.2** are supplied for reference only; no special configuration is required.

5.1. Verify OPS Capacity

Using the SAT, verify that the Off-PBX Telephones - OPS feature is enabled on the **Optional Features** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative. On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

display system-parameters customer-options		Page 1 of 11
OPTIONAL FEATURES		
G3 Version: V16	Software Package: Enterprise	
Location: 2	System ID (SID): 1	
Platform: 28	Module ID (MID): 1	
		USED
Platform Maximum Ports:	6400	143
Maximum Stations:	2400	44
Maximum XMOBILE Stations:	2400	0
Maximum Off-PBX Telephones - EC500:	9600	5
Maximum Off-PBX Telephones - OPS:	9600	35
Maximum Off-PBX Telephones - PBFMC:	9600	0
Maximum Off-PBX Telephones - PVFMC:	9600	0
Maximum Off-PBX Telephones - SCCAN:	0	0
Maximum Survivable Processors:	313	0
(NOTE: You must logoff & login to effect the permission changes.)		

5.2. Verify QoS

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 now utilized to prioritize VoIP traffic and should be implemented throughout the entire network.

In order to achieve prioritization of VoIP traffic, the VoIP traffic must be classified. The Avaya Aura® telephony infrastructure supports both IEEE 802.1p and DiffServ.

The DiffServ and 802.1p/Q values configured here will be downloaded to the Avaya H.323 IP Telephones via Communication Manager. Avaya SIP IP Telephones will get QoS settings by downloading the 46xxsettings file from the HTTP server. For more information on QoS settings refer to **Section 9**.

On **Page 1** of the **change ip-network-region** form, verify the Differentiated Services Code Points. The Differentiated Services Code Point for **Call Control PHB Value** and **Audio PHB Value** are **46** and the **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: Authoritative Domain: dev4.com		
Name: Main		
MEDIA PARAMETERS		
Intra-region IP-IP Direct Audio: yes		
Inter-region IP-IP Direct Audio: yes		
IP Audio Hairpinning? n		
Codec Set: 1		
UDP Port Min: 2048		
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
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		
RSVP Enabled? n		
H.323 IP ENDPOINTS		
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

6. Configure the Corporate Talari T730

It is assumed that all appropriate Talari licenses are installed. For instructions, refer to **Section 9**.

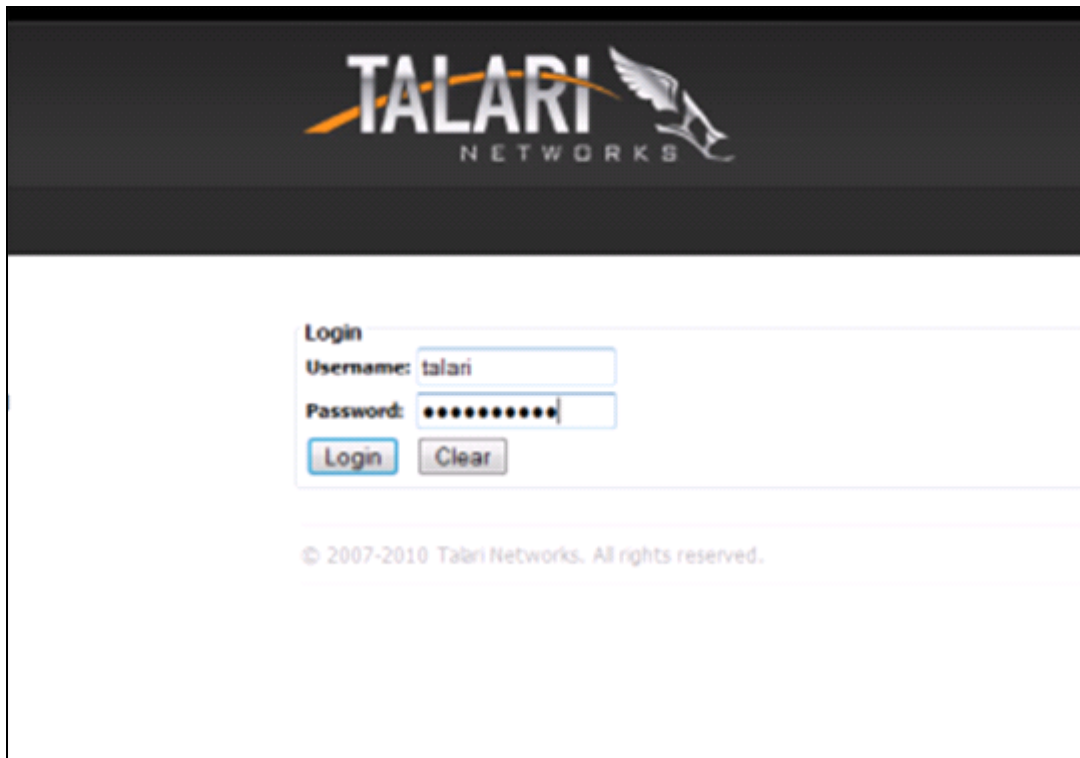
6.1. Connecting the Talari T730 to a PC

By default, the IP interface of the Talari T730 Aux mgt port (#5) is configured with 192.168.0.2/30.

Configure a PC with the following IP Address information:

- IP address – 192.168.0.1
- Subnet Mask - 255.255.255.252

Configure the Talari T730 using the built-in web-based APNA Web console. Access this tool by establishing a web browser connection to the Talari. Connect the LAN port of the computer being used to LAN port 5 on the Talari T730. Start the web browser and enter <https://192.168.0.2> to access the Talari APNA Web console. The **System Administrator Login** page is displayed. Log into the Talari T730 using default credentials which can be obtained from the Talari T730 documentation, refer to **Section 9**.

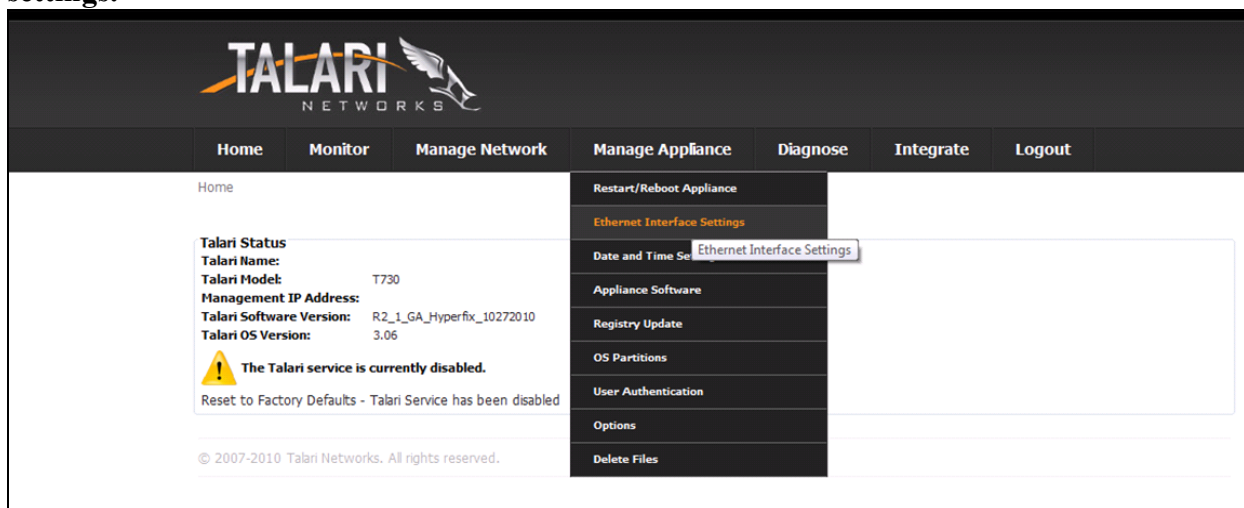


The screenshot shows the Talari Networks APNA Web console login page. At the top, there is a dark header with the Talari Networks logo, which includes the word "TALARI" in large white letters and "NETWORKS" in smaller white letters below it, with a stylized bird icon to the right. Below the header, the page has a white background. In the center, there is a "Login" section with a light blue border. It contains a "Username:" label with a text input field containing "talari", and a "Password:" label with a text input field containing ten dots. Below these fields are two buttons: a blue "Login" button and a grey "Clear" button. At the bottom of the page, there is a copyright notice: "© 2007-2010 Talari Networks. All rights reserved."

6.2. Configuring the IP Management interface of the T730

Perform this task to update the IP interface settings of an operational or newly installed Talari T730.

Step 1: From the Administration menu, select **Manage Appliance** → **Ethernet interface settings**.



Step 2: The **Manage Appliance** → **Ethernet interface settings** page is displayed. Update the **Management Interface** attributes for the **IP Address**, **Subnet Mask**, **Gateway IP Address** and **DNS** settings with the information shown in **Figure 1**. Select **Change Settings** to continue.

TALARI NETWORKS

Home Monitor Manage Network Manage Appliance Diagnose Integrate Logout

Manage Appliance -> Ethernet Interface Settings

Management Interface

IP Address: 10.32.100.80
 Subnet Mask: 255.255.255.0
 Gateway IP Address: 10.32.100.254
 Change Settings

DNS Settings

Primary DNS: 10.32.100.250
 Secondary DNS:
 Change Settings Clear Settings

Ethernet Interface Settings

Interface	Autonegotiate	Speed	Duplex
1:	<input checked="" type="checkbox"/>	Unknown	Unknown
2:	<input checked="" type="checkbox"/>	Unknown	Unknown
3:	<input checked="" type="checkbox"/>	Unknown	Unknown

Step 3: Enable the NCN (network control node) so the APN GUI editor can be used. From the Administration menu, select **Manage Appliance** → **Options**

TALARI NETWORKS

Home Monitor Manage Network Manage Appliance Diagnose Integrate Logout

Home

Talari Status


Talari Name:
 Talari Model: T730
 Management IP Address:
 Talari Software Version: R2_1_GA_P1_11102010
 Talari OS Version: 3.06

The Talari service is currently disabled.
 No configuration file has been applied to this appliance.
 You must update the configuration registry on this appliance.
 Update Registry

Manage Appliance Options:

- Restart/Reboot Appliance
- Ethernet Interface Settings
- Date and Time Settings
- Appliance Software
- Registry Update
- OS Partitions
- User Authentication
- Options**
- Delete File Options

The **Manage Appliance** → **Options** page is displayed. Select **Switch Console** to enable the APN Configuration Editor.



Home

Monitor

Manage Network

Manage Appliance

Diagnose

Integrate

Logout

Manage Appliance -> Options

LCD Mode

The Talari Service is currently disabled, the LCD mode cannot be retrieved unless the service is enabled.

Change Web Console Timeout

Timeout:

15

Enter the new timeout value in minutes (1-9999).

Change Timeout

Switch to NCN Console

Switch the mode of the Web Console to enable configuration of NCN functionality.

Switch Console

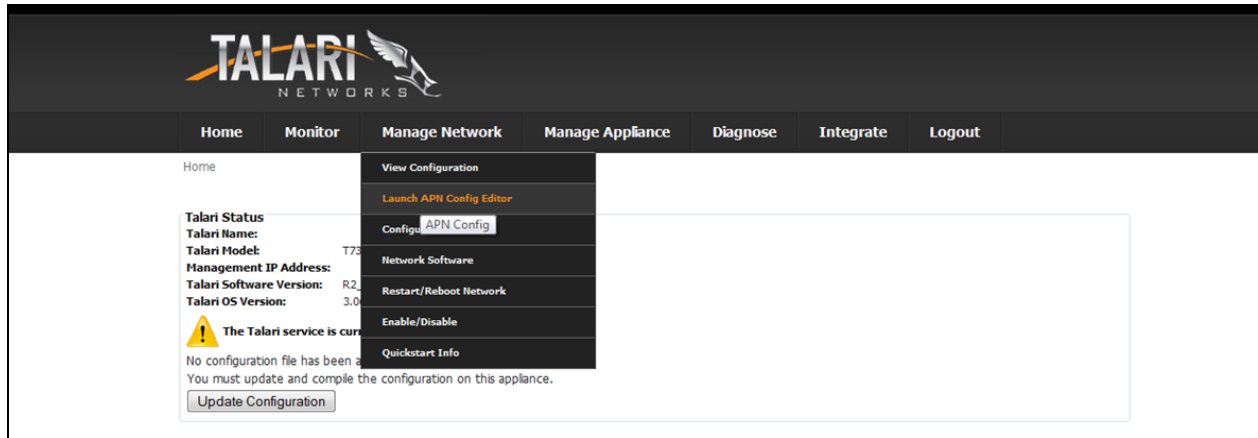
Revert to Factory Defaults

Clear out user data, logs, history, and local configuration data on this appliance, approximating the state as delivered by the factory.

Revert to Defaults

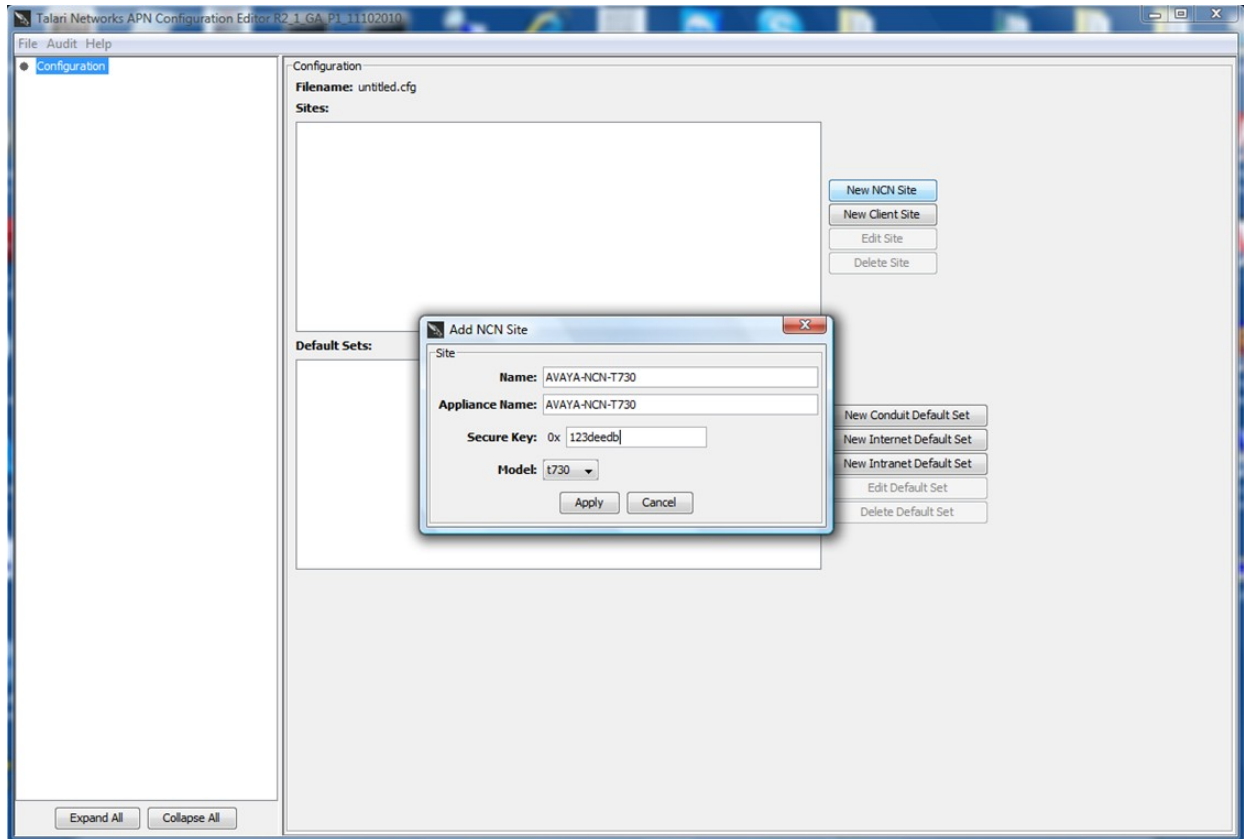
Step 4: Start the APN Configuration Editor. From the Administration menu, select **Manage Network** → **Launch APN Config Editor**.

Note: the **APN Config Editor** is a standalone JAVA app (java 6 recommended)



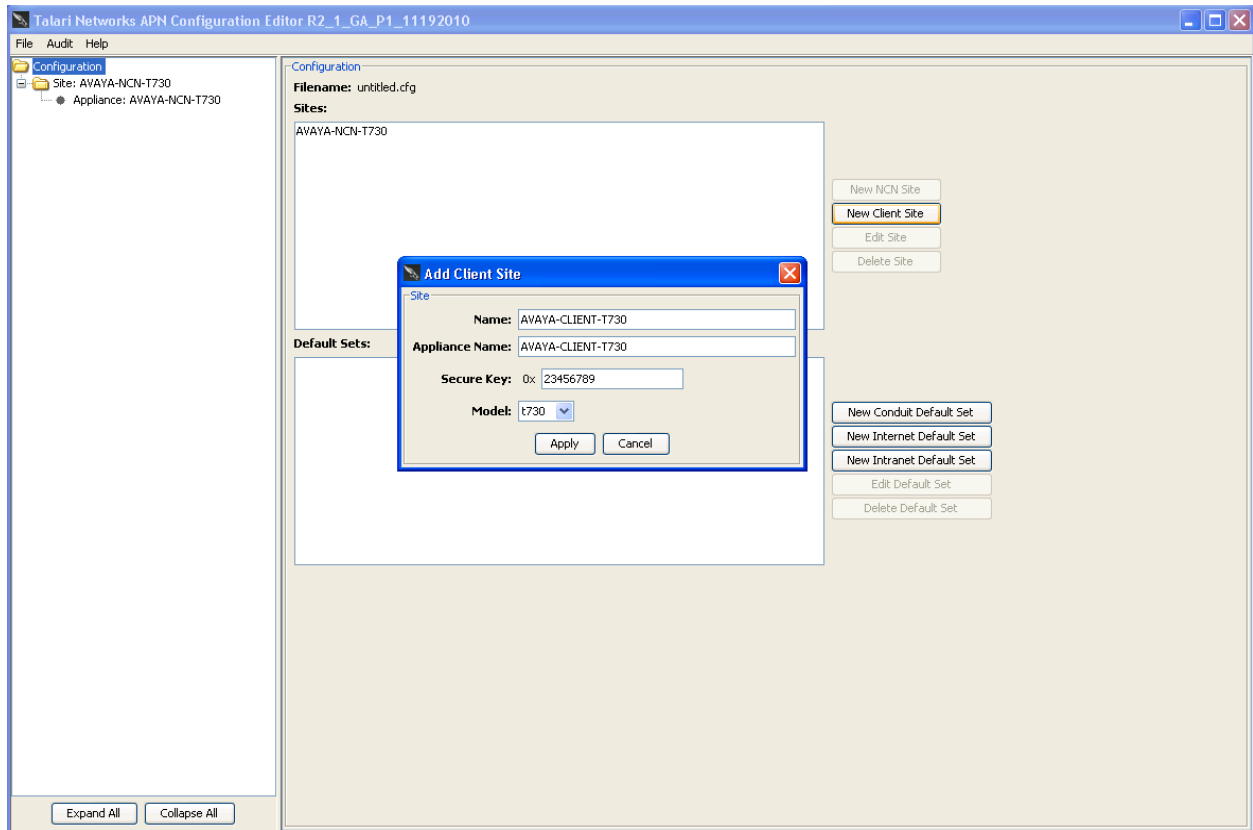
Step 5: Create NCN Site

Once the Talari APN Configuration Editor page is displayed, select **New NCN Site**. The **Add NCN Site** dialogue box is displayed. Enter a unique **Name**, **Appliance Name**, 8 digit hex **Secure Key**, Select the Talari **Model** being used. Select **Apply** to continue.



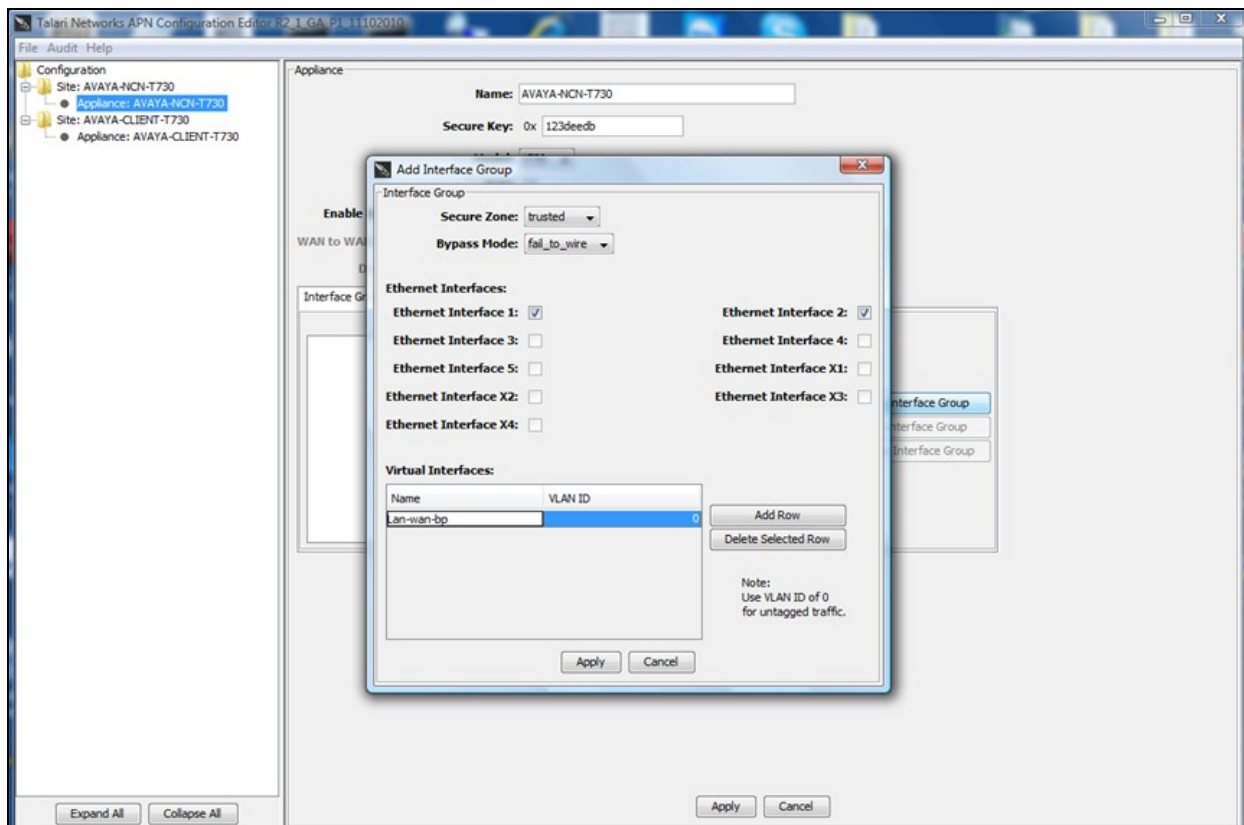
Step 6: Add Client Site

Select **New Client Site**. The **Add Client Site** dialogue box is displayed. Enter a unique **Name**, **Appliance Name**, 8 digit hex **Secure Key**, Select the Talari **Model** being used. Select **Apply** to continue.

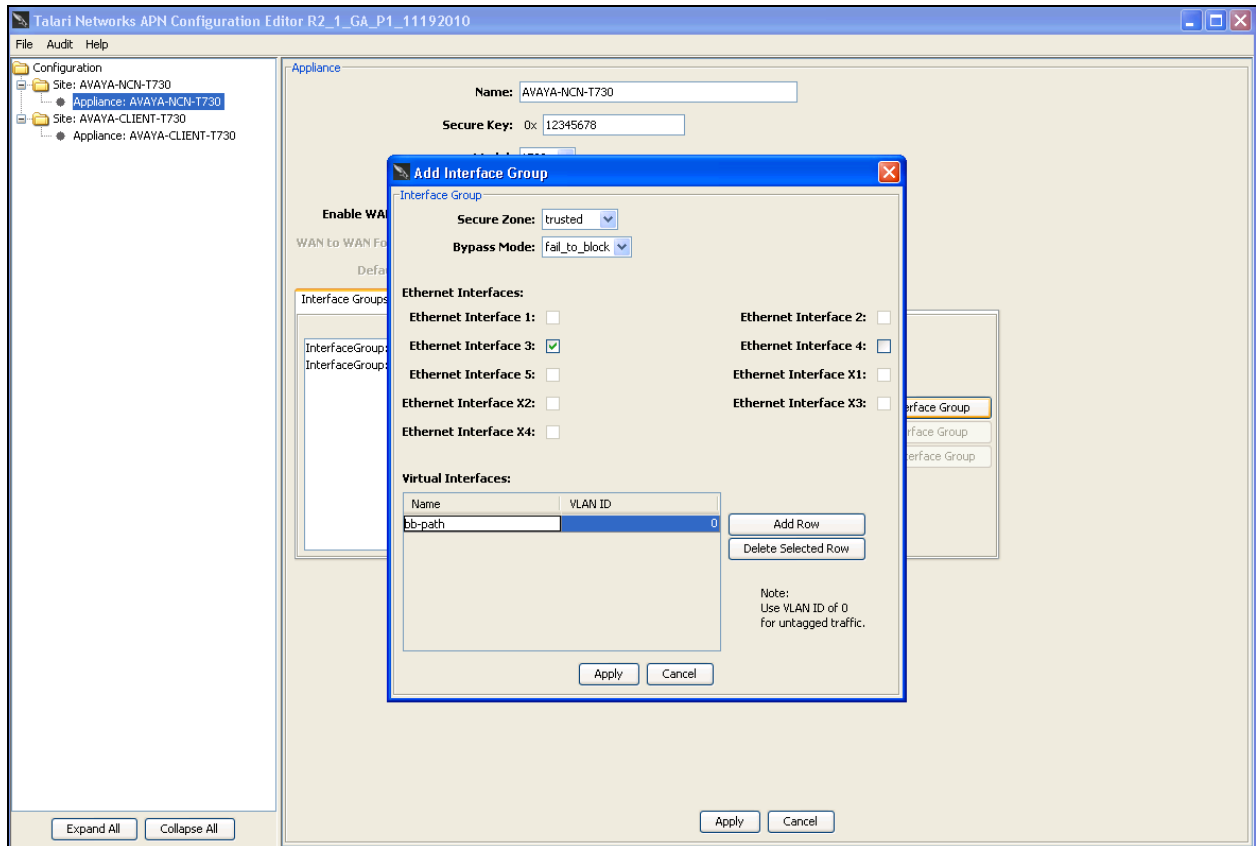


Step 7: Create fail-to-wire Path

From the **Configuration** menu, select the NCN site created in **Step 5**. Select **Appliance** → **Interface Groups** → **New Interface Group**. The **Add Interface Group** dialogue box is displayed, Select **trusted** from the **Secure Zone**: dropdown menu. Select **fail_to_wire** from the **Bypass Mode**: dropdown menu. Select the desired interfaces to be used, **Ethernet Interface 1:** and **Ethernet Interface 2:** were used for compliance testing. Select the **Add Row** button. Under **Name**, enter a unique **Name**. Select **Apply** to continue.

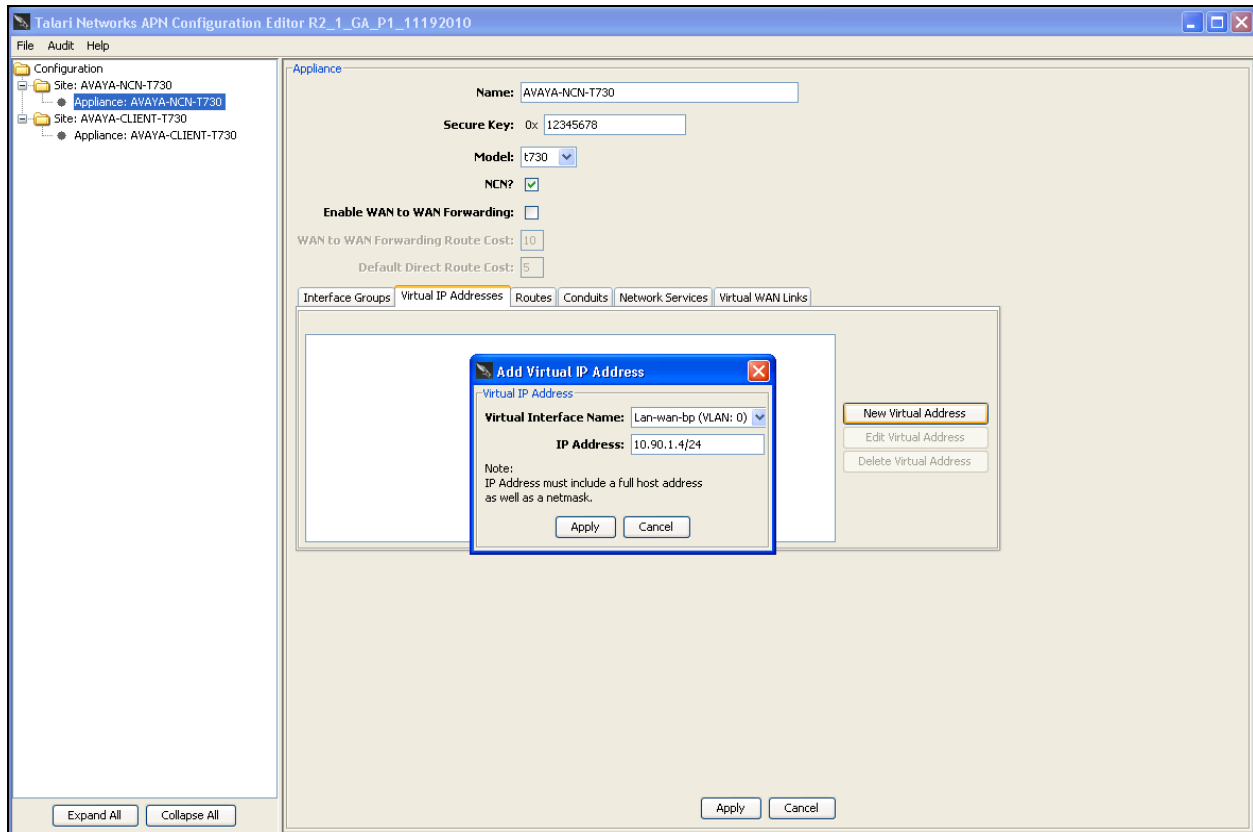


Step 8: Create fail-to-block Path (Secondary Interface Group for alternate path)
 Select **New Interface Group**. The **Add Interface Group** dialogue box is displayed. Select **trusted** from the **Secure Zone**: dropdown menu. Select **fail_to_block** from the **Bypass Mode**: dropdown menu. Select the desired interfaces to be used, **Ethernet Interface 1:** and **Ethernet Interface 2:** were used for compliance testing. Select the **Add Row** tab. Under Name, enter a unique **Name**. Select **Apply** to continue.



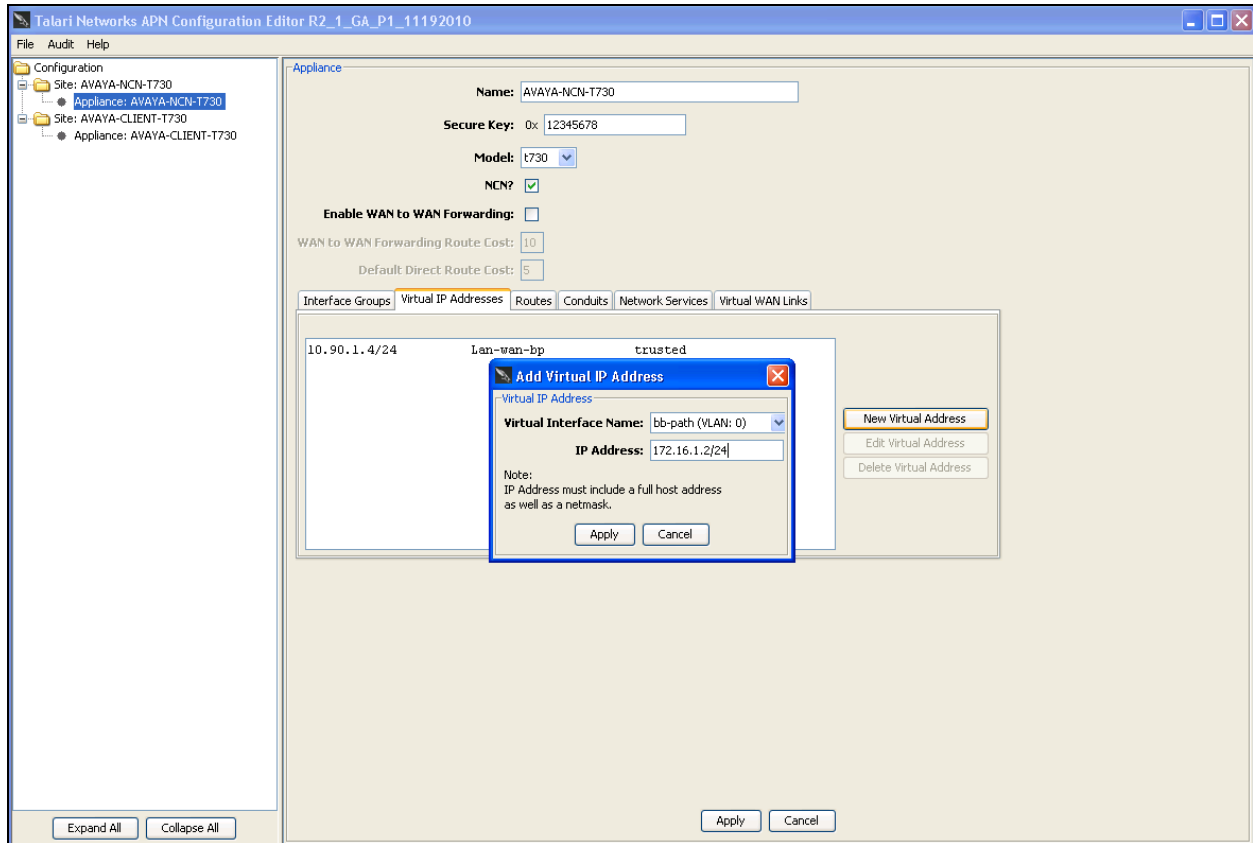
Step 9: Create a Virtual IP for the fail-to-wire Path

Select **Virtual IP Addresses** → **New Virtual Address**. The **Add Virtual IP Address** dialogue box is displayed. Select the name created in **Step 7** from the **Virtual Interface Name** dropdown menu. Enter the **IP Address**. Select **Apply** to continue.



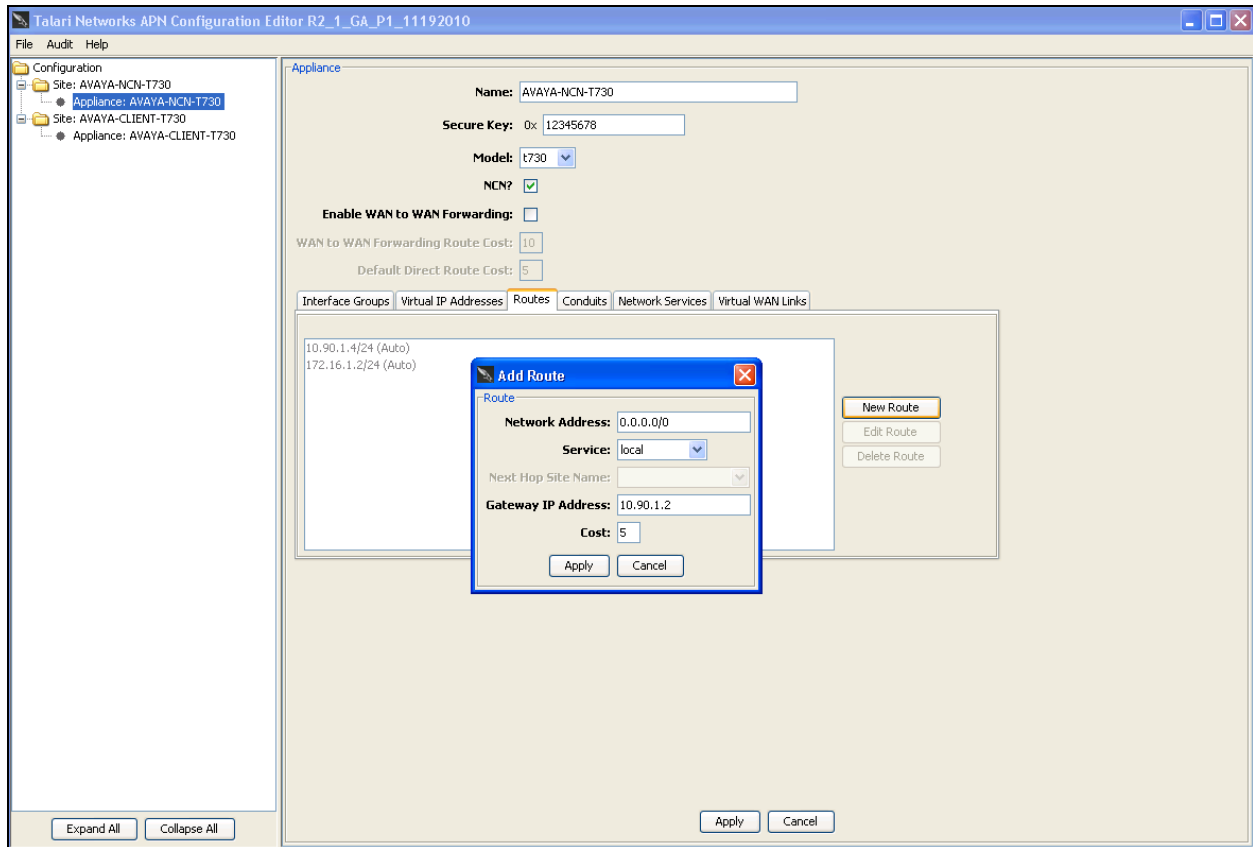
Step 10: Create a Virtual IP for the fail-to-block Path

Select **Virtual IP Addresses** → **New Virtual Address**. The **Add Virtual IP Address** dialogue box is displayed. Select the name created in **Step 8** from the **Virtual Interface Name** dropdown menu. Enter the **IP Address**. Select **Apply** to continue.



Step 11: Create default routes for local downstream subnet(s)

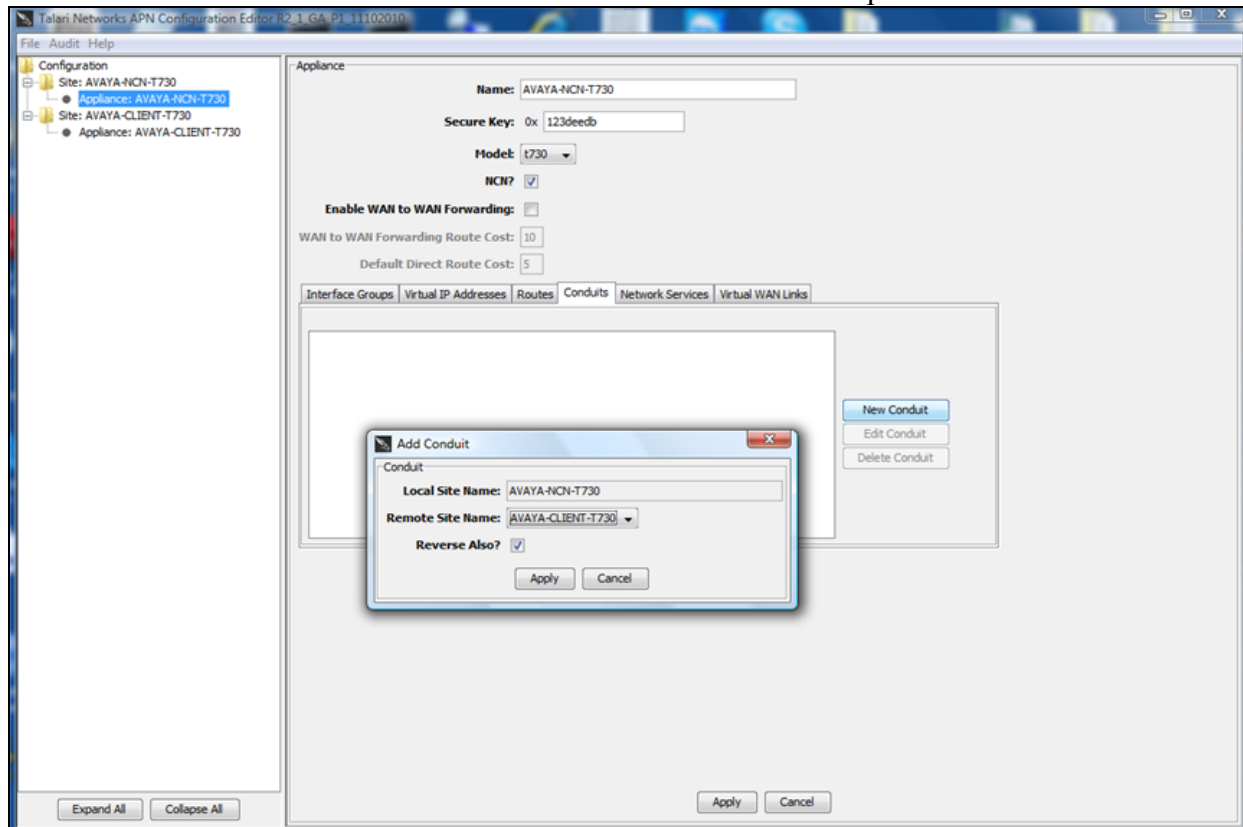
Select **Routes** → **New Route**. The **Add Route** dialogue box is displayed. Enter the **Network Address** 0.0.0.0/0, Select **local** from the **Service** dropdown menu. Enter the **Gateway IP Address**. Select **Apply** to continue.



Step 12: Create the Conduit Relationship between the two sites

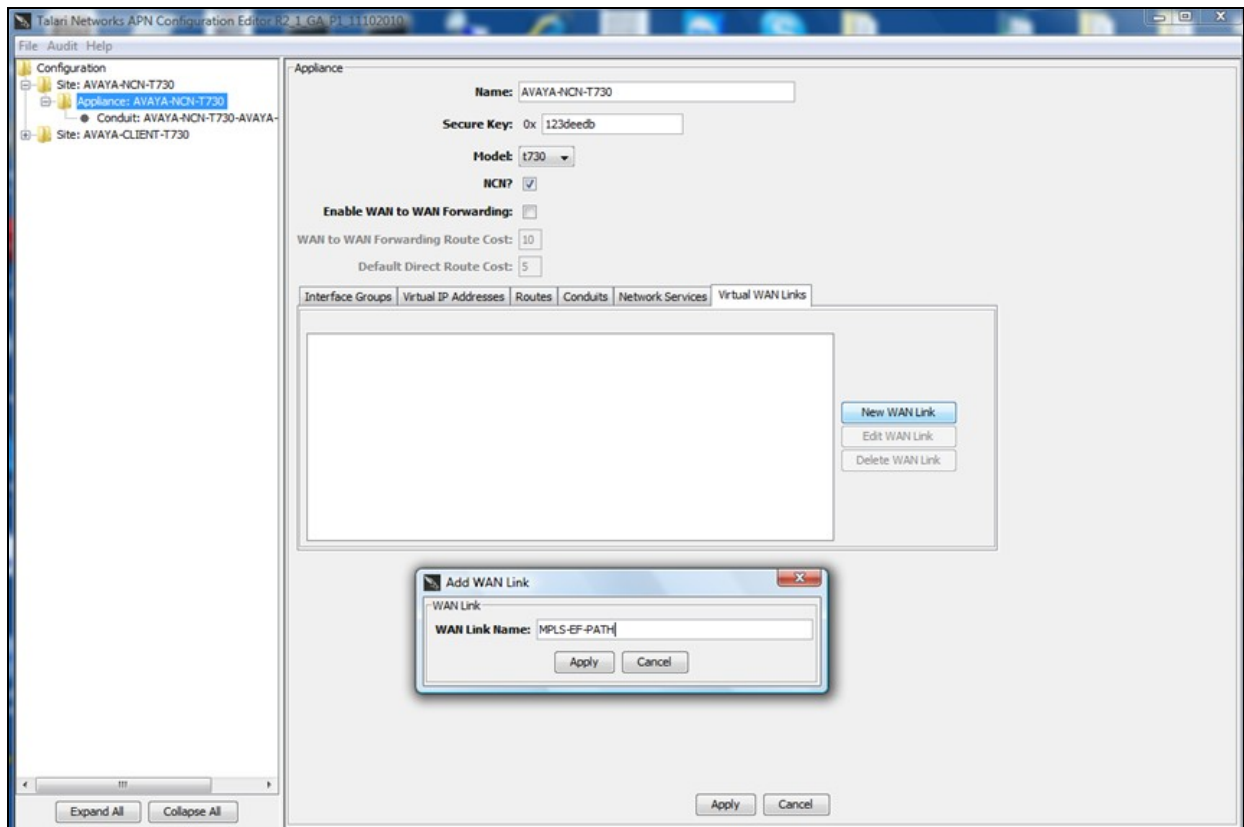
Select **Conduit** → **New Conduit**. The **Add Conduit** dialogue box is displayed. Select the remote site created in **Step 6** from the **Remote Site Name** dropdown menu. Check the **Reverse Also?** checkbox. Select **Apply** to continue.

Note: The Client Site must be created before the conduit relationship can be made between them.



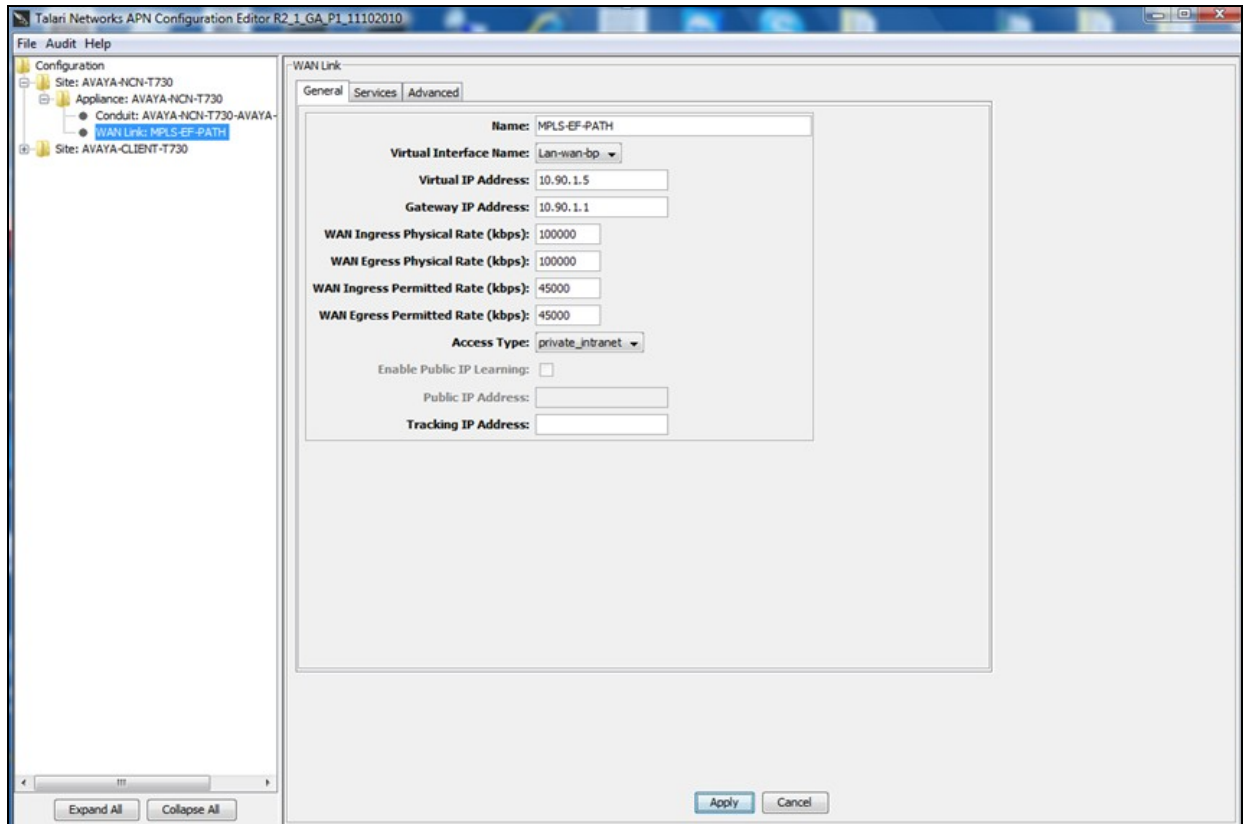
Step 13: Create the Virtual WAN links (Main Site)

Select **Virtual WAN links** → **New WAN links**. The **Add WAN links** dialogue box is displayed. Enter a unique **WAN Link Name**. Select **Apply** to continue.



From the left navigation tree, select the added WAN link, then select the **General** tab in the right WAN Link pane. Select the Virtual Interface created in **Step 7** from the **Virtual Interface Name** dropdown menu. Enter the **Virtual IP Address**, **Gateway IP Address** and the Physical Bandwidth (ingress and egress) information.

Note: If this is a private Wan link (i.e MPLS or point to point) the **Access Type** is set to **private_intranet**. If this is a public internet link set **Access Type** to **public_internet**. For Compliance testing this was set to **private_intranet**

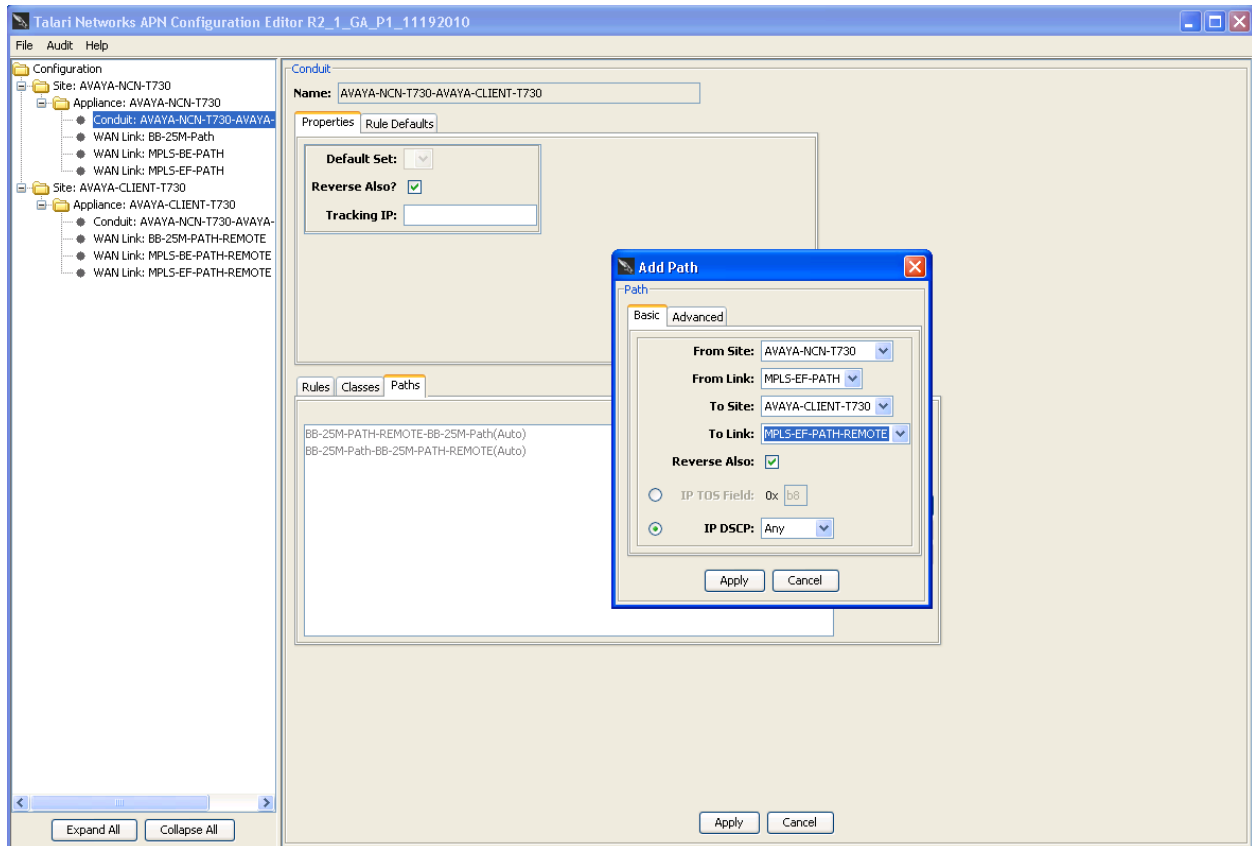


Step 14: Repeat **Step 13** to create the **MPLS-BE-PATH** and **BB-25M-PATH** with smaller throughput settings.

Step 15: Repeat **Steps 7** through **14** for the Client Site Talari 730.

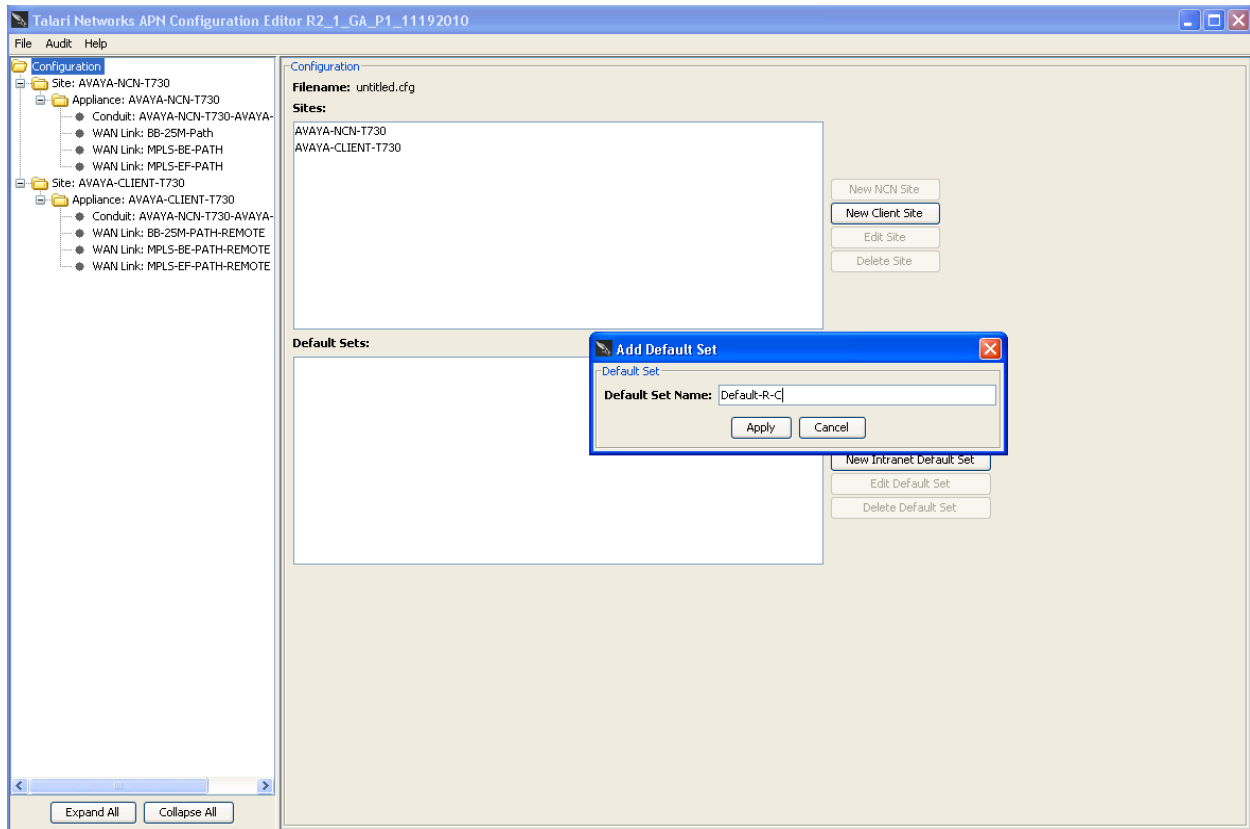
Step 16: Add the conduit paths to the conduit

From the **Configuration** menu, select the **NCN Appliance** site created in **Step 5**. Select the **Conduit** created in **Step 12**. Select the **Paths** tab, and then select the **New Path** button. The **Add Path** dialogue box is displayed. From the **From Site** dropdown menu, select the site created in **Step 5**. From the **From Link** dropdown menu, select the link created in **Step 13**. From the **To Site** dropdown menu, select the site created in **Step 6**. From the **To Link** dropdown menu, select the link to the client site created in **Step 15**:



Step 17: Create a Conduit Default Set

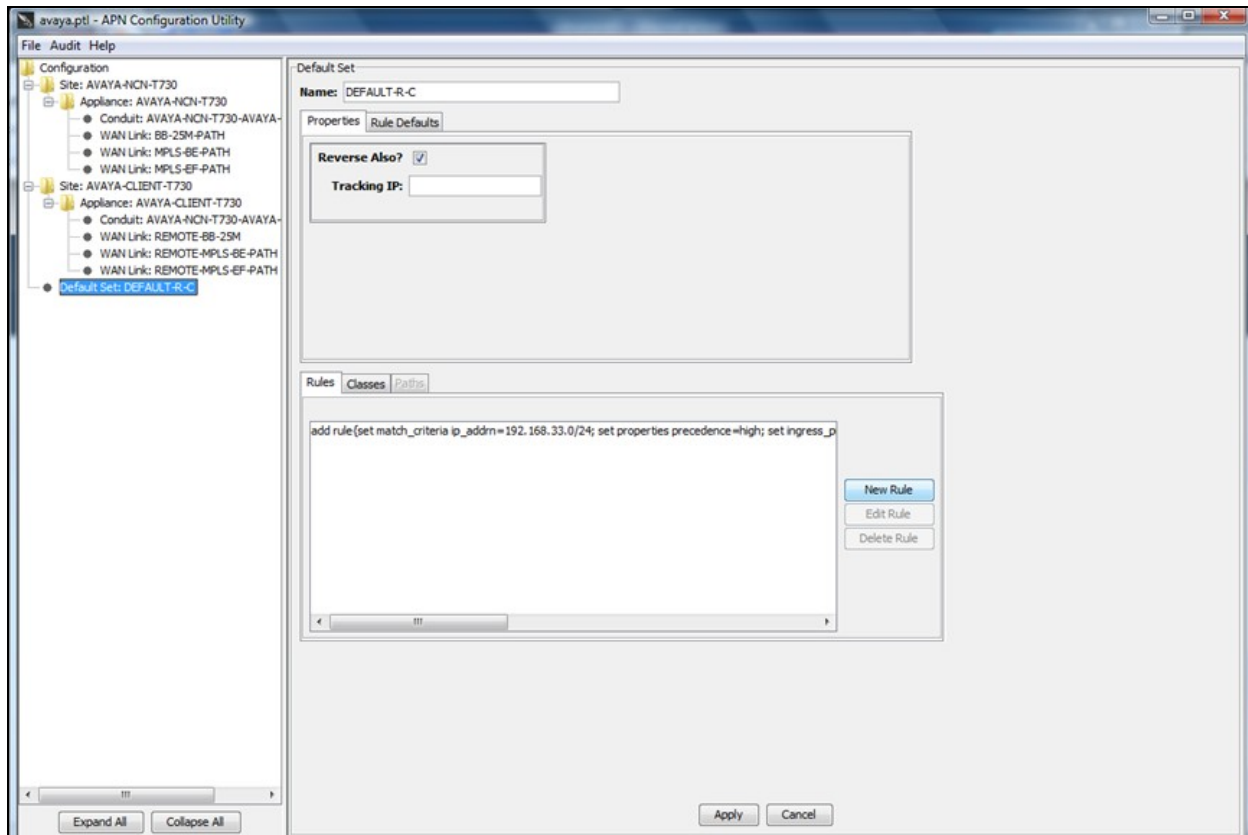
From **Configuration** → **New Conduit Default Set**. The **Default Set Name** dialogue box is displayed. Enter a unique **Default Set Name**. Select **Apply** to continue.



Step 18: Add Application Rules and Class configurations

The application rules govern how the Talari will prioritize and optimize each type of traffic flow. There is a match and a set condition. A basic rule is shown as an example. In real deployments, rules will vary per customer requirements. Please refer to the Talari Network deployment guide for more information or consult with Talari technical support.

Select the Default Set created in **Step 17** in the left navigation tree, then select **New Rule** in the right-side Default Set pane.



Step 19: Create a rule for the VOIP traffic.

The **Edit Rule** dialogue box is displayed. Under **Selection Criteria**, select the **Address** tab. Identify the SIP calls by the IP address subnet of the Phones. Under **Properties**, select the **WAN ingress** tab, select **realtime class 0** (not shown). Select the **WAN General** tab, select **duplicate_paths** from the **Transmit Mode:** dropdown menu. Assign an **Application Name** to the rule, for example, "SIP-Phones". Select **Apply** to continue

Note: Repeat as necessary for other applications

The screenshot shows the 'Edit Rule' dialog box with the following configuration:

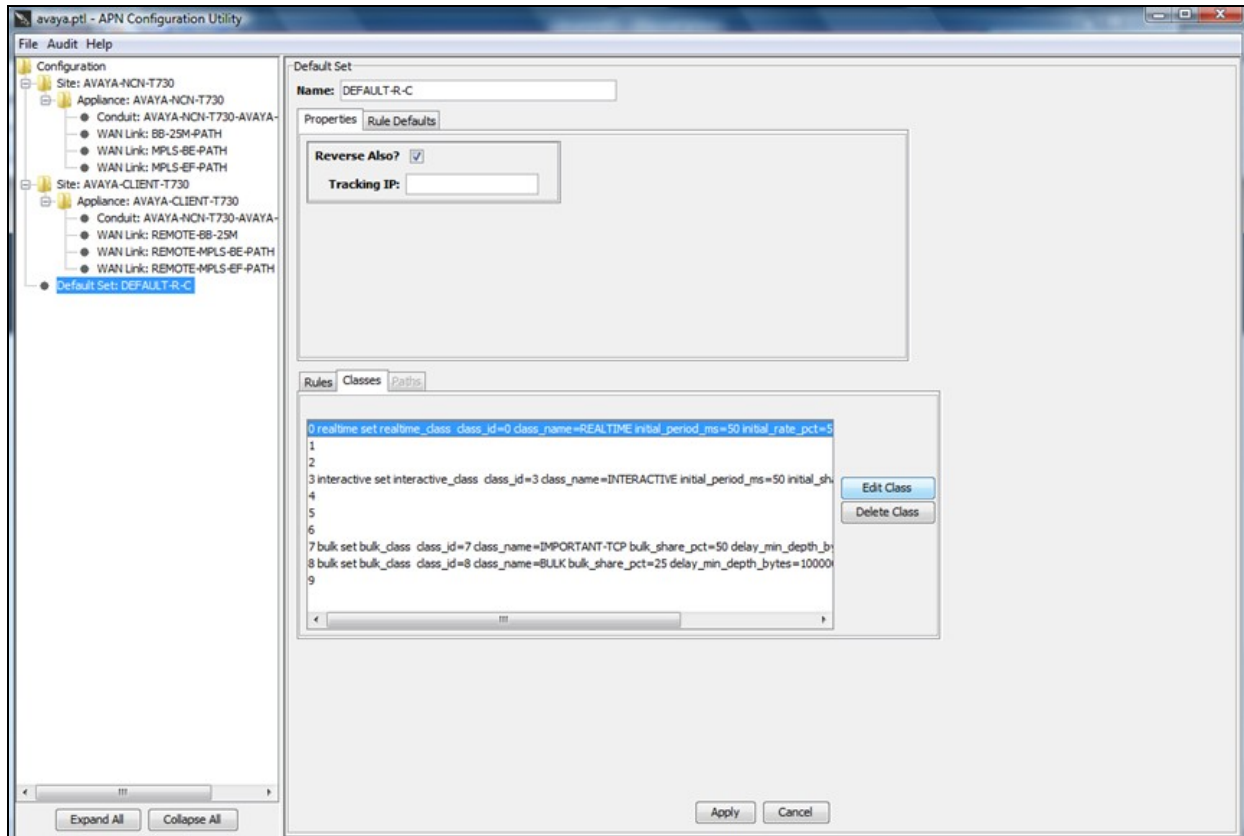
- Selection Criteria:**
 - General | **Address** | Protocol | DSCP/TOS
 - ☐ Don't Care
 - ☒ **IP Network Address:** 10.32.75.0/24
 - ☐ Source IP Network Address: [Empty]
 - ☐ Destination IP Network Address: [Empty]
- Properties:**
 - WAN Egress | Traffic Optimization | Deep Packet Inspection
 - WAN General | WAN Ingress
 - Transmit Mode:** duplicate_paths
 - Transmit Lost Packets?** ☐
 - Enable Override Service?** ☐
 - Override Service:** [Empty]
 - Application Name:** SIP-Phones

Buttons: Apply, Cancel

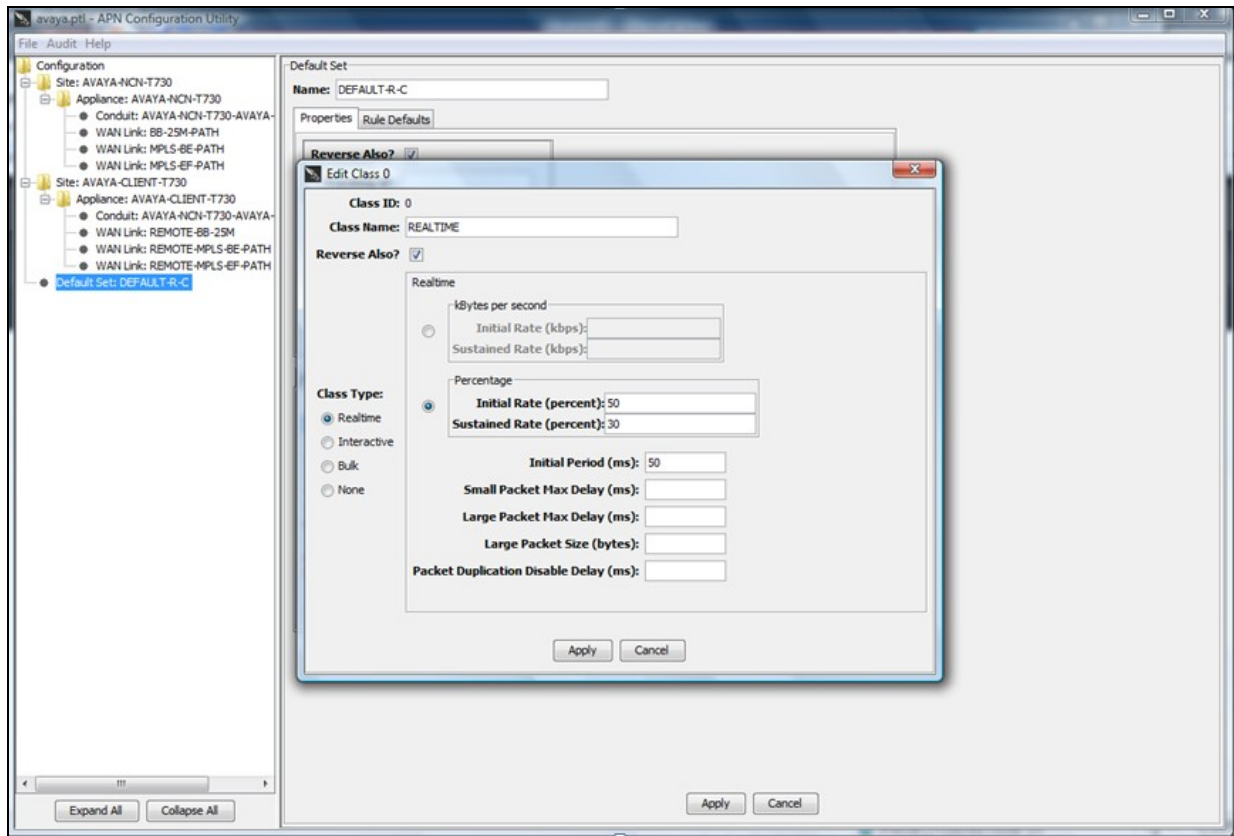
Step 20: Create QoS rule

The Talari QoS classes define how traffic is managed onto the WAN links. Each class can be defined as Real time, Interactive or Bulk, and the QoS parameters can be adjusted. Please refer to the Talari Network Deployment guide or consult with Talari Technical support for more information.

From **Configuration** → **Default Set:Default-R-C**, select the **Classes** tab. Select class **0** and select the **Edit Class** button.

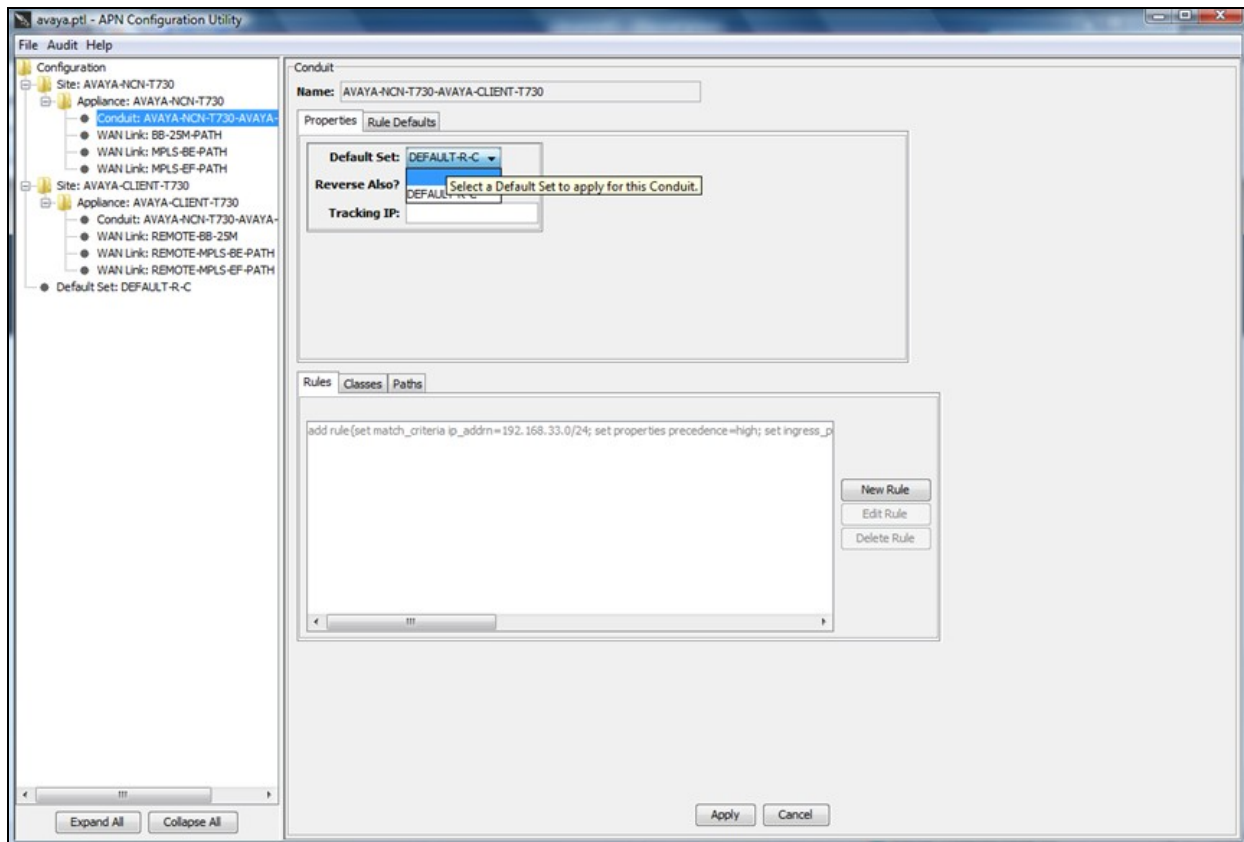


The **Edit Class 0** dialogue box is displayed. Enter **Class Name**, for example, “REAL TIME”. Select the **Reverse Also?** checkbox, select the **Realtime** radio button, select the radio button for **Percentage**. Enter the rates for **Initial Rate (percent):**, **Sustained Rate (percent):** and **Initial Period (ms):**. For compliance testing, **50** was used for **Initial Rate (percent):**, **30** for **Sustained Rate (percent):** and **50** for **Initial Period (ms):**. Select **Apply** to continue.



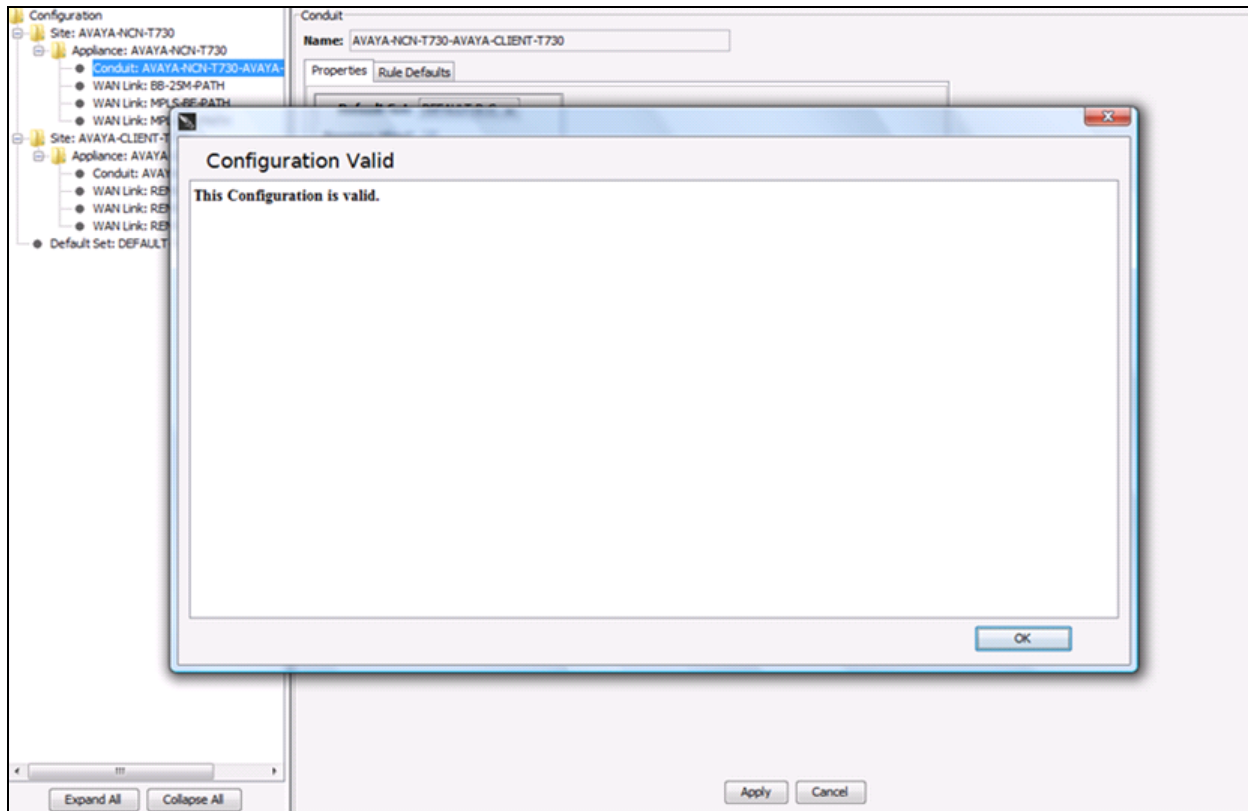
Step 21: Apply the conduit default set

From **Configuration** → **Appliance: Avaya-NCN...**, select the Conduit created in **Step 12** and edit the existing conduit (not shown). From the **Default Set** drop down menu under the **Properties** tab, select the conduit default set created in **Step 17**. and select **Apply**.



Step 22: Audit and Save Configuration

From the **APN** Menu, select **Audit** → **Audit Configuration** (not shown). Select OK to continue. Select **File** and save the configuration as <filename>.cfg.



Step 23: Compile the configuration file:

From the NCN management console, select **Manage Network** → **Configuration**. Select the **Browse** box under **Compile Configuration File**. The **Chose file** dialogue box is displayed. Select the file saved from **Step 22**, select **Open**, select **Compile**. Once the compile is complete, select the **Update** box to load the configuration to each node. If this is the first time loading the configuration to the remote client, go to **Step 25** to continue.

The screenshot shows the 'Manage Network -> Configuration' page. At the top is a navigation bar with links: Home, Monitor, Manage Network, Manage Appliance, Diagnose, Integrate, and Logout. Below the navigation bar, the page title is 'Manage Network -> Configuration'. The main content area is divided into three sections. The first section, 'Compile Configuration File', contains a 'Filename:' text box, a 'Browse...' button, and a 'Compile' button. The second section, 'Compilation Results', displays the output of the compilation process. It starts with 'Begin Compilation...', followed by two warning messages about bandwidth allocation on link 'CORP-INTERNET'. The warnings state that only 4000 kbps and 9000 kbps will be used, leaving 6000.0 kbps and 1000.0 kbps of unused bandwidth respectively. Below the warnings, it states 'This Configuration is valid, but please note the above warnings. (version 1296588787)'. The third section, 'Files created:', lists three files: 'alex-testbed-1-31-11.lst', 'CORP_1296588787.ncn', and 'REMOTE_1296588787.client'. The final section, 'Update NCN and All Clients', contains a 'Delay update for:' field with '0' hours and '0' minutes, and an 'Update' button.

Home Monitor Manage Network Manage Appliance Diagnose Integrate Logout

Manage Network -> Configuration

Compile Configuration File

Filename: Browse...

Compile

Compilation Results

Begin Compilation...

*Line: 156 -> WARNING: EC278: 10000.0 kbps WAN egress bandwidth on link 'CORP-INTERNET' is allocated to conduit 'CORP-REMOTE', but only 4000 Kbps will be used, leaving 6000.0 kbps of unused bandwidth

*Line: 156 -> WARNING: EC278: 10000.0 kbps WAN ingress bandwidth on link 'CORP-INTERNET' is allocated to conduit 'CORP-REMOTE', but only 9000 Kbps will be used, leaving 1000.0 kbps of unused bandwidth

This Configuration is valid, but please note the above warnings. (version 1296588787)

Files created:

alex-testbed-1-31-11.lst
CORP_1296588787.ncn
REMOTE_1296588787.client

Update NCN and All Clients

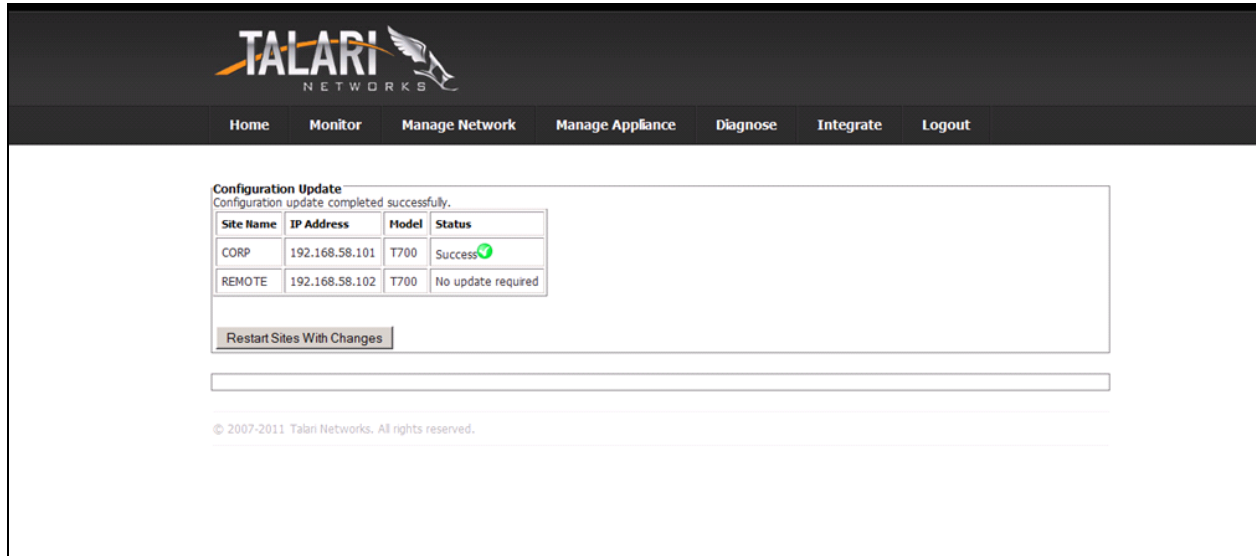
Delay update for: hours minutes

Update

Step 24: Configuration Update

The **Configuration Update** dialog page is displayed. Select **Restart Sites With Changes** to continue.

Note: this will reset the Talari.



The screenshot shows the Talari Networks web interface. At the top is a dark header with the Talari Networks logo and a navigation menu with links: Home, Monitor, Manage Network, Manage Appliance, Diagnose, Integrate, and Logout. Below the header, the main content area displays a 'Configuration Update' dialog. The dialog has a title bar and a message: 'Configuration update completed successfully.' Below this message is a table with four columns: Site Name, IP Address, Model, and Status. The table contains two rows: one for 'CORP' with IP '192.168.58.101', Model 'T700', and Status 'Success' (indicated by a green checkmark), and another for 'REMOTE' with IP '192.168.58.102', Model 'T700', and Status 'No update required'. Below the table is a button labeled 'Restart Sites With Changes'. At the bottom of the dialog is a copyright notice: '© 2007-2011 Talari Networks. All rights reserved.'

Site Name	IP Address	Model	Status
CORP	192.168.58.101	T700	Success ✓
REMOTE	192.168.58.102	T700	No update required

Restart Sites With Changes

© 2007-2011 Talari Networks. All rights reserved.

Step 25: If this is the first time loading the configuration to the remote client, it must be uploaded via the remote client management port:

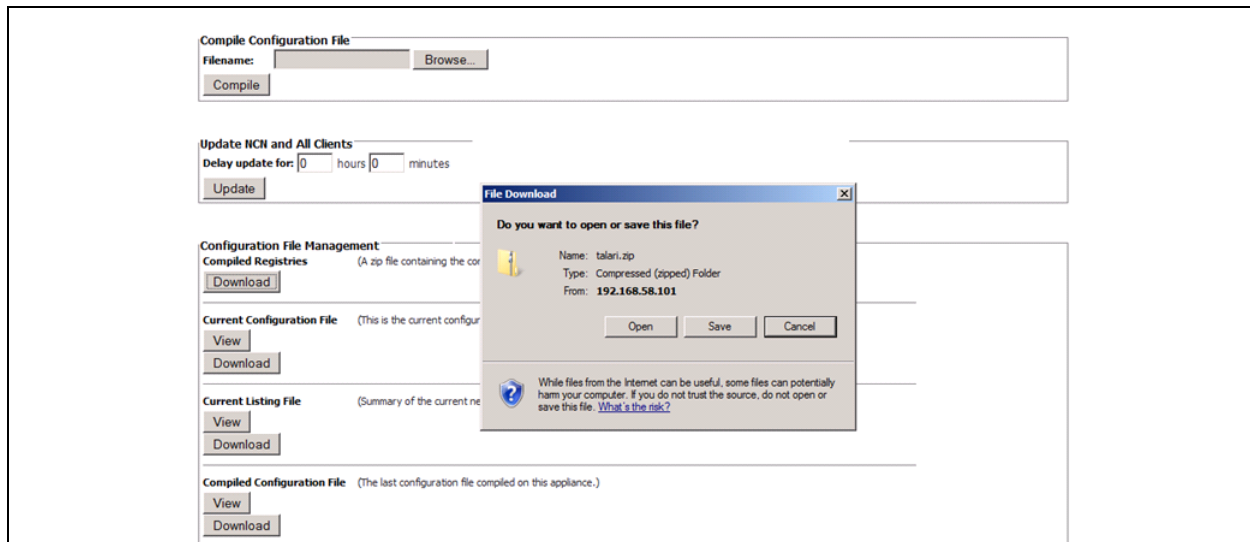
Connect a PC to the IP interface of the Client Talari T730 (configured with 192.168.0.2/30).

Configure a PC with the following IP Address information:

- IP address – 192.168.0.1
- Subnet Mask - 255.255.255.252

Start the web browser and enter https://192.168.0.2 to access the Talari APNA Web console. The **System Administrator Login** page is displayed. Log into the Talari T730.

From the NCN management console, select **Manage Network → Configuration → Configuration File Management**, select **Download**, and **Save** the talari.zip file.



At the remote Talari management console, select **Manage Appliance** → **Registry Update**, browse for the talari.zip file and upload. Once the update is complete, select the remote talari configuration and select **Update** (not shown). This will load the configuration file to the remote Talari for the first time.

The screenshot shows the Talari Networks management console interface. The top navigation bar includes links for Home, Monitor, Manage Network, Manage Appliance, Diagnose, Integrate, and Logout. The 'Manage Appliance' menu is open, displaying a list of options: Restart/Reboot Appliance, Ethernet Interface Settings, Date and Time Settings, Appliance Software, Registry Update (highlighted in orange), OS Partition Registry Update, User Authentication, Options, and Delete Files. The main content area is titled 'Manage Network -> Configuration' and contains three sections: 'Compile Configuration File' with a filename input and a 'Browse...' button, an 'Update NCH and All Clients' section with a delay update for 0 hours and 0 minutes, and a 'Configuration File Management' section with 'Compiled Registries' and 'Current Configuration File' subsections, each containing a 'Download' button.

7. Verification Steps

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

- Place calls between the corporate and remote site Avaya IP Telephones.
- Place calls between the Avaya 2410 Digital Telephone and Avaya IP Telephones at the remote site.
- Verify DHCP relay is functioning by confirming that the Avaya IP Telephones in the remote site received their IP addresses from the DHCP server connected to the corporate network.
- From the Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group connecting Communication Manager and Session Manager is in-service.
- From the Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group connecting Communication Manager and Session Manager is in-service.
- From System Manager web administration interface, verify that all remote endpoints are registered with Session Manager. To view user registration status, navigate to **Elements → Session Manager → System Status → User Registrations**.
- Verify that the Avaya IP endpoints have successfully registered with Avaya Communication Manager by the **list registered-ip-stations** command at the SAT.

8. Conclusion

These Application Notes describe the configuration necessary for integrating the Talari Networks Adaptive Private Networking Solution into an Avaya Aura® Telephony Infrastructure including Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya IP Telephones in a Multi-Site Converged VoIP and Data Network.

For the configuration described in these Application Notes, the Talari Networks Adaptive Private Networking Solution was responsible for network connectivity for the voice and data traffic between the Corporate and Remote Sites and enforcing load balancing, Layer2/Layer3 Quality of Service, and traffic shaping policies. Good voice quality was successfully achieved in the Avaya/Talari configuration described herein.

9. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6, June 2010.
- [2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.
- [3] *Administering Avaya Aura® Communication Manager*, May 2009, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, May 2009, Document Number 555-245-205.
- [5] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, November 2009, Document Number 16-300698.
- [6] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.0, Document Number 16-601944.
- [7] *Modular Messaging, Release 5.0 with the Avaya MSS Messaging Application Server (MAS) Administration Guide*, January 2009.
- [8] *Avaya Aura® Communication Manager Messaging Installation and Initial Configuration*.

The product documentation is provided by Talari. For additional product and company information, visit <http://www.talari.com/>

©2011 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.