QualNet 7.1
Multimedia and Enterprise Model Library

August 2013

SCALABLE
NETWORK TECHNOLOGIES

Copyright Information

© 2013 SCALABLE Network Technologies, Inc. All rights reserved.

QualNet and EXata are registered trademarks of SCALABLE Network Technologies, Inc.

All other trademarks and trade names used are property of their respective companies.

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

Chapter 3   Network Protocol Models 44

Chapter 4   Unicast Routing Protocol Models 48

1 Overview of Model Library

1.1 List of Models in the Library

The models described in the Multimedia and Enterprise Model Library are listed in Table 1-1.

TABLE 1-1.   Multimedia and Enterprise Library Models

Model Name	Model Type	Section Number
Border Gateway Protocol version 4 (BGPv4)	Routing Protocol	Section 4.1
Detailed Switch Model	MAC Layer	Section 2.1
Differentiated Services (DiffServ)	QoS Model	Section 7.1
Distance Vector Multicast Routing Protocol (DVMRP)	Routing Protocol	Section 5.1
Enhanced Interior Gateway Routing Protocol (EIGRP)	Routing Protocol	Section 4.2
H323 and H225 Protocols	Multimedia Application	Section 8.1
Hot Standby Router Protocol (HSRP)	Router Configuration	Section 6.1
Interior Gateway Routing Protocol (IGRP)	Routing Protocol	Section 4.3
Mobile IPv4	Network Layer	Section 3.1
Multicast Extensions to OSPF (MOSPF)	Routing Protocol	Section 5.2
Multi-Protocol Label Switching (MPLS)	QoS Model	Section 7.2
Open Shortest Path First version 2 (OSPFv2) Routing Protocol	Routing Protocol	Section 4.4
Open Shortest Path First version 3 (OSPFv3) Routing Protocol	Routing Protocol	Section 4.5
Policy-Based Routing (PBR)	Router Configuration	Section 6.2
Protocol Independent Multicast Protocol: Dense Mode (PIM-DM) and Sparse Mode (PIM-SM)	Routing Protocol	Section 5.3
Quality of Service Extensions to OSPF (QOSPF)	QoS Model	Section 7.3
Real-time Transport Protocol (RTP)	Multimedia Application	Section 8.2
Route Maps	Router Configuration	Section 6.3
Route Redistribution	Router Configuration	Section 6.4
Router Access Lists	Router Configuration	Section 6.5

TABLE 1-1.   Multimedia and Enterprise Library Models (Continued)

Model Name	Model Type	Section Number
Router Model	Router Configuration	Section 6.6
Session Initiation Protocol (SIP)	Multimedia Application	Section 8.3
Switched Ethernet	MAC Layer	Section 2.2
Virtual LAN (VLAN)	MAC Layer	Section 2.3
Voice over Internet Protocol (VoIP)	Multimedia Application	Section 8.4

1.2 Conventions Used

1.2.1 Format for Command Line Configuration

This section describes the general format for specifying parameters in input files, the precedence rules for parameters, and the conventions used in the description of command line configuration for each model.

1.2.1.1 General Format of Parameter Declaration

The general format for specifying a parameter in an input file is:

```
[<Qualifier>] <Parameter Name> [<Index>] <Parameter Value>
```
where

<Qualifier>   The qualifier is optional and defines the scope of the parameter declaration. The scope can be one of the following: Global, Node, Subnet, and Interface. Multiple instances of a parameter with different qualifiers can be included in an input file. Precedence rules (see Section 1.2.1.2) determine the parameter value for a node or interface.

Global: The parameter declaration is applicable to the entire scenario (to all nodes and interfaces), subject to precedence rules. The scope of a parameter declaration is global if the qualifier is not included in the declaration.

Example:

```
MAC-PROTOCOL            MACDOT11
```

Node: The parameter declaration is applicable to specified nodes, subject to precedence rules. The qualifier for a node-level declaration is a list of space-separated node IDs or a range of node IDs (specified by using the keyword `thru`) enclosed in square brackets.

Example:

```
[5 thru 10] MAC-PROTOCOL           MACDOT11
```

Subnet: The parameter declaration is applicable to all interfaces in specified subnets, subject to precedence rules. The qualifier for a subnet-level declaration is a space-separated list of subnet addresses enclosed in square brackets. A subnet address can be specified in the IP dot notation or in the QualNet N syntax.

Example:

```
[N8-1.0 N2-1.0] MAC-PROTOCOL        MACDOT11
```

Interface: The parameter declaration is applicable to specified interfaces. The qualifier for an interface-level declaration is a space-separated list of subnet addresses enclosed in square brackets.

Example:

```
[192.168.2.1 192.168.2.4] MAC-PROTOCOL MACDOT11
```

`<Parameter Name>`	Name of the parameter.
`<Index>`	Instance of the parameter to which this parameter declaration is applicable, enclosed in square brackets. This should be in the range 0 to *n* -1, where *n* is the number of instances of the parameter.
	The instance specification is optional in a parameter declaration. If an instance is not included, then the parameter declaration is applicable to all instances of the parameter, unless otherwise specified.
`<Parameter Value>`	Value of the parameter.

Note: There should not be any spaces between the parameter name and the index.

Examples of parameter declarations in input files are:

```
PHY-MODEL                                    PHY802.11b
[1] PHY-MODEL                                PHY802.11a
[N8-1.0] PHY-RX-MODEL                        BER-BASED
[8 thru 10] ROUTING-PROTOCOL                 RIP
[192.168.2.1 192.168.2.4] MAC-PROTOCOL       GENERICMAC
NODE-POSITION-FILE                           ./default.nodes
PROPAGATION-CHANNEL-FREQUENCY[0]             2.4e9
[1 2] QUEUE-WEIGHT[1]                        0.3
```

Note   In the rest of this document, we will not use the qualifier or the index in a parameter's description. Users should use a qualifier and/or index to restrict the scope of a parameter, as appropriate.

1.2.1.2 Precedence Rules

Parameters without Instances

If the parameter declarations do not include instances, then the following rules of precedence apply when determining the parameter values for specific nodes and interfaces:

Interface > Subnet > Node > Global

This can be interpreted as follows:

* The value specified for an interface takes precedence over the value specified for a subnet, if any.
* The value specified for a subnet takes precedence over the value specified for a node, if any.
* The value specified for a node takes precedence over the value specified for the scenario (global value), if any.

Parameters with Instances

If the parameter declarations are a combination of declarations with and without instances, then the following precedence rules apply (unless otherwise stated):

Interface[i] > Subnet[i] > Node[i] > Global[i] > Interface > Subnet > Node > Global

This can be interpreted as follows:

* Values specified for a specific instance (at the interface, subnet, node, or global level) take precedence over values specified without the instance.

- For values specified for the same instance at different levels, the following precedence rules apply:
  - The value specified for an interface takes precedence over the value specified for a subnet, if any, if both declarations are for the same instance.
  - The value specified for a subnet takes precedence over the value specified for a node, if any, if both declarations are for the same instance.
  - The value specified for a node takes precedence over the value specified for the scenario (global value), if any, if both declarations are for the same instance.

1.2.1.3 Parameter Description Format

In the Model Library, most parameters are described using a tabular format described below. The parameter description tables have three columns labeled "Parameter", "Values", and "Description". Table 1-2 shows the format of parameter tables. Table 1-4 shows examples of parameter descriptions in this format.

TABLE 1-2.   Parameter Table Format

Parameter	Values	Description
<Parameter Name>	*<Type>*	*<Description>*
<Designation>	[<Range>]	
<Scope>	[<Default Value>]	
[<Instances>]	[<Unit>]	

Parameter Column

The first column contains the following entries:

- ***<Parameter Name>*:** The first entry is the parameter name (this is the exact name of the parameter to be used in the input files).

- ***<Designation>:*** This entry can be *Optional* or *Required*. These terms are explained below.
  - ***Optional***: This indicates that the parameter is optional and may be omitted from the configuration file. (If applicable, the default value for this parameter is included in the second column.)
  - ***Required***: This indicates that the parameter is mandatory and must be included in the configuration file.

- ***<Scope>:*** This entry specifies the possible scope of the parameter, i.e., if the parameter can be specified at the global, node, subnet, or interface levels. Any combination of these levels is possible.If the parameter can be specified at all four levels, the keyword "All" is used to indicate that.

    Examples of scope specification are:
    Scope: All
    Scope: Subnet, Interface
    Scope: Global, Node

- ***<Instances>:*** If the parameter can have multiple instances, this entry indicates the type of index. If the parameter can not have multiple instances, then this entry is omitted.

Examples of instance specification are:

> *Instances*: channel number
>
> *Instances*: interface index
>
> *Instances*: queue index

Values Column

The second column contains the following information:

- *<Type>*: The first entry is the parameter type and can be one of the following: Integer, Real, String, Time, Filename, IP Address, Coordinates, Node-list, or List. If the type is a List, then all possible values in the list are enumerated below the word "List". (In some cases, the values are listed in a separate table and a reference to that table is included in place of the enumeration.)

  Table 1-3 shows the values a parameter can take for each type.

TABLE 1-3.   Parameter Types

Type	Description
Integer	Integer value Examples: `2`, `10`
Real	Real value Examples: `15.0`, `-23.5`, `2.0e9`
String	String value Examples: `TEST`, `SWITCH1`
Time	Time value expressed in QualNet time syntax (refer to *QualNet User's Guide*) Examples: `1.5S`, `200MS`, `10US`

Filename	Name of a file in QualNet filename syntax (refer to *QualNet User's Guide*)
	Examples:
	`../../data/terrain/los-angeles-w`
	(For Windows and UNIX)
	`C:\scalable\qualnet\7.1\scenarios\WF\WF.nodes`
	(For Windows)
	`/root/scalable/qualnet/7.1/scenarios/WF/WF.nodes`
	(For UNIX)

Path	Path to a directory in QualNet path syntax (refer to *QualNet User's Guide*)
	Examples:
	`../../data/terrain` (For Windows and UNIX)
	`C:\scalable\qualnet\7.1\scenarios\default`
	(For Windows)
	`/root/scalable/qualnet/7.1/scenarios/default`
	(For UNIX)

IP Address	IPv4 or IPv6 address Examples: `192.168.2.1`, `2000:0:0:0::1`

TABLE 1-3.   Parameter Types (Continued)

Type	Description
IPv4 Address	IPv4 address Examples: `192.168.2.1`
IPv6 Address	IPv6 address Examples: `2000:0:0:0::1`
Coordinates	Coordinates in Cartesian or Lat-Lon-Alt system. The altitude is optional. Examples: `(100, 200, 2.5)`, `(-25.3478, 25.28976)`
Node-list	List of node IDs separated by commas and enclosed in "{" and "}". Examples: `{2, 5, 10}`, `{1, 3 thru 6}`
List	One of the enumerated values. Example: See the parameter `MOBILITY` in Table 1-4.

Note: If the parameter type is List, then options for the parameter available in QualNet Developer and the commonly used model libraries are enumerated. Additional options for the parameter may be available if some other model libraries or addons are installed. These additional options are not listed in this document but are described in the corresponding model library or addon documentation.

- ***<Range>*:** This is an optional entry and is used if the range of values that a parameter can take is restricted. The permissible range is listed after the label "*Range:*" The range can be specified by giving the minimum value, the maximum value, or both. If the range of values is not restricted, then this entry is omitted.

  If both the minimum and maximum values are specified, then the following convention is used to indicate whether the minimum and maximum values are included in the range:

`(min, max)`	`min` < parameter value < `max`
`[min, max)`	`min` ≤ parameter value < `max`
`(min, max]`	`min` < parameter value ≤ `max`
`[min, max]`	`min` ≤ parameter value ≤ `max`

`min` (or `max`) can be a parameter name, in which case it denotes the value of that parameter.

Examples of range specification are:

Range: ≥ `0`
Range: `(0.0, 1.0]`
Range: `[1, MAX-COUNT]`
Range: `[1S, 200S]`

Note: If an upper limit is not specified in the range, then the maximum value that the parameter can take is the largest value of the type (integer, real, time) that can be stored in the system.

- ***<Default>:*** This is an optional entry which specifies the default value of an optional or conditional-optional parameter. The default value is listed after the label "*Default:*"

- ***<Unit>:*** This is an optional entry which specifies the unit for the parameter, if applicable. The unit is listed after the label "*Unit:*". Examples of units are: meters, dBm, slots.

Description Column

The third column contains a description of the parameter. The significance of different parameter values is explained here, where applicable. In some cases, references to notes, other tables, sections in the User's Guide, or to other model libraries may be included here.

Table 1-4 shows examples of parameter descriptions using the format described above.

TABLE 1-4.   Example Parameter Table

Parameter	Values	Description
MOBILITY Optional *Scope:* Global, Node	List: • NONE • FILE • GROUP-MOBILITY • RANDOM-WAYPOINT Default: NONE	Mobility model used for the node. If MOBILITY is set to NONE, then the nodes remain fixed in one place for the duration of the simulation. See Table 7-11 for a description of mobility models.
BACKOFF-LIMIT Required *Scope:* Subnet, Interface	Integer *Range:* [4,10] *Unit:* slots	Upper limit of backoff interval after collision. A backoff interval is randomly chosen between 1 and this number following a collision.
IP-QUEUE-PRIORITY-QUEUE-SIZE Required *Scope:* All *Instances:* queue index	Integer *Range:* [1, 65535] *Unit:* bytes	Size of the output priority queue.
MAC-DOT11-DIRECTIONAL-ANTENNA-MODE Optional *Scope:* All	List • YES • NO *Default:* NO	Indicates whether the radio is to use a directional antenna for transmission and reception.

1.2.2 Format for GUI Configuration

The GUI configuration section for a model outlines the steps to configure the model using the GUI. The following conventions are used in the GUI configuration sections:

Path to a Parameter Group

As a shorthand, the location of a parameter group in a properties editor is represented as a path consisting of the name of the properties editor, name of the tab within the properties editor, name of the parameter group within the tab (if applicable), name of the parameter sub-group (if applicable), and so on.

Example

The following statement:

Go to **Default Device Properties Editor > Interfaces > Interface # > MAC Layer**

is equivalent to the following sequence of steps:

1. Open the Default Device Properties Editor for the node.

2. Click the **Interfaces** tab.

3. Expand the applicable Interface group.

4. Click the **MAC Layer** parameter group.

The above path is shown in Figure 1-1.
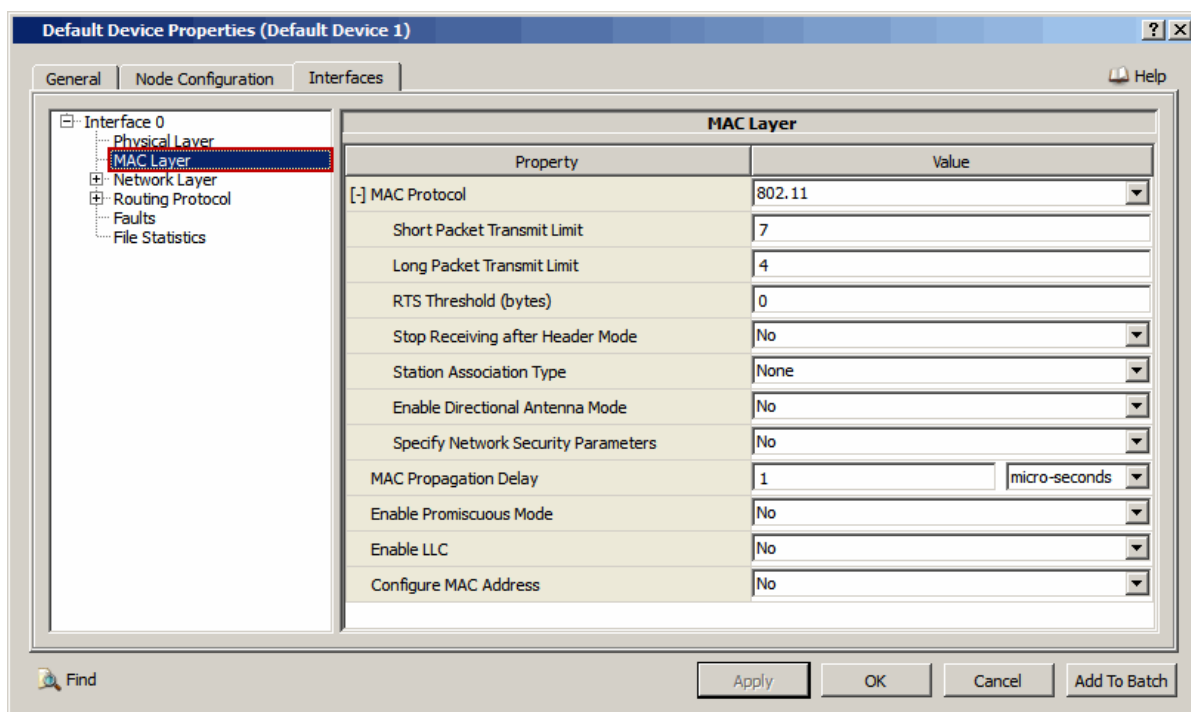
FIGURE 1-1.   Path to a Parameter Group

Path to a Specific Parameter

As a shorthand, the location of a specific parameter within a parameter group is represented as a path consisting of all ancestor parameters and their corresponding values starting from the top-level parameter. The value of an ancestor parameter is enclosed in square brackets after the parameter name.

Example

The following statement:

Set **MAC Protocol** *[= 802.11]* **> Station Association Type** *[= Dynamic]* **> Set Access Point** *[= Yes]* **>** *Enable Power Save Mode* to *Yes*

is equivalent to the following sequence of steps:

1. Set **MAC Protocol** to *802.11*.

2. Set **Station Association Type** to *Dynamic.*

3. Set **Set Access Point** to *Yes.*

4. Set **Enable Power Save Mode** to *Yes.*

The above path is shown in Figure 1-2.
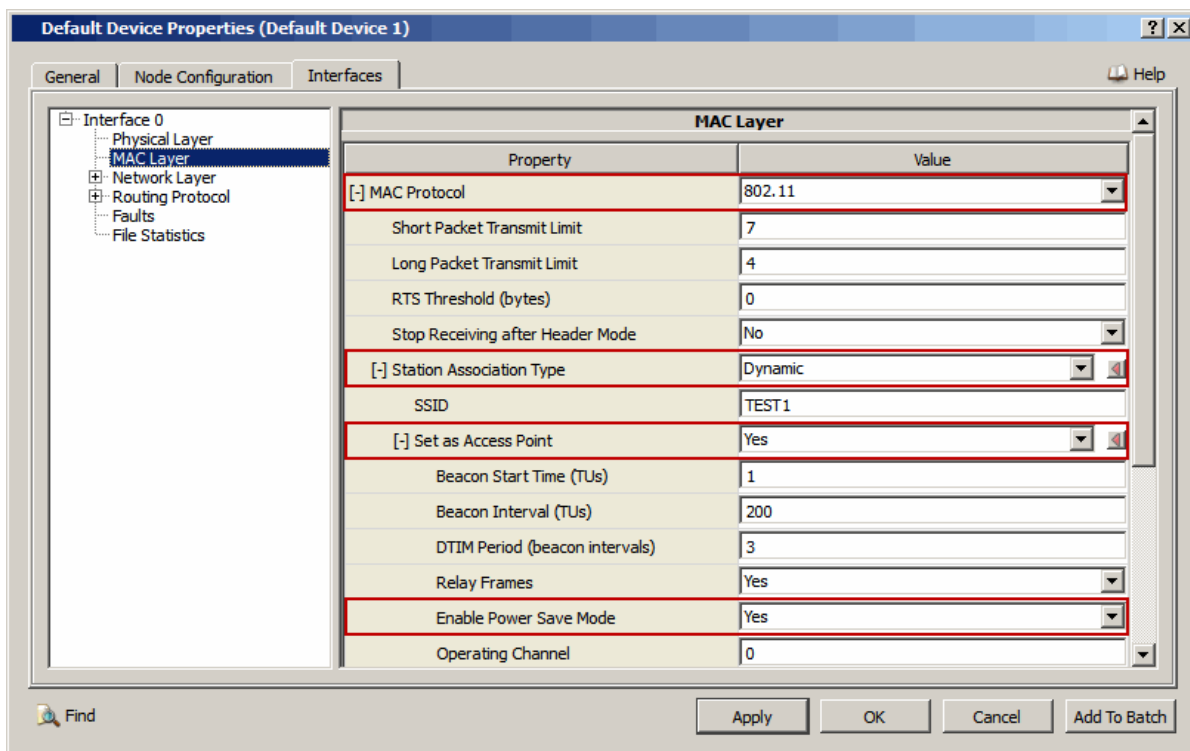
FIGURE 1-2.   Path to a Specific Parameter

Parameter Table

GUI configuration of a model is described as a series of a steps. Each step describes how to configure one or more parameters. Since the GUI display name of a parameter may be different from the name in the configuration file, each step also includes a table that shows the mapping between the GUI names and command line names of parameters configured in that step. For a description of a GUI parameter, see the description of the equivalent command line parameter in the command line configuration section.

The format of a parameter mapping table is shown in Table 1-5.

TABLE 1-5.   Mapping Table

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
<GUI Display Name>	*<Scope>*	*<Command Line Parameter Name>*

The first column, labeled "GUI Parameter", lists the name of the parameter as it is displayed in the GUI.

The second column, labeled "Scope of GUI Parameter", lists the level(s) at which the parameter can be configured. *<Scope>* can be any combination of: Global, Node, Subnet, Wired Subnet, Wireless Subnet, Point-to-point Link, and Interface.

Table 1-6 lists the Properties Editors where parameters with different scopes can be set.

Notes: 1. Unless otherwise stated, the "Subnet" scope refers to "Wireless Subnet".

2. The scope column can also refer to Properties Editors for special devices and network components (such as ATM Device Properties Editor) which are not included in Table 1-6.

TABLE 1-6.   Properties Editors for Different Scopes

Scope of GUI Parameter	Properties Editor
Global	Scenario Properties Editor
Node	Default Device Properties Editor (General and Node Configuration tabs)
Subnet Wireless Subnet	Wireless Subnet Properties Editor
Wired Subnet	Wired Subnet Properties Editor
Point-to-point Link	Point-to-point Link Properties Editor
Interface	Interface Properties Editor, Default Device Properties Editor (Interfaces tab)

The third column, labeled "Command Line Parameter", lists the equivalent command line parameter.

Note: For some parameters, the scope may be different in command line and GUI configurations (a parameter may be configurable at fewer levels in the GUI than in the command line).

Table 1-7 is an example of a parameter mapping table.

TABLE 1-7.   Example Mapping Table

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Define Area	Node	OSPFv2-DEFINE-AREA
OSPFv2 Configuration File	Node	OSPFv2-CONFIG-FILE
Specify Autonomous System	Node	N/A
Configure as Autonomous System Boundary Router	Node	AS-BOUNDARY-ROUTER
Inject External Route	Node	N/A
Enable Stagger Start	Node	OSPFv2-STAGGER-START

2 MAC Layer Models

This chapter describes features, configuration requirements and parameters, statistics, and scenarios for MAC Layer Models, and consists of the following sections:

- Detailed Switch Model
- Switched Ethernet
- Virtual LAN (VLAN)

2.1 Detailed Switch Model

The QualNet Detailed Switch model is based on the following standards:

- IEEE standard 802.1D
- IEEE standard 802.1t
- IEEE standard 802.1w
- IEEE draft P802.1y/D2
- IEEE standard 802.1Q
- IEEE standard 802.1u
- IEEE standard 802.1v

2.1.1 Description

The Detailed Switch model is based on the IEEE 802.1 standards that allow a MAC switch to:

- Connect 802 LANs.
- Allow the LANs to have different MAC protocols.
- Allow the connected LAN segments to be transparent to upper layers.

Detailed Switch uses GARP (Generic Attribute Registration Protocol) and GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) to support VLAN. Following is a brief description of VLAN, GARP and GVRP.

A VLAN (virtual LAN) is a local area network that maps workstations on some basis other than geographic location. It can also be considered as a broadcast domain created by switches.

GARP is a local area network (LAN) protocol that defines procedures by which end stations and switches can register and de-register attributes, such as network identifiers or addresses, with each other. Every end station and switch thus has a record or a list of all the other end stations and switches that can be reached at any given time. This defined set of participants at any given time, along with their attributes, is a subset of the network topology called the reachability tree. The implementation is based on IEEE 802.1D. Note that the GARP applicant/registrar state machines apply only to switch ports; end-stations do not participate in the dynamic application and registration process in the implementation.

GVRP is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices and create the VLAN member sets in a switched network. If GVRP is enabled, it suffices to set the port VLAN ID for access links. Also note that GVRP does not create the untagged member set.

It covers Level 2 switches and port based VLANs. Currently in QualNet, two models, MAC 802.3 and LINK, are supported at the switched ports. Refer to the appropriate sections in *Developer Model Library*. The Detailed Switch model uses the FIFO queue and the Strict Priority scheduler.

2.1.2 Features and Assumptions

This section describes the implemented features, omitted features, assumptions and limitations of the Detailed Switch model.

2.1.2.1 Implemented Features

- Conformance with the MAC protocol models implemented at the switch ports. Currently, two MAC models are supported: Link and 802.3.
- Relay of frames between ports including conversion of frame format, if required.
- Basic filtering service to enable relay between ports of the switch.
- Multiple priority queue based buffering at each port. However, both the supported MAC protocols do not carry priority information in frames.
- Spanning tree algorithm to determine a loop-free route between connected LANs.

2.1.2.2 Omitted Features

None.

2.1.2.3 Assumptions and Limitations

None.

2.1.3 Command Line Configuration

To enable the Detailed Switch model, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] SWITCH  YES
```

The scope of this parameter declaration can be Global or Node. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

>   **Note:**   The default value of parameter `SWITCH` is `NO`.

For switched networks, multiple LAN segments are permitted using the same network or subnet address. For example, to specify three LAN segments in subnet 1.0 and connected to ports of a switch with node ID 100, use the following:

```
LINK N8-1.0 {100, 1}
LINK N8-1.0 {100, 2}
SUBNET N8-1.0 (100, 3 thru 10}
```

>   **Note:**   The `N` syntax uses a number large enough for the mask to cover all the interfaces of the 1.0 subnet; the `LINK` statement does not use `N2` as it would be the common practice in non-switch scenarios.

Detailed Switch General Parameters

Table 2-1 shows the general parameters for the Detailed Switch Model. See Section 1.2.1.3 for a description of the format used for the parameter tables.

TABLE 2-1.   General Parameters for the Detailed Switch Model

Parameter	Value	Description
`SWITCH-PORT-MAPPING-TYPE` *Optional* *Scope:* Global, Node	List: • AUTO • MANUAL *Default:* MANUAL	Each switch port needs to be mapped to an interface address if port specific parameters would be input. If no port specific parameters would be input for a switch, an AUTO mapping may be used.
`SWITCH-PORT-MAP` *Optional* *Scope:* Global, Node, Interface *Instances:* port number	IP Address	Specifies the interface address. Maps each switch port to an interface address. **Note:** This parameter is required if SWITCH-PORT-MAPPING-TYPE is of type MANUAL.
`SWITCH-DATABASE-MAX-ENTRIES` *Optional* *Scope:* Global, Node	Integer *Range:* ≥ 0 *Default:* 500	Specifies the maximum number of dynamic entries of the filtering/learning database.

`SWITCH-DATABASE-AGING-TIME`
`SWITCH-DATABASE-AGEING-TIME`
 	
Optional
 	
Scope: Global, Node
	Time
	
	Range: [10S, 1000000S]
	
	Default: 300S
		Specifies the aging time for dynamic entries in the filtering/learning database.

`SWITCH-QUEUE-NUM-PRIORITIES` *Optional* *Scope:* Global, Node, Interface *Instances:* port number	Integer *Range:* [1, 8] *Default:* 3	Specifies the number of output queues.
`SWITCH-OUTPUT-QUEUE-SIZE` *Optional* *Scope:* Global, Node, Interface *Instances:* port number	Integer *Range:* ≥ 0 *Default:* 150000 *Unit:* bytes	Specifies the size of output queues.
`SWITCH-INPUT-QUEUE-SIZE` *Optional* *Scope:* Global, Node, Interface *Instances:* port number	Integer *Range:* ≥ 0 *Default:* 150000 *Unit:* bytes	Specifies the size of input queue.

TABLE 2-1.   General Parameters for the Detailed Switch Model (Continued)

Parameter	Value	Description
SWITCH-CPU-QUEUE-SIZE *Optional* *Scope:* Global, Node	Integer *Range:* ≥ 0 *Default:* 640000 *Unit:* bytes	Specifies the size of CPU queue.
SWITCH-BACKPLANE-THROUGHPUT *Optional* *Scope:* Global, Node	Real *Range:* ≥ 0 *Default:* 0 *Unit:* bps	Specifies the backplane throughput. The default value is 0 bps, which implies that there will be no backplane delay.
SWITCH-RUN-STP *Optional* *Scope:* Global, Node	List: • YES • NO *Default:* YES	Specifies if the Spanning Tree Protocol (STP) is run. **Note:** If STP is not run, then the switched network should loop free. If this parameter is set to YES, set the STP parameters listed in Table 2-2.
SWITCH-RUN-GVRP *Optional* *Scope:* Global, Node	List: • YES • NO *Default:* NO	Switch uses GVRP. Applicable only to VLAN aware switches. If this parameter is set to YES, set the GVRP parameters listed in Table 2-15.
MAC-LAYER-STATISTICS *Optional* *Scope:* All	List: • YES • NO *Default:* NO	Enables MAC layer statistics. MAC layer statistics should be enabled in order to collect additional statistics for the Detailed Switch model.
SWITCH-SCHEDULER-STATISTICS *Optional* *Scope:* All *Instances:* port number	List: • YES • NO *Default:* NO	Enables scheduler specific statistics at each port.
SWITCH-QUEUE-STATISTICS *Optional* *Scope:* All *Instances:* port number	List: • YES • NO *Default:* NO	Enables output queue statistics at each port.
SWITCH-BACKPLANE-STATISTICS *Optional* *Scope:* Global, Node	List: • YES • NO *Default:* NO	Enables backplane statistics.

TABLE 2-1.   General Parameters for the Detailed Switch Model (Continued)

Parameter	Value	Description
SWITCH-DATABASE-STATISTICS *Optional* *Scope:* Global, Node	List: • YES • NO *Default:* NO	Enables database specific statistics.
SWITCH-PORT-STATISTICS *Optional* *Scope:* All *Instances:* port number	List: • YES • NO *Default:* NO	Enables port specific statistics.

Spanning Tree Protocol (STP) Parameters
Table 2-2 shows the Spanning Tree Protocol (STP) parameters for the Detailed Switch model. The implementation follows the single rapid spanning tree of 802.1w. For specific root election, SWITCH-PRIORITY parameter can be used to specify a priority value on it.

TABLE 2-2.   STP Parameters for the Detailed Switch Model

Parameter	Value	Description
SWITCH-PRIORITY *Optional* *Scope:* Global, Node	Integer *Range:* [0, 61440] *Default:* 32768	Specifies the priority of a switch. If the value is not a multiple of 4096, the nearest multiple is used. **Note:** A lower value of priority is better; 0 is the highest priority.
SWITCH-HELLO-TIME *Optional* *Scope:* Global, Node	Time *Range:* [1S, 10S] *Default:* 2S	Specifies hello time for STP. This is time between generation of BPDUs by the root switch.
SWITCH-MAX-AGE *Optional* *Scope:* Global, Node	Integer *Range:* [6S, 40S] *Default:* 20S	Specifies maximum age time for BPDUs.
SWITCH-FORWARD-DELAY *Optional* *Scope:* Global, Node	Time *Range:* [4S, 30S] *Default:* 15S	Specifies time for forward delay.
SWITCH-HOLD-COUNT *Optional* *Scope:* Global, Node	Integer *Range:* [1, 10] *Default:* 3	Specifies the limit of number of BPDU transmits in hello time.

TABLE 2-2.   STP Parameters for the Detailed Switch Model (Continued)

Parameter	Value	Description
`SWITCH-PORT-PATH-COST` *Optional* *Scope:* Global, Node, Interface *Instances:* port number	Integer *Range:* $\geq$ 0 *Default:* See Note	Specifies the path cost for a port. The default value is based on a computation based on the bandwidth of the protocol connected to the port. **Note:** If the port bandwidth is in the range [0, 9999], the default path cost is 200000000. Else if it is in the range [10000, 2147483647], the default value is(200000000 * 10000) divided by interface bandwidth. However, if the port bandwidth is greater than 10000000000 bytes, the default value is taken as 1.
`SWITCH-PORT-POINT-TO-POINT` *Optional* *Scope:* Global, Node, Interface *Instances:* port number	List: • `AUTO` • `FORCE-TRUE` • `FORCE-FALSE` *Default:* `AUTO`	Specifies that the port is attached to a point-to-point link. The default value is `AUTO`, which means that if the Link MAC protocol is configured at the port, it will support point to point connectivity.
`SWITCH-PORT-EDGE` *Optional* *Scope:* Global, Node, Interface *Instances:* port number	List: • `YES` • `NO` *Default:* `NO`	Specifies that the port is the only switch port in a switched network attached to a LAN.
`SWITCH-PORT-PRIORITY` *Optional* *Scope:* Global, Node, Interface *Instances:* port number	Integer *Range:* `[0, 240]` *Default:* 128	Specifies the switch priority. If the input value is not a multiple of 16, the nearest value is used. **Note:** A lower value of priority is better; 0 is the highest priority.

2.1.4 GUI Configuration

This section describes how to configure the Detailed Switch model in the GUI.

Switch Device

The Detailed Switch is modeled by the Switch device in the Devices toolbar of the Standard Toolset.

FIGURE 2-1.   Switch Device in Devices Toolbar

2.1.4.1 Configuring General Switch Parameters

To configure the general switch parameters, perform the following steps:

1. Go to **Switch Properties Editor > Switch > General**.

2. Set the general switch parameters listed in Table 2-3.

FIGURE 2-2.   Configuring Switch Parameters

TABLE 2-3.   Command Line Equivalent of Switch Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Run STP	Node	`SWITCH-RUN-STP`
Maximum Number of Database Entries	Node	`SWITCH-DATABASE-MAX-ENTRIES`
Database Entry Aging Time	Node	`SWITCH-DATABASE-AGING-TIME`
Database Statistics	Node	`SWITCH-DATABASE-STATISTICS`
Backplane Throughput	Node	`SWITCH-BACKPLANE-THROUGHPUT`
Backplane Statistics	Node	`SWITCH-BACKPLANE-STATISTICS`
CPU Queue Size	Node	`SWITCH-CPU-QUEUE-SIZE`
Input Queue Size	Node	`SWITCH-INPUT-QUEUE-SIZE`
Output Queue Size	Node	`SWITCH-OUTPUT-QUEUE-SIZE`

Note: See Section 2.3 for details of configuring VLAN parameters.

2.1.4.2 Configuring Spanning Tree Protocol (STP)

To configure STP, perform the following steps:

1. Go to **Switch Device Properties Editor > Switch > General**.

2. Set **Run STP** to *Yes* and set the dependent parameters listed in Table 2-4.
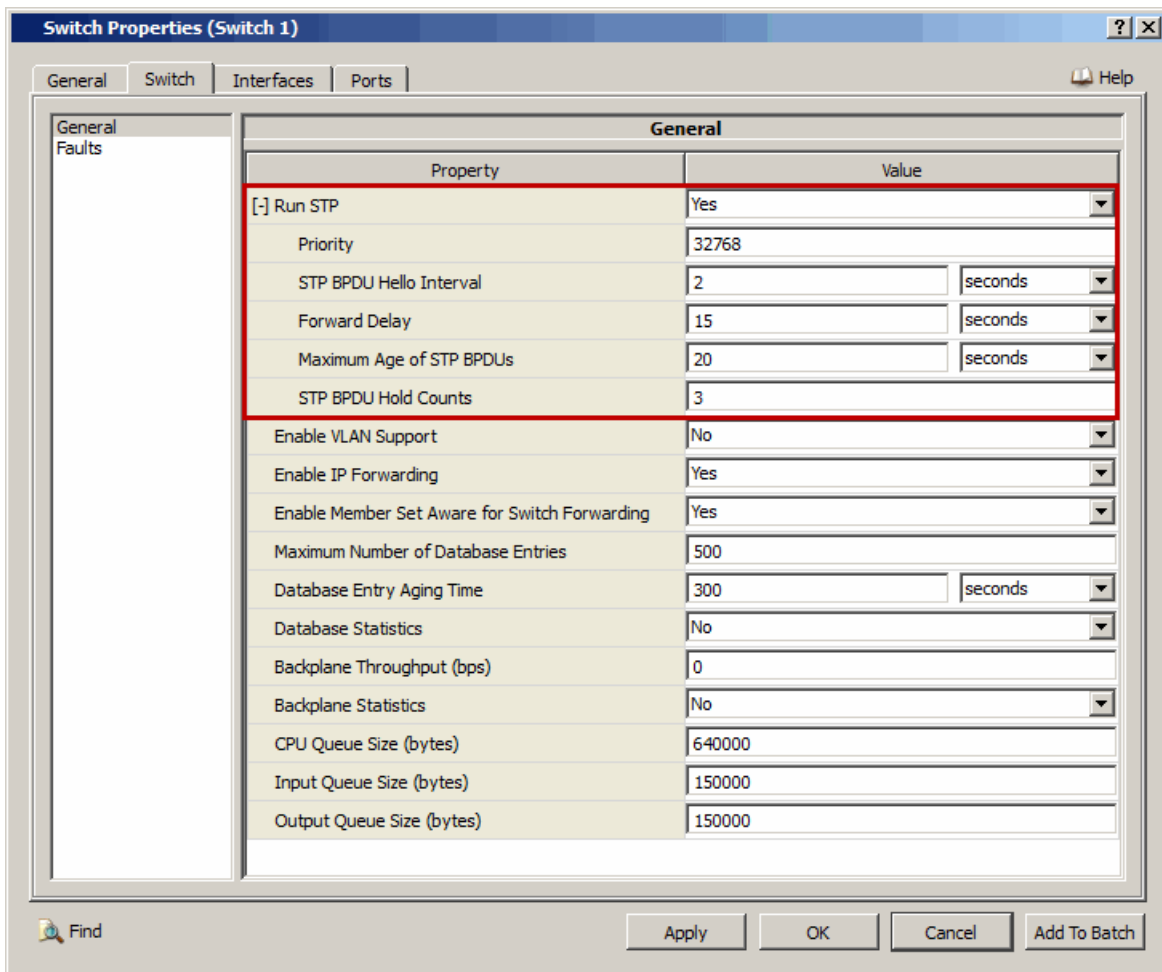
FIGURE 2-3.   Configuring STP

TABLE 2-4.   Command Line Equivalent of STP Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Priority	Node	SWITCH-PRIORITY
STP BPDU Hello Interval	Node	SWITCH-HELLO-TIME
Forward Delay	Node	SWITCH-FORWARD-DELAY
Maximum Age of STP BPDUs	Node	SWITCH-MAX-AGE
STP BPDU Hold Counts	Node	SWITCH-HOLD-COUNT

2.1.4.3 Configuring Switch Port Parameters

To configure switch port parameters perform the following steps:

1. Go to **Switch Device Properties Editor > Ports > Port #**.

2. Set the switch port parameters listed in Table 2-5.
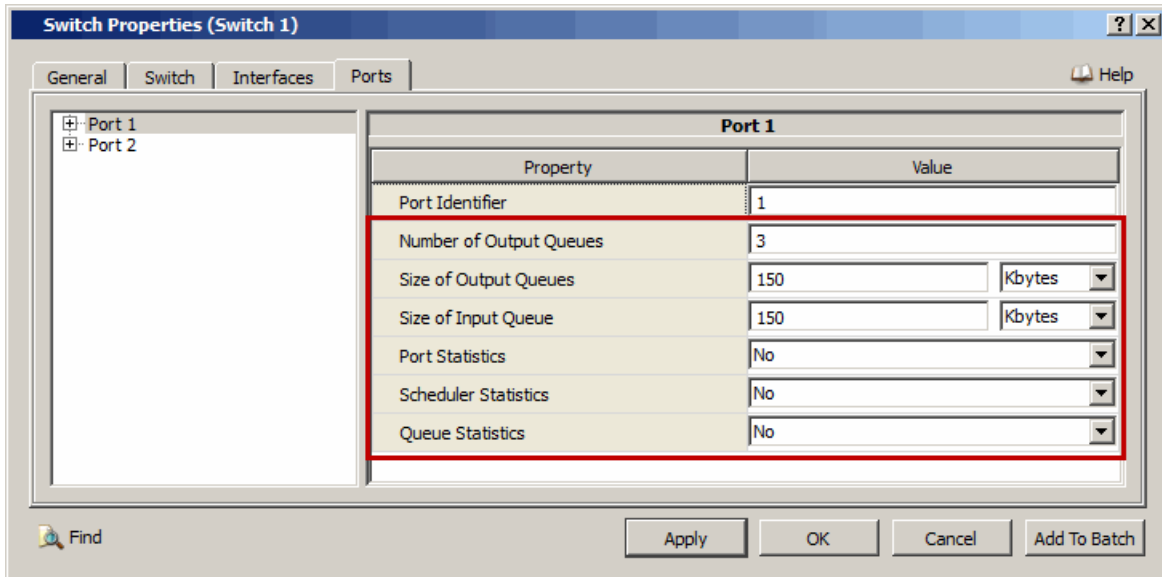
FIGURE 2-4.   Configuring Switch Ports

TABLE 2-5.   Command Line Equivalent of Switch Port Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Number of Output Queues	Node	`SWITCH-QUEUE-NUM-PRIORITIES`
Size of Output Queues	Node	`SWITCH-OUTPUT-QUEUE-SIZE`
Size of Input Queue	Node	`SWITCH-INPUT-QUEUE-SIZE`
Port Statistics	Node	`SWITCH-PORT-STATISTICS`
Scheduler Statistics	Node	`SWITCH-SCHEDULER-STATISTICS`
Queue Statistics	Node	`SWITCH-QUEUE-STATISTICS`

2.1.4.4 Configure STP Port Parameters

To configure STP port parameters, perform the following steps:

1. Go to the **Switch Device Properties Editor > Port > Port # > STP**.

2. Set the STP port parameters listed in Table 2-6.
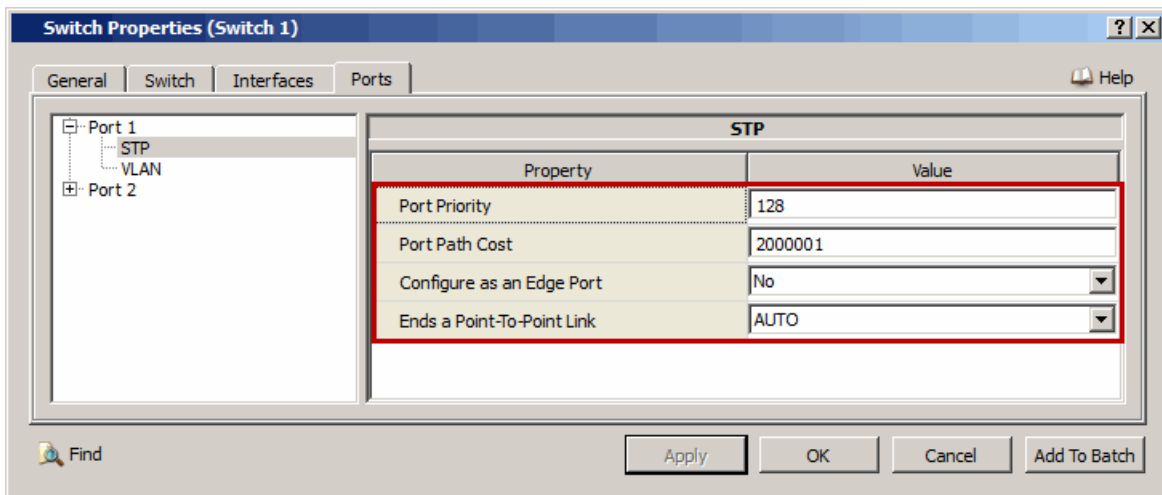
FIGURE 2-5.   Configuring STP Port Parameters

TABLE 2-6.   Command Line Equivalent of STP Port parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Port Priority	Node	SWITCH-PORT-PRIORITY
Port Path Cost	Node	SWITCH-PORT-PATH-COST
Configure as an Edge Port	Node	SWITCH-PORT-EDGE
Ends a Point-To-Point Link	Node	SWITCH-PORT-POINT-TO-POINT

2.1.4.5 Configuring Statistics Parameters

Statistics for the Detailed Switch model can be collected at the global, node, subnet, and interface node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable MAC Layer statistics, port statistics, scheduler statistics and queue statistics, check the box labeled **MAC**, **Switch Port**, **Switch Scheduler** and **Switch Queue** in the appropriate properties editor.

TABLE 2-7.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
MAC	Global, Node, Subnet, Interface	MAC-LAYER-STATISTICS
Switch Port	Global, Node, Subnet, Interface	SWITCH-PORT-STATISTICS
Switch Scheduler	Global, Node, Subnet, Interface	SWITCH-SCHEDULER-STATISTICS
Switch Queue	Global, Node, Subnet, Interface	SWITCH-QUEUE-STATISTICS

In addition, statistics for the Detailed Switch model can also be collected for each port. To collect port statistics, scheduler statistics and queue statistics for a specific port, set the respective statistics parameters as described in Section 2.1.4.3.

2.1.5 Statistics

This section describes the file, database, and dynamic statistics of the Detailed Switch model.

2.1.5.1 File Statistics

Table 2-8 lists the Detailed Switch statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 2-8.   Detailed Switch Statistics

Statistic	Description
Port Statistics	
Total frames received	Total number of frames received by the switch.
Unicast frames forwarded directly	Total number of unicast frames forwarded directly by the switch.
Unicast frames flooded	Total number of unicast frames flooded by the switch.
Unicast frames delivered to upper layer	Total number of unicast frames delivered to upper layer by the switch.
Unicast frames dropped	Total number of unicast frames dropped by the switch.
Broadcast frames forwarded	Total number of broadcast frames forwarded by the switch.
Broadcast frames dropped	Total number of broadcast frames dropped by the switch.
Frames dropped in discard state	Total number of frames dropped in discard state by the switch.
Frames dropped in learning state	Total number of frames dropped in learning state by the switch.
Frames dropped by ingress filtering	Total number of frames dropped by ingress filtering by the switch.
Frames dropped, received from unknown vlan	Total number of frames dropped, received from unknown vlan by the switch.
STP Statistics	
RST BPDUs sent	Total number of RST BPDUs sent by the switch.
RST BPDUs received	Total number of RST BPDUs received by the switch.
Config BPDUs sent	Total number of Config BPDUs sent by the switch.
Config BPDUs received	Total number of Config BPDUs received by the switch.
Backplane Statistics	
Frames dropped at Backplane	Total number of frames dropped at Backplane by the switch.
DB Statistics	
Number of entry inserted	Total number of entries inserted by the switch.
Number of LRU entry deleted	Total number of LRU entries deleted by the switch.
Number of entry aged out	Total number of entries aged out by the switch.
Number of entry flushed	Total number of entries flushed by the switch.
Hit ratio	Ratio of Number of entries found to Number of entries searched by the switch.
GVRP Statistics	
Join Empty received	Number of join empty messages received by the switch.
Join In received	Number of join in messages received by the switch.
Leave All received	Number of leave all messages received by the switch.
Leave Empty received	Number of leave empty messages received by the switch.
Leave In received	Number of leave in messages received by the switch.
Join Empty transmitted	Number of join empty messages transmitted by the switch.
Join In transmitted	Number of join in messages transmitted by the switch.

TABLE 2-8.   Detailed Switch Statistics (Continued)

Statistic	Description
Leave All transmitted	Number of leave all messages transmitted by the switch.
Leave Empty transmitted	Number of leave empty messages transmitted by the switch.
Leave In transmitted	Number of leave in messages transmitted by the switch.

2.1.5.2 Database Statistics

In addition to the file statistics, the Detailed Switch model also enters statistics in various scenario statistics database tables. Refer to *QualNet Statistics Database User's Guide* for details.

2.1.5.3 Dynamic Statistics

No dynamic statistics are supported for the Detailed Switch model.

2.1.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the Detailed Switch model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/mac-switch. Table 2-9 lists the sub-directory where each scenario is located.

TABLE 2-9.   Detailed Switch Model Scenarios Included in QualNet

Scenario	Description
gvrp/sample1	Shows the functionality of GVRP.
gvrp/sample2	Shows the functionality of GVRP in parallel with STP.
performance/sample1	Shows that switch can improve performance of a single broadcast domain.
performance/sample2	Shows that switch can improve performance of a single broadcast domain where nodes have the full bandwidth.
stp/sample1	Shows the functionality of Spanning Tree protocol with a scenario having loops.
stp/sample2	Shows the functionality of Spanning Tree protocol with a scenario having interface faults that result in re-computation of different spanning trees.
vlan/sample1	Shows the functionality of VLAN.
vlan/sample2	Shows the functionality of VLAN in multicast network.

2.1.7 References

1. IEEE standard 802.1D. "Part 3: Media Access Control (MAC) Bridges." 1998.

2. IEEE standard 802.1t. "Part 3: Media Access Control (MAC) Bridges Amendment 1." 2001.

3. IEEE standard 802.1w. "Part 3:Media Access Control (MAC) Bridges - Amendment 2:Rapid Reconfiguration." 2001.

4. IEEE draft P802.1y/D2. "Media Access Control (MAC) Bridges - Amendment 3: Technical and Editorial Corrections." January 2002.

5. IEEE standard 802.1Q. "Virtual Bridged Local Area Networks." 1998.

6. IEEE standard 802.1u. "Amendment 1: Technical and editorial corrections." 2001.

7. IEEE standard 802.1v. "Amendment 2: VLAN Classification by Protocol and Port." 2001.

■ ■

2.2 Switched Ethernet

The QualNet Switched Ethernet model is based on the IEEE 802.3 standard.

2.2.1 Description

Switched Ethernet is an abstract store-and-forward single switch-based 802.3 LAN with fixed bandwidth and propagation delay. The model considers the switching fabric to be equivalent to a set of point-to-point links connecting all sources and receivers, except that when multiple sources attempt to send to a single receiver, their transmissions are serialized without additional buffering overhead.

2.2.2 Assumptions and Limitations

- QualNet handles the backoff situation using 'Truncated Binary Exponential Backoff' algorithm.So under a heavy load, a station may capture the channel.
- Frame will face same propagation delay for all the destination stations. So distance is not a factor between any pair of station.

2.2.3 Command Line Configuration

To select Switched Ethernet as the MAC protocol, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] MAC-PROTOCOL SWITCHED-ETHERNET
```

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

Switched Ethernet Parameters

Table 2-10 describes the Switched Ethernet configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 2-10.   Switched Ethernet Parameters

Parameter	Value	Description
SUBNET-DATA-RATE Required *Scope:* All	Real *Unit:* bps	Specifies the data rate.
SUBNET-PROPAGATION-DELAY Required *Scope:* All	Time *Range:* ≥ 0S	Specifies propagation delay.

2.2.4 GUI Configuration

This section describes how to configure Switched Ethernet in the GUI.

Configuring Switched Ethernet Parameters

To configure the Switched Ethernet parameters, perform the following steps:

1. Go to **Wired Subnet Properties Editor > General**.

2. Set **MAC Protocol** to *Switched Ethernet* and set the dependent parameters listed in Table 2-11.
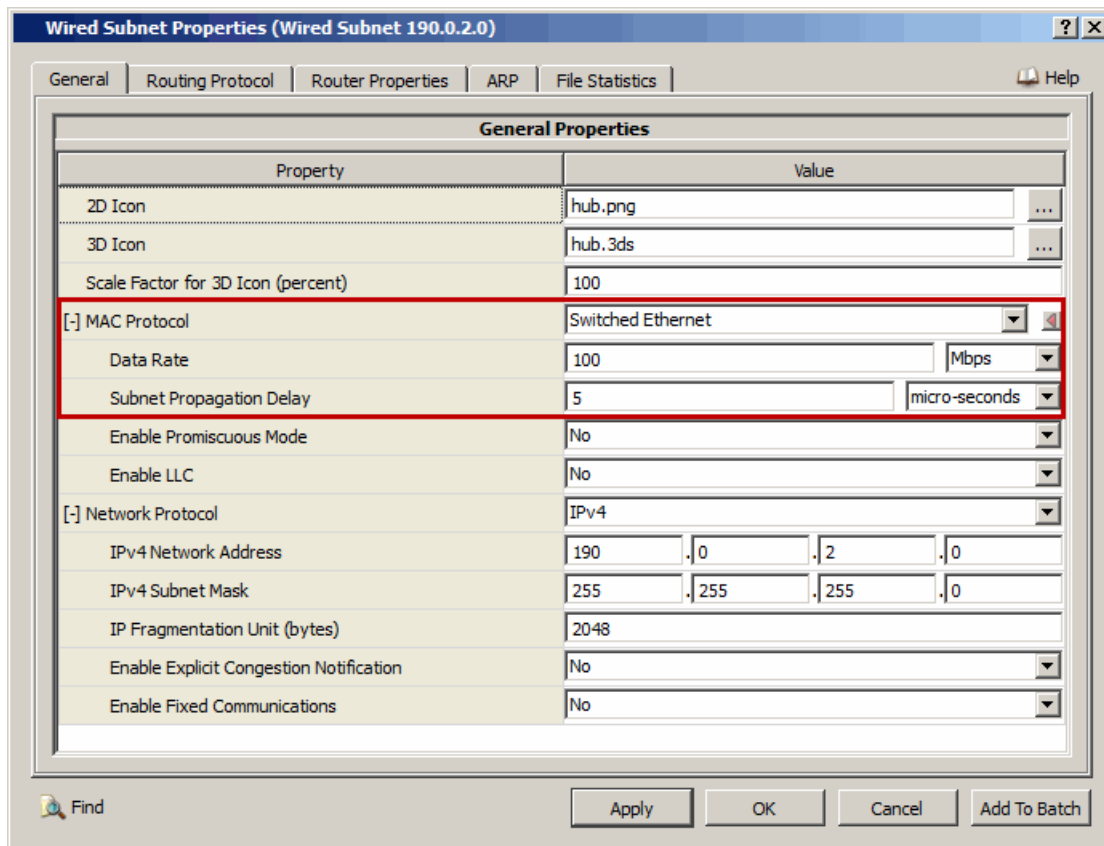
FIGURE 2-6.   Setting Switched Ethernet Parameters

TABLE 2-11.   Command Line Equivalent of Switched Ethernet Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Data Rate	Subnet	`SUBNET-DATA-RATE`
Subnet Propagation Delay	Subnet	`SUBNET-PROPAGATION-DELAY`

Configuring Statistics Parameters

Statistics for the Switched Ethernet model can be collected at the global, node, subnet, and interface levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for Switched Ethernet, check the box labeled **MAC** in the appropriate properties editor.

TABLE 2-12.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
MAC	Global, Node, Subnet, Interface	`MAC-LAYER-STATISTICS`

2.2.5 Statistics

Table 2-13 shows the Switched Ethernet model statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 2-13.   Switched Ethernet Statistics

Statistic	Description
Frames sent	Packets sent to the switch.
Frames received	Packets received from the switch.

2.3 Virtual LAN (VLAN)

The QualNet VLAN model is based on the IEEE 802.1g standard.

2.3.1 Description

Virtual LAN (VLAN) allows for the configuring of multiple subnets into one virtual network. VLAN is often used by large organizations to organize internal networks. With larger switched networks, it is desirable to logically group end stations in such a way that they appear to be connected to multiple LANs. This view effectively makes each logical group appear as a single Layer 2 broadcast domain or a virtual LAN. In terms of performance, this reduces the propagation of broadcasts, multicast and unlearned unicast addresses. In terms of privacy, traffic meant for the logical group does not "leak" to other logical groups.

Segments with the same VLAN ID should be given the same subnet address and mask. Segments with different VLAN IDs should have different subnet addresses for inter-VLAN communication and require routing. The implementation supports port-based VLANs based on 802.1g.

2.3.2 Command Line Configuration

To enable the VLAN model, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] SWITCH-STATION-VLAN-ID   <vlan-id>
```

where

<vlan-id>   VLAN ID of the station. This should be an integer between 1 and 4090. The default value of this parameter is 1.

The scope of this parameter declaration can be Global, Subnet or Interface. See Section 1.2.1.1 for a description of <Qualifier> for each scope.

VLAN Parameters

Table 2-14 describes the VLAN configuration parameters. Table 2-15 lists the GVRP and GARP configuration parameters for the VLAN model. See Section 1.2.1.3 for a description of the format used for the parameter tables.

TABLE 2-14.   VLAN Configuration Parameters

Parameter	Value	Description
SWITCH-STATION-VLAN-TAGGING *Required* *Scope:* Global, Subnet, Interface	List: • YES • NO	Specifies whether end stations need to send tagged or untagged frames.
SWITCH-VLAN-MEMBER-SET *Optional* *Scope:* Global, Node *Instances:* VLAN ID	Port number list (see note 1)	Specifies member set for each VLAN at a switch. The member set for a VLAN is the set of ports across which broadcasts for that VLAN are flooded. The list of port numbers is specified as a space-separated list of port numbers enclosed in "{" and "}".

TABLE 2-14.   VLAN Configuration Parameters (Continued)

Parameter	Value	Description
SWITCH-VLAN-UNTAGGED-MEMBER-SET *Optional* *Scope:* Global, Node *Instances:* VLAN ID	Port number list (see note 1)	Specifies untagged set. This is a subset of the member set where egress frames are not tagged.
SWITCH-VLAN-LEARNING *Optional* *Scope:* Global, Node	List: • SHARED • INDEPENDENT • COMBINED *Default:* SHARED	Specifies VLAN learning type for a switch database. For SHARED learning, there is one database for all VLANs. For INDEPENDENT learning, there is one database per VLAN. For COMBINED learning, there is a m:n relationship between VLANs and databases. This requires additional input.
SWITCH-VLAN-COMBINED-LEARNING *Optional* *Scope:* Global, Node *Instances:* Filter database ID (see description)	VLAN ID list (see note 2)	Specifies the VLAN to database mapping for COMBINED learning. By default, VLAN mappings that are not explicitly mapped to any other filter database ID are mapped to filter database ID 1. The filter database ID can be an integer between 2 and 4090.
SWITCH-VLAN-AWARE *Optional* *Scope:* Global, Node	List: • YES • NO *Default:* NO	Specifies whether the switch supports VLANs.
SWITCH-PORT-VLAN-ID *Optional* *Scope:* Global, Node, Interface *Instances:* port number (see note 3)	Integer *Range:* [[1, 4090] *Default:* 1	Specifies VLAN ID for a switch port. For an access link, this is typically the value of the VLAN ID of the end stations attached to the port. For trunk links, this is typically the default VLAN ID and does not need to be specified. For hybrid segments, the value is typically that of the untagged end stations.
SWITCH-PORT-VLAN-ADMIT-FRAMES *Optional* *Scope:* Global, Node, Interface *Instances:* port number (see note 3)	List: • ALL • TAGGED *Default:* ALL	Specifies whether the port will admit all frames or only VLAN tagged frames. If TAGGED is specified, the port will filter untagged frames.

TABLE 2-14.   VLAN Configuration Parameters (Continued)

Parameter	Value	Description
SWITCH-PORT-VLAN-INGRESS-FILTERING *Optional* *Scope:* Global, Node, Interface *Instances:* port number (see note 3)	List: • NONE • VLAN *Default:* NONE	Specifies whether the port will admit all VLAN frames or only those for which it is in the member set.
SWITCH-FORWARDING-IS-MEMBER-SET-AWARE *Optional* *Scope:* Global, Node, Interface	List: • YES • NO *Default:* YES	Specifies whether the switch is aware of its member set.
SWITCH-PORT-VLAN-STATISTICS *Optional* *Scope:* Global, Node, Interface *Instances:* port number (see note 3)	List: • YES • NO *Default:* NO	Specifies whether the general port statistics should be collected per VLAN.

Notes: 1. A port number list is specified as a space-separated list of port numbers enclosed in "{ " and "}".

       2. A VLAN ID list is specified as a space-separated list of VLAN IDs enclosed in "{ " and "}".

       3. Parameters `SWITCH-PORT-VLAN-ID`, `SWITCH-PORT-VLAN-ADMIT-FRAMES`, `SWITCH-PORT-VLAN-INGRESS-FILTERING`, and `SWITCH-PORT-VLAN-STATISTICS` are specified using the following format:

          `[<Node ID>] <Parameter Name> [<Port Num>] <Parameter Value>`

or

          `<Port Address List> <Parameter Name> <Parameter Value>`

  where

`<Node ID>`	Node identifier(s) to which this parameter declaration is applicable, enclosed in square brackets. This qualifier is optional, and if it is not included, then the parameter declaration is applicable to all nodes, subject to precedence rules.
`<Parameter Name>`	Name of the parameter (`SWITCH-PORT-VLAN-ID`, `SWITCH-PORT-VLAN-ADMIT-FRAMES`, `SWITCH-PORT-VLAN-INGRESS-FILTERING`, or `SWITCH-PORT-VLAN-STATISTICS`).
`<Port Num>`	Port number to which this parameter declaration is applicable, enclosed in square brackets.
	This should be in the range 0 to *n* -1, where *n* is the number of ports.
	This index is optional, and if it is not included, then the parameter declaration is applicable to all ports, subject to precedence rules.
`<Port Address List>`	List of space-separated port IP addresses to which this parameter declaration is applicable, enclosed in square brackets.
`<Parameter Value>`	Value of the parameter.

Table 2-15 lists the GVRP and GARP configuration parameters for the VLAN model.

TABLE 2-15.   GVRP and GARP Parameters for the VLAN Model

Parameter	Value	Description
SWITCH-GVRP-MAXIMUM-VLANS *Optional* *Scope:* Global, Node	Integer *Range:* [1, 4090] *Default:* 10	Maximum number of VLANS for GVRP to work with.
SWITCH-GARP-JOIN-TIME *Optional* *Scope:* Global, Node	Time *Range:* > 0S *Default:* 200MS	Average time between Join messages sent by the applicant.
SWITCH-GARP-LEAVE-TIME *Optional* *Scope:* Global, Node	Time *Range:* > 0S *Default:* 600MS	Specifies the time a registrar takes to transition from In state to Empty state. **Note:** The leave time should be three times the join time.
SWITCH-GARP-LEAVEALL-TIME *Optional* *Scope:* Global, Node	Time *Range:* > 0S *Default:* 10S	Specifies the periodic interval between LeaveAll messages. **Note:** This value should be at least 10 times the leave time.
SWITCH-GVRP-STATISTICS *Optional* *Scope:* Global, Node	List: • YES • NO *Default:* NO	Enables additional GVRP statistics at a switch.
SWITCH-PORT-VLAN-STATISTICS *Optional* *Scope:* Global, Node, Interface *Instances:* port number	List: • YES • NO *Default:* NO	Enables additional VLAN specific statistics at each port.

2.3.3 GUI Configuration

This section describes how to configure VLAN in the GUI.

Configuring Switch-level Properties

To configure the switch-level VLAN parameters, perform the following steps:

1. Go to **Switch Properties Editor > Switch > General**.

2. Set **Enable VLAN Support** to *Yes* and set the dependent parameters listed in Table 2-16.
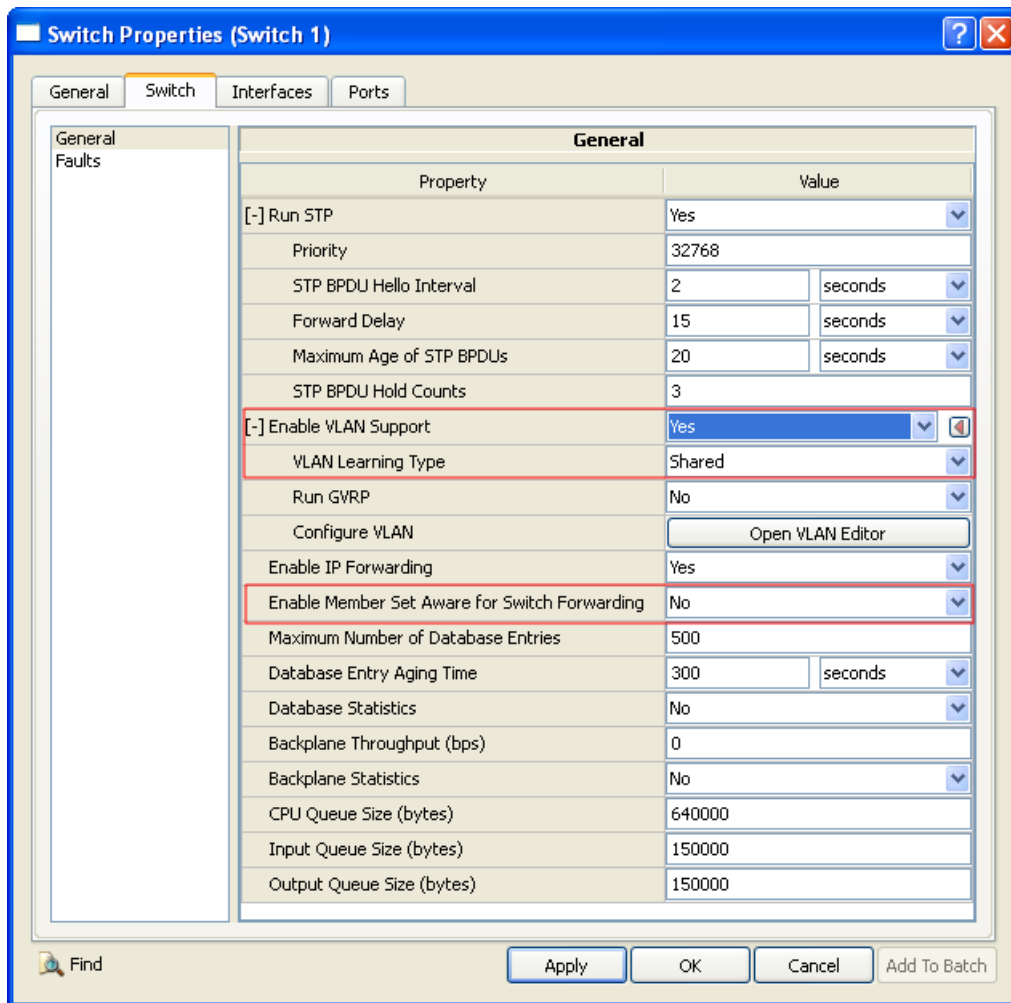
FIGURE 2-7.   Setting VLAN Parameters

TABLE 2-16.   Command Line Equivalent of VLAN Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
VLAN Learning Type	Node	SWITCH-VLAN-LEARNING
Enable Member Set Aware for Switch Forwarding	Node	SWITCH-FORWARDING-IS-MEMBER-SET-AWARE

Setting Parameters

- **VLAN Learning Type** can be set to the any value from *Combined*, *Independent*, *Shared*.

3. To configure GVRP, set **Run GVRP** is set to *Yes,* and set the dependent parameters listed in Table 2-17.

FIGURE 2-8.   Setting VLAN Parameters

TABLE 2-17.   Command Line Equivalent of VLAN Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Maximum Number of VLANs	Node	`SWITCH-GVRP-MAXIMUM-VLANS`
Interval between GVRP Join Messages	Node	`SWITCH-GARP-JOIN-TIME`
Leave Time	Node	`SWITCH-GARP-LEAVE-TIME`
Interval between GVRP LeaveAll Messages	Node	`SWITCH-GARP-LEAVEALL-TIME`
GVRP Statistics	Node	`SWITCH-GVRP-STATISTICS`

4. To configure VLANs, do the following:

   a. Open the **VLAN Editor** by clicking the **Open VLAN Editor** button**.**
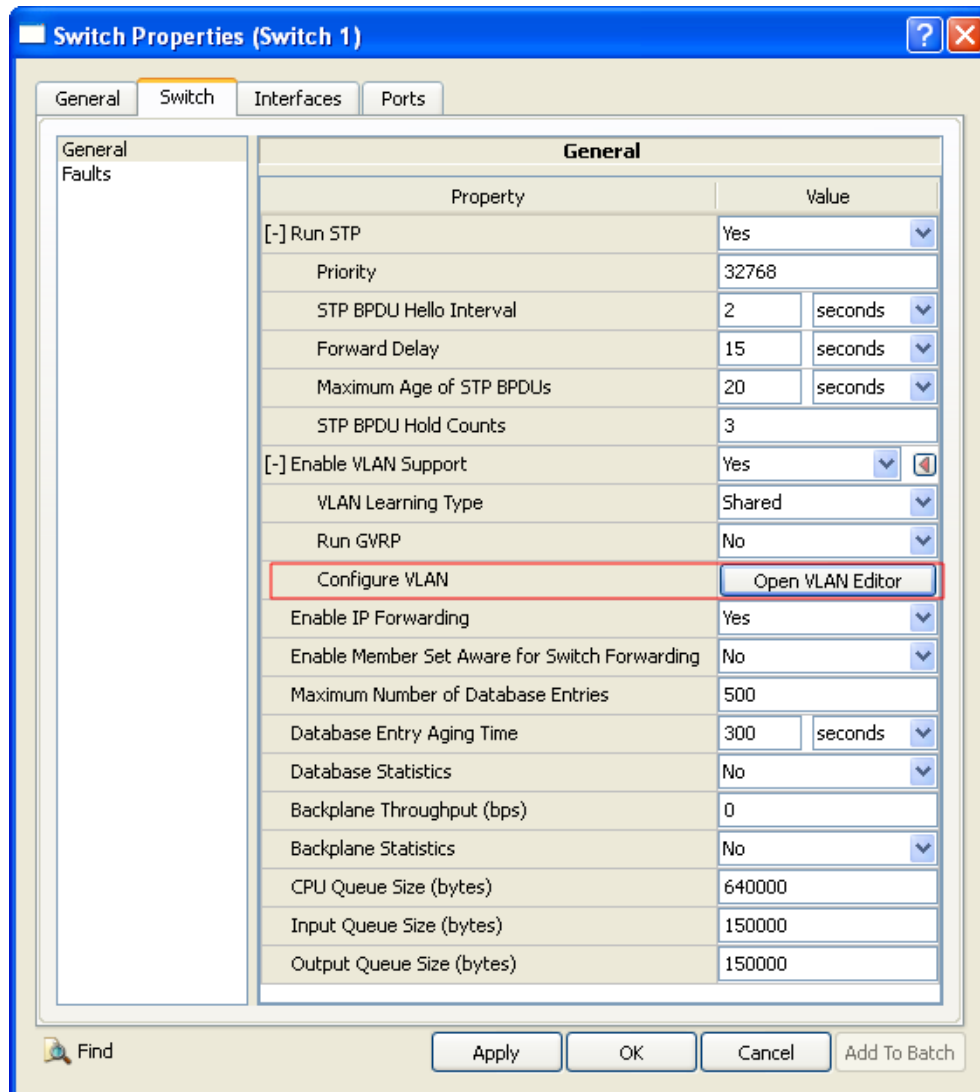
FIGURE 2-9.   Opening VLAN Editor
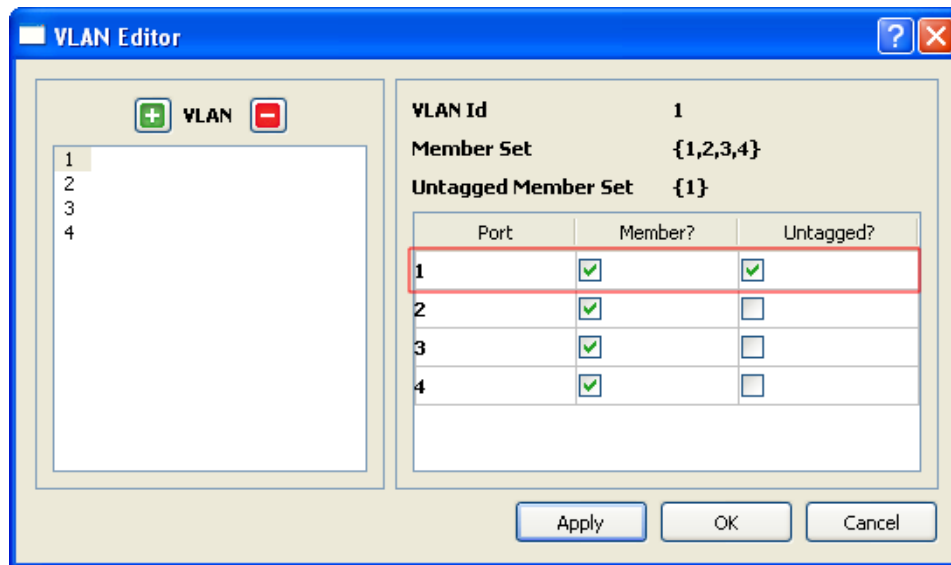
FIGURE 2-10.   Configuring VLANs in the VLAN Editor

b. To create a VLAN, click on the ⊞ button. To delete a VLAN, select the VLAN ID from the list and click on the ⊟ button.

c. To edit the membership of a VLAN, select a VLAN in the left panel. In the right panel, to include a port in the VLAN, check the box in the **Member** column. To mark the port as untagged, check the box in the **Untagged** column.

d. Click the **Apply** or **OK** button.

TABLE 2-18.   Command Line Equivalent of VLAN Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Member Set	Node	`SWITCH-VLAN-MEMBER-SET`
Untagged Member Set	Node	`SWITCH-VLAN-UNTAGGED-MEMBER-SET`

Configuring Port-level Properties

To configure the port-level VLAN parameters, perform the following steps:

1. Go to **Switch Properties Editor > Ports > Port # > VLAN**.

2. Set the parameters listed in Table 2-19.
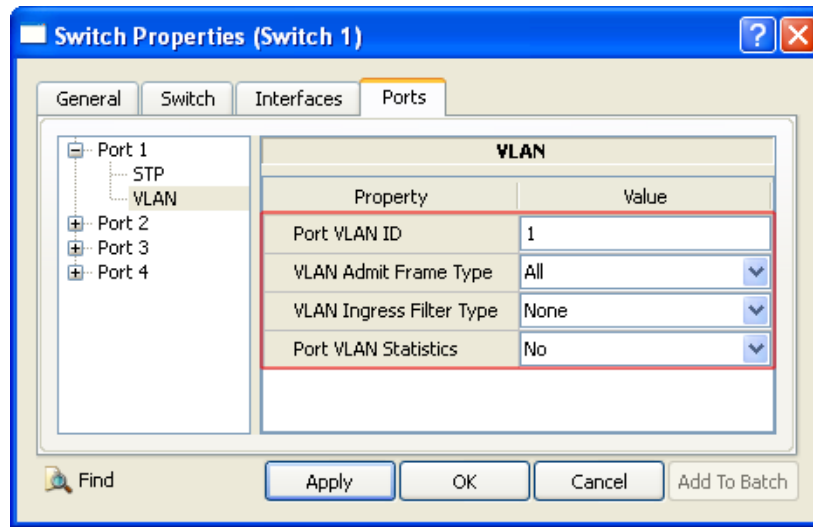
FIGURE 2-11.   Setting VLAN Parameters for Ports

TABLE 2-19.   Command Line Equivalent of Port VLAN Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Port VLAN ID	Node	SWITCH-PORT-VLAN-ID
VLAN Admit Frame Type	Node	SWITCH-PORT-VLAN-ADMIT-FRAMES
VLAN Ingress Filter Type	Node	SWITCH-PORT-VLAN-INGRESS-FILTERING
Port VLAN Statistics	Node	SWITCH-PORT-VLAN-STATISTICS

Configuring VLAN Parameters for Links

To configure the VLAN parameters for a point-to-point link, perform the following steps:

1. Go to **Point-to-point Link Properties Editor > Point-to-point Link Properties > General**.

2. Set the parameters listed in Table 2-20.
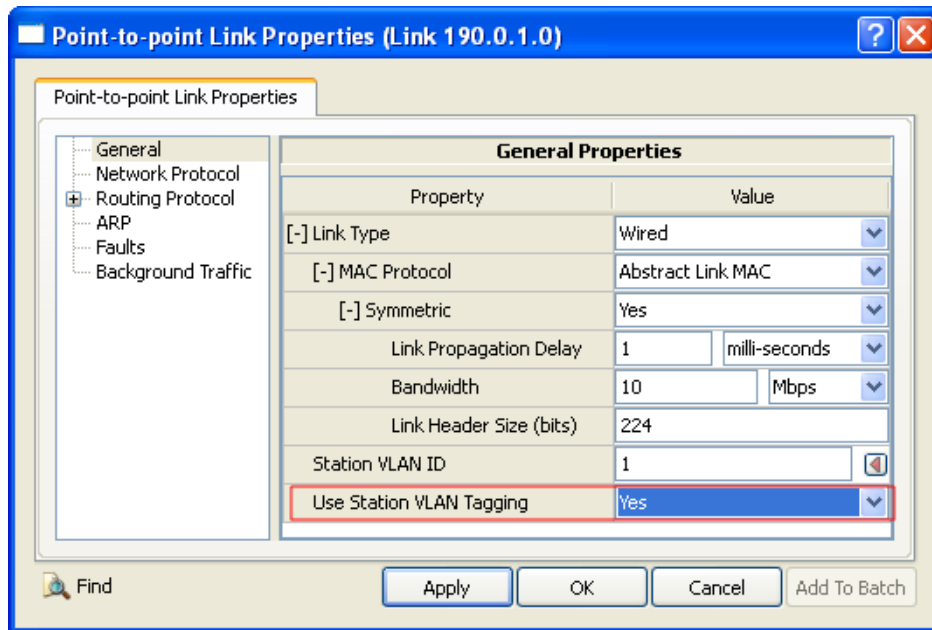
FIGURE 2-12.   Setting VLAN Parameters for Links

TABLE 2-20.   Command Line Equivalent of Link VLAN Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Use Station VLAN Tagging	Node	SWITCH-STATION-VLAN-TAGGING

2.3.4 Statistics

Table 2-21 lists the statistics for the VLAN model that are output to the statistics (.stat) file at the end of simulation.

TABLE 2-21.   VLAN Statistics

Statistic	Description
Total frames received	Total number of frames received from the PHY layer.
Unicast frames forwarded directly	Total number of frames forwarded directly dropped.
Unicast frames flooded	Total number of unicast frames forwarded based on the member set for vlan.
Unicast frames delivered to upper layer	Total number of unicast frames forwarded to upper layers.
Unicast frames dropped	Total number of unicast frames dropped at MAC layer, when the queue is full.
Broadcast frames forwarded	Total number of broadcast frames forwarded.
Broadcast frames dropped	Total number of broadcast frames dropped at MAC layer, when the queue is full.

TABLE 2-21.   VLAN Statistics (Continued)

Statistic	Description
Frames dropped in discard state	Total number of frames dropped when port is disabled.
Frames dropped in learning state	Total number of frames dropped when port is in learning state.
Frames dropped by ingress filtering	Total number of frames due to ingress filtering.

2.3.5 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the VLAN model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/mac-switch/vlan. Table 2-22 lists the sub-directory where each scenario is located.

TABLE 2-22.   VLAN Model Scenarios Included in QualNet

Scenario	Description
sample1	This scenario illustrates the VLAN related configuration for VLAN member sets, untagged sets, port VLAN ID at the switch and switch ports.
sample2	This scenario illustrates multicast in a VLAN aware switched configuration.

2.3.6 References

1. IEEE standard 802.1Q, "Virtual Bridged Local Area Networks." 1998.

2. IEEE standard 802.1u, "Amendment 1: Technical and editorial corrections." 2001.

3. IEEE standard 802.1v, "Amendment 2: VLAN Classification by Protocol and Port." 2001.

3   Network Protocol Models

This chapter describes features, configuration requirements and parameters, statistics, and scenarios for Network Protocol Models, and consists of the following section:

- Mobile IPv4

3.1 Mobile IPv4

The QualNet Mobile IPv4 Model is based on the RFC 2002.

3.1.1 Description

Mobile nodes were not considered when the Internet Protocol (IPv4) was designed. Then and now, a node's IP address, which indicates its point of attachment to the Internet, is assumed to remain unchanged for the duration of a session. Mobile IP, a standard proposed by the Internet Engineering Task Force (IETF), was designed to solve this problem by allowing the mobile node to use two IP addresses: a fixed Home Address and a Care-of Address (COA) that changes at each new point of attachment to the Internet.

Mobility Support for IPv4 defines a protocol that allows transparent routing of IP datagrams to Mobile Nodes as they move about from one domain to another on the Internet. When a Mobile Node moves into a foreign network, its computing activities are not disrupted. Instead, all the needed reconnection occurs automatically and without user interaction. Each mobile node is always identified by its home address, which is static regardless of its current point of attachment to the Internet. While situated away from its home agent, a mobile node is also associated with a care-of-address, which provides information about its current point of attachment to the Internet. When the mobile node is attached to the home network, it operates without any mobility support. Whenever the mobile node is not attached to its home network (and is therefore attached to any foreign network), the home agent gets all the packets destined for the mobile node and arranges to deliver them to the mobile node's current point of attachment. The home agent sends datagrams destined for the mobile node through a tunnel to the care-of-address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node. The mobile IP protocol provides for registering the care-of address with a home agent.

3.1.2 Features and Assumptions

This section describes the implemented features, omitted features, assumptions and limitations of the Mobile IPv4 model

3.1.2.1 Implemented Features
- Foreign agent care-of address.
- Routing of unicast datagrams.

3.1.2.2 Omitted Features
- Routing capabilities in a mobile node.
- Co-located care-of address.
- Authentication.
- Virtual Networks in mobile IP.
- Broadcast and multicast datagram routing for mobile IP.

3.1.2.3 Assumptions and Limitations
- The mobile IPv4 is supported only when OSPFv2 is running as the routing protocol on router nodes.
- The mobile IPv4 is supported only when 802.11MAC is running as the MAC protocol.
- The mobile IPv4 is supported only when the file-based mobility model is configured as mobility model for mobile nodes.
- The Mobile IPv4 model relies on the link layer mechanism to automatically discover the current point of attachment to a network for mobile nodes.

- One foreign network can only contain one foreign agent.
- When the care-of-address of the mobile node is of co-located type, there is no foreign agent for the node.
- One network can have only one home agent and one foreign agent.
- Any wireless node running mobile IPv4 cannot have more than one wireless interfaces.
- Ally agent is the mobile node's default router.

3.1.3 Command Line Configuration

To enable Mobile IPv4, include the following parameter in the scenario configuration (.config) file.

        [<Qualifier>] MOBILE-IP   YES

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of <Qualifier> for each scope.

> **Note:**   The default value of parameter MOBILE-IP is NO.

Configuration Requirements

To use Mobile IPv4, Internet Control Message Protocol (ICMP) must be enabled and every mobile agent should be configured to be an ICMP router, i.e. it should be included in the ICMP router list. Refer to *Developer Model Library* for details of configuring ICMP.

Mobile IPv4 Parameters

Table 3-1 describes the Mobile IPv4 configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 3-1.   Mobile IPv4 Parameters

Parameter	Value	Description
HOME-AGENT *Optional* *Scope:* All	Node-list	List of nodes that will act as home agents.
FOREIGN-AGENT *Optional* *Scope:* All	Node-list	List of nodes that will act as foreign agents.
MOBILE-NODE *Optional* *Scope:* All	Node-list	List of hosts or routers that can be attached to a home or foreign network.
MOBILE-IP-STATISTICS *Optional* *Scope:* Global, Node	List: • YES • NO *Default:* NO	Enables Mobile IPv4 statistics.

3.1.4 Statistics

This section describes the Mobile IPv4 statistics that are output to the statistics (.stat) file at the end of simulation. Table 3-2 lists the statistics collected for a mobile node.

TABLE 3-2.   Mobile IPv4 Statistics Collected for Mobile Node

Statistics	Description
Registration requested	Total number of registration requests initiated from the mobile node for being foreign or home agent.
Registration reply accepted	Total number of registration replies accepted.

Table 3-3 lists the statistics collected for a home agent.

TABLE 3-3.   Mobile IPv4 Statistics Collected for Home Agent

Statistics	Description
Registration request received by Home Agent	Total number of registration requests received by the home agent either from foreign agent or directly from mobile node.
Registration replied by Home Agent	Total number of registration replies generated from the home agent towards the mobile node or foreign agent.
Number of Datagrams Encapsulate by Home Agent	Total number of datagrams encapsulated by home agent.

Table 3-4 lists the statistics collected for a foreign agent.

TABLE 3-4.   Mobile IPv4 Statistics Collected for Foreign Agent

Statistics	Description
Registration request relayed by Foreign Agent	Total number of registration requests relayed to the home agent by the foreign agent.
Registration reply relayed by Foreign Agent	Total number of registration replies relayed to the mobile node by foreign agent.
Number of Datagrams Decapsulate by Foreign Agent	Total number of datagrams decapsulated by foreign agent.

3.1.5 References

1. RFC 2002, "IP Mobility Support" C. Perkins. October 1996.

2. RFC 792, "INTERNET CONTROL MESSAGE PROTOCOL" J. Postel. September 1981.

3. RFC 1256, "ICMP Router Discovery Messages" S. Deering. September 1991.

4 Unicast Routing Protocol Models

This chapter describes features, configuration requirements and parameters, statistics, and scenarios for Unicast Routing Protocol Models, and consists of the following sections:

- Border Gateway Protocol version 4 (BGPv4)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Interior Gateway Routing Protocol (IGRP)
- Open Shortest Path First version 2 (OSPFv2) Routing Protocol
- Open Shortest Path First version 3 (OSPFv3) Routing Protocol

4.1 Border Gateway Protocol version 4 (BGPv4)

The QualNet BGPv4 is based on the following documents:

- RFC 1772
- RFC 2460
- RFC 2461
- RFC 2545
- RFC 2858
- RFC 4271
- RFC 4456

4.1.1 Description

BGP is a distant vector inter Autonomous System (AS) routing protocol which came up after EGP to eliminate the inefficiency of EGP with respect to flexibility and scalability and to give support of an actual routing protocol. BGP handles the scalability problem using Classless Inter-domain Routing (CIDR) and solves the inefficiency of EGP by accumulating all the possible route information to a destination and running a decision process to select a route to use and to advertise to the peers. This also provides some flexibility over EGP in loop detection in the route, hence eliminating some unwanted routes. EGP does not work with topology containing a loop.

The routing vector BGP exchanges with its peers a SEQUENCE or SET of a number through which a packet should traverse to get to the destination. It relies on underlying transport protocol TCP for routing exchange to get rid of the trouble of reliable transfer. After gathering sufficient route information to a destination, BGP runs its decision process to select the possible routes to use for the AS. It also maintains synchronization of route information within an AS through IBGP if there are a number of BGP speakers in the AS, and with other routes through IGP-BGP interaction.

BGPv4 protocol was originally designed to support only IPv4. Multiprotocol extension of BGP (called MBGP) enables BGP to work with different classes of protocols including IPv4/IPv6, multicast/unicast, and VPN/MPLS. Multiprotocol BGP (MBGP) is defined in RFC 2858 (which is the latest RFC version and obsoletes the RFC 2283.) This RFC defines extensions to the existing BGP protocol to allow it to carry more than just IPv4 route prefixes. Examples of some of the new types of routing information include (but are not limited to):

- IPv4 prefixes for Unicast routing.
- IPv4 prefixes for Multicast RPF checking.
- IPv6 prefixes for Unicast routing.

In this project, we particularly focus on extension of BGP to support IPv6/IPv4 protocols. To support the Multiprotocol extension, the UPDATE message in BGPv4 has been modified by adding two new attributes.

MBGP defines the format of two new attributes that can be used to announce and withdraw the announcement of reachability information. The attributes are as follows:

- MP-REACH-NRLI, which specifies new routes to the reachable networks.
- MP-UNREACH-NRLI, which specifies the withdrawn routes.

Furthermore, the new attributes identify the address family (IPv4 or IPv6) and sub-address family (Unicast, Multicast, and so on.) of the routes.

4.1.1.1 Interaction of BGP with IGP Routing Protocols

The routes which are discovered by the BGP advertising mechanism are reflected in the IP forwarding table of the BGP speakers. Therefore, it is required that these routes be advertised by IGP routing protocols inside the subnet or network to which BGP speakers are connected. (Note that each IGP routing protocol has its own specific way for advertising newly learnt routes inside an autonomous system.) The method for distributing routes from one IGP/EGP routing protocol to another IGP/EGP routing protocol is called "route redistribution".

4.1.1.2 BGP Next Hop Implementation

In the BGP legacy implementation, an EBGP speaker modifies the next hop attribute of an incoming UP-DATE message received from an EBGP peer, before forwarding it to the IBGP peers. Since this implementation does not conform to the BGP standard, an alternative solution has been implemented that con-forms to the BGP standard. In the new solution the EBGP speaker shall not modify the next hop attribute of an incoming UPDATE message received from an EBGP peer before forwarding it to the IBGP peers. Instead, the same next-hop value shall be propagated further to the IBGP peers that were received from the external EBGP peer. When BGP Legacy support is disabled, external routes should be defined for the reachable next hop.

4.1.1.3 Route Reflectors

A Route Reflector (RR) is BGP router that is allowed to break the iBGP loop avoidance rule. Route reflectors can advertise updates received from one iBGP peer to another iBGP peer under specific conditions. Route reflectors provide a mechanism for both minimizing the number of update messages transmitted within the AS, and reducing the amount of data that is propagated in each message. The deployment of BGP route reflectors leads to much higher levels of network scalability.

4.1.2 Features and Assumptions

This section describes the implemented features, omitted features, assumptions and limitations of the BGPv4 model.

4.1.2.1 Implemented Features

- Sending and handling OPEN, KEEPALIVE, NOTIFICATION and UPDATE message types.
- Detailed implementation of UPDATE message processing.
- Implementing full set of following states:
    - Predicting and processing any event which may occur in any state.
    - Taking appropriate action for any event.
- Handling errors and taking appropriate action as follows:
    - NOTIFICATION message is sent to notify the BGP peer of an occurred error.
    - Any unexpected message in each state is considered an error.
- Advertising feasible and unfeasible routes to the BGP peers.
- Supporting the policy-based path selection strategies.
- Supporting metric-based path selection.
- Different path attributes in UPDATE messages:
    - Origin
    - Multi Exit Disc (MED)
    - Local Preference
    - AS_PATH (sequence of traversed ASs)

- NEXT_HOP
- Collaborating with IGP in route advertisement as follows:
    - Announcing routes learnt from IGP to BGP peers.
    - Updating RIB by valid existing routes in IP forwarding table.
- Support for both IPv4 and IPv6.
- Use of DualIP within an AS.
- Route Reflectors.

4.1.2.2 Omitted Features

- Route Map.
- Policy based routing.
- Enabling DualIP on BGP speakers.
- Cluster ID in Route Reflectors.
- AS PATH Overflow.

4.1.2.3 Assumptions and Limitations

- BGP speakers are themselves border routers, so all traffic would pass through them.
- Only one version of BGP is used.
- There is no authentication of BGP peer.
- If Dual-IP is enabled within an AS, a BGP speaker with an IPv4 address type advertises only IPv4 routes to the BGP peers. Similarly, a BGP speaker with an IPv6 address will advertise only IPv6 routes.
- Synchronization with IGP is implemented at initialization only. At run time, synchronization with IGP is not implemented.
- When BGP Legacy support is disabled, the end user must define external routes for the reachable next hop. For example, static routes for reachable next hop can be configured at BGP speakers.

4.1.3 Command Line Configuration

To select BGPv4 as the exterior gateway routing protocol, specify the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>]EXTERIOR-GATEWAY-PROTOCOL      BGPv4
```

The scope of this parameter declaration can be Global or Node. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

BGP Parameters

Table 4-1 describes the BGP configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

<div align="center">

TABLE 4-1.   BGP Parameters

</div>

Parameter	Value	Description
`BGP-NEXT-HOP-LEGACY-SUPPORT` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `YES`	Specifies whether BGP Legacy implementation is enabled or disabled. **Note:** For more information on BGP Legacy implementation, refer to Section 4.1.1.2.
`BGP-START-TIME` Optional *Scope:* Global, Node	Time *Range:* ≥ `0S` *Default:* `0S`	Specifies the time when the BGP router starts its operation.
`BGP-HOLD-TIME-INTERVAL` Optional *Scope:* Global, Node	Time *Range:* `[3S, 65535S)` *Default:* `90S`	Specifies the length of time a speaker will wait to listen for activities from a peer.
`BGP-LARGE-HOLD-TIME-INTERVAL` Optional *Scope:* Global, Node	Time *Range:* `(0S, 65535S)` *Default:* `4M`	Specifies the hold time in active state.
`BGP-MIN-RT-ADVERTISEMENT-INTERVAL-IBGP` Optional *Scope:* Global, Node	Time *Range:* `(0S, 65535S)` *Default:* `5S`	Specifies the interval between two subsequent update messages for internal peers.
`BGP-MIN-RT-ADVERTISEMENT-INTERVAL-EBGP` Optional *Scope:* Global, Node	Time *Range:* `(0S, 65535S)` *Default:* `30S`	Specifies the interval between two subsequent update messages for external peers.
`BGP-MIN-AS-ORIGINATION-INTERVAL` Optional *Scope:* Global, Node	Time *Range:* `(0S, 65535S)` *Default:* `15S`	Specifies the interval between two subsequent update messages for internal peers.
`BGP-KEEPALIVE-INTERVAL` Optional *Scope:* Global, Node	Time *Range:* `(0S, 65535S)` *Default:* `30S`	Specifies the interval between two successive keep alive messages.

TABLE 4-1.   BGP Parameters (Continued)

Parameter	Value	Description
`BGP-CONNECT-RETRY-INTERVAL` Optional *Scope:* Global, Node	Time *Range:* ≥ `0S` *Default:* `120S`	Specifies the length of time to wait before re-opening a TCP connection.
`BGP-ROUTE-WAITING-INTERVAL` Optional *Scope:* Global, Node	Time *Range:* ≥ `0S` *Default:* `15S`	Specifies the length of time to wait to determine if a neighbor is no longer reachable.
`BGP-CONFIG-FILE` Required *Scope:* Global	Filename	Name of the BGP configuration file. The BGP configuration file is used to configure BGP routers. The format of the BGP configuration file is described in Section 4.1.3.1.
`EXTERIOR-GATEWAY-PROTOCOL-STATISTICS` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Specifies whether exterior gateway protocol statistics are collected.

4.1.3.1 Format of the BGP Configuration File

The BGP configuration (.bgp) file contains the configuration parameters for one or more BGP routers. The BGP configuration file describes the relationship between each BGP router and its neighbors and the interaction of a BGP router with the IGP protocols.

A BGP router configuration consists of the following elements in the following order:

```
<Router ID Specification>
<Networks Specification>
<Neighbor AS Specification>
<Neighbor Route Reflector Client Specification>
<Neighbor Weight Specification>
<Neighbor Default Metric Specification>
<Local Preference Specification>
<Default Metric Specification>
<IGP Route Synchronization Indication>
<IGP Route Advertisement Indication>
<BGP Probe Interval Specification>
<Route Redistribution Indication>
```

These elements are described in Table 4-2.

TABLE 4-2.   BGP Router Configuration Parameters

Element	Description
`<Router ID Specification>`	The router ID specification associates a BGP speaker with an autonomous system and has the following format: ROUTER `<node-ID>` BGP `<AS-ID>` where `<node-ID>` Node ID of the router `<AS-ID>` ID of the autonomous system with which the router is associated
`<Networks Specification>`	The networks specification identifies all networks to which the BGP speaker belongs and consists of one or more occurrences of the following line: NETWORK `<IP-address>` where `<IP-address>` IP address of the network to which the BGP speaker belongs **Notes**: 1. At least one network address must be specified for each BGP speaker. 2. All network addresses specified for a BGP speaker should be of the same type (IPv4 or IPv6).
`<Neighbor AS Specification>`	The neighbor AS specification identifies the IP address and autonomous system ID of the neighboring BGP speakers of the BGP speaker and consists of one or more occurrences of the following line: NEIGHBOR `<IP-address>` REMOTE-AS `<AS-ID>` where `<IP-address>` IP address of the neighboring BGP speaker `<AS-ID>` AS ID of the autonomous system to which the neighbor belongs.
`<Neighbor Route Reflector Client Specification>`	The neighbor route reflector client specification identifies the neighboring BGP speakers that is configured as the route reflector clients and consists of zero or more occurrences of the following line: NEIGHBOR `<IP-address>` ROUTE-REFLECTOR-CLIENT where `<IP-address>` IP address of the neighboring BGP speaker

TABLE 4-2.   BGP Router Configuration Parameters (Continued)

Element	Description
`<Neighbor Weight Specification>`	The neighbor weight specification specifies the weight associated with each of the neighboring BGP speakers of a BGP speaker and consists of one or more occurrences of the following line: `NEIGHBOR <IP-address> WEIGHT <weight>` where `<IP-address>` IP address of the neighboring BGP speaker `<weight>` Weight associated with the neighboring BGP speaker. This should be an integer in the range 0 to 65535. A higher weight means the speaker is more preferred. The default value is 0.
`<Neighbor Default metric Specification>`	The default metric specification specifies the multi-exit discriminator and consists of zero or one occurrence of the following line: `NEIGHBOR <IP-address> DEFAULT-METRIC <metric>` where `<IP-address>` IP address of the neighboring BGP speaker `<metric>` Multi-exit discriminator. The metric is used to decide the best route externally or outside the AS. MED's are passed and received in UPDATE messages. This should be a non-negative integer. **Note:** This parameter is optional. If this parameter is not included, then the default multi-exit discriminator is 0.
`<Local Preference Specification>`	The local preference specification specifies the local preferences for internal paths and consists of zero or one occurrence of the following line: `DEFAULT-LOCAL-PREFERENCE <preference>` where `<preference>` Specifies the local preferences for internal paths. The preference is used to select the best route internally. Routes with the highest local preference are selected. BGP speaker sends and receives this preference in UPDATE messages, if the message is sent internally or within an AS. This should be a non-negative integer. **Note:** This parameter is optional. If this parameter is not included, then the default local preference is 100.

TABLE 4-2.   BGP Router Configuration Parameters (Continued)

Element	Description
`<Default Metric Specification>`	The default metric specification specifies the multi-exit discriminator and consists of zero or one occurrence of the following line: `DEFAULT-METRIC <metric>` where `<metric>` — Multi-exit discriminator. The metric is used to decide the best route externally or outside the AS. MED's are passed and received in UPDATE messages. This should be a non-negative integer. **Note:** This parameter is optional. If this parameter is not included, then the default multi-exit discriminator is 0.
`<IGP Route Synchronization Indication>`	The IGP route synchronization indication specifies that IGP routes are not synchronized and consists of zero or one occurrence of the following line: `NO SYNCHRONIZATION` **Note:** This parameter is optional. If this parameter is not included, then IGP routes are synchronized.
`<IGP Route Advertisement Indication>`	The IGP route advertisement indication specifies that IGP routes are not injected into BGP and consists of zero or one occurrence of the following line: `NO-ADVERTISEMENT-FROM-IGP` **Note:** This parameter is optional. If this parameter is not included, then IGP routes are injected into BGP.
`<BGP Probe Interval Specification>`	The BGP probe interval specification specifies the BGP probe interval and consists of zero or one occurrence of the following line: `BGP-PROBE-IGP-INTERVAL <interval>` where `<interval>` BGP probe interval. A BGP speaker re-advertises the update message to its neighbors once every probe interval. This should be specified as a time value. **Note:** This parameter is optional. If this parameter is not included, then BGP probe interval is 10M.
`<Route Redistribution Indication>`	The route redistribution indication specifies that redistribution to OSPFv2 is disabled and consists of zero or one occurrence of the following line: `NO-REDISTRIBUTION-TO-OSPF` **Note:** This parameter is optional. If this parameter is not included, then route redistribution to OSPFv2 is enabled.

Example of BGP Configuration File

The following example shows how BGP neighbors in an Autonomous System (AS) are configured to share information. The topology of the scenario is shown in Figure 4-1.
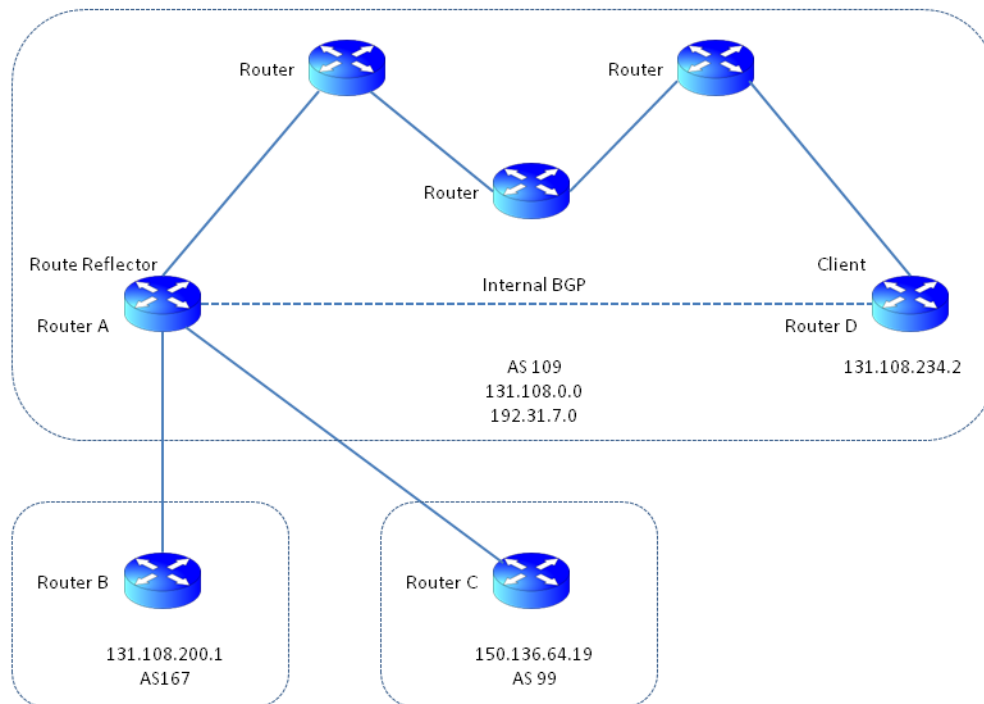
FIGURE 4-1.   Sample BGP Scenario

Router A (whose node ID is 1) is in AS 109 and shares information about networks 131.108.0.0 and 192.31.7.0 with the neighboring routers.

Router B is in AS 167 and its IP address on the BGP connection is 131.108.200.1.

Router C is in AS 99 and its IP address on the BGP connection is 150.136.64.19.

Router D is also in AS 109 and its IP address on the BGP connection is 131.108.234.2.

Because Routers A, B and C are in different ASes, Router A is directly connected to Routers B and C. Since Routers A and D are in the same AS, they need not be directly connected router.

Router A is a route reflector and Router D is its client.

The following lines in the BGP configuration file configure Router A:

```
ROUTER 1 BGP 109
NETWORK 131.108.0.0
NETWORK 192.31.7.0
NEIGHBOR 131.108.200.1 REMOTE-AS 167
NEIGHBOR 131.108.234.2 REMOTE-AS 109
NEIGHBOR 131.108.234.2 ROUTE-REFLECTOR-CLIENT
NEIGHBOR 150.136.64.19 REMOTE-AS 99

#To specify weight associated with each BGP speaker
NEIGHBOR 131.108.200.1 WEIGHT 100
NEIGHBOR 131.108.234.2 WEIGHT 70
NEIGHBOR 150.136.64.19 WEIGHT 90

#Default local preference is set to 250
DEFAULT LOCAL-PREFERENCE 250

#Default metric is set to 1500
DEFAULT-METRIC 1500

#IGP routes are synchronized
#NO SYNCHRONIZATION

#To inject IGP routes into BGP
#NO-ADVERTISEMENT-FROM-IGP

#BGP probe interval is set to 50S
BGP-PROBE-IGP-INTERVAL 50S
```

4.1.4 GUI Configuration

This section describes how to configure BGP in the GUI.

Configuration Requirements

To configure BGP parameters, hierarchies should be designated as Autonomous Systems.

To configure a hierarchy as an Autonomous Systems, perform the following steps:

1. Go to **Hierarchy Properties Editor > General**.

2. Set **Autonomous System** to *Yes* and enter an integer value for the autonomous system ID in the **Autonomous System ID** field.
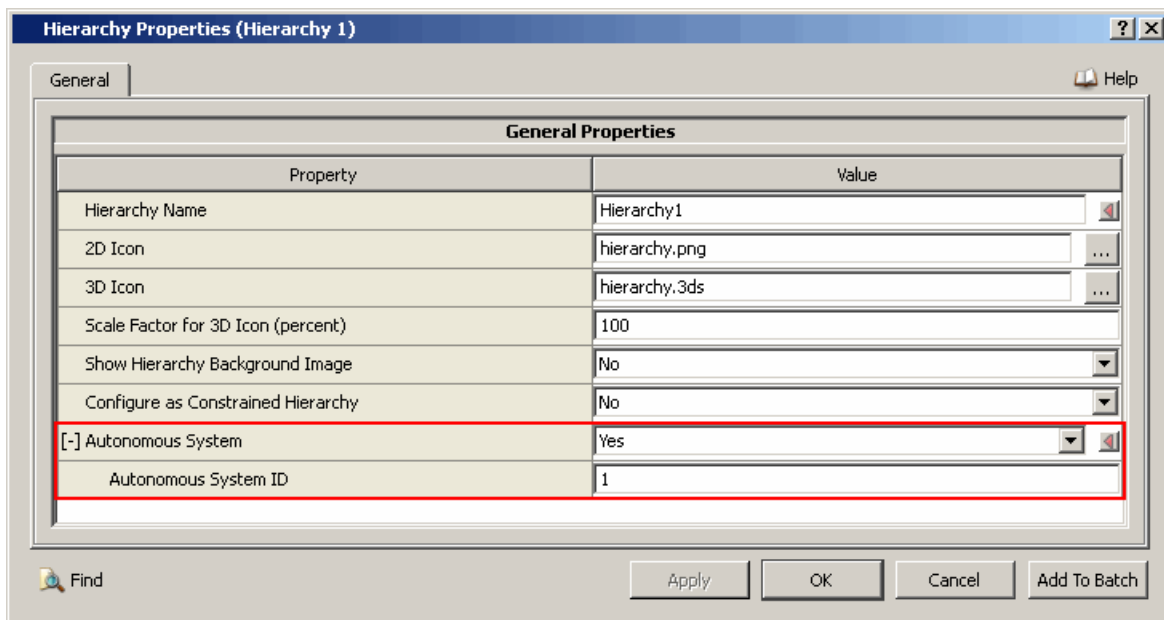
FIGURE 4-2.   Setting Autonomous System Parameters

Adding IBGP Links

To create an IBGP link (connecting two nodes within a hierarchy), perform the following steps:

1. Configure the hierarchy as an autonomous system, as described above.

2. Open the hierarchy by either double-clicking on the hierarchy or right-clicking on the hierarchy and selecting **Open** from the menu.

3. Connect the two nodes by a point-to-point link or a wired or wireless subnet.

4. Select BGP Link by clicking the [icon] button on the Links toolbar of the Standard Toolset.

5. Create a BGP link between the nodes by clicking on one node, dragging the mouse to the other, and releasing.

Adding EBGP Links

To create an EBGP Link (connecting two nodes in different hierarchies), perform the following steps:

1. Configure the hierarchies as autonomous systems, as described above.

2. Open each hierarchy by either double-clicking on the hierarchy or right-clicking on the hierarchy and selecting **Open** from the menu.

3. Connect the two nodes (one in each hierarchy) by a point-to-point link or a wired or wireless subnet.

4. Select BGP Link by clicking the [icon] button on the Links toolbar of the Standard Toolset.

5. Create a BGP link between the nodes by clicking on one node, dragging the mouse to the other, and releasing.

Configuring BGP Parameters

To configure the BGP parameters, perform the following steps:

1. Go to one of the following locations:

   - To set properties for a specific point-to-point link, go to **Point-to-point Link Properties Editor > Point-to-point Link Properties > Routing Protocol > BGP Configuration**.

   - To set properties for a specific node, go to **Default Device Properties Editor > Node Configuration > Routing Protocol > BGP Configuration**.

   In this section, we show how to configure BGP parameters for a specific node using the Default Device Properties Editor. Parameters can be set in the other properties editors in a similar way.

2. Set the parameters shown below and listed in Table 4-3.
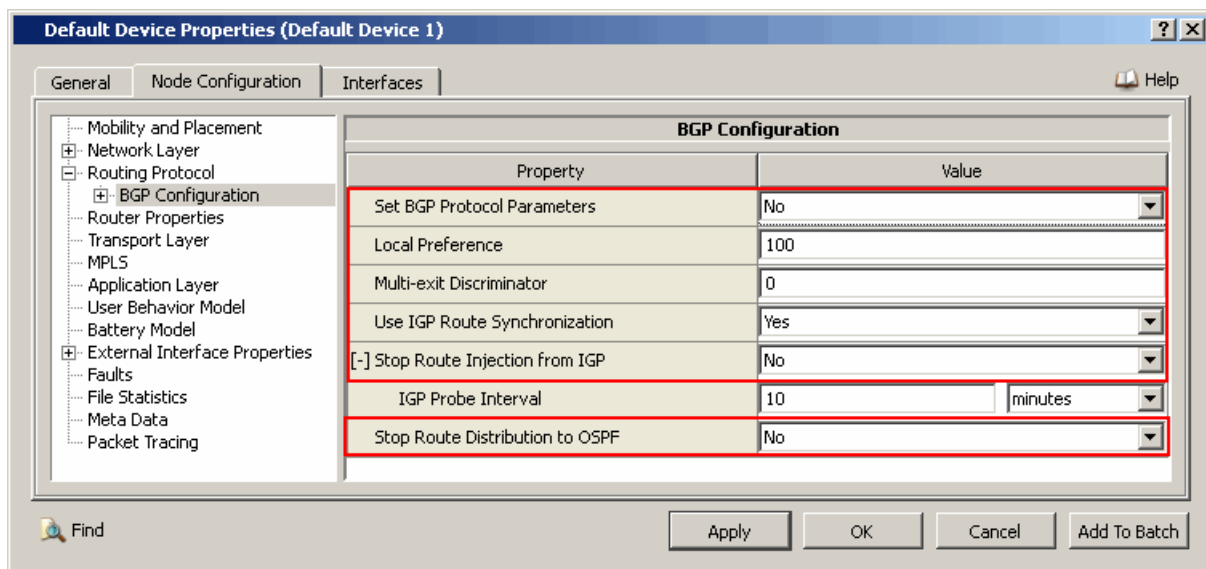
FIGURE 4-3.   Setting BGP Parameters

TABLE 4-3.   Command Line Equivalent of BGP Protocol Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Set BGP Protocol Parameters	Node, Point-to-point Link	N/A
Local Preference	Node, Point-to-point Link	`DEFAULT-LOCAL-PREFERENCE`
Multi-exit Discriminator	Node, Point-to-point Link	`DEFAULT-METRIC`

TABLE 4-3. Command Line Equivalent of BGP Protocol Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Use IGP Route Synchronization	Node, Point-to-point Link	NO SYNCHRONIZATION
Stop Route Injection from IGP	Node, Point-to-point Link	NO-ADVERTISEMENT-FROM-IGP
Stop Route Distribution to OSPF	Node, Point-to-point Link	NO-REDISTRIBUTION-TO-OSPF

Setting Parameters

- To specify BGP Protocol parameters, set **Set BGP Protocol Parameters** to *Yes*; otherwise, set **Set BGP Protocol Parameters** to *No*.

- To disable route injection from IGP, set **Stop Route Rejection from IGP** to *Yes*; otherwise, set **Stop Route Rejection from IGP** to *No*.

- To stop redistribution of OSPF from BGP, set **Stop Route Distribution to OSPF** to *Yes*; otherwise, set **Stop Route Distribution to OSPF** to *No.*

3. If **Set BGP Protocol Parameters** is set to *Yes*, then set the dependent parameters listed in Table 4-4.
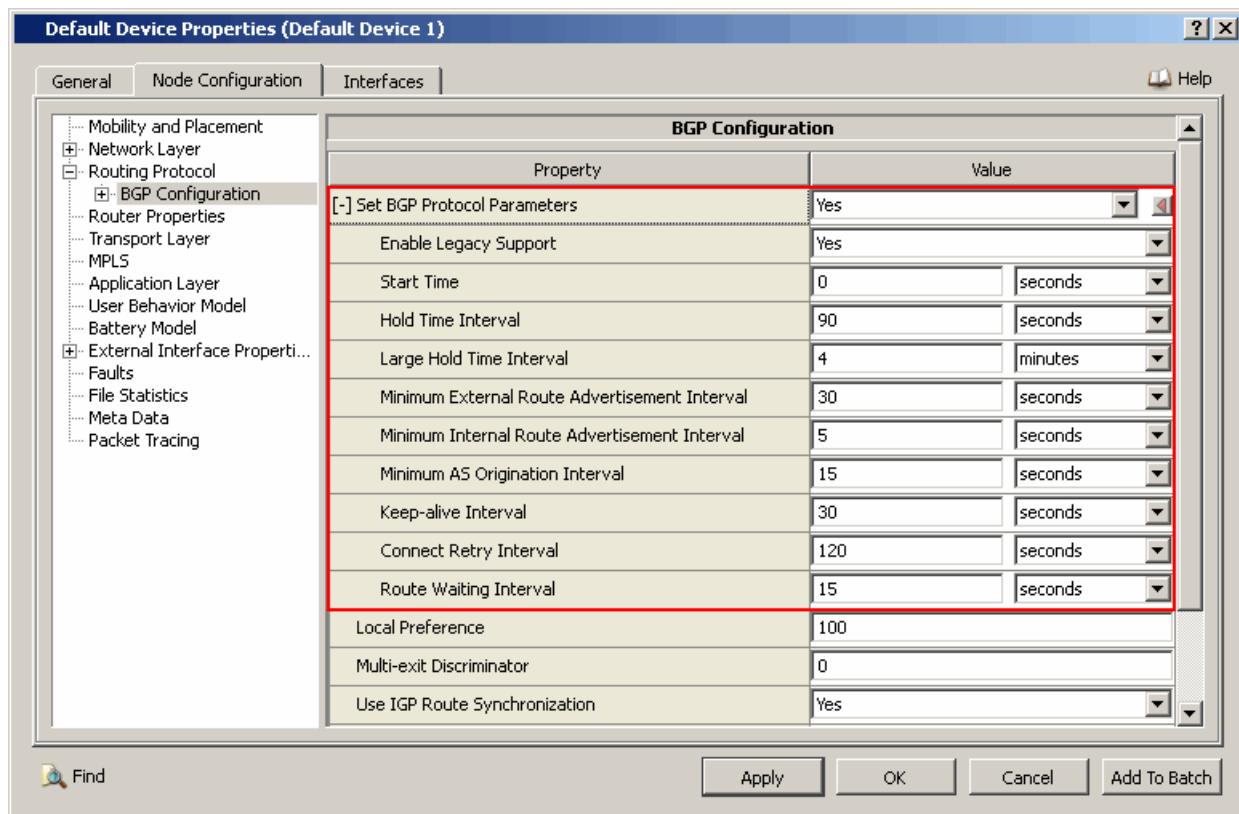
FIGURE 4-4. Setting BGP Protocol Parameters

TABLE 4-4.　Command Line Equivalent of BGP Protocol Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Enable Legacy Support	Node, Point-to-point Link	`BGP-NEXT-HOP-LEGACY-SUPPORT`
Start Time	Node, Point-to-point Link	`BGP-START-TIME`
Hold Time Interval	Node, Point-to-point Link	`BGP-HOLD-TIME-INTERVAL`
Large Hold Time Interval	Node, Point-to-point Link	`BGP-LARGE-HOLD-TIME-INTERVAL`
Minimum External Route Advertisement Interval	Node, Point-to-point Link	`BGP-MIN-RT-ADVERTISEMENT-INTERVAL-IBGP`
Minimum Internal Route Advertisement Interval	Node, Point-to-point Link	`BGP-MIN-RT-ADVERTISEMENT-INTERVAL-EBGP`
Minimum AS Origination Interval	Node, Point-to-point Link	`BGP-MIN-AS-ORIGINATION-INTERVAL`
Keep-alive Interval	Node, Point-to-point Link	`BGP-KEEPALIVE-INTERVAL`
Connect Retry Interval	Node, Point-to-point Link	`BGP-CONNECT-RETRY-INTERVAL`
Route Waiting Interval	Node, Point-to-point Link	`BGP-ROUTE-WAITING-INTERVAL`

4. If **Stop Route Rejection from IGP** is set to *No*, then set the dependent parameters shown in Figure 4-5.
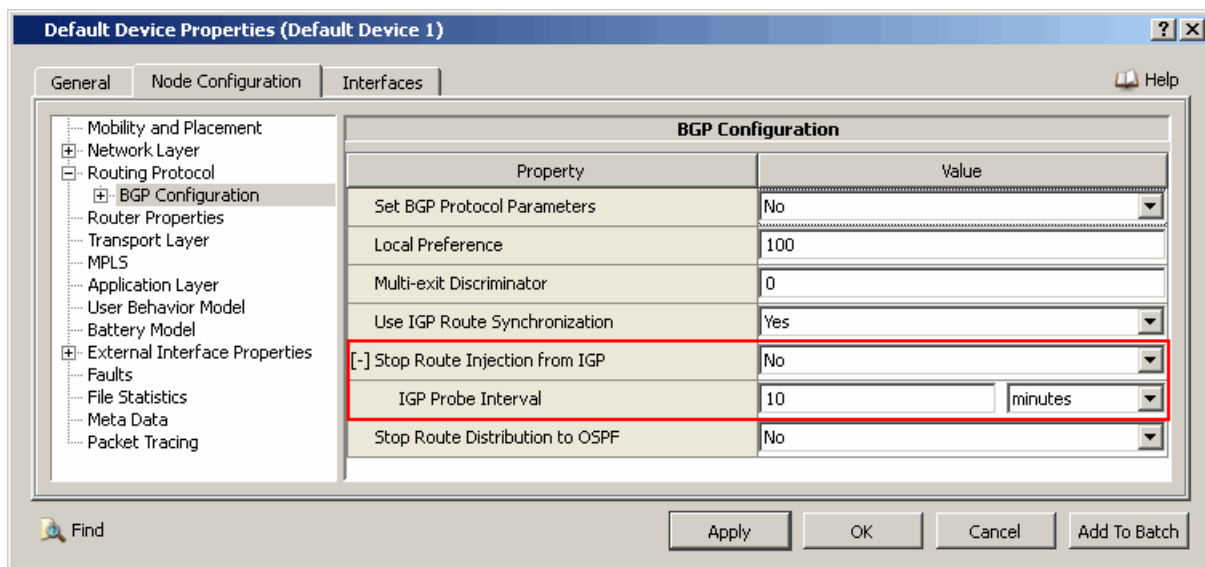
FIGURE 4-5.　Set IGP Probe Interval

Configuring Advertised Networks and Neighbor Parameters

To configure the networks to be advertised by a BGP speaker, perform the following steps:

1. Go to **Default Device Properties Editor > Node Configuration > Routing Protocol > BGP Configuration > Networks Advertised**.

2. Check the appropriate **Network Address** box that needs to be advertised.
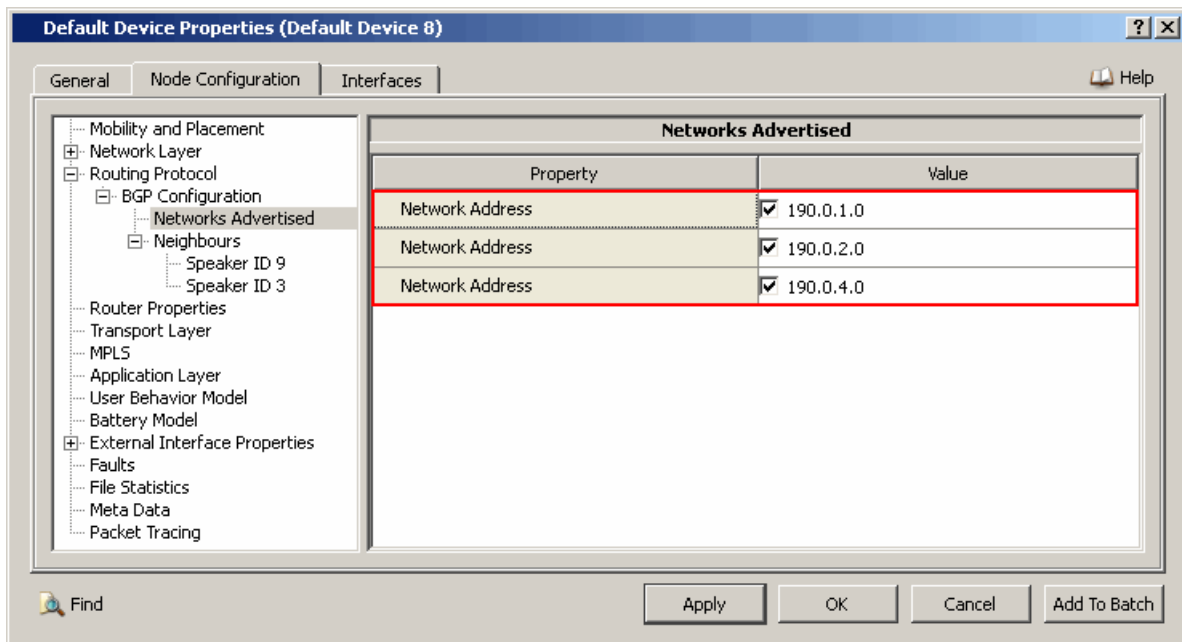
FIGURE 4-6. Setting Networks Advertised Parameters

To configure neighbor parameters, perform the following steps:

1. Go to **Default Device Properties Editor > Node Configuration > Routing Protocol > BGP Configuration > Neighbors > Speaker ID #**.

2. Set **Weight Assigned**, as shown in Figure 4-7.
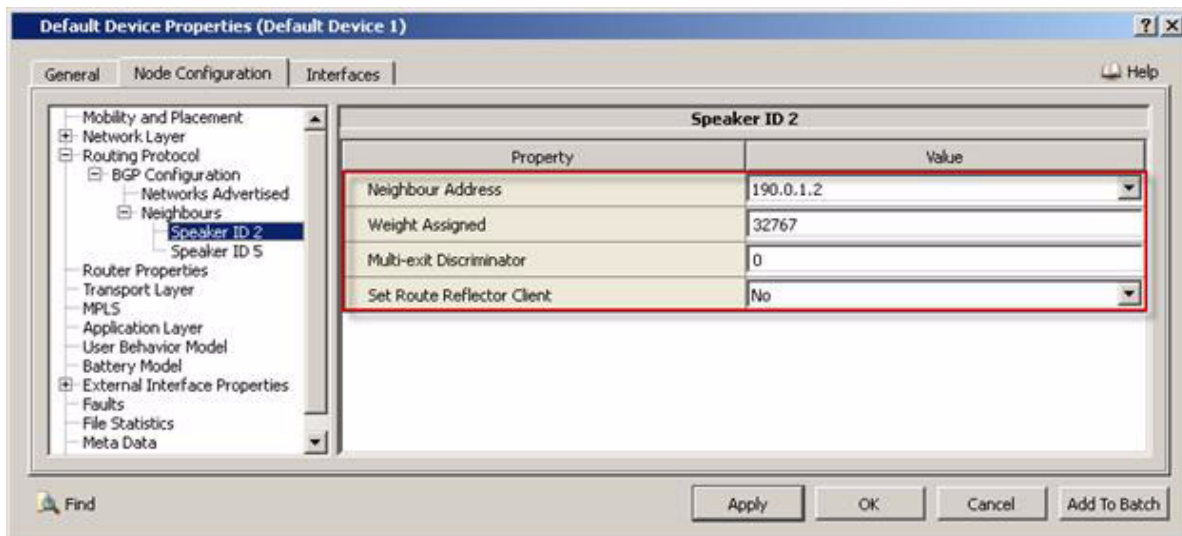
FIGURE 4-7. Setting Neighbor- specific Parameters

Setting Parameters

- Set **Neighbour Address** to the interface address of the Neighbor that is connected to the BGP speaker.

- **Weight Assigned** should be between 0 and 32767 (both inclusive).

- To set **Multi-exit Discriminator** for a specific neighbor, set the value as desired.

- To configure Neighbor BGP speaker as Route Reflector Client, set **Is Route Reflector Client?** to *Yes*; otherwise set **Is Route Reflector Client?** to *No.*

Configuring Statistics Parameters

Statistics for BGP can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for routing protocols including BGP, check the box labeled **BGP** in the appropriate properties editor.

TABLE 4-5.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
BGP	Global, Node	`EXTERIOR-GATEWAY-PROTOCOL-STATISTICS`

4.1.5 Statistics

Table 4-6 lists the BGPv4 statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 4-6.   BGPv4 Statistics

Statistic	Description
Open Messages Sent	Total number of open messages sent to the BGP peer.
Keep Alive Messages Sent	Total number of keep alive messages sent to the BGP peer.
Update Messages Sent	Total number of update messages sent to the peer.
Notification Messages Sent	Total number of notification messages sent to the peer.
Open Messages Received	Total number of open messages received by BGP peer.
Keep Alive Messages Received	Total number of keep alive messages received from the BGP peer.
Update Messages Received	Total number of update messages received from the peer.
Notification Messages Received	Total number of notification messages received from the peer.
Reflected Update Messages Sent	Total number of reflected update messages sent by BGP Route Reflector to its BGP peers.

4.1.6 Sample Scenario

In this section, we provide a scenario to verify the functionality of BGP. The scenario topology is shown in Figure 4-8.

FIGURE 4-8.   Sample Scenario Topology

4.1.6.1 Scenario Description

The topology of the scenario contains the following:

- Number of Hierarchies: 3
- Total number of nodes: 9
- Nodes are connected by wired links (as shown in Figure 4-8.)
- Nodes 1, 4, 5, and 8 are BGP speakers.
- The routing protocol within AS is OSPFv2.
- On EBGP links (links between nodes 1 and between nodes 5 and 8), the routing protocol is configured as NONE.
- One CBR application is configured from node 2 to node 9.
- BGP NEXT HOP support is disabled.

4.1.6.2 Command Line Configuration

The key configuration parameters for the BGP sample scenario are shown below.

Scenario Configuration File

```
# The scenario is executed for a simulation time of 10 minutes.

SIMULATION-TIME 10M
SUBNET N8-190.0.1.0 {1 thru 3}
SUBNET N8-190.0.2.0 {5 thru 7}
LINK N8-190.0.3.0 { 4, 5 }
LINK N8-190.0.5.0 { 8, 9 }
LINK N8-190.0.6.0 { 1, 4 }
LINK N8-190.0.7.0 { 5, 8 }
[1 thru 9]      ROUTING-PROTOCOL OSPFv2
[ N8-190.0.6.0 ]  ROUTING-PROTOCOL NONE
[ N8-190.0.7.0 ]  ROUTING-PROTOCOL NONE
EXTERIOR-GATEWAY-PROTOCOL  BGPv4
BGP-CONFIG-FILE sample.bgp

BGP-NEXT-HOP-LEGACY-SUPPORT NO

[4 5]           STATIC-ROUTE YES
[4 5]           STATIC-ROUTE-FILE sample.routes-static
APP-CONFIG-FILE   sample.app
```

BGP Configuration File (sample.bgp)

```
ROUTER 1 BGP 1
NETWORK N8-190.0.1.0
NETWORK N8-190.0.6.0
NEIGHBOR 190.0.6.2 REMOTE-AS 2
DEFAULT LOCAL-PREFERENCE 250
DEFAULT-METRIC 100
BGP-PROBE-IGP-INTERVAL 60S

ROUTER 4 BGP 2
NEIGHBOR 190.0.1.1 REMOTE-AS 1
NEIGHBOR 190.0.6.1 REMOTE-AS 2
ROUTER 5 BGP 2
NEIGHBOR 190.0.4.2 REMOTE-AS 3
NEIGHBOR 190.0.3.1 REMOTE-AS 2
DEFAULT LOCAL-PREFERENCE 250
DEFAULT-METRIC 100
BGP-PROBE-IGP-INTERVAL 60S

ROUTER 8 BGP 3
NETWORK N8-190.0.4.0
NETWORK N8-190.0.5.0
NETWORK N8-190.0.7.0
NEIGHBOR 190.0.3.2 REMOTE-AS 2
DEFAULT LOCAL-PREFERENCE 250
DEFAULT-METRIC 100
BGP-PROBE-IGP-INTERVAL 60S

#IGP routes are synchronized
#NO SYNCHRONIZATION

#To inject IGP routes into BGP
#NO-ADVERTISEMENT-FROM-IGP

#To inject BGP routes into OSPFv2
#NO-REDISTRIBUTION-TO_OSPF
```

Applications Configuration File (sample.app)

```
CBR 1 9 100 512 1S 15M 25M PRECEDENCE 0
```

Static Routes File (sample.static-routes)

```
5   N8-190.0.6.0 190.0.3.1
4   N8-190.0.7.0 190.0.3.2
```

4.1.6.3 GUI Configuration

To configure the sample scenario in GUI, perform the following steps:

1. Create a new scenario. Go to **Scenario Properties Editor > General**.

    - Set **Experiment Name** to *sample*.
    - Set **Simulation Time** to *10 minutes*.

2. Place three hierarchies on the canvas.

3. For Hierarchy 1, go to **Hierarchy Properties Editor > General**.

    - Set **Autonomous System** to *Yes*.
    - Set **Autonomous system ID** to *AS-1*.

4. Open Hierarchy 1 and place three default nodes and a Hub on the canvas, Create wired links between them as shown in Figure 4-9.
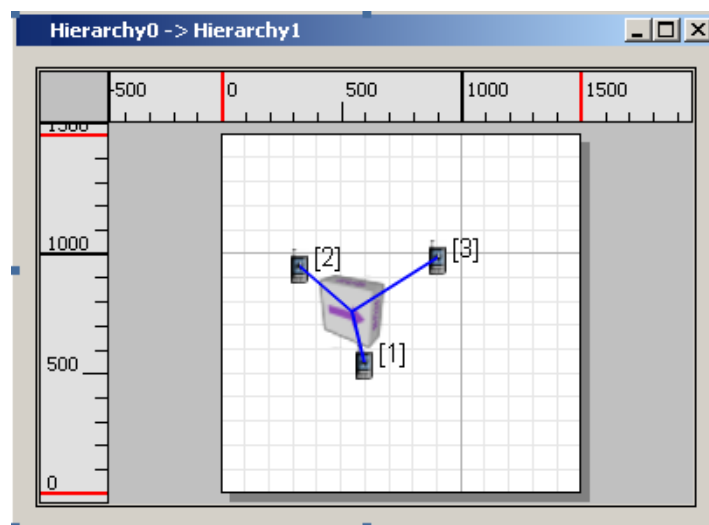
FIGURE 4-9.   Hierarchy 1

5. For Hierarchy 2, go to **Hierarchy Properties Editor > General**.

    - Set **Autonomous System** to *Yes*.
    - Set **Autonomous system ID** to *AS-2*.

6. Open Hierarchy 2 and place 4 nodes and a Hub. Create links between them as shown in Figure 4-10.
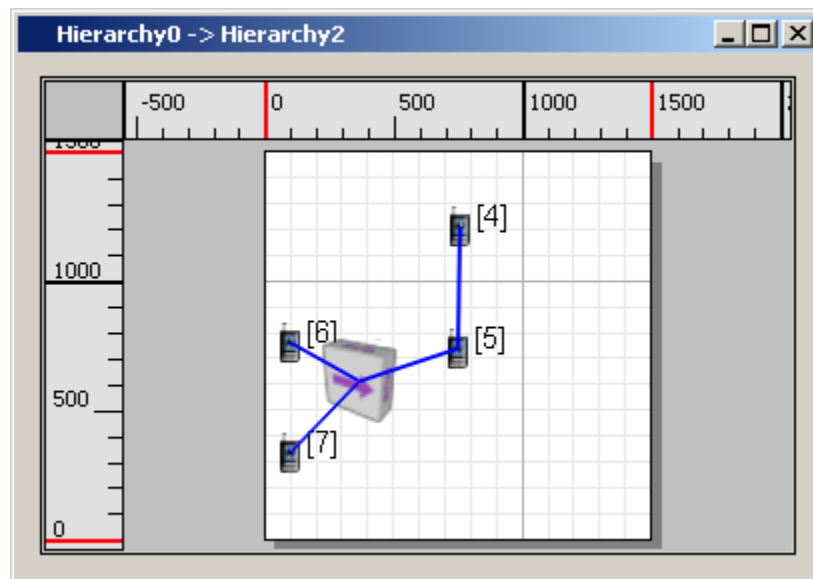
FIGURE 4-10.   Hierarchy 2

7. For Hierarchy 3, go to **Hierarchy Properties Editor > General**.

- Set **Autonomous System** to *Yes*.
- Set **Autonomous system ID** to *AS-3*.

8. Open Hierarchy 3 and place 2 nodes. Create a link between them as shown in Figure 4-11.
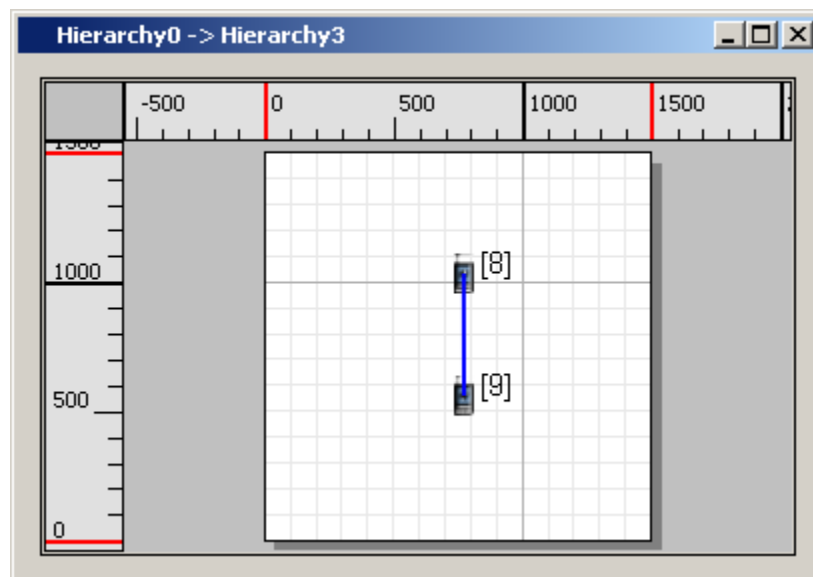
FIGURE 4-11.   Hierarchy 3

9. Create BGP Links.

    - Create an EBGP Link between Nodes 1 and 4 as specified in Section 4.1.6.1.
    - Create an EBGP Link between Nodes 5 and 8 as specified in Section 4.1.6.1.
    - Create an IBGP Link between Nodes 4 and 5 as specified in Section 4.1.6.1.

Set BGP Protocol Parameters

For nodes 1, 4, 5, and 8. Go to **Default Device Properties Editor > Node Configuration > Routing Protocol > BGP Configuration** and set the following parameters:

    - Set **BGP Protocol Parameters** to *Yes.*
    - Set **Enable Legacy Support** to *Yes.*
    - Set **Stop Route Injection from IGP** to *No.*
    - Set **IGP Probe Interval** to 1 minute.

FIGURE 4-12.   Setting BGP Parameters

Configuring Routing Protocol

1. For all nodes, go to **Default Device Properties Editor > Node Configuration > Routing Protocol** and set **Routing Protocol IPv4** to *OSPFv2*.
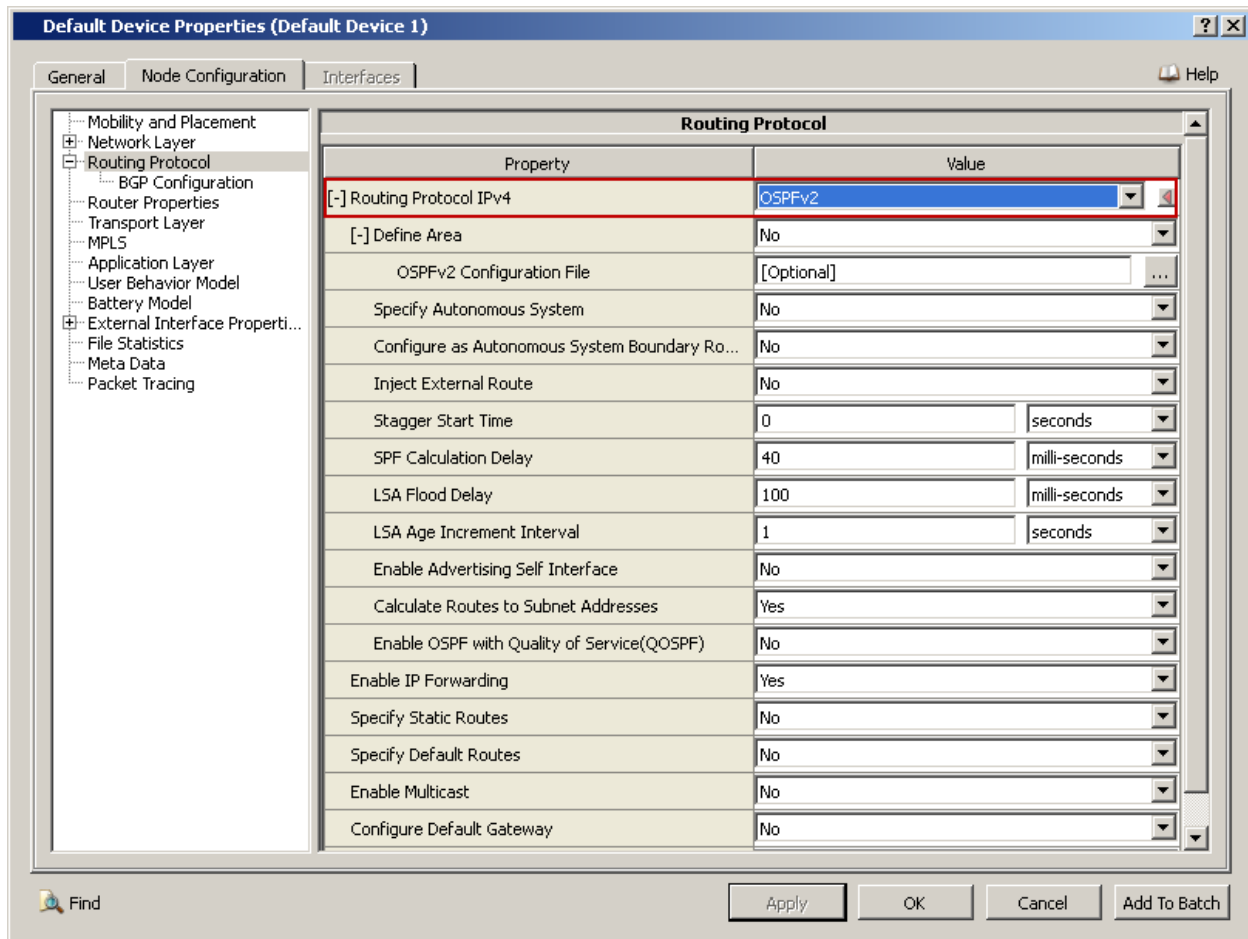
FIGURE 4-13.   **Configure Routing Protocol for Nodes**

2. For links connecting nodes 1 to 4 and node 5 to 8, go to **Point-to-point Link Properties Editor > Routing Protocol** and set **Routing Protocol IPv4** to *None (*Figure 4-14).
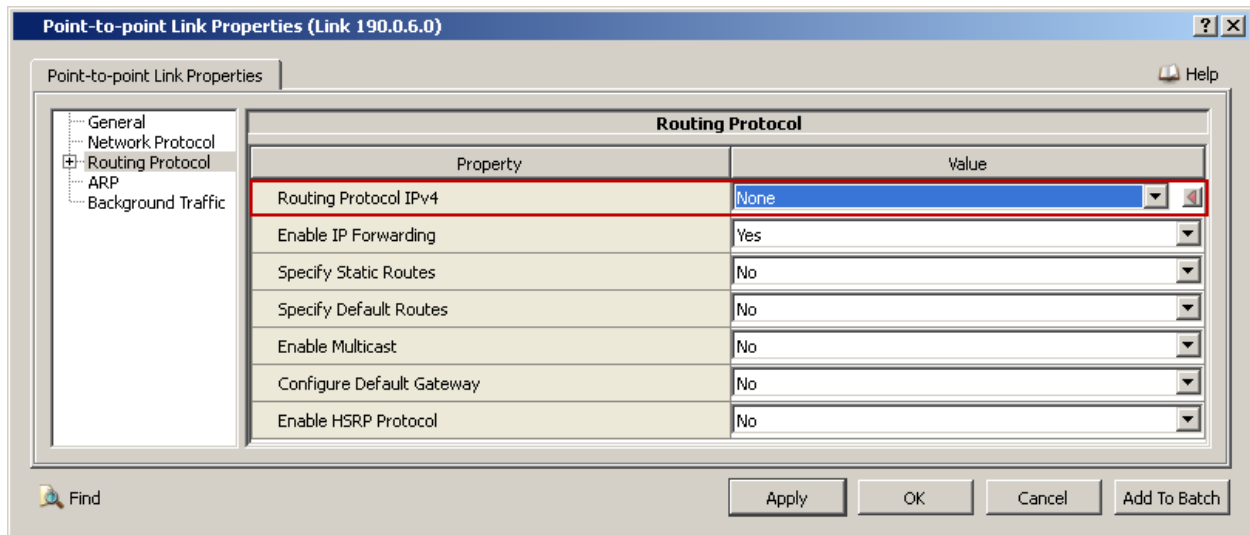
FIGURE 4-14.   Configure Routing Protocol for Links

3. For nodes 4 and 5, go to **Default Device Properties Editor > Node Configuration > Routing Protocol**. Set **Specify Static Routes** to *Yes* and set **Static Route File** to the name of the static routes file, as shown in Figure 4-15.
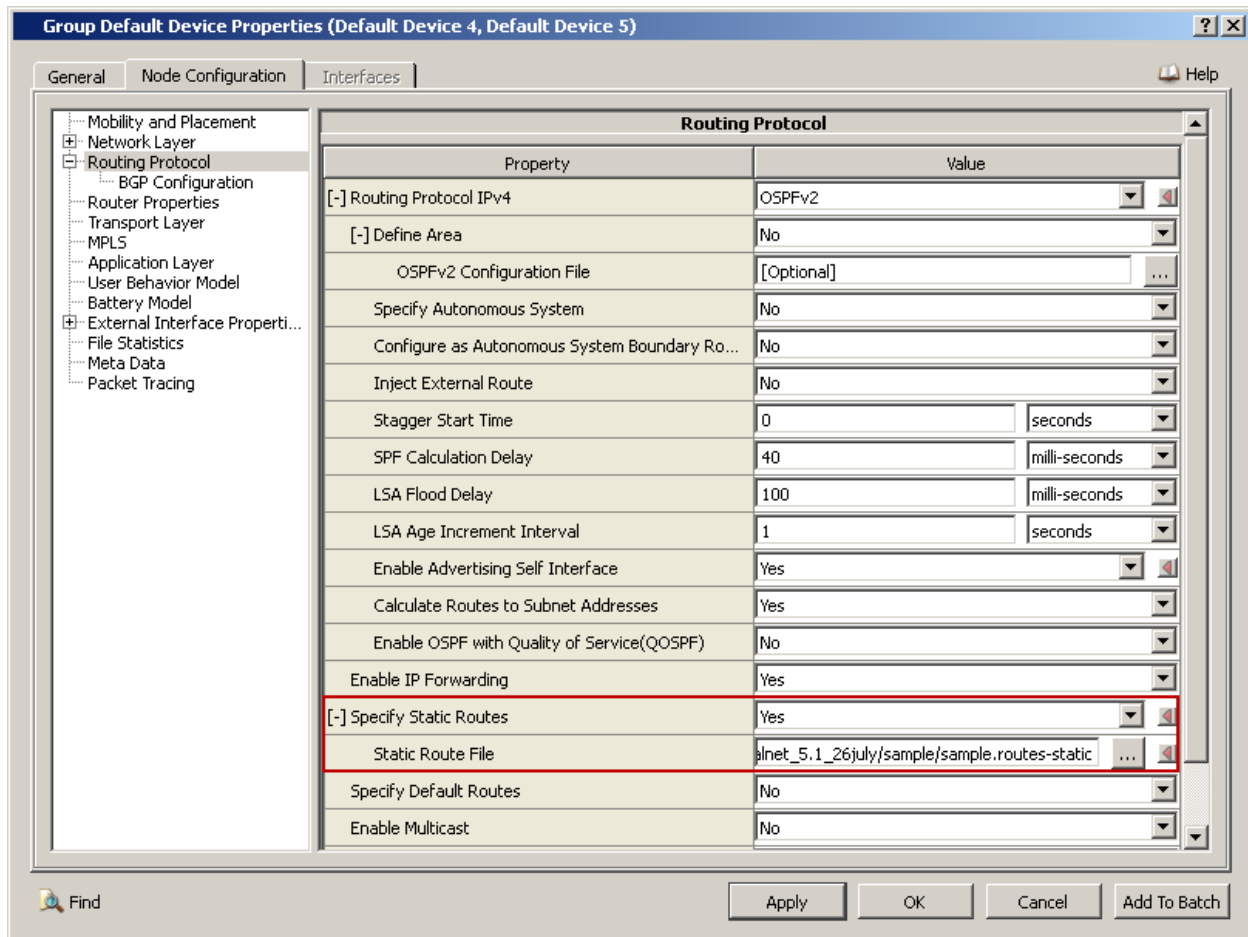
FIGURE 4-15.   Setting Static Route Protocol

Note: If BGP Next Hop Legacy support is enabled, then specification of static routes is not required.

Configuring the Application

1. Create a CBR session from node 2 to node 9.

2. Set the CBR parameters as follows:

- Set **Items to Send** to *500.*
- Set **Item Size** to *512.*
- Set **Interval** to 1 *seconds.*
- Set **Start Time** to *2 minutes.*
- Set **End Time** to *10 minutes.*

FIGURE 4-16.   Setting CBR Properties

4.1.7 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the BGPv4 model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/bgp. Table 4-7 lists the sub-directory where each scenario is located.

TABLE 4-7.   BGPv4 Scenarios Included in QualNet

Scenario	Description
disjoint	Shows two indirectly connected BGP speakers.
fault	Shows the BGP operation under a faulty scenario.
ibgp	Shows the operation of multiple BGP speakers within the same AS (IBGP).
igp	Shows IGP route injection into BGP.
igp-mix-v4	Shows the BGP implementation in a mixed igp network scenario.
igp-mix-v6	Shows the BGP implementation in ASes which run IGP with IPv6 protocol.

TABLE 4-7.   BGPv4 Scenarios Included in QualNet (Continued)

Scenario	Description
mbgp_test1	Shows normal activities of BGP in which two BGP speakers are connected to each other and each speaker belongs to different AS.
mbgp_test2	Shows normal activities of BGP in which two BGP speakers are connected to each other and each speaker belongs to different AS.
normal1	Shows normal activities of BGP in which two BGP speakers are connected to each other and each speaker belongs to different AS.
normal2	Shows normal BGP operation with topological loop.
normal3	Shows normal BGP scenario under a star-shaped topology.
normal4	Shows normal BGP scenario with multiple hops and multiple paths.
route-reflector	Shows normal BGP scenario route reflector operation.

4.1.8 References

1. RFC 1772. "Application of the Border Gateway Protocol in the Internet." Y. Rekhter, P. Gross. March 1995.

2. RFC 2460. "Internet Protocol, Version 6 (IPv6) Specification." S. Deering, R. Hinden. December 1998.

3. RFC 2461. "Neighbor Discovery for IP Version 6 (IPv6)." T. Narten, E. Nordmark, W. Simpson. December 1998.

4. RFC 2545. "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing." P. Marques, F. Dupont. March 1999.

5. RFC 2858. "Multiprotocol Extensions for BGP-4." T. Bates, Y. Rekhter, R. Chandra, D. Katz. June 2000.

6. RFC 4271. "A Border Gateway Protocol 4 (BGP-4)." Y. Rekhter, T. Li, S. Hares. January 2006.

7. RFC 4456. "BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)." T. Bates, E. Chen, R. Chandra. April 2006.

8. Guide to Cisco Router Configuration, http://www.typo.org/~web/router/cisco-configuration.html.

....

4.2 Enhanced Interior Gateway Routing Protocol (EIGRP)

The QualNet EIGRP model is based on the CISCO standard. CISCO had defined EIGRP in its white paper and the same is followed as reference guide and standard:

• http://www.cisco.com/application/pdf/paws/16406/eigrp-toc.pdf

4.2.1 Description

EIGRP is a distance vector routing protocol that has been designed for fast convergence. EIGRP works only for wired networks.

4.2.2 Omitted Features and Assumptions

This section describes the omitted features, assumptions and limitations of the EIGRP model.

4.2.2.1 Omitted Features

• Interaction with BGP or route redistribution.
• External route and route tagging.
• Route summarization and route aggregation.
• Reliable Transfer Protocol (RTP).

4.2.2.2 Assumptions and Limitations

• Used only for wired scenarios.

4.2.3 Command Line Configuration

To select EIGRP as the routing protocol, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] ROUTING-PROTOCOL    EIGRP
```

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

EIGRP General Parameters

Table 4-8 lists the EIGRP configuration parameters specified in the scenario configuration (.config) file. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 4-8.   EIGRP General Parameters

Parameter	Value	Description
`EIGRP-CONFIG-FILE` Required *Scope:* All	Filename	Specifies the name of the EIGRP configuration file. The EIGRP configuration file is used to configure EIGRP parameters. The extension of this file is usually ".eigrp". The format of the EIGRP configuration file is described in Section 4.2.3.1.
`ROUTING-STATISTICS` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Specifies whether EIGRP statistics are collected.

4.2.3.1 Format of EIGRP Configuration File

The EIGRP configuration (.eigrp) file contains the configuration parameters for one or more EIGRP routers.

An EIGRP router configuration consists of the following elements in the following order:

```
<Router ID Specification>
<Networks Specification>
<Hello Interval Specification>
<Hold Time Specification>
<Sleep Time Specification>
<Split Horizon Specification>
<Poison Reverse Specification>
<Route Filtering Specification>
<Default Routes Specification>
<Default Network Specification>
<Auto-summary Specification>
```

These elements are described in Table 4-9.

TABLE 4-9.   EIGRP Configuration File Parameters

Element	Description
`<Router ID Specification>`	The router ID specification associates an EIGRP router with an autonomous system and has the following format: ROUTER <node-ID> <AS-ID> where `<node-ID>` Node ID of the router. `<AS-ID>` ID of the autonomous system with which the router is associated.
`<Networks Specification>`	The networks specification identifies all networks which are directly attached to an EIGRP router. EIGRP sends updates only to the interfaces in the specified networks. The networks specification consists of one or more occurrences of the following line: NETWORK <IP-address> <subnet-mask> where `<IP-address>` IP address of the network which is directly attached to the EIGRP router. `<subnet-mask>` Subnet mask of the directly attached network.
`<Hello Interval Specification>`	The hello interval specification specifies the EIGRP hello interval (the time between hello packets) and has the following format: EIGRP-HELLO-INTERVAL <int-index> <hello-interval> where `<int-index>` Interface index. `<hello-interval>` Hello interval. **Note:** The hello interval specification is optional. If this specification is not included, then the default hello interval is 60S.
`<Hold Time Specification>`	The hold time specification specifies the EIGRP hold time. The hold time is advertised in hello packets and indicates to the neighbors the length of time for which the sender should be considered as valid. The hold time specification has the following format: EIGRP-HOLD-TIME <int-index> <hold-time> where `<int-index>` Interface index. `<hold-time>` Hold time. **Note:** The hold time specification is optional. If this specification is not included, then the default hold time is 180S.

TABLE 4-9. EIGRP Configuration File Parameters (Continued)

Element	Description
`<Sleep Time Specification>`	The sleep time specification specifies the EIGRP sleep time and has the following format: `EIGRP-SLEEP-TIME <sleep-time>` where `<sleep-time>` Sleep time. **Note:** The sleep time specification is optional. If this specification is not included, then the default sleep time is 5S.

`<Split Horizon Specification>`	The split horizon specification enables or disables the IP split horizon. Split horizon controls the sending of EIGRP update and query packets. If split horizon is enabled on an interface, the update and query packets are not sent to destinations for which the interface is the next hop.
	
	To enable or disable split horizon, include one of the following lines:
	
	    `IP-SPLIT-HORIZON`
	or
	    `NO-IP-SPLIT-HORIZON`
	
	Note: The split horizon specification is optional. If this specification is not included, then IP split horizon is enabled by default.

`<Poison Reverse Specification>`	The poison reverse specification enables or disables the IP poison reverse. Poison reverse is a way of avoiding routing loops. If poison reverse is enabled and if a route to a particular node is learnt through a particular interface, that node is advertised to that interface as being unreachable. For example, if router 3 learns about router 1 from router 2, and if poison reverse is on, then router 3 advertises router 1 to router 2 as unreachable. To enable or disable poison reverse, include the following line: `EIGRP-POISON-REVERSE ON	OFF` **Note:** The poison reverse specification is optional. If this specification is not included, then poison reverse is not enabled by default.

TABLE 4-9.   EIGRP Configuration File Parameters (Continued)

Element	Description
`<Route Filtering Specification>`	The route filtering specification specifies zero or more commands for route filtering. Each route filtering command has the following format: `DISTRIBUTE-LIST <ACL-List> <int-type> [<int-index>]` where `<ACL-List>` Name or number of an access list in the router configuration file. `<int-type>` Interface type. This can be `IN` or `OUT`. `<int-index>` Interface index. **Note:** This is an optional parameter. **Note:** The route filtering specification is optional.
`<Default Routes Specification>`	The default routes specification injects default routes into EIGRP. Each default route has the following format: `IP-ROUTE <network-address> <mask> <int-address>` where `<network-address>` Address of the network for which the route is being created. `<mask>` Subnet mask of the network. `<int-address>` IP address of the interface to which packets are to be routed. **Note:** The default routes specification is optional.

TABLE 4-9.   EIGRP Configuration File Parameters (Continued)

Element	Description

`<Default Network Specification>`	The default network is used for default candidate routing.
	
	The default network specification has the following format:
	
	    `IP-DEFAULT-NETWORK   <network-address>`
	
	  where
	    `<network-address>` Address of the default network.
	
	Note: The default network specification is optional.

`<Auto-summary Specification>`	EIGRP performs an auto-summary each time it crosses a border between two different major networks. The auto-summary command enables or disables route summarization.
	
	To enable or disable auto-summary, include one of the following lines:
	
	    `AUTO-SUMMARY`
	  or
	    `NO-AUTO-SUMMARY`
	
	Note: The auto summary specification is optional. If this specification is not included, then auto-summary is enabled by default.

Example of EIGRP Configuration File

The following is an example of EIGRP configuration file:
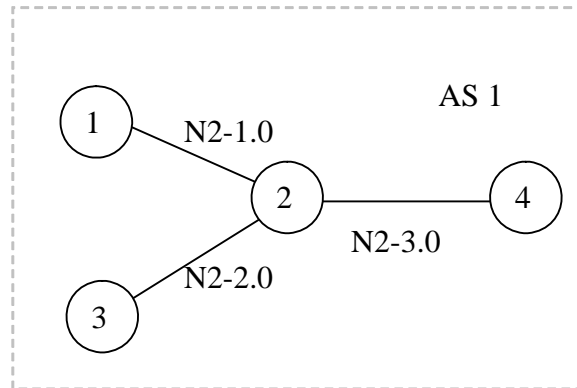
FIGURE 4-17.   Sample EIGRP scenario

```
#EIGRP routers 1, 2 and 3 belong to AS 1.
#Router 1 is directly attached to network having IP address 0.0.1.0.
#Router 2 is directly attached to networks having IP addresses 0.0.1.0,
0.0.2.0 and 0.0.3.0.
#Router 3 is directly attached to network with IP address 0.0.2.0.
#Router 4 is directly attached to network with IP address 0.0.3.0.


#Configuring router 1


ROUTER 1  1
NETWORK 0.0.1.0     255.255.255.252


#Hello interval and hold time are configured on interface 1
EIGRP-HOLD-TIME        1  5S
EIGRP-HELLO-INTERVAL  1 10S


#EIGRP sleep time specification
EIGRP-SLEEP-TIME     5S
```

```
#To disable split horizon
NO-IP-SPLIT-HORIZON

#Poison reverse specification
EIGRP-POISON-REVERESE ON

#EIGRP route filtering specification with access list EigrpFilter1 and
interface type OUT
DISTRIBUTE-LIST EigrpFilter1 OUT

# To specify the default IP route, in which router 1 has a default
route thru the interface #whose IP address is 0.0.1.1.
IP-ROUTE 0.0.0.0  0.0.0.0  0.0.1.1

#default network specification
IP-DEFAULT-NETWORK 0.0.2.0

#auto-summary specification
AUTO-SUMMARY
```

4.2.4 GUI Configuration

This section describes how to configure EIGRP in the GUI.

Configuring EIGRP Parameters

To configure the EIGRP parameters, perform the following steps:

1. Go to one of the following locations:

- To set properties for a specific wireless subnet, go to **Wireless Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific wired subnet, go to **Wired Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific point-to-point link, go to **Point-to-point Link Properties Editor > Point-to-point Link Properties > Routing Protocol**.

- To set properties for a specific node, go to **Default Device Properties Editor > Node Configuration > Routing Protocol**.

- To set properties for a specific interface of a node, go to one of the following locations:

  – **Interface Properties Editor > Interfaces > Interface # > Routing Protocol**.

  – **Default Device Properties Editor > Interfaces > Interface # > Routing Protocol**.

In this section, we show how to configure EIGRP parameters for a specific node using the Default Device Properties Editor. Parameters can be set in the other properties editors in a similar way.

2. Set **Routing Protocol IPv4** to *EIGRP* and set the dependent parameters listed in Table 4-10.
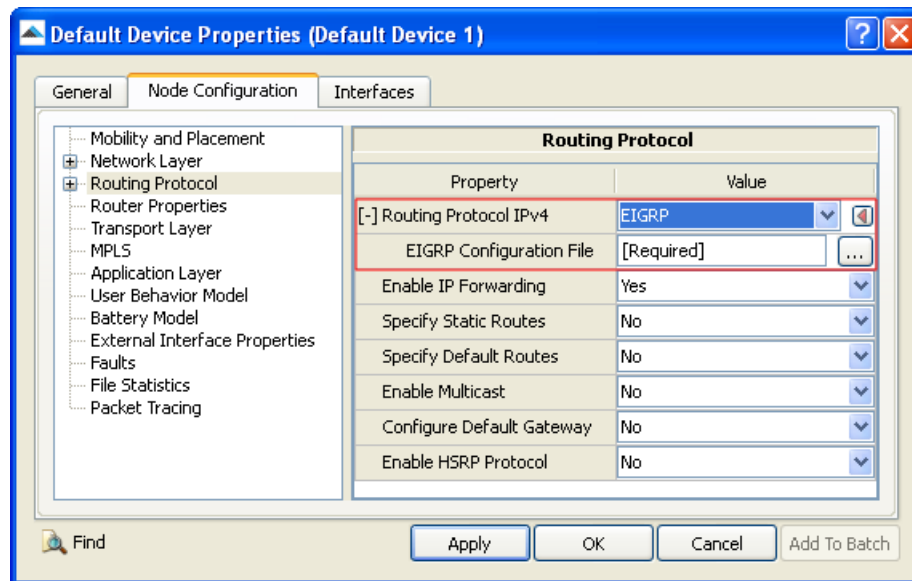
FIGURE 4-18.   Setting EIGRP Parameters

TABLE 4-10.   Command Line Equivalent of EIGRP Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
EIGRP Configuration File	Node, Interface, Subnet	EIGRP-CONFIG-FILE

Setting Parameters

- Set **EIGRP Configuration File** to the name of the EIGRP configuration file. The format of the EIGRP configuration file is described in Section 4.2.3.1.

Configuring Statistics Parameters

Statistics for EIGRP can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for routing protocols including EIGRP, check the box labeled **Routing** in the appropriate properties editor.

TABLE 4-11.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Routing	Global, Node	ROUTING-STATISTICS

4.2.5 Statistics

Table 4-12 lists the EIGRP statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 4-12.   EIGRP Statistics

Statistic	Description
Number of triggered Updates	Total number of triggered updates sent by the node.
Number of query send	Total number of query requests sent by the node.
Number of reply received	Total reply packets received in response by the node.
Number of Updates Received	Total number of update packets that were received by the node.
Number of query Received	Total number of query packets received by the node.
Number of Reply send	Total number of reply packets sent by the node.
Number of hello send	Total number of hello packets sent by the node.
Number of hello received	Total number of hello packets received by the node.

4.2.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the EIGRP model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/eigrp. Table 4-13 lists the sub-directory where each scenario is located.

TABLE 4-13. EIGRP Scenarios Included in QualNet

Scenario	Description
least-cost-path1	Shows EIGRP's least-cost path selection property.
least-cost-path2	Shows EIGRP's least-cost path selection property with interface fault.
normal-scenario1	Shows the normal operation of EIGRP protocol.
normal-scenario2	Shows the normal operation of EIGRP protocol using same topology but different network conditions.
query-reply1	Shows the EIGRP query-reply procedure with link failures.
query-reply2	Shows the EIGRP query-reply procedure with link failures using another topology.
route-filter1	Shows EIGRP's route filtering property.
route-filter2	Shows EIGRP's route filtering property using another topology.
route-summary1	Shows EIGRP route summarization feature.
route-summary2	Shows EIGRP's least-cost path selection property.

4.3 Interior Gateway Routing Protocol (IGRP)

4.3.1 Description

IGRP is a routing protocol that was developed with the principal goal of providing a robust protocol for routing within an autonomous system (AS).

4.3.2 Omitted Features and Assumptions

This section describes the omitted features, assumptions and limitations of the IGRP model.

4.3.2.1 Omitted Features

- Applying offsets to the routing metric.
- Point to point routing information exchange.
- Controlling traffic distribution.
- Validating source IP address.
- Unequal cost load balancing.

4.3.2.2 Assumptions and Limitations

- Following fields are not used in metric calculation of IGRP:
  - mtu (maximum transferable unit).
  - reliability (channel reliability / rate of error).
  - load (current load on the channel).
- Only one type of service called DEFAULT_TOS is assumed.
- IGRP exchanges only system routes and exterior routes but no interior routes.

4.3.3 Command Line Configuration

To select IGRP as the routing protocol, specify the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] ROUTING-PROTOCOL       IGRP
```

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

IGRP Parameters

Table 4-14 lists the IGRP parameters specified in the scenario configuration (.config) file. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 4-14.   IGRP Parameters

Parameter	Value	Description
`IGRP-MAXIMUM-HOPS` Required *Scope:* All	Integer *Range:* ≥ 5 *Default:* 100	Specifies the maximum number of hop count supported.
`IGRP-CONFIG-FILE` Optional *Scope:* All	Filename	Specifies the name of the IGRP configuration file. The IGRP configuration file is used to configure IGRP parameters. The extension of this file is usually ".igrp". The format of the IGRP configuration file is described in Section 4.3.3.2.
`IGRP-BROADCAST-TIME` Optional *Scope:* All	Time *Range:* > 0S *Default:* 90S	Specifies the time period after which a node broadcasts update messages. **Note:** It is recommended that this parameter be set in range [80S, 100S].
`IGRP-INVALID-TIME` Optional *Scope:* All	Time *Range:* (See note) *Default:* 270S	Specifies the time period after a path is timed out if no update is received. **Note:** The range of this parameter is [max(0, 3*IGRP-BROADCAST-TIME - 10), 3*IGRP-BROADCAST-TIME + 10].
`IGRP-HOLD-TIME` Optional *Scope:* All	Time *Range:* (See note) *Default:* 300S	Specifies the time period during which no path will be accepted for a destination after a destination becomes unreachable. **Note:** The range of this parameter is [(3*IGRP-BROADCAST-TIME, 3*IGRP-BROADCAST-TIME + 20S].
`IGRP-FLUSH-TIME` Optional *Scope:* All	Time *Range:* (See note) *Default:* 630S	Specifies the time after which an entry is removed from the routing table if no update is received. **Note:** The range of this parameter is [max(0, 7*IGRP-BROADCAST-TIME - 10S), 7*IGRP-BROADCAST-TIME + 10S].
`IGRP-PERIODIC-TIMER` Optional *Scope:* All	Time *Range:* [0S, 11S] *Default:* 1S	Specifies the timer value that is used for periodic processing.

TABLE 4-14.   IGRP Parameters (Continued)

Parameter	Value	Description
IGRP-SLEEP-TIME Optional *Scope:* All	Time *Range:* > 0S *Default:* 5S	Specifies the timer value that is used for setting sleep time.
ROUTING-STATISTICS Optional *Scope:* All	List: • YES • NO *Default:* NO	Specifies whether IGRP statistics are collected.

4.3.3.1

[max(0, 3*IGRP-BROADCAST-TIME - 10), 3*IGRP-BROADCAST-TIME + 10]

4.3.3.2 Format of IGRP Configuration File

The IGRP configuration (.igrp) file contains the configuration parameters for one or more IGRP routers. The IGRP configuration file specifies the network addresses of each router's interface to attach with the EIGRP routing process, as well as additional configuration parameters.

An IGRP router configuration consists of the following elements in the following order:

```
<Router ID Specification>
<Networks Specification>
<Variance Specification>
<Weights Specification>
<Hold Down Specification>
<Split Horizon Specification>
```

These elements are described in Table 4-15.

TABLE 4-15.   IGRP Router Configuration Parameters

Element	Description
`<Router ID Specification>`	The router ID specification associates an IGRP router with an autonomous system and has the following format: `ROUTER <node-ID> <AS-ID>` where `<node-ID>` Node ID of the router `<AS-ID>` ID of the autonomous system with which the router is associated
`<Networks Specification>`	The networks specification identifies all networks which are directly attached to an IGRP router. The networks specification consists of one or more occurrences of the following line: `NETWORK <IP-address>` where `<IP-address>` IP address of the network to which is directly attached to the IGRP router
`<Variance Specification>`	The variance specification specifies a user modifiable attribute that specifies the percentage by which the performance of different links can vary, yet still be considered viable paths to the same destination. The variance specification has the following format: `VARIANCE <multiplier>` where `<multiplier>` Interface index **Note:** The variance specification is optional. If this specification is not included, then the default variance is 1.0. It is recommended that the variance be set to a value less than 1.1.

TABLE 4-15.   IGRP Router Configuration Parameters (Continued)

Element	Description
`<Weights Specification>`	The weights specification specifies the weight factors for each type of service. The weight factors are used in the calculation of routing metric. For each type of service, the weights are specified using the following format: METRIC WEIGHTS `<tos-value>` `<K1>` `<K2>` `<K3>` `<K4>` `<K5>` where `<tos-value>` TOS value `<K1>`,`<K2>`,`<K3>`,`<K4>`,`<K5>` Values of factors K1, k2, K3, K4, and K5, respectively, used in the calculation of routing metric. **Notes:** 1. Metric weights for only TOS value of 1 are supported. 2. The weights specification is optional. If it is not included, the default value of factors K1 and K3 is 1 and the default value of factors K2, K4, and K5 is 0.
`<Hold Down Specification>`	The hold down specification enables or disables hold down. To enable or disable hold down include the following line: METRIC-HOLDDOWN YES | NO **Note:** The hold down specification is optional. If this specification is not included, then hold down is enabled by default.
`<Split Horizon Specification>`	The split horizon specification enables or disables the IP split horizon. To enable or disable split horizon, include the following line: IP-SPLIT-HORIZON YES | NO **Note:** The split horizon specification is optional. If this specification is not included, then IP split horizon is enabled by default.

Example of IGRP Configuration File

The following is an example IGRP configuration file:
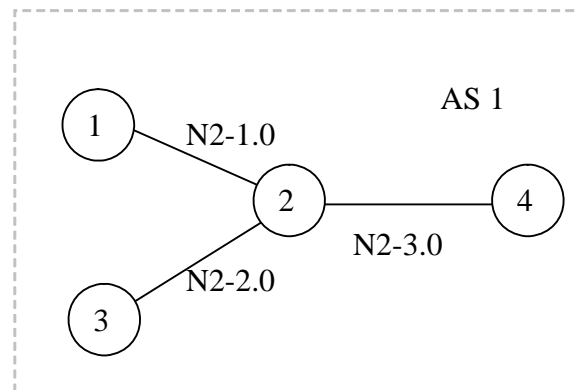
FIGURE 4-19.   Sample IGRP Scenario

```
#IGRP routers 1, 2 and 3 belong to AS 1.
#Router 1 is directly attached to network having IP address 0.0.1.0.
#Router 2 is directly attached to networks having IP addresses 0.0.1.0,
0.0.2.0 and 0.0.3.0.
#Router 3 is directly attached to network with IP address 0.0.2.0.
#Router 4 is directly attached to network with IP address 0.0.3.0.

#Configuring router 1
ROUTER 1  1
NETWORK 0.0.1.0     255.255.255.252

#Variance specification
VARIANCE 1.0

#To enable split horizon
IP-SPLIT_HORIZON YES

#To enable Metric Hold Down.
METRIC-HOLDDOWN YES

#Metric Weights specification for TOS value 1.
METRIC WEIGHTS 1 1 1 0 0
```

4.3.4 GUI Configuration

This section describes how to configure IGRP in the GUI.

Configuring IGRP Parameters

To configure the IGRP parameters, perform the following steps:

1. Go to one of the following locations:

- To set properties for a specific wireless subnet, go to **Wireless Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific wired subnet, go to **Wired Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific point-to-point link, go to **Point-to-point Link Properties Editor > Point-to-point Link Properties > Routing Protocol**.

- To set properties for a specific node, go to **Default Device Properties Editor > Node Configuration > Routing Protocol**.

- To set properties for a specific interface of a node, go to one of the following locations:

   - **Interface Properties Editor > Interfaces > Interface # > Routing Protocol**.

   - **Default Device Properties Editor > Interfaces > Interface # > Routing Protocol**.

In this section, we show how to configure IGRP parameters for a specific node using the Default Device Properties Editor. Parameters can be set in the other properties editors in a similar way.

2. Set **Routing Protocol IPv4** to *IGRP* and set the dependent parameters listed in Table 4-16.
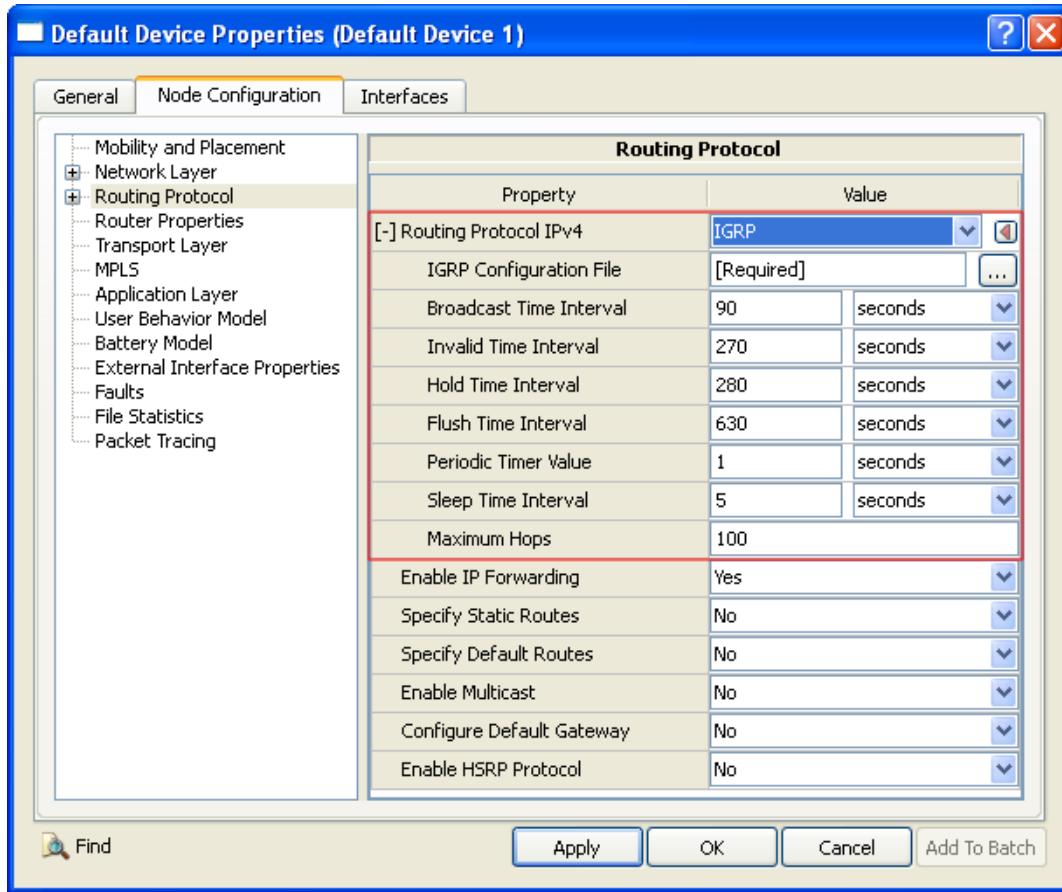
FIGURE 4-20.   Setting IGRP Parameters

TABLE 4-16.   Command Line Equivalent of IGRP Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
IGRP Configuration File	Node, Interface and Subnet	`IGRP-CONFIG-FILE`
Broadcast Time Interval	Node, Interface and Subnet	`IGRP-BROADCAST-TIME`
Invalid Time Interval	Node, Interface and Subnet	`IGRP-INVALID-TIME`
Hold Time Interval	Node, Interface and Subnet	`IGRP-HOLD-TIME`
Flush Time Interval	Node, Interface and Subnet	`IGRP-FLUSH-TIME`
Periodic Timer Value	Node, Interface and Subnet	`IGRP-PERIODIC-TIMER`
Sleep Time Interval	Node, Interface and Subnet	`IGRP-SLEEP-TIME`
Maximum Hops	Node, Interface and Subnet	`IGRP-MAXIMUM-HOPS`

Setting Parameters

- Set **IGRP Configuration File** to the name of the IGRP configuration file. The format of the IGRP configuration file is described in Section 4.3.3.2.

Configuring Statistics Parameters

Statistics for IGRP can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for routing protocols including IGRP, check the box labeled **Routing** in the appropriate properties editor.

TABLE 4-17.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Routing	Global, Node	ROUTING-STATISTICS

4.3.5 Statistics

Table 4-18 lists the IGRP statistics that are output to the statistics (.stat) file at the end of simulation:

TABLE 4-18.   IGRP Statistics

Statistic	Description
Number of Regular Updates	Number of regular updates sent by the node.
Number of Triggered Updates	Number of triggered updates sent by the node.
Number of Route Timeouts	Number of routes that timed out at the node.
Number of Packets Sent Thru interface (<InterfaceId>) is	Number of packets that were sent by the node, through interface with the specified interface ID.

4.3.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the IGRP model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/igrp. Table 4-19 lists the sub-directory where each scenario is located.

TABLE 4-19.   IGRP Scenarios Included in QualNet

Scenario	Description
node-interface-fault1	Shows the operation of protocol in a faulty scenario, where routers are going up and down and Interfaces 0, 1 and 2 of node 9 have encountered interface fault from 3 minutes to 8 minutes.
node-interface-fault2	Shows the operation of protocol in a faulty scenario, where routers are going up and down and node 5 at interface 0 has encountered interface fault from 150 seconds to 8 minutes.
nodes-go-up-n-down	Shows the operation of protocol in a faulty scenario, where routers are going up and down with all nodes as IGRP routers.
normal-scenario1	Shows normal operation of the protocol with nodes 4, 5, 9, 13 and 17 as IGRP routers.

TABLE 4-19.   IGRP Scenarios Included in QualNet (Continued)

Scenario	Description
normal-scenario2	Shows normal operation of the protocol with nodes 4, 5, 9 and 13 as IGRP routers and CBR applied between nodes 1-12 and 11-7.
normal-scenario3	Shows normal operation of the protocol with nodes 4, 5, 9 and 13 as IGRP routers.
normal-scenario4	Shows normal operation of the protocol with nodes 4, 5,9,13 and 17 as IGRP routers and CBR applied between 1-16 and 11-7.
normal-scenario5	Shows normal operation of the protocol with routing update generation by gateway 3 in the scenario.

4.3.7 References

1. Charles L. Hedrick Rutgers. "An Introduction to IGRP." Cisco IGRP implementation. 22 August 1991. http://www.cisco.com/application/pdf/paws/26825/5.pdf

4.4 Open Shortest Path First version 2 (OSPFv2) Routing Protocol

The QualNet OSPFv2 model is based on RFC 2328, RFC 1793, and RFC 1587.

4.4.1 Description

OSPFv2 is classified as an Interior Gateway Protocol (IGP). An IGP distributes routing information between routers belonging to an Autonomous System (AS). The protocol is based on link-state routing scheme. It requires each OSPFv2 router to maintain a database of internal topology of the AS domain. From this database, routing table is obtained by performing SPF algorithm (Dijkstra's Algorithm) and by constructing a shortest-path tree.

A major advantage of OSPFv2 is that it can operate within a hierarchy. The largest entity within the hierarchy is Autonomous System (AS), which is a collection of networks under a single administrative control. Though OSPFv2 is an Interior Gateway Protocol, it can receive and update external routing information from other ASes. An AS can further be divided into a number of areas, which are groups of contiguous networks and attached hosts. As a dynamic routing protocol, OSPFv2 quickly detects topology changes in the AS and calculates new loop free routes after a period of convergence.

Demand Circuit Extension

Demand circuits refer to those network segments whose cost depends on either connect time and/or usage. Examples include ISDN circuits and X.25 SVCs. On these circuits, it is desirable for a routing protocol to send as little routing traffic as possible. In fact, when there is no change in network topology, it is desirable for a routing protocol to send no routing traffic at all. If there is no data to send (either routing protocol traffic or application data), the data-link connection remains closed. As soon as there is data to be sent, an attempt to open the data-link connection is made.

Not-So-Stubby Area (NSSA) Extension

The OSPF Not-So-Stubby area (NSSA) feature is an extension of the stub area feature that allows the injection of external routes in a limited fashion into the stub area. Redistribution into an NSSA area creates a special type of Link-State Advertisement (LSA) known as Type 7, which can only exist in an NSSA area. An NSSA Autonomous System Boundary Router (ASBR) generates this LSA and an NSSA Area Border Router (ABR) translates it into a Type 5 LSA, which gets propagated into the OSPF domain.

4.4.2 Omitted Features and Assumptions

This section describes the omitted features, assumptions and limitations of the OSPFv2 model.

4.4.2.1 Omitted Features

- Virtual Link.
- Equal cost multipath.
- Incremental LSA update.
- NBMA (Non Broadcast Multiple Access) mode.

4.4.2.2 Assumptions and Limitations

- All nodes are considered as routers.
- All external paths are considered as Type2 external path.
- ASBR will not calculate the AS-External routes; BGP will be responsible to inject them into the IP Forwarding table.

4.4.3 Command Line Configuration

To select OSPFv2 as the routing protocol, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] ROUTING-PROTOCOL    OSPFv2
```

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

Configuration Requirements

- In order to use OSPFv2, IPv4 must be enabled, i.e., `NETWORK-PROTOCOL` must be set to `IPv4`, `DUAL-IP`, `CELLULAR-LAYER3`, or `GSM-LAYER3`.
- To use unnumbered interfaces in an OSPFv2 scenario, Address Resolution Protocol (ARP) and the Logical Link Control (LLC) model also need to be configured. See *Developer Model Library* for a description of these two models.

OSPFv2 Parameters

Table 4-20 describes the OSPFv2 configuration parameters. Table 4-21 describes the parameters for configuring the OSPFv2-specific tables in the statistics database tables (refer to *QualNet Statistics Database User's Guide* for details).

See Section 1.2.1.3 for a description of the format used for the parameter tables.

TABLE 4-20.   OSPFv2 Parameters

Parameter	Value	Description
OSPFv2-DEFINE-AREA Optional *Scope:* All	List • YES • NO *Default:* NO	Indicates whether or not the AS is partitioned into several areas. **Note:** OSPFv2 considers the entire domain as a single area by default.
OSPFv2-CONFIG-FILE Optional *Scope:* All	Filename	Name of the OSPFv2 configuration file. Area parameters are specified in the OSPFv2 configuration file. The format of the OSPFv2 configuration file is described in Section 4.4.3.1. **Note:** This parameter is required if OSPFv2-DEFINE-AREA is set to YES; otherwise, this parameter is optional.
AS-NUMBER Optional *Scope:* All	Integer *Range:* [1, 65535] *Default:* 1	Autonomous system ID for a node.
AS-BOUNDARY-ROUTER Optional *Scope:* All	List • YES • NO *Default:* NO	Indicates whether the node is the Autonomous System Boundary Router (ASBR) for an autonomous system.

TABLE 4-20.   OSPFv2 Parameters (Continued)

Parameter	Value	Description
OSPFv2-INJECT-EXTERNAL-ROUTE Optional *Scope:* All	List • YES • NO *Default:* NO	Indicates whether external routes are injected into an OSPF capable autonomous system through a file.
OSPFv2-INJECT-ROUTE-FILE Optional *Scope:* All	Filename	Name of the external routes file. The format of the external routes file is described in Section 4.4.3.2. **Note:** This parameter is required if OSPFv2-INJECT-EXTERNAL-ROUTE is set to YES.
OSPFv2-STAGGER-START-TIME Optional *Scope:* All	Time *Range:* ≥ 0S *Default:* 0S	Time at which the node should act as an OSPF router. Before this time, the node rejects all OSPF protocol packets.
OSPFv2-SPF-CALCULATION-DELAY Optional *Scope:* All	Time *Range:* ≥ 0S *Default:* 40MS	Delay after which SPF calculation is scheduled.
OSPFv2-LSA-FLOOD-DELAY Optional *Scope:* All	Time *Range:* ≥ 0S *Default:* 100MS	Delay after which LSA is flooded to interfaces.
OSPFv2-LSA-AGE-INCREMENT-INERVAL Optional *Scope:* All	Time *Range:* ≥ 0S *Default:* 1S	Interval after which LSA's age is incremented.
OSPFv2-ADVRT-SELF-INTF Optional *Scope:* All	List • YES • NO *Default:* NO	Enables individual host's entry besides network entries in the routing table. This may be useful in a typical loop topology for finding a better route to a node. This works within a single area only. **Note:** This parameter is meaningful only if unnumbered interfaces are configured for the node (refer to *QualNet User's Guide*).
OSPFv2-INCLUDE-SUBNET-ROUTES Optional *Scope:* All	List • YES • NO *Default:* YES	Indicates whether OSPFv2 should calculate routes to subnet addresses. In some situations, it may be desirable to not include subnet routes in the OSPFv2 routing table as this can lead to routing black holes during network partitions.

TABLE 4-20. OSPFv2 Parameters (Continued)

Parameter	Value	Description
OSPFv2-DEMAND-CIRCUIT-EXTENSION-ENABLED Optional *Scope:* All	List • YES • NO *Default:* NO	Enables demand circuit extension on a router. If the demand circuit extension is enabled on an OSPF router, then that router will be able to process DoNotAge LSA's.
ROUTING-STATISTICS Optional *Scope:* Global, Node	List • YES • NO *Default:* NO	Indicates whether statistics are collected for OSPFv2.
TRACE-OSPFv2 Optional *Scope:* Global, Node	List • YES • NO *Default:* NO	Indicates whether packet tracing is enabled for OSPFv2. **Note:** To enable packet tracing, some other parameters need to be configured as well. Refer to *Section 4.2.10 of QualNet User's Guide* for details.

Table 4-21 lists the parameters for configuring OSPFv2-specific tables in the statistics database.

TABLE 4-21. OSPFv2 Statistics Database Tables Configuration Parameters

Parameter	Value	Description
STATS-DB-OSPF-AGGREGATE-TABLE *Optional* *Scope:* Global	List: • YES • NO *Default:* NO	Indicates whether the OSPF Aggregate table is to be generated.
STATS-DB-OSPF-AGGREGATE-INTERVAL *Optional* *Scope:* Global	Time *Range:* > 0S *Default:* 600S	The time between consecutive entries in the OSPF Aggregate statistics table.
STATS-DB-OSPF-EXTERNAL-LSA-TABLE *Optional* *Scope:* Global	List: • YES • NO *Default:* NO	Indicates whether the OSPF External LSA table is to be generated.
STATS-DB-OSPF-EXTERNAL-LSA-INTERVAL *Optional* *Scope:* Global	Time *Range:* > 0S *Default:* 600S	The time between consecutive entries in the OSPF External LSA table.

TABLE 4-21.   OSPFv2 Statistics Database Tables Configuration Parameters

Parameter	Value	Description
STATS-DB-OSPF-INTERFACE-STATE-TABLE *Optional* *Scope:* Global	List: • YES • NO *Default:* NO	Indicates whether the OSPF Interface State table is to be generated.
STATS-DB-OSPF-INTERFACE-STATE-INTERVAL *Optional* *Scope:* Global	Time *Range:* > 0S *Default:* 600S	The time between consecutive entries in the OSPF Interface State table.
STATS-DB-OSPF-NEIGHBOR-STATE-TABLE *Optional* *Scope:* Global	List: • YES • NO *Default:* NO	Indicates whether the OSPF Neighbor State table is to be generated.
STATS-DB-OSPF-NEIGHBOR-STATE-INTERVAL *Optional* *Scope:* Global	Time *Range:* > 0S *Default:* 600S	The time between consecutive entries in the OSPF Neighbor State table.
STATS-DB-OSPF-NETWORK-LSA-TABLE *Optional* *Scope:* Global	List: • YES • NO *Default:* NO	Indicates whether the OSPF Network LSA table is to be generated.
STATS-DB-OSPF-NETWORK-LSA-INTERVAL *Optional* *Scope:* Global	Time *Range:* > 0S *Default:* 600S	The time between consecutive entries in the OSPF Network LSA table.
STATS-DB-OSPF-ROUTER-LSA-TABLE *Optional* *Scope:* Global	List: • YES • NO *Default:* NO	Indicates whether the OSPF Router LSA table is to be generated.
STATS-DB-OSPF-ROUTER-LSA-INTERVAL *Optional* *Scope:* Global	Time *Range:* > 0S *Default:* 600S	The time between consecutive entries in the OSPF Router LSA table.

TABLE 4-21.   OSPFv2 Statistics Database Tables Configuration Parameters

Parameter	Value	Description
`STATS-DB-OSPF-SUMMARY-LSA-TABLE` *Optional* *Scope:* Global	List: • `YES` • `NO` *Default:* `NO`	Indicates whether the OSPF Summary LSA table is to be generated.
`STATS-DB-OSPF-SUMMARY-LSA-INTERVAL` *Optional* *Scope:* Global	Time *Range:* `> 0S` *Default:* `600S`	The time between consecutive entries in the OSPF Summary LSA table.
`STATS-DB-OSPF-SUMMARY-TABLE` *Optional* *Scope:* Global	List: • `YES` • `NO` *Default:* `NO`	Indicates whether the OSPF Summary statistics table is to be generated.
`STATS-DB-OSPF-SUMMARY-INTERVAL` *Optional* *Scope:* Global	Time *Range:* `> 0S` *Default:* `600S`	The time between consecutive entries in the OSPF Summary statistics table.

4.4.3.1 Format of the OSPFv2 Configuration File

The OSPFv2 configuration file specifies properties of one or more areas.

An area configuration consists of the following elements:

```
<Area ID Specification>
<Address Range Specification>
<Area Stub Specification>
<OSPF Interface Properties>
<Host Route Specification>
<NSSA Specification>
<Stub Area Summary LSA Filter Specification>
```

These elements are described in Table 4-22.

TABLE 4-22.   OSPFv2 Configuration File Parameters

Element	Description

`<Area ID Specification>`	An area ID specification identifies the ID of the area to which an interface belongs. An area ID is a unique identifier associated with an area within an autonomous system.
	
	An area ID specification has the following format:
	
	`[<Address>]  AREA-ID  <Area-ID>`
	
	where
	
	`<Address>` Interface address(es)
	
	`<Area-ID>` Unique ID for the area specified in 32-bit IP address format. Area ID 0.0.0.0 is reserved for the backbone.
	
	The following is an example of an area ID specification:
	
	`[N8-1.0]  AREA-ID  0.0.0.1`
	
	Note: The area ID specification is optional. If the area ID is not specified for an interface, it belongs to area 0.0.0.0 (i.e., the backbone).

`<Address Range Specification>`	An address range is a list of IP addresses contained within an area. An address range is specified in the following format:
	
	`AREA <Area-ID> RANGE <Network-list> [<AS-ID>]`
	
	where
	
	`<Area-ID>` Area ID in 32-bit IP address format
	
	`<Network-list>` List of IP addresses contained within the area. Items in the list are separated by commas and the list is enclosed in "{" and "}"
	
	`<AS-ID>` Autonomous system ID.
	This is optional except when OSPF is running on multiple autonomous systems with BGP. Since two different autonomous systems can have areas with the same area ID, the autonomous system ID is used to distinguish between them.
	
	The following is an example of an address range specification:
	
	`AREA 0.0.0.1 RANGE {N8-192.168.1.0, N8-192.168.2.0}  1`
	
	Note: One address range specification is required for each area.

TABLE 4-22.   OSPFv2 Configuration File Parameters (Continued)

Element	Description

`<Area Stub Specification>`	A stub area is an area that does not receive external routes, that is routes which are distributed to OSPFv2 by another routing protocol. A stub area relies on static and /or default routes to send traffic outside its AS domain. An area stub is specified in the following format:
	
	    `AREA <Area-ID> STUB <Default-cost> [<AS-ID>]`
	
	where
	
	  `<Area-ID>` Area ID in 32-bit IP address format
	
	  `<Default-cost>` Default cost for the stub area
	
	  `<AS-ID>` Autonomous system ID.
	        This is optional except when OSPF is running on multiple autonomous systems with BGP. Since two different autonomous systems can have areas with the same area ID, the autonomous system ID is used to distinguish between them.
	
	The following is an example of an area stub definition:
	
	   `AREA  0.0.0.3  STUB  5000  1`
	
	Note: The stub area specification is optional for an area.

`<OSPF Interface Properties>`	OSPF interface properties are specified by using the parameters listed in Table 4-23.

`<Host Route Specification>`	A host-based route is a route with a 32-bit mask. It is used to route to a specific host instead of the entire subnet. A host route is specified using the following format:
	
	    `<Node-ID> HOST-IP <IP-address> <Cost> <Area-ID>`
	
	where
	
	  `<Node-ID>` ID of the node to which the host is connected, enclosed in square brackets
	
	  `<IP-address>` IP address of the host
	
	  `<Cost>` Cost for the route to the host
	
	  `<Area-ID>` Area ID in 32-bit IP address format
	
	The following is an example of a host route specification:
	
	   `[1] HOST-IP 192.168.1.2  5  0.0.0.1`
	
	The above statement specifies that the host with IP address 192.168.1.2 is a neighbor of node 1 and belongs to area 0.0.0.1.
	
	Note: The host route specification is optional.

TABLE 4-22.   OSPFv2 Configuration File Parameters (Continued)

Element	Description
`<NSSA Specification>`	To enable the NSSA feature, at least one area should be configured as an NSSA area.

• An area can be configured as an NSSA as follows:

        AREA <Area-ID> NSSA <Default-Cost> [<AS-ID>]

 where

    `<Area-ID>`   Area ID in 32-bit IP address format

    `<Default-cost>`   Default cost for the NSSA area

    `<AS-ID>`   Autonomous system ID.
                         This is optional except when OSPF is running
                         on multiple autonomous systems with BGP.
                         Since two different autonomous systems can
                         have areas with the same area ID, the
                         autonomous system ID is used to distinguish
                         between them.

• An NSSA can be configured as totally stub area as follows:

        AREA <Area-ID> NSSA NO-SUMMARY

• An NSSA can be configured to not inject external routes into the NSSA as Type 7 as follows:

        AREA <Area-ID> NSSA NO-REDISTRIBUTION

• An NSSA can be configured to generate Type 7 default routes as follows:

        AREA <Area-ID> NSSA DEFAULT-INFORMATION-ORIGINATE

• An NSSA can be configured to prevent Type 7 LSAs from being translated outside the NSSA as follows:

        [<Node-ID>] SUMMARY-ADDRESS [<Subnet-address>]
        [<Mask>] NOT-ADVERTISE

 where

    `<Node-ID>`   Node ID of an ASBR or ABR node

    `<Subnet-address>`   Subnet address

    `<Mask>`   Subnet mask

• An NSSA can be configured with a range of addresses which it can advertise as follows:

        [<Node-ID>] SUMMARY-ADDRESS [<Subnet-address>]
        [<Mask>] ADVERTISE

Note: The NSSA specification is optional.

TABLE 4-22.　OSPFv2 Configuration File Parameters (Continued)

Element	Description

`<Stub Area Summary LSA Filter Specification>`	An NSSA or stub area can be configured to prevent Network Summary LSAs (Type 3 LSAs) from being originated inside the area or to only allow Type 3 LSAs from being originated inside the area.
	
	An NSSA or stub area can be configured to prevent Type 3 LSAs from being originated inside the area as follows:
	
	`[<Node-ID>] NETWORK-SUMMARY-LSA [<Address>] [<Mask>] NOT-ADVERTISE <Area-ID>`
	
	where
	　　`<Node-ID>`　　　　　Node ID of an ABR node
	　　`<Address>`　　　　　Subnet address
	　　`<Mask>`　　　　　　Subnet mask
	　　`<Area-ID>`　　　　　Area ID of the stub area or NSSA area
	
	An NSSA or stub area can be configured to only allow specific Type 3 LSAs from being originated inside the area as follows:
	
	`[<Node-ID>] NETWORK-SUMMARY-LSA [<Address>] [<Mask>] ADVERTISE <Area-ID>`
	
	Note: The stub area summary LSA filter specification is optional.

TABLE 4-23.　OSPF Interface Parameters

Parameter	Value	Description
`INTERFACE-COST` Optional *Scope:* Subnet, Interface	Integer *Range:* `[1, 65535]` *Default:* `1`	Specifies the Interface output cost, which is the cost of sending a packet on the interface, expressed in the link state metric. This is advertised as the link cost for this interface in the router's router-LSA.
`RXMT-INTERVAL` Optional *Scope:* Subnet, Interface	Time *Range:* `> 0S` *Default:* `5S`	Specifies the retransmission interval, which is the time between LSA retransmissions for adjacencies belonging to this interface. This is also used when retransmitting Database Description and Link State Request Packets. This should be well over the expected round-trip delay between any two routers on the attached network. The retransmission interval should be set conservatively to avoid needless retransmissions. A typical value for a local area network is 5 seconds.

TABLE 4-23.   OSPF Interface Parameters (Continued)

Parameter	Value	Description
INF-TRANS-DELAY Optional *Scope:* Subnet, Interface	Time *Range:* > 0S *Default:* 1S	Specifies the Interface transmission delay, which is the estimated time it takes to transmit a Link State Update Packet over this interface. LSAs contained in the update packet must have their age incremented by this amount before transmission. This interface retransmission delay should take into account the transmission and propagation delays of the interface. A typical value for a local area network is 1 second.
ROUTER-PRIORITY Optional *Scope:* Subnet, Interface	Integer *Range:* ≥ 0 *Default:* 1	Specifies the Router priority. When two routers that are attached to a network, both attempt to become the designated router, and the one with the higher router priority takes precedence. If there is still a tie, the router with the higher router ID takes precedence. A router whose router priority is set to 0 is ineligible to become the designated router on the attached network. **Note:** Router priority is configured only for interfaces to broadcast and BMA networks.
HELLO-INTERVAL Optional *Scope:* Subnet, Interface	Time *Range:* [1S, 65535S] *Default:* 10S	Specifies the duration between successive Hello packets that the router sends on the interface. This value is advertised in the router's Hello packets. The smaller the Hello interval, the faster the topological changes will be detected; however, more OSPF routing protocol traffic will ensue. A typical value for a X.25 PDN network is 30 seconds and for a local area network is 10 seconds. **Note:** The hello interval must be the same for all routers attached to a common network.
ROUTER-DEAD-INTERVAL Optional *Scope:* Subnet, Interface	Time *Range:* [1S, 65535S] *Default:* 40S	Specifies the duration from the time a router's neighbor hears the last Hello packet from the router to the time when the neighbor declares the router down. This value is advertised in the router's Hello packets. The router dead interval should be a multiple (say 4) of the Hello interval. **Note:** The router dead interval must be the same for all routers attached to a common network.

TABLE 4-23.   OSPF Interface Parameters (Continued)

Parameter	Value	Description
`INTERFACE-TYPE` Optional *Scope:* Subnet, Interface	List • `BROADCAST` • `POINT-TO-POINT` • `POINT-TO-MULTIPOINT` *Default:* (see description)	Specifies the OSPF interface type. `BROADCAST` is used when the network is a one-hop broadcast network. `POINT-TO-POINT` is used for point-to- point wired/ wireless link or wireless adhoc networks. `POINT-TO-MULTIPOINT` is used for point-to- multipoint interfaces. The default value depends on the underlying network type of the interface.
`OSPFv2-DEMAND-CIRCUIT-INTERFACE` Optional *Scope:* Subnet, Interface	List • `YES` • `NO` *Default:* `NO`	Specifies whether the interface is connected to a demand circuit network. If the interface is connected to a demand circuit network, the router will flood DoNotAge LSA's over the demand circuit network and perform hello suppression over this interface.

Example OSPFv2 Configuration File

The following is an example of an OSPFv2 configuration file:

```
# Area ID Specification

# Area 1
[N8-192.168.1.0] AREA-ID  0.0.0.1
[N8-192.168.2.0] AREA-ID  0.0.0.1
[N8-192.168.3.0] AREA-ID  0.0.0.1
[N8-192.168.4.0] AREA-ID  0.0.0.1
[N8-192.168.5.0] AREA-ID  0.0.0.1

AREA  0.0.0.1  RANGE  {N8-192.168.1.0, N8-192.168.2.0, N8-192.168.3.0,
N8-192.168.4.0, N8-192.168.5.0}  1
[4] HOST-IP 192.168.1.1  3   0.0.0.1

# Area 2
[N8-192.168.6.0] AREA-ID  0.0.0.2
[N8-192.168.7.0] AREA-ID  0.0.0.2
[N8-192.168.8.0] AREA-ID  0.0.0.2
[N8-192.168.9.0] AREA-ID  0.0.0.2
[N8-192.168.10.0] AREA-ID  0.0.0.2

# Area Range Specification

AREA  0.0.0.2  RANGE  {N8-192.168.6.0, N8-192.168.7.0, N8-192.168.8.0,
N8-192.168.9.0, N8-192.168.10.0}  1
[10] HOST-IP 192.168.6.1  3   0.0.0.2

# Area 3 (Stub Area)
[N8-192.168.11.0] AREA-ID  0.0.0.3
[N8-192.168.12.0] AREA-ID  0.0.0.3
[N8-192.168.13.0] AREA-ID  0.0.0.3

AREA  0.0.0.3  RANGE  {N8-192.168.11.0, N8-192.168.12.0, N8-
192.168.13.0}  1
[15] HOST-IP 192.168.11.1  3   0.0.0.3

# Area Stub Specification

AREA  0.0.0.3  STUB  5000  1

# Backbone Area
[N2-192.168.14.0] AREA-ID  0.0.0.0
[N2-192.168.14.4] AREA-ID  0.0.0.0
[N2-192.168.14.8] AREA-ID  0.0.0.0
[N2-192.168.14.12] AREA-ID  0.0.0.0
[N2-192.168.14.16] AREA-ID  0.0.0.0
[N2-192.168.14.20] AREA-ID  0.0.0.0

AREA  0.0.0.0  RANGE  {N2-192.168.14.0, N2-192.168.14.4, N2-
192.168.14.8, N2-192.168.14.12, N2-192.168.14.16, N2-192.168.14.20}  1
...
```

```
# OSPF Interface Properties
[15] HOST-IP 192.168.11.1  3   0.0.0.3

[N8-192.168.1.0] INTERFACE-TYPE POINT-TO-MULTIPOINT
[N8-192.168.1.0] INTERFACE-COST 50

[N8-192.168.2.0] INTERFACE-TYPE POINT-TO-MULTIPOINT
[N8-192.168.2.0] INTERFACE-COST 50
...

# Host Route Specification
[1] HOST-IP 192.168.1.2  5  0.0.0.1

# Demand Circuit Interface Specification
[N8-192.168.1.0] OSPFv2-DEMAND-CIRCUIT-INTERFACE YES

# NSSA Specification
AREA  0.0.0.1  NSSA  5000  1

# Stub Area Summary LSA Filter Specification
[7] NETWORK-SUMMARY-LSA 192.168.4.0 255.255.255.0 NOT-ADVERTISE 0.0.0.3
[7] NETWORK-SUMMARY-LSA 192.168.4.0 255.255.255.0 ADVERTISE 0.0.0.3
```

4.4.3.2 Format of the External Routes File

The external routes file specifies external routes that can be injected into the network.

Each line in the external routes file has the following format:

```
<Node-ID> <Destination-Address> <Next-Hop> [<Cost>]
```

where

`<Node-ID>`	Node identifier.
`<Destination-Address>`	Destination address.
	This can be either a host IP address or a network IP address.
`<Next-Hop>`	IP address of the next hop.
`<Cost>`	Cost associated with using this route.
	Cost is expressed as an integer value (> 0).
	This is an optional entry. If this entry is not included, the default cost is 1.

Example External Routes File

The following is an example of an external routes file:

```
1    N2-2.0   1.2    3
2    N2-3.0   2.2
3    N2-1.0   2.1    2
...
```

4.4.4 GUI Configuration

This section describes how to configure OSPFv2 in the GUI.

Configuration Requirements

To use unnumbered interfaces in an OSPFv2 scenario, Address Resolution Protocol (ARP) and the Logical Link Control (LLC) model also need to be configured. See *Developer Model Library* for configuring these two models.

Configuring OSPFv2 Parameters

To configure the OSPFv2 parameters, perform the following steps:

1. Go to one of the following locations:

- To set properties for a specific wireless subnet, go to **Wireless Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific wired subnet, go to **Wired Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific point-to-point link, go to **Point-to-point Link Properties Editor > Point-to-point Link Properties > Routing Protocol**.

- To set properties for a specific node, go to **Default Device Properties Editor > Node Configuration > Routing Protocol**.

- To set properties for a specific interface of a node, go to one of the following locations:

  - **Interface Properties Editor > Interfaces > Interface # > Routing Protocol**, or

  - **Default Device Properties Editor > Interfaces > Interface # > Routing Protocol**.

In this section, we show how to configure OSPFv2 parameters for a specific node using the Default Device Properties Editor. Parameters can be set in the other properties editors in a similar way.

2. Set **Routing Protocol IPv4** to *OSPFv2* and set the dependent parameters listed in Table 4-24.
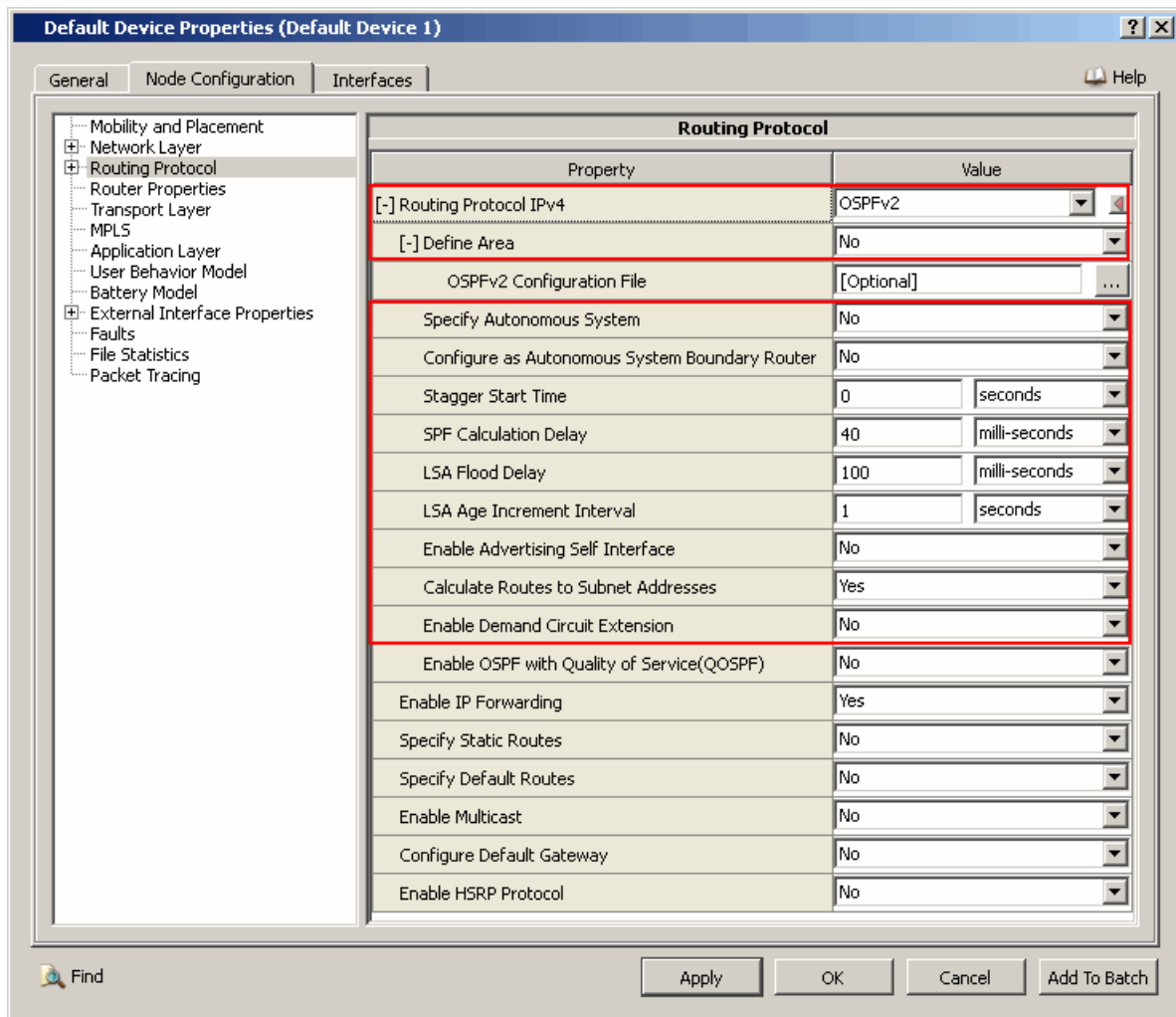
FIGURE 4-21.   Setting OSPFv2 Parameters

TABLE 4-24.   Command Line Equivalent of OSPFv2 Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Define Area	Node, Subnet, Interface	`OSPFv2-DEFINE-AREA`
Specify Autonomous System	Node, Subnet, Interface	N/A
Configure as Autonomous System Boundary Router	Node, Subnet, Interface	`AS-BOUNDARY-ROUTER`
Stagger Start Time	Node, Subnet, Interface	`OSPFv2-STAGGER-START-TIME`
SPF Calculation Delay	Node, Subnet, Interface	`OSPFv2-CALCULATION-DELAY`
LSA Flood Delay	Node, Subnet, Interface	`OSPFv2-LSA-FLOOD-DELAY`
LSA Age Increment Interval	Node, Subnet, Interface	`OSPFv2-LSA-AGE-INCREMENT-INTERVAL`
Enable Advertising Self Interface	Node, Subnet, Interface	`OSPFv2-ADVRT-SELF-INTF`

TABLE 4-24.   Command Line Equivalent of OSPFv2 Parameters (Continued)

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Calculate Routes to Subnet Addresses	Node, Subnet, Interface	`OSPFv2-INCLUDE-SUBNET-ROUTES`
Enable Demand Circuit Extension	Node, Subnet, Interface	`OSPFv2-DEMAND-CIRCUIT-EXTENSION-ENABLED`

Setting Parameters

- **Define Area** should be set to the same value for all nodes in an area.

- To specify autonomous system-specific parameters, set **Specify Autonomous System** to *Yes*; otherwise, set **Specify Autonomous System** to *No*.

3. If **Define Area** is set to *Yes*, then you must set **OSPFv2 Configuration File**; otherwise, **OSPFv2 Configuration File** is an optional parameter.
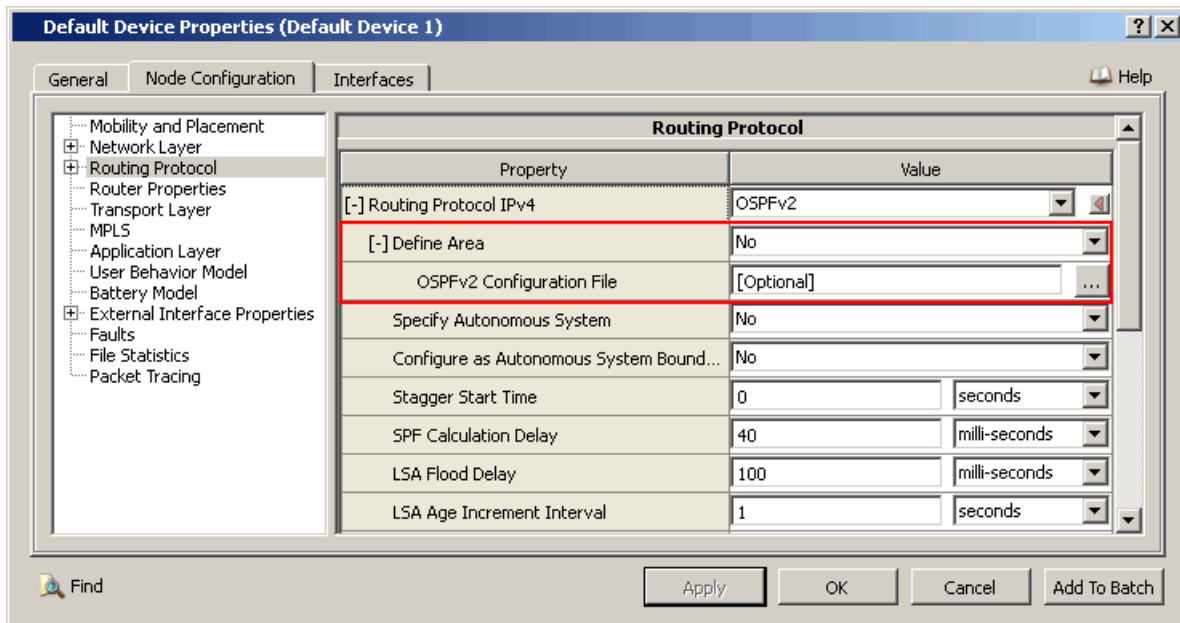
FIGURE 4-22.   Specifying OSPFv2 Configuration File

TABLE 4-25.   Command Line Equivalent of OSPFv2 Configuration File Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
OSPFv2 Configuration File	Node, Subnet, Interface	`OSPFv2-CONFIG-FILE`

Setting Parameters

- Set **OSPFv2 Configuration File** to the name of the OSPFv2 configuration file, if needed. The format of the OSPFv2 configuration file is described in Section 4.4.3.1.

4. If **Specify Autonomous System** is set to *Yes*, then set the dependent parameters listed in Table 4-26.
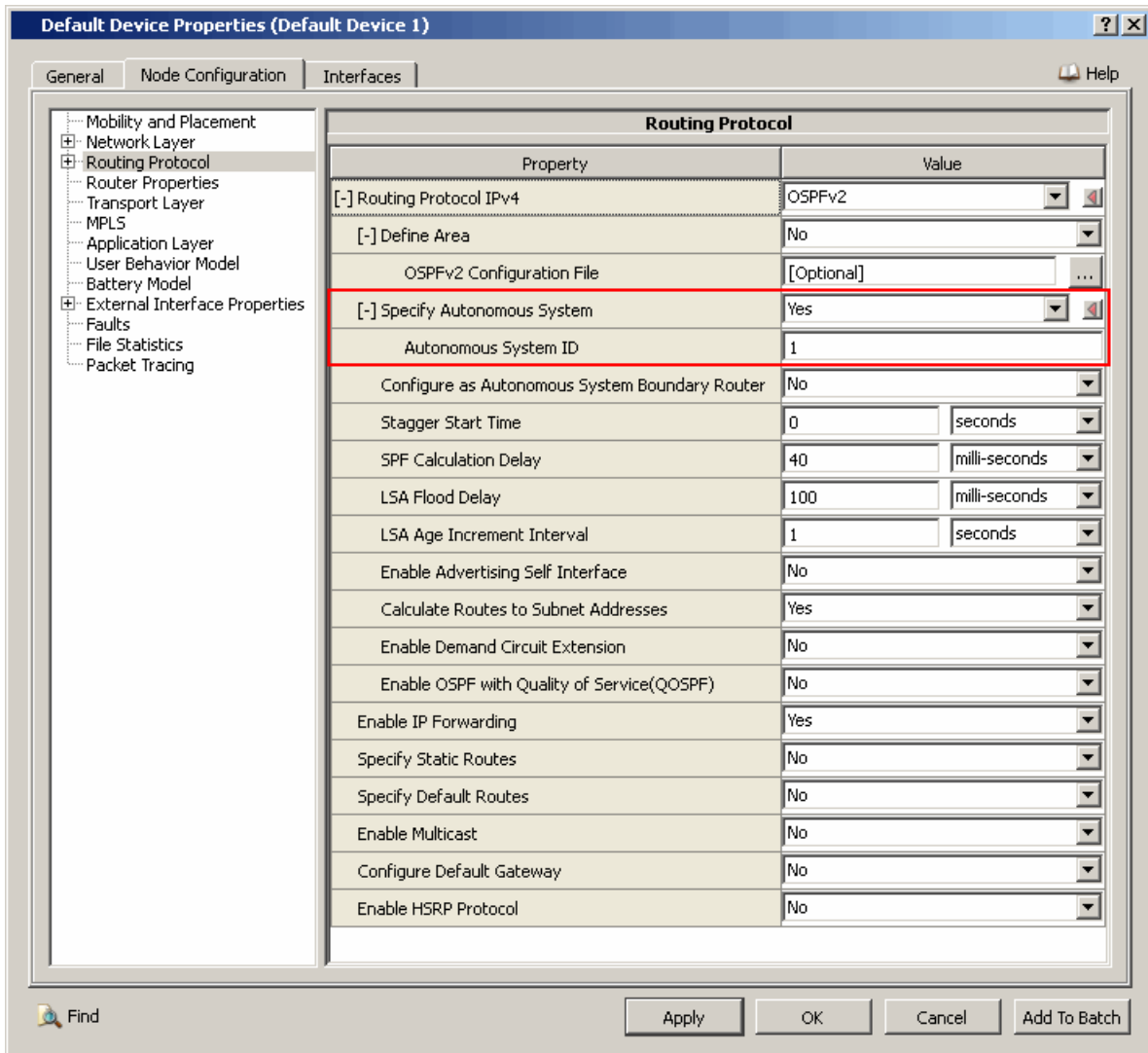
FIGURE 4-23.   Setting Autonomous System-specific Parameters

TABLE 4-26.   Command Line Equivalent of Autonomous System-specific Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Autonomous System ID	Node, Subnet, Interface	`AS-NUMBER`

5. If **Configure as Autonomous System Boundary Router** is set to *Yes*, then set the dependent parameters listed in Table 4-26.
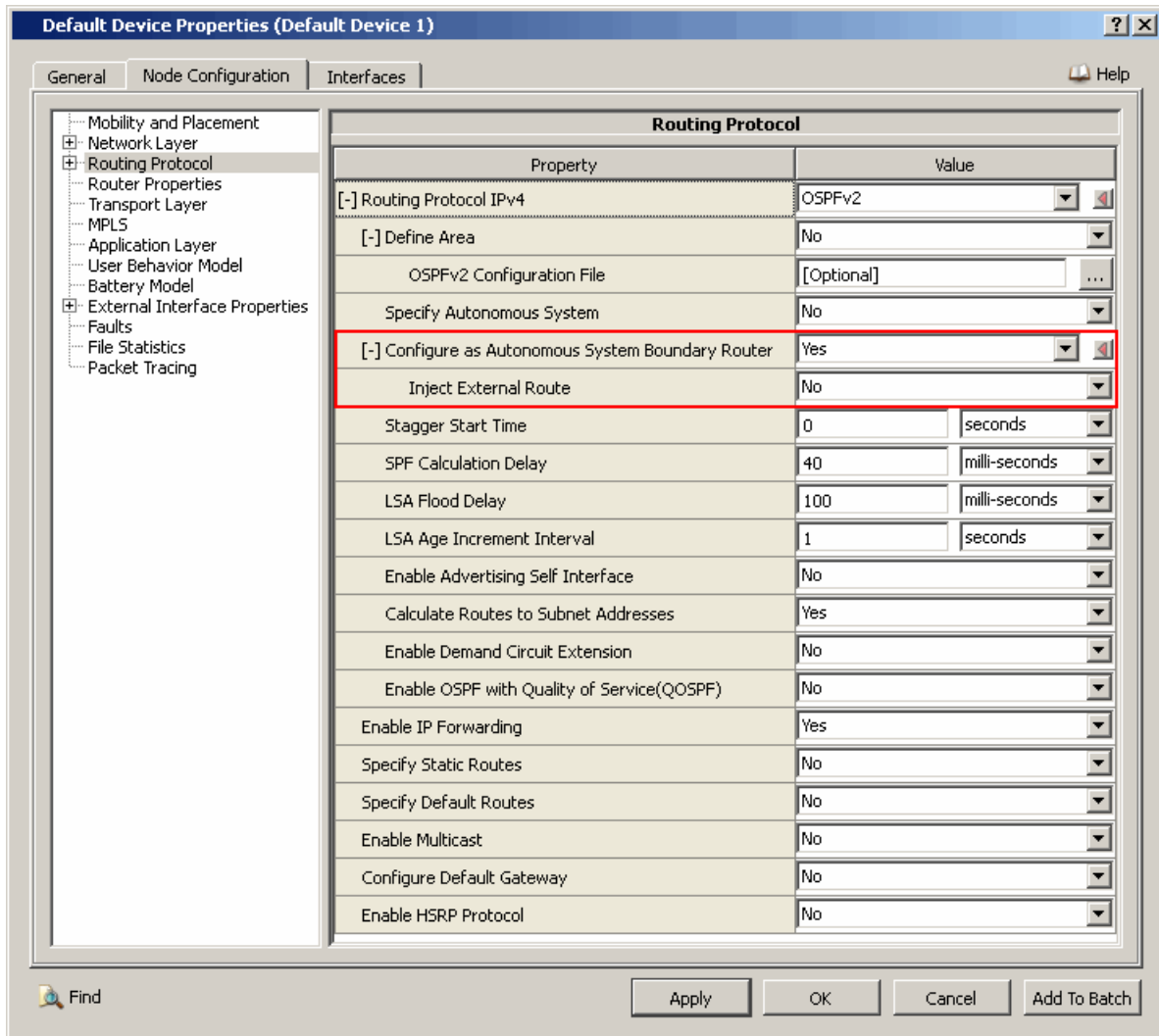
FIGURE 4-24.   Configure AS Boundary Router Parameters

TABLE 4-27.   Command Line Equivalent of AS Boundary Router Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Inject External Route	Node, Interface	OSPFv2-INJECT-EXTERNAL-ROUTE

Setting Parameters

- To enable injection of external routes, set **Inject External Route** to *Yes*; otherwise, set **Inject External Route** to *No*.

6. If **Routing Protocol IPV4** *[= OSPFv2]* **> Configure as Autonomous System Boundary Router** *[= Yes]* **> Inject External Route** is set to *Yes*, then set the dependent parameters listed in Table 4-28.
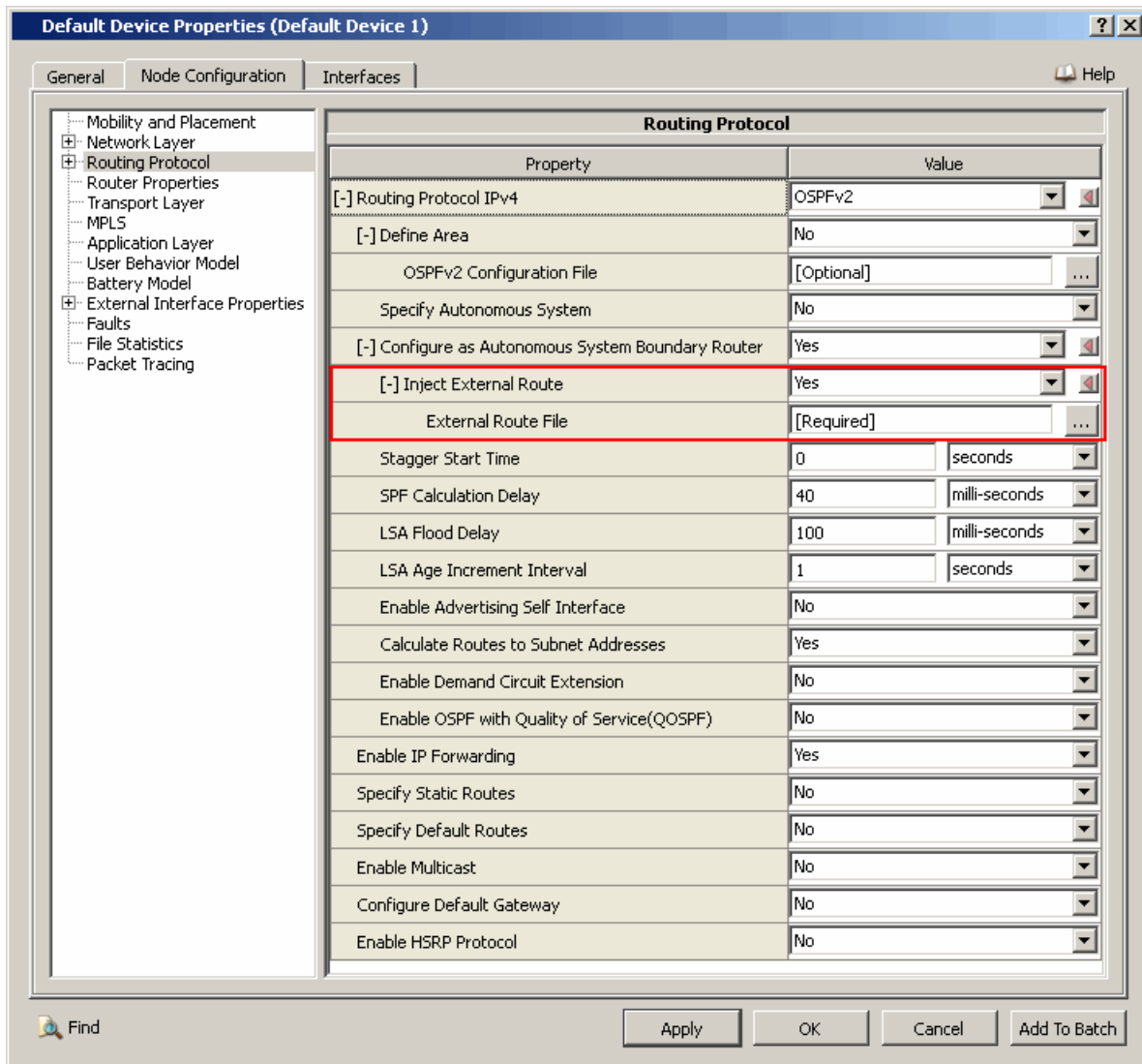
FIGURE 4-25.   Specifying External Route File

TABLE 4-28.   Command Line Equivalent of External Route File Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
External Routes File	Node, Subnet, Interface	`OSPFv2-INJECT-ROUTE-FILE`

Setting Parameters
- Set **External Route File** to the name of the external routes file. The format of the external routes file is described in Section 4.4.3.2.

Configuring File Statistics Parameters

File statistics for OSPFv2 can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for routing protocols including OSPFv2, check the box labeled **Routing** in the appropriate properties editor.

TABLE 4-29.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Routing	Global, Node	ROUTING-STATISTICS

Configuring Statistics Database Parameters

To configure the OSPFv2-specific tables in the statistics database, perform the following steps:

1. Go to **Scenario Properties Editor > Statistics > Statistics Database**.

2. Set **Enable Statistics Database** to *Yes*.

3. Set **Model-specific Tables** set to *Yes* and set the OSPFv2 database table parameters listed in Table 4-30.
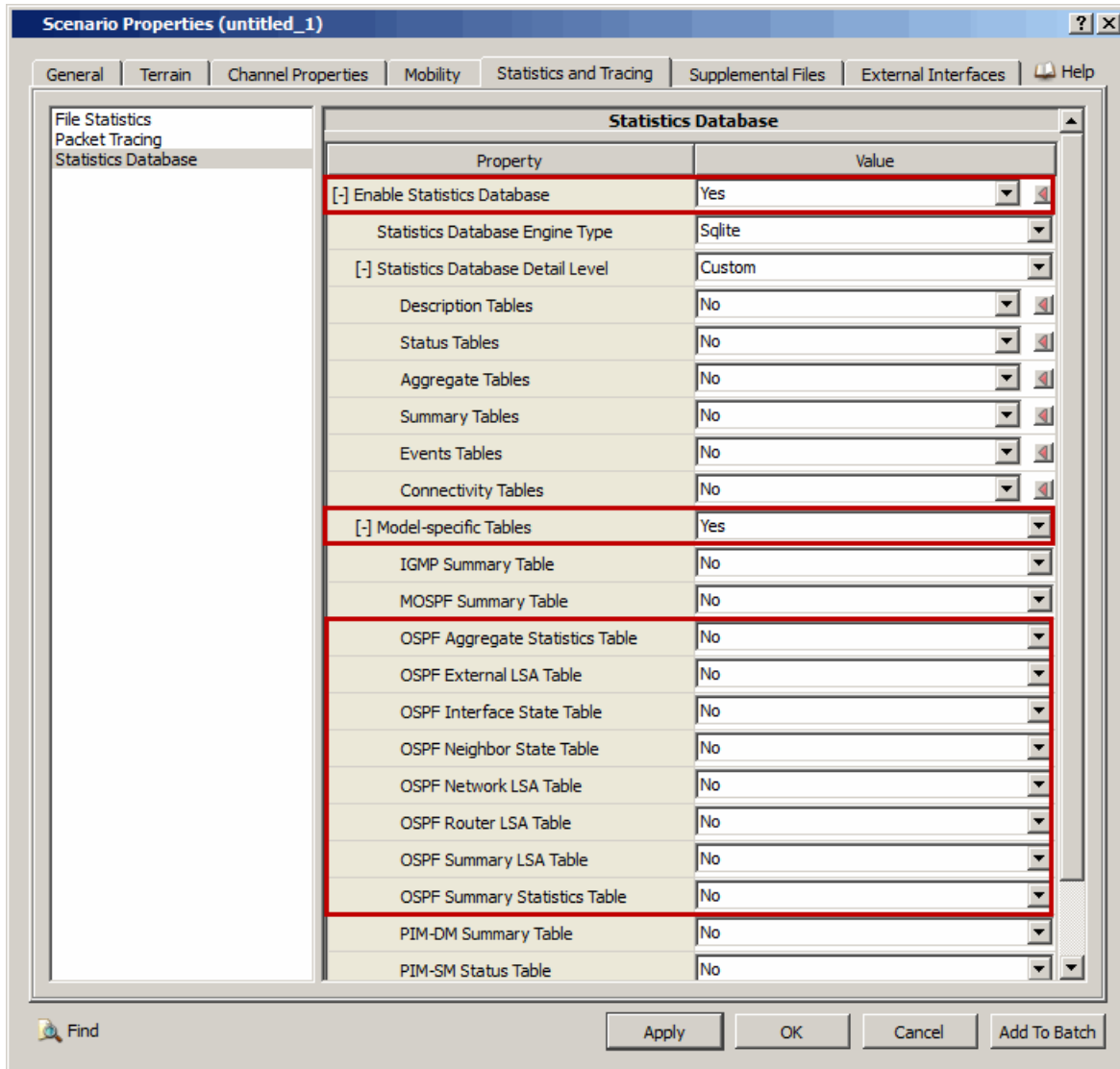
FIGURE 4-26.   Configuring OSPFv2 Tables in Statistics Database

TABLE 4-30.   Command Line Equivalent of OSPFv2 Statistics Database Table Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
OSPF Aggregate Statistics Table	Global	STATS-DB-OSPF-AGGREGATE-TABLE
OSPF External LSA Table	Global	STATS-DB-OSPF-EXTERNAL-LSA-TABLE
OSPF Interface State Table	Global	STATS-DB-OSPF-INTERFACE-STATE-TABLE
OSPF Neighbor State Table	Global	STATS-DB-OSPF-NEIGHBOR-STATE-TABLE
OSPF Network LSA Table	Global	STATS-DB-OSPF-NETWORK-LSA-TABLE
OSPF Router LSA Table	Global	STATS-DB-OSPF-ROUTER-LSA-TABLE
OSPF Summary LSA Table	Global	STATS-DB-OSPF-SUMMARY-LSA-TABLE
OSPF Summary Statistics Table	Global	STATS-DB-OSPF-SUMMARY-TABLE

4. If **OSPF Aggregate Statistics Table** is set to *Yes*, then set the OSPFv2 aggregate statistics update interval parameters listed in Table 4-31. Configure the statistics update interval for the other OSPFv2 tables in a similar manner.
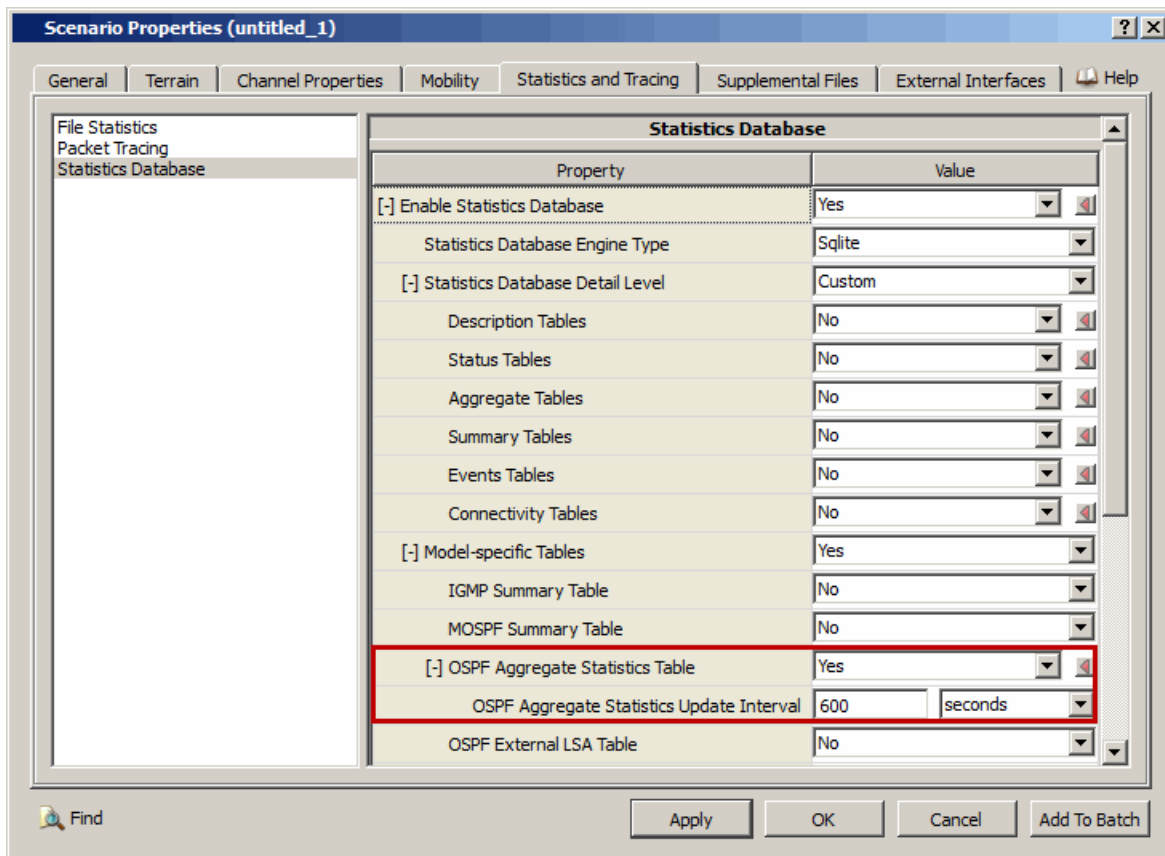
FIGURE 4-27.   Configuring OSPFv2 Aggregate Statistics Update Interval

TABLE 4-31.   Command Line Equivalent of OSPFv2 Aggregate Statistics Update Interval Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
OSPF Aggregate Statistics Update Interval	Global	STATS-DB-OSPF-AGGREGATE-INTERVAL
OSPF External LSA Update Interval	Global	STATS-DB-OSPF-EXTERNAL-LSA-INTERVAL
OSPF Interface State Update Interval	Global	STATS-DB-OSPF-INTERFACE-STATE-INTERVAL
OSPF Neighbor State Update Interval	Global	STATS-DB-OSPF-NEIGHBOR-STATE-INTERVAL
OSPF Network LSA Update Interval	Global	STATS-DB-OSPF-NETWORK-LSA-INTERVAL
OSPF Router LSA Update Interval	Global	STATS-DB-OSPF-ROUTER-LSA-INTERVAL
OSPF Summary LSA Update Interval	Global	STATS-DB-OSPF-SUMMARY-LSA-INTERVAL
OSPF Summary Statistics Update Interval	Global	STATS-DB-OSPF-SUMMARY-INTERVAL

Configuring Packet Tracing Parameters

Packet tracing for OSPFv2 can be enabled at the global and node levels. To enable packet tracing for OSPFv2, in addition to setting the OSPFv2 trace parameter, **Trace OSPF**, several other trace parameters also need to be set. See Section 4.2.10 of *QualNet User's Guide* for details of configuring packet tracing parameters.

TABLE 4-32.   Command Line Equivalent of Packet Tracing Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Trace OSPF	Global, Node	TRACE-OSPFv2

4.4.5 Statistics

This section describes the file, database, and dynamic statistics of the OSPFv2 model.

4.4.5.1 File Statistics

Table 4-33 lists the OSPFv2 statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 4-33.   OSPFv2 Statistics

Statistic	Description
Hello Packets Sent	Number of Hello packets sent by a node.
Hello Packets Received	Number of Hello packets received by a node.
Link State Update Packets Sent	Number of Link State Update packets sent by a node.
Link State Update Bytes Sent	Total number of bytes of Link State Update packets sent by a node.
Link State Update Packets Received	Number of Link State Update packets received by a node.
Link State ACK Packets Sent	Number of Acknowledge packets sent by a node.
Link State ACK Bytes Sent	Total number of bytes of Acknowledge packets sent by a node.
Link State ACK Packets Received	Number of Acknowledge packets received by a node.

TABLE 4-33.   OSPFv2 Statistics (Continued)

Statistic	Description
Link State Update Packets Retransmitted	Number of Link State Update packets retransmitted by a node.
Link State Advertisements Expired	Number of LSA expired on this router by a node.
Database Description Packets Sent	Number of Database Description packets sent by a node.
Database Description Bytes Sent	Total number of bytes of Database Description packets sent by a node.
Database Description Packets Received	Number of Database Description packets received by a node.
Database Description Packets Retransmitted	Number of Database Description packets retransmitted by a node.
Database Description Bytes Retransmitted	Total number of bytes of Database Description packets retransmitted by a node.
Link State Request Packets Sent	Number of Link State Request packets sent by a node.
Link State Request Bytes Sent	Total number of bytes of Link State Request packets sent by a node.
Link State Request Packets Received	Number of Link State Request packets received by a node.
Link State Request Packets Retransmitted	Number of Link State Request packets retransmitted by a node.
Router LSA Originated	Number of router LSA originated by a node.
Network LSA Originated	Number of network LSA originated by a node.
Summary LSA Originated	Number of summary LSA originated by a node.
AS-External LSA Originated	Number of AS-External LSA originated by a node.
Number of LSA Refreshed	Number of LSA refreshed by a node.
Number of DoNotAge LSA Sent	Number of DoNotAge LSA originated by a node.
Number of DoNotAge LSA Received	Number of DoNotAge LSA received by a node.

4.4.5.2 Database Statistics

In addition to the file statistics, the OSPFv2 model also enters statistics in various scenario statistics database tables. Refer to *QualNet Statistics Database User's Guide* for details.

The OSPFv2 model also enters statistics in the following OSPFv2-specific database tables:

- OSPF Aggregate Statistics Table
- OSPF External LSA Table
- OSPF Interface State Table
- OSPF Neighbor State Table
- OSPF Network LSA Table
- OSPF Router LSA Table
- OSPF Summary LSA Table
- OSPF Summary Statistics table

4.4.5.3 Dynamic Statistics

No dynamic statistics are supported for the OSPFv2 model.

4.4.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the OSPFv2 protocol. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/ospfv2. OSPFv2 Demand

Circuit scenarios are located at QUALNET_HOME/scenarios/multimedia_enterprise/ospfv2/demand-circuit. Table 4-34 lists the sub-directory where each scenario is located.

TABLE 4-34.   OSPFv2 Scenarios Included in QualNet

Scenario Sub-directory	Description
2-as-default-lsa	Shows the interaction between BGP and OSPF, as well as AS-External LSA, default Summary LSA, and so on.
area-1subnet	Shows OSPFv2 operation in a domain divided into several areas.
disjoint	Shows OSPFv2 operation in a disjoint network.
fault-down-up	Shows OSPFv2 operation in a four-node network when there is a temporary link fault between two nodes.
fault-no-route	Shows OSPFv2 operation in a four-node network when there is a permanent link fault between two nodes.
normal-2node	Shows normal OSPFv2 operation in a two-node network.
normal-4node	Shows normal OSPFv2 operation in a four-node network.
demand-circuit /area1-DC-area2-DC	Shows the working of the demand circuit if all routers support demand circuit and more than one area is present in the scenario.
demand-circuit / area1-DC-area2-notDC	Shows the working of demand circuit if one area contains all DC capable routers and another area contains a router which is not demand circuit capable (i.e., to generate indication LSA).
demand-circuit/ single-area-all-DC	Shows the operation of demand circuit in OSPFv2 in a four-node network and all OSPFv2 routers supports demand circuit.
demand-circuit / single-area-all-DC-except-1	Shows the operation of demand circuit in OSPFv2 in a four-node network and all OSPFv2 routers support demand circuit except one router.
demand-circuit/ single-area-subnet-all-DC	Shows the operation of demand circuit in OSPFv2 in a four-node network containing subnet and all OSPFv2 routers supports demand circuit.
point-to-multipoint	Shows OSPFv2 operation in a wireless network in point-to-multipoint mode.

4.4.7 References

1. RFC 2328. "OSPF Version 2." J. Moy. August 1998.

2. RFC 1793 "Extending OSPF to Support Demand Circuits" J. Moy. August 1995.

4.5 Open Shortest Path First version 3 (OSPFv3) Routing Protocol

The QualNet OSPFv3 model is based on RFC 2740.

4.5.1 Description

Open Shortest Path First version 3 (OSPFv3) is an Interior Gateway Protocol (IGP) developed to be used in an IPv6 environment. OSPFv3, as OSPFv2, is a hierarchical routing protocol that arranges and classifies the whole of the network into different areas and is capable of quickly detecting topological changes within the AS and also converges to these changes by learning the changed topology quickly. Each router manages and maintains databases called the link-state database synchronized with adjacent routers to learn the Autonomous System's topology. OSPFv3 differs from OSPFv2 as follows:

- Protocol processing is per link, not per subnet.
- Some address semantics have been removed, such as IPv6 addresses, which are not present in OSPF packets except LSA payloads.
- Flooding scope has been added into OSPFv3 and is classified as Link local scope, area scope, and AS scope.
- Explicit support for multiple instances per link has been added into OSPFv3.
- Link local addresses are used in Neighbor discovery, auto-config, etc.
- OSPFv3 relies on the IPv6 for authentication.
- OSPFv3 is network protocol independent.

4.5.2 Features and Assumptions

This section describes the implemented features, omitted features, assumptions and limitations of the OSPFv3 model.

4.5.2.1 Implemented Features

- Flooding scope.
- Intra-area-prefix-LSA.
- IPV6 prefix representation of group of addresses.
- Single Area and Splitting AS into areas.
- Physically contiguous Backbone Area.
- Inter area routing.
- Hello protocol.
- Broadcast Network.
- Point-to-point networks.
- Point-to-Multipoint networks.
- Ageing of LSA.
- AS-External LSA.

4.5.2.2 Omitted Features

- Virtual link.
- Multiple OSPF instance on a single link.
- NBMA (Non broadcast Multiple Access).
- Equal cost Multi-path.

- Incremental LS update.
- Type-7 LSA.
- Unknown LSA types handling.
- Backbone that are physically discontinuous.

4.5.2.3 Assumptions and Limitations

- While running over non broadcast network, OSPFv3 will consider underlying network as point-to-point, unless user specifies/configures the same.
- ASBR will not calculate AS-External routes. BGP will be responsible to inject AS-External routes in IP Forwarding table.
- Link local addressing is not used because of IPv6 Addressing restriction. Although for future use, Link local LSA will be generated and flooded across the defined scopes.
- Each router configured with multiple interfaces will originate single aggregated router lsa and the intra area prefix lsa for the OSPF node.
- Permissible Area-ID configuration is within the range of 0.0.0.0 to 255.255.255.253.
- Users need to insert appropriate Outgoing Interface Cost inside the .ospfv3 file in order to choose a High Bandwidth Route path.
- As Link-Local Addressing is not used, the Intra-Area-Prefix LSA with reference to Network LSA is not generated.
- All Area Border Routers must have an interface connected to the Backbone area.
- Multiple common interfaces between nodes are not supported.
- Interface type broadcast needs to be specified for Wireless Subnet.

4.5.3 Command Line Configuration

To select OSPFv3 as the routing protocol, specify the following parameter(s) in the scenario configuration (.config) file:

- For a dual IP-node, use the following parameter:

      [<Qualifier>] ROUTING-PROTOCOL-IPv6   OSPFv3

- For an IPv6 node, use *either* of the following parameters:

      [<Qualifier>] ROUTING-PROTOCOL   OSPFv3
  or
      [<Qualifier>] ROUTING-PROTOCOL-IPv6   OSPFv3

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of <Qualifier> for each scope.

OSPFv3 Parameters

Table 4-35 describes the OSPFv3 configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 4-35.   OSPFv3 Parameters

Parameter	Value	Description
OSPFv3-DEFINE-AREA Optional *Scope:* All	List • YES • NO *Default:* NO	Indicates whether or not the AS is partitioned into several areas. **Note:** OSPFv3 considers the entire domain as a single area by default.
OSPFv3-CONFIG-FILE Optional *Scope:* All	Filename	Name of the OSPFv3 configuration file. Area parameters are specified in the OSPFv3 configuration file. The format of the OSPFv3 configuration file is described in Section 4.5.3.1. **Note:** This parameter is required if OSPFv3-DEFINE-AREA is set to YES.
AS-NUMBER Optional *Scope:* All	Integer *Range:* [1, 65535] *Default:* 1	Autonomous system ID for a node.
AS-BOUNDARY-ROUTER Optional *Scope:* All	List • YES • NO *Default:* NO	Indicates whether the node is the Autonomous System Boundary Router (ASBR) for an autonomous system.
OSPFv3-INJECT-EXTERNAL-ROUTE Optional *Scope:* All	List • YES • NO *Default:* NO	Indicates whether external routes are injected into an OSPF capable autonomous system through a file.
OSPFv3-INJECT-ROUTE-FILE Optional *Scope:* All	Filename	Name of the external routes file. The format of the external routes file is described in Section 4.5.3.2. This parameter must be specified if OSPFv3-INJECT-EXTERNAL-ROUTE is set to YES.
OSPFv3-STAGGER-START Optional *Scope:* All	List • YES • NO *Default:* NO	Indicates whether or not the router start up times are staggered.

TABLE 4-35.   OSPFv3 Parameters (Continued)

Parameter	Value	Description
ROUTING-STATISTICS Optional *Scope:* Global, Node	List • YES • NO *Default:* NO	Indicates whether statistics are collected for routing protocols.
TRACE-OSPFv3 Optional *Scope:* Global, Node	List • YES • NO *Default:* NO	Indicates whether packet tracing is enabled for OSPFv3. **Note:** To enable packet tracing, some other parameters need to be configured as well. Refer to Section 4.2.10 of *QualNet User's Guide* for details.

4.5.3.1 Format of the OSPFv3 Configuration File

The OSPFv3 configuration file specifies properties of one or more areas.

An area configuration consists of the following elements:

```
<Area ID Specification>
<Address Range Specification>
<Area Stub Specification>
<OSPF Interface Properties>
```

The format for each of these statements are described below. All these statements are optional and can be entered in the file in any order.

These elements are described in Table 4-36.

TABLE 4-36.   OSPFv3 Configuration File Parameters

Element	Description

`<Area ID Specification>`	An area ID specification identifies the ID of the area to which a network belongs. An area ID is a unique identifier associated with an area within an autonomous system.
	
	An area ID specification has the following format:
	
	`[<Network-address>]  AREA-ID  <Area-ID>`
	
	where
	
	`<Network-address>` Network address
	
	`<Area-ID>` A 32-bit number that uniquely identifies the area within an AS.
	Area ID is specified in IP address format. Area ID 0.0.0.0 is reserved for the backbone
	
	The following is an example of an area ID specification:
	
	`[TLA-0.NLA-0.SLA-1]  AREA-ID  0.0.0.1`

`<Address Range Specification>`	An address range is a list of IP addresses contained within an area. An address range is specified in the following format:
	
	`AREA <Area-ID> RANGE <Network-list> [<AS-ID>]`
	
	where
	
	`<Area-ID>` Area ID in IP address format
	
	`<Network-list>` List of IP addresses contained within the area. Items in the list are separated by commas and the list is enclosed in "{" and "}"
	
	`<AS-ID>` Autonomous system ID.
	This is optional except when OSPF is running on multiple autonomous systems with BGP. Since two different autonomous systems can have areas with the same area ID, the autonomous system ID is used to distinguish between them.
	
	The following is an example of an address range specification:
	
	`AREA 0.0.0.1 RANGE SLA-1, SLA-2  1`
	
	Note: One address range specification is required for each area.

TABLE 4-36.   OSPFv3 Configuration File Parameters (Continued)

Element	Description

`<Area Stub Specification>`	A stub area is an area that does not receive external routes that is, routes which are distributed to OSPFv3 by another routing protocol). A stub area relies on static and /or default routes to send traffic outside its AS domain. An area stub is specified in the following format:
	
	    `AREA <Area-ID> STUB <Default-cost> [<AS-ID>]`
	
	where
	
	  `<Area-ID>` Area ID in IP address format
	
	  `<Default-cost>` Default cost for the stub area
	
	  `<AS-ID>` Autonomous system ID.
	This is optional except when OSPF is running on multiple autonomous systems with BGP. Since two different autonomous systems can have areas with the same area ID, the autonomous system ID is used to distinguish between them.
	
	The following is an example of an area stub definition:
	
	  `AREA  0.0.0.3  STUB  5000  1`
	
	Note: The stub area specification is optional for an area.

`<OSPF Interface Properties>`	OSPFv3 interface properties are specified by using the parameters listed in Table 4-37.

TABLE 4-37.   OSPFv3 Interface Parameters

Parameter	Value	Description
`INTERFACE-COST` Optional *Scope:* Subnet, Interface	Integer *Range:* `[1, 65535]` *Default:* `1`	Specifies the Interface output cost, which is the cost of sending a packet on the interface, expressed in the link state metric. This is advertised as the link cost for this interface in the router's router-LSA.
`RXMT-INTERVAL` Optional *Scope:* Subnet, Interface	Time *Range:* `> 0S` *Default:* `5S`	Specifies the retransmission interval, which is the time between LSA retransmissions for adjacencies belonging to this interface. This is also used when retransmitting Database Description and Link State Request Packets. This should be well over the expected round-trip delay between any two routers on the attached network. The retransmission interval should be set conservatively to avoid needless retransmissions. A typical value for a local area network is 5 seconds.

TABLE 4-37.   OSPFv3 Interface Parameters (Continued)

Parameter	Value	Description
INF-TRANS-DELAY Optional *Scope:* Subnet, Interface	Time *Range:* > 0S *Default:* 1S	Specifies the Interface transmission delay, which is the estimated time it takes to transmit a Link State Update Packet over this interface. LSAs contained in the update packet must have their age incremented by this amount before transmission. This interface retransmission delay should take into account the transmission and propagation delays of the interface. A typical value for a local area network is 1 second.
ROUTER-PRIORITY Optional *Scope:* Subnet, Interface	Integer *Range:* [0, 255] *Default:* 1	Specifies the Router priority. When two routers that are attached to a network, both attempt to become the designated router, and the one with the higher router priority takes precedence. If there is still a tie, the router with the higher router ID takes precedence. A router whose router priority is set to 0 is ineligible to become the designated router on the attached network. **Note:** Router priority is configured only for interfaces to broadcast and BMA networks.
HELLO-INTERVAL Optional *Scope:* Subnet, Interface	Time *Range:* [1S, 65535S] *Default:* 10S	Specifies the duration between successive Hello packets that the router sends on the interface. This value is advertised in the router's Hello packets. The smaller the Hello interval, the faster the topological changes will be detected; however, more OSPF routing protocol traffic will ensue. A typical value for a X.25 PDN network is 30 seconds and for a local area network is 10 seconds. **Note:** The hello interval must be the same for all routers attached to a common network.
ROUTER-DEAD-INTERVAL Optional *Scope:* Subnet, Interface	Time *Range:* [1S, 65535S] *Default:* 40S	Specifies the duration from the time a router's neighbor hears the last Hello packet from the router to the time when the neighbor declares the router down. This value is advertised in the router's Hello packets The router dead interval should be a multiple (say 4) of the Hello interval. **Note:** The router dead interval must be the same for all routers attached to a common network.
INTERFACE-TYPE Optional *Scope:* Subnet, Interface	List • BROADCAST • POINT-TO-POINT • POINT-TO-MULTIPOINT *Default:* (See Note)	Specifies the OSPF interface type. BROADCAST is selected when network is one-hop broadcast network like hub. POINT-TO-POINT is selected for point-to-point wired/wireless link or wireless adhoc networks. POINT-TO-MULTIPOINT is selected for point-to-multipoint interface. **Note:** The default value depends on the underlying network type of the interface.

Example OSPFv3 Configuration File

The following is an example of an OSPFv3 configuration file:

```
# Area 1
SLA-1  AREA-ID  0.0.0.1
SLA-2  AREA-ID  0.0.0.1
SLA-3  AREA-ID  0.0.0.1
SLA-4  AREA-ID  0.0.0.1
SLA-5  AREA-ID  0.0.0.1

AREA  0.0.0.1  RANGE  SLA-1, SLA-2, SLA-3, SLA-4, SLA-5  1

# Area 2
SLA-6 AREA-ID  0.0.0.2
SLA-7 AREA-ID  0.0.0.2
SLA-8 AREA-ID  0.0.0.2
SLA-9 AREA-ID  0.0.0.2
SLA-10 AREA-ID  0.0.0.2

AREA  0.0.0.2  RANGE  SLA-6, SLA-7, SLA-8, SLA-9, SLA-10 1

# Area 3 (Stub Area)
SLA-11 AREA-ID  0.0.0.3
SLA-12 AREA-ID  0.0.0.3
SLA-13 AREA-ID  0.0.0.3

AREA  0.0.0.3  RANGE  SLA-11, SLA-12, SLA-13  1

AREA  0.0.0.3  STUB  5000  1

# Backbone Area
SLA-14 AREA-ID  0.0.0.0
2000::14:0:0:0:4 AREA-ID  0.0.0.0
2000::14:0:0:0:8 AREA-ID  0.0.0.0
2000::14:0:0:0:12 AREA-ID 0.0.0.0
2000::14:0:0:0:16 AREA-ID 0.0.0.0
2000::14:0:0:0:20 AREA-ID 0.0.0.0

AREA  0.0.0.0  RANGE  SLA-14, 2000::14:0:0:0:4, 2000::14:0:0:0:8,
2000::14:0:0:0:12, 2000::14:0:0:0:16, 2000::14:0:0:0:20  1
...
SLA-1 INTERFACE-TYPE POINT-TO-MULTIPOINT
SLA-1 INTERFACE-COST 50

SLA-2 INTERFACE-TYPE POINT-TO-MULTIPOINT
SLA-2 INTERFACE-COST 50
...
```

4.5.3.2 Format of the External Routes File

The external routes file specifies external routes that can be injected into the network.

Each line in the external routes file has the following format:

```
<Node-ID> <Destination-Address> <Next-Hop> [<Cost>]
```

where

`<Node-ID>`	Node identifier.
`<Destination-Address>`	Destination address.
	This can be either a host IP address or a network IP address.
`<Next-Hop>`	IPv6 address of the next hop.
`<Cost>`	Cost associated with using this route.
	Cost is expressed as an integer value (> 0).
	This is an optional entry. If this entry is not included, the default cost is 1.

Example External Routes File

The following is an example of an external routes file:

```
1    SLA-2    2000::1:0:0:0:2    3
2    SLA-3    2000::2:0:0:0:2
3    SLA-1    2000::2:0:0:0:1    2
...
```

4.5.4 GUI Configuration

This section describes how to configure OSPFv3 in the GUI.

Configuration Requirements

To configure OSPFv3 scenario, **Network Protocol** should be set to *IPv6* or *Dual IP.*

Configuring OSPFv3 Parameters

To configure the OSPFv3 parameters, perform the following steps:

1. Go to one of the following locations:

- To set properties for a specific wireless subnet, go to **Wireless Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific wired subnet, go to **Wired Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific point-to-point link, go to **Point-to-point Link Properties Editor > Point-to-point Link Properties > Routing Protocol**.

- To set properties for a specific node, go to **Default Device Properties Editor > Node Configuration > Routing Protocol**.

- To set properties for a specific interface of a node, go to one of the following locations:

    – **Interface Properties Editor > Interfaces > Interface # > Routing Protocol**,

– **Default Device Properties Editor > Interfaces > Interface # > Routing Protocol**.

In this section, we show how to configure OSPFv3 parameters for a specific node using the Default Device Properties Editor. Parameters can be set in the other properties editors in a similar way.

2. Set **Routing Protocol IPv6** to *OSPFv3* and set the dependent parameters listed in Table 4-38.
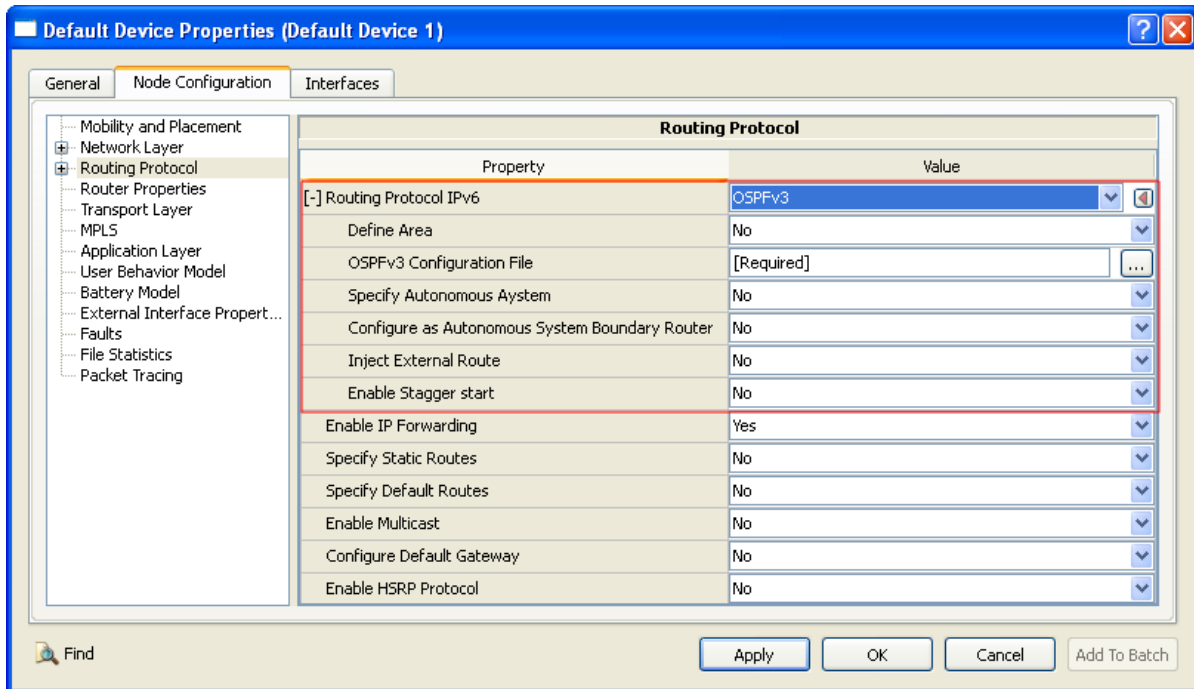
FIGURE 4-28.   Setting OSPFv3 Parameters

TABLE 4-38.   Command Line Equivalent of OSPFv3 Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Define Area	Node, Subnet, Interface	`OSPFv3-DEFINE-AREA`
OSPFv3 Configuration File	Node, Subnet, Interface	`OSPFv3-CONFIG-FILE`
Specify Autonomous System	Node, Subnet, Interface	N/A
Configure as Autonomous System Boundary Router	Node, Subnet, Interface	`AS-BOUNDARY-ROUTER`
Inject External Route	Node, Subnet, Interface	N/A
Enable Stagger Start	Node, Subnet, Interface	`OSPFv3-STAGGER-START`

Setting Parameters

- **Define Area** should be set to the same value for all nodes in an area.

- Set **OSPFv3 Configuration File** to the name of the OSPFv3 configuration file. The format of the OSPFv3 configuration file is described in Section 4.5.3.1.

- To specify autonomous system-specific parameters, set **Specify Autonomous System** to *Yes*; otherwise, set **Specify Autonomous System** to *No*.

- To enable injection of external routes, set **Inject External Route** to *Yes*; otherwise, set **Inject External Route** to *No*.

3. If **Specify Autonomous System** is set to *Yes*, then set the dependent parameters listed in Table 4-39.
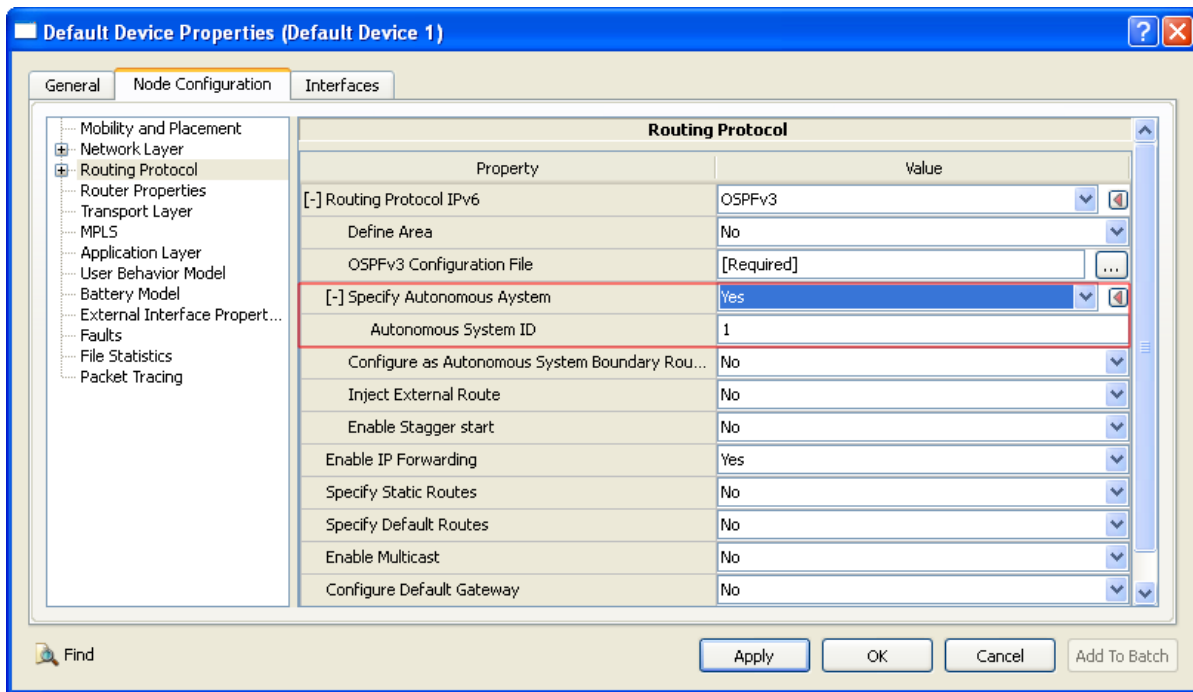
FIGURE 4-29.   Setting Autonomous System-specific Parameters

TABLE 4-39.   Command Line Equivalent of Autonomous System-specific Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Autonomous System ID	Node, Subnet, Interface	AS-NUMBER

4. If **Routing Protocol IPv6** *[= OSPFv3]* **> Inject External Route** is set to *Yes,* then set the dependent parameters listed in Table 4-40.
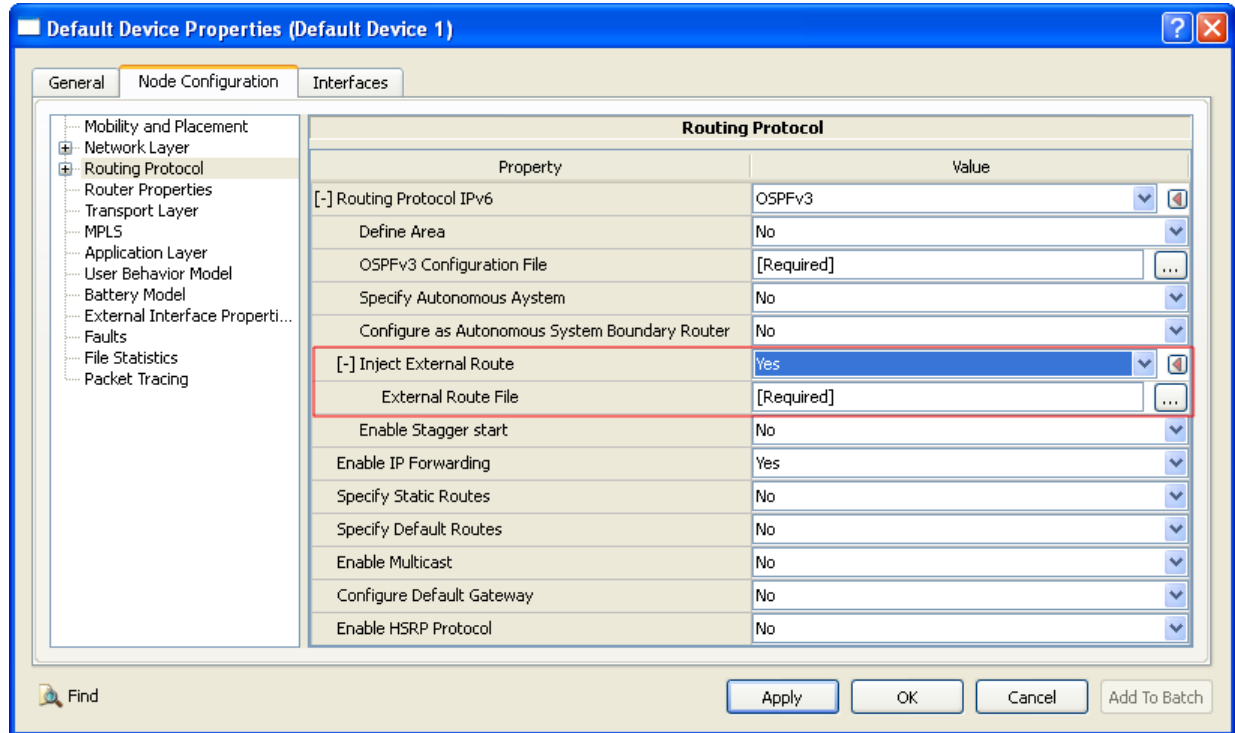
FIGURE 4-30.   Specifying External Route File

TABLE 4-40.   Command Line Equivalent of External Route File Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
External Routes File	Node, Subnet, Interface	`OSPFv3-INJECT-ROUTE-FILE`

Setting Parameters

- Set **External Route File** to the name of the external routes file. The format of the external routes file is described inSection 4.5.3.2.

Configuring Statistics Parameters

Statistics for OSPFv3 can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for routing protocols including OSPFv3, check the box labeled **Routing** in the appropriate properties editor.

TABLE 4-41.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Routing	Global, Node	`ROUTING-STATISTICS`

Configuring Packet Tracing Parameters

Packet tracing for OSPFv3 can be enabled at the global and node levels. To enable packet tracing for OSPFv3, in addition to setting the OSPFv3 trace parameter, **Trace OSPF**, several other trace parameters also need to be set. See Section 4.2.10 of *QualNet User's Guide* for details of configuring packet tracing parameters.

TABLE 4-42.   Command Line Equivalent of Packet Tracing Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Trace OSPFv3	Global, Node	`TRACE-OSPFv3`

4.5.5 Statistics

Table 4-43 lists the OSPFv3 statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 4-43.   OSPFv3 Statistics

Statistic	Description
Hello Packets Sent	Number of OSPFv3 Hello packets sent by a node.
Hello Packets Received	Number of OSPFv3 Hello packets received by a node.
Link State Update Packets Sent	Number of OSPFv3 Link State Update packets sent by a node.
Link State Update Packets Received	Number of OSPFv3 Link State Update packets received by a node.
Link State ACK Packets Sent	Number of OSPFv3 Link State Acknowledgement packets sent by a node.
Link State ACK Packets Received	Number of OSPFv3 Link State Acknowledgement packets received by a node.
Link State Update Packets Retransmitted	Number of OSPFv3 Link State Update packets retransmitted by a node.
Link State Advertisements Expired	Number of OSPFv3 Link State Advertisements expired on the node.
Database Description Packets Sent	Number of OSPFv3 Database Description packets sent by a node.
Database Description Packets Received	Number of OSPFv3 Database Description packets sent.
Database Description Packets Retransmitted	Number of OSPFv3 Database Description packets retransmitted.
Link State Request Packets Sent	Number of Link State Request packets sent by a node.
Link State Request Packets Received	Number of OSPFv3 Link State Request packets received by a node.
Link State Request Packets Retransmitted	Number of OSPFv3 Database Description packets retransmitted by a node.
Router LSA Originated	Number of OSPFv3 Router LSA packets originated by a node.
Network LSA Originated	Number of OSPFv3 Network LSA packets originated by a node.

TABLE 4-43. OSPFv3 Statistics (Continued)

Statistic	Description
Inter-Area-Prefix LSA Originated	Number of OSPFv3 Inter Area Prefix Link State Advertisement packets originated by a node.
Inter-Area-Router LSA Originated	Number of OSPFv3 Inter Area Router Link State Advertisement packets originated by a node.
Link LSA Originated	Number of OSPFv3 Link LSA packets originated by a node.
Intra-Area-Prefix LSA Originated	Number of OSPFv3 Intra Area Prefix Link State Advertisement packets originated by a node.
AS External LSA Originated	Number of OSPFv3 AS External LSA originated by a node.
Number of LSA Refreshed	Number of OSPFv3 Link State Advertisement refreshed by a node.

4.5.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the OSPFv3 model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/ospfv3. Table 4-44 lists the sub-directory where each scenario is located.

TABLE 4-44. OSPFv3 Scenarios Included in QualNet

Scenario	Description
2-as	Shows the OSPFv3 interaction with the external AS.
adhoc	Shows the OSPFv3 behavior in a simple IPv6 adhoc multiple hops wireless network.
adhoc-mobility	Shows the OSPFv3 behavior in a simple IPv6 adhoc multiple hops wireless network configured with mobility.
dr-bdr	Shows the OSPFv3 behavior in a simple IPv6 network, for DR-BDR election and LS Aging.
ipv4-ipv6-ipv4	Shows the OSPFv3 behavior in a simple IPv4-IPv6 mixed protocol network.
linkcost	Shows the OSPFv3 behavior in a simple IPv6 network for the link cost.
multiple-area	Shows the OSPFv3 behavior configured with multiple areas and origination of OSPF packets.
single-area	Shows the OSPFv3 behavior configured with single area and origination of OSPF packets.
stub-area	Shows the OSPFv3 behavior with the external AS when configured with Stub area.
wireless	Shows the OSPFv3 behavior in a simple IPv6 wireless network.

4.5.7 References

1. RFC 2740. "OSPF for IPv6." R. Coltun, D. Ferguson, J. Moy. December 1999.

2. RFC 2328. "OSPF Version 2." J. Moy. August 1998.

5 Multicast Routing Protocol Models

This chapter describes features, configuration requirements and parameters, statistics, and scenarios for Multicast Routing Protocol Models, and consists of the following sections:

- Distance Vector Multicast Routing Protocol (DVMRP)
- Multicast Extensions to OSPF (MOSPF)
- Protocol Independent Multicast Protocol: Dense Mode (PIM-DM) and Sparse Mode (PIM-SM)

5.1 Distance Vector Multicast Routing Protocol (DVMRP)

The QualNet DVMRP model is based on draft-ietf-idmr-dvmrp-v3-10.

5.1.1 Description

DVMRP is a multicast routing protocol. It is designed for traditional wired network multicast routing, and operates similarly to a distance vector routing protocol like RIPv2 (Routing Information Protocol Version 2). DVMRP is a tree-based, multicast scheme that uses Reverse Path Multicasting (RPM).

5.1.2 Omitted Features

- Aggregation for reducing the size of routing table.
- Tunneling.

5.1.3 Command Line Configuration

To select DVMRP as the mulitcast routing protocol, specify the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] MULTICAST-PROTOCOL     DVMPRP
```

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

Configuration Requirements

Use of DVMRP in a scenario requires the following:

- Internet Group Management Protocol (IGMP) must be configured. See *Developer Model Library* for details of configuring IGMP.
- A multicast group file specifying multicast groups must be configured. See *QualNet User's Guide* for details.

DVMRP Parameters

Table 5-1 lists the parameters for configuring DVMRP. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 5-1.   DVMRP Parameters

Parameter	Value	Description
MULTICAST-GROUP-FILE *Optional* *Scope:* Global	Filename	Name of the Multicast Group file. Refer to *QualNet User's Guide* for the description of the Multicast Group file.
ROUTING-STATISTICS Optional *Scope:* Global, Node	List: • YES • NO *Default:* NO	Enables statistics collection for routing protocols, including DVMRP.

5.1.4 GUI Configuration

This section describes how to configure DVMRP in the GUI.

Configuring Multicast Groups

Refer to *QualNet User's Guide* for details of configuring multicast groups using the Multicast Group Editor.

Configuring DVMRP Parameters

To configure the DVMRP parameters, perform the following steps:

1. Go to one of the following locations:

- To set wireless subnet properties, go to **Wireless Subnet Properties Editor > Routing Protocol**.
- To set properties for a specific node, go to **Node Properties Editor > Node Configuration > Routing Protocol**.
- To set properties for a specific interface of a node, go to one of the following locations:
  - **Interface Properties Editor > Interfaces > Interface # > Routing Protocol**.
  - **Default Device Properties Editor > Interfaces > Interface # > Routing Protocol**.

In this section, we show how to configure DVMRP parameters for a specific node using the Default Device Properties Editor. Parameters can be set in the other properties editors in a similar way.

2. Set **Enable Multicast** to *Yes* and set the dependent parameters listed in Table 5-2.

FIGURE 5-1.   Configuring Multicast Routing Protocols

TABLE 5-2.   Command Line Equivalent of Multicast Routing Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Group Management Protocol	Node, Subnet, Interface	`GROUP-MANAGEMENT-PROTOCOL`
Multicast Protocol	Node, Subnet, Interface	`MULTICAST-PROTOCOL`

Setting Parameters

- Set **Group Management Protocol** to *IGMP* and configure the IGMP parameters. Refer to *Developer Model Library* for details.

- Set **Multicast Protocol** to *DVMRP*.

Configuring Statistics Parameters

Statistics for DVMRP can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for multicast routing protocols including DVMRP, check the box labeled **Routing** in the appropriate properties editor.

TABLE 5-3.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Routing	Global, Node	`ROUTING-STATISTICS`

5.1.5 Statistics

Table 5-4 shows the DVMRP model statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 5-4.   DVMRP Statistics

Statistic	Description
Packets Sent	Total number of packets sent by a node.
Packets Received	Total number of packets received by a node.
Probe Packets Sent	Total number of Probe packets sent by a node.
Probe Packets Received	Total number of Probe packets received by a node.
Neighbors	Total number of neighbors of a node.
Routing Updates Sent	Total number of routing Updates sent by a node.
Routing Updates Received	Total number of routing Updates received by a node.
Triggered Updates Sent	Total number of triggered Updates sent by a node.
Prunes Sent	Total number of prunes sent by a node.
Prunes Received	Total number of prunes received by a node.
Grafts Sent	Total number of grafts sent by a node.
Grafts Received	Total number of grafts received by a node.
Graft ACKs Sent	Total number of graft ACKs sent by a node.
Graft ACKs Received	Total number of graft ACKs received by a node.
Multicast Packets Sent as Data Source	Total number of multicast packets sent as data source by a node.
Multicast Packets Forwarded	Total number of multicast data packets forwarded by a node.
Multicast Packets Discarded	Total number of multicast data packets discarded by a node.

5.1.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the DVMRP model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/dvmrp. Table 5-5 lists the sub-directory where each scenario is located.

TABLE 5-5.   DVMRP Scenarios Included in QualNet

Scenario	Description
string-graft	This scenario shows the graft operation of DVMRP in a string topology network. The multicast receiver will receive most, but not all the data sent since the receiver leaves the group and rejoins. (Causing prunes and grafts).
string-normal	This scenario shows the operation of DVMRP in a string topology network.
string-prune	This scenario shows the prune operation of DVMRP in a string topology network. The multicast receiver will not received all data sent by the source since the receiver leaves the group early, causing a prune.
tree-graft	This scenario shows the graft operation of DVMRP in a tree topology network. In this scenario, some receivers will not receive all the data sent by the source since these receivers leave the group early (thus leading to pruning) and then rejoin the group (thus leading to grafting).
tree-normal	This scenario shows the operation of DVMRP in a tree topology network.
tree-prune	This scenario shows the prune operation of DVMRP in a tree topology network. In this scenario, some receivers will not receive all the data sent by the source since these receivers leave the group early (thus leading to pruning).

5.1.7 References

1. Draft-ietf-idmr-dvmrp-v3-10. "Distance Vector Multicast Routing Protocol." T. Pusateri. August 2000.

5.2 Multicast Extensions to OSPF (MOSPF)

The QualNet MOSPF model is based on RFC 1584.

5.2.1 Description

MOSPF creates a multicast routing protocol by extending OSPFv2. These extensions are designed for traditional wired network multicast routing, and operate on top of the link state routing algorithm OSPFv2. MOSPF is a pruned tree-based multicast scheme, taking advantage of path commonality from source to destinations.

5.2.2 Command Line Configuration

To select MOSPF as the multicast routing protocol, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>]  MULTICAST-PROTOCOL    MOSPF
```

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of <Qualifier> for each scope.

Configuration Requirements

Use of MOSPF in a scenario requires the following:

- Internet Group Management Protocol (IGMP) must be configured. See *Developer Model Library* for details of configuring IGMP.
- A multicast group file specifying multicast groups must be configured. See the *QualNet User's Guide* for details.
- Routing protocol must be set to OSPFv2 for handling unicast packets. See Section 4.4 for details of configuring OSPFv2.

MOSPF Parameters

Table 5-6 describes MOSPF configuration parameters. Table 5-7 describes the parameters for configuring the MOSPF-specific tables in the statistics database tables (refer to *QualNet Statistics Database User's Guide* for details).

See Section 1.2.1.3 for a description of the format used for the parameter tables.

TABLE 5-6.   MOSPF Parameters

Parameter	Value	Description
MULTICAST-GROUP-FILE *Optional* *Scope:* Global	Filename	Name of the Multicast Group file. Refer to *QualNet User's Guide* for the description of the Multicast Group file.
INTER-AREA-MULTICAST-FORWARDER Optional *Scope:* Global, Node	Node-list	List of node IDs that are multicast forwarders. A multicast forwarder is used to configure a subset of the area border routers. They are configured to convey group-related information and to forward multicast packets when the domain is divided into multiple areas.
ROUTING-STATISTICS Optional *Scope:* Global, Node	List: • YES • NO *Default:* NO	Specifies whether MOSPF statistics are collected.
TRACE-OSPFv2 Optional *Scope:* Global, Node	List: • YES • NO *Default:* YES	Specifies whether trace is enabled for MOSPF. **Note:** To enable packet tracing, some other parameters need to be configured as well. Refer to Section 4.2.10 of *QualNet User's Guide* for details.

Table 5-7 lists the parameters for configuring MOSPF-specific tables in the statistics database.

TABLE 5-7.   MOSPF Statistics Database Tables Configuration Parameters

Parameter	Value	Description
STATS-DB-MULTICAST-MOSPF-SUMMARY-TABLE *Optional* *Scope:* Global	List: • YES • NO *Default:* NO	Indicates whether the MOSPF Summary table is to be generated. The time between consecutive entries in the MOSPF Summary table is determined by the parameter STATS-DB-SUMMARY-INTERVAL. Refer to *QualNet Statistics Database User's Guide* for details.

5.2.3 GUI Configuration

This section describes how to configure MOSPF in the GUI.

Configuring Multicast Groups

Refer to *QualNet User's Guide* for details of configuring multicast groups using the Multicast Group Editor.

Configuring MOSPF Parameters

To configure the MOSPF parameters, perform the following steps:

1. Go to one of the following locations:

- To set properties for a specific wireless subnet, go to **Wireless Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific wired subnet, go to **Wired Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific point-to-point link, go to **Point-to-point Link Properties Editor > Point-to-point Link Properties > Routing Protocol**.

- To set properties for a specific node, go to **Default Device Properties Editor > Node Configuration > Routing Protocol**.

- To set properties for a specific interface of a node, go to one of the following locations:

    - **Interface Properties Editor > Interfaces > Interface # > Routing Protocol**.

    - **Default Device Properties Editor > Interfaces > Interface # > Routing Protocol**.

In this section, we show how to configure MOSPF parameters for a specific node using the Default Device Properties Editor. Parameters can be set in the other properties editors in a similar way.

2. Set **Routing Protocol IPv4** to *OSPFv2.* See Section 4.4 for details of configuring OSPFv2.

3. Set **Enable Multicast** to *Yes* and set the dependent parameters listed in Table 5-8.
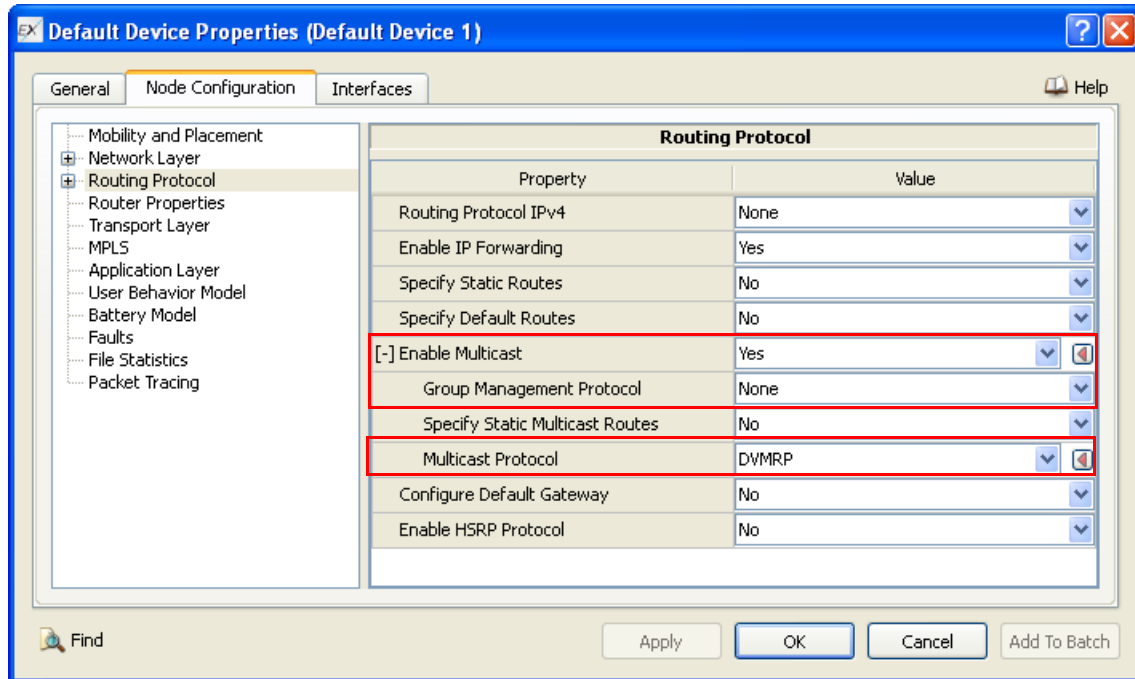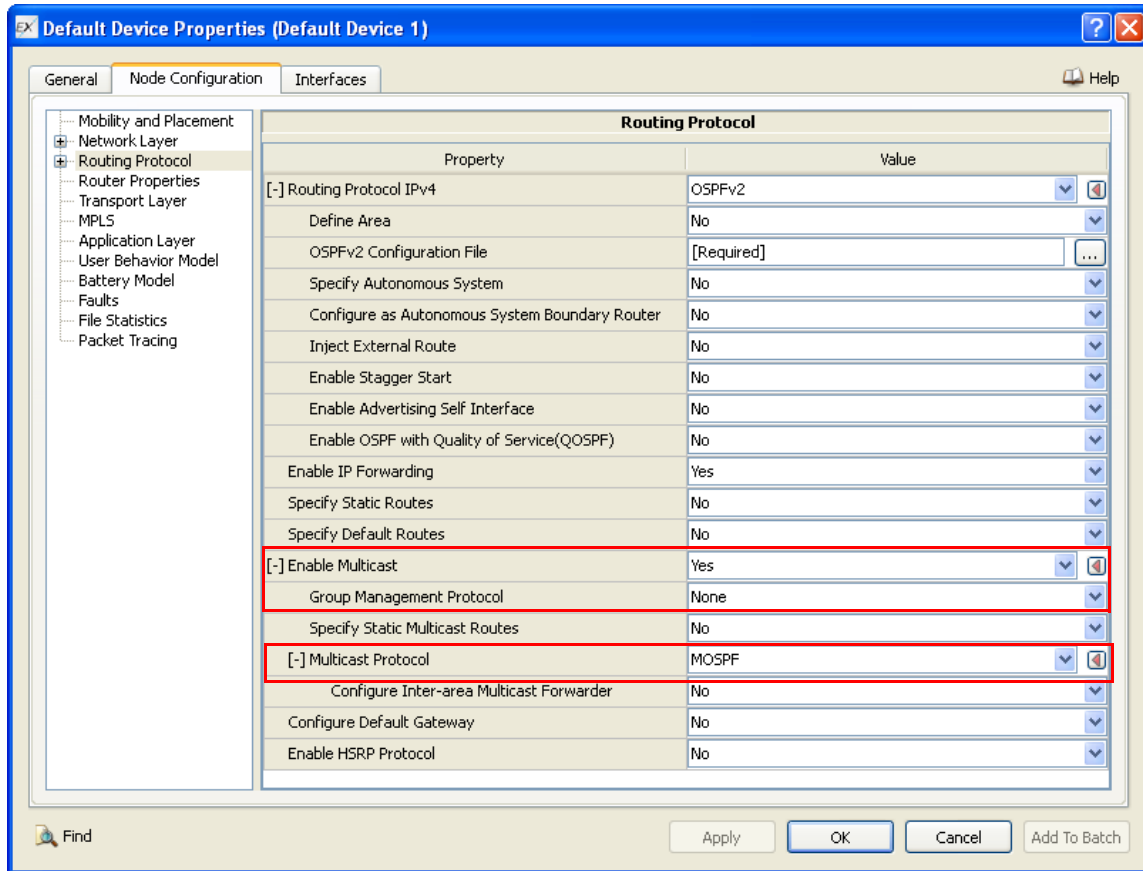

FIGURE 5-2.   Configuring Multicast Routing Protocols

TABLE 5-8.   Command Line Equivalent of Multicast Routing Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Group Management Protocol	Node, Subnet, Interface	`GROUP-MANAGEMENT-PROTOCOL`
Multicast Protocol	Node, Subnet, Interface	`MULTICAST-PROTOCOL`

Setting Parameters

- Set **Group Management Protocol** to *IGMP* and configure the IGMP parameters. Refer to *Developer Model Library* for details.
- Set **Multicast Protocol** to *MOSPF*.

4. To specify the multicast forwarder list, set **Configure Inter-area Multicast Forwarder** to *Yes*; otherwise set **Configure Inter-area Multicast Forwarder** to *No*.
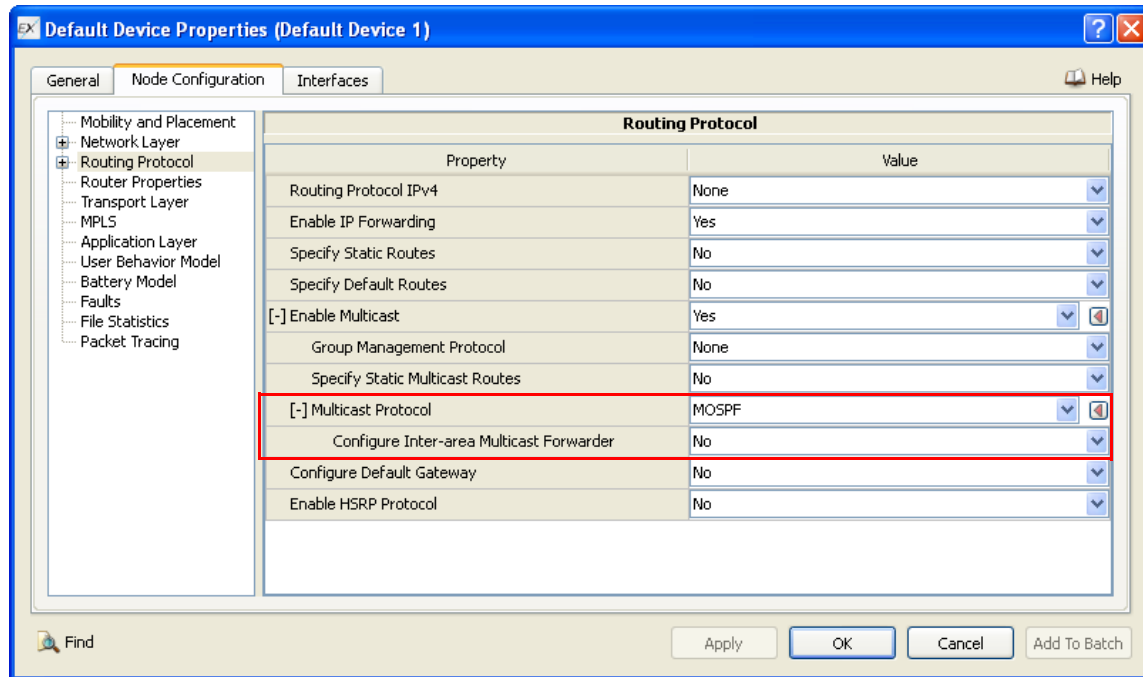
FIGURE 5-3.　Setting MOSPF Parameters

5. If **Configure Inter-area Multicast Forwarder** is set to *Yes*, then set the dependent parameters listed in Table 5-9.
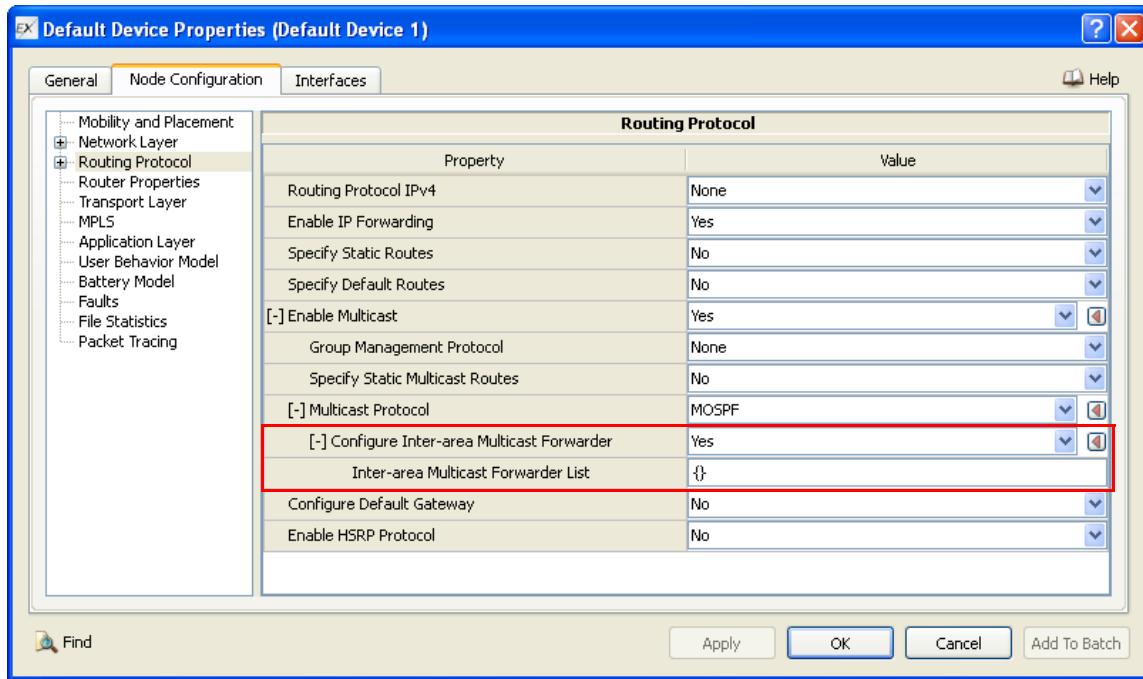
FIGURE 5-4.   Configuring Inter-area Multicast Forwarder Parameters

TABLE 5-9.   Command Line Equivalent of Configure Inter-area Multicast Forwarder Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Inter-area Multicast Forwarder List	Node	`INTER-AREA-MULTICAST-FORWARDER`

Configuring File Statistics Parameters

File statistics for MOSPF can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for routing protocols including MOSPF, check the box labeled **Routing** in the appropriate properties editor.

TABLE 5-10.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Routing	Global, Node	`ROUTING-STATISTICS`

Configuring Statistics Database Parameters

To configure the MOSPF-specific tables in the statistics database, perform the following steps:

1. Go to **Scenario Properties Editor > Statistics > Statistics Database**.

2. Set **Enable Statistics Database** to *Yes*.

3. Set **Model-specific Tables** set to *Yes* and set the MOSPF database table parameters listed in Table 5-11.
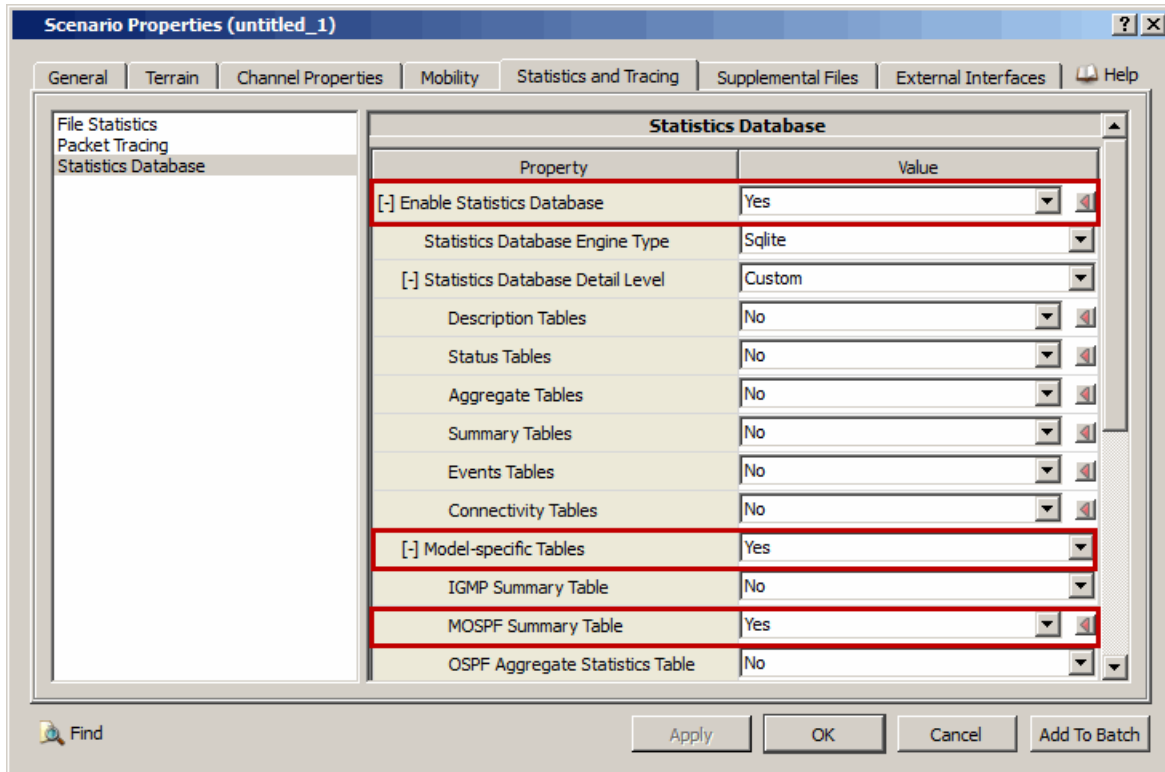
FIGURE 5-5. Configuring MOSPF Tables in Statistics Database

TABLE 5-11. Command Line Equivalent of MOSPF Statistics Database Table Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
MOSPF Summary Table	Global	`STATS-DB-MULTICAST-MOSPF-SUMMARY-TABLE`

Configuring Packet Tracing Parameters

Packet tracing for MOSPF can be enabled at the global and node levels. To enable packet tracing for OSPF, in addition to setting the MOSPF trace parameter, **Trace OSPF**, several other trace parameters also need to be set. See Section 4.2.10 of *QualNet User's Guide* for details of configuring packet tracing parameters.

TABLE 5-12.   Command Line Equivalent of Packet Tracing Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Trace OSPF	Global, Node	`TRACE-OSPFv2`

5.2.4 Statistics

This section describes the file, database, and dynamic statistics of the MOSPF model.

5.2.4.1 File Statistics

Table 5-13. lists the MOSPF statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 5-13.   MOSPF Statistics

Statistic	Description
Group Membership LSAs Generated	Number of group membership LSAs sent by the node.
Group Membership LSAs Flushed	Number of membership LSAs flushed by the node.
Group Joins	Number of group joins.
Group Leaves	Number of group leaves.
Multicast Packets Generated	Number of multicast packets sent as data source.
Multicast Packets Received	Number of multicast packets received.
Multicast Packets Discarded	Number of multicast packets discarded.
Multicast Packets Forwarded	Number of multicast packets forwarded.

5.2.4.2 Database Statistics

In addition to the file statistics, the MOSPF model also enters statistics in various scenario statistics database tables. Refer to *QualNet Statistics Database User's Guide* for details.

The MOSPF model also enters statistics in the following MOSPF-specific database table:

- MOSPF Summary Table

5.2.4.3 Dynamic Statistics

No dynamic statistics are supported for the MOSPF model.

5.2.5 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the MOSPF model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/mospf. Table 5-14 lists the sub-directory where each scenario is located.

TABLE 5-14.   MOSPF Scenarios Included in QualNet

Scenario	Description
inter-area-fault	Shows the operation of MOSPF in an inter-area topology with link fault.
inter-area-graft	Shows the graft operation of MOSPF in an inter-area topology.
inter-area-normal	Shows the normal operation of MOSPF in an inter-area topology.

TABLE 5-14. MOSPF Scenarios Included in QualNet (Continued)

Scenario	Description
inter-area-prune	Shows the prune operation of MOSPF in an inter-area topology.
string-graft	Shows the graft operation of MOSPF in a string topology network.
string-normal	Shows the normal operation of MOSPF in a string topology network.
string-prune	Shows the prune operation of MOSPF in a string topology network.
tree-graft	Shows the graft operation of MOSPF in a tree topology network.
tree-normal	Shows the normal operation of MOSPF in a tree topology network.
tree-prune	Shows the prune operation of MOSPF in a tree topology network.

5.2.6 References

1. RFC 1584. "Multicast Extensions to OSPF." J. Moy. March 1994.

5.3 Protocol Independent Multicast (PIM) Protocol: Dense and Sparse Modes

This section describes the QualNet Dense Mode Protocol Independent Multicast (PIM-DM) and Sparse Mode Protocol Independent Multicast (PIM-SM) models.

The QualNet PIM-DM model is based on draft-ietf-pim-v2-dm-03, draft-ietf-pim-dm-new-v2-05, and RFC 3973. The QualNet PIM-SM model is based on draft-ietf-pim-sm-v2-new-03, RFC 2362, and RFC 4601.

5.3.1 Description

Protocol Independent Multicast (PIM) relies on an underlying topology-gathering protocol to populate a routing table with routes. This routing table is called the MRIB or Multicast Routing Information Base. The routes in this table may be taken directly from the unicast routing table, or it may be different and provided by a separate routing protocol such as MBGP. Regardless of how it is created, the primary role of the MRIB in the PIM protocol is to provide the next hop router along a multicast-capable path to each destination subnet. The MRIB is used to determine the next hop neighbor to which any PIM Join/Prune message is sent. Data flows along the reverse path of the Join messages. Thus, in contrast to the unicast RIB which specifies the next hop that a data packet would take to get to some subnet, the MRIB gives reverse-path information, and indicates the path that a multicast data packet would take from its origin subnet to the router that has the MRIB.

5.3.1.1 Dense Mode PIM

Dense Mode PIM (PIM-DM) is a multicast routing protocol that assumes that multicast group members are densely located, that is, many or most of the routers in the area need to be involved in routing multicast datagrams. Thus it adopts a technique like RPF (Reverse Path Forwarding) that floods datagrams to every multicast router (unless a router explicitly prunes itself) if the receiving interface is the one used to forward unicast datagrams to the source of the datagram. If some areas of the network do not have group members, PIM-DM will prune off the forwarding branch by setting up prune state. The prune state has an associated timer, which on expiration will turn the interface in forwarding state and thus allowing data to go down the branch previously in prune state. The broadcast of datagrams followed by pruning of unwanted branches is often referred to as a broadcast-and-prune cycle, typical of dense mode protocol. When a new member appears in a pruned area, a router can graft towards the source for the group turning the pruned branch into forwarding state. Unlike DVMRP, which uses a built in unicast routing algorithm for topology discovery, PIM-DM relies solely on unicast routing protocol for this purpose.

5.3.1.1.1 PIM-DM Optimizations for Wireless Networks

The following optimizations can improve the performance of PIM-DM over wireless networks.

5.3.1.1.1.1 Hello Suppression

Under the assumption that every router on a multi-hop, multi-access radio network supports PIM, PIM Hellos become unnecessary. Neighbor routers can be identified by scanning the IP unicast forwarding table for route entries with the RTF_GATEWAY flag set and the gateway address set to one of the IP interface addresses of the current router onto the multi-hop, multi-access radio network. The PIM-DM model looks specifically for OSPFv2 IP addresses in the unicast forwarding table. The model identifies new neighbors and former neighbors by scanning the IP unicast forwarding table periodically according to the PIM Hello interval.

5.3.1.1.1.2 Broadcast Mode

PIM-DM exhibits significant scaling problems involving user multicast traffic flows in large routing domains. Suppression of unneeded flows to portions of the domain without any group members by means of Prune

messages is only partially effective, with the result that user traffic and Prune messages flow alternately throughout all portions of the routing domain whether there are any recipients in that portion or not. In particular, traffic and Prune messages may flow intermittently across a low-capacity radio network even for remote groups with no members or sources anywhere near the radio network itself. Although not unique to multihop radio networks, this problem is exacerbated by the longer delays and limited capacity characteristic of such networks.

PIM-DM is a purely reactive protocol. It carries no *positive* information as to multicast group membership, but only *negative* information as to non-membership. It assumes by default that all multicast traffic is to be delivered to every host or router in the routing domain. Unneeded flows are then suppressed by means of Prune messages, which may in turn be cancelled by Join messages from other routers on the same network.

In PIM-DM, Prune messages and user traffic alternate cyclically. As a result, user traffic flows intermittently even through portions of the routing domain with no group members.

PIM-DM is particularly ineffective at localizing multicast traffic at low data rates (slower than the Prune Hold timer), or at localizing bursty traffic with burst duration less than the Prune Hold timer. In such cases, by the time the Prune message is returned to the source, the source has stopped sending anyway; and by the time it resumes, the Prune Hold timer has expired. Consequently, such traffic will flow in its entirety throughout the routing domain. Under such conditions, PIM-DM would actually perform worse than simple RPF (Reversed Shortest Path Forwarding) broadcast, where every multicast packet is always distributed over reversed shortest path without any attempt at pruning.

Broadcast mode will be implemented as a configurable mode in which pruning is disabled and simple RPF broadcast is used.

5.3.1.1.1.3 Join/Prune Suppression

Optional Join/Prune suppression, as specified for PIM-SM by RFC 2362 § 2.9, is essential to permit scaling to large radio networks and is thus mandatory for both PIM-SM and PIM-DM. Although the PIM-DM specifications make no explicit mention of an equivalent mechanism for PIM-DM, the same mechanism specified for PIM-SM in RFC 2362 § 2.9 can be employed by PIM-DM as well.

5.3.1.1.1.4 Assert Optimization

When the cost between every pair of routers on a single multi-access network is the same, every exit point from the network will compute (using the usual reverse-shortest-path rules) the same entry point for each source. Thus, the combined effect of the reverse-shortest path rules at the exit points from the network and PIM Join/Prune messages generated as a result is to elect a single, common entry point to the network for each group and source (see Figure 5-6). This is the usual situation for a multi-access network, such as an Ethernet.
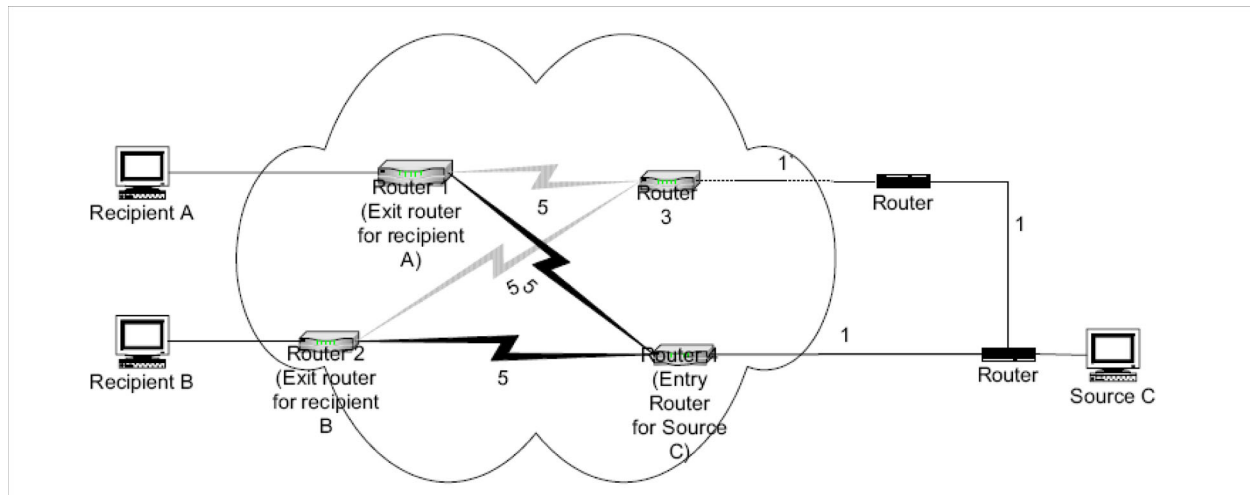
FIGURE 5-6.   Network with Same Cost between All Pairs of Routers

When the cost between every pair of routers on the radio network is the same, the reverse-shortest-path-rule applied at the exit routers automatically results in the selection of a single entry router for each source. Here, the exit routers for both recipients A and B select the same upstream router (4) as the entry router for source C, because it is the "next hop" on the shortest path back to the source from each of them.

However, the in a radio network this assumption may be violated. The cost between pairs of routers may be different. In this case, the exit routers may no longer elect a single entry point to the multi-access network through the automatic effect of the reverse-shortest-path rule. Instead, as shown in Figure 5-7, the reverse-shortest path rule may result in the choice of different entry points by each recipient, even though the source is the same.
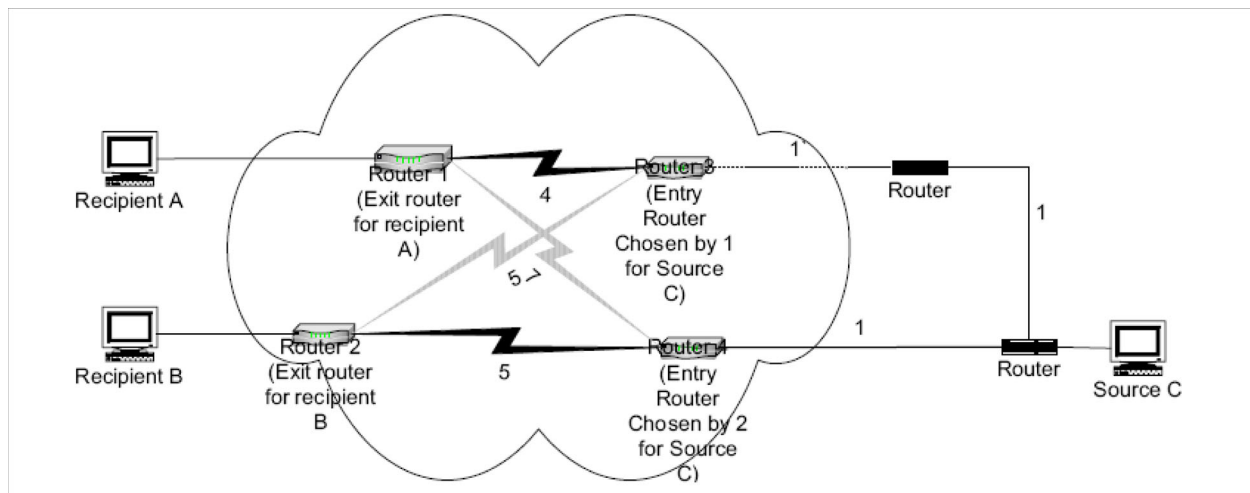
FIGURE 5-7.   Network with Different Costs between Pairs of Routers

When the cost between pairs of routers on the radio network may be different, the reverse-shortest-path rule applied at the exit routers may result in selection of different entry routers for the same source for each destination. Here, the exit routers for recipients A and B each select different upstream routers (3 and 4) as

the entry points for source C, because each finds a different upstream router to be the "next hop" on the shortest path back to the source from each.

Standard PIM enforces the election of a single entry point for each source, as shown in Figure 5-8. If multiple entry points are elected by the reverse-shortest-path rule, then the multiple entry points elect one of themselves as the preferred entry point through the exchange of Assert messages among themselves, as described in RFC 2362 § 3.5. These Assert messages are multicast on the multi-access network. The exit routers from the network listen in on the Assert traffic, and adjust their notion of the upstream router towards the relevant source accordingly. In this special case, therefore, the exit routers' idea of the upstream router towards the source may differ from the "next hop" as computed by the usual reverse-shortest-path rule.
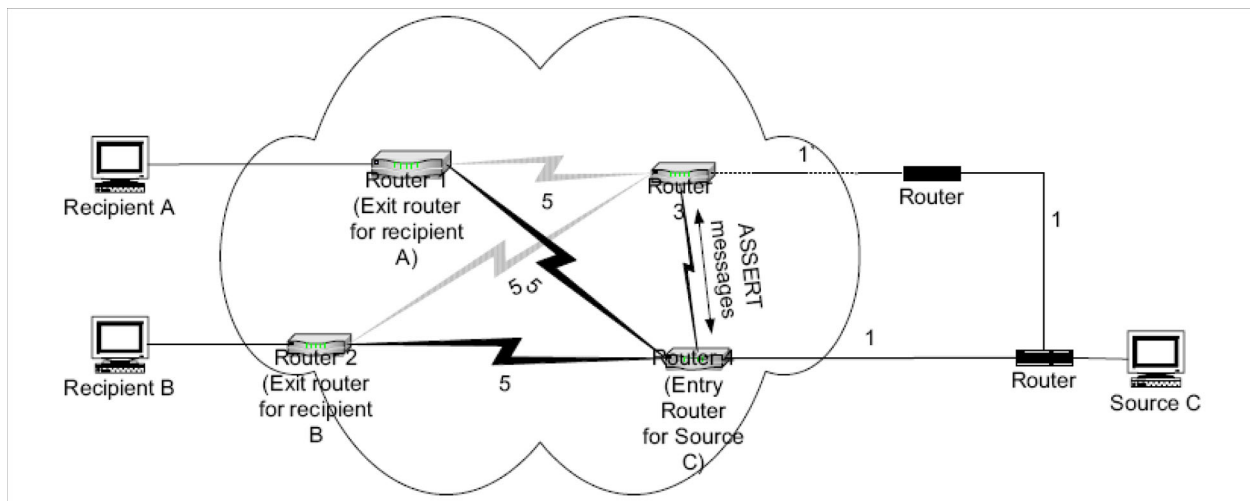
FIGURE 5-8.   Network with Assert Optimization

The standard PIM Assert mechanism does not scale well to large multi-hop radio networks. Assert messages scale worse than Join/Prune messages by a factor proportional to the number of distinct entry points computed by the reverse-shortest-path algorithms for each source. In a wireless network, the unicast cost may be different between each pair of routers, and so the reverse-shortest-path algorithms may select a large number of different entry points. Thus, it is the load from Assert messages, not the load from the Join/Prune messages that form the heart of the PIM protocol, that would become the limiting factor on a multi-hop radio network.

Reasonably good performance should be obtainable with PIM-DM by always choosing the closest entry point to the source, regardless of the distribution of group members (and hence independent of group). By its nature, PIM-DM does not perform well unless the distribution of group members is dense, and even using the standard PIM-DM Assert mechanism, every such group is likely to elect the entry point closest to the source (or a close approximation thereof) as its preferred entry point anyway. In those cases where this assumption is violated, PIM-DM is not a suitable routing algorithm anyway.

The usual Assert mechanism can be maintained, but made group-independent. Note that this requires that every entry point itself belong to every group for which it sources traffic, which is a reasonable assumption for groups supportable by PIM-DM.

5.3.1.2 Sparse Mode PIM

Sparse Mode PIM (PIM-SM) is a multicast routing protocol that can use the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared trees rooted at a Rendezvous Point (RP) per group, and optionally creates shortest-path trees per source. PIM-SM is able to route data packets from sources to receivers without either the sources or receivers knowing apriori of the existence of the others.

The multicast tree rooted at an RP, called the Rendezvous Point Tree (RPT), is shared by all receivers in all the groups to which the RP forwards packets. Each source initially encapsulates its data packets in PIM Register packets and sends them to the RP using an IP tunnel. When the RP receives such a data packet from a source, it creates the Shortest Path Tree (SPT) towards the source by initiating source-specific Joins. Once the SPT is created, subsequent data packets from the source to a receiver are sent natively (i.e., not using an IP tunnel). The Designated Router (DR) for each receiver may optionally send source-specific Joins towards the source to create a direct SPT and prune itself from the RPT.

5.3.1.2.1 Source-Specific Multicast (SSM)

In Source-Specific Multicast (SSM) routing, traffic is forwarded from a source to a receiver only if the receiver has explicitly expressed an interest in receiving traffic from that source. In the Any-Source Multicast (ASM) service model, a receiver expresses interest in receiving traffic sent to a multicast address and all traffic sent to that multicast address is forwarded to the receiver. In the SSM service model, in addition to specifying the multicast address, the receiver also specifies the sources from which it is interested in receiving traffic; traffic from only those sources is forwarded to the receiver.

The SSM service model can be implemented with a strict subset of the PIM-SM protocol mechanisms. Both regular IP multicast and SSM functionalities can coexist on a single router, and both can be implemented using the PIM-SM protocol.

In PIM-SM with SSM enabled, routers build trees that are rooted towards sources. A range of multicast addresses are reserved for SSM. For groups within SSM range, routers only generate (S,G) join/prune messages; no (*,G) or (S,Grpt) reports are sent by the routers.

5.3.1.2.2 RP Determination in Sparse Mode

Rendezvous Points can be configured statically for each PIM router or can be selected dynamically by a PIM router as follows.

1. The PIM router generates an RP set using the Bootstrap Router (BSR) mechanism as follows: A BSR is elected from the set of PIM routers that are configured to be Candidate BSRs. All the PIM routers will learn the result of this election through Bootstrap messages. The PIM routers that are configured to be Candidate RPs then report their candidacy to the elected BSR which distributes corresponding group-to-RP mappings to all the routers through Bootstrap messages. The RP set received in the Bootstrap messages is used to select the final RP.

    If the PIM router is also configured with a static RP, then that static RP is added to the RP set.

2. The final RP is selected from the RP set as follows:

    a. Perform the longest prefix match on the group-range to obtain a list of matching RPs.
    b. From this list of matching RPs, select those with the highest priority.
    c. If there is only one RP with the highest priority, use that RP.
    d. If there are multiple RPs with the highest priority, then apply a hash function. (The hash function is defined in RFC 5059. See Section 5.3.8.) Select the candidate RP with the highest hash value.
    e. If multiple RPs with the highest priority have the same hash value, then select the one with the highest IP address.

Example

Table 5-15 shows a sample RP set for a PIM router.

TABLE 5-15.   Sample RP Set

Entry	RP Address	RP Priority	Group Range	
1	190.0.1.1	10	Group-Address	225.0.0.0
			Mask	0.255.255.255
2	190.0.2.1	20	Group-Address	225.0.0.0
			Mask	0.255.255.255
3	190.0.3.1	30	Group-Address	226.0.0.0
			Mask	0.0.255.255
4	190.0.3.1	40	Group-Address	226.0.0.0
			Mask	0.255.255.255
5	190.0.5.1	50	Group-Address	227.0.0.0
			Mask	0.0.255.255
6	190.0.7.10	50	Group-Address	227.0.0.0
			Mask	0.0.255.255

The RPs selected for some of the groups are explained below.

- For G=225.0.0.1: The longest matching RP entries for this group are entries 1 and 2. Based on their priorities, entry 1 (i.e., RP address 190.0.1.1) is selected. (Note that a lower value of RP priority number implies a higher priority.)

- For G=226.0.0.1: The longest matching RP entry for this group is entry 3. Therefore, RP address 190.0.3.1. is selected.

- For G=227.0.0.1: The longest matching RP entries for this group are entries 5 and 6. These two entries have the same priority. A hash function is applied to them and the RP with the highest hash value is selected. If the hash values are the same, then the one with the higher address is selected.

5.3.1.2.3 PIM-SM Optimizations for Wireless Networks

The following optimizations can improve the performance of PIM-SM over wireless networks.

5.3.1.2.3.1 Source Rooted Tree Only Mode

This mode disables the use of RPs and directly constructs source-rooted trees upon first learning of group membership. All other PIM-SM features are left intact with the exception of RP election and joining (*, G). This means that all routers joining a particular group must join (S, G). For testing purposes, it can be assumed that the source of traffic for (S, G) is known a priori.

5.3.1.3 Sparse-Dense Mode PIM

The Sparse-Dense Mode allows an interface to operate in either Sparse or Dense Mode on a per-group basis. Dense Mode is used for a multicast group for which no RP is known, i.e., data packets destined for that particular multicast group are forwarded by using PIM-DM rules. Spare Mode is used for a multicast group for which an RP is known, i.e., data packets destined for that particular multicast group are forwarded by using PIM-SM rules. If an RP for a multicast group fails, then the mode of operation for that group changes from Sparse to Dense Mode. If the RP becomes operational again, the mode of operation switches back to Sparse Mode.

5.3.2 Features and Assumptions

This section describes the implemented features, omitted features, assumptions and limitations of the PIM model.

5.3.2.1 Implemented Features

Dense Mode

- Neighbor Discovery and Leaf Network Detection
- Maintain a Forwarding Cache
- Grafting
- Pruning
- Joining
- Assert Procedures
- Adapting to Unicast Route Change
- Advanced optimization features for wireless networks:
    - Hello Suppression
    - Broadcast Mode
    - Join/Prune Suppression
    - Assert Optimization

Sparse Mode

- Neighbor Discovery and Leaf Network Detection
- Maintain a Forwarding Cache
- Designated Forwarder Election
- Registering with RP
- Joining
- Pruning
- Assert Procedures
- Adapting to Unicast Route Change
- Receivers Switching to Source Path Tree (SPT)
- Bootstrap Router (BSR) Election
- Rendezvous Point (RP) Selection
- Optimization in wireless networks using Source Routed Tree Only Mode
- Source-Specific Multicast (SSM) routing

Sparse-Dense Mode

- Automatic switching between Sparse Mode (when an RP is known and operational) and Dense Mode (when an RP is not known or is not operational)

5.3.2.2 Omitted Features

Dense Mode

- Reduced Prune Propagation Delay on LANs
- Forwarding of State Refresh messages
- State Refresh Message origination

- Sending compound Join/Prune messages
- Inter-working with non-PIM Multicast Domains

Sparse Mode

- (*, *, RP) State
- Reducing Prune Propagation Delay on LANs
- Maintaining Secondary Address lists
- Receiving (*, *, RP) Join/Prune messages
- Sending (*, *, RP) Join/Prune Messages
- Source-specific multicast
- Join/Prune message fragmentation
- Bootstrap messages with No-Forward bit
- Unicasting bootstrap messages
- Semantic fragmentation of BSMs
- Inter-working with non-PIM Multicast Domains

5.3.2.3 Assumptions and Limitations

- Only routing protocols that update IP forwarding table should be used with PIM. Reactive (on-demand) routing protocols, such as AODV and DSR, will not work with PIM.
- For PIM-SSM IGMP version 3 must be configured. However, the QualNet PIM-SSM model does not support the EXCLUDE filter of the Multicast Group File (refer to *QualNet User's Guide*).

5.3.3 Command Line Configuration

To enable PIM, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] MULTICAST-PROTOCOL PIM
```

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of <Qualifier> for each scope.

Configuration Requirements

Use of PIM in a scenario requires the following:

- Internet Group Management Protocol (IGMP) must be configured in subnets which have multicast receivers. For PIM-SSM, IGMP version 3 must be configured. See the IGMP section of *Developer Model Library* for details of configuring IGMP.
- A multicast group file specifying subscription of nodes to multicast groups must be configured. See *QualNet User's Guide* for details.
- There can be multiple IGMP routers in a broadcast network, but it must be ensured that the elected PIM-SM DR for a multicast receiver is also configured as an IGMP router.
- To enable SSM, parameter ENABLE-SSM-ROUTING should be set to YES and the SSM routing parameters must be configured. See the IGMP section of *Developer Model Library* for details.

PIM Parameters

The PIM configuration parameters used by all modes are listed in Table 5-16. Table 5-17 lists configuration parameters for Dense Mode and Table 5-18 lists the additional configuration parameters for Sparse Mode. For Sparse-Dense Mode, both Dense Mode and Sparse Mode parameters must be configured.

Table 5-19 describes the parameters for configuring the PIM-specific tables in the statistics database tables (refer to *QualNet Statistics Database User's Guide* for details).

See Section 1.2.1.3 for a description of the format used for the parameter tables.

TABLE 5-16.   PIM Parameters for All Modes

Parameter	Value	Description
MULTICAST-GROUP-FILE *Optional* *Scope:* Global	Filename	Name of the Multicast Group file. Refer to *QualNet User's Guide* for the description of the Multicast Group file.
PIM-ROUTING-MODE *Required* *Scope:* All	List: • DENSE • SPARSE • SPARSE-DENSE	Specifies the PIM routing mode. If PIM-ROUTING-MODE is set to DENSE, then set the additional Dense Mode parameters listed in Table 5-17. If PIM-ROUTING-MODE is set to SPARSE, then set the additional Sparse Mode parameters listed in Table 5-18. If PIM-ROUTING-MODE is set to SPARSE-DENSE, then set the additional Dense Mode and Sparse Mode parameters listed in Table 5-17 and Table 5-18.
ROUTING-PIM-HELLO-PERIOD *Optional* *Scope:* All	Time *Range:* > 0S *Default:* 30S	Specifies the default time period for sending Hello messages.
ROUTING-STATISTICS *Optional* *Scope:* Global, Node	List: • YES • NO *Default:* NO	Indicates whether statistics are collected for PIM protocol.

Table 5-17 lists the additional configuration parameters for Dense Mode.

TABLE 5-17.   Additional Dense Mode Parameters

Parameter	Value	Description
ROUTING-PIMDM-HELLO-SUPPRESSION Optional *Scope:* All	List: • YES • NO *Default:* NO	Specifies whether to enable Hello suppression in Dense Mode. In this mode, new and former neighbors are identified by scanning the IP unicast forwarding table periodically according to the PIM Hello interval.

TABLE 5-17.   Additional Dense Mode Parameters (Continued)

Parameter	Value	Description
ROUTING-PIMDM-BROADCAST-MODE Optional *Scope:* All	List: • YES • NO *Default:* NO	Specifies whether to enable broadcast mode in Dense Mode. In broadcast mode, pruning is disabled and simple RPF broadcast is used.
ROUTING-PIMDM-JOIN-PRUNE-SUPPRESSION Optional *Scope:* All	List: • YES • NO *Default:* NO	Specifies whether to enable Join/Prune suppression in Dense Mode. Join/Prune suppression can be used to reduce the unnecessary Join/Prune message generated in one broadcast subnet.
ROUTING-PIMDM-ASSERT-OPTIMIZATION Optional *Scope:* All	List: • YES • NO *Default:* NO	Specifies whether to enable Assert optimization in Dense Mode. This mode can be used to resolve the issue of different entry points selected by each recipient in the same broadcast subnet, even though the source is the same.

Table 5-18 lists the additional configuration parameters for Sparse Mode.

TABLE 5-18.　Additional Sparse Mode Parameters

Parameter	Value	Description
ROUTING-PIM-DR-PRIORITY Optional *Scope:* All	Integer *Range:* ≥ 0 *Default:* 1	Priority of the router to be elected the Designated Router (DR). This priority is sent in Hello messages and is used in the Designated Router (DR) election algorithm.

ROUTING-PIMSM-SWITCH-SPT-THRESHOLD
 	
Optional
 	
Scope: All
	String
	
	Default: see description
		Specifies the packet threshold above which PIM router switches to SPT tree.
		
		This parameter is specified as a string which has the following format:
		
		`<num-packets> GROUP-RANGE`
		`<group-range-spec>`
		
		where
		
		`<num-packets>`　Number of packets above which router switches to SPT tree.
		
		`<group-range-spec>`　Range of multicast groups to which this threshold applies. See note 1 for the format of the string that specifies the group range.
		
		Example:
		
		`3 GROUP-RANGE`
		`<225.0.0.0,255.255.255.255>`
		`<226.0.0.0,0.0.0.255>`
		
		In this example, if the number of packets received in any of the groups specified by the group range spec is larger than 3, then the PIM router switches to SPT tree in that group.
		
		The default value of this parameter is:
		
		`1 GROUP-RANGE`
		`<224.0.0.0,15.255.255.255>`

PIM-SM-CANDIDATE-RP Optional *Scope:* All	List: • YES • NO *Default:* NO	Specifies whether the node is a candidate to become an RP. The candidate RPs report their candidacy to the elected BSR learned through Bootstrap messages. A subset of the candidate RPs are eventually used as the actual RPs for the domain.
ROUTING-PIMSM-CANDIDATE-RP-TIMEOUT Optional *Scope:* All	Time *Range:* > 0S *Default:* 60S	Specifies the RP timeout. Routers configured as candidate RP's use this timer to periodically send Candidate-RP-Advertisement messages to the elected BSR.

TABLE 5-18.   Additional Sparse Mode Parameters (Continued)

Parameter	Value	Description
PIM-SM-CANDIDATE-RP-PRIORITY Optional *Scope:* All	Integer *Range:* [0, 255] *Default:* 192	Specifies the RP priority for the candidate RP. If more than one candidate RPs support the same group, then the candidate RP with the highest priority will be chosen as the final RP for that group. **Note:** The lower the value of this parameter, the higher the priority.
PIM-SM-RP-GROUP-RANGE Optional *Scope:* All	String *Default:* see description	Specifies the RP group range supported by the candidate RP. See note 1 for the format of the string that specifies the group range. The default value of this parameter is: <224.0.0.0,15.255.255.255>
PIM-SM-CANDIDATE-BSR Optional *Scope:* All	List: • YES • NO *Default:* NO	Specifies whether the node is a candidate to become a Bootstrap Router (BSR). One of the candidate BSRs is elected as the bootstrap router. All PIM routers in the domain learn the outcome of the election via Bootstrap messages.
PIM-SM-CANDIDATE-BSR-PRIORITY Optional *Scope:* All	Integer *Range:* [0, 255] *Default:* 64	Specifies the BSR priority for the candidate BSR. **Note:** The higher the value of this parameter, the higher the priority.
ROUTING-PIMSM-BOOTSTRAP-TIMEOUT Optional *Scope:* All	Time *Range:* > 0S *Default:* 60S	Specifies the time after which the elected BSR will be assumed to be unreachable when Bootstrap messages are not received from it.
PIM-SM-STATIC-NUMBER-OF-RP Optional *Scope:* All	Integer *Range:* ≥ 1	Specifies the number of static RPs whose IP address is specified in the scenario configuration (.config) file.
PIM-SM-STATIC-RP-ADDRESS Optional *Scope:* All *Instances:* RP number (see description)	IPv4 Address	Specifies the IPv4 address of the static RP. If parameter PIM-SM-STATIC-NUMBER-OF-RP is specified, then there should be PIM-SM-STATIC-NUMBER-OF-RP instances of PIM-SM-STATIC-RP-ADDRESS. If parameter PIM-SM-STATIC-NUMBER-OF-RP is not specified, then there should be one instance of PIM-SM-STATIC-RP-ADDRESS. If parameter PIM-SM-STATIC-NUMBER-OF-RP is specified and set to 1, then the IPv4 address of the static RP should be specified by the parameter instance PIM-SM-STATIC-RP-ADDRESS[0].

TABLE 5-18.   Additional Sparse Mode Parameters (Continued)

Parameter	Value	Description
PIM-SM-STATIC-RP-PRIORITY Optional *Scope:* All *Instances:* RP number (see description)	Integer *Range:* [0, 255] *Default:* 192	Specifies the RP priority for the static RP. If more than one RPs support the same group, then the RP with the highest priority will be chosen as the final RP for that group. If parameter PIM-SM-STATIC-NUMBER-OF-RP is specified, then there should be PIM-SM-STATIC-NUMBER-OF-RP instances of PIM-SM-STATIC-RP-PRIORITY. If parameter PIM-SM-STATIC-NUMBER-OF-RP is not specified, then there should be one instance of PIM-SM-STATIC-RP-PRIORITY. If parameter PIM-SM-STATIC-NUMBER-OF-RP is specified and set to 1, then the RP priority should be specified by the parameter instance PIM-SM-STATIC-RP-PRIORITY[0]. **Note:** The lower the value of this parameter, the higher the priority.
PIM-SM-STATIC-RP-GROUP-RANGE Optional *Scope:* All *Instances:* RP number (see description)	String *Default:* see description	Specifies the RP group range supported by the static RP. If parameter PIM-SM-STATIC-NUMBER-OF-RP is specified, then there should be PIM-SM-STATIC-NUMBER-OF-RP instances of PIM-SM-STATIC-RP-GROUP-RANGE. If parameter PIM-SM-STATIC-NUMBER-OF-RP is not specified, then there should be one instance of PIM-SM-STATIC-RP-GROUP-RANGE. If parameter PIM-SM-STATIC-NUMBER-OF-RP is specified and set to 1, then the RP group range should be specified by the parameter instance PIM-SM-STATIC-RP-GROUP-RANGE[0]. See note 1 for the format of the string that specifies the group range. The default value of this parameter is: <224.0.0.0,15.255.255.255>
ROUTING-PIMSM-TRIGGERED-DELAY Optional *Scope:* All	Time *Range:* > 0S *Default:* 30S	Specifies the delay between sending triggered PIM messages, e.g., a triggered Hello message that is sent when a new neighbor is discovered or a triggered Join message.
ROUTING-PIMSM-KEEPALIVE-TIMEOUT Optional *Scope:* All	Time *Range:* > 0S *Default:* 210S	Specifies time-to-live for a message in the network. Once the time is reached, the message is dropped and is not transmitted again.

TABLE 5-18. Additional Sparse Mode Parameters (Continued)

Parameter	Value	Description
ROUTING-PIMSM-JOINPRUNE-HOLD-TIMEOUT Optional *Scope:* All	Time *Range:* > 0S *Default:* 210S	Specifies hold time to be sent in Join/Prune messages in either periodic or triggered join/prunes. This is the default time period used to time out the Join/Prune state of a downstream interface. It is recommended that this be set to 3.5 *ROUTING-PIMSM-T-PERIODIC-INTERVAL.
ROUTING-PIMSM-T-PERIODIC-INTERVAL Optional *Scope:* All	Time *Range:* > 0S *Default:* 60S	Specifies the upstream join timer value after which periodic Join messages are sent to the upstream router.
ROUTING-PIMSM-ASSERT-TIMEOUT Optional *Scope:* All	Time *Range:* > 0S *Default:* 180S	Specifies the timeout interval for an Assert state.
ROUTING-PIMSM-REGISTER-SUPRESSION-TIME Optional *Scope:* All	Time *Range:* > 0S *Default:* 60S	Specifies the mean interval between receiving a Register-Stop and allowing Registers to be sent again. A lower value results in more frequent register bursts at RP, while a higher value results in a longer join latency for new receivers.
ROUTING-PIMSM-REGISTER-PROBE-TIME Optional *Scope:* All	Time *Range:* > 0S *Default:* 5S	Specifies the time before the Register-Suppression timer expires when a DR may send a Null-Register message to the RP to cause it to resend a Register-Stop message. **Note:** This parameter must be set to a value less than half the value of ROUTING-PIMSM-REGISTER-SUPRESSION-TIME to prevent a negative value for the Register-Stop timer.
ROUTING-PIMSM-DIRECT-SPT Optional *Scope:* All	List: • YES • NO *Default:* NO	Specifies whether to enable source-rooted tree only mode in PIM-SM mode. This mode disables the use of RPs and directly constructs source-rooted trees upon first learning of group membership. All other PIM-SM features are left intact with the exception of RP election and joining (*, G).
ROUTING-PIMSM-SOURCE-GROUP-PAIR Optional *Scope:* All	String (see note 2)	Specifies the pairs of source address and the corresponding group address. This parameter is used only if ROUTING-PIMSM-DIRECT-SPT is set to YES. See note 2 for the format of the string that specifies pairs of source and group addresses.

Notes: 1. Group ranges are specified as string composed of group address and subnet masks in the following format:

<Group-Address-1, *Subnet-Mask-1> <Group-Address-2*, *Subnet-Mask-2> ….*

where

Group-Address-i is the address of the ith group

Subnet-Mask-i the subnet mask for the ith group

Example:
```
<228.0.0.0, 0.0.0.255> <230.0.15.240, 0.0.0.0>
```

In this example, for the group range `<228.0.0.0, 0.0.0.255>`, the number of bits used to mask the group address `228.0.0.0` is 24 (number of leading zero bits in `0.0.0.255`). Therefore, the group range is `228.0.0.1` to `228.0.0.255`.

For the group range `<230.0.15.240, 0.0.0.0>`, the number of bits used to mask the group address `230.0.15.240` is 32 (number of leading zero bits in `0.0.0.0`). Therefore, the group range supported by this PIM router is `230.0.15.240` to `230.0.15.240`, i.e., the single group address `230.0.15.240`.

2. The value of the parameter `ROUTING-PIMSM-SOURCE-GROUP-PAIR` is a string composed of pairs of source and group addresses in the following format:

<Source-Address-1, *Group-Address-1> <Source-Address-2, Group-Address-2> ….*

where

Source-Address-i is the address of the source of multicast traffic to the ith group

Group-Address-i the address of the ith multicast group

Example:
```
ROUTING-PIMSM-SOURCE-GROUP-PAIR <10.1.1.1, 224.0.0.1> <10.1.1.2,
    224.0.0.2>
```

Table 5-19 lists the parameters for configuring PIM-specific tables in the statistics database.

TABLE 5-19.   PIM Statistics Database Tables Configuration Parameters

Parameter	Value	Description
`STATS-DB-MULTICAST-PIM-DM-SUMMARY-TABLE` *Optional* *Scope:* Global	List: • `YES` • `NO` *Default:* `NO`	Indicates whether the PIM-DM Summary table is to be generated. The time between consecutive entries in the PIM-DM Summary table is determined by the parameter `STATS-DB-SUMMARY-INTERVAL` (refer to *QualNet Statistics Database User's Guide*).

TABLE 5-19.   PIM Statistics Database Tables Configuration Parameters (Continued)

Parameter	Value	Description
`STATS-DB-MULTICAST-PIM-SM-STATUS-TABLE` *Optional* *Scope:* Global	List: • `YES` • `NO` *Default:* `NO`	Indicates whether the PIM-SM Status table is to be generated. The time between consecutive entries in the PIM-SM Status table is determined by the parameter `STATS-DB-STATUS-INTERVAL` (refer to *QualNet Statistics Database User's Guide*).
`STATS-DB-MULTICAST-PIM-SM-SUMMARY-TABLE` *Optional* *Scope:* Global	List: • `YES` • `NO` *Default:* `NO`	Indicates whether the PIM-SM Summary table is to be generated. The time between consecutive entries in the PIM-SM Summary table is determined by the parameter `STATS-DB-SUMMARY-INTERVAL` (refer to *QualNet Statistics Database User's Guide*).

5.3.4 GUI Configuration

This section describes how to configure PIM in GUI.

Configuration Requirements

Use of PIM in a scenario requires the following:

- Internet Group Management Protocol (IGMP) must be configured in subnets which have multicast receivers. For PIM-SSM, IGMP version 3 must be configured. See the IGMP section of *Developer Model Library* for details of configuring IGMP.

- A multicast group file specifying subscription of nodes to multicast groups must be configured. See *QualNet User's Guide* for details.

- There can be multiple IGMP routers in a broadcast network, but it must be ensured that the elected PIM-SM DR for a multicast receiver is also configured as an IGMP router.

- To enable SSM, parameter `ENABLE-SSM-ROUTING` should be set to `YES` and the SSM routing parameters must be configured. See the IGMP section of *Developer Model Library* for details.

Section 5.3.4.2 describes how to set the general PIM parameters. Section 5.3.4.3 describes how to set the Dense Mode parameters. Section 5.3.4.4 describes how to set the Sparse Mode parameters. Section 5.3.4.5 describes how to set the Sparse-Dense Mode parameters. Section 5.3.4.7 describes how to set the file statistics parameters. Section 5.3.4.8 describes how to set the database statistics parameters.

5.3.4.1 Configuring Multicast Groups

Refer to *QualNet User's Guide* for details of configuring multicast groups using the Multicast Group Editor.

5.3.4.2 Configuring General PIM Parameters

To configure the general PIM parameters, perform the following steps:

1. Go to one of the following locations:

- To set properties for a specific wireless subnet, go to **Wireless Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific wired subnet, go to **Wired Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific point-to-point link, go to **Point-to-point Link Properties Editor > Point-to-point Link Properties > Routing Protocol**.

- To set properties for a specific node, go to **Default Device Properties Editor > Node Configuration > Routing Protocol**.

- To set properties for a specific interface of a node, go to one of the following locations:

  - **Interface Properties Editor > Interfaces > Interface # > Routing Protocol**.

  - **Default Device Properties Editor > Interfaces > Interface # > Routing Protocol**.

In this section, we show how to configure PIM parameters for a specific node using the Default Device Properties Editor. Parameters can be set in the other properties editors in a similar way.

2. Set **Enable Multicast** to *Yes* and set the dependent parameters listed in Table 5-20.
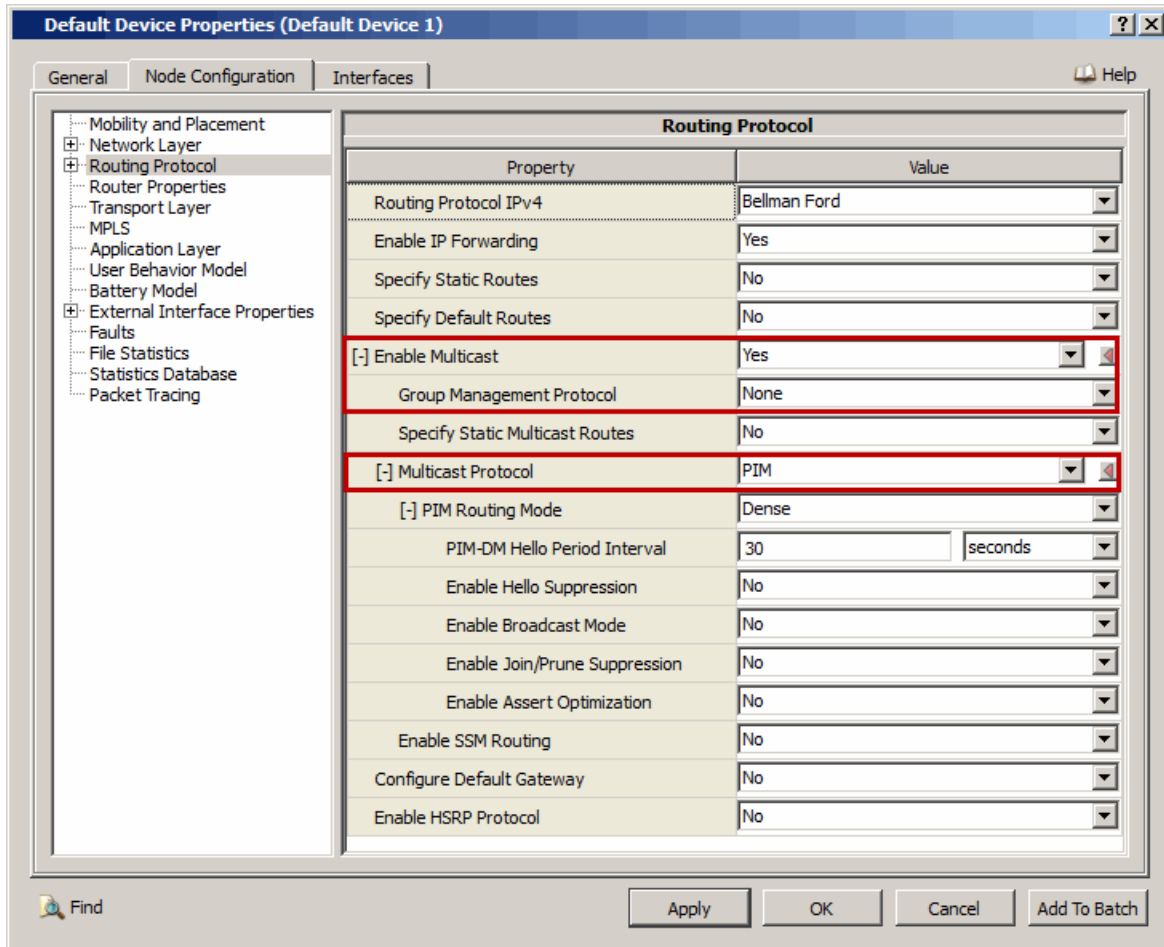
FIGURE 5-9.   Configuring Multicast Routing Protocols

TABLE 5-20.   Command Line Equivalent of Multicast Routing Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Group Management Protocol	Node, Subnet, Interface	`GROUP-MANAGEMENT-PROTOCOL`
Multicast Protocol	Node, Subnet, Interface	`MULTICAST-PROTOCOL`

Setting Parameters

- **Set Group Management Protocol** to *IGMP* and configure the IGMP parameters. Refer to *Developer Model Library* for details.
- **Set Multicast Protocol** to *PIM*.

3. Set the PIM parameters listed in Table 5-21.
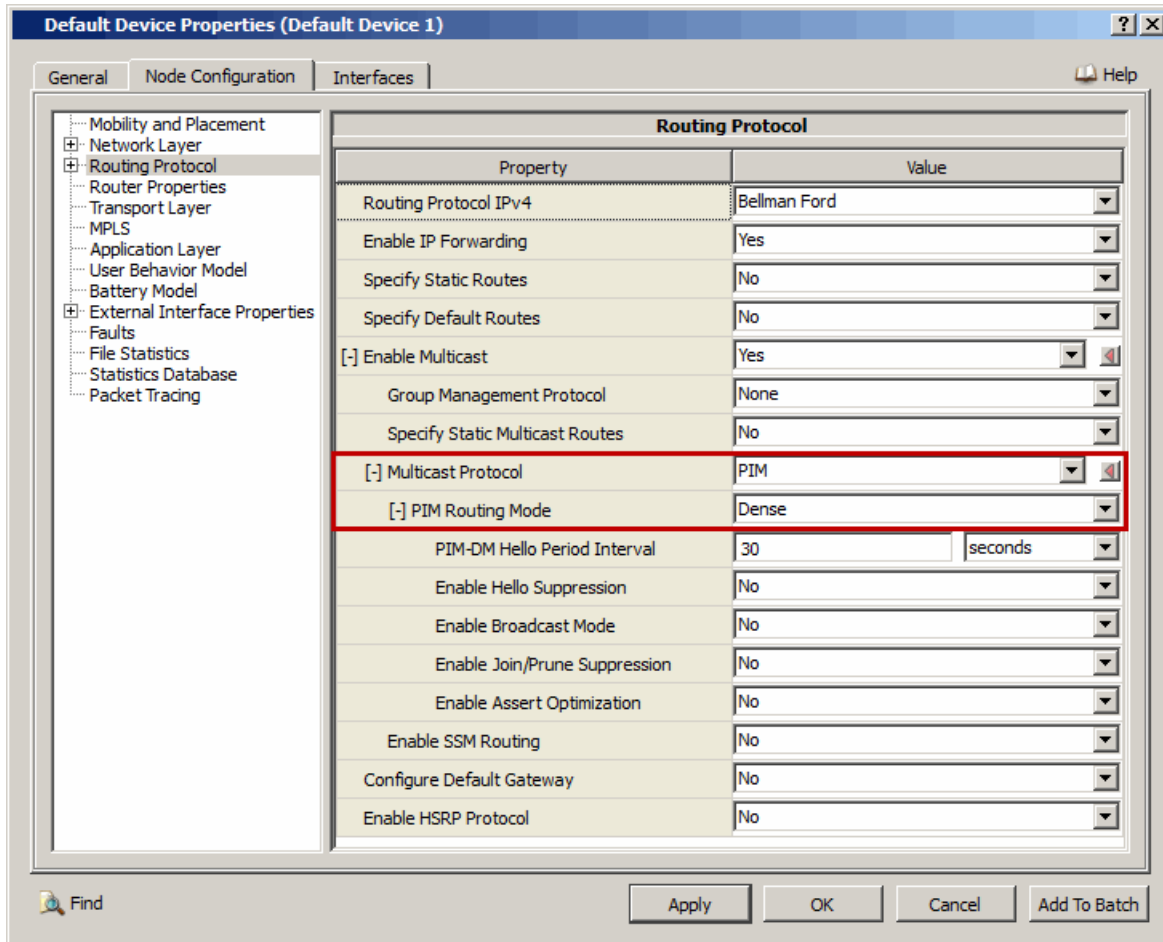
FIGURE 5-10.   Setting General PIM Parameters

TABLE 5-21.   Command Line Equivalent of PIM Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
PIM Routing Mode	Node, Subnet, Interface	PIM-ROUTING-MODE

Setting Parameters

- Set **PIM Routing Mode** to *Dense* to enable PIM in Dense Mode.
- Set **PIM Routing Mode** to *Sparse* to enable PIM in Sparse Mode.
- Set **PIM Routing Mode** to *Sparse-Dense* to enable PIM in Sparse-Dense Mode.

5.3.4.3 Configuring Dense Mode Parameters

To configure the Dense Mode parameters, perform the following steps:

1. Configure the general PIM parameters as described in Section 5.3.4.2. Set **PIM Routing Mode** to *Dense.*

2. **Set the dependent parameters listed in** Table 5-22**.**
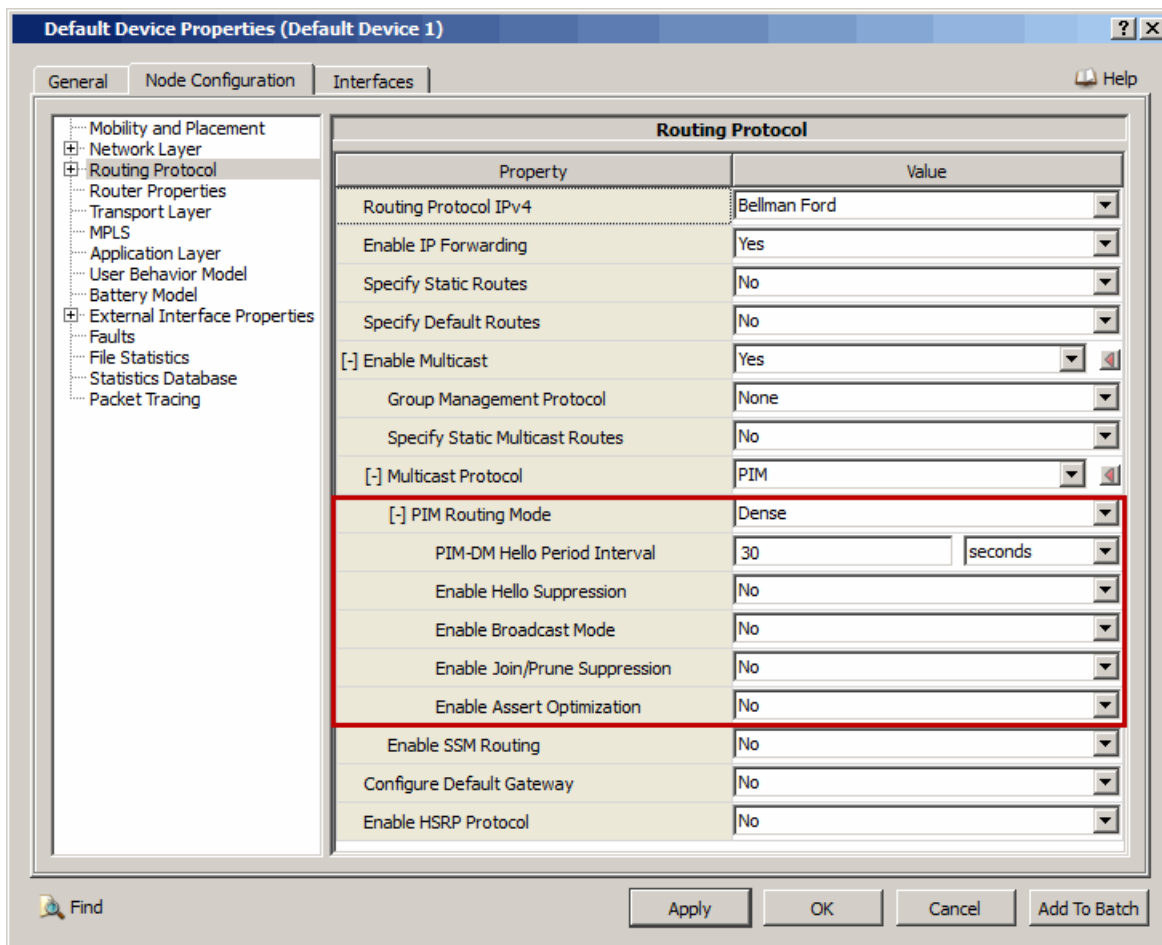
FIGURE 5-11.   Setting Dense Mode Parameters

TABLE 5-22.   Command Line Equivalent of Dense Mode Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
PIM-DM Hello Period Interval	Node, Subnet, Interface	ROUTING-PIM-HELLO-PERIOD
Enable Hello Suppression	Node, Subnet, Interface	ROUTING-PIMDM-HELLO-SUPPRESSION
Enable Broadcast Mode	Node, Subnet, Interface	ROUTING-PIMDM-BROADCAST-MODE
Enable Join/Prune Suppression	Node, Subnet, Interface	ROUTING-PIMDM-JOIN-PRUNE-SUPPRESSION
Enable Assert Optimization	Node, Subnet, Interface	ROUTING-PIMDM-ASSERT-OPTIMIZATION

5.3.4.4 Configuring Sparse Mode Parameters

To configure the Sparse Mode parameters, perform the following steps:

1. Configure the general PIM parameters as described in Section 5.3.4.2. Set **PIM Routing Mode** to *Sparse.*

2. Set the dependent parameters listed in Table 5-23.

FIGURE 5-12.   Setting Sparse Mode Parameters

TABLE 5-23.   Command Line Equivalent of Sparse Mode Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
PIM-SM Hello Period Interval	Node, Subnet, Interface	`ROUTING-PIM-HELLO-PERIOD`
PIM-SM DR Priority	Node, Subnet, Interface	`ROUTING-PIM-DR-PRIORITY`
PIM-SM Switch To SPT	Node, Subnet, Interface	N/A
PIM-SM Static RP Present	Node, Subnet, Interface	N/A
PIM-SM Triggered Delay	Node, Subnet, Interface	`ROUTING-PIMSM-TRIGGERED-DELAY`
PIM-SM Keep-alive Timeout Interval	Node, Subnet, Interface	`ROUTING-PIMSM-KEEPALIVE-TIMEOUT`
PIM-SM Join/Prune Hold Timeout Interval	Node, Subnet, Interface	`ROUTING-PIMSM-JOINPRUNE-HOLD-TIMEOUT`
PIM-SM T Periodic Interval	Node, Subnet, Interface	`ROUTING-PIMSM-T-PERIODIC-INTERVAL`
PIM-SM Assert Timeout Interval	Node, Subnet, Interface	`ROUTING-PIMSM-ASSERT-TIMEOUT`
PIM-SM Registered Supression Time	Node, Subnet, Interface	`ROUTING-PIMSM-REGISTER-SUPRESSION-TIME`
PIM-SM Register Probe Time	Node, Subnet, Interface	`ROUTING-PIMSM-REGISTER-PROBE-TIME`
Use SPT Directly	Node, Subnet, Interface	`ROUTING-PIMSM-DIRECT-SPT`

Setting Parameters

- To specify a threshold for switching to SPT, set **PIM-SM Switch to SPT** to *Yes*; otherwise, set **PIM-SM Switch to SPT** to *No*.

- To configure static RPs, set **PIM-SM Static RP Present** to *Yes*; otherwise, set **PIM-SM Static RP Present** to *No*.

3. If **PIM-SM Switch to SPT** is set to *Yes*, then set the dependent parameters listed in Table 5-24.
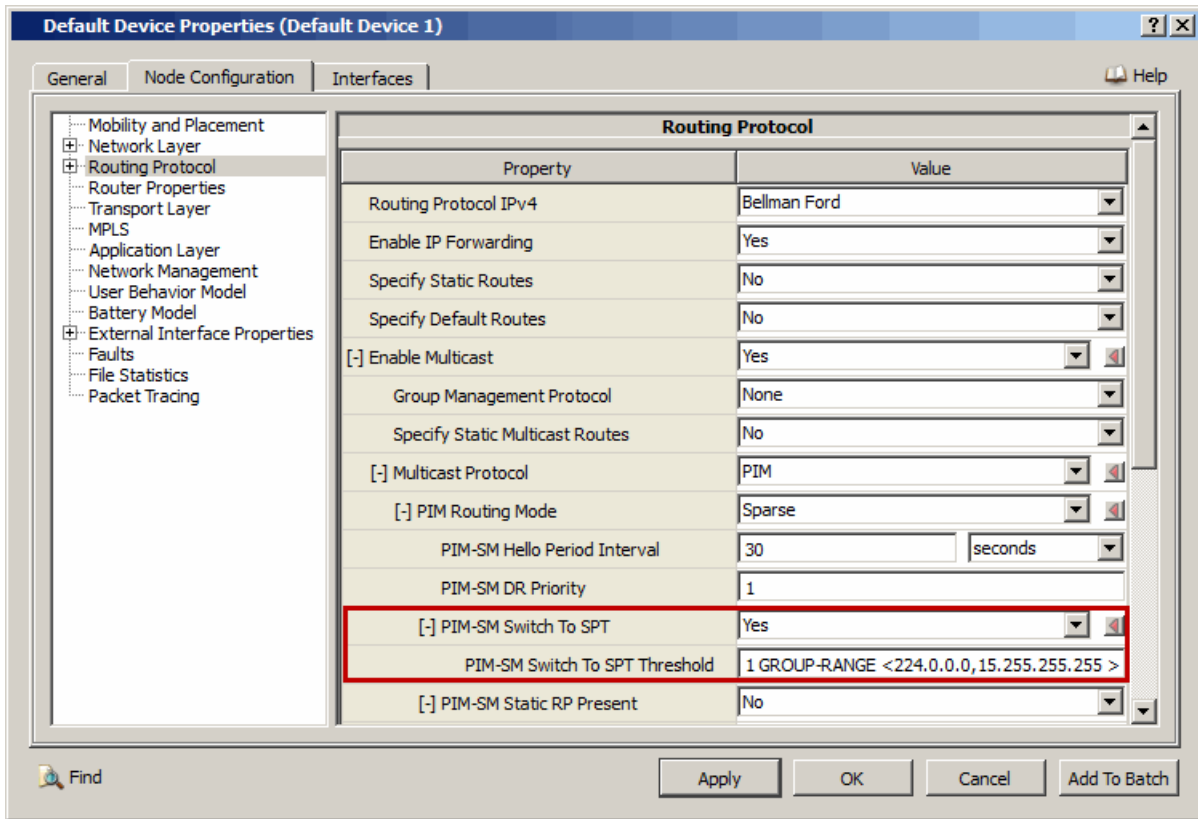
FIGURE 5-13.   Setting SPT Threshold Parameters

TABLE 5-24.   Command Line Equivalent of SPT Threshold Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
PIM-SM Switch To SPT Threshold	Node, Subnet, Interface	`ROUTING-PIMSM-SWITCH-SPT-THRESHOLD`

Setting Parameters

- See Section 5.3.3 for the format of the value of the parameter **PIM-SM Switch To SPT Threshold**.

4. If **PIM-SM Static RP Present** is set to *No*, then set the dependent parameters listed in Table 5-25.
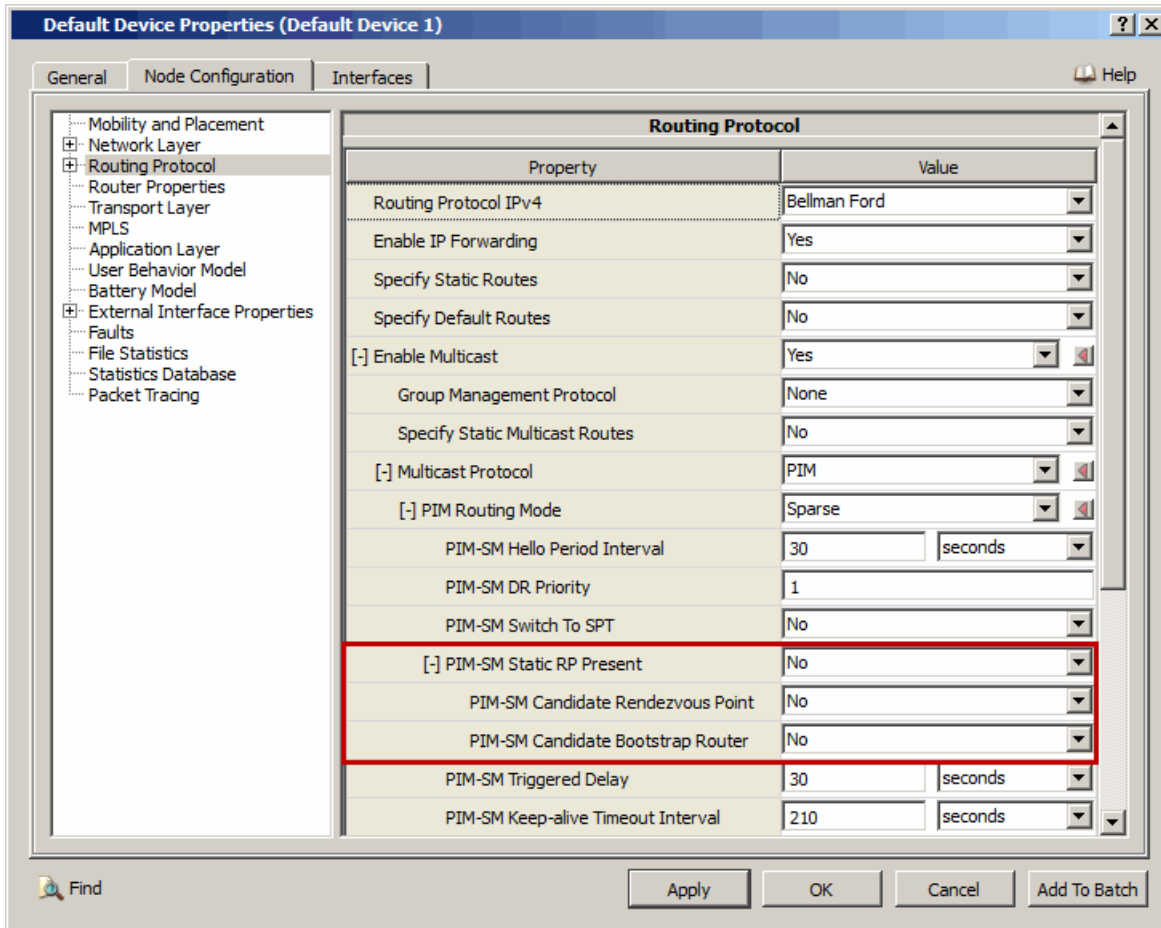
FIGURE 5-14.   Setting RP Election Parameters

TABLE 5-25.   Command Line Equivalent of RP Election Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
PIM-SM Candidate Rendezvous Point	Node, Subnet, Interface	`PIM-SM-CANDIDATE-RP`
PIM-SM Candidate Bootstrap Router	Node, Subnet, Interface	`PIM-SM-CANDIDATE-BSR`

5. If **PIM-SM Candidate Rendezvous Point** is set to *Yes*, then set the dependent parameters listed in Table 5-26.
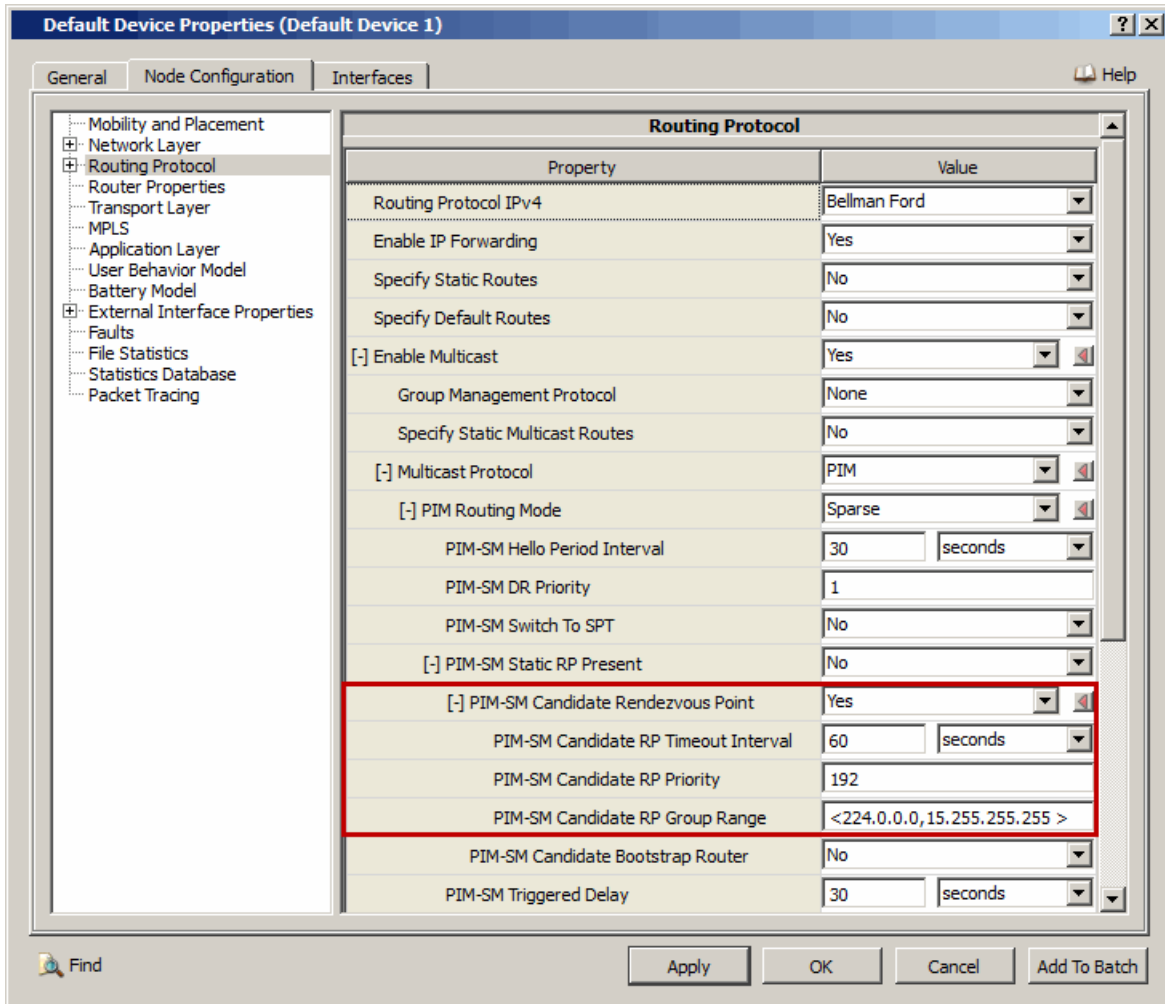
FIGURE 5-15.   Setting Candidate RP Parameters

TABLE 5-26.   Command Line Equivalent of Candidate RP Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
PIM-SM Candidate RP Timeout Interval	Node, Subnet, Interface	`ROUTING-PIMSM-CANDIDATE-RP-TIMEOUT`
PIM-SM Candidate RP Priority	Node, Subnet, Interface	`PIM-SM-CANDIDATE-RP-PRIORITY`
PIM-SM Candidate RP Group Range	Node, Subnet, Interface	`PIM-SM-RP-GROUP-RANGE`

Setting Parameters

- See Section 5.3.3 for the format of the value of the parameter **PIM-SM Candidate RP Group Range**.

6. If **PIM-SM Candidate Bootstrap Router** is set to *Yes*, then set the dependent parameters listed in Table 5-27.
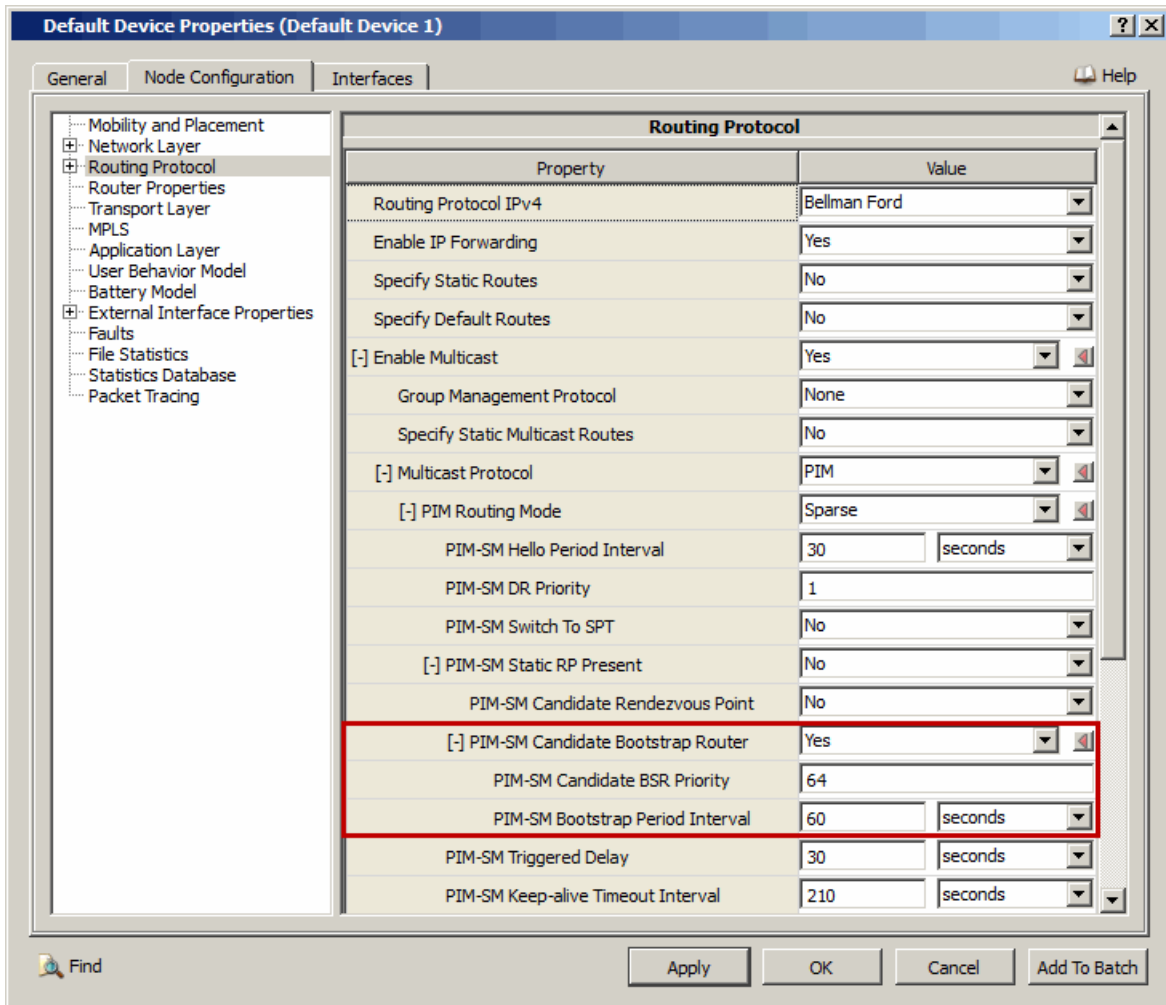
FIGURE 5-16. **Setting Bootstrap Router Parameters**

TABLE 5-27. **Command Line Equivalent of Bootstrap Router Parameters**

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
PIM-SM Candidate BSR Priority	Node, Subnet, Interface	`PIM-SM-CANDIDATE-BSR-PRIORITY`
PIM-SM Bootstrap Period Interval	Node, Subnet, Interface	`ROUTING-PIMSM-BOOTSTRAP-TIMEOUT`

7. If **PIM-SM Static RP Present** is set to *Yes*, then set the dependent parameters listed in Table 5-28.
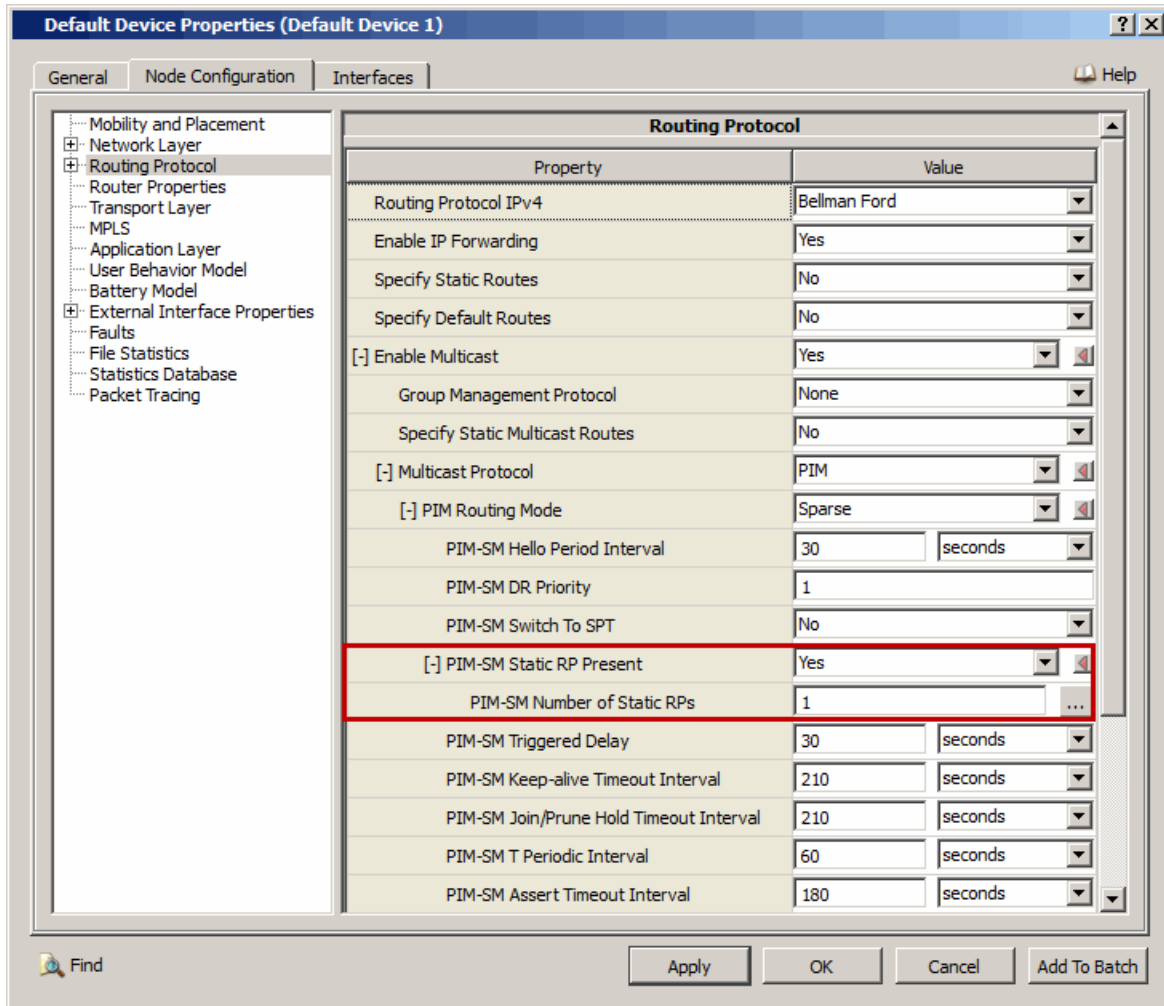
FIGURE 5-17.   Setting Number of Static RPs

TABLE 5-28.   Command Line Equivalent of Number of Static RPs Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
PIM-SM Number of Static RPs	Node, Subnet, Interface	`PIM-SM-STATIC-NUMBER-OF-RP`

Setting Parameters

- Set **PIM-SM Number of Static RPs** to a desired value as shown in Figure 5-17.

8. To configure the properties of Static RPs, do the following:

a. Click the **Open Editor** ⟨...⟩ button in the **Value** column. This opens the Array Editor (see Figure 5-18).

b. In the left panel of the Array Editor, select the index of the static RP to be configured. In the right panel, set the parameters listed in Table 5-29.
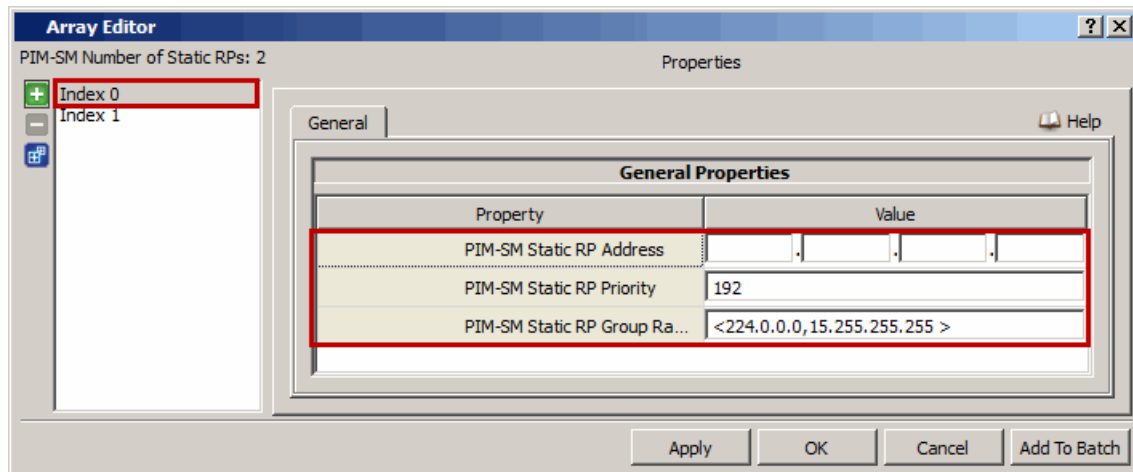
FIGURE 5-18.   Setting Static RP Parameters

TABLE 5-29.   Command Line Equivalent of Static RP Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
PIM-SM Static RP Address	Node, Subnet, Interface	`PIM-SM-STATIC-RP-ADDRESS`
PIM-SM Static RP Priority	Node, Subnet, Interface	`PIM-SM-STATIC-RP-PRIORITY`
PIM-SM Static RP Group Range	Node, Subnet, Interface	`PIM-SM-STATIC-RP-GROUP-RANGE`

Setting Parameters

- See Section 5.3.3 for the format of the value of the parameter **PIM-SM Static RP Group Range**.

9. If **Use SPT Directly** is set to *Yes*, then set the dependent parameters listed in Table 5-30.
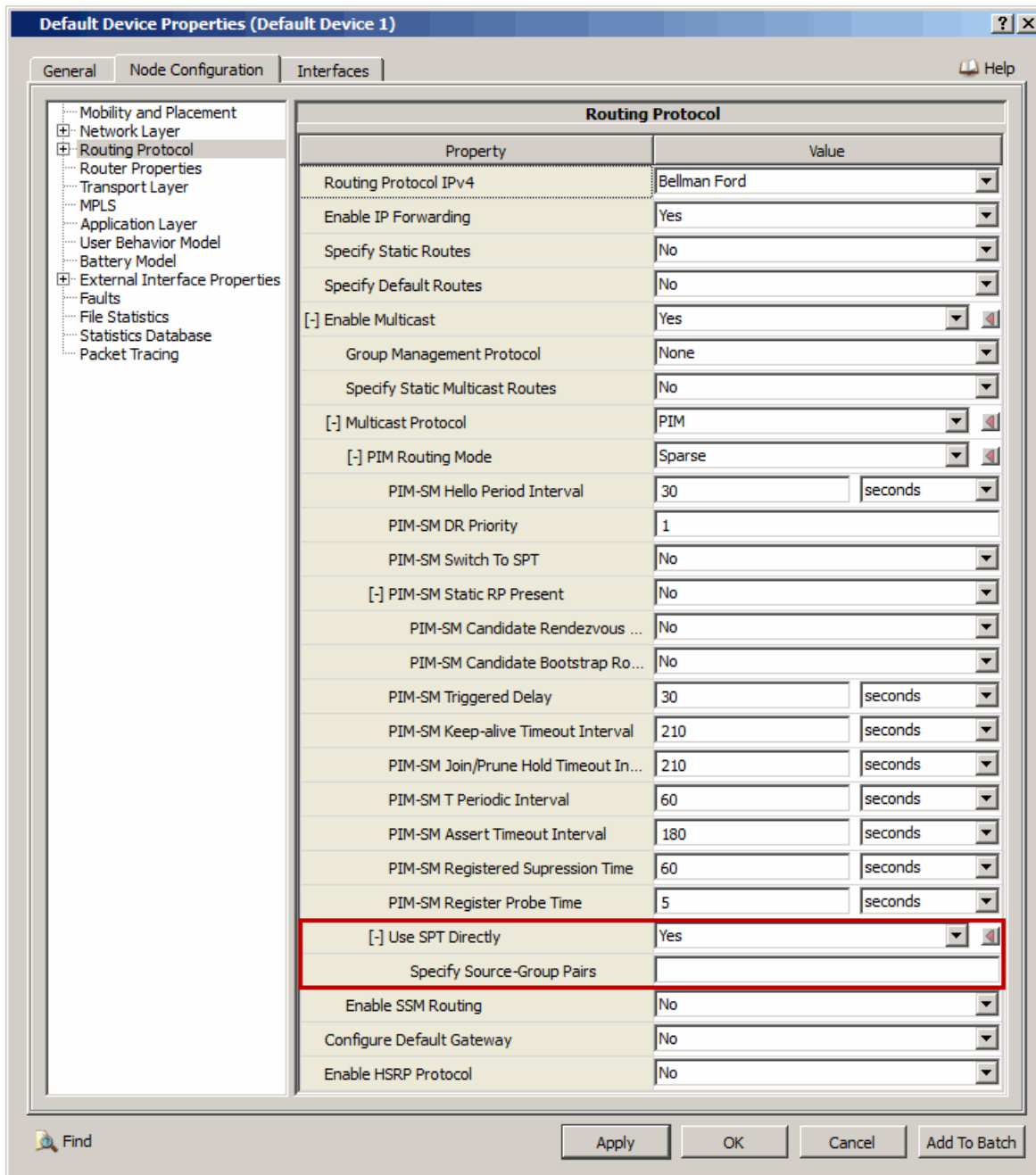
FIGURE 5-19.   Setting Direct SPT Parameters

TABLE 5-30.   Command Line Equivalent of Direct SPT Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Specify Source-Group Pairs	Node, Subnet, Interface	`ROUTING-PIMSM-SOURCE-GROUP-PAIR`

Setting Parameters

- See Section 5.3.3 for the format of the value of the parameter **PIM-SM Static RP Group Range**.

5.3.4.5 Configuring Sparse-Dense Mode Parameters

To configure the Sparse-Dense Mode parameters, perform the following steps:

1. Configure the general PIM parameters as described in Section 5.3.4.2. Set **PIM Routing Mode** to *Sparse-Dense.*

2. Dependent parameters for Sparse-Dense mode are the same as for Dense Mode and Sparse Mode. Set the parameters as described in Section 5.3.4.3 and Section 5.3.4.4.

5.3.4.6 Configuring PIM-SSM Parameters

To configure the PIM-SSM parameters, perform the following steps:

1. Configure PIM-SM parameters, as described in Section 5.3.4.4.

2. Configure IGMP version 3 to run on the node. See the IGMP section of *Developer Model Library* for details.

3. Configure the SSM routing parameters, as described in the IGMP section of *Developer Model Library*.

5.3.4.7 Configuring File Statistics Parameters

File statistics for PIM can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for routing protocols including PIM, check the box labeled **Routing** in the appropriate properties editor.

TABLE 5-31.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Routing	Global, Node	ROUTING-STATISTICS

5.3.4.8 Configuring Database Statistics Parameters

To configure the PIM-specific tables in the statistics database, perform the following steps:

1. Go to **Scenario Properties Editor > Statistics > Statistics Database**.

2. Set **Enable Statistics Database** to *Yes*.

3. Set **Model-specific Tables** set to *Yes* and set the PIM database table parameters listed in Table 5-32.

FIGURE 5-20.　Configuring PIM Tables in Statistics Database

TABLE 5-32.   Command Line Equivalent of PIM Statistics Database Table Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
PIM-DM Summary Table	Global	STATS-DB-MULTICAST-PIM-DM-SUMMARY-TABLE
PIM-SM Status Table	Global	STATS-DB-MULTICAST-PIM-SM-STATUS-TABLE
PIM-SM Summary Table	Global	STATS-DB-MULTICAST-PIM-SM-SUMMARY-TABLE

5.3.5 Statistics

This section describes the file, database, and dynamic statistics of the PIM model.

5.3.5.1 File Statistics

Table 5-33 shows the PIM-DM statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 5-33.   PIM-DM Statistics

Statistic	Description
Number of Hello Packets Sent	Number of periodic hello packets sent.
Number of Triggered Hello Packets Sent	Number of triggered hello packets sent.
Number of Hello Packets Received	Number of hello packets received.
Current Number of Neighbors	Number of neighbors when the statistic is printed.
Number of Join/Prune Packets Sent	Total number of Join/Prune Packets sent.
Number of Join/Prune Packets Received	Total number of Join/Prune Packets received.
Number of Join Packets Sent	Total number of Join Packets sent.
Number of Prune Packets Sent	Total number of Prune Packets sent.
Number of Join Packets Received	Total number of Join Packets received.
Number of Prune Packets Received	Total number of Prune Packets received.
Number of Graft Packets Sent	Number of Graft packets sent by the node.
Number of Graft Packets Received	Number of Graft packets received by the node.
Number of Graft ACK Packets Sent	Number of Graft acknowledgement packets sent by the node.
Number of Graft ACK Packets Received	Number of Graft acknowledgement packets received by the. node
Number of Assert Packets Sent	Number of Assert packets sent by the node.
Number of Assert Packets Received	Number of Assert packets received by the node.
Number of Data Packets Sent as Data Source	Number of multicast data packets sent as the data source by the node.
Number of Data Packets Received	Number of multicast data packets received by the node.
Number of Data Packets Forwarded	Number of multicast data packets forwarded by the node.
Number of Data Packets Discarded	Number of multicast data packets discarded by the node.

Table 5-34 shows the PIM-SM statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 5-34.   PIM-SM Statistics

Statistic	Description
Number Of Neighbors	Number of neighbors of the node when the statistics is printed.
Number of Receivers Joined	Number of multicast groups for which the node has received IGMP joins.
Number Of Receivers Left	Number of multicast groups for which the node has received IGMP leave.
Number Of Hello Packets Received	Total number of hello packets received by the node.
Number Of Triggered Hello Packets Sent	Total number of triggered hello packets sent by the node
Number Of Hello Packets Sent	Total number of hello packets sent by the node
Number of Registered Packets Received	Total number of registered packets received by the node.
Number of Registered Packets Sent	Total number of registered packets sent by the node.
Number of encapsulated (Registered Packets) data packets Forwarded	Total number of encapsulated (Registered Packets) data packets forwarded by the node.
Number of Register-Stop Packets Received	Total number of Registered-Stop Packets received by the node.
Number of Register-Stop Packets Forwarded	Total number of Registered-Stop Packets forwarded by the node.
Number of Join/Prune Packets Received	Total number of Join/Prune Packets received by the node.
Number of Join/Prune Packets Forwarded	Total number of Join/Prune Packets forwarded by the node.
Number of (*,G) Join Packets Received	Total number of (*, G) Join Packets received by the node.
Number of (*,G) Prune Packets Received	Total number of (*, G) Prune Packets received by the node.
Number of (*,G) Join Packets Forwarded	Total number of (*, G) Join Packets forwarded by the node.
Number of (*,G) Prune Packets Forwarded	Total number of (*, G) Prune Packets forwarded by the node.
Number of (S,G) Join Packets Received	Total number of (S, G) Join Packets received by the node.
Number of (S,G) Prune Packets Received	Total number of (S, G) Prune Packets received by the node.
Number of (S,G) Join Packets Forwarded	Total number of (S, G) Join Packets forwarded by the node.
Number of (S,G) Prune Packets Forwarded	Total number of (S, G) Prune Packets forwarded by the node.
Number of (S,G,Rpt) Join Packets Received	Total number of (S, G, Rpt) Join Packets received by the node.
Number of (S,G,Rpt) Prune Packets Received	Total number of (S, G, Rpt) Prune Packets received by the node.
Number of (S,G,Rpt) Join Packets Forwarded	Total number of (S, G, Rpt) Join Packets forwarded by the node.
Number of (S,G,Rpt) Prune Packets Forwarded	Total number of (S, G, Rpt) Prune Packets forwarded by the node.
Number of (*,G) Assert Packets Received	Total number of (*,G) Assert Packets received by the node.
Number of (*,G) Assert Packets Forwarded	Total number of (*,G) Assert Packets forwarded by the node.
Number of (S,G) Assert Packets Received	Total number of (S,G) Assert Packets received by the node.
Number of (S,G) Assert Packets Forwarded	Total number of (S,G) Assert Packets forwarded by the node.

TABLE 5-34.   PIM-SM Statistics (Continued)

Statistic	Description
Number of (*,G) Assert Cancel Packets Received	Total number of (*,G) Assert Cancel Packets received by the node.
Number of (*,G) Assert Cancel Packets Forwarded	Total number of (*,G) Assert Cancel Packets forwarded by the node.
Number of (S,G) Assert Cancel Packets Received	Total number of (S,G) Assert Cancel Packets received by the node.
Number of (S,G) Assert Cancel Packets Forwarded	Total number of (S,G) Assert Cancel Packets forwarded by the node.
Number of Bootstrap Packets Originated	Total number of Bootstrap Packets originated by the node.
Number of Bootstrap Packets Received	Total number of Bootstrap Packets received by the node.
Number of Bootstrap Packets Forwarded	Total number of Bootstrap Packets forwarded by the node.
Number of Candidate-RP Packets Received	Total number of number of Candidate-RP Packets received by the node.
Number of Candidate-RP Packets Forwarded	Total number of number of Candidate-RP Packets forwarded by the node.
Number of Data Packets Sent As Data Source	Number of multicast data packets sent as the source.
Number of Data Packets Received	Number of multicast data packets received by the node.
Number of Data Packets Forwarded	Number of multicast data packets forwarded.
Number of Data Packets Discarded	Number of multicast data packets discarded.

5.3.5.2 Database Statistics

In addition to the file statistics, the PIM model also enters statistics in various scenario statistics database tables. Refer to *QualNet Statistics Database User's Guide* for details.

The PIM model also enters statistics in the following PIM-specific database tables:

* PIM-DM Summary Table
* PIM-SM Status Table
* PIM-SM Summary Table

5.3.5.3 Dynamic Statistics

No dynamic statistics are supported for the PIM model.

5.3.6 Sample Scenarios

This section describes three PIM sample scenarios and their configuration in command line and GUI. Section 5.3.6.1 describes a sample scenario using PIM in Dense Mode. Section 5.3.6.2 describes a sample scenario using PIM in Sparse Mode. Section 5.3.7 describes a sample scenario using PIM in Sparse-Dense Mode.

5.3.6.1 Dense Mode Sample Scenario

5.3.6.1.1 Scenario Description

This scenario uses PIM in Dense Mode in a wired network. Multicast traffic is sent from one source to one receiver. The scenario topology is shown in Figure 5-21.
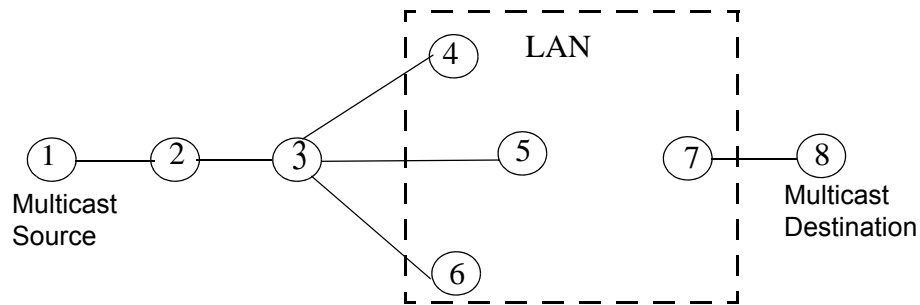
FIGURE 5-21.   Dense Mode Sample Scenario Topology

- Point-to-point wired links connect nodes 1 and 2, 2 and 3, 3 and 4, 3 and 5, 3 and 6, and 7 and 8.
- Nodes 4 to 7 are in a wired subnet.
- Nodes 2 to 7 run PIM in Dense Mode.
- Bellman-Ford is used as the underlying routing protocol.
- Multicast traffic (MCBR) is sent from node 1 to node 8.

5.3.6.1.2 Command Line Configuration

This section describes the command line configuration for the sample scenario.

Scenario Configuration File

Include the following parameters in the scenario configuration (.config) file:

```
SIMULATION-TIME   200S

# Configure a subnet consisting of nodes 4 thru 7
SUBNET N8-190.0.1.0 {4 thru 7}

# Create point-to-point links between the following pairs of nodes
# By default, these are wired links running the Abstract Link MAC
# protocol.
LINK N8-190.0.2.0 { 1, 2 }
LINK N8-190.0.3.0 { 2, 3 }
LINK N8-190.0.4.0 { 3, 5 }
LINK N8-190.0.5.0 { 3, 4 }
LINK N8-190.0.6.0 { 3, 6 }
LINK N8-190.0.7.0 { 7, 8 }
```

```
# Routing protocol running on every node is Bellman Ford
[1 thru 8]ROUTING-PROTOCOL BELLMANFORD

# Group management protocol for multicasting is IGMP on every node
# Node 7 is the IGMP router
[1 thru 8]GROUP-MANAGEMENT-PROTOCOL IGMP
[1 thru 8]IGMP-ROUTER-LIST {7}

# Enable PIM in Dense Mode on nodes 2 to 7
[2 thru 7]MULTICAST-PROTOCOL PIM
[2 thru 7]PIM-ROUTING-MODE DENSE

# Specify PIM Hello period
[2 thru 7]ROUTING-PIM-HELLO-PERIOD 30S

# Disable all PIM Dense Mode optimizations
[2 thru 7]ROUTING-PIMDM-ASSERT-OPTIMIZATION NO
[2 thru 7]ROUTING-PIMDM-JOIN-PRUNE-SUPPRESSION NO
[2 thru 7]ROUTING-PIMDM-HELLO-SUPPRESSION NO
[2 thru 7]ROUTING-PIMDM-BROADCAST-MODE NO

# Specify the multicast group member file
MULTICAST-GROUP-FILE Sample-Scenario-DenseMode.member

# Specify the application configuration file
APP-CONFIG-FILE  Sample-Scenario-DenseMode.app
```

Application Configuration File

Configure a multicast group consisting of node 8 by including the following line in the multicast group (Sample-Scenario-DenseMode.member) file:

```
8 225.0.0.1 0S 200S
```

Application Configuration File

Configure an MCBR session between node 1 and the multicast group 225.0.0.1 by including the following line in the application configuration (Sample-Scenario-DenseMode.app) file:

```
MCBR 1 225.0.0.1 200 512 1 1S 200S
```

5.3.6.1.3 GUI Configuration

This section describes the GUI configuration for the sample scenario.

Network Setup

Using the Toolset, configure the sample scenario network topology as shown in Figure 5-22.
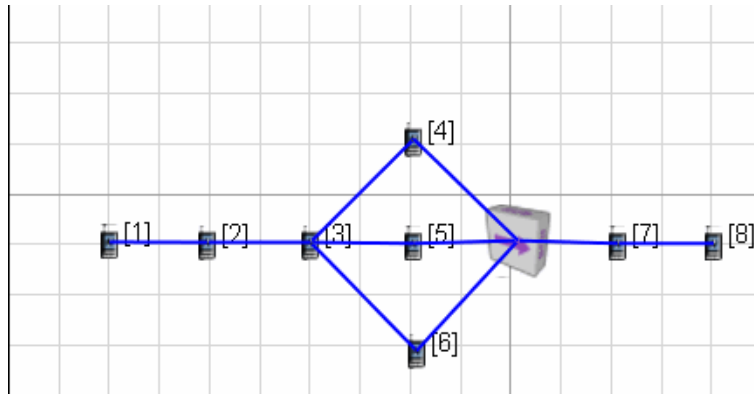
FIGURE 5-22.   PIM Dense Mode Sample Scenario in GUI

General Simulation Parameters

Go to Scenario Properties Editor **>** General and set **Simulation Time** to *200 seconds.*

Routing Protocol and IGMP Configuration

For each of the nodes 1 to 8, configure Bellman-Ford and IGMP parameters as follows (see Figure 5-23):

1. Go to Default Device Properties Editor **>** Node Configuration.

2. Set **Routing Protocol IPV4** to *Bellman Ford.*

3. Set **Enable Multicast** to *Yes.*

4. Set **Group Management Protocol** to *IGMP.*

5. Set **Router List** to *{7}.*
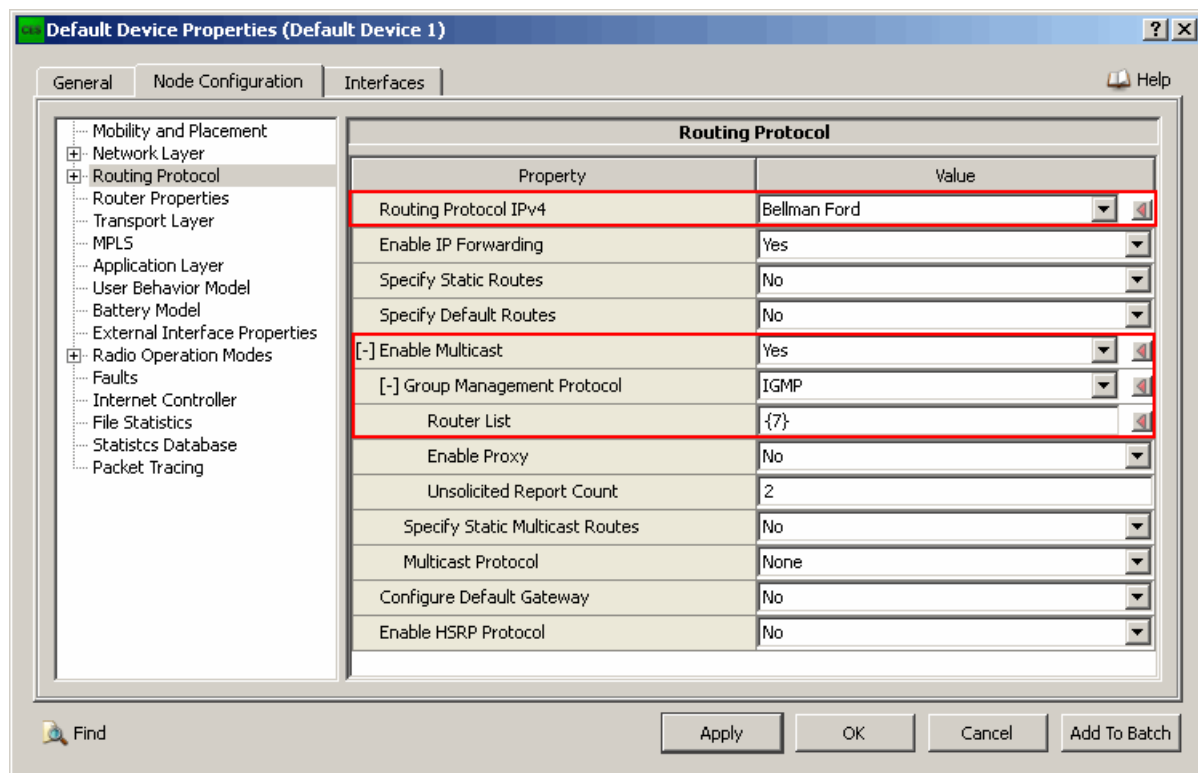
FIGURE 5-23. Dense Mode Sample Scenario Configuration - 1

PIM Dense Mode Configuration

For each of the nodes 2 to 7, configure PIM parameters as follows (see Figure 5-24):

1. Set **Multicast Protocol** to *PIM*.

2. Set **PIM Routing Mode** to *Dense*.

3. Set **PIM-DM Hello Period Interval** to *30 seconds*.

4. Set **Enable Hello Suppression**, **Enable Broadcast Mode**, **Enable Join/Prune Suppression**, and **Enable Assert Optimization** to *No*.

FIGURE 5-24.   Dense Mode Sample Scenario Configuration - 2

Multicast Group Configuration

Create a multicast group as follows:

1. Select **Tools > Multicast Group Editor** to launch the Multicast Group Editor.

2. Create a multicast group with address 255.0.0.1.

3. Create an entry for node 8 to join this group at time 0 seconds and leave at 200 seconds.

Application Configuration

Set up multicast traffic from node 1 to node 8 as follows:

1. Configure an MCBR session at node 1.

2. Set **Multicast Group Address** to *225.0.0.1*, **Items to Send** to *200*, **Item Size** to *512*, **Interval** to *1 second*, **Start Time** to *1 second*, and **End Time** to *200 seconds*.

5.3.6.2 Sparse Mode Sample Scenario

5.3.6.2.1 Scenario Description
This scenario uses PIM in Sparse Mode in a wired network. Multicast traffic is sent from one source to one receiver. The scenario topology is shown in Figure 5-25.
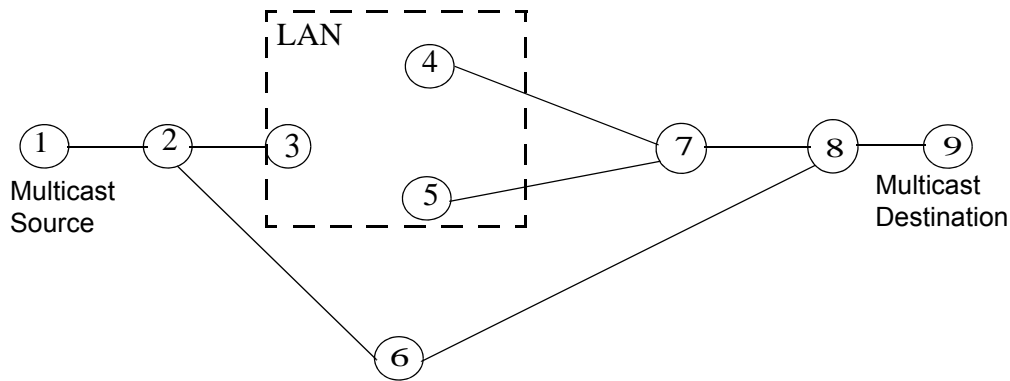
FIGURE 5-25.   Sparse Mode Sample Scenario Topology

- Point-to-point wired links connect nodes 1 and 2, 2 and 3, 2 and 6, 4 and 7, 5 and 7, 7 and 8, 8 and 9, and 6 and 8.
- Nodes 3 to 5 are in a wired subnet.
- Nodes 2 to 8 run PIM in Sparse Mode.
- Bellman-Ford is used as the underlying routing protocol.
- Multicast traffic (MCBR) is sent from node 1 to multicast group 225.0.0.1, which has node 9 as its member.
- For multicast group 225.0.0.1, node 5 is a candidate RP for multicast group range 225.0.0.0 to 225.0.0.255.
- PIM routers 3 and 4 are candidate BSRs.
- SPT switchover is enabled on PIM router 8 for every multicast group.

5.3.6.2.2 Command Line Configuration

This section describes the command line configuration for the sample scenario.

Scenario Configuration File

Include the following parameters in the scenario configuration (.config) file:

```
SIMULATION-TIME    600S


# Configure a subnet consisting of nodes 3 thru 5
SUBNET N8-190.0.1.0 {3 thru 5}

# Create point-to-point links between the following pairs of nodes
# By default, these are wired links running the Abstract Link MAC
# protocol.
LINK N8-190.0.2.0 { 1, 2 }
LINK N8-190.0.3.0 { 2, 3 }
LINK N8-190.0.3.0 { 2, 6 }
LINK N8-190.0.4.0 { 4, 7 }
LINK N8-190.0.5.0 { 5, 7 }
LINK N8-190.0.6.0 { 7, 8 }
LINK N8-190.0.7.0 { 8, 9 }
LINK N8-190.0.7.0 { 6, 7 }

# Routing protocol running on every node is Bellman ford
[1 thru 9]ROUTING-PROTOCOL BELLMANFORD

# Group management protocol for multicasting is IGMP on every node
# Node 7 is the IGMP router
[1 thru 9]GROUP-MANAGEMENT-PROTOCOL       IGMP
[1 thru 9]IGMP-ROUTER-LIST                {8}

# Enable PIM in Sparse Mode on nodes 2 to 8
[2 thru 8]MULTICAST-PROTOCOL             PIM
[2 thru 8]PIM-ROUTING-MODE               SPARSE

# Specify PIM Hello period
[2 thru 8]ROUTING-PIM-HELLO-PERIOD       30S

#Specify DR Priority for Sparse Mode
[2 thru 8]ROUTING-PIM-DR-PRIORITY        4

#Specify Candidate BSR for Sparse Mode
[3 4]PIM-SM-CANDIDATE-BSR YES

#Specify Candidate BSR related parameters for Sparse Mode
[3 4]PIM-SM-CANDIDATE-BSR-PRIORITY       64
[3 4]ROUTING-PIMSM-BOOTSTRAP-PERIOD      60S

#Specify Candidate RP for sparse mode
[5]PIM-SM-CANDIDATE-RP                   YES
```

```
#Specify Candidate RP parameters for Sparse Mode
[5]ROUTING-PIMSM-CANDIDATE-RP-TIMEOUT      60S
[5]PIM-SM-CANDIDATE-RP-PRIORITY            192
[5]PIM-SM-RP-GROUP-RANGE                   <225.0.0.0,0.0.0.255 >

#Specifying SPT threshold value and its group-range for Sparse Mode
[8]PIMSM-SWITCH-SPT-THRESHOLD 1 GROUP-RANGE <224.0.0.0,15.255.255.255>

#Specify various timer values for Sparse Mode
[2 thru 8]ROUTING-PIMSM-TRIGGERED-DELAY                    30S
[2 thru 8]ROUTING-PIMSM-KEEPALIVE-TIMEOUT                  210S
[2 thru 8]ROUTING-PIMSM-REGISTER-SUPRESSION-TIME           60S
[2 thru 8]ROUTING-PIMSM-T-PERIODIC-INTERVAL                60S
[2 thru 8]ROUTING-PIMSM-JOINPRUNE-HOLD-TIMEOUT             210S
[2 thru 8]ROUTING-PIMSM-ASSERT-TIMEOUT                     180S

# Specify the multicast group member file
MULTICAST-GROUP-FILE Sample-Scenario-SparseMode.member

# Specify the application configuration file
APP-CONFIG-FILE  Sample-Scenario-SparseMode.app
```

Application Configuration File

Configure a multicast group consisting of node 8 by including the following line in the multicast group (Sample-Scenario-SparseMode.member) file:

```
9 225.0.0.1 0S 600S
```

Application Configuration File

Configure an MCBR session between node 1 and the multicast group 225.0.0.1 by including the following line in the application configuration (Sample-Scenario-SparseMode.app) file:

```
MCBR 1 225.0.0.1 200 512 1 1S 600S
```

5.3.6.2.3 GUI Configuration
This section describes the GUI configuration for the sample scenario.

Network Setup
Using the Toolset, configure the sample scenario network topology as shown in Figure 5-22.
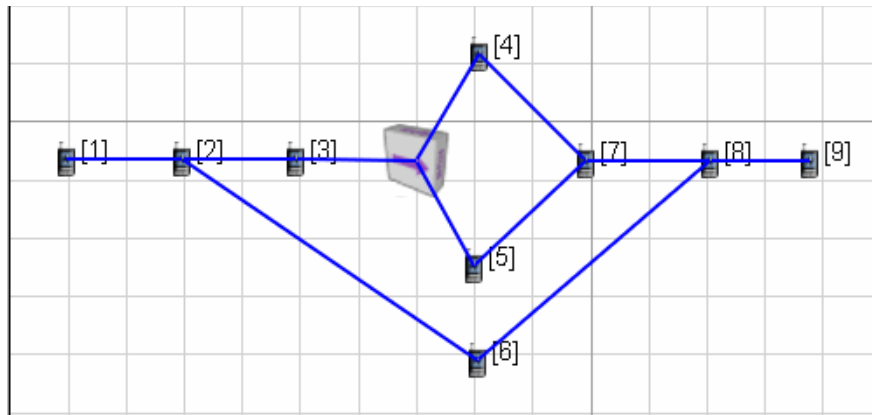
FIGURE 5-26.   PIM Sparse Mode Sample Scenario in GUI

General Simulation Parameters
Go to Scenario Properties Editor **>** General and set **Simulation Time** to *600 seconds.*

Routing Protocol and IGMP Configuration
For each of the nodes 1 to 9, configure Bellman-Ford and IGMP parameters as follows (see Figure 5-27):

1. Go to **Default Device Properties Editor > Node Configuration**.

2. Set **Routing Protocol IPV4** to *Bellman Ford*.

3. Set **Enable Multicast** to *Yes.*

4. Set **Group Management Protocol** to *IGMP.*

5. Set **Router List** to *{8}.*
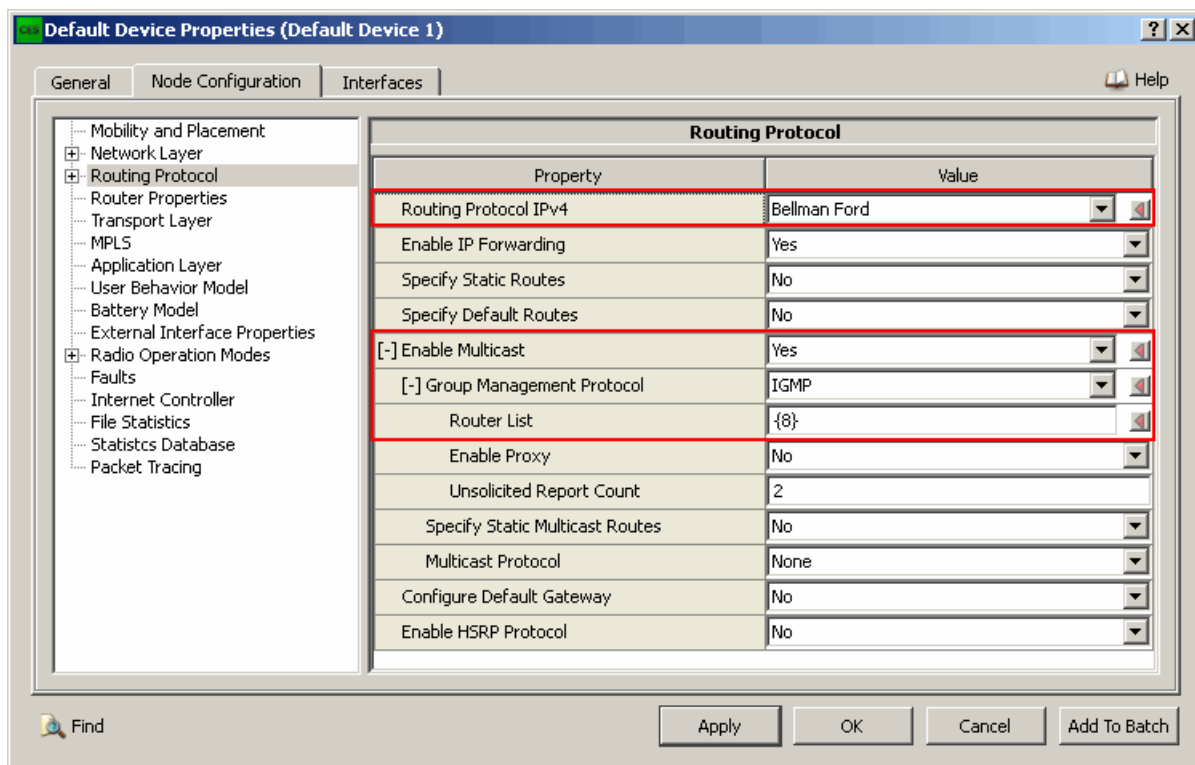
FIGURE 5-27.   Sparse Mode Sample Scenario Configuration - 1

PIM Sparse Mode Configuration

For each of the nodes 2 to 8, configure PIM parameters as follows (see Figure 5-28):

1. Set **Multicast Protocol** to *PIM*.

2. Set **PIM Routing Mode** to *Sparse*.

3. Set **PIM-SM Hello Period Interval** to *30 seconds*.

4. Set **PIM-SM DR Priority** to *4*.

5. Set **PIM-SM Triggered Delay** to *30 seconds*.

6. Set **PIM-SM Keep-alive Timeout Interval** to *210 seconds*.

7. Set **PIM-SM Join/Prune Hold Timeout Interval** to *210 seconds*.

8. Set **PIM-SM T Periodic Interval** to *60 seconds*.

9. Set **PIM-SM Assert Timeout Interval** to *180 seconds*.

10. Set **PIM-SM Registered Suppression Time** to *60 seconds*.

11. Set **PIM-SM Register Probe Time** to *5 seconds*.

12. Set **Use SPT Directly** to *No*.

FIGURE 5-28.   Sparse Mode Sample Scenario Configuration - 2

Candidate BSR Configuration

For each of the nodes 3 and 4, configure the candidate BSR parameters as follows (see Figure 5-29):

1. Set **PIM-SM Static RP Present** to *No.*

2. Set **PIM-SM Candidate Bootstrap Router** to *Yes.*

3. Set **PIM-SM Candidate BSR Priority** to *64.*

4. Set **PIM-SM Bootstrap Period Interval** to *60 seconds.*
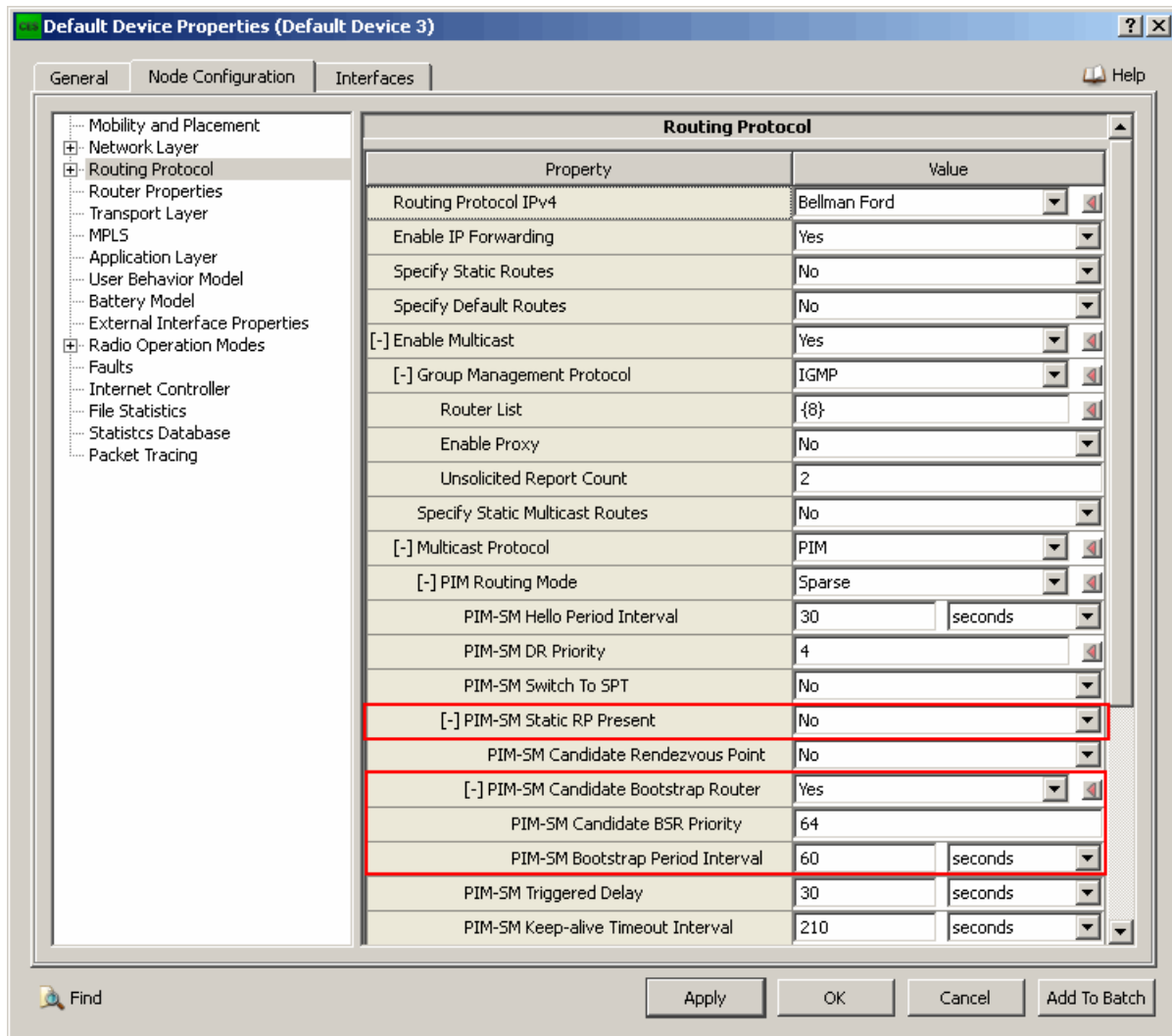
FIGURE 5-29.   Sparse Mode Sample Scenario Configuration - 3

Candidate RP Configuration

For node 5, configure the candidate RP parameters as follows (see Figure 5-30):

1. Set **PIM-SM Static RP Present** to *No.*

2. Set **PIM-SM Candidate RP Timeout Interval** to *60 seconds.*

3. Set **PIM-SM Candidate RP Priority** to *192.*

4. Set **PIM-SM Candidate RP Group Range** to *<225.0.0.0,0.0.0.255>.*
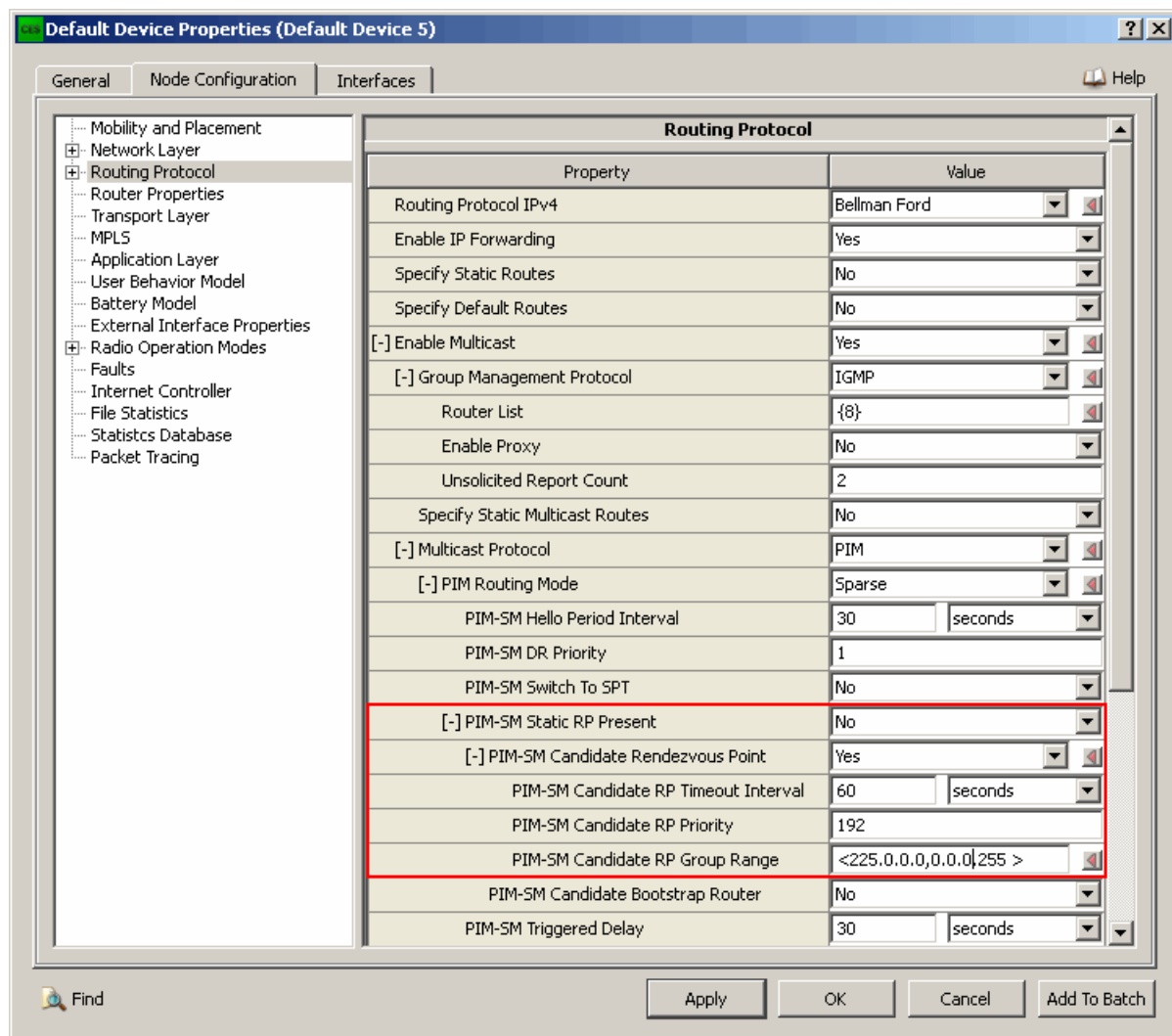
FIGURE 5-30.   Sparse Mode Sample Scenario Configuration - 4

SPT Configuration

For node 8, configure the SPT parameters as follows (see Figure 5-31):

1. Set **PIM-SM Switch To SPT** to *Yes*.

2. Set **PIM-SM Switch To SPT Threshold** to *1 GROUP-RANGE <224.0.0.0,15.255.255.255>*.
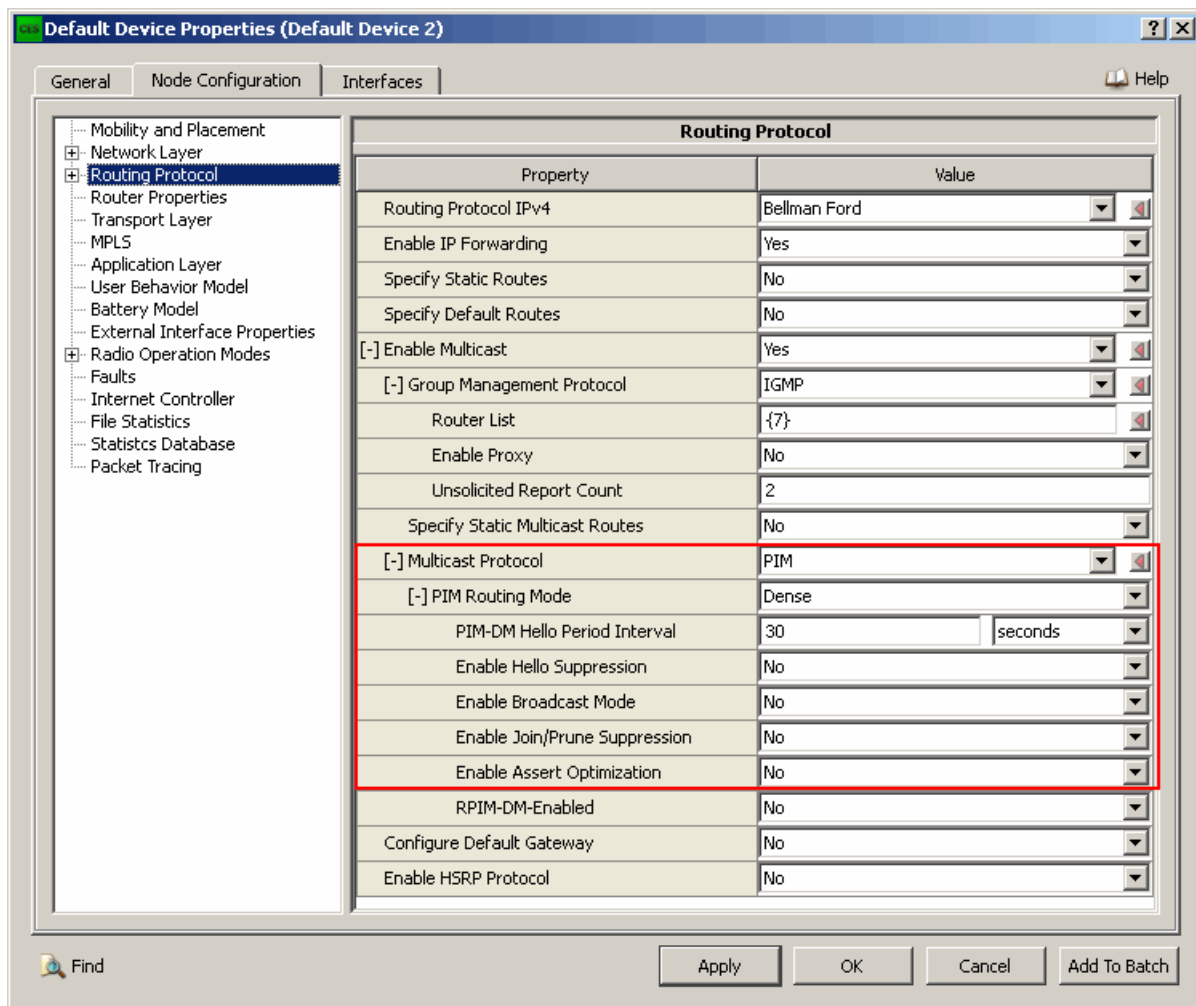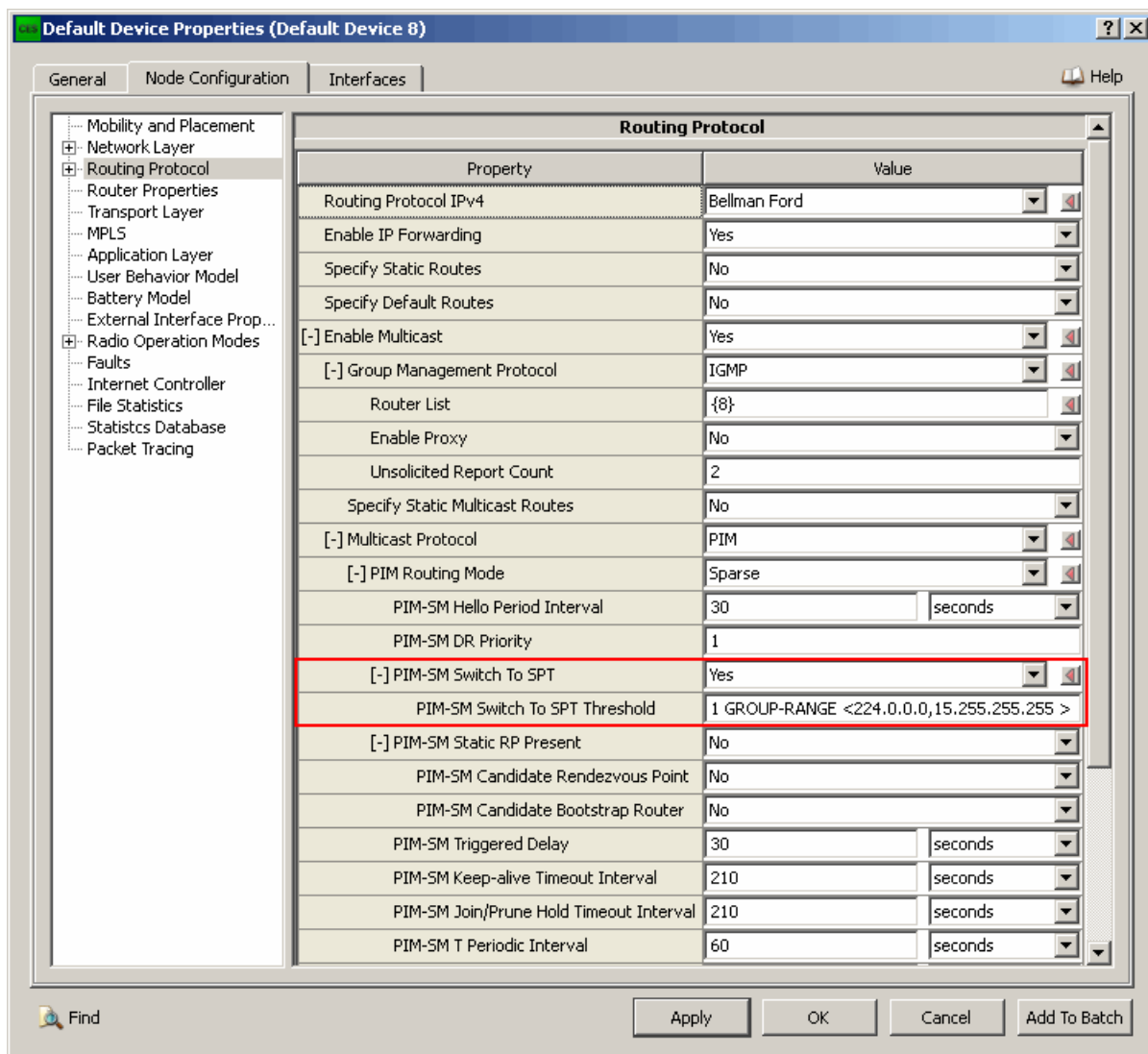
FIGURE 5-31.   Sparse Mode Sample Scenario Configuration - 5

Multicast Group Configuration

Create a multicast group as follows:

1. Select **Tools > Multicast Group Editor** to launch the Multicast Group Editor.

2. Create a multicast group with address 255.0.0.1.

3. Create an entry for node 9 to join this group at time 0 seconds and leave at 600 seconds.

Application Configuration

Set up multicast traffic from node 1 to node 9 as follows:

1. Configure an MCBR session at node 1.

2. Set **Multicast Group Address** to *225.0.0.1*, **Items to Send** to *200*, **Item Size** to *512*, **Interval** to *1 second*, **Start Time** to *1 second*, and **End Time** to *600 seconds*.

5.3.7 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the PIM model.

PIM-DM Scenarios

All scenarios are located in QUALNET_HOME/scenarios/multimedia_enterprise/pim-dm. Table 5-35 lists the sub-directory where each scenario is located.

TABLE 5-35.   PIM-DM Scenarios Included in QualNet

Scenario	Description
string-graft	Shows the graft operation of PIM-DM in a string topology network. The multicast receiver will receive most, but not all the data sent since the receiver leaves the group in between the joins (causing prunes and grafts).
string-normal	Shows the operation of PIM-DM in a string topology network.
string-prune	Shows the prune operation of PIM-DM in a string topology network. The multicast receiver will not receive all data sent by the source, since the receiver leaves the group early, causing a prune.
tree-graft	Shows the graft operation of PIM-DM in a tree topology network.In this scenario, some receivers will not receive all the data sent by the source since these receivers leave the group early (thus leading to pruning) and then rejoin the group (thus leading to grafting).
tree-normal	Shows the operation of PIM-DM in a tree topology network.
tree-prune	Shows the prune operation of PIM-DM in a tree topology network. In this scenario, some receivers will not receive all the data sent by the source since these receivers leave the group early (thus leading to pruning).

PIM-SM Scenarios

All scenarios are located in QUALNET_HOME/scenarios/multimedia_enterprise/pim-sm. Table 5-35 lists the sub-directory where each scenario is located.

TABLE 5-36.   PIM-SM Scenarios Included in QualNet

Scenario	Description
designated-forwarder-sm	Shows the selection of designated router in PIM-SM protocol in a multi-access LAN topology.
multiaccessLAN-join-sm	Shows the operation of PIM-SM protocol in a tree topology network, where some receivers join in middle of the simulation across multi-access LAN segment.
string-normal-sm	Shows the operation of PIM-SM protocol in a string topology network with node 4 as the IGMP router.
tree-join-sm	Shows the operation of PIM-SM protocol in a tree topology network where some receivers join in middle of the simulation.
tree-normal-sm	Shows the operation of PIM-SM protocol in a string topology network with node 5 as the IGMP router.
tree-prune-sm	Shows the operation of PIM-SM protocol in a string topology network with node 5 as the IGMP router and 10Mbps as the link capacity for all links.
unicast-route-change-sm	Shows the operation of PIM-SM, where one of the intermediate multicast router goes down and then comes back up while its downstream remains on multicast group.

5.3.8 References

1. draft-ietf-pim-v2-dm-03. "Protocol Independent Multicast Version 2 Dense Mode Specification." Stephen Deering, Deborah Estrin, Dino Farinacci, Van Jacobson, Ahmed Helmy, David Meyer, Liming Wei. June 1999.

2. draft-ietf-pim-dm-new-v2-05. "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)." Andrew Adams, Jonathan Nicholas, William Siadak. June 2004.

3. draft-ietf-pim-sm-v2-new-11. "Protocol Independent Multicast - Sparse Mode (PIM-SM):Protocol Specification (Revised)." Bill Fenner, Mark Handley, Hugh Holbrook, Isidor Kouvelas. October 2004.

4. RFC 2362, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification." D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei. June 1998.

5. A. Adams, et al, RFC 3973, Protocol Independent Multicast-Dense Mode (PIM-DM): Protocol Specification (Revised), Jan. 2005.

6. RFC 4601, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", August 2006.

7. RFC 5059, "Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)", January 2008.

6 Router Configuration Models

This chapter describes features, configuration requirements and parameters, statistics, and scenarios for Router Configuration Models, and consists of the following sections:

- Hot Standby Router Protocol (HSRP)
- Policy-based Routing Protocol (PBR)
- Route Map
- Route Redistribution
- Router Access List
- Router Model

. . . .

6.1 Hot Standby Router Protocol (HSRP)

The QualNet HSRP model is based on RFC 2281.

6.1.1 Description

HSRP allows a host to specify a virtual next hop router to forward packets. Routers participating in the same standby group will dynamically determine the active and standby routers. Only the active router will forward packets.

6.1.2 Features and Assumptions

This section describes the implemented features, omitted features, assumptions and limitations of the HSRP model.

6.1.2.1 Implemented Features

- Multiple standby groups.

6.1.2.2 Omitted Features

- Authentication of messages.

6.1.2.3 Assumptions and Limitations

- Same virtual IP address is used within a group.

6.1.3 Command Line Configuration

To enable the HSRP protocol, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] HSRP-PROTOCOL      YES
```

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

> **Note:**   The default value of parameter `HSRP-PROTOCOL` is `NO`.

HSRP Parameters

Table 6-1 describes the HSRP configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 6-1.   HSRP Parameters

Parameter	Value	Description
HSRP-STANDBY-GROUP-NUMBER Optional *Scope:* All	Integer *Range:* [0, 255] *Default:* 0	Specifies the HSRP standby group number. HSRP routers must belong to a group. Currently QualNet does not consider different groups within a broadcast LAN.
HSRP-VIRTUAL-IP-ADDRESS Required *Scope:* All	IP Address *Default:* 255.255.255.255	Specifies the virtual IP address of the next hop router that will forward packets. This IP address must be used in default route file to specify the next hop on the host that relies on the HSRP routers.
HSRP-PRIORITY Optional *Scope:* All	Integer *Range:* > 0 *Default:* 0	Specifies the priority used in scheduling. The higher the value, the higher the priority.
HSRP-HELLO-TIME Optional *Scope:* All	Time *Range:* > 0S *Default:* 3S	Specifies the hello time interval.
HSRP-HOLD-TIME Optional *Scope:* All	Time *Range:* > HSRP- HELLO-TIME *Default:* 10S	Specifies the hold time interval.
HSRP-PREEMPTION- CAPABILITY Optional *Scope:* All	List: • YES • NO *Default:* NO	Specifies whether to allow higher priority routers to claim active status from the currently active router. **Note:** If set to NO, higher priority routers will yield to current active router even if current active router has lower priority.

6.1.4 GUI Configuration

This section describes how to configure HSRP in the GUI.

Configuring HSRP Parameters

To configure the HSRP parameters, perform the following steps:

1. Go to one of the following locations:

- To set properties for a specific wireless subnet, go to **Wireless Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific wired subnet, go to **Wired Subnet Properties Editor > Routing Protocol > General**.

- To set properties for a specific point-to-point link, go to **Point-to-point Link Properties Editor > Point-to-point Link Properties > Routing Protocol**.

- To set properties for a specific node, go to **Default Device Properties Editor > Node Configuration > Routing Protocol**.

- To set properties for a specific interface of a node, go to one of the following locations:

  - **Interface Properties Editor > Interfaces > Interface # > Routing Protocol**.

  - **Default Device Properties Editor > Interfaces > Interface # > Routing Protocol**.

In this section, we show how to configure HSRP parameters for a specific node using the Default Device Properties Editor. Parameters can be set in the other properties editors in a similar way.

2. Set **Enable HSRP Protocol** to *Yes* and set the dependent parameters listed in Table 6-2.
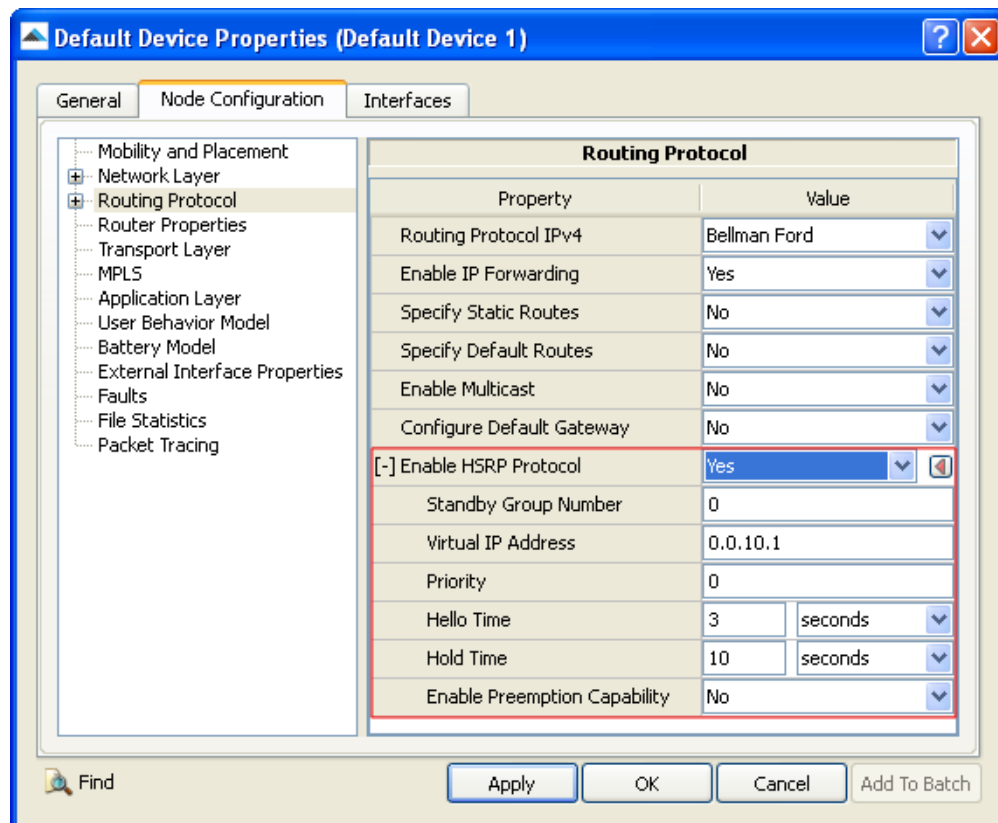
FIGURE 6-1.   Setting HSRP Parameters

TABLE 6-2.   Command Line Equivalent of HSRP Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Standby Group Number	Node, Interface, Subnet	`HSRP-STANDBY-GROUP-NUMBER`
Virtual IP Address	Node, Interface, Subnet	`HSRP-VIRTUAL-IP-ADDRESS`
Priority	Node, Interface, Subnet	`HSRP-PRIORITY`
Hello Time	Node, Interface, Subnet	`HSRP-HELLO-TIME`

TABLE 6-2.   Command Line Equivalent of HSRP Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Hold Time	Node, Interface, Subnet	HSRP-HOLD-TIME
Enable Preemption Capability	Node, Interface, Subnet	HSRP-PREEMPTION-CAPABILITY

Configuring Statistics Parameters

Statistics for HSRP can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for routing protocols including HSRP, check the box labeled **Routing** in the appropriate properties editor.

TABLE 6-3.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Routing	Global, Node	ROUTING-STATISTICS

6.1.5 Statistics

Table 6-4 lists the HSRP statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 6-4.   HSRP Statistics

Statistic	Description
Number of Hello messages sent	Total number of Hello messages sent.
Number of Coup messages sent	Total Number of Coup messages sent.
Number of Resign messages sent	Total Number of Resign messages sent.
Number of Hello messages received	Total Number of Hello messages received.
Number of Coup messages received	Total Number of Coup messages received.
Number of Resign messages received	Total Number of Resign messages received.
Last state	Last state of the HSRP enabled interface.

6.1.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the HSRP model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/hsrp. Table 6-5 lists the sub-directory where each scenario is located.

TABLE 6-5.   HSRP Scenarios Included in QualNet

Scenario Sub-directory	Description
failover	Tests HSRP functionality in case of failover of active router.
hello-messages	Tests HSRP hello message generation in a simple wired network.

6.1.7 References

1. RFC 2281, "Cisco Hot Standby Router Protocol (HSRP)." T. Li, B. Cole, P. Morton, D. Li. March 1998.

∎∎∎

6.2 Policy-Based Routing (PBR)

The QualNet PBR model is based on the CISCO IOS implementation [1].

6.2.1 Description

Policy-Based Routing (PBR) provides a mechanism to mark packets so that certain kinds of traffic receive differentiated, and preferential treatment. PBR allows expressing, and implementing forwarding/routing of data packets, based on the policies defined by the network administrators.

PBR makes use of route maps. See Section 6.3 for details of route maps.

6.2.2 Features and Assumptions

This section describes the implemented features, omitted features, assumptions and limitations of the PBR model.

6.2.2.1 Implemented Features

• PBR and local PBR.

6.2.2.2 Omitted Features

• Fast-Switched and CEF-Switched PBR.

6.2.2.3 Assumptions and Limitations

• The interface command should be put before the PBR command.
• There exists only one set command for a given set type.
• No particular check is available to ascertain whether its a data or a control packet. Hence, TOS is checked to IPTOS_PREC_INTERNETCONTROL to segregate the control and data packet. If a data packet is sent with this TOS, PBR wont work.
• If only the interface is set, its passed to the connected network.

6.2.3 Command Line Configuration

Commands for policy-based routing are specified in the router configuration file. The name of the router configuration file is specified in the scenario configuration (.config) file.

PBR Parameters
Table 6-6 describes the PBR configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 6-6. Policy-based Routing Parameters

Parameter	Value	Description
ROUTER-CONFIG-FILE Optional *Scope:* Global, Node	Filename	Name of the router configuration file. The router configuration file specifies commands for policy-based routing, route maps, route redistribution, and router access lists. The format of policy-based routing commands in the router configuration file is described in Section 6.2.3.1.
POLICY-ROUTING-STATISTICS Optional *Scope:* Global, Node	List: • YES • NO *Default:* NO	Specifies whether policy-based routing statistics are enabled.

6.2.3.1 Format of PBR Commands in Router Configuration File

Commands for policy-based routing are specified in the router configuration file using the following format:

```
<Node ID Specification>
<Interface Specification>
<Policy Specification>
```

These elements are described in Table 6-7.

> **Note:** All entries in the router configuration file are case insensitive.

TABLE 6-7.   PBR Specification

Element	Description
`<Node ID Specification>`	The node ID specification identifies the node for which the policy is being defined and has the following format: `NODE-IDENTIFIER <node-ID>` where `<node-ID>` Node ID of the node for which the policy is being defined.
`<Interface Specification>`	The interface specification identifies the type and number of interface for which the policy is being defined and has the following format: `INTERFACE <interface-number>` where `<interface-number>` Interface number.

`<Policy Specification>`	The policy specification identifies the route map tag to use for PBR. One interface can have only one route-map tag, but multiple route-map entries with different sequence numbers are allowed. These entries are evaluated in the order of sequence numbers until a match is found. If there is no match, packets are routed as usual. See Section 6.3 for details of route maps.
	
	The policy specification has the following format:
	
	`IP POLICY ROUTE-MAP <map-tag>`
	or
	
	`IP LOCAL POLICY ROUTE-MAP <map-tag>`
	
	where
	
	`<map-tag>` Tag associated with the route map to use.
	
	The second format is used for local policy-based routing.

Example of PBR Commands in Router Configuration File

The following is a segment of a router configuration file showing PBR commands and the route map used in the PBR commands:

```
NODE-IDENTIFIER 3
 INTERFACE 0
 IP POLICY ROUTE-MAP SRC-ROUTE-3IF0

ROUTE-MAP SRC-ROUTE-3IF0 PERMIT 1
    MATCH LENGTH 500 700
    SET IP NEXT-HOP 192.168.3.2
```

6.2.4 GUI Configuration

This section describes how to configure PBR in the GUI.

Configuring PBR Parameters

To configure the PBR parameters, perform the following steps:

1. Go to **Default Device Properties Editor > Node Configuration > Router Properties**.

2. Set **Router Configuration File** to the name of the router configuration file. The format of the router configuration file is described in Section 6.2.3.1.
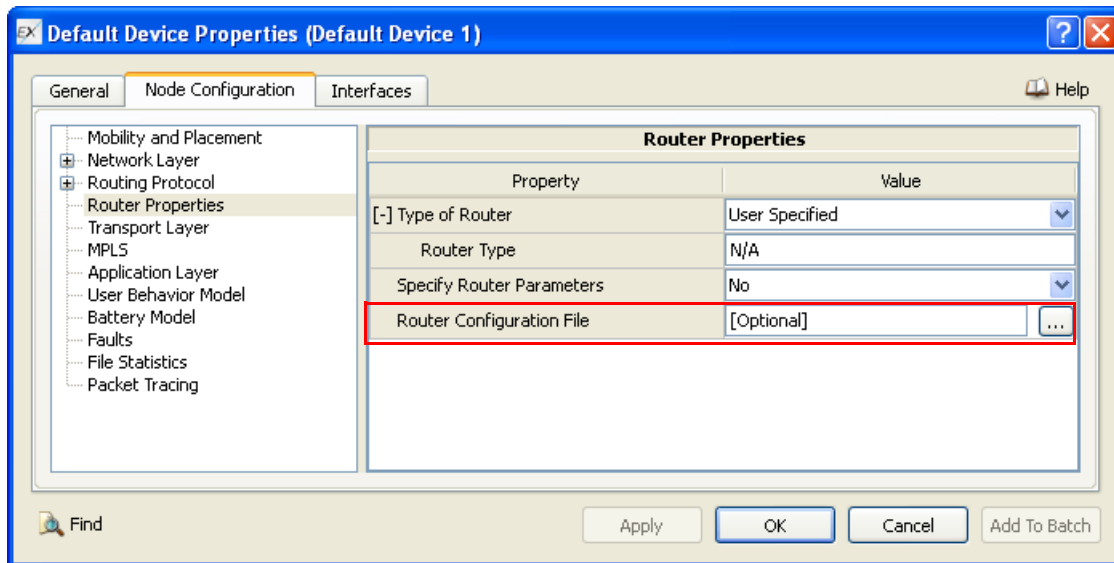
FIGURE 6-2.   Specifying Router Configuration File

TABLE 6-8.   Command Line Equivalent of Router Configuration File Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Router Configuration File	Node	`ROUTER-CONFIG-FILE`

Configuring Statistics Parameters

Statistics for PBR can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

TABLE 6-9.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Policy Routing	Global, Node	`POLICY-ROUTING-STATISTICS`

6.2.5 Statistics

Table 6-10 shows the PBR statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 6-10.   PBR Statistics

Statistic	Description
Packet Policy routed	Number of packets policy routed.
Packet Policy routed by LOCAL	Number of packets policy routed by local PBR.
Packet not Policy routed	Number of packets that are not policy routed.
Packet precedence set	Number of packets whose precedence is set by PBR.
Packet precedence set by LOCAL	Number of packets whose precedence is set by local PBR.

6.2.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the PBR model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/policy-routing. Table 6-11 lists the sub-directory where each scenario is located.

TABLE 6-11.   PBR Scenarios Included in QualNet

Scenario	Description
match-length	Shows PBR is enabled at Router 3. Whenever it receives packets whose level 3 length is between 500 and 700, it sets node 6 (192.168.3.2) as the adjacent next hop for that traffic.
set-next-hop	Shows PBR is enabled at Router 2. Whenever it receives a packet from node 1 and destined for node 7, it sets node 4 as the adjacent next hop for this traffic.
set-precedence	Shows PBR is enabled at Router 3. Whenever it receives packets whose level 3 length is between 500 and 600, it sets the precedence to 4 and when it is between 600 and 700, it sets the precedence to 2.

6.2.7 References

1. "Configuring Policy-Based Routing." Cisco IOS Release 12.0 Quality of Service Solutions Configuration Guide. http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart1/qcpolicy.htm#xtocid214451.

6.3 Route Maps

6.3.1 Description

A route map defines a set of rules or conditions. This route map is invoked by route redistribution and policy- based routing for defining the required criteria.

6.3.2 Command Line Configuration

Commands for defining route maps are specified in the router configuration file. The name of the router configuration file is specified in the scenario configuration (.config) file.

Route Map Parameters
Table 6-12 describes the route map configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 6-12.   Route Map Parameters

Parameter	Value	Description
`ROUTER-CONFIG-FILE` *Optional* *Scope:* Global, Node	Filename	Name of the router configuration file. The router configuration file specifies commands for policy-based routing, route maps, route redistribution, and router access lists. The format of commands for defining route maps in the router configuration file is described in Section 6.3.2.1.

6.3.2.1 Format of Route Map Commands in Router Configuration File

Route maps are specified in the router configuration file using the following format:

```
[<Node Specification>]
[<Interface Specification>]
<Add-route-map Command>
[<Match Commands>]
<Action Commands>
```

These elements are described in Table 6-13.

> **Note:**   All entries in the router configuration file are case insensitive.

TABLE 6-13. Route Map Specification

Element	Description

`<Node Specification>`	The node specification identifies the node for which router configuration parameters (including route maps) are being defined and has the following format:
	
	    `NODE-IDENTIFER <node-ID>`
	
	  where
	
	    `<node-ID>` Node ID.
	
	The node specification is optional and if it is not included, then the router configuration parameters apply to all nodes.

`<Interface Specification>`	The interface specification identifies the interface for which router configuration parameters (including route maps) are being defined and has the following format:
	
	    `INTERFACE <interface-number>`
	
	  where
	
	    `<interface-number>` Interface number.
	
	The interface specification is optional and if it is not included, then the router configuration parameters apply to all interfaces.

`<Add-route-map Command>`	A route map is added by using the following command:
	
	    `ROUTE-MAP <map-tag> [<filter>] [<seq-num>]`
	
	  where
	
	    `<map-tag>` Name associated with the route map.
	
	    `<filter>` This can be `PERMIT` or `DENY`. The filter specification is optional and if it is not included, then the default value is `PERMIT`.
	
	    If the filter is `PERMIT`, and criteria specified by the match commands are met, then the packet is processed as specified by the action commands.
	
	    If the filter is `PERMIT`, and criteria specified by the match commands are not met, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, then the normal forwarding algorithm is used.
	
	    If the filter is `PERMIT`, and criteria specified by the match commands are met, then the normal forwarding algorithm is used. No further route maps sharing the same map tag name are examined.
	
	    `<seq-num>` Sequence number of the route map in the list of route maps configured with the same name. The sequence number specification is optional.

TABLE 6-13. Route Map Specification (Continued)

Element	Description

<Match Commands>	Match commands can be specified to match packet lengths or IP addresses.
	
	The command to match the packet length has the following format:
	
	`MATCH LENGTH <min> <max>`
	
	where
	
	`<min>` Minimum packet length.
	
	`<max>` Maximum packet length.
	
	The command to match the IP address has the following format:
	
	`MATCH IP ADDRESS <list-of-ACLs>`
	
	where
	
	`<list-of-ACLs>` Non-empty list of access list numbers and/or access list names. See Section 6.5 for details of router access lists.
	
	Note: The match commands use the Cisco syntax. None, one, or both match commands can be specified for a route map. If a match command is not included, then the route map applies to all packets.

TABLE 6-13. Route Map Specification (Continued)

Element	Description

`<Action Commands>`	The action commands specify the action(s) to be performed when a packet matches the criteria specified by the match command(s). One or more of the following commands can be specified.
	
	Note: The action commands use the Cisco syntax.
	
	To set the precedence value in the IP header, use the following command:
	
	`SET IP PRECEDENCE <precedence>`
	
	where
	
	`<precedence>` Precedence number or precedence name to which the precedence filed of the IP header should be set.
	
	To set the next hop to which to route the packet, use the following command:
	
	`SET IP NEXT-HOP <address-list>`
	
	where
	
	`<address-list>` Non-empty list of IP addresses. The next hop must be adjacent to the node.
	
	To set the output interface for the packet, use the following command:
	
	`SET INTERFACE <interface-list>`
	
	where
	
	`<interface-list>` Non-empty list of interface type/ interface name pairs.
	
	To set the default next hop to which to route the packet when there is no explicit route to the destination, use the following command:
	
	`SET IP DEFAULT NEXT-HOP <address-list>`
	
	where
	
	`<address-list>` Non-empty list of IP addresses.
	
	To set the default output interface for the packet when there is no explicit route to the destination, use the following command:
	
	`SET DEFAULT INTERFACE <interface-list>`
	
	where
	
	`<interface-list>` Non-empty list of interface type/ interface name pairs.

Examples of Route Maps in Router Configuration File

The following lines show examples of route map configuration in the router configuration file.

```
ROUTE-MAP SRC-ROUTE-3IF0 PERMIT 1
MATCH LENGTH 500 700
SET IP NEXT-HOP 192.168.3.2
#

ROUTE-MAP LOAD-SHARE PERMIT 1
MATCH IP ADDRESS 106
SET IP NEXT-HOP 192.168.2.3
```

6.3.3 GUI Configuration

This section describes how to configure route map in GUI.

Configuring Route Map Parameters

To configure the Route Map parameters, perform the following steps:

1. Go to **Default Device Properties Editor > Node Configuration > Router Properties**.

2. Set **Router Configuration File** to the name of the router configuration file. The format of the router configuration file is described in Section 6.3.2.1.
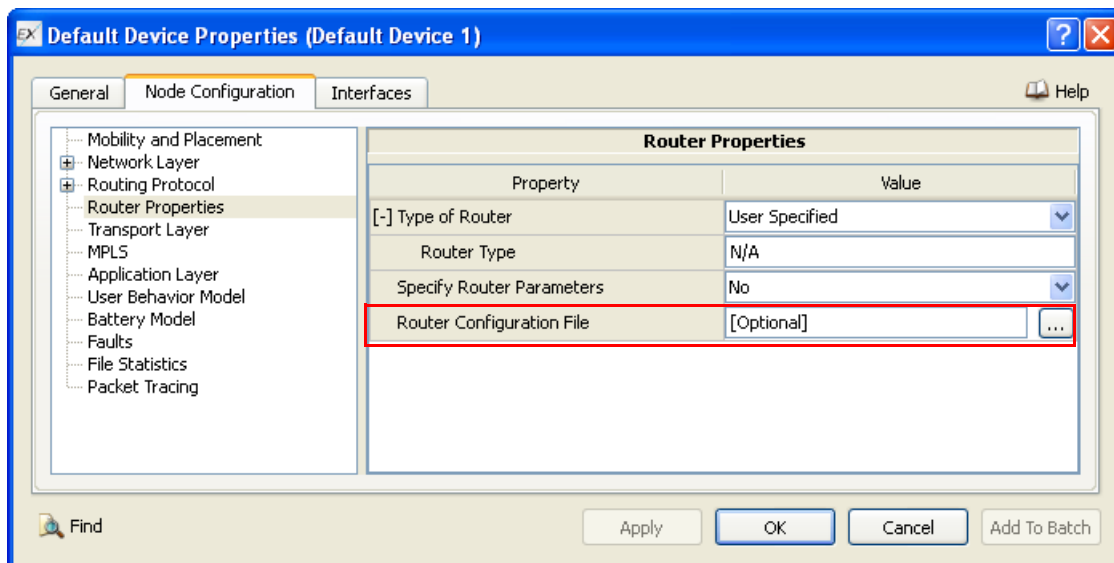
FIGURE 6-3.   **Specifying Router Configuration File**

TABLE 6-14.   **Command Line Equivalent of Router Configuration File Parameters**

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Router Configuration File	Node	ROUTER-CONFIG-FILE

6.3.4 Statistics

No statistics are collected for the Route Map model.

••

6.4 Route Redistribution

6.4.1 Description

Redistribution is a process used by a routing protocol to advertise routes learned by other means, such as another routing protocol, static routes, or directly connected routes. While running a single routing protocol throughout the entire IP internetwork is desirable, multi-protocol routing is useful for a number of reasons including company mergers, multiple departments managed by multiple network administrators, and multi-vendor environments. Often, running different routing protocols is part of a network design. Route redistribution makes it possible for nodes in a network to run multiple routing protocols.

6.4.2 Command Line Configuration

Commands for route redistribution are specified in the router configuration file. The name of the router configuration file is specified in the scenario configuration (.config) file.

Route Redistribution Parameters

Table 6-15 describes the route redistribution configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 6-15. Route Redistribution Parameters

Parameter	Value	Description
ROUTER-CONFIG-FILE Optional *Scope:* Global, Node	Filename	Name of the router configuration file. The router configuration file specifies commands for policy-based routing, route maps, route redistribution, and router access lists. The format of route redistribution commands in the router configuration file is described in Section 6.4.2.1.
ROUTE-REDISTRIBUTION-STATISTICS Optional *Scope:* Global, Node	List: • YES • NO *Default:* NO	Enables route redistribution statistics collection.

6.4.2.1 Format of Route Redistribution Commands in Router Configuration File

Route redistribution commands are specified in the router configuration file using the following format:

```
<Node ID Specification>
<Router Specification>
<Redistribute Commands>
```

These elements are described in Table 6-16.

> **Note:** All entries in the router configuration file are case insensitive.

TABLE 6-16.   Route Redistribution Specification

Element	Description

`<Node ID Specification>`	The node ID specification identifies the node for which redistribution is defined and has the following format:
	
	    `NODE-IDENTIFIER <node-ID>`
	
	  where
	
	    `<node-ID>` Node ID of the node for which redistribution is being defined.

`<Router Specification>`	The router specification identifies the protocol to which routes should be redistributed and has the following format:
	
	    `ROUTER <protocol>`
	
	  where
	
	    `<protocol>` Protocol to which routes should be redistributed. It can be one of the following:
	
	      • `BELLMANFORD`
	      • `BGP`
	      • `EIGRP`
	      • `IGRP`
	      • `OSPFv2`
	      • `RIPv2`
	      • `RIPv1`

TABLE 6-16.   Route Redistribution Specification (Continued)

Element	Description

`<Redistribute Commands>`	The redistribute commands specify the redistribution policy and have the following format:
	
	 `REDISTRIBUTE <protocol> [METRIC <metric>]`
	`               [ROUTE-MAP [<map-tag>]]`
	`               [<start-time>] [<end-time>]`
	 or
	 `NO REDISTRIBUTE <protocol> [METRIC <metric>]`
	`                  [ROUTE-MAP <map-tag>]`
	`                  <start-time> <end-time>`
	
	 where
	
	 `<protocol>` — Protocol from which routes are redistributed.
	
	 `METRIC <metric>` — Cost to reach the destination. This parameter is optional.
	
	 `ROUTE-MAP [<map-tag>]` — Tag associated with the route map to use. See Section 6.3 for details of route maps. This parameter is optional. If it is not specified, then all routes are redistributed. If the keyword `ROUTE-MAP` is specified but a route map tag is not specified, then no routes are distributed.
	
	 `<start-time>` — Time when route redistribution starts. This parameter is optional. If not specified, redistribution starts when the simulation starts.
	
	 `<end-time>` — Time when route redistribution ends. This parameter is optional but must be specified if the start time is specified. If not specified, redistribution ends when the simulation ends.
	
	 Note: The `NO REDISTRIBUTE` command has a higher priority than the `REDISTRIBUTE` command. If both were specified for the same router, routes would not be redistributed if the start time and end time are the same for both.

Examples of Route Redistribution Commands in Router Configuration File

The following examples show route redistribution configuration in the router configuration file.

Example 1:

```
NODE-IDENTIFIER 4
ROUTER ospfv2
REDISTRIBUTE RIPv2 10S 60S

NODE-IDENTIFIER 10
ROUTER ospfv2
REDISTRIBUTE RIPv2 METRIC 21
# Routes are redistributed with metric 21
NO REDISTRIBUTE RIPv2 50S 70S
# Routes would not be redistributed in this interval
#
NODE-IDENTIFIER 7
# ROUTER ospfv2
# REDISTRIBUTE RIPv2 ROUTE-MAP ospf-to-rip
# Route map has been tagged
#
# ROUTE-MAP ospf-to-rip permit 1  5
```

Example 2: Multi-protocol Redistribution:

```
NODE-IDENTIFIER 4
ROUTER OSPFv2
REDISTRIBUTE RIPv2
ROUTER IGRP
REDISTRIBUTE RIPv2 METRIC 10000 100 255 1 1500
# RIP routes are redistributed
#
# NODE-IDENTIFIER 10
# ROUTER OSPFv2
# REDISTRIBUTE RIPv2
# REDISTRIBUTE IGRP
```

6.4.3 GUI Configuration

This section describes how to configure Route Redistribution in the GUI.

Configuring Route Redistribution Parameters

To configure the PBR parameters, perform the following steps:

1. Go to **Default Device Properties Editor > Node Configuration > Router Properties**.
2. Set **Router Configuration File** to the name of the router configuration file. The format of the router configuration file is described in Section 6.4.2.1.
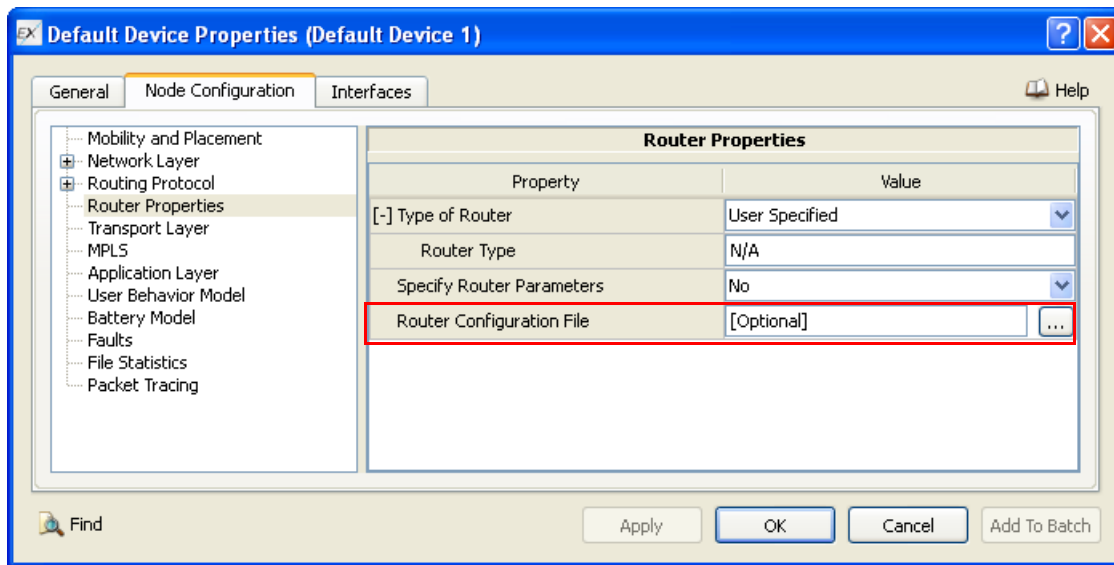
FIGURE 6-4.   Specifying Router Configuration File

TABLE 6-17.   Command Line Equivalent of Router Configuration File Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Router Configuration File	Node	ROUTER-CONFIG-FILE

Configuring Statistics Parameters

Statistics for Route Redistribution can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

TABLE 6-18.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Route Redistribution	Global, Node	ROUTE-REDISTRIBUTION-STATISTICS

6.4.4 Statistics

Table 6-19 shows the statistics collected by Route Redistribution model that are output to the statistics (.stat) file at the end of simulation.

TABLE 6-19.   Route Redistribution Statistics

Statistic	Description
Total Routes Found	Total number of routes found to redistribute.
Routes Redistributed	Number of routes redistributed.

TABLE 6-19.   Route Redistribution Statistics (Continued)

Statistic	Description
Routes Blocked for NO REDISTRIBUTE	Number of routes blocked due to NO REDISTRIBUTE command.
Unreachable Routes Informed	Number of routes that become unreachable.
Routes Discarded by Route Map	Number of routes discarded by the route map.
Routes Discarded for Time Range	Number of routes discarded due to start time and end time of REDISTRIBUTE command.

6.4.5 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the Route Redistribution model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/route-redistribution. Table 6-20 lists the sub-directory where each scenario is located.

TABLE 6-20.   Route Redistribution Scenarios Included in QualNet

Scenario	Description
bellmanford-eigrp	Shows one-way redistribution between Bellmanford and EIGRP routing protocols. The redistribution is configured to redistribute Bellmanford into EIGRP.
eigrp-bellmanford	Shows one-way redistribution between Bellmanford and EIGRP routing protocols. The redistribution is configured to redistribute EIGRP into Bellmanford.
igrp-bellmanford	Shows one-way redistribution between Bellmanford and IGRP routing protocols. The redistribution is configured to redistribute IGRP into Bellmanford.
one-way-multiple-protocol	Shows one-way redistribution between RIPv2, IGRP and OSPFv2 routing protocols. The redistribution is configured to redistribute IGRP and OSPFv2 routes into RIPv2.
one-way-with-metric	Shows one-way redistribution using multiple border routers between two different routing protocols - RIPv2 and OSPFv2 with 'metric' parameter. The redistribution is configured to redistribute OSPFv2 routes into RIPv2.
one-way-with-route-map	Shows one-way redistribution between two different routing protocols - RIPv2 and OSPFv2 with 'route-map' parameter. The redistribution is configured to redistribute OSPFv2 routes into RIPv2.
ospf-bellmanford	Shows one-way redistribution between Bellmanford and OSPFv2 routing protocols. The redistribution is configured to redistribute OSPFv2 into Bellmanford.
rip-bellmanford	Shows one-way redistribution between Bellmanford and RIP routing protocols. The redistribution is configured to redistribute RIP into Bellmanford.
rip-eigrp	Shows one-way redistribution between Bellmanford and EIGRP routing protocols. The redistribution is configured to redistribute Bellmanford and EIGRP.
two-way	Shows two-way redistribution between RIPv2 and OSPFv2 routing protocols.

∎∎
6.5 Router Access Lists

6.5.1 Description

A router access list is a filter for configuring routers to restrict access to specific types of traffic. A router or gateway uses access list to increase network security by accepting or denying packets based on the traffic type or network address.

6.5.2 Command Line Configuration

Commands for defining router access lists are specified in the router configuration file. The name of the router configuration file is specified in the scenario configuration (.config) file.

Router Access List Parameters
Table 6-21 describes the router access list configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 6-21.   Router Access List Parameters

Parameter	Value	Description
ROUTER-CONFIG-FILE *Optional* *Scope:* Global, Node	Filename	Name of the router configuration file. The router configuration file specifies commands for policy-based routing, route maps, route redistribution, and router access lists. The format of commands for defining router access lists in the router configuration file is described in Section 6.5.2.1.
ACCESS-LIST-STATISTICS *Optional* *Scope:* Global, Node	List: • YES • NO *Default:* NO	Enables router access list statistics collection.
ACCESS-LIST-TRACE *Optional* *Scope:* Global, Node	List: • YES • NO *Default:* NO	Enables router access list trace.

6.5.2.1 Format of Router Access List Commands in the Router Configuration File

Router access lists are specified in the router configuration file using the following format:

```
[<Node Specification>]
[<Interface Specification>]
<Access Lists Specification>
```

These elements are described in Table 6-22.

Note: **1.** All contents of the router configuration file are case insensitive.

2. The access list definitions follow the Cisco syntax.

TABLE 6-22.   Router Access List Specification

Element	Description
`<Node Specification>`	The node specification identifies the node for which router configuration parameters (including router access lists) are being defined and has the following format: `NODE-IDENTIFER <node-ID>` where `<node-ID>` Node ID. The node specification is optional and if it is not included, then the router configuration parameters apply to all nodes.
`<Interface Specification>`	The interface specification identifies the interface for which router configuration parameters (including router access lists) are being defined and has the following format: `INTERFACE <interface-number>` where `<interface-number>` Interface number. The interface specification is optional and if it is not included, then the router configuration parameters apply to all interfaces.
`<Access Lists Specification>`	One or more access lists of the following types can be specified: • Standard Numbered Access List • Standard Named Access List • Numbered Extended Access List • Named Extended Access List • Numbered Extended Access List for IP • Named Extended Access List for IP • Numbered Extended Access List for TCP • Named Extended Access List for TCP • Numbered Extended Access List for UDP • Named Extended Access List for UDP • Numbered Extended Access List for ICMP • Named Extended Access List for ICMP • Numbered Extended Access List for IGMP • Named Extended Access List for IGMP The syntax of each type of access list is described below.

Syntax of Access Lists

- Standard Numbered Access List

    The standard numbered access list has the following format:

    ```
    access-list access-list-number {permit | deny}
                    {source}{source-wildcard}[log| log-input]
    ```

    Notes: 1. access-list-number is in the range of 1-99 for standard numbered access lists.

            2. {source}{source-wildcard} can be replaced by ANY (0.0.0.0 255.255.255.255) or HOST {source} (source address 0.0.0.0). The same remains for any address declaration.

- Standard Named Access List

    The standard named access list has the following format:

    ```
    ip access-list standard {name} {deny | permit}{source}{source-
    wildcard}[log| log-input]
    ```
    or
    ```
    ip access-list standard {name}
    deny {source [source-wildcard] | any}}[log| log-input]
    ```
    or
    ```
    ip access-list standard {name}
    permit {source [source-wildcard] | any}}[log| log-input]
    ```

- Numbered Extended Access List

    The numbered extended access list has the following format:

    ```
    access-list access-list-number {permit | deny} protocol {source-
    address}{source-wildcard}[operator port] destination-address
    destination-wildcard [operator port] [precedence precedence] [tos tos]
    [log| log-input]
    ```

    Note: Extended access-list-number is in the range of 100-199.

- Named Extended Access List

    The named extended access list has the following format:

    ```
    ip access-list extended {name}{deny | permit} {protocol} {source}
    {source-wildcard}[operator port] {destination} {destination-wildcard}
    [operator port][precedence precedence name or number] [tos tos name or
    number] [log | log-input]
    ```
    or
    ```
    ip access-list extended name

    {deny | permit} {protocol} {source} {source-wildcard} {destination}
    {destination-wildcard} [precedence precedence] [tos tos] [log | log-
    input]
    ```

- Numbered Extended access list for IP:

  The numbered extended access list for IP has the following format:

  ```
  access-list {access-list-number | access-list-name} {deny | permit} ip
  {source} {source-wildcard} {destination} {destination-wildcard}
  [precedence precedence name or number] [tos tos name or number] [log |
  log-input]
  ```

- Named Extended access list for IP:

  The named extended access list for IP has the following format:

  ```
  ip access-list extended name

  {deny | permit} ip {source} {source-wildcard} {destination}
  {destination-wildcard} [precedence precedence] [tos tos] [log | log-
  input]
  ```

- Numbered Extended access list for TCP:

  The numbered extended access list for TCP has the following format:

  ```
  access-list {access-list-number} {deny | permit} tcp {source} {source-
  wildcard} [operator port [port]] {destination} {destination-wildcard}
  [operator port] [established][precedence precedence name or number]
  [tos tos name or number] [log | log-input]
  ```

- Named Extended access list for TCP:

  The named extended access list for TCP has the following format:

  ```
  ip access-list extended name

  {deny | permit} tcp {source} {source-wildcard} {destination}
  {destination-wildcard} [precedence precedence] [tos tos] [log | log-
  input]
  ```

- Numbered Extended access list for UDP:

  The numbered extended access list for UDP has the following format:

  ```
  access-list {access-list-number} {deny | permit} udp {source} {source-
  wildcard} [operator port [port]] {destination} {destination-wildcard}
  [operator port] [precedence precedence name or number] [tos tos name or
  number] [log | log-input]
  ```

- Named Extended access list for UDP:

  The named extended access list for UDP has the following format:

  ```
  ip access-list extended name

  {deny | permit} udp {source} {source-wildcard} {destination}
  {destination-wildcard} [precedence precedence] [tos tos] [log | log-
  input]
  ```

- Numbered Extended access list for ICMP:

  The numbered extended access list for ICMP has the following format:

  ```
  access-list {access-list-number | access-list-name} {deny | permit}
  icmp {source}{source-wildcard}{destination}{destination-wildcard}
  [icmp-type [icmp-code] | icmp-message] [precedence precedence name or
  number] [tos tos name or number] [log | log-input]
  ```

- Named Extended access list for ICMP:

  The named extended access list for ICMP has the following format:

  ```
  ip access-list extended name

  {deny | permit} icmp {source}{source-
  wildcard}{destination}{destination-wildcard} [icmp-type [icmp-code] |
  icmp-message] [precedence precedence name or number] [tos tos name or
  number] [log | log-input]
  ```

- Numbered Extended access list for IGMP:

  The numbered extended access list for IGMP has the following format:

  ```
  access-list {access-list-number | access-list-name} {deny | permit}
  igmp {source}{source-wildcard}{destination}{destination-
  wildcard}[igmp-type | igmp-message] [precedence precedence name or
  number] [tos tos name or number] [log | log-input]
  ```

- Named Extended access list for IGMP:

  The named extended access list for IGMP has the following format:

  ```
  ip access-list extended name

  {deny | permit} igmp {source}{source-
  wildcard}{destination}{destination-wildcard}[igmp-type | igmp-message]
  [precedence precedence name or number] [tos tos name or number] [log |
  log-input]]
  ```

6.5.3 GUI Configuration

This section describes how to configure router access list in GUI.

Configuring Router Access List Parameters

To configure the router access list parameters, perform the following steps:

1. Go to **Default Device Properties Editor > Node Configuration > Router Properties**.

2. Set **Router Configuration File** to the name of the router configuration file. The format of the router configuration file is described in Section 6.5.2.1.
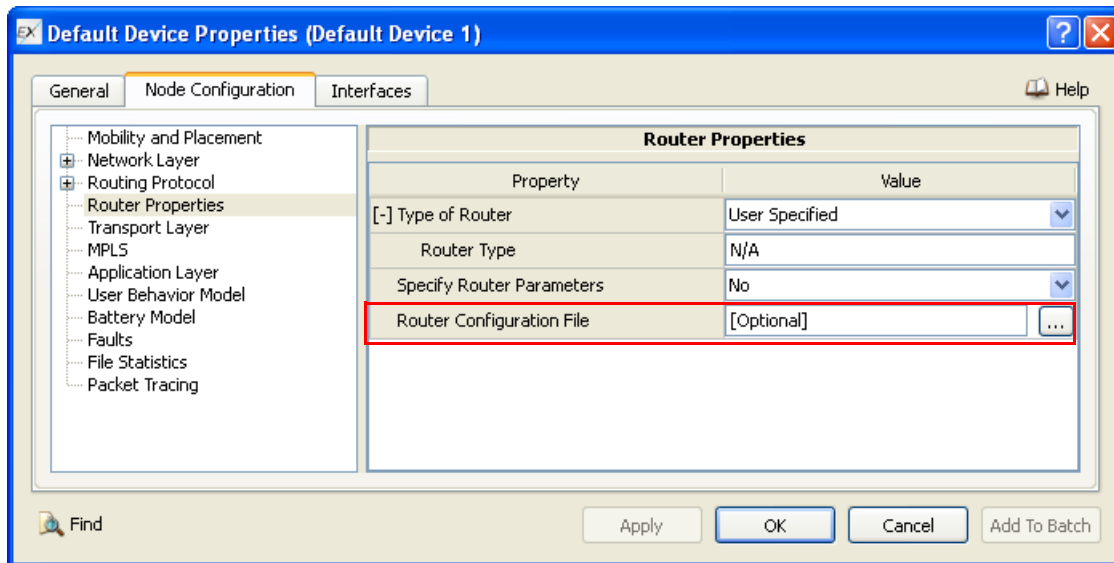
FIGURE 6-5.   Specifying Router Configuration File

TABLE 6-23.   Command Line Equivalent of Router Configuration File Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Router Configuration File	Node	ROUTER-CONFIG-FILE

Configuring Statistics Parameters

Statistics for Router Access List model can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for the Router Access List model, check the box labeled **Access List** in the appropriate properties editor.

TABLE 6-24.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Access List	Global, Node	`ACCESS-LIST-STATISTICS`

Configuring Tracing Parameters

To enable Access List tracing in the GUI, perform the following steps:

1. Go to one of the following locations:

- To enable tracing at the global level, go to **Scenario Properties Editor > Statistics and Tracing > Packet Tracing**.

- To enable tracing for a specific node, go to **Default Device Properties Editor > Node Configuration > Packet Tracing**.

In this section, we show how to configure access list tracing parameters for a node in the **Default Device Properties Editor**. Parameters can be set in the other properties editors in a similar way.

2. To enable access list tracing, set **Enable Access List Tracing** to *Yes.*
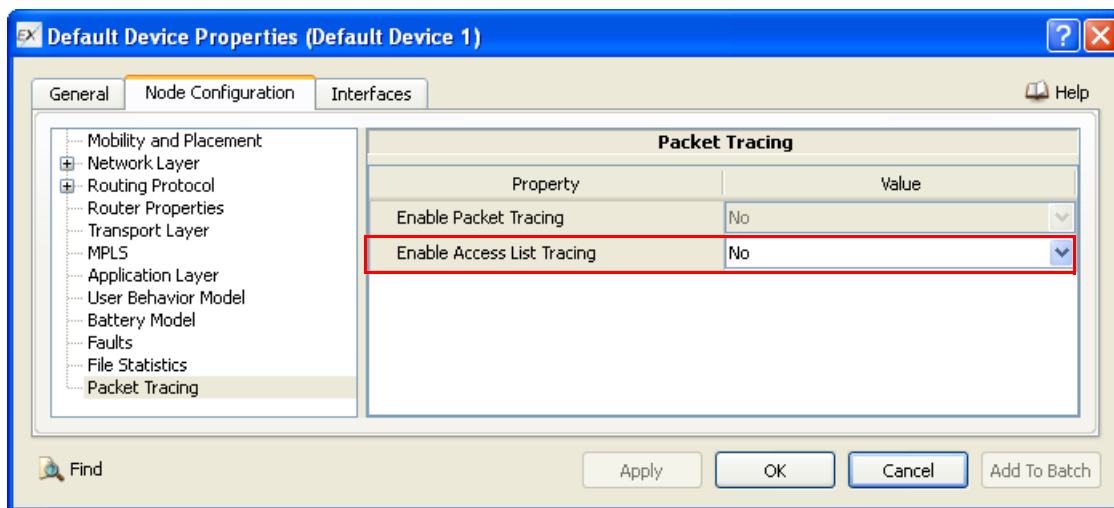
FIGURE 6-6.   Enabling Access List Tracing

TABLE 6-25.   Command Line Equivalent of Access List Tracing Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Enable Access List Tracing	Global, Node	`ACCESS-LIST-TRACE`

6.5.4 Statistics

Table 6-26 shows the statistics collected by the Router Access List model that are output to the statistics (.stat) file at the end of simulation.

TABLE 6-26.   Router Access List Statistics

Statistics	Description
Standard ACL	
Packet Dropped at IN	Total number of packets dropped at the incoming interface for the standard access list.
Packet Dropped at OUT	Total number of packets dropped at the outgoing interface for the standard access list.
Extended ACL	
Packet Dropped at IN	Total number of packets dropped at the incoming interface for the extended access list.
Packet Dropped at OUT	Total number of packets dropped at the outgoing interface for the extended access list.
ACL	
Packet Dropped for mismatch at IN	Total number of packets dropped at the incoming interface for no matching access list.
Packet Dropped for mismatch at OUT	Total number of packets dropped at the outgoing interface for no matching access list.

░░

6.6 Router Model

6.6.1 Description

Routers are modeled as special devices. A router model characterizes the hardware and software capabilities of the router, including the backplane throughput, queue type, and scheduler type. QualNet provides pre-configured models for many popular routers used in enterprise networks. Users can also configure their own router models.

6.6.2 Omitted Features and Assumptions

This section describes the omitted features, assumptions and limitations of the router model.

6.6.2.1 Omitted Features

• Configuring the routers online through a hyper terminal type interface.
• Support for logical interfaces.
• Console and AUX ports.
• Buffering mechanisms like various buffer pools and processors used inside the routers.
• Importing and exporting devices.
• Internal Scheduler for Central backplane (to handle all INPUT and CPU queue).
• Update of existing router models with input queue related parameters.

6.6.2.2 Assumptions and Limitations

• Various Switch mechanisms are entirely dependent on the assigned backplane values.
• A 64 byte packet size is used in computing the bps equivalent of the pps values for the router performances.
• A 1460 byte, Ethernet MSS packet size is used in computing the Input and Output queue sizes.
• In case of "BACKPLANE-TYPE CENTRAL", there is no input queue for each interface.

6.6.3 Command Line Configuration

The router model for a node can be specified in one of the following ways:

• The user can preconfigure router models in a router models file. To specify the router models file, include the following parameter in the scenario configuration (.config) file:

```
ROUTER-MODEL-CONFIG-FILE      <router-models-file>
```

where

<router-models-file>   Name of the Router model configuration file.

The format of this file is described in Section 6.6.3.1.

Each router model in the router model file is identified by a unique name as the value of the parameter ROUTER-MODEL. All configuration parameters for that router model are entered after the model name. The user can then specify one of the preconfigured router models by setting the parameter ROUTER-MODEL (see Table 6-27) in the scenario configuration file to the name of the router model. All

parameters associated with that preconfigured router model then apply to the node. Typically, the system properties of the router are specified in this manner.

QualNet provides pre-configured models for many popular routers. QualNet's router models are contained in the file QUALNET_HOME/scenarios/default/default.router-models. The user can copy a router model from that file to the router models file and use it in a scenario by setting the parameter `ROUTER-MODEL` (see Table 6-27) in the scenario configuration file to the name of the QualNet router model.

- The user can specify router configuration parameters for a node directly in the scenario configuration file (see Table 6-27).

Router Parameters

Table 6-27 describes the router configuration parameters for the scenario configuration (.config) file. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 6-27.   Router Configuration Parameters

Parameter	Value	Description
`ROUTER-MODEL` Optional *Scope:* Global, Node	String *Default:* `GENERIC`	Specifies the name of the router model. This should be the name of one of the router models in the router model configuration file.
`ROUTER-BACKPLANE-TYPE` Optional *Scope:* Global, Node	List: • `CENTRAL` • `DISTRIBUTED` *Default:* `DISTRIBUTED`	Specifies the type of processing mechanism used by the router model. If the value is `CENTRAL`, then the packets are processed using a central processor. If the value is `DISTRIBUTED`, then interface processors are also used for processing packets.
`ROUTER-BACKPLANE-THROUGHPUT` Optional *Scope:* Global, Node	Real *or* List: • `UNLIMITED` Unit: bps *Default:* `UNLIMITED`	Backplane throughput or capacity of the router model. The value `UNLIMITED` for this parameter specifies that the backplane throughput is not limited.
`ROUTER-PERFORMANCE-VARIATION` Optional *Scope:* Global, Node	Real *Default:* `0.0`	Specifies the variation in the backplane throughput. To process a packet, a throughput value is randomly chosen in the range (*throughput - variation*) to (*throughput + variation*), where t*hroughput* is the value of the parameter `ROUTER-BACKPLANE-THROUGHPUT` and *variation* is the value of the parameter `ROUTER-PERFROMANCE-VARIATION`.

6.6.3.1 Format of the Router Models File

The router models file defines router models. Each router model definition consists of a router model name followed by parameters that specify the characteristics of that router.

The format for defining a router model is:

```
ROUTER-MODEL                        <router-model-name>
ROUTER-BACKPLANE-TYPE               <backplane-type>
ROUTER-BACKPLANE-THROUGHPUT         <throughput>
ROUTER-PERFORMANCE-VARIATION        <variation>
IP-QUEUE-TYPE                       <queue-type>
IP-QUEUE-SCHEDULER                  <scheduler-type>
IP-QUEUE-NUM-PRIORITIES             <num-priorities>
IP-QUEUE-PRIORITY-QUEUE-SIZE        <queue-size>
```

where

`<router-model-name>`	Unique name (string) identifying the model.
`<backplane-type>`	Type of processing mechanism used by the router model. See the description of `ROUTER-BACKPLANE-TYPE` in Table 6-27.
`<throughput>`	Backplane throughput or capacity of the router model. See the description of `ROUTER-BACKPLANE-THROUGHPUT` in Table 6-27.
`<variation>`	Variation in the backplane throughput. See the description of `ROUTER-PERFORMANCE-VARIATION` in Table 6-27.
`<queue-type>`	Type of priority queue. Refer to the description `IP-QUEUE-TYPE` of *QualNet User's Guide* for details.
`<scheduler-type>`	Type of scheduler. Refer to the description `IP-QUEUE-SCHEDULER` of *QualNet User's Guide* for details.
`<num-priorities>`	Number of priority queues. Refer to the description `IP-QUEUE-NUM-PRIORITIES` of *QualNet User's Guide* for details.
`<queue-size>`	Size of each output priority queue. Refer to the description `IP-QUEUE-PRIORITY-QUEUE-SIZE` of *QualNet User's Guide* for details.

Notes: 1. Parameters specifying the router characteristics can be included in the router models file as well as the scenario configuration (.config) file. The values specified in the scenario configuration file take precedence over the values specified in the router models file.

2. In the router models file, all parameters following the parameter `ROUTER-MODEL` are optional and can be specified in any order.

3. All parameters in the router models file are specified without a qualifier or instance specification.

6.6.4 GUI Configuration

This section describes how to configure router models in GUI.

Specifying Router Models File

To specify the name of the router models file, do the following:

1. Go to **Scenario Properties Editor > Supplemental FIles**.

2. Set the parameter **Router Models File** to the name of the router models file.
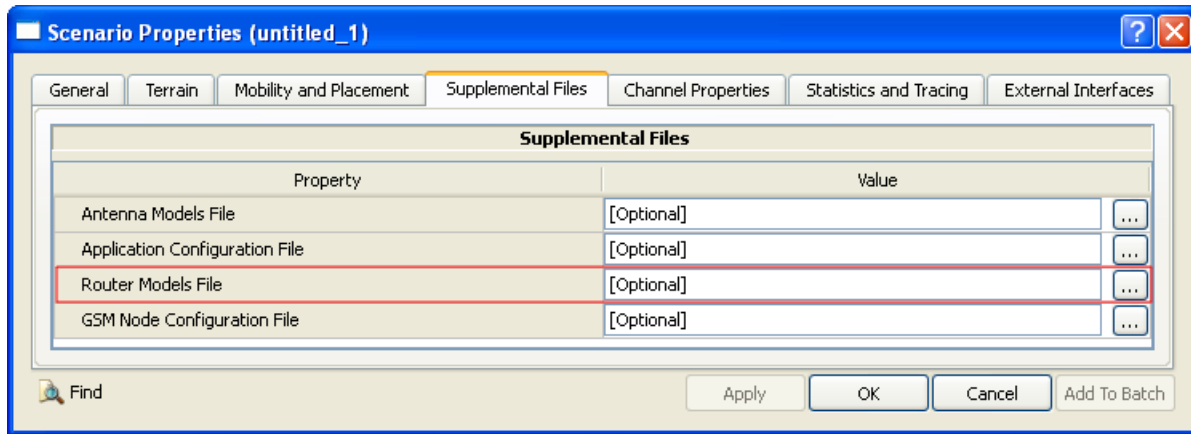
FIGURE 6-7.   Specifying Router Models File

TABLE 6-28.   Command Line Equivalent of Router Models File Parameter

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Router Models File	Global	`ROUTER-MODEL-CONFIG-FILE`

Configuring Router Properties at a Node

To configure the router model for a specific node, do the following:

1. Go to **Default Device Properties Editor > Node Configuration > Router Properties**.

2. To use a preconfigured router model, do the following:

   a. To use one of QualNet's router models, set **Type of Router** to *Predefined* and set **Router Type** to the name of the desired model by selecting it from the pull-down list.

      To use one of the user-configured router models, set **Type of Router** to *User Specified* and set **Router Type** to the name of one of the router models in the router models file.
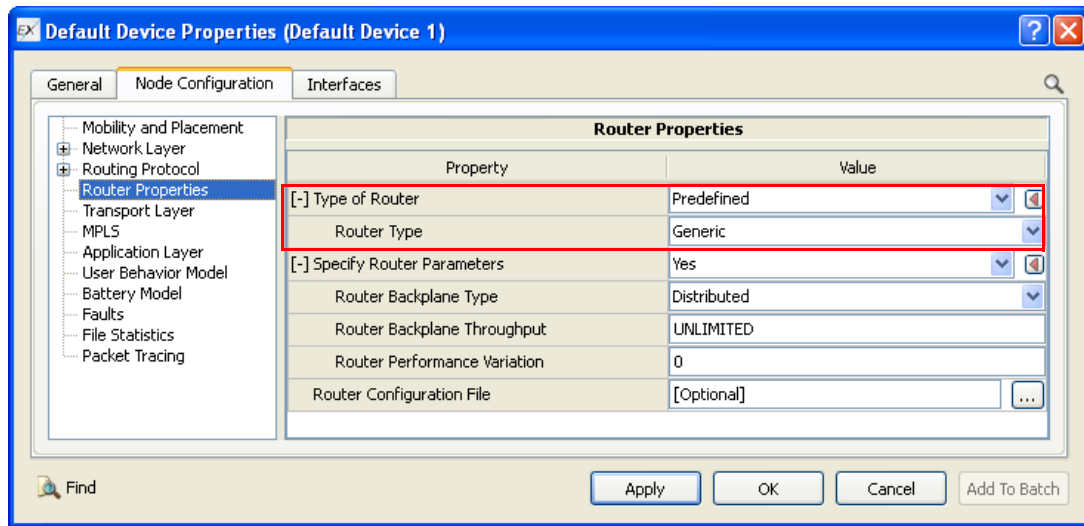
FIGURE 6-8.   Setting Router Type for Predefined Routers

TABLE 6-29.   Command Line Equivalent of Router Type Parameter

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Router Type	Node	ROUTER-MODEL

b. To overwrite any of the parameter values associated with the selected router model, set **Specify Router Parameters** to *Yes* and set the parameters listed in Table 6-30.
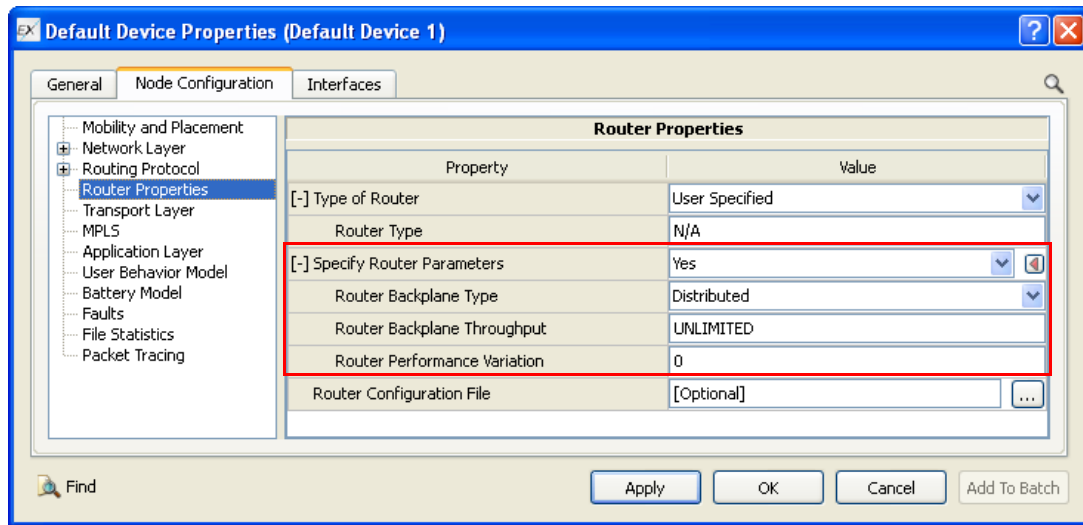
FIGURE 6-9.   Setting Router Parameters

TABLE 6-30.   Command Line Equivalent of Router Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Router Backplane Type	Node	`ROUTER-BACKPLANE-TYPE`
Router Backplane Throughput	Node	`ROUTER-BACKPLANE-THROUGHPUT`
Router Performance Variation	Node	`ROUTER-PERFORMANCE-VARIATION`

3. To specify router parameters independently (i.e., without using any preconfigured router model), do the following:

    a. Set **Type of Router** to *User Specified* and **Router Type** to *N/A*.
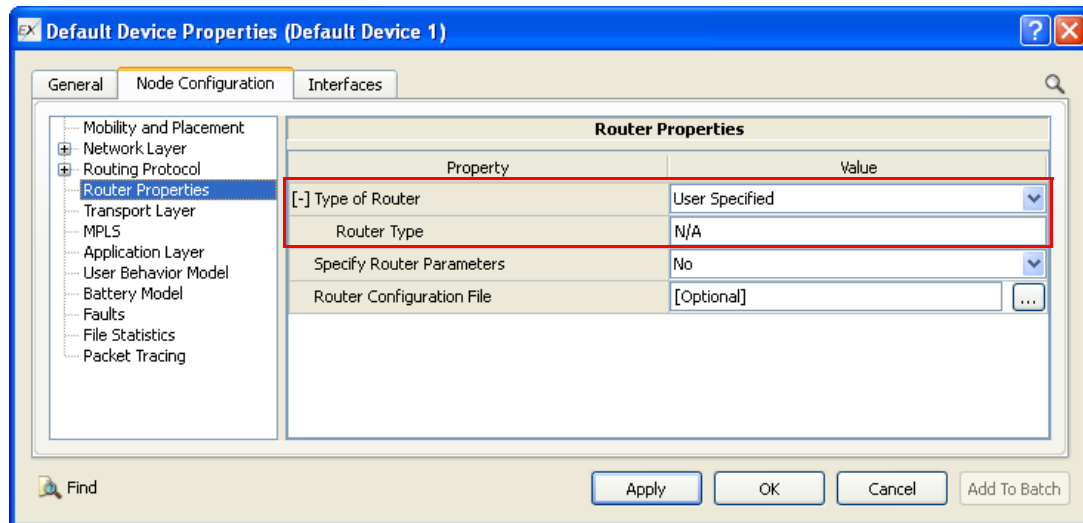
FIGURE 6-10.   Specifying Router Properties Independently

    b. Set **Specify Router Parameters** to *Yes* and set the parameters listed in Table 6-30.

4. To specify a router configuration file for the node, set the parameter **Router Configuration File** to the name of the router configuration file.
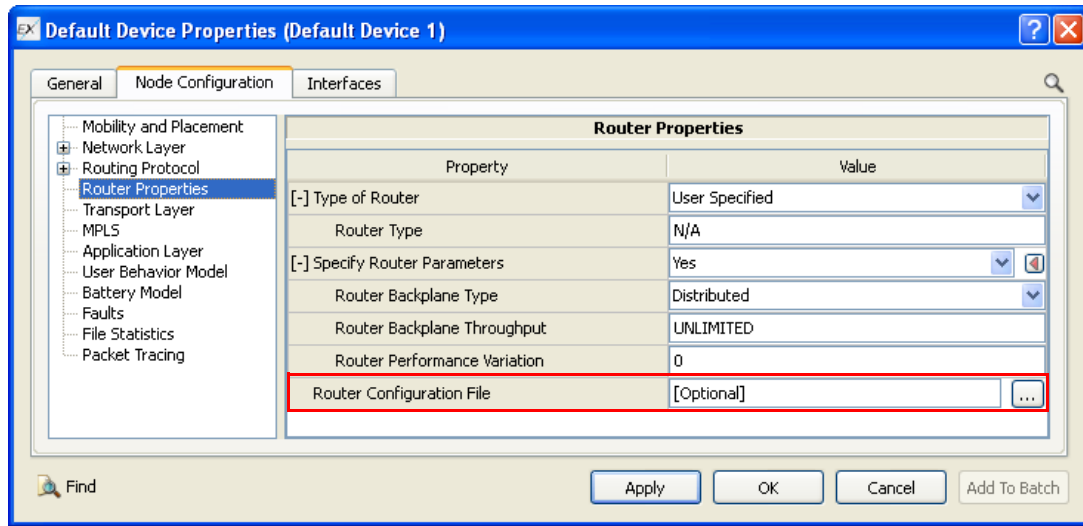
FIGURE 6-11.   Specifying Router Configuration File

TABLE 6-31.   Command Line Equivalent of Router Configuration File Parameter

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Router Configuration File	Node	`ROUTER-MODEL-CONFIG-FILE`

6.6.5 Statistics

Table 6-32 lists the router model statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 6-32.   Router Model Statistics

Statistic	Description
Queue Statistics	
Total packets queued	Total number of packets enqueued in the Queue (INPUT/CPU).
Total packets dequeued	Total number of packets dequeued from the Queue (INPUT/CPU).
Total packets dropped	Total number of packets dropped due to Queue overflow (INPUT/CPU).
Average Queue Length (bytes)	Average size of Queue (INPUT/CPU) length through out the simulation in bytes.
Peak Queue Size (bytes)	The Maximum queue length for the entire simulation time (INPUT/CPU) in bytes.
Average Time In Queue	Average time of the packet stay (in seconds) inside the Queue (INPUT/CPU).
Longest Time in Queue	The peak time of the packet stay (in seconds) inside the Queue (INPUT/CPU) throughout the simulation.
Total Packets Dropped Forcefully	Total number of Packets Dropped Forcefully.
Scheduler Statistics	
Packets Queued	Total number of packets enqueued for specified scheduler (INPUT/CPU Scheduler).

TABLE 6-32.   Router Model Statistics (Continued)

Statistic	Description
Packets Dequeued	Total number of packets dequeued for specified scheduler (INPUT/CPU Scheduler).
Packets Dropped	Total number of packets dropped for the specified scheduler (INPUT/CPU Scheduler) due to queue overflow.

6.6.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the Router model. All scenarios are located in the directory QUALNET_HOME/scenarios/developer/router-model. Table 6-33 lists the sub-directory where each scenario is located.

TABLE 6-33.   Router Model Scenarios Included in QualNet

Scenario	Description
central	Shows the functionality of router backplane throughput with complex scenario.
central-normal	Shows the functionality of router backplane throughput.
distributed	Shows the functionality of router backplane throughput with backplane type as distributed.
routeripv6	Shows the switch configuration of IPv6.
router-with-subnet1	Shows the router model with wireless subnet.
router-with-subnet2	Shows the router model with subnet.

6.6.7 References

1. Portable Product Sheet - Router Performance. Last Updated: March 31, 2004.

2. Quick Reference Guide: Cisco Access Routers, Spring 2003 V.1.

3. RFC 879,"The TCP Maximum Segment Size and Related Topics." J.Postel. November 1983.

7 Quality of Service (QOS) Models

This chapter describes features, configuration requirements and parameters, statistics, and scenarios for QOS Models, and consists of the following sections:

- Differentiated Services (DiffServ)
- Multi-Protocol Label Switching (MPLS)
- Quality of Service Extensions to OSPF (QOSPF)

7.1 Differentiated Services (DiffServ)

The QualNet DiffServ Model is based on the RFC 2475 and RCF 2474.

7.1.1 Description

DiffServ is an architecture for deploying IP QoS (Quality of Service), where QoS is a set of service requirements (e.g., bandwidth, link delay) to be met by the network during transmission of traffic. This architecture is flexible and allows for either end-to-end QoS or intra-domain QoS by implementing complex classification and mapping functions at the network boundary or access points. Within the DiffServ network, packet behavior is regulated by classification and mapping.

When it enters the network, flow of traffic is classified and assigned a PHB (Per-Hop Behavior) based on that classification. PHB is the externally observable forwarding treatment that packets with the same DiffServ Code Point (DSCP) receive from a network node. The contents of the DSCP are the six most significant bits in the IP header Type of Service field. Within the IP packet, the DSCP tells how the packet should be treated at each network node. Additionally, the mapping of DSCP to PHB is configurable, and DSCP may be re-marked as it passes into a DiffServ network. Re-marking of DSCP allows for the variable treatment of packets based on network specifications or desired levels of service.

Within PHB, there are two standard groups: Assured Forwarding (AF) and Expedited Forwarding (EF). Within AF, the group is further divided into four independent classes with three drop precedence levels. AF offers different levels of forwarding resources in each DiffServ node. In the case of network congestion, the relative importance of the packet determines its drop precedence among other packets in its AF class. EF, on the other hand, known as "Premium" service, gives the best service your network can offer. EF is defined as a forwarding treatment where the rate of packet flow from any DiffServ node is whatever rate ensures highest priority and no packet loss for in-profile traffic.

7.1.2 Features and Assumptions

This section describes the implemented features, omitted features, assumptions and limitations of the DiffServ model.

7.1.2.1 Implemented Features

- Packet Classifier: supports both BA (Behavior Aggregate) classifier and MF (Multi-Field) classifier.
  - Traffic Conditioner: Supports the following algorithms,
  - Token Bucket.
  - Single Rate Three Color Marker with Color Aware.
  - Two Rate Three Color Marker with Color Aware.
  - Time Sliding Window Two Color Meter.
  - Time Sliding Window Three Color Meter.
- Scheduler (DiffServ Scheduler).
- Topology: Supports Diffserv-Diffserv and Diffserv-Non Diffserv topologies.
- Per-Hop Behavior: Three types of Per-Hop Behavior are supported.
  - AF
  - EF
  - BE
- Meter: QualNet supports five types of meters

- Token Bucket.
- Single Rate Three Color Meter with color aware.
- Two Rate Three Color Meter with color aware.
- Time Sliding Window Two Color Meter.
- Time Sliding Window Three Color Meter.
- Marker/Re-Marker
- Queue: Following IP queue types are supported
  - First In, First Out (FIFO)
  - Random Early Detection(Drop) (RED)
  - Random Early Detection(Drop) with In/Out Bit (RIO)
  - Weighted Random Early Detection(Drop) (WRED)
  - Generalized RIO (G-RIO)
- IP protocol
  - IPv4
  - IPv6
  - DUAL-IP
- Dropper: Absolute/Algorithmic.

7.1.2.2 Omitted Features
- Head Dropper and Random Dropper.
- Class-Selector PHBs.
- Differentiated services by multicast traffic.

7.1.2.3 Assumptions and Limitations
- Diffserv applies only on unicast packets.
- In each output interface Diffserv takes the Scheduler as the combination of Outer (Main) and Inner (Second) Scheduler. It uses strict priority as Outer and WFQ/WRR as Inner Scheduler.

7.1.3 Command Line Configuration

To select DiffServ as the IP scheduler, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] IP-QUEUE-SCHEDULER DIFFSERV-ENABLED
```

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of <Qualifier> for each scope.

DiffServ General Parameters

Table 7-1 lists the DiffServ configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 7-1.   DiffServ General Parameters

Parameter	Value	Description
`DS-SECOND-SCHEDULER` *Required* *Scope:* All	String: • `WEIGHTED-FAIR` • `WEIGHTED-ROUND-ROBIN`	Type of scheduler to use as the inner scheduler. DiffServ is a combination of two schedulers: inner and outer schedulers. Both schedulers are required for DiffServ. Generally, Strict Priority is chosen as the outer scheduler and Weighted Fair Queue (WFQ) or Weighted Round Robin (WRR) is chosen as the inner scheduler.
`DIFFSERV-ENABLE-EDGE-ROUTER` *Optional* *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Specifies whether this node is a DiffServ-enabled edge router or not. If the value of this parameter is `YES`, then this router is DS capable edge router. By default any DS capable router is an interior router.
`IP-QUEUE-NUM-PRIORITIES` *Required* *Scope:* All	Integer *Range:* `[1, 256]`	Specifies the total number of queues associated with the inner and outer schedulers.
`TRAFFIC-CONDITIONER-FILE` *Required* *Scope:* Global, Node	Filename	Name of the Diffserv Traffic conditioner file. The traffic conditioner file characterizes classes of traffic, desired data rate and burstiness characteristics, and action to take with Out-Profile packets. The format of the DiffServ traffic conditioner file is described in Section 7.1.3.1.
`PER-HOP-BEHAVIOR-FILE` *Optional* *Scope:* Global, Node	Filename	Specifies the name of the per-hop behavior file. By default there is mapping between queue and DSCP traffic flow into QualNet DiffServ. Per Hop Behavior (PHB) is implemented as a configuration file. It is used for DS to Priority Mapping to specify in which queue the packets are inserted. The format of the per-hop behavior file is described in Section 7.1.3.2.
`DIFFSERV-EDGE-ROUTER-STATISTICS` *Optional* *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Specifies if the DiffServ related statistics are to be output.

7.1.3.1 Format of the Traffic Conditioner File

For the DiffServ model, a traffic conditioner file needs to be configured. The DiffServ Multi-Field Traffic Conditioner is composed of four parts:

- Traffic Classifier specification
- Traffic Meter specification

- Traffic Conditioner specification
- Traffic service specification

Traffic Classifier specifications assign IP packets to appropriate traffic classes. Traffic Conditioner, Traffic Meter, and Traffic Service specifications indicate how packets from each traffic class are treated.

> **Note:** For each traffic class defined by a Traffic Classifier specification, there should be at least one corresponding Traffic Conditioner, Traffic Meter, or Traffic Service specification.

A Traffic Classifier specification has the following format:

```
TRAFFIC-CLASSIFIER <Source Address> <Destination Address> <DSCP value>
                   <protocol-id> <Source Port> <Destination Port>
                   <incoming interface> <Condition Class>
```

> **Note:** All parameters must be entered on the same line.

The Traffic Classifier parameters are described below.

`<Source Address>`	Node ID or IP address of the packet source.
`<Destination Address>`	IP address of the packet destination.
`<DSCP value>`	Value of the DiffServ bits in the IP header.
`<protocol-id>`	Value of the protocol field in the IP header.
`<Source Port>`	Source port field of the IP header.
`<Destination Port>`	Destination port field of the IP header.
`<incoming interface>`	IP address of the interface on which this packet was received, if applicable.
`<Condition Class>`	A unique positive integer that describes this class of traffic.

A Traffic Meter specification defines the allowed range of bandwidth usage and burstiness characteristics for packets in a traffic class. Packets within this allowed range are 'In-Profile', while the remaining packets are either 'Part-Profile' or 'Out-Profile' depending on the Meter used ("srTCM", "trTCM", "TSW3CM"), and is subject to the Traffic Conditioner, which can mark or drop them.

A Traffic Meter specification has the following format:

```
TRAFFIC-METER <Condition Class> TokenBucket <rate>
              <committed-burst-size>
```
or
```
TRAFFIC-METER <Condition Class> srTCM <rate> <committed-burst-size>
              <excess-burst-size> <color-aware>
```
or
```
TRAFFIC-METER <Condition Class> trTCM <rate> <committed-burst-size>
              <peak-information-rate> <excess-burst-size>
```
or
```
TRAFFIC-METER <Condition Class> TSW2CM <rate>
```
or
```
TRAFFIC-METER <Condition Class> TSW3CM <rate> <peak-information-rate>
```

Note: All parameters must be entered on the same line.

The Traffic Meter parameters are described below.

`<Condition Class>`	Identifier for the class of traffic.
	This should be the same as the `<Condition Class>` parameter of one of the Traffic Class specifications.
`<rate>`	Data rate, in bps, of In-Profile packets.
`<committed-burst-size>`	Size of largest burst (in bytes) that can be accepted as In-Profile, if the meter type is `TokenBucket`, `srTCM`, or `trTCM`.
`<peak-information-rate>`	Peak information rate (in bps) if the meter type is `TSW3CM` or `trTCM`.
`<excess-burst-size>`	Size of largest burst (in bytes) that can be accepted as Part-Profile, if the meter type is `srTCM` or `trTCM`.
`<color-aware>`	Specifies whether or not the Traffic Meter is color aware, if the meter type is `srTCM`. This argument can be `YES` or `NO`.

Traffic Conditioner specifications indicate the action to be taken, when packets are determined to be Out-Profile.

A Traffic Conditioner specification has the following format:

```
TRAFFIC-CONDITIONER <Condition Class> DROP
```
or
```
TRAFFIC-CONDITIONER <Condition Class> MARK <DSCP value>
```

The Traffic Conditioner parameters are described below.

<Condition Class>   Identifier for the class of traffic.

                             This should be the same as the <Condition Class>
                             parameter of one of the Traffic Class specifications.

<DSCP value>   New value to assign to the description field in the IP header of
                             Out-Profile packets, if the Traffic Conditioner specifies that the
                             packets are to be marked.

A Traffic Service specification assigns a Per-Hop Behavior (PHB) for any particular traffic flow. A PHB is
the externally observable forwarding behavior of a DS node applied to a particular DS behavior aggregate.

A Traffic Service specification has the following format:

        TRAFFIC-SERVICE <Condition Class> <Service Class>

The Traffic Service parameters are described below.

<Condition Class>   Identifier for the class of traffic.

                     This should be the same as the <Condition Class> parameter of
                     one of the Traffic Class specifications.

<Service Class>   Type of PHB Service.

                     This argument can be one of the following: EF, AF1, AF2, AF3, or AF4. -

                     where,

                     EF (Expedited Forwarding) PHB defines a low latency, low-jitter and
                     low-loss behavior that a Diffserv node may implement.

                     AF (Assured Forwarding) family of PHB groups defines four different
                     levels of forwarding guarantee that a Diffserv node may support.

                     AF1 >= AF2 >= AF3 >= AF4 in terms of low delay

                     AF4 >= AF3 >= AF2 >= AF1 in terms of high throughput.

                     AF1/AF2 is associated with delay sensitive low volume applications
                     such as voice, telnet, and so on, while AF3, AF4 is associated with
                     throughput sensitive applications like FTP, HTTP, and so on.

Example of Traffic Conditioner File

The following is an example traffic conditioner file.

```
TRAFFIC-CLASSIFIER 1 6 46 ANY ANY ANY ANY  1
TRAFFIC-CLASSIFIER 2 6 10 ANY ANY ANY ANY  2
TRAFFIC-CLASSIFIER 2 6 12 ANY ANY ANY ANY  2
TRAFFIC-CLASSIFIER 2 6 14 ANY ANY ANY ANY  2

TRAFFIC-METER 1 TokenBucket 1000000 2000
TRAFFIC-METER 2 srTCM 4000000 2000 6000 NO

TRAFFIC-CONDITIONER 1 DROP

TRAFFIC-SERVICE 1 AF1
TRAFFIC-SERVICE 2 AF1
```

7.1.3.2 Format of the Per-Hop Behavior File

The per-hop behavior file is used by DiffServ for priority mapping. It specifies the queues in which packets are inserted.

Each line in the per-hop behavior file has one of the following formats:

```
DS-TO-PRIORITY-MAP <DS-field> <Priority>
```
or
```
DEFAULT-DS-TO-PRIORITY-MAP <Default-priority>
```
where

`<DS-field>`	Differentiated services field of the IP header of the packet.
`<Priority>`	Priority of the queue in which the packet should be inserted.
`<Default-priority>`	Priority of the queue in which the packet should be inserted for the default case (i.e., best-effort service).

Example of Per-hop Behavior File

The following is an example per-hop behavior file.

```
DS-TO-PRIORITY-MAP 10 0
DS-TO-PRIORITY-MAP 12 0
DS-TO-PRIORITY-MAP 14 0

DEFAULT-DS-TO-PRIORITY-MAP 2
```

7.1.4 GUI Configuration

This section describes how to configure DiffServ in the GUI.

Configuring DiffServ Parameters

To configure the DiffServ parameters, perform the following steps:

1. Go to **Default Device Properties Editor > Network Layer > Scheduler and Queues**.

2. Set **IP Output Queue Scheduler** to *DiffServ* and set the dependent parameters listed in Table 7-2.
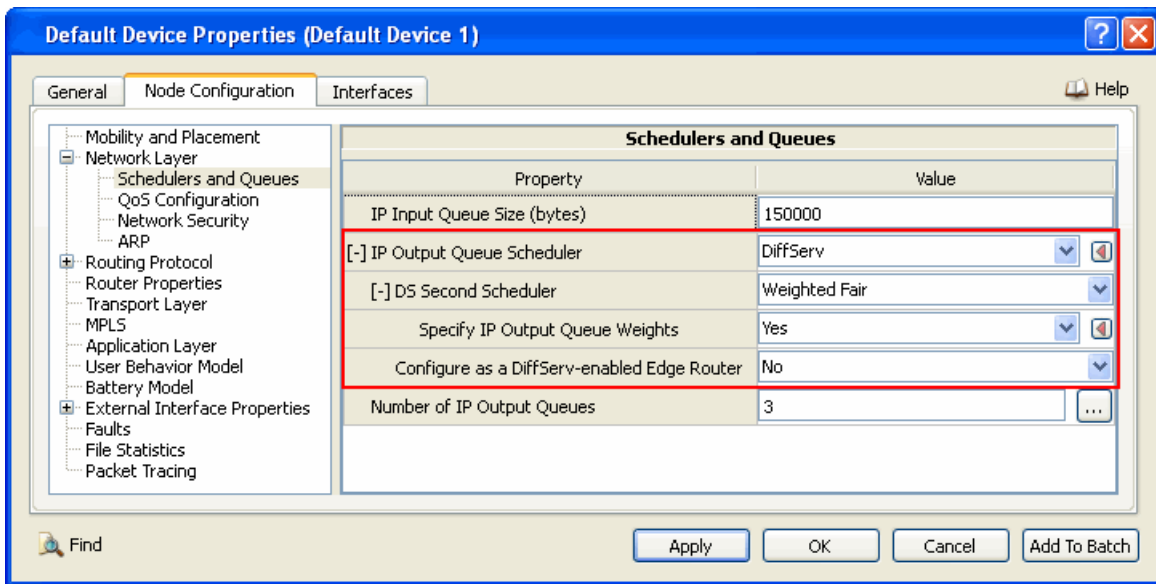
FIGURE 7-1.   Setting DiffServ Parameters

TABLE 7-2.   Command Line Equivalent of DiffServ Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
DS Second Scheduler	Node	DS-SECOND-SCHEDULER
Specify IP Output Queue Weights	Node	N/A
Configure as a DiffServ-enabled Edge Router	Node	DIFFSERV-ENABLE-EDGE-ROUTER

Setting Parameters

- To specify IP Output Queue Weights, Set **Specify IP Output Queue Weights** to *Yes*; otherwise, set **Specify IP Output Queue Weights** to *No*.

- To configure DiffServ-enabled Edge Router, set **Configure as a DiffServ-enabled Edge Router** to *Yes*; otherwise, set **Configure as a DiffServ-enabled Edge Router** to *No*.

3. If **Specify IP Output Queue Weights** is set to *Yes*, then configure the queue weights as follows:

   a. Set **Number of IP Output Queues** to the desired value.

   b. Click on the **Open Array Editor** ⬚ button in the **Value** column. This opens the Array Editor.

   c. In the left panel of the Array Editor, select the index of the queue to be configured. In the right panel, set the queue weight parameters listed in Table 7-3 and the other parameters for the queue.
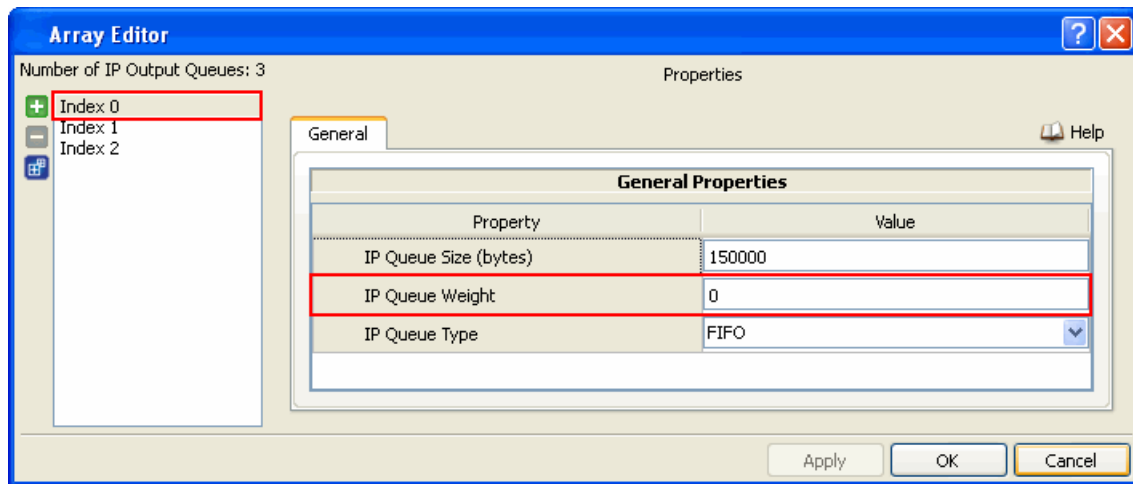
FIGURE 7-2.   Setting Queue Weight Parameters

TABLE 7-3.   Command Line Equivalent of Queue Weight Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
IP Queue Weight	Node, Subnet, Interface	QUEUE-WEIGHT

4. If **Configure as a DiffServ-enabled Edge Router** is set to *Yes*, set the dependent parameter listed in Table 7-4.
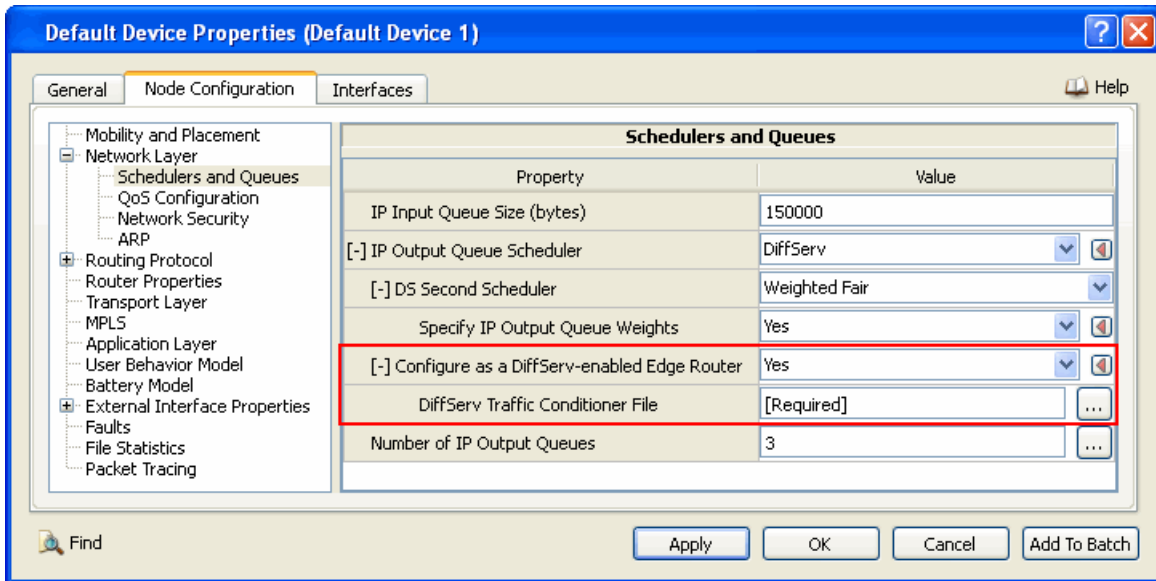
FIGURE 7-3.   Setting DiffServ-enabled Edge Router Parameters

TABLE 7-4.   Command Line Equivalent of DiffServ Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
DiffServ Traffic Conditioner File	Node	`TRAFFIC-CONDITIONER-FILE`

Configuring QoS Parameters

To configure QoS parameters, perform the following steps:

1. Go to Default Device Properties Editor **>** Network Layer **>** QoS.

2. Set the parameters listed in Table 7-5.
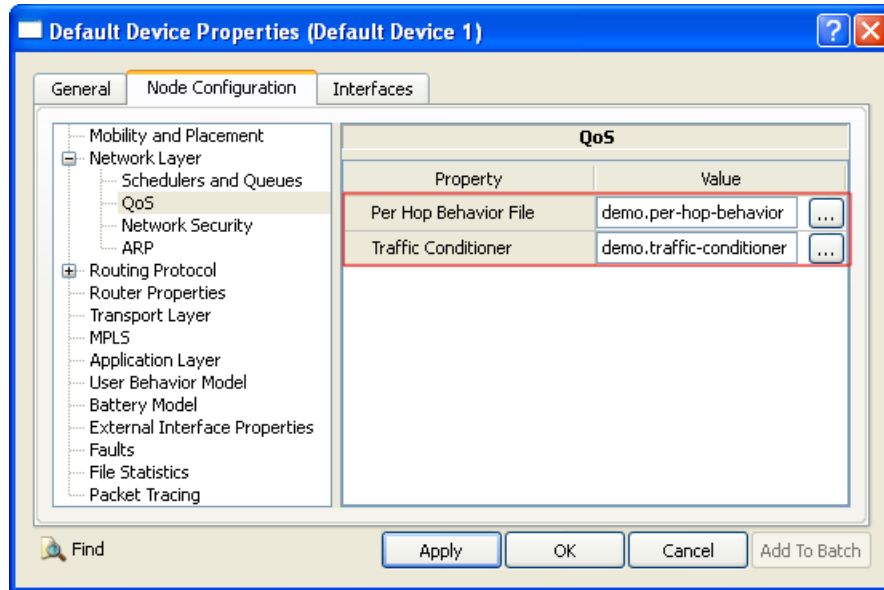
FIGURE 7-4.   Setting QoS Parameters

TABLE 7-5.   Command Line Equivalent of DiffServ Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Per Hop Behavior File	Node	`PER-HOP-BEHAVIOR-FILE`
Traffic Conditioner	Node	`TRAFFIC-CONDITIONER-FILE`

Setting Parameters

- Set **Per Hop Behavior File** to the name of the Per Hop Behavior file. The format of the Per Hop Behavior file is described in Section 7.1.3.2.

- Set **Traffic Conditioner** to the name of the Traffic Conditioner file. The format of the Traffic Conditioner file is described in Section 7.1.3.1.

Configuring Statistics Parameters

Statistics for DiffServ can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for DiffServ, check the box labeled **DiffServ** in the appropriate properties editor.

TABLE 7-6.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
DiffServ	Global, Node	DIFFSERV-EDGE-ROUTER-STATISTICS

7.1.5 Statistics

Table 7-7 shows the statistics for each traffic conditioner at each edge node that are output to the statistics (.stat) file at the end of simulation:

TABLE 7-7.   DiffServ Statistics

Statistic	Description
Incoming Packets	Number of incoming packets of each class at each DS capable edge router.
Conforming Packets	Number of packets of each class conforming by meter at each DS capable edge router.
Dropped Packets	Number of packets of each class dropped by meter at each DS capable edge router.
Partially Conforming Packets	Number of packets of each class that are partially conforming by meter at each DS capable edge router.
Non-Conforming Packets	Number of packets of each class that are non-conforming by meter at each DS capable edge router.
Remarked Packets	Number of packets of each class that are remarked by meter at each DS capable edge router.

7.1.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the DiffServ model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/diffserv. Table 7-8 lists the sub-directory where each scenario is located.

TABLE 7-8.   DiffServ Scenarios Included in QualNet

Scenario	Description
ipv4/diff-diff-topology	Shows the overall behavior of DiffServ-DiffServ Topology for 6 nodes.
ipv4/diff-nondiff-topology	Shows the overall behavior of DiffServ-Non DiffServ Topology for 12 nodes.
ipv4/srtcm-coloraware	Shows the Single Rate Three Color Meter & Marker (Color Aware) for 6 nodes.
ipv4/srtcm-meter	Shows the Single Rate Three Color Meter & Marker (Color Blind) for 6 nodes.
ipv4/token-meter	Shows Token Bucket Meter & Marker for 6 nodes.
ipv4/trtcm-coloraware	Shows Two Rate Three Color Meter & Marker (Color Aware) for 6 nodes.
ipv4/trtcm-meter	Shows Two Rate Three Color Meter & Marker (Color Blind) for 6 nodes.

TABLE 7-8.   DiffServ Scenarios Included in QualNet (Continued)

Scenario	Description
ipv4/tsw2cm-meter	Shows Time Sliding Window Two Color Meter & Marker for 6 nodes.
ipv4/tsw3cm-meter	Shows Time Sliding Window Three Color Meter & Marker for 6 nodes.
ipv4/wfq-schd-service	Shows Service Differentiation among the Three Service Classes with WFQ as inner Scheduler for 6 nodes.
ipv4/wrr-schd-service	Shows Service Differentiation among the Three Service Classes with WRR as inner Scheduler for 6 nodes.
ipv6/diff-diff-topology	Shows the overall behavior of DiffServ-DiffServ Topology for 6 nodes.
ipv6/Srtcm-meter	Shows the Single Rate Three Color Meter & Marker (Color Blind) for 6 nodes.

7.1.7 References

1. RFC 2475, "An Architecture for Differentiated Services." S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss. December 1998.

2. RFC 2474, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers." K. Nichols, S. Blake, F. Baker, D. Black. December 1998.

3. RFC 2597, "Assured Forwarding PHB Group." J. Heinanen, F. Baker, W. Weiss, J. Wroclawski. June 1999.

4. RFC 2598, "An Expedited Forwarding PHB." V. Jacobson, K. Nichols, K. Poduri. June 1999.

5. RFC 2836, "Per Hop Behavior Identification Codes." S. Brim, B. Carpenter, F. Le Faucheur. May 2000.

6. draft-ietf-diffserv-phbid-00, "Per Hop Behavior Identification Codes." S. Brim, B. Carpenter, F. Le Faucheur. October 1999.

··

7.2 Multi-Protocol Label Switching (MPLS)

The QualNet MPLS model is based on the following documents:

- RFC 3031
- RFC 3036
- RFC 3209

7.2.1 Description

MPLS support in QualNet is composed of a label-swapping framework between the Network Layer (IP) and MAC Layer, which interacts with a label distribution protocol, generally at the Application or Transport Layers. At the ingress points to an MPLS network (cloud), IP packets are assigned a Forwarding Equivalence Class (FEC) and a corresponding fixed-length label. As the packet travels through the MPLS cloud, the label is used to make forwarding decisions. At the egress point, the last label is stripped off, and IP forwarding continues outside the cloud, or up the network stack if the destination is within the cloud. MPLS is useful for traffic engineering in a differentiated services network, being able to use ingress information in the label assigning, and being able to use those labels to create delay and bandwidth guaranteed paths through the cloud.

> **Note:** It can also be simpler to implement the switches inside an MPLS cloud, because they only need to be capable of performing label lookup and replacement.

In normal connectionless model of IP protocol, packets travel from one router to next, and each router makes an independent forwarding decision for that packet. That is, each router analyzes the packet's header, and each router runs a network layer routing algorithm. Each router independently chooses a next hop for the packet, based on its analysis of the packet's header and the results of running the routing algorithm.

Packet headers contain considerably more information than is needed simply to choose the next hop. Choosing the next hop can therefore be thought of as the composition of two functions. The first function partitions the packets into a set of "Forwarding Equivalence Classes" (FECs). The second function maps each FEC into a next hop. In so far as the forwarding decision is concerned, different packets, which get mapped into the same FEC, are indistinguishable. All packets, which belong to a particular FEC and travel from a particular node, will follow the same path (or if certain kinds of multi-path routing are in use, they will all follow one of a set of paths associated with the FEC).

In conventional IP forwarding, a particular router will typically consider two packets to be in the same FEC if there is some address prefix X in that router's routing tables such that X is the "longest match" for each packet's destination address. As the packet traverses the network, each hop in turn re-examines the packet's header and assigns it to an FEC.

In MPLS, the assignment of a particular packet to a particular FEC is done just once, as the packet enters the network. The FEC to which the packet is assigned is encoded as a short fixed length value known as a "label". When a packet is forwarded to its next hop, the label is sent along with it. That is, the packets are "labeled" before they are forwarded to the next hop. At all subsequent hops, there is no further analysis of the packet's network layer header, only the label is used as an index into a table which specifies its next hop, and a new label. So the data forwarding becomes very fast due to just switching instead of making decision at each router.

In the MPLS forwarding paradigm, once a packet is assigned to an FEC, subsequent routers do no further header analysis; all forwarding in the subsequent routers are driven by the labels. This has a number of advantages over conventional network layer forwarding.

7.2.1.1 Label Distribution Methods

The MPLS architecture does not assume a single label distribution protocol. In fact, a number of different label distribution protocols are being standardized. Existing protocols have been extended so that label distribution can be piggybacked on them. New protocols have also been defined for the explicit purpose of distributing labels. There are several label distribution methods in use, such as Label Distribution Protocol (LDP) and Resource Reservation Protocol - Traffic Engineering extension (RSVP-TE).

7.2.1.2 Label Distribution Protocol (LDP)

The routers capable of forwarding and switching packets on the basis of labels only, are known as Label Switched Routers (LSR) as described in RFC 3031. Two LSRs, which use LDP to exchange FEC to label mapping information, are known as "LDP Peers". When two LSRs are set to FEC to label mapping information, there exists an "LDP Session" between them. A single LDP session allows each peer to learn the other's label mappings; i.e., the protocol is bi-directional. Two LDP peer can directly communicate between them, and can establish an LDP session. LDP peers follow a set of procedures to establish a Label Switched Path (LSP) among them.

LDP handles the assignment of labels to Forward Equivalent Classes (FECs) and the distribution of those labels to routers within the MPLS cloud. LDP allows label switched routers (LSRs) to exchange messages through UDP and TCP.

LDP protocol works as an application in the application layer, and comes to an "agreement" about the use of a "label" for forwarding and switching use. This "label information" can be passed down below to the MAC layer. This "label" is used by "kernel" of MPLS that does switching /forwarding of packets.

7.2.1.3 Resource Reservation Protocol - Traffic Engineering (RSVP-TE)

The Resource Reservation Protocol (RSVP) is a network-control protocol that enables Internet applications to obtain differing qualities of service (QoS) for their data flows. RFC 3209 describes RSVP-TE as traffic-engineering extensions to RSVP that allow the protocol to create Label Switched Path (LSP) tunnels in MPLS. This LSP creates a tunnel between ingress and egress nodes, which is used in Traffic Engineering (TE) in MPLS. Traffic Engineering is concerned with performance optimization and facilitates reliable and efficient network operation by considering the resource utilization throughout the path.

When a LSP is established between two MPLS nodes, packets can be delivered through this LSP tunnel without considering the IP layer routing technique. If a set of packets is assigned the same label by a specific node, then they form a Forwarding Equivalent Class (FEC). The FEC packets are then sent through the LSP tunnel and the router can identify the reservation states for a packet based on the current label value. When an ingress node receives a data packet to forward to a specific destination, it first requests an RSVP Path message to bind labels to create a LSP tunnel with the destination node. An RSVP Resv message is initiated by the receiver of the packet and propagated upstream towards the sender of the packet. The request for resources is done by the receivers using the Resv message and it thereby distributes the label

.

> **Note:**   Creation of RSVP-TE sessions is supported only by the Constant Bit Rate (CBR) application. Both the client and the server of the CBR session must lie within the same MPLS backbone.

7.2.1.4 Integrating IP with MPLS Backbone

In high-speed and huge-data-transmission scenarios, where bandwidths as well as time-constraints are critical, normal IP forwarding cannot be considered for fast data delivery. It is desirable to use MPLS network to get the data forwarded to destination in time constrained scenarios, as MPLS only uses switching and no decision making happens inside any of the routers in it (a decision is only made once at

the Ingress router). Hence it becomes a desirable option to use MPLS backbone to forward packets between two very distant IP nodes.

When MPLS is integrated with IP, an IP packet is forwarded through MPLS backbone as default. If the router is not able to transmit the data via MPLS, due to not finding a path to destination, then the packet is forwarded to IP or dropped based on the user configuration for the respective behavior. The ingress node (Label Edge Router) keeps sending these packets via usual the IP forwarding or buffers them in the Ingress Queue until the LSP gets established by LDP in the MPLS backbone. LDP is the label distribution protocol supported for IP-MPLS interconnection.

7.2.2 Features and Assumptions

This section describes the implemented features, omitted features, assumptions and limitations of the MPLS model.

7.2.2.1 Implemented Features

- Assignment of FEC based on destination IP address only for dynamic LDP.
- Assignment of FEC based on destination and priority for static routes for MPLS.
- MPLS SHIM Label encoding.
- Label Operations such as create, add, replace and remove MPLS shim header over network layer header.
- Label distribution control modes (Ordered as well as Independent).
- Ingress and Egress LERs in MPLS inter-connection with IPV4 networks.
- Supported dynamic label distribution protocols are LDP and RSVP-TE.
- Static routes for MPLS.
- Loop Control inside MPLS network.
- Label retention mode (conservative and liberal).
- Identification of Ingress and Egress LERs to distinguish between the IPv4 network and MPLS backbone.
- Support multiple MPLS domains which are not contiguous.
- Precedence option in Type of Service (TOS) of IP in MPLS.
- Directed broadcast packets for an IP subnet.
- Forwarding the packets to IP or dropping it at a LSR, when outgoing MTU is less or there is an Invalid Label, is a configurable option.
- Fragmenting a packet by IP to be sent through MPLS at Ingress, if required.
- Longest prefix match for static MPLS.
- Network ID for creating FTN entries in static MPLS.
- Packets arriving with IP `Source Routing' option as true will be forwarded through IP.

7.2.2.2 Omitted Features

- Label Stacks of depth two or more.
- Fragmentation support inside MPLS Backbone.
- MPLS over switches.
- Explicit Routing by LDP.
- Interconnection of IPv6 network with MPLS network.
- Default gateway of IP forwarding table.
- Support for MPLS Tunnel.

- Penultimate-hop-popping (PHP).
- IPv6 or IPv4 tunnels.
- Checking the number of hops inside the MPLS backbone at Ingress LER.
- Support for DiffServ.
- Support for IP Multicast.
- UNSOLICITED label advertisement mode.

7.2.2.3 Assumptions and Limitations

- MPLS will support packets of size less than or equal to: "Network outgoing interface MTU - 4 bytes (of MPLS SHIM) - 8 bytes (of LLC header)".
- Lower layers (MAC) will send signal on fault detection to MPLS.
- LLC is enabled to support MPLS and all MAC protocols.

7.2.3 Command Line Configuration

To enable MPLS, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] MPLS-PROTOCOL        YESSection 1.2.1.1
```

The scope of this parameter declaration can be Global, Node, Subnet, or Interface. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

> **Notes: 1.** The default value of parameter `MPLS-PROTOCOL` is `NO`.
>
> **2.** If a node that is inside an MPLS-enabled subnet needs to interact with another MPLS-enabled node that is outside the subnet, then MPLS needs to be enabled for the node at the node level also, so that all interfaces of the node in the subnet are MPLS-enabled.

Section 7.2.3.1 describes the general parameters to configure MDLP. Section 7.2.3.1 describes the parameters to configure LDP. Section 7.2.3.1 describes the parameters to configure RSVP-TE. See Section 1.2.1.3 for a description of the format used for the parameter tables.

7.2.3.1 General Configuration

Table 7-9 describes the general MPLS configuration parameters.

TABLE 7-9.   General MPLS Parameters

Parameter	Value	Description
`MPLS-EDGE-ROUTER` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Sets an MPLS node as an edge router.
`MPLS-ROUTE-TO-IP-ON-ERROR` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Allows configuring MPLS behavior on error, that is, whether to forward the packet to IP or drop it.

TABLE 7-9.   General MPLS Parameters (Continued)

Parameter	Value	Description

`MPLS-LABEL-DISTRIBUTION-`
`PROTOCOL`
 	
Optional
 	
Scope: All
	List:
	• `LDP`
	• `RSVP-TE`
	
	Default: `LDP`
		Enables LDP or RSVP-TE as the label distribution protocol. If it is omitted for a node, no label distribution protocol is enabled at the node.
		
		If `LDP` is specified as the label distribution protocol, set the `LDP` parameters described in Section 7.2.3.2.
		
		If `RSVP-TE` is specified as the label distribution protocol, set the `RSVP-TE` parameters described in Section 7.2.3.3.

`MPLS-STATIC-ROUTE-FILE` Optional *Scope:* All	Filename	Specifies the name of the static label assignment file. The extension of this file is usually ".mpls-routes". The format of the static label assignment file is described in Section 7.2.3.4.
`MPLS-STATISTICS` Optional *Scope:* All	List: • `YES` • `NO` *Default:* `NO`	Enables the MPLS statistics.

7.2.3.2 Configuring LDP

If LDP is specified as the MPLS label distribution protocol, then LDP parameters described in Table 7-10 also need to be set.

TABLE 7-10.   LDP Parameters

Parameter	Value	Description

`MPLS-LABEL-DISTRIBUTION-`
`CONTROL-MODE`
 	
Optional
 	
Scope: Global, Node
	List:
	• `INDEPENDENT`
	• `ORDERED`
	
	Default: `ORDERED`
		Describes whether or not an LSR can advertise labels whenever it requires (`INDEPENDENT`), or only when it has a label mapping for the next hop, or it is the egress point from the MPLS cloud (`ORDERED`).

`MPLS-LDP-LABEL-`
`ADVERTISEMENT-MODE`
 	
Optional
 	
Scope: Global, Node
	List:
	• `ON-DEMAND`
	• `UNSOLICITED`
	
	Default: `ON-`
	`DEMAND`
		Describes which LSR is responsible for advertising labels. In `UNSOLICITED` mode, the downstream LSR is responsible for advertising a label mapping when it wants an upstream LSR to use the label. In `ON-DEMAND` mode, the upstream LSR is responsible for requesting label mappings.

`MPLS-LABEL-RETENTION-MODE` Optional *Scope:* Global, Node	List: • `LIBERAL` • `CONSERVATIVE` *Default:* `LIBERAL`	Describes whether or not labels received from LSRs that are not the next hop for a given FEC are kept. In `CONSERVATIVE` mode, only those labels that are used to forward packets are kept. In `LIBERAL` mode, all labels are kept. The `LIBERAL` mode incurs more overhead in keeping and maintaining labels that are not currently in use, but may respond more quickly to changes.

TABLE 7-10.   LDP Parameters (Continued)

Parameter	Value	Description
`CONFIGURED-FOR-LABEL-RELEASE-MESSAGE-PROPAGATE` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Describes whether or not the LSR is configured to propagate label release messages.
`MPLS-LDP-LOOP-DETECTION` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Describes whether or not the LSR performs the optional loop detection mechanism to prevent Label Request messages from looping.
`MPLS-LDP-PATH-VECTOR-LIMIT` Optional *Scope:* Global, Node	Integer *Range:* `> 0` *Default:* `64`	If the parameter `MPLS-LDP-LOOP-DETECTION` is enabled then this parameter sets the path vector limit.
`MPLS-MEMBER-OF-DECREMENT-TTL-DOMAIN` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Specifies whether or not LSR belongs to member of TTL decrementing domain.
`SUPPORT-LABEL-MERGING` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Specifies whether or not LSR will support label merging.
`MAX-ALLOWABLE-HOP-COUNT` Optional *Scope:* Global, Node	Integer *Range:* $\geq$ `0` *Default:* `64`	Configures the maximum allowable hop count value.
`MPLS-LDP-MAX-PDU-LENGTH` Optional *Scope:* Global, Node	Integer *Range:* `> 256` *Default:* `4096`	Specifies the maximum PDU length.
`MPLS-LDP-DECREMENTS-TTL` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Specifies whether ttl should be decremented.

TABLE 7-10.   LDP Parameters (Continued)

Parameter	Value	Description
`MPLS-LDP-STATISTICS` Optional *Scope:* Global, Node	List: ● `YES` ● `NO` *Default:* `NO`	Specifies whether statistics should be collected for LDP.
`HOP-COUNT-REQUIRED-IN-LABEL-REQUEST` Optional *Scope:* Global, Node	List: ● `YES` ● `NO` *Default:* `NO`	Specifies whether hop count is required in label request or not.

7.2.3.3 Configuring RSVP-TE

If RSVP-TE is specified as the MPLS label distribution protocol, then the RSVP-TE parameters described in Table 7-11 also need to be set.

TABLE 7-11.   RSVP-TE Parameters

Parameter	Value	Description
`RSVP-TE-RECORD-ROUTE` Optional *Scope:* Global, Node	List: ● `OFF` ● `LABELED` ● `NORMAL` *Default:* `OFF`	Specifies whether or not the total path of the LSP will be recorded along the path of establishing RSVP messages. If set to `OFF`, there will be no recording of the path during LSP creation, and no loop detection. If set to `NORMAL`, the path will be recorded. If set to `LABELED`, the label ID of the RSVP messages will also be considered.
`RSVP-RESERVATION-STYLE` Optional *Scope:* Global, Node	List: ● `FF` ● `SE` ● `FF` ● `SE` ● `WF` *Default:* `FF`	Specifies the reservation style to be used by RSVP-TE. If set to `FF`, then RSVP-TE will use the Fixed Filter reservation style, which creates a distinct reservation for traffic from each sender that is not shared by other senders. If set to `SE`, then RSVP-TE will use the Shared Explicit reservation style, which allows a receiver to explicitly specify the senders to be included in a reservation, and utilize a single reservation on a link for all the senders listed.
`RSVP-TE-EXPLICIT-ROUTE-FILE` Optional *Scope:* Global	Filename	Specifies the name of the explicit route file. This file usually has the extension ".routes-explicit". The format of this file is described in Section 7.2.3.5.
`RSVP-STATISTICS` Optional *Scope:* Global, Node	List: ● `YES` ● `NO` *Default:* `NO`	Specifies whether statistics should be collected for RSVP-TE.

7.2.3.4 Format of the Static Label Assignment File

The static label assignment file contains FEC-To-NHLFE (FTN) maps and Incoming Label Maps (ILMs).

FTN entries map FECs (Forward Equivalence Classes) to NHLFEs (Next Hop Label Forwarding Entry), indicating the outgoing label, or the label to place on IP packets that match the respective FEC (destination IP).

ILM entries apply to the router with the given source IP, and map the incoming label to an outgoing label and the IP address of the next hop.

FTN and ILM entries in the static label assignment file have the following format:

```
FTN <src IP> <dest IP> <outgoing label> <next hop IP>[<priority>]
ILM <src IP> <incoming label> <outgoing label> <next hop IP>
```

where

`<src IP>`	IP address of the source node
`<dest IP>`	IP address of the destination node
`<outgoing label>`	Label to place on the IP packet
`<next hop IP>`	IP address of the next hop node
`<incoming label>`	Label of the incoming packet
`<priority>`	Priority used to classify routes. This parameter is optional.

Notes: 1. For FTN entries, labels 0-15 are reserved, and have special meaning. An outgoing label of 3 represents the implicit NULL label (as described in RFC 3036). This is a label that an LSR may assign and distribute, but which never actually appears in the encapsulation.

2. For ILM entries, an outgoing label of 3 indicates that the incoming packet has reached its final (MPLS cloud) destination. MPLS will then strip off the label, and hand the packet to IP.

Example Static Label Assignment File
The following is an example of a static label assignment file:

```
FTN 1.1 1.2 17 1.2 1
FTN 1.1 2.2 19 1.2 2
FTN 1.2 1.1 18 1.1
FTN 2.1 2.2 19 2.2
FTN 2.2 2.1 20 2.1
FTN 2.2 1.1 18 2.1
ILM 2.1 18 18 1.1
ILM 1.2 19 19 2.2
ILM 1.2 17 3 1.2
ILM 1.1 18 3 1.1
ILM 2.2 19 3 2.2
ILM 2.1 20 3 2.1
```

7.2.3.5 Format of the Explicit Route File

Each line in the explicit route file has the following format:

```
<node-ID> <explicit route>
```
where

    `<node-ID>`   Node identifier

    `<explicit route>` Explicit route specified as a comma-delimited list of node IDs enclosed in "{" and "}".

Example Explicit Route File

The following is an example of an explicit route file:

```
1 {1.2, 2.2, 3.2, 4.2, 5.2, 3.2, 4.2, 5.2, 6.2, 7.2}
```

7.2.4 GUI Configuration

This section describes how to configure MPLS in the GUI.

Section 7.2.4.2 describes how to configure general MPLS parameters. Section 7.2.4.2 describes how to configure LDP parameters. Section 7.2.4.3 describes how to configure RSVP-TE parameters. Section 7.2.4.4 describes how to configure MPLS and LDP statistics parameters.

7.2.4.1 Configuring MPLS Parameters

To configure the MPLS parameters, perform the following steps:

1. Go to **Default Device Properties Editor > Node Configuration > MPLS**.

2. Set **Enable MPLS** to *Yes* and set the dependent parameters listed in Table 7-12.
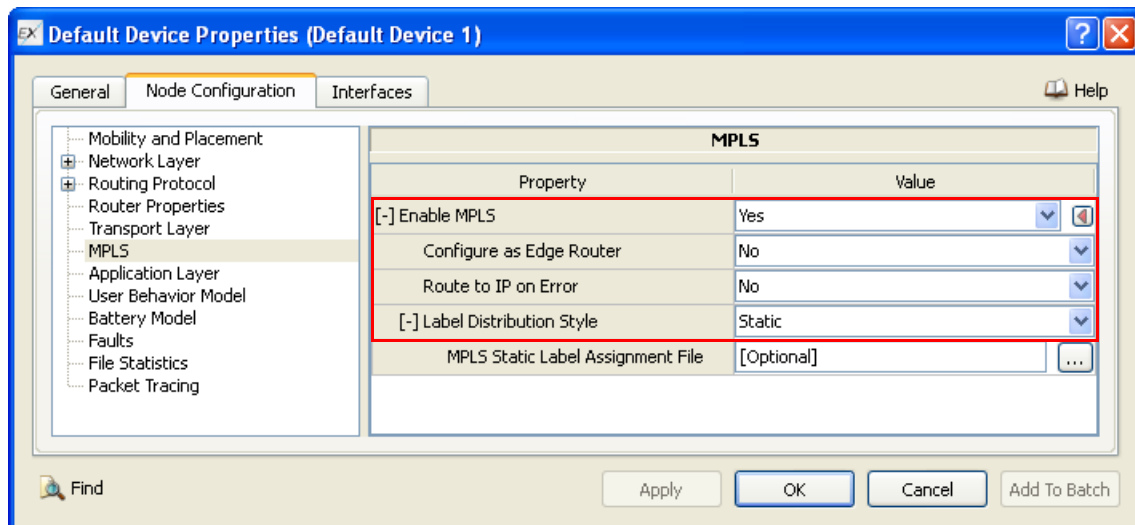
FIGURE 7-5.   Setting MPLS Parameters

TABLE 7-12.   Command Line Equivalent of MPLS Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Configure as Edge Router	Node	`MPLS-EDGE-ROUTER`
Route to IP on Error	Node	`MPLS-ROUTE-TO-IP-ON-ERROR`
Label Distribution Style	Node	`N/A`

Setting Parameters

- To configure a node as Edge Router, set **Configure as Edge Router** to *Yes*; otherwise, set **Configure as Edge Router** to *No*.

- To enable route to IP on error, set **Route to IP on Error** to *Yes*; otherwise, set **Route to IP on Error** to *No*.

- To configure LDP or RSVP-TE, set **Label Distribution Style** to *Dynamic*; otherwise, set **Label Distribution Style** to *Static*.

3. If **Label Distribution Style** is set to *Static*, set the dependent parameters listed in Table 7-13.
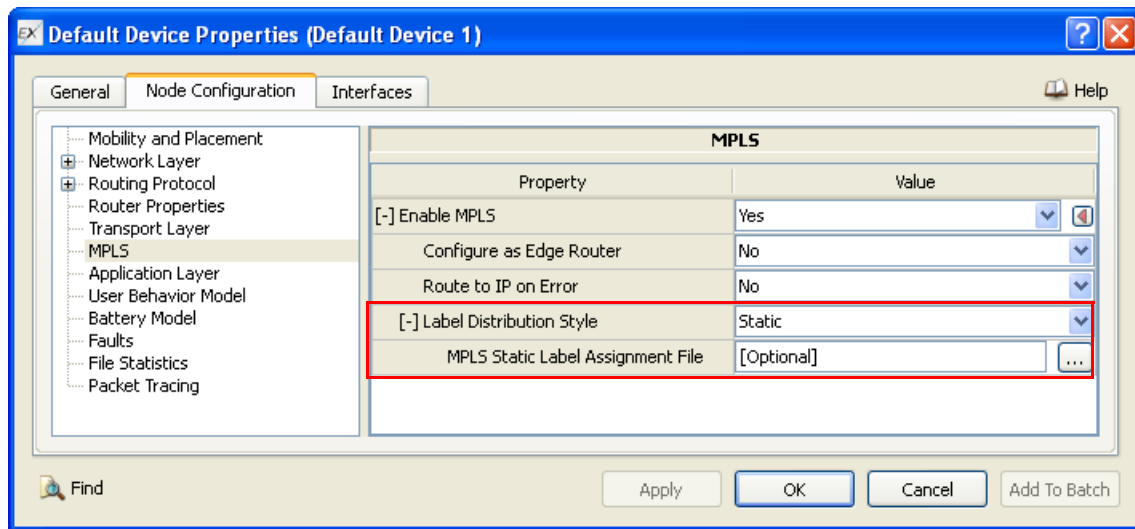
FIGURE 7-6.   Setting MPLS Static Label Assignment File

TABLE 7-13.   Command Line Equivalent of MPLS Static Label Assignment File Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
MPLS Static Label Assignment File	Node	`MPLS-STATIC-ROUTE-FILE`

Setting Parameters

- Set **MPLS Static Label Assignment File** to the name of the MPLS Static Route file. The format of the MPLS Static Route file is described in Section 7.2.3.4.

4. If **Label Distribution Style** is set to *Dynamic*, set the dependent parameters listed in Table 7-14.
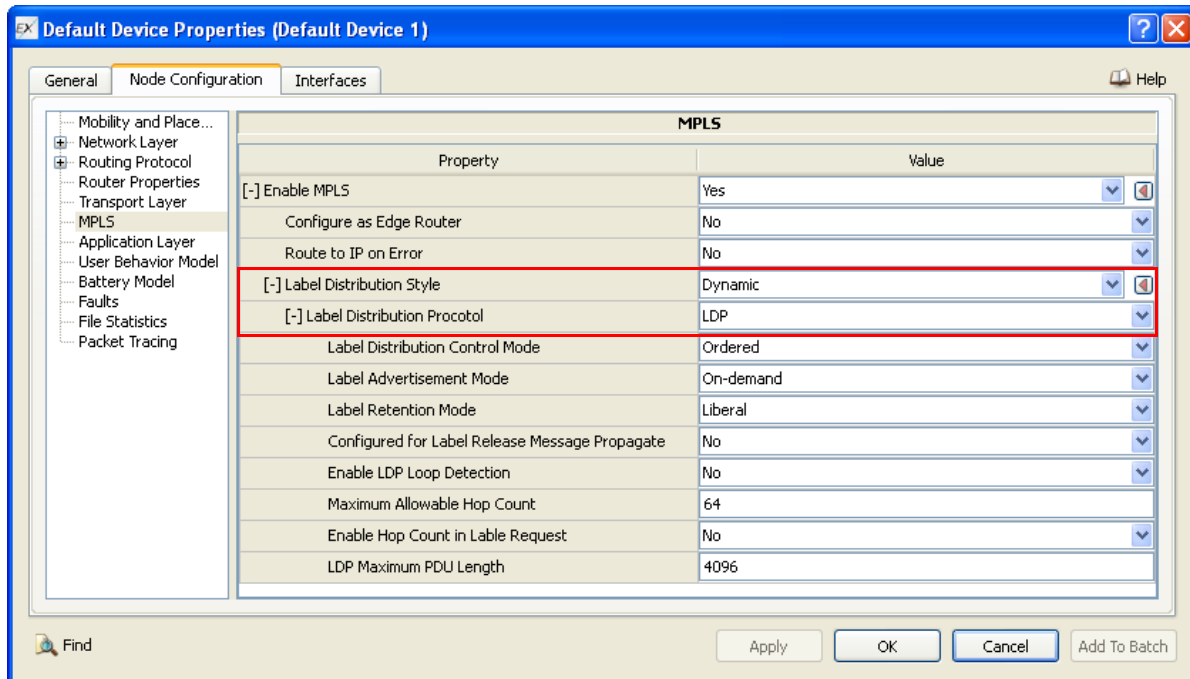
FIGURE 7-7.   Setting Label Distribution Protocol

TABLE 7-14.   Command Line Equivalent of Label Distribution Protocol Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Label Distribution Protocol	Node	`MPLS-LABEL-DISTRIBUTION-PROTOCOL`

Setting Parameters

- To configure LDP, set **Label Distribution Protocol** to *LDP* and configure the LDP parameters described in Section 7.2.4.2.
- To configure RSVP-TE, set **Label Distribution Protocol** to *RSVP-TE* and configure the RSVP-TE parameters described in Section 7.2.4.3.

7.2.4.2 Configuring LDP

To configure LDP, perform the following steps:

1. Configure MPLS parameters, as described in Section 7.2.4.1.

2. Set **Enable MPLS** *[= Yes]* **> Label Distribution Style >** *[= Dynamic]* **> Label Distribution Protocol** to *LDP* and set the dependent parameters listed in Table 7-15.
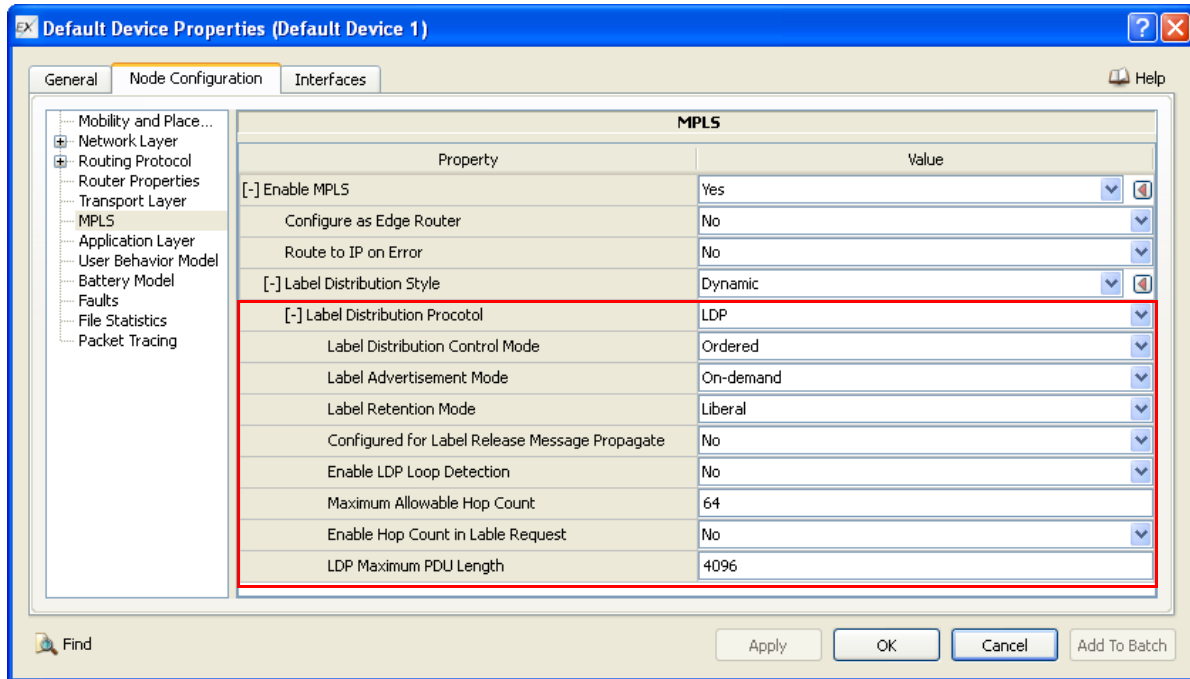
FIGURE 7-8.   Setting LDP Parameters

TABLE 7-15.   Command Line Equivalent of LDP Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Label Distribution Control Mode	Node	`MPLS-LABEL-DISTRIBUTION-CONTROL-MODE`
Label Advertisement Mode	Node	`MPLS-LDP-LABEL-ADVERTISMENT-MODE`
Label Retention Mode	Node	`MPLS-LABEL-RETENTION-MODE`
Configured for Label Release Message Propagate	Node	`CONFIGURED-FOR-LABEL-RELEASE-MESSAGE-PROPAGATE`
Enable LDP Loop Detection	Node	`MPLS-LDP-LOOP-DETECTION`
Maximum Allowable Hop Count	Node	`MAX-ALLOWABLE-HOP-COUNT`
Enable Hop Count in Label Request	Node	`HOP-COUNT-REQUIRED-IN-LABEL-REQUEST`
LDP Maximum PDU Length	Node	`MPLS-LDP-MAX-PDU-LENGTH`

Setting Parameters

- To configure LDP loop detection parameters, set **Enable LDP Loop Detection** to *Yes*; otherwise, set **Enable LDP Loop Detection** to *No.*

3. If **Enable LDP Loop Detection** is set to *Yes*, then set the dependent parameters listed in Table 7-16.
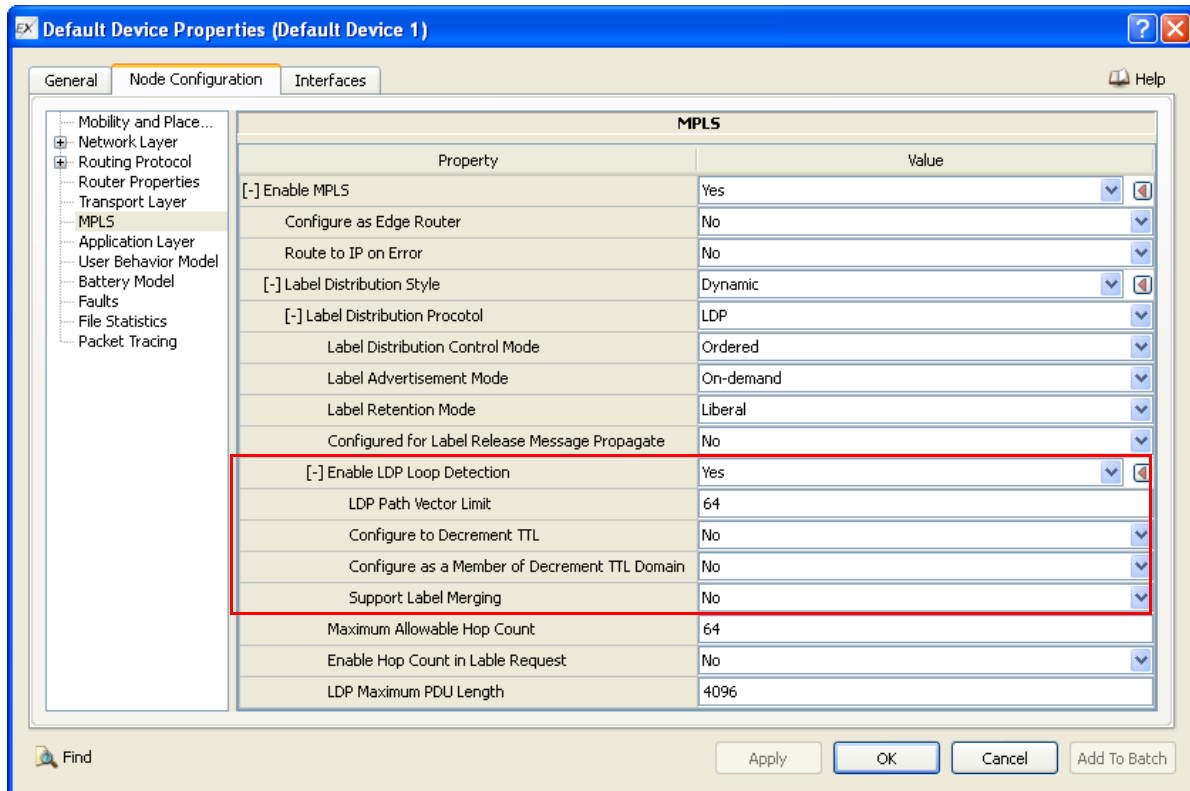
FIGURE 7-9.   Enabling LDP Loop Detection

TABLE 7-16.   Command Line Equivalent of LDP Loop Detection Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
LDP Path Vector Limit	Node	`MPLS-LDP-PATH-VECTOR-LIMIT`
Configure to Decrement TTL	Node	`MPLS-LDP-DECREMENTS-TTL`
Configure as a Member of Decrement TTL Domain	Node	`MPLS-MEMBER-OF-DECREMENT-TTL-DOMAIN`
Support Label Merging	Node	`SUPPORT-LABEL-MERGING`

7.2.4.3 Configuring RSVP-TE

To configure RSVP-TE, perform the following steps:

1. Configure MPLS parameters, as described in Section 7.2.4.1.

2. Set **Enable MPLS** *[= Yes]* **> Label Distribution Style >** *[= Dynamic]* **> Label Distribution Protocol** to *RSVP-TE* and set the dependent parameters listed in Table 7-17.
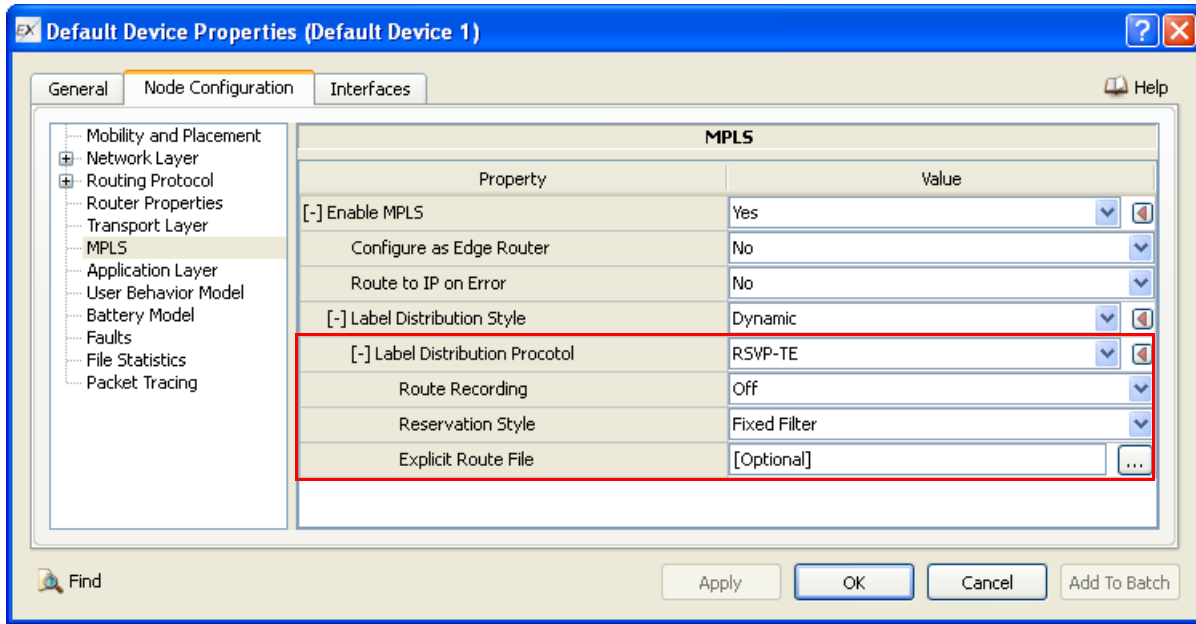
FIGURE 7-10.   Setting RSVP-TE Parameters

TABLE 7-17.   Command Line Equivalent of RSVP-TE Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Route Recording	Node	RSVP-TE-RECORD-ROUTE
Reservation Style	Node	RSVP-RESERVATION-STYLE
Explicit Route File	Node	RSVP-TE-EXPLICIT-ROUTE-FILE

7.2.4.4 Configuring Statistics Parameters

Statistics for MPLS can be collected at the global, node, subnet, and interface levels. Statistics for LDP can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for MPLS and LDP, check the box labeled **MPLS** and **MPLS LDP**, respectively, in the appropriate properties editor.

TABLE 7-18.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
MPLS	Global, Node, Subnet, Interface	`MPLS-STATISTICS`
MPLS LDP	Global, Node	`MPLS-LDP-STATISTICS`

7.2.5 Statistics

Table 7-19 lists the general MPLS statistics that are output to the statistics (.stat) file at the end of simulation. Table 7-20 lists the statistics collected by the LDP model. Table 7-21 lists the statistics collected by the RSVP-TE model.

TABLE 7-19.   MPLS Statistics

Statistic	Description
Number of packets received from IP Layer	Number of packets received from IP layer.
Number of packets sent to Mac Layer	Number of packets sent to the MAC layer.
Number of packets received from Mac Layer	Number of packets received from the MAC layer.
Total number of packets sent to IP layer	Sum of number of packets sent to IP layer when packet has reached destination and the number of packets sent to IP due to any Error.
Number of pending packet cleared	Number of pending packets cleared.
Number of packets dropped at source due to Buffer full	Number of packets dropped at source due to Buffer full.
Number of packets dropped due to bad Label	Number of packets dropped due to bad Label.
Number of packets dropped due to Packet size bigger than IP Fragmentation Unit	Number of packets dropped due to Packet size bigger than IP Fragmentation Unit.
Number of packets dropped due to expired TTL	Number of packets who's TTL expired.
Number of packets sent to IP due to no FTN at ingress	Number of packets sent to IP as FTN is not found at Ingress Node.
Number of packets sent to IP due to bad Label	Number of packets sent to IP due to bad Label.
Number of packets sent to IP due to Packet size bigger than IP Fragmentation Unit	Number of packets sent to IP due to Packet size bigger than IP Fragmentation Unit.

TABLE 7-20.   LDP Statistics

Statistic	Description
Number of Label Request Message Send	Number of label request messages sent.
Number of Label Mapping Send	Number of label mapping sent.
Number of Notification Message Send	Number of notification messages sent.
Number of Keep Alive Message Send	Number of keep alive messages sent.
Number of Label Withdraw Message Send	Number of label withdraw messages sent.
Number of Label Release Message Send	Number of label release messages sent.
Number of Address Message Send	Number of address messages sent.

TABLE 7-20.   LDP Statistics (Continued)

Statistic	Description
Number of Initialization Message Send	Number of initialization messages sent.
Number of UDP link hello Message Send	Number of UDP link hello messages sent.
Number of Label Request Message Received	Number of label request messages received.
Number of Label Mapping Received	Number of label mapping received.
Number of Notification Message Received	Number of notification messages received.
Number of Keep Alive Message Received	Number of keep alive messages received.
Number of Label Withdraw Message Received	Number of label withdraw messages received.
Number of Label Release Message Received	Number of label release messages received.
Number of Address Message Received	Number of address messages received.
Number of Initialization Message Received	Number of initialization messages received.
Number of Initialization Message Received in active	Number of initialization messages received in active mode.
Number of Initialization Message Received in passive	Number of initialization messages received in passive mode.
Number of UDP Link Hello Message Received	Number of UDP link hello received messages received.

TABLE 7-21.   RSVP-TE Statistics

Statistic	Description
Path Messages Received	Number of Path Messages Received.
Path Messages Sent	Number of Path Messages Sent.
Resv Messages Received	Number of Resv Messages Received.
Resv Messages Sent	Number of Resv Messages Sent.
PathErr Messages Received	Number of Path Error Messages Received.
PathErr Messages Sent	Number of Path Error Messages Sent.
ResvErr Messages Received	Number of Resv Error Messages Received.
ResvErr Messages Sent	Number of Resv Error Messages Sent.
PathTear Messages Received	Number of Path Tear Messages Received.
PathTear Messages Sent	Number of Path Tear Messages Sent.
ResvTear Messages Received	Number of Resv Tear Messages Received.
ResvTear Messages Sent	Number of Resv Tear Messages Sent.
HelloRequest Messages Received	Number of Hello Request Messages Received.
HelloRequest Messages Sent	Number of Hello Request Messages Sent.
HelloAck Messages Received	Number of Hello Acknowledgement Messages Received.
HelloAck Messages Sent	Number of Hello Acknowledgement Messages Sent.

7.2.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the MPLS model. All scenarios are located in the directories QUALNET_HOME/scenarios/multimedia_enterprise/mpls and QUALNET_HOME/ multimedia_enterprise/rsvp-te. Table 7-22 lists the sub-directory where each scenario is located.

TABLE 7-22.   MPLS Scenarios Included in QualNet

Scenario	Description
MPLS-LDP	
ldp/conservative	Shows MPLS-LDP conservative label retention mode.
ldp/independent	Shows the operation of MPLS-LDP when Label Distribution Control Mode is Independent.
ldp/liberal	Shows MPLS-LDP Liberal label retention mode.
ldp/next-hop-tlv	Shows Mpls-Ldp "Loop" detection depending on maximum allowable hop count. If hop count exceeds maximum allowable hop count then there is a potential loop.
ldp/ordered	Shows operation of MPLS-LDP when Label Distribution Control Mode is Ordered.
mpls-ip/fault-recovery	Shows that MPLS based fault recovery occurs after the fault is UP.
mpls-ip/fault-recovery-alternate-path	Shows that the Alternate recovery path is chosen correctly when there is a fault occurred in the working path and the Alternate path is Merged at PML to working path.
mpls-ip/ip-mpls-ip	Shows Propagation of Packets from IP to MPLS backbone and then to IP.
mpls-ip/lsr-egress	Shows that an LSR can act as both Egress as well as Intermediate LSR depending on the scenario topology in an IP-MPLS scenario.
mpls-ip/multiple-backbones	Shows Propagation of Packets from Source Node (Pure IP) to destination Node (PureIP) via multiple MPLS backbones.
mpls-ip/static-fec-classification	Shows FEC classification based on TOS (priority) of IP traffic in an IP-MPLS scenario.
mpls-ip/static-fec-classification-network-id	Shows that MPLS static routes can be configured with the destination being a network-id in an IP-MPLS scenario.
mpls-ip/static-ip-mpls	Shows that static routes configurations are supported in MPLS backbone in an IP-MPLS-IP scenario.
static	Shows the operation of MPLS when Label Distribution Style is static.
RSVP-TE	
ff-normal-explicit-loop	Shows RSVP-TE operation with Record route NORMAL and reservation style FF. In addition to that an explicit route is set such that a loop will be detected at node 3.
ff-normal-no-explicit	Shows RSVP-TE operation with Record route NORMAL and reservation style FF.
resv-ff	Shows reservation style in FF mode.
resv-ff-explicit-route-no-loop	Shows reservation style FF (Shared Explicit) with no explicit route.
resv-ff-no-explicit-route	Shows reservation style FF (Fixed Filter) with no explicit route.
resv-se	Shows reservation style in SE mode.
resv-se-no-explicit-route	Shows reservation style SE (Shared Explicit) with no explicit route.

7.2.7 References

1. RFC 3031, "Multiprotocol Label Switching Architecture." E. Rosen, A. Viswanathan, R. Callon. January 2001.

2. RFC 3469, "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery." V. Sharma,F. Hellstrand. February 2003.

3. RFC 3032, "MPLS Label Stack Encoding." Rosen, D. Tappan, G. Fedorkow, Y. Rekhter, D. Farinacci, T. Li, A. Conta. January 2001.

4. RFC 4023, "Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)." T. Worster, Y. Rekhter and E. Rosen. March 2005.

5. RFC 791, "Internet Protocol." Postel, J. September 1981.

6. RFC3036, "LDP Specification." Andersson, L., P. Doolan, N. Feldman, A. Fredette, B. Thomas. January 2001.

7. RFC 3209, "RSVP-TE: Extensions to RSVP for LSP Tunnels." D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow. December 2001.

∎∎

7.3 Quality of Service Extensions to OSPF (QOSPF)

The QualNet QOSPF model is based on RFC 2676.

7.3.1 Description

QOSPF is a set of extensions to OSPFv2 that address QoS flow support. It includes the acquisition of information needed to compute QoS paths, the selection of appropriate paths to meet the QoS requirements of a flow, and the maintenance of these paths.

> **Note:** When QOSPF operates without a resource reservation framework (e.g., RSVP), it uses a statistical method of provisioning. This statistical method measures the bandwidth and delay characteristics currently present on the links, and uses these to estimate the link's ability to meet the delay and bandwidth constraints being requested. Without explicit resource reservation, QOSPF cannot provide a guarantee that these constraints will not be violated.

7.3.2 Assumptions and Limitations

- The scope of QoS route computation is limited to a single area.
- All routers within an area run a QoS enabled version of OSPF and all interfaces on this router are QoS capable.
- Extended Breadth First Search for single path algorithm is used to accommodate more than one QoS metrics during path calculation.
- All interfaces of a given node should have the same number of queues, which will be between 1 and 8.

7.3.3 Command Line Configuration

To enable QOSPF, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] QUALITY-OF-SERVICE Q-OSPF
```

The scope of this parameter declaration can be Global or Node. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

Configuration Requirements
To use QOSPF, the routing protocol must be set to OSPFv2.

QOSPF Parameters

Table 7-23 describes the QOSPF configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 7-23.   QOSPF Parameters

Parameter	Value	Description
`QOSPF-COMPUTATION-ALGORITHM` Optional *Scope:* Global, Node	List • `EXTENDED_ BREADTH_ FIRST_SEARCH _SINGLE_PATH` *Default:* `EXTENDED_ BREADTH_ FIRST_SEARCH _SINGLE_PATH`	Specifies the algorithm that is used for calculation of paths between nodes. Currently the only supported value is `EXTENDED_BREADTH_FIRST_SEARCH_SINGLE_PATH`.
`QUEUEING-DELAY-FOR-QOS-PATH-CALCULATION` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	This parameter specifies whether or not queue delay will be considered during path calculation.
`QOSPF-INTERFACE-OBSERVATION-INTERVAL` Optional *Scope:* Global, Node	Time *Range:* `> 0S` *Default:* `2S`	Specifies monitoring interval for each interface of a node.
`QOSPF-FLOODING-INTERVAL` Optional *Scope:* Global, Node:	Time *Range:* `≥ 0S` *Default:* `0S`	Specifies the interval for flooding of QOSPF Link State Advertisements (LSAs).
`QOSPF-FLOODING-FACTOR` Optional *Scope:* Global, Node	Real *Range:* `[0, 1]` *Default:* `0.1`	Specifies the ratio of change in link utilization of an interface during the last period to the total link bandwidth.
`QOSPF-STATISTICS` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	This parameter enables QOSPF statistics collection.

7.3.4 GUI Configuration

This section describes how to configure QOSPF in the GUI.

Configuring QOSPF Parameters

To configure the QOSPF parameters, perform the following steps:

1. Go to the Default Device Properties Editor **>** Node Configuration **>** Routing Protocol.

1. Set **Routing Protocol IPv4** to *OSPFv2.* See Section 4.4 for configuring OSPFv2.

2. Set **Enable OSPF with Quality of Service(QOSPF)** to *Yes* and set the dependent parameters listed in Table 7-24.
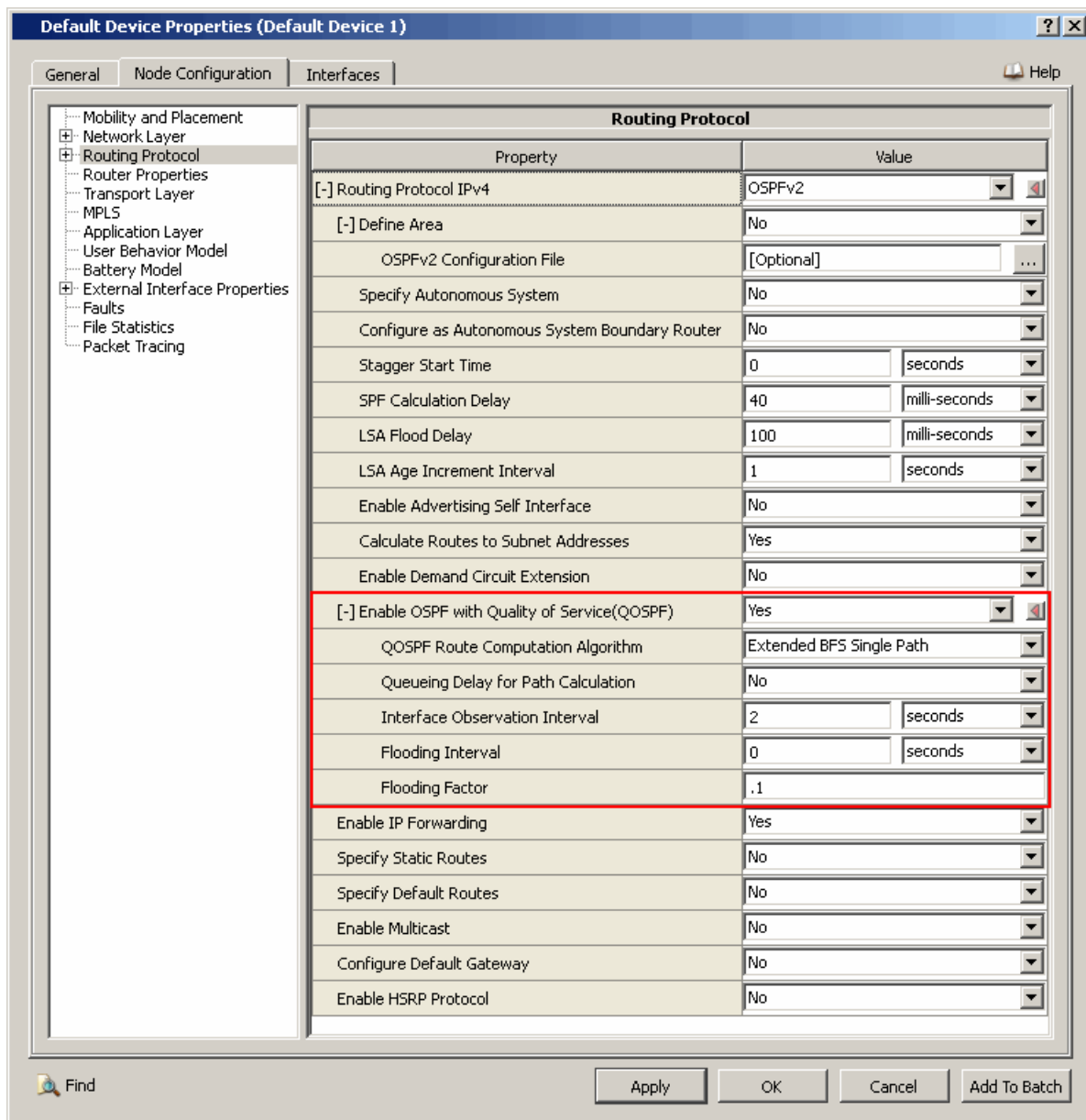
FIGURE 7-11.   Setting QOSPF Parameters

TABLE 7-24.   Command Line Equivalent of QOSPF Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
QOSPF Route Computation Algorithm	Node	QOSPF-COMPUTATION-ALGORITHM
Queuing Delay for Path Calculation	Node	QUEUEING-DELAY-FOR-QOS-PATH-CALCULATION
Interface Observation Interval	Node	QOSPF-INTERFACE-OBSERVATION-INTERVAL
Flooding Interval	Node	QOSPF-FLOODING-INTERVAL
Flooding Factor	Node	QOSPF-FLOODING-FACTOR

Configuring Statistics Parameters

Statistics for QOSPF can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for routing protocols including QOSPF, check the box labeled **Routing** in the appropriate properties editor.

TABLE 7-25.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Routing	Global, Node	ROUTING-STATISTICS

7.3.5 Statistics

Table 7-26 lists the QOSPF model statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 7-26.   QOSPF Statistics

Statistic	Description
Active Connections	Number of active connections to a node.
Rejected Connections	Number of rejected connections to a node.
Periodic Update send	Number of periodic updates sent to a node.
Triggered Update send	Number of triggered updates sent to a node.
Link Bandwidth	Link bandwidth of every interface of a node.
Maximum Utilization of Bandwidth	Total bandwidth utilization of a link interface.

7.3.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the QOSPF model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/qospf. Table 7-27 lists the sub-directory where each scenario is located.

TABLE 7-27.   QOSPF Scenarios Included in QualNet

Scenario	Description
best-path-selection1	Shows that QOSPF finds the best available shortest path which can satisfy the QoS requirements for each session from source to destination.
best-path-selection2	Shows that existing applications influence the remaining amount of bandwidth available for QoS applications and the paths chosen by the protocol.
best-path-selection3	Shows that QOSPF provides the best of available shortest paths to connection requests.
end-to-end-delay	Shows that QOSPF is able to check whether bandwidth and end-to-end delay can be satisfied by providing a path for a session.
link-fault	Shows that QOSPF finds the best path from source to destination and that this path is 'pinned down' throughout the session.
qos-app-retry-property	Shows the retry property of QoS application.
queue-delay-consideration1	Shows the overall functionality of QOSPF. Here, queuing delay is not considered during path calculation.
queue-delay-consideration2	Shows the overall functionality of QOSPF. Here, queuing delay is considered during path calculation.

7.3.7 References

1. RFC 2676. "QoS Routing Mechanisms and OSPF Extensions." G. Apostolopoulos, D. Williams, S. Kamat, R. Guerin, A. Orda, T. Przygienda. August 1999.

8 Multimedia Applications

This chapter describes features, configuration requirements and parameters, statistics, and scenarios for Multimedia Applications, and consists of the following sections:

- H323 and H225 Protocols
- Real-time Transfer Protocols
- Session Initiation Protocol (SIP)
- Voice over Internet Protocol (VoIP)

∙∙∙

8.1 H323 and H225 Protocols

The QualNet H323 and H225 protocols are based on the following recommendations:

- ITU-T Recommendation H.323, Packet-based multimedia communications systems. (http://www.itu.int/rec/T-REC-H.323/en/)
- ITU-T Recommendation H.225.0, Call signalling protocols and media stream packetization for packet-based multimedia communication systems. (http://www.itu.int/rec/T-REC-H.225.0/en/)

The main frameworks of Internet Telephony are H323, H225, H245, and Q931. Of these, QualNet supports H323 and H225.

8.1.1 Description

H323 is a standard, recommended by ITU-T, for transmission of real time audio, video and data communications over packet based networks. It specifies the components, protocols, and procedures for multimedia communication. One of the primary goals of H323 standard is the interoperability with other multimedia service networks through the use of Gateways. H323 is an umbrella protocol consisting of following frameworks.

- H225 Registration Admission and Status (RAS)
- H225 Call signaling
- H245 Control signaling
- RTP/RTCP
- Audio/Video application (G.711, H.261, etc.)

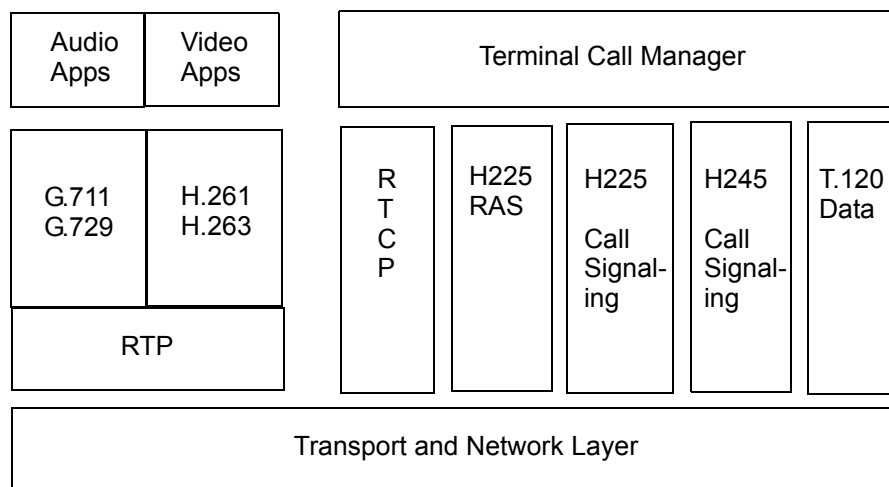The H323 protocol stack on top of the transport and network layers is shown in Figure 8-1.

FIGURE 8-1.   H323 Protocol Stack on Top of Transport and Network Layers

VoIP consists of Audio/Video applications with RTP/RTCP in between application and transport layers and different ITU-T recommended standards.

H323 is not a single protocol model. Detailed description of each H323 item and different protocol models are given below.

8.1.1.1 H323 Components

The H323 standard specifies the following four kinds of components:

- **Terminal**

  Terminal (a personal computer) is used for real-time bi-directional multimedia communications. The multimedia application and H323 should run in this device. It supports audio communication, can optionally support video and data communications.

- **Gateways**

  A gateway connects two dissimilar networks. A H323 gateway provides connectivity between a H323 network and a non-H323 network. For example, a gateway can connect and provide communication between an H323 terminal and SCN networks. This is achieved by converting the media format between different networks and transferring information between different networks. A gateway has the characteristics of both an H323 terminal on the H323 network and the other terminal on the non-H323 network.

- **Gatekeepers**

  A gatekeeper is considered as the brain of H323 network. It provides important services like addressing, authentication, bandwidth management, accounting, billing, etc. However a gatekeeper is not a mandatory component in a H323 network.

- **Multi-point Control Unit (MCU)**

  MCU provides support for conferences of more than two H323 terminals. All such terminals participating in the conference call establish a connection with the MCU first. MCU manages conference resources and may handle the media stream.

8.1.1.2 H323 Zone

An H323 zone is the collection of all H323 terminals, gateways, and MCUs managed by a single gatekeeper. An H323 zone includes at least one terminal and may or may not include gateways or MCUs. A gatekeeper is optional in a H323 zone. There can be at most one gatekeeper in a zone.

8.1.1.3 H323 Specified Protocols

Audio CODEC

An audio CODEC encodes audio signals into digitized form. This digitized signal is sent to the receiver by using packet based Internet. The receiving terminal receives packets and decodes them to transform into audio signal again. G711 is one such recommendation from ITU-T. However, the QualNet H323 model does not implement any audio CODEC.

Video CODEC

A video CODEC encodes analog signals collected from camera for transmission on the H323 network. The receiving end receives the IP packet based encoded video signal and decodes it to collect the video signal back.

RTP/RTCP

Real-time Transport Protocol (RTP) provides end-to-end delivery service of real time audio and video. RTP works in between the application layer and transport layer and uses UDP in transport layer to carry media stream. Real-time Transport Control Protocol (RTCP) is the counterpart of RTP that provides control services. It provides quality of data distribution.

H225 RAS

H323 endpoints use H225 RAS service for following services:

- **Gatekeeper Discovery**: H323 endpoints discover the gatekeeper in that zone for registration with it. If endpoints know the gatekeeper transport address, gatekeeper discovery can be done statically. Otherwise, endpoints multicast a Gatekeeper Request (GRQ) message on the gatekeeper discovery

multicast address. The gatekeeper receives this discovery message and acknowledges with Gatekeeper Confirmation (GCF).

If the gatekeeper is unable to serve any endpoint then, instead of GCF, it sends a Gatekeeper Reject (GRJ) message. The endpoint receives the gatekeeper's transport address from this GCF message. This gatekeeper discovery process is done through unreliable UDP channels. For this reason, the gatekeeper discovery process is refreshed periodically.

- **Endpoint Registration**: After discovering the gatekeeper, endpoints register with the gatekeeper by providing their transport and alias addresses. An endpoint sends a Registration Request (RRQ) message to the gatekeeper. This message contains the endpoint's transport and alias addresses. The gatekeeper responds with a Registration Confirmation (RCF) or Registration Reject (RRJ) message to the endpoint. The RRQ message is also sent periodically because of the unreliable channel. An endpoint can also unregister with its gatekeeper by sending an Unregister Request (URQ) message.

- **Endpoint Location**: An endpoint sends a Location Request (LRQ) message to the gatekeeper to get the transport address of another endpoint. The requesting endpoint knows the alias address of the other endpoint and sends it through the LRQ message. The gatekeeper finds the corresponding transport address of that alias address. If there is more than one H323 zone, then the LRQ request should be multicast to the gatekeeper multicast group. The proper gatekeeper receives this message and sends a Location Confirmation (LCF) message in response. In the case of a rejection, the gatekeeper sends a Location Reject (LRJ) message to the endpoint.

- **Admission Control**: An endpoint sends an Admission Request (ARQ) message to the gatekeeper to request bandwidth required for the transmission. The gatekeeper replies with an Admission Confirmation (ACF) message. The ACF message may possibly allow less than the requested bandwidth. If the gatekeeper cannot allow this bandwidth requirement, it rejects the connection by sending an Admission Reject (ARJ) message.

H225 RAS Messages

The implemented H225 RAS messages described below.

- **Gatekeeper Discovery (GRQ)**: An endpoint sends a GRQ message to discover a gatekeeper. The endpoint may send the message with the unicast address of a gatekeeper if it knows this address, otherwise, it multicasts to the gatekeeper multicast address.

- **Gatekeeper Confirmation (GCF)**: A gatekeeper receives a GRQ message from an endpoint and sends back a GCF message with its transport address. When the endpoint receives the first GCF from a gatekeeper, it acknowledges the gatekeeper. The subsequent GCF messages will be rejected by that endpoint. Thus, each endpoint will have only one gatekeeper.

- **Gatekeeper Reject (GRJ)**: A gatekeeper sends a GRJ message to an endpoint if it is unable to serve the endpoint as a gatekeeper. When the endpoint receives the GRJ, message it neglects the sender of the GRJ as its gatekeeper.

- **Registration Request (RRQ)**: An endpoint sends an RRQ message to a gatekeeper with its alias address to register with the gatekeeper. The gatekeeper transport address is discovered in the gatekeeper discovery process.

- **Registration Confirmation (RCF)**: A gatekeeper receives an RRQ message and registers an endpoint. The gatekeeper sends an RCF message to the endpoint to confirm the registration.

- **Registration Reject (RRJ)**: If a gatekeeper is unable to register an endpoint because of some reasons, it sends an RRJ message to the endpoint without registering the endpoint.

- **Location Request (LRQ)**: An endpoint sends an LRQ message to the gatekeeper when a call is requested. The initiator endpoint sends the alias address of the receiving node through the LRQ message to get the transport address of the receiver.

- **Location Confirmation (LCF)**: When a gatekeeper receives the alias address of the receiver in an LRQ message, it searches for any corresponding endpoint that has registered with this alias address. If such an endpoint is found, the gatekeeper sends an LCF message to the initiator with the transport

address of the receiver. This transport address of the receiver is used to create the connection by using H225 call signaling.

- **Location Reject (LRJ)**: If a gatekeeper is unable to find any endpoint that has registered with the alias address contained in an LRQ message received by the gatekeeper, it sends an LRJ message to the initiator. If all the gatekeepers form a multicast group, then only one gatekeeper from that group has the entry of the receiver endpoint. In this case, the rest of the gatekeepers should send LRJ messages. However, to reduce the network traffic, the model does not send LRJ messages in this situation; only the registering gatekeeper sends an LCF message.

- **Admission Request (ARQ)**: An endpoint sends an ARQ message to the gatekeeper for an admission request. It sends the maximum bandwidth requirement with the message.

- **Admission Confirmation (ACF)**: A gatekeeper receives the bandwidth requirement from the ARQ message. If that much bandwidth can be allowed, it sends an ACF message. It may also send an ACF message with less than the requested bandwidth.

- **Admission Reject (ARJ)**: A gatekeeper sends an ARJ message to an endpoint if admission is not accepted. The connection procedure will be canceled after receiving this message by the initiator.

Table 8-1 describes the overall message processing.

TABLE 8-1.   Overall Message Processing

Message	Sender	Receiver	Description
GRQ	Endpoint	Gatekeeper	Gatekeeper discovery starts
GCF	Gatekeeper	Endpoint	Gatekeeper discovered
GRJ	Gatekeeper	Endpoint	Gatekeeper discovery rejected
RRQ	Endpoint	Gatekeeper	Registration with gatekeeper
RCF	Gatekeeper	Endpoint	Endpoint registered
RRJ	Gatekeeper	Endpoint	Endpoint registration rejected
LRQ	Endpoint	Gatekeeper	Location requested for a alias address
LCF	Gatekeeper	Endpoint	Location returned for that alias address
LRJ	Gatekeeper	Endpoint	Location not found for that alias
ARQ	Endpoint	Gatekeeper	Admission request
ACF	Gatekeeper	Endpoint	Admission granted
ARJ	Gatekeeper	Endpoint	Admission not granted

H225 RAS Self Timers

The H225 RAS service is implemented over UDP (unreliable channel) and requires the following two self-timers:

- **Gatekeeper Discovery Timer**: This timer is used to refresh the latest gatekeeper discovery information periodically.

- **Registration Request Timer**: This timer is used to refresh the latest registration request information periodically.

H225 Call Signaling Messages

H225 call signaling is used to setup connections between H323 endpoints, over which real-time data can be transported. H225 messages use a reliable channel (TCP) for this connection setup. If there is no gatekeeper present in the network, an endpoint creates a connection directly with another endpoint by using call-signaling messages. If a gatekeeper exists, then call-signaling messages are either carried directly between endpoints (direct call signalling) or are routed through the gatekeeper (gatekeeper routed call signaling). The messages used to create the connection are discussed below.

- **Setup**: The call initiator endpoint sends a Setup message to the receiver. All the call-signaling messages are sent over a reliable channel. When there is a call request from a VoIP application at an endpoints, H323 opens a TCP channel for call establishment. The Setup message is sent over this channel. If the H323 zone contains a gatekeeper, then before sending the Setup message, the initiator should know the receiver's transport address by RAS messaging. If call signal routing is selected through the gatekeeper, then the Setup message is first sent to the gatekeeper and gatekeeper relays it to the receiver.

- **Call Proceeding**: The receiver endpoint accepts a Setup message and sends a Call Proceeding message to the initiator, indicating that it is trying to establish the call. The Call Proceeding message can be sent directly to the initiator or to the gatekeeper depending on the call signaling routing type. After sending this message, the receiver tries to find out the required bandwidth by sending a Admission Request RAS message to the gatekeeper.

- **Alerting**: The receiver gets confirmation about the admission from gatekeeper and sends an Alerting message to the initiator. When the initiator endpoint receives this message, it comes to know that ringing is in place at the receiver endpoint.

- **Connect**: The receiver endpoint sends a Connect message to the initiator when the user at the receiver endpoint accepts the call. The Connect message can be sent directly to the initiator or through the gatekeeper, depending on the call signal routing type. When this message is received, connection establishment is complete and conversation can be taken place.

- **Release Complete**: After the conversation is over, either the caller endpoint or the called endpoint sends a Release Complete message to release the connection. As soon as the connection is released, then TCP connection is closed.

H225 Call Model

Two types of call models are supported by the RAS service: direct and gatekeeper-routed. In the direct call model, a call-signaling connection is created directly from the initiator to the receiver. In the gatekeeper-routed call model, call signaling messages are sent through the gatekeeper. In this case, a TCP channel is created from the initiator to the gatekeeper and from the gatekeeper to the receiver.

H225 Call Signal Message Flow

Figure 8-2 through Figure 8-6 show some of the call signal message flows.
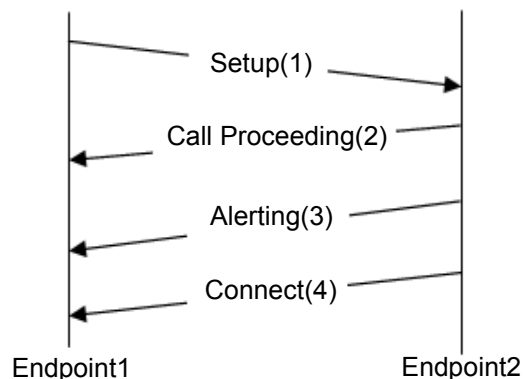
FIGURE 8-2.   Basic Call Setup with no Gatekeepers
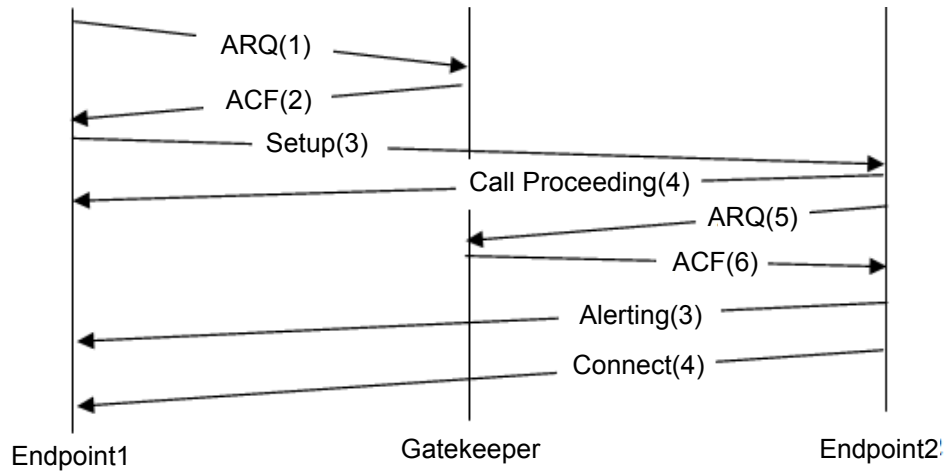
FIGURE 8-3.   Endpoints Registered with Same Gatekeeper - Direct Call Signaling
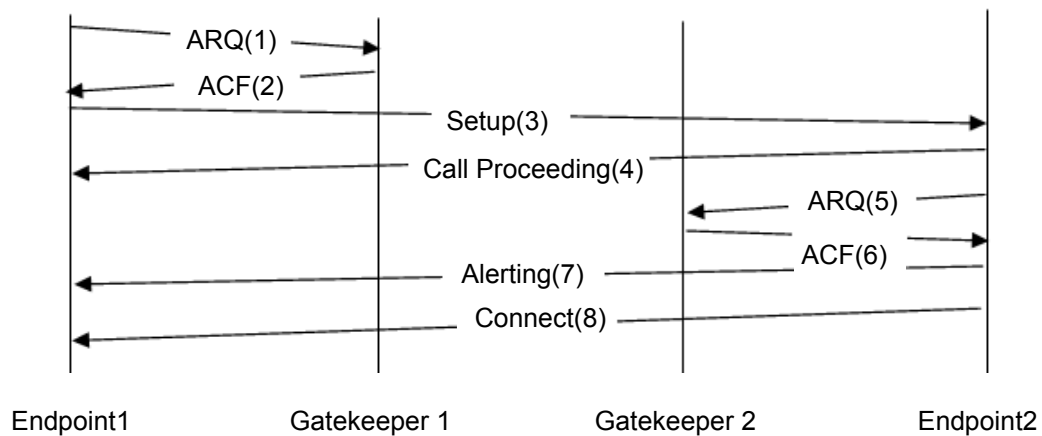
FIGURE 8-4.   Endpoints Registered with Different Gatekeepers - Direct Call Signaling
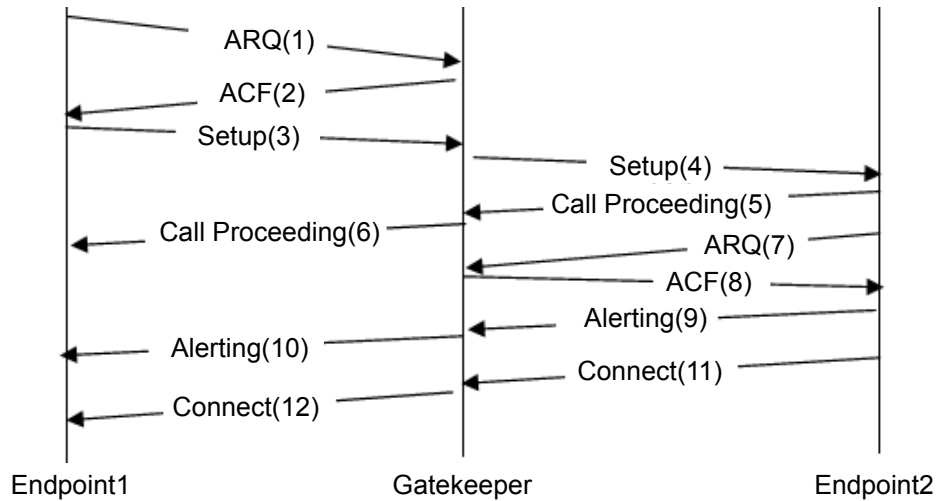
FIGURE 8-5.   Endpoints Registered with Same Gatekeeper - Gatekeeper-routed Call Signaling
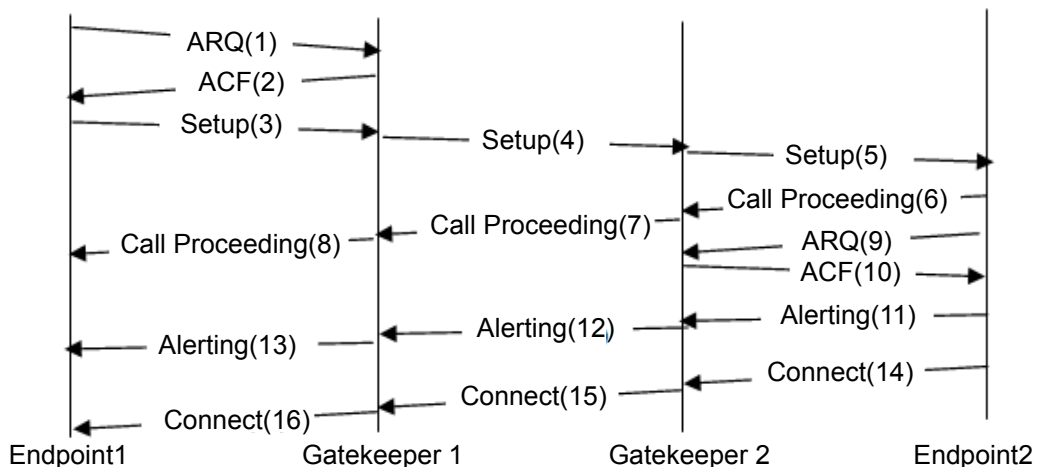
FIGURE 8-6.   Endpoints Registered with Different Gatekeepers - Gatekeeper-routed Call Signaling

8.1.1.4 Control Flow

Here we describe the basic flow as viewed at the application layer.

Caller End

- VoIP initiator (<src>) structure will be initialized at QualNet initialization time; it sets a self-timer, which will fire at <start time> to initiate the call.

- Upon expiration of this timer, VoIP will request H.323 to establish a connection with <dest>.

- When connection is established H.323 will inform VoIP (at <src> end) and it starts sending data for a random amount of time determined by exponential distribution.

Callee End

- H.323 indicates that <src> wants to talk with this node. Depending on flag (ACCEPT or REJECT), VoIP will accept or reject the call.
- If the callee accepts the call, it initializes its data structure and informs H.323 to establish the call.

Data Generation

After the connection establishment, the caller end node starts transmission. The random amount of time for which a node will talk is determined by exponential distribution whose mean is <interval> * MeanSpurtGapRatio. During this time a node continuously sends packets to the other node (through RTP) at an interval of <packetization interval>. When this node has finished transmitting packets, the other node starts sending packets in a similar fashion. This process continues until <end time>.

Session Close

When a node closes the VoIP session, it requests H.323 to close the connection. H.323 will inform the other end that this node has closed the connection.

8.1.1.5 H323 Call Creation/Release and Media Communication Establishment

An endpoint first identifies its gatekeeper by sending a GRQ message to the multicast group of gatekeepers. The endpoint considers its gatekeeper to be the one from which it receives the first acknowledgement. The endpoint registers with the gatekeeper by sending a RRQ message to the gatekeeper. After this registration process, each gatekeeper knows the alias address and corresponding transport address of all the endpoints that have registered with it.

If a gatekeeper is not present, then RAS service is not required. Endpoints know each other's address and communicate directly with each other. First, two endpoints establish a connection by using the H225 Call Signaling messages. Then, the two terminals talk to each other by exchanging IP packets that encode voice and are transmitted by using RTP/UDP.

If RAS service is present in the network, each terminal registers with the nearest gatekeeper as described above. When one terminal initiates a new call, it sends an Admission Request (ARQ) message to its gatekeeper. The gatekeeper checks the possibility of the call and sends an ARJ message if the call is not permitted for some reason, such as the requested bandwidth not being available, or the receiver not having registered, etc. If there is no such error, the gatekeeper sends an Admission Confirm (ACF) message to the terminal. In the direct call model, the gatekeeper sends the transport address of the receiver with this message. In the gatekeeper-routed call model, the gatekeeper sends its own address to the terminal.

The terminal creates a TCP channel with its receiver address. After channel establishment, the initiator sends a Setup message through this TCP channel. In the direct call model, the Setup message directly goes to the receiver and the receiver acknowledges with a Call Proceeding message. The initiator receives the Call Proceeding message which indicates that the receiver is trying to establish the call. next, the receiver sends an ARQ message to its gatekeeper for admission request. If the request is granted, then the receiver sends an Alerting message to the initiator; otherwise, the call is rejected.

The Alerting message indicates the call is in ringing state. When the user at the receiver end receives the call, the receives sends a Connect message to the initiator. The Connect message indicates to the initiator that the call is established. The two terminals start talking through the RTP/UDP channel. Note that the call establishment must be done over a reliable channel like TCP, but the conversation takes place over an unreliable channel.

In the gatekeeper-routed call model, all the above call signaling messages are transmitted via the gatekeeper. In this case, the initiator sends a Setup message to its own gatekeeper. The gatekeeper forwards this message to the receiver if the receiver has directly registered with that gatekeeper. Otherwise, the message is relayed to the gatekeeper with whom the receiver has registered.All the Call signaling messages are transmitted via gatekeeper in a similar way.

If the receiver does not receive the call within the call timeout interval, the call is rejected. The call timeout value can be configured through the configuration file.

After the conversation is over, the receiver or initiator sends a Release Complete message. Whoever receives the last voice packet sends a Release Complete message to the other. Following this, the reliable channel is also closed.

A terminal is engaged in conversation in only one connection. If a terminal sends a call request to another terminal that is already engaged in a conversation, the call request is rejected.

8.1.2 Command Line Configuration

To enable H323-H225 include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] MULTIMEDIA-SIGNALLING-PROTOCOL  H323
```

The scope of this parameter declaration can be Global or Node. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

H323 Parameters

Table 8-2 lists the H323 configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 8-2.   H323 Parameters

Parameter	Value	Description
H323-GATEKEEPER Optional *Scope:* Global, Node	Node-list	Specifies the list of gatekeepers in the network. **Note:** If the gatekeeper list is not specified, connections can be established but without the RAS functionality.
TERMINAL-ALIAS-ADDRESS-FILE Required *Scope:* Global, Node	Filename	Specifies the terminal alias address file. This file contains the node ID and alias address for each terminal. The file extension must be ".endpoint". The format of this file is described in Section 8.1.2.1. This parameter is required if H323 is enabled.
H323-CALL-MODEL Optional *Scope:* Global	List: • GATEKEEPER-ROUTED • DIRECT *Default:* DIRECT	Specifies the H323 call model.
VOIP-SIGNALLING-STATISTICS Optional *Scope:* Global, Node	List: • YES • NO *Default:* NO	Specifies whether H323 statistics collection is enabled.
GATEKEEPER-ADDRESS Optional *Scope:* Global, Node	IP Address *Default:* 224.0.1.41	Specifies the gatekeeper address. If the gatekeeper has a predefined unicast address then that address is specified using this parameter. If gatekeeper discovery is done dynamically, then a multicast protocol and group management protocol with the IGMP router must be specified.

8.1.2.1 Format of the Terminal Alias Address File

Each line in the terminal alias address file specifies the alias address of one terminal and has the following format:

```
<Node ID> <Alias Address>
```

where

`<Node ID>`	Node identifier of the terminal.
`<Alias Address>`	Alias address of the terminal. The alias address may be an email ID, phone number, etc.

Example

The following lines show a segment of a terminal alias address file:

```
1 one@hotmail.com
2 two@hotmail.com
3 17083861050
```

8.1.3 GUI Configuration

This section describes how to configure H323 and H225 in the GUI.

Configuring H323 and H225 Parameters

To configure the H323 and H225 parameters, perform the following step:

1. Go to **Node Properties Editor > Node Configuration > Application Layer**.

2. Set **Multimedia Signalling Protocol** to *H323* and set the dependent parameters listed in Table 8-3.
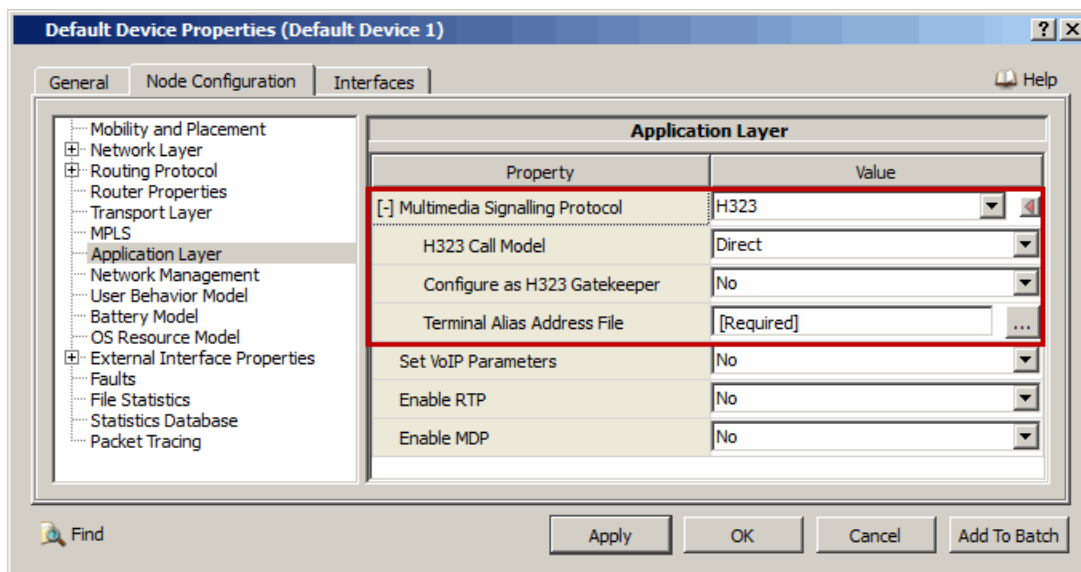
FIGURE 8-7.   Setting H323 Parameters

TABLE 8-3. **Command Line Equivalent of H323 and H225 Parameters**

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
H323 Call Model	Node	`H323-CALL-MODEL`
Configure as H323 GateKeeper	Node	N/A
Terminal Alias Address File	Node	`TERMINAL-ALIAS-ADDRESS-FILE`

3. If **H323 Call Model** is set to *Gatekeeper Routed*, set the dependent parameters listed in Table 8-4.
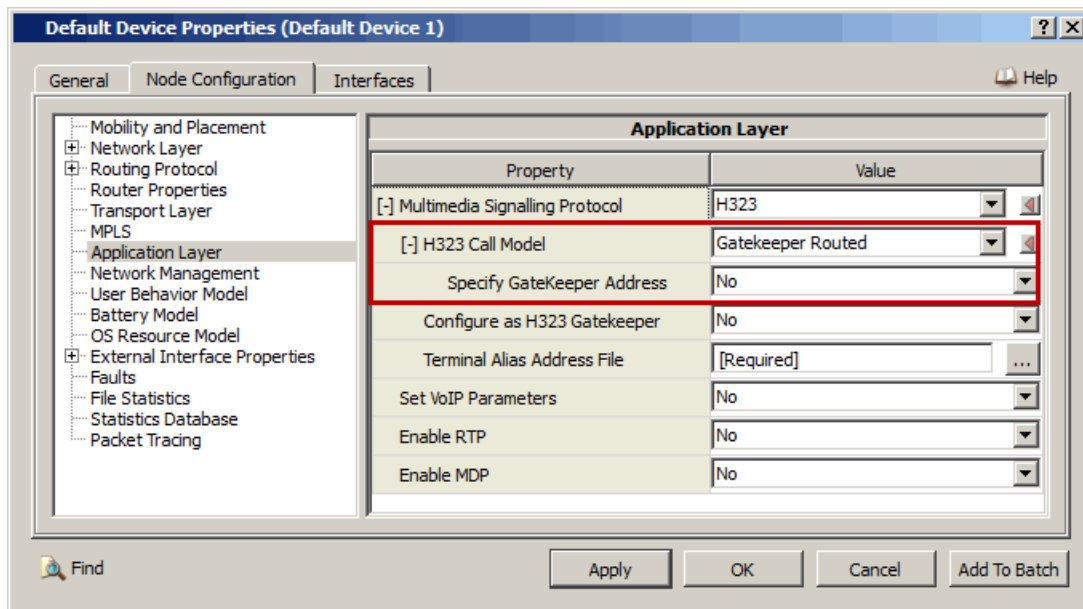
FIGURE 8-8. **Setting H323 Call Model specific Parameters**

TABLE 8-4. **Command Line Equivalent of H323 Call Model specific Parameters**

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Specify GateKeeper Address	Node	N/A

Setting Parameters

- To specify the gatekeeper address, set **Specify GateKeeper Address** to *Yes*; otherwise set **Specify GateKeeper Address** to *No*.

4. If **Specify GateKeeper Address** is set to *Yes*, then set the dependent parameters listed in Table 8-5.
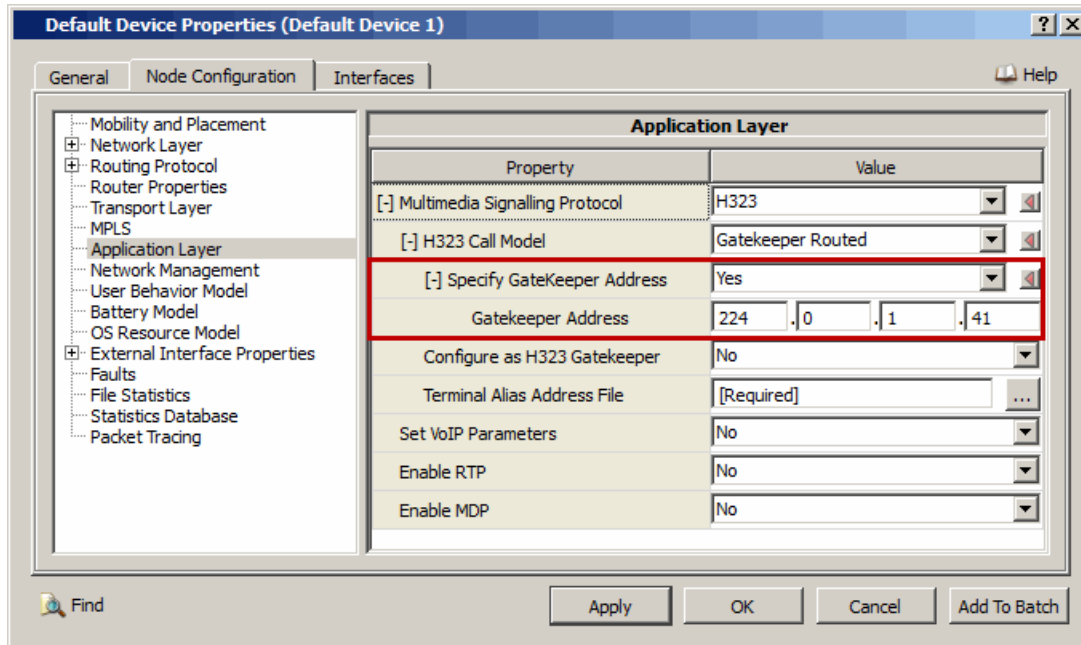
FIGURE 8-9.   Setting GateKeeper Address

TABLE 8-5.   Command Line Equivalent of H323 Call Model specific Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Gatekeeper Address	Node	H323-GATEKEEPER

8.1.4 Statistics

Table 8-6 list the H323-H225 statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 8-6.   H323 - H225 Statistics

Statistic	Description
H225 Statistics	
Number Of GRQ Sent	Number of Gatekeeper Request Messages (GRQ) sent.
Number Of GCF Sent	Number of Gatekeeper Confirm Messages (GCF) sent.
Number Of GRJ Sent	Number of gatekeeper Reject Messages (GRJ) sent.
Number Of RRQ Sent	Number of Registration Request Messages (RRQ) sent.
Number Of RCF Sent	Number of Registration Confirm Messages (RCF) sent.
Number Of RRJ Sent	Number of Registration Reject Messages (RRJ) sent.
Number Of ARQ Sent	Number of Admission Request Messages (ARQ) sent.
Number Of ACF Sent	Number of Admission Confirm Messages (ACF) sent.
Number Of ARJ Sent	Number of Admission Reject Messages (ARJ) sent.
Number Of LRQ Sent	Number of Location Request Messages (LRQ) sent.
Number Of LCF Sent	Number of Location Confirm Messages (LCF) sent.

TABLE 8-6.   H323 - H225 Statistics (Continued)

Statistic	Description
Number Of LRJ Sent	Number of Location Reject Messages(LRJ) sent.
H323 Call Signaling Statistics (Terminal)	
Number Of Calls Initiated	Number of calls initiated by a terminal.
Number Of Calls Received	Number of calls received by a terminal.
Number Of Calls Established	Number of calls established by a terminal.
Number Of TCP Connections Rejected	Number of calls rejected by a terminal.
H323 Call Signaling Statistics (GateKeeper)	
Number Of Calls Forwarded	Number of calls forwarded by the gatekeeper.

8.1.5 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the H323-H225 model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/voip/h323. Table 8-7 lists the sub-directory where each scenario is located.

TABLE 8-7.   H323-H225 Scenarios Included in QualNet

Scenario	Description
diff-encoding-scheme	Shows whether VOIP application with Jitter buffer runs perfectly with the support of different encoding scheme and can make H323 call signaling direct from initiator to receiver.
jitter-multiple-gatekeeper-direct	Shows whether VOIP application with Jitter buffer runs perfectly with the support of multiple gatekeepers and can make H323 call signaling direct from initiator to receiver.
jitter-single-gatekeeper-direct	Shows whether VOIP application with Jitter buffer runs perfectly with the support of one gatekeeper and make H323 call signaling direct from initiator to receiver.
jitter-two-gatekeeper-direct	Shows whether VOIP application with Jitter buffer runs perfectly with the support of two gatekeepers and can make H323 call signaling direct from initiator to receiver.
multiple-gatekeeper-direct	Shows whether VOIP application without Jitter buffer runs perfectly with the support of two gatekeepers and can make H323 call signaling direct from initiator to receiver.
multiple-gatekeeper-gr	Shows whether VOIP application without Jitter buffer runs perfectly with the support of multiple gatekeepers and makes H323 call signaling through gatekeeper from initiator to receiver.
no-gatekeeper	Shows whether VOIP application without Jitter buffer runs perfectly without the support of gatekeeper.
single-gatekeeper-direct	Shows whether VOIP application without Jitter buffer runs perfectly with the support of one gatekeeper and make H323 call signaling direct from initiator to receiver.

TABLE 8-7.   H323-H225 Scenarios Included in QualNet (Continued)

Scenario	Description
two-gatekeeper-direct	Shows whether VOIP application without Jitter buffer runs perfectly with the support of two gatekeepers and can make H323 call signaling direct from initiator to receiver.
two-gatekeeper-gr	Shows whether VOIP application without Jitter buffer runs perfectly with the support of two gatekeepers and can make H323 call signaling through gatekeeper from initiator to receiver.

8.1.6 References

1. ITU-T Recommendation H.323, Packet-based multimedia communications systems. (http://www.itu.int/rec/T-REC-H.323/en/)

2. ITU-T Recommendation H.225.0, Call signalling protocols and media stream packetization for packet-based multimedia communication systems. (http://www.itu.int/rec/T-REC-H.225.0/en/)

••

8.2 Real-time Transport Protocol (RTP)

The QualNet RTP model is based on RFC 3550.

8.2.1 Description

The Real-time Transport Protocol (RTP) is a standardized packet format for delivering audio and video over the Internet. It was developed by the Audio-Video Transport Working Group of the IETF and first published in 1996 as RFC 1889 which was made obsolete in 2003 by RFC 3550. RTP can also be used in conjunction with the RSVP protocol which enhances the field of multimedia applications.

RFC 3550 also defines Real-time Transport Control Protocol (RTCP), which is a companion protocol of RTP. RTCP provides out-of-band control information for an RTP flow. It supplements RTP in the delivery and packaging of multimedia data, but does not transport any data itself. It is used to periodically transmit control packets to participants in a streaming multimedia session. The primary function of RTCP is to provide feedback on the quality of service being provided by RTP. RTCP gathers statistics on a media connection and information such as bytes sent, packets sent, packets lost, jitter, and round trip delay. An application may use this information to increase the quality of service, perhaps by limiting the flow or by using a different codec.

There are several types of RTCP packets: Sender Report packets, Receiver Report packet, Source Description RTCP packets, Goodbye RTCP packets, and Application-specific RTCP packets.

RTP does not have a standard TCP or UDP port on which it communicates. The only standard that it follows is that UDP communications are done via an even-numbered port and the next higher odd-numbered port is used for RTP Control Protocol (RTCP) communications. RTP can carry any data with real-time characteristics, such as interactive audio and video.

QualNet implements RTP/RTCP as a layer between the application and transport layers. Any application layer traffic generator application can use the RTP model by using the RTP APIs. The RTP model encapsulates the data provided by the traffic generator model in an RTP packet and sends them over UDP.

RTP Jitter Buffer

Real-time communications, such as RTP, are sensitive to delay and variation in packet arrival times, and require a steady, dependable stream of packets to provide reasonable playback quality. Delay is the time it takes a packet to reach its destination. Whenever packets travel across a network, some delay is inevitable. Because of this, the delay budget for reasonable two-way conversations is about 150 milliseconds each way. When a delay exceeds the budget, callers may be confused about who should speak or listen.

Early, late, or out of sequence arrival of packets may cause undesirable variation (called jitter) in the delay between packet transmission and reception times. Excessive jitter causes the users to experience quality degradation during a call.

A way to compensate for excessive jitter is to increase the size of the jitter buffer. The jitter buffer on the phone is responsible for reassembling packet streams. When there is an issue with packets, such as arriving out of sequence or too late, the buffer will try and adjust to compensate or fill in with white comfort noise if necessary. Adjusting the buffer can minimize jitter problems, but it can also introduce other issues such as latency, which can cause conversations to be clipped. For example, adjusting the buffer to 300 milliseconds would make normal conversation difficult. Increasing buffer size can help, but only to a point. Just as critical as adjustments is the ability to measure and understand jitter. Tracking jitter measurements provide hard data that an administrator can use to improve call quality.

8.2.2 Features and Assumptions

This section describes the implemented features, omitted features, assumptions and limitations of the RTP model.

8.2.2.1 Implemented Features

- RTP over UDP.
- Generation and reception of control information packets for SR (Sender Report), RR (Receiver Report), SDES (Source DEScription), BYE.
- RTP/RTCP multisession support.
- Jitter buffer implementation.
- Support of IPv6 in RTP.

8.2.2.2 Omitted Features

- RTP Translators and Mixers.
- RTCP APP packet.
- Use of SDP for any signaling model to negotiate RTP/RTCP ports, codec or any other media parameters.
- CSRC list.
- VoIP with RTP multisession.
- DSP functionality.

8.2.2.3 Assumptions and Limitations

- QualNet supports only the mandatory CNAME among the SDES items.

8.2.3 Command Line Configuration

To enable RTP, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] RTP-ENABLED      YES
```

The scope of this parameter declaration can be Global or Node. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

> **Note:** The default value of parameter `RTP-ENABLED` is `NO`.

RTP Parameters

Table 8-8 describes the RTP configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 8-8.   RTP Parameters

Parameter	Value	Description
`RTCP-SESSION-MANAGEMENT-BANDWIDTH` Optional *Scope:* Global, Node	Integer *Range:* `> 0` *Default:* `64000` *Unit:* bps	Specifies total available bandwidth for all data and control packets in the network.
`RTP-JITTER-BUFFER-ENABLED` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Specifies whether the jitter buffer functionality is enabled for VoIP.
`RTP-JITTER-BUFFER-MAXNO-PACKET` Optional *Scope:* Global, Node	Integer *Range:* `> 0` *Default:* `100` *Unit:* packets	Specifies the maximum size of the jitter buffer (in number of packets).
`RTP-JITTERBUFFER-MAXIMUM-DELAY` Optional *Scope:* Global, Node	Integer *Range:* `> 0S` *Default:* `10MS`	Specifies the maximum duration that a packet can stay in the jitter buffer. This is required for processing the first packet received from the network. After that, this value is dynamically changed depending on the packet receiving rate.
`RTP-JITTER-BUFFER-TALKSPURT-DELAY` Optional *Scope:* Global, Node	Time *Range:* `> 0S` *Default:* `10MS`	Specifies the time interval at which the new maximum delay of a packet in the jitter buffer is calculated.
`RTP-STATISTICS` Optional *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Specifies whether RTP statistics collection is enabled.

8.2.4 GUI Configuration

This section describes how to configure RTP in the GUI.

Configuring RTP Parameters

To configure the RTP parameters, perform the following steps:

1. Go to **Node Properties Editor > Node Configuration > Application Layer**.

2. Set **Enable RTP** to *Yes* and set the dependent parameters listed in .
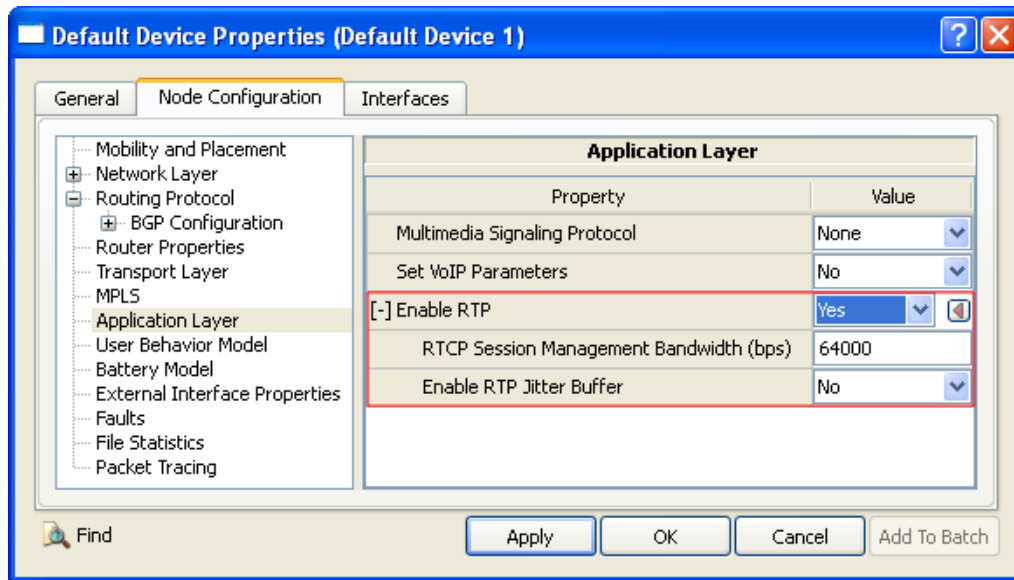
FIGURE 8-10.   Setting RTP Parameters

TABLE 8-9.   Command Line Equivalent of RTP Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
RTCP Session Management Bandwidth	Node	`RTCP-SESSION-MANAGEMENT-BANDWIDTH`
Enable RTP Jitter Buffer	Node	`RTP-JITTER-BUFFER-ENABLED`

Setting Parameters

- To enable RTP Jitter Buffer, set **Enable RTP Jitter Buffer** to *Yes*; otherwise, set **Enable RTP Jitter Buffer** to *No.*

3. If **Enable RTP Jitter Buffer** is set to *Yes*, then set the dependent parameters listed in Table 8-10.
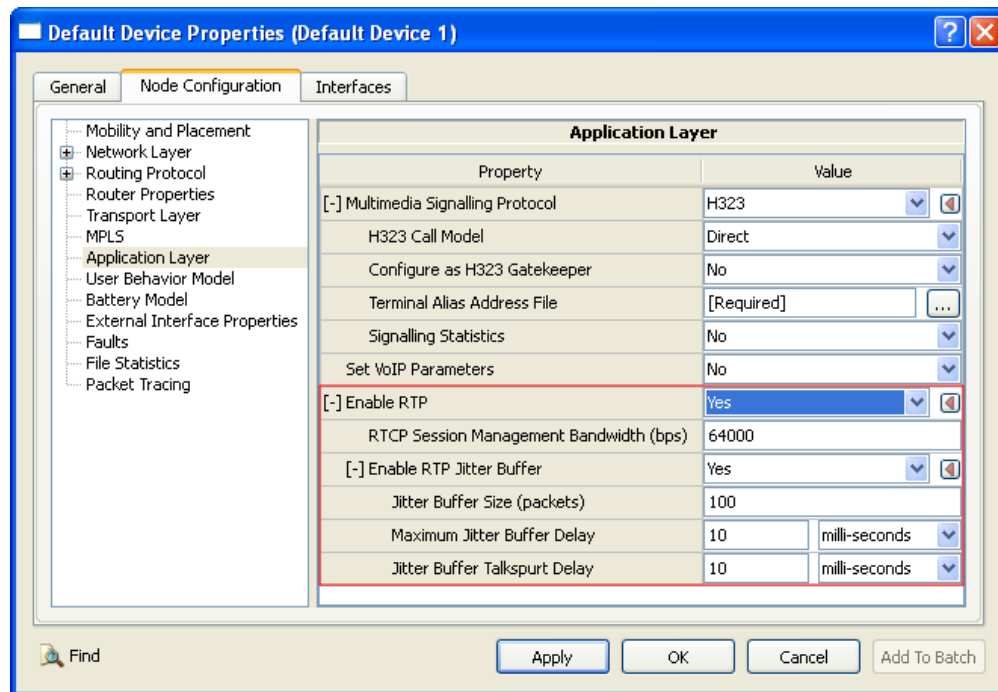
FIGURE 8-11.   Setting RTP Jitter Buffer Parameters

TABLE 8-10.   Command Line Equivalent of RTP Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Jitter Buffer Size	Node	`RTP-JITTER_BUFFER-MAXNO-PACKET`
Maximum Jitter Buffer Delay	Node	`RTP-JITTER-BUFFER-MAXIMUM-DELAY`
Jitter Buffer Talkspurt Delay	Node	`RTP-JITTER-BUFFER-TALKSPURT-DELAY`

Configuring Statistics Parameters

Statistics for RTP can be collected at the global and node levels. See Section 4.2.9 of *QualNet User's Guide* for details of configuring statistics parameters.

To enable statistics collection for application protocol RTP, check the box labeled **RTP** in the appropriate properties editor.

TABLE 8-11.   Command Line Equivalent of Statistics Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
RTP	Global, Node	`RTP-STATISTICS`

8.2.5 Statistics

Table 8-12 lists the RTP model statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 8-12.   RTP Statistics

Statistic	Description
Total Sessions	Total number of RTP sessions.
Remote Address	RTP Session Remote Address of a node.
Remote SSRC	Remote Synchronization Source (SSRC) identifier.
Max Sequence Received	Maximum sequence received.
Session Started At (s)	Time in seconds when the RTP session started.
Session Closed At (s)	Time in seconds when the RTP session closed.
Session Status	RTP session status (Active or Closed) when the session ends.
Number of Packets Sent	Total number of RTP packets sent.
Number of Bytes Sent	Total number of bytes sent.
Number of Packets Received	Total number of RTP packets received.
Number of Bytes Received	Total number of bytes received.
Number of Packets Dropped Due To Source Validation	Total number of initial packets lost for packets in probationary period.
Number of Invalid Packets Discard	Total number invalid packets discarded by receiver due to wrong format.
Average End-to-End Delay (s)	Average end-to-end delay (in seconds) for packets.
Average Jitter (s)	Average jitter (in seconds).
Total No. of Packet dropped in Jitter Buffer	Total packets dropped by the jitter buffer. **Note:** This statistic is displayed only if RTP jitter buffer is enabled.
Max. No. Consecutive Packet dropped in Jitter Buffer	Maximum number of consecutive packets dropped for maintaining the adaptive algorithm for the jitter buffer. **Note:** This statistic is displayed only if RTP jitter buffer is enabled.

Table 8-13 lists the RTCP model statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 8-13.   RTCP Statistics

Statistic	Description
Total Sessions	Total number of sessions.
Session Started At (s)	Time when the session started (in seconds).
Session Closed At (s)	Time when the session closed (in seconds).
Session Status	Session status (Active or Closed) when the session ends.
Session Management Bandwidth	Session management bandwidth utilized.
Session SSRC Count	Total Source Synchronization Source count.
Total Bye Count Received	Total RTCP BYE packets received.
Canonical Name of Source	Canonical name of the source, usually provided by the signaling protocol by the terminal alias address file.

TABLE 8-13.   RTCP Statistics (Continued)

Statistic	Description
Canonical Name of Remote Source	Canonical name of the remote source, usually provided by the signaling protocol by the terminal alias address file.
Last RTCP packet Sent Time At (s)	Last RTCP packets send time (in seconds), normally the RTPCP BYE packet.
Session Average RTCP Packet Size	Average RTCP packet size for the session.
Number of RTCP SR Sent	Total number of RTCP Sender Reports sent.
Number of RTCP SR Received	Total number of RTCP Sender Reports received.
Number of RTCP RR Sent	Total number of RTCP Receiver Reports sent.
Number of RTCP RR Received	Total number of RTCP RRs received.
Number of RTCP SDES Sent	Total number of RTCP SDESs sent.
Number of RTCP SDES Received	Total number of RTCP SDESs received.
Number of RTCP BYE Sent	Total number of RTCP BYEs sent.
Number of RTCP BYE Received	Total number of RTCP BYEs received.
Number of RTCP APP Sent	Total number of RTCP APPs sent.
Number of RTCP APP Received	Total number of RTCP APPs received.
Session Maximum Round Trip Delay Time (s)	Maximum round trip delay (in seconds) the session encountered.
Session Minimum Round Trip Delay Time (s)	Minimum round trip delay (in seconds) the session encountered.
Session Average Round Trip Time (s)	Average round trip delay (in seconds) the session encountered.
Number of Total RTCP Packets Received	Total number of RTCP Compound packets received.
Number of Total RTCP Packets Sent	Total number of RTCP Compound packets sent.

8.2.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the RTP model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/rtp. Table 8-14 lists the sub-directory where each scenario is located.

TABLE 8-14.   RTP Scenarios Included in QualNet

Scenario	Description
rtp-enabled	Shows RTP behavior when used by any application to send real time data in an ad hoc and point-to-point networks.
rtp-jitter-enabled	Shows the effect of Jitter in RTP when Jitter Buffer mechanism is enabled in RTP in a wired network.
rtp-session-management-bandwidth	Shows the RTP behavior by configuring value of Session Management Bandwidth in a wired network.

8.2.7 References

1. RFC 3550. "RTP: A Transport Protocol for Real-Time Applications." H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. July 2003.

▪ ▪

8.3 Session Initiation Protocol (SIP)

The QualNet SIP model is based on RFC 3261.

8.3.1 Description

The Session Initiation Protocol (SIP) is an alternative to H323. It is part of the Internet Engineering Task Force (IETF) standard process for transmission of real time audio, video, and data over the Internet. It is modeled on other Internet protocols such as HTTP and SMTP. SIP is an application layer signaling protocol (end-to-end) used to set up, modify, or terminate multimedia sessions in Internet.

8.3.2 Command Line Configuration

To enable SIP, include the following parameter in the scenario configuration (.config) file:

```
[<Qualifier>] MULTIMEDIA-SIGNALLING-PROTOCOL  SIP
```

The scope of this parameter declaration can be Global or Node. See Section 1.2.1.1 for a description of `<Qualifier>` for each scope.

> **Note:** We recommend all nodes of a simulated network to be SIP enabled. But if there are nodes that are not SIP enabled, then the nodes must form a connected graph.

SIP Parameters

Table 8-15 describes the SIP configuration parameters. See Section 1.2.1.3 for a description of the format used for the parameter table..

TABLE 8-15.   SIP Parameters

Parameter	Value	Description
`SIP-PROXY` Required *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	A proxy server must be present in a network irrespective of the call mode chosen. A node is configured as a SIP-PROXY by marking this parameter as Yes. QualNet currently supports inter domain calls.
`SIP-TRANSPORT-LAYER-PROTOCOL` Optional *Scope:* Global, Node	List: • `TCP` *Default:* `TCP`	SIP is independent of the underlying transport layer protocol and any transport protocol - TCP, UDP and SCRP may be used. However, QualNet currently uses only TCP. Hence only TCP can be chosen as the transport protocol.
`SIP-CALL-MODEL` Optional *Scope:* Global, Node	List: • `PROXY-ROUTED` • `DIRECT` *Default:* `DIRECT`	There are two types of call models: direct and proxy-routed.

TABLE 8-15.   SIP Parameters (Continued)

Parameter	Value	Description
TERMINAL-ALIAS-ADDRESS-FILE Required *Scope:* Global, Node	Filename	Name of the alias address file. Each terminal (user agent) may have one or more alias addresses. Currently, QualNet supports only one alias address. The format of this file is described in Section 8.3.2.1.
DNS-ADDRESS-FILE Required *Scope:* Global, Node	Filename	Name of the DNS address file. Each proxy node carries a list of other proxy nodes present in the SIP network. The format of this file is described in Section 8.3.2.2.
SIGNALLING-STATISTICS Optional *Scope:* Global, Node	List: • YES • NO *Default:* NO	Enables SIP statistics.

8.3.2.1 Format of the Alias Address File

Each node of the SIP network is represented by one or more lines, depending on the number of interfaces that the node has.

Each line in the terminal alias address file has the following format:

```
<UA-ID> <UA-IP> <host-alias> <domain> <proxy-ID> <proxy-IP-address>
```
where

`<UA-ID>`	ID of the node.
`<UA-IP>`	IP address of the node interface.
`<host-alias>`	Alias name of the host.
`<domain>`	SIP domain that provides service to this user.
`<proxy-ID>`	Node ID of the proxy configured for this domain.
`<Proxy-IP-address>`	IP address of the proxy.

Example Alias Address File

The following is an example of a line in the alias address file:

```
1   192.10.10.1   stephen   snt.com   5   192.168.100.10
```

8.3.2.2 Format of the DNS Address File

Each line in the DNS address file has the following format:

```
<proxy-node-ID> <domain-name> <proxy-interface-address>
```

where

`<proxy-node-ID>`	ID of the proxy node.
`<domain-name>`	Domain name (other than the node's own domain).
`<proxy-interface-address>`	Domain's proxy interface address as seen by this proxy.

Example DNS Address File

The following are examples of lines in a DNS address file:

```
3  a2.com  interface2
7  a1.com  interface1
```

8.3.3 GUI Configuration

This section describes how to configure SIP in the GUI.

Configuring SIP Parameters

To configure the SIP parameters, perform the following steps:

1. Go to **Node Properties Editor > Node Configuration > Application Layer**.

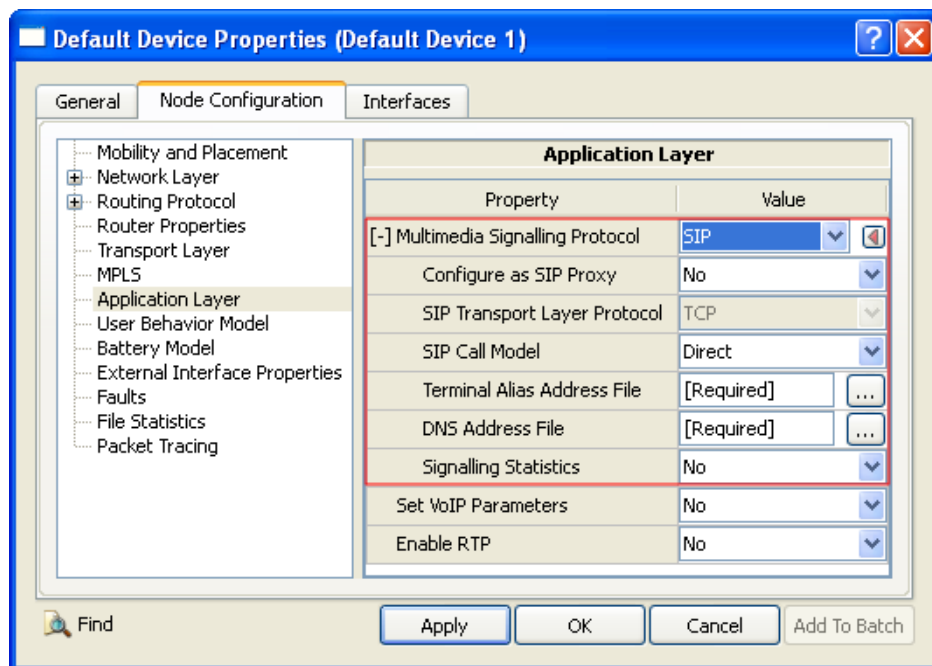2. Set **Multimedia Signaling Protocol** to *SIP* and set the dependent parameters listed in Table 8-16.

FIGURE 8-12.   Setting SIP Parameters

TABLE 8-16.   Command Line Equivalent of SIP Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
Configure as SIP Proxy	Node	SIP-PROXY
SIP Call Model	Node	SIP-CALL-MODEL
Terminal Alias Address File	Node	TERMINAL-ALIAS-ADDRESS-FILE
DNS Address File	Node	DNS-ADDRESS-FILE
Signaling Statistics	Node	SIGNALLING-STATISTICS

Setting Parameters

- To configure SIP Proxy, set **Configure as SIP Proxy** to *Yes*; otherwise, set **Configure as SIP Proxy** to *No*.

- To select SIP Call Model as Proxy Routed, set **SIP Call Model** to *Proxy Routed*; otherwise set **SIP Call Model** to *Direct*.

- Set **Terminal Alias Address File** to the name of the Address file. The format of the Address file is described in Section 8.3.2.1.

- Set **DNS Address File** to the name of the Address file. The format of the Address file is described in Section 8.3.2.2.

- To enable signaling statistics, set **Signaling Statistics** to *Yes*; otherwise, set **Signaling Statistics** to *No*.

8.3.4 Statistics

Table 8-17 list the SIP statistics that are output to the statistics (.stat) file at the end of simulation.

TABLE 8-17.   SIP Statistics

Statistic	Description
UAC part	
Number Of Invite Requests Sent	Specifies the total number of Invite requests sent by a SIP node.
Number Of Ack Requests Sent	Specifies the total number of ACK requests sent by a SIP node.
Number Of Bye Requests Sent	Specifies the total number of BYE requests sent by a SIP node.
Number Of Trying Responses Received	Specifies the total number of 100 Trying responses received by a SIP node.
Number Of Ringing Responses Received	Specifies the total number of Ringing responses received by a SIP node.
Number Of Ok Responses Received	Specifies the total number of OK responses received by SIP node.
UAS part	
Number Of Invite Requests Received	Specifies the total number of Invite requests received by a SIP node.
Number Of Ack Requests Received	Specifies the total number of ACK requests received by a SIP node.
Number Of Bye Requests Received	Specifies the total number of BYE requests received by a SIP node.
Number Of Ringing Responses Sent	Specifies the total number of Ringing responses sent by a SIP node.
Number Of Ok Responses Sent	Specifies the total number of OK responses sent by a SIP node.

TABLE 8-17.   SIP Statistics (Continued)

Statistic	Description
Proxy part	
Number Of Requests Forwarded	Specifies the total number of requests forwarded by a SIP node.
Number Of Responses Forwarded	Specifies the total number of responses forwarded by a SIP node.
Number Of Requests Dropped	Specifies the total number of requests dropped by a SIP node.
Number Of Responses Dropped	Specifies the total number of responses dropped by a SIP node.
Number Of Trying Responses Sent	Specifies the total number of 100 trying responses sent by a SIP node.
Overall	
Number Of Attempted Calls	Specifies the total number of calls attempted by a SIP node.
Number Of Attempted Calls Successful	Specifies the total number of call attempts successfully connected by a SIP node.
Number Of Calls Received	Specifies the total number of calls received by a SIP node.
Number Of Calls Rejected	Specifies the total number of calls rejected by a SIP node.

8.3.5 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the SIP model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/voip/sip. Table 8-18 lists the sub-directory where each scenario is located.

TABLE 8-18.   SIP Scenarios Included in QualNet

Scenario	Description
multi-domain-2	Shows proper call set up and release between a set of nodes belonging to two domains.
multi-domain-4	Shows proper call set up and release in multiple domains when calls are made concurrently and across several domains.
singledomain-direct-normal	Shows normal call set up and release using VOIP in single domain scenario in direct call mode.
singledomain-direct-reject	Shows what happens if REJECT is selected for a VOIP session in proxy routed call mode.
singledomain-proxy-routed-normal	Shows normal call set up and termination in a single domain with the scenario run in proxy routed mode.
singledomain-proxy-routed-timeout	Shows proper handling of call time out values and see if the call times out properly if no answer comes within the set time. The test is made here for proxy routed call mode.

8.3.6 References

1. RFC 3261. "SIP: Session Initiation Protocol" J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. June 2002.

2. "What Is SIP Introduction." Sipcenter. http://www.sipcenter.com/sip.nsf/html/What+Is+SIP+Introduction

. . . .
8.4 Voice over Internet Protocol (VoIP)

8.4.1 Description

VoIP (Voice over IP) is an IP telephony term for a set of facilities used to manage the delivery of voice information over the Internet. VoIP involves sending voice information in digital form in discrete packets rather than by using the traditional circuit-committed protocols of the Public Switched Telephone Network (PSTN). A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service by making use of the existing DSL/Cable lines, thereby reducing the overall call cost to the service provider and the end customer.

VoIP uses a wide variety of protocols to provide the above mentioned services. H323 and SIP are the broadly used protocols for call signaling and management purposes. Once the session is established, the actual data is carried over RTP packets. RTCP is a companion control protocol to RTP that is used to collect end-to-end information about the quality of the session to each participant.

In QualNet, the VoIP model has the following modules:

- Traffic generator (VoIP Initiator/Receiver)
- Call Signaling Modules (H323 and SIP)
- Media transmission over RTP/RTCP

For details of H323, SIP, and RTP/RTCP models, see Section 8.1, Section 8.3, and Section 8.2, respectively. The VoIP traffic generator module is described in this section.

The QualNet VoIP traffic generator model simulates end to end voice conversations. The initiator and receiver generate real time traffic with an exponential distribution function that simulates a real life telephone conversation.

8.4.2 Command Line Configuration

The application parameters for the VoIP traffic generator have to be specified in the application configuration (.app) file (see Section 8.4.2.1). In addition, some VoIP related parameters have to be specified in the scenario configuration (.config) file (see Section 8.4.2.2).

8.4.2.1 VoIP Parameters Specified in the Application Configuration File

The VoIP traffic generator is specified in the application configuration (.app) file using the following format:

```
VOIP <initiator> <receiver> <average talk time> <start time> <end time>
     [CALL-STATUS <call status>] [ENCODING <encoding>]
     PACKETIZATION-INTERVAL <interval>]
     [PRECEDENCE <precedence value> | DSCP <dscp value> |
       TOS <tos value>]
     [APPLICATION-NAME <application-name>]
```

   Note: All parameters must be entered on the same line.

The VoIP traffic generator parameters are described in Table 8-19. See Section 1.2.1.3 for a description of the format used for the parameter table.

TABLE 8-19. VoIP Traffic Generator Parameters

Parameter	Value	Description
`<initiator>` Required	Integer or IP Address	Node ID or IP address of the node that initiates the call.
`<receiver>` Required	Integer or IP Address	Node ID or IP address of the node to which the call is addressed.
`<average talk time>` Required	Time *Range:* `> 0S`	Average talking time when a terminal starts talking.
`<start time>` Required	Time *Range:* `> 0S`	Time when the initiating terminal sends a call establishment request to the receiver for the voice conversation.
`<end time>` Required	Time *Range:* $\geq$ `0S`	Time when the conversation ends. If end time is specified as 0, then conversation continue until the end of simulation.
`CALL-STATUS <status>` Optional	List: • `ACCEPT` • `REJECT` *Default:* `ACCEPT`	Specifies the call status. When this is set to `ACCEPT`, the receiver will receive the call. When this is set to `REJECT`, the receiver will reject the call and there will be no conversation. When not set, the call will be received by default.
`ENCODING <encoding>` Optional	List: • `G.711` • `G.729` • `G.723.1ar6.3` • `G.723.1ar5.3` • `G.726ar32` • `G.726ar24` • `G.728ar16` *Default:* `G.711`	Codec to use when transmitting RTP packets. If the user-specified string does not match any of the above mentioned values or the user does not specify any encoding scheme, the default value G.711 is used to establish the call.
`PACKETIZATION-INTERVAL <interval>` Optional	Time *Range:* `> 0S` *Default:* see description	Specifies interval at which VoIP application sends packets to RTP. **Note:** The default value is `20MS` for the codecs G.711, G.729, G.726ar32 and G.726ar24. The default value is `30MS` for G.723.1ar6.3, G.723.1ar5.3 and G.728ar16.
`PRECEDENCE <precedence-value>` Optional	Integer *Range:* `[0, 7]`	Value of the 3-bit Precedence field of the IP header for the packets generated. See note.
`DSCP <dscp value>` Optional	Integer *Range:* `[0, 63]`	Value of the 6-bit DSCP field of the IP header for the packets generated. See note.

TABLE 8-19.   VoIP Traffic Generator Parameters (Continued)

Parameter	Value	Description
TOS <tos value> Optional	Integer *Range:* [0, 255]	Value of the 8-bit TOS field of the IP header for the packets generated. See note.
APPLICATION-NAME <application-name> *Optional*	String	Name of the VoIP Traffic Generator session. This name is printed in the statistics file and statistics database.

> **Note:**   At most one of the three parameters PRECEDENCE, DSCP, and TOS can be specified. If PRECEDENCE, DSCP, and TOS are not specified, a <tos-value> of 0 is assumed.

Examples of Parameter Usage

The following are examples of configuring the VoIP traffic generator in the application configuration (.app) file:

1. Node 1 initiates a call to node 19 with average talking time of 10 seconds. The call is initiated after 1 minute into the simulation and terminates after 5 minutes from the start. The call is received by the receiver.

   ```
   VOIP 1 19 10S 1M 5M
   ```

2. This connection continues until the end of simulation and the call is accepted by the receiver.

   ```
   VOIP 3 18 10S 4M 0 CALL-STATUS ACCEPT
   ```

3. The packetization interval is explicitly set to 30 milliseconds.

   ```
   VOIP 4 17 10S 4M 5M CALL-STATUS ACCEPT PACKETIZATION-INTERVAL 30MS
   ```

4. This call from node 2 is rejected by node 20 and the call is not established.

   ```
   VOIP 2 20 10S 4M 6M CALL-STATUS REJECT PACKETIZATION-INTERVAL 20MS
   ```

5. The TOS field of the IP header is explicitly set to 0.

   ```
   VOIP 4 17 10S 4M 5M CALL-STATUS ACCEPT PACKETIZATION-INTERVAL 30MS TOS
   0
   ```

8.4.2.2 VoIP Parameters Specified in the Scenario Configuration File

Table 8-20 describes the VoIP parameters specified in the scenario configuration (.config) file.

TABLE 8-20.   VoIP Parameters Specified in Scenario Configuration File

Parameter	Value	Description
`VOIP-CONNECTION-DELAY` Optional *Scope:* Global, Node	Integer *Range:* `> 0S` *Default:* `8S`	Specifies the delay from the start of the alerting/ringing to the time that the called party receives the call.
`VOIP-CALL-TIMEOUT` Optional *Scope:* Global, Node	Integer *Range:* `> 0S` *Default:* `60S`	Specifies the maximum delay, from the initiation of the call, within which the caller can get an answer to the call. After this delay, the call will be rejected. As a rule of thumb, the call timeout should be at least four times the connection delay.

`VOIP-TOTAL-LOSS-`
`PROBABILITY`
 	
Optional
 	
Scope: Global, Node
	Real
	
	Range: `> 0`
	
	Default: `0.0507`
		Specifies total loss probability.
		
		The loss probability is used in MOS (Mean Opinion Score) calculation.

`APPLICATION-STATISTICS` *Optional* *Scope:* Global, Node	List: • `YES` • `NO` *Default:* `NO`	Indicates whether statistics are collected for application protocols (including VoIP).

8.4.3 GUI Configuration

This section describes how to configure VoIP using the GUI.

Section 8.4.2.1 describes how to configure a VoIP session. Section 8.4.2.2 describes how to configure node-level parameters fro VoIP.

8.4.3.1 Configuring a VoIP Session

To configure a VoIP session, perform the following steps:

1. Click the **VoIP** button in the **Applications** tab of the Standard Toolset.

- To set up a VoIP session between two nodes, on the canvas, click on the source node, drag the mouse to the destination node, and release. An application link is displayed between the two nodes.

- To set up a loopback VoIP session, on the canvas, double-click on the node. A ⟳ symbol is displayed next to the node.

2. Open the VoIP Properties Editor by doing one of the following:

- Right-click in the application link on the canvas and select **Properties** from the menu.

- On the canvas, right-click on the ⟳ symbol next to the node and select **Properties** from the menu.

- In the **Applications** tab of Table View, either double-click on the application row or right-click on the application row and select Properties from the menu.

3. Set the parameters listed in Table 8-21.

FIGURE 8-13.   Setting VoIP Parameters

TABLE 8-21.   Command Line Equivalent of VoIP Parameters

GUI Parameter	Command Line Parameter
Source	`<initiator>`
Destination	`<receiver>`
Average Talking Time	`<average talk time>`
Start Time	`<start-time>`
End Time	`<end-time>`
Call Status	`CALL-STATUS`
Encoding CODEC	`ENCODING <encoding>`
Packetization	`N/A`
Packetization Interval	`PACKETIZATION-INTERVAL <interval>`
Priority	`N/A`
TOS Value	`TOS <tos value>`
Session Name	`APPLICATION-NAME <application-name>`

4. If **Priority** is set to *DSCP, Precedence,* or *TOS,* set the appropriate dependent parameter listed in Table 8-22. Figure 8-14 shows how to set the dependent parameter when **Priority** is set to *DSCP.* Setting dependent parameters for the other two options is similar.
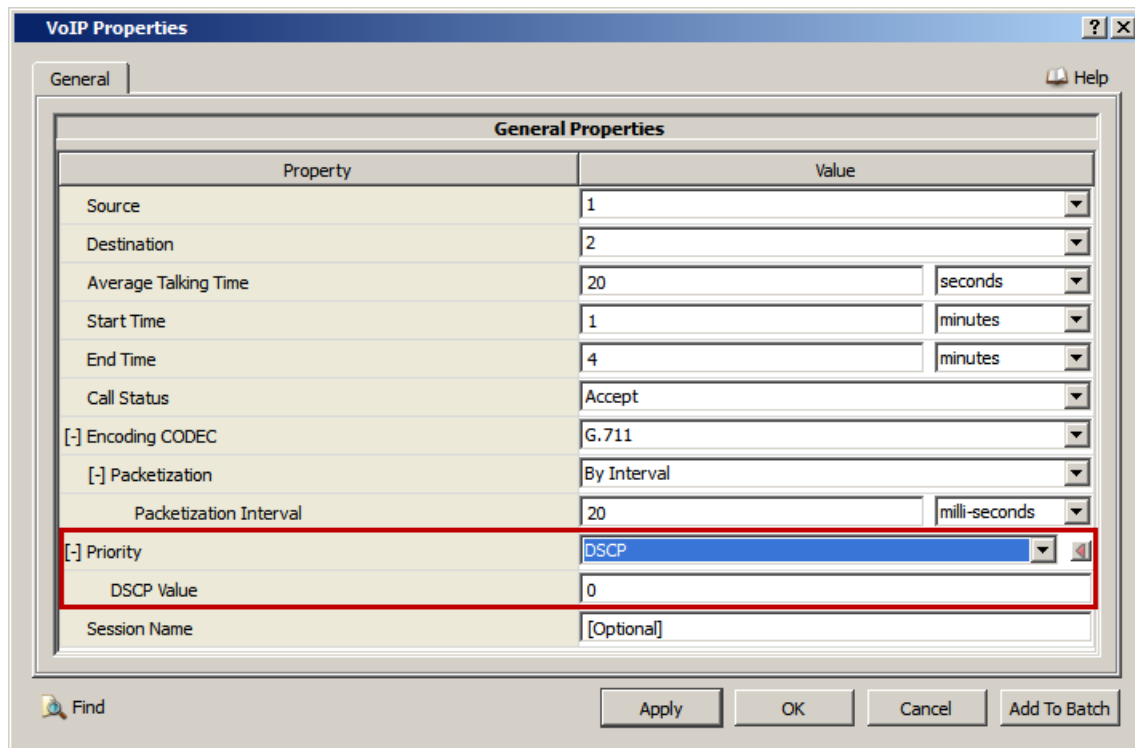

FIGURE 8-14. Setting DSCP Value

TABLE 8-22. Command Line Equivalent of VoIP QOS Parameters

GUI Parameter	Command Line Parameter
DSCP Value	`DSCP <dscp value>`
Precedence Value	`PRECEDENCE <precedence-value>`
TOS Value	`TOS <tos-value>`

8.4.3.2 Configuring VoIP Node-level Parameters

To configure the node-level parameters for VoIP, do the following:

1. Go to **Node Properties Editor > Node Configuration > Application Layer**.

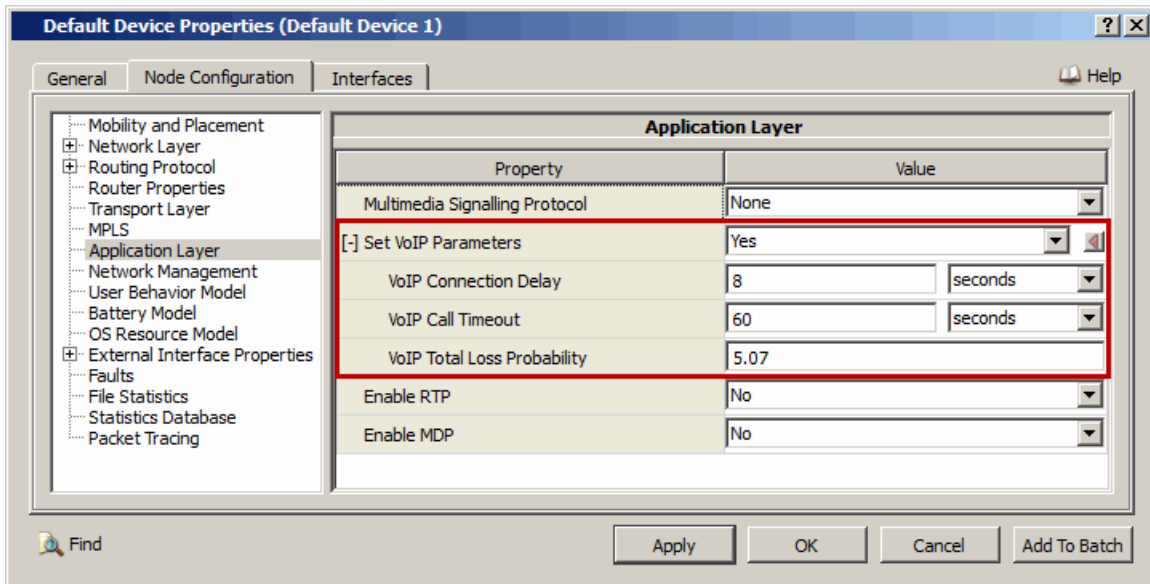2. Set **Set VoIP Parameters** to *Yes* and set the dependent parameters listed in Table 8-23.

FIGURE 8-15.   Setting VoIP Node-level Parameters

TABLE 8-23.   Command Line Equivalent of VoIP Node-level Parameters

GUI Parameter	Scope of GUI Parameter	Command Line Parameter
VoIP Connection Delay	Node	`VOIP-CONNECTION-DELAY`
VoIP Call Timeout	Node	`VOIP-CALL-TIMEOUT`
VoIP Total Loss Probability	Node	`VOIP-TOTAL-LOSS-PROBABILITY`

8.4.4 Statistics

This section describes the file, database, and dynamic statistics of the VoIP model.

8.4.4.1 File Statistics

Table 8-24 lists the VoIP statistics that are output to the statistics (.stat) file at the end of simulation
.

TABLE 8-24.   VoIP Statistics

Statistic	Description
Receiver Address	Peer address (initiator end only).
Initiator Address	Peer address (receiver end only).
Session Status	Status of session at the end of simulation (open/closed).

TABLE 8-24.   VoIP Statistics (Continued)

Statistic	Description
Session Initiated At (s)	Time in seconds, when session was initiated (initiator end only).
Unicast Session Start (seconds)	Time in seconds, when unicast session was started.
Unicast Session Finish (seconds)	Time in seconds, when unicast session was finished.
First Unicast Fragment Sent (seconds)	Time in seconds, when first unicast fragment was sent.
Last Unicast Fragment Sent (seconds)	Time in seconds, when last unicast fragment was sent.
First Unicast Fragment Received (seconds)	Time in seconds, when first unicast fragment was received.
Last Unicast Fragment Received (seconds)	Time in seconds, when last unicast fragment was received.
Total Unicast Fragments Sent (fragments)	Total number of unicast fragments sent.
Total Unicast Fragments Received (fragments)	Total number of unicast fragments received.
First Unicast Message Sent (seconds)	Time in seconds, when first unicast message was sent.
Last Unicast Message Sent (seconds)	Time in seconds, when last unicast message was sent.
First Unicast Message Received (seconds)	Time in seconds, when first unicast message was received.
Last Unicast Message Received (seconds)	Time in seconds, when last unicast message was received.
Total Unicast Messages Sent (messages)	Total number of unicast messages sent.
Total Unicast Messages Received (messages)	Total number of unicast messages received.
Total Unicast Data Sent (bytes)	Total number of unicast data bytes sent.
Total Unicast Data Received (bytes)	Total number of unicast data bytes received.
Total Unicast Overhead Sent (bytes)	Total number of unicast overhead bytes sent.
Total Unicast Overhead Received (bytes)	Total number of unicast overhead bytes received.
Average Unicast End-to-End Delay (seconds)	Average unicast end-to-end delay.
Unicast Offered Load (bits/second)	Unicast offered load.
Unicast Received Throughput (bits/second)	Unicast received throughput.
Smoothed Unicast Jitter (seconds)	Smoothed unicast jitter.
Average Unicast Jitter (seconds)	Average unicast jitter.
Total Unicast Jitter (seconds)	Total unicast jitter.
Talking Time	Total talking time in seconds.
Maximum One Way Delay (s)	Maximum one way delay (in seconds).
Minimum One Way Delay (s)	Minimum one way delay (in seconds).
Average One Way Delay (s)	Average one way delay (in seconds).
Maximum MOS	Maximum mean opinion score.
Minimum MOS	Minimum mean opinion score.
Average MOS	Average mean opinion score. This is calculated as the total MOS score divided by total number of packets received.

8.4.4.2 Database Statistics

In addition to the file statistics, the VoIP model also enters statistics in various scenario statistics database tables. Refer to *QualNet Statistics Database User's Guide* for details.

8.4.4.3 Dynamic Statistics

No dynamic statistics are supported for the VoIP model.

8.4.5 Sample Scenario

8.4.5.1 Scenario Description

Figure 8-16 shows the topology for a sample VoIP scenario. Nodes 1, 2, 3, and 4 form a wired network. Nodes 1 and 4 communicate over a wired VoIP link.
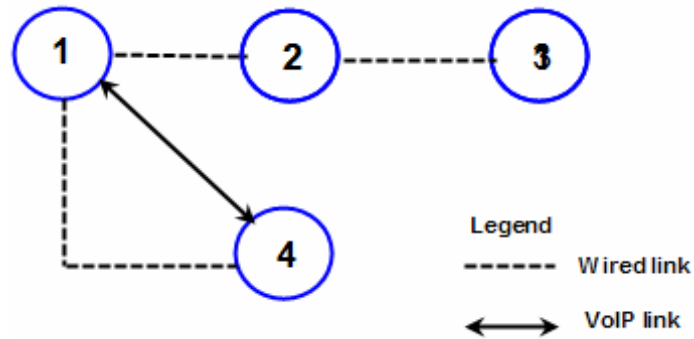

FIGURE 8-16.   Topology of the Sample VoIP Scenario

8.4.5.2 Command Line Configuration

The following steps describe how to configure the above sample scenario for command line.

1. For nodes 1 and 4, set the VoIP properties.

```
[1 4] VOIP-TOTAL-LOSS-PROBABILITY   4.07
[1 4] VOIP-CONNECTION-DELAY         9S
[1 4] VOIP-CALL-TIMEOUT             70S
```

2. For nodes 1 and 4, set the multimedia signalling protocol as H323 and set the H323 parameters.

```
[1 4] MULTIMEDIA-SIGNALLING-PROTOCOL H323
[1 4] TERMINAL-ALIAS-ADDRESS-FILE H323.endpoint
```

3. For nodes 1 and 4, enable the RTP jitter buffer and set the jitter buffer parameters.

```
[1 4] RTP-JITTER-BUFFER-ENABLED           YES
[1 4] RTP-JITTER-BUFFER-MAXNO-PACKET       200
[1 4] RTP-JITTER-BUFFER-TALKSPURT-DELAY   30MS
[1 4] RTP-JITTER-BUFFER-MAXIMUM-DELAY     20MS
[1 4] RTP-STATISTICS                      YES
[1 4] RTP-ENABLED                         YES
```

To configure the VOIP application for nodes 1 and 4, specify the following in application config file (.app):

```
VOIP 1 4 20S 15S 29S
```

8.4.5.3 GUI Configuration

Follows these steps to configure VoIP using the GUI:

1. Create a new scenario. Place four nodes as shown in topology.

2. Click the **VoIP** button in the **Applications** tab of the Standard Toolset.

3. On the canvas, click on the source node 1 and drag the mouse to the destination node 4, and release.

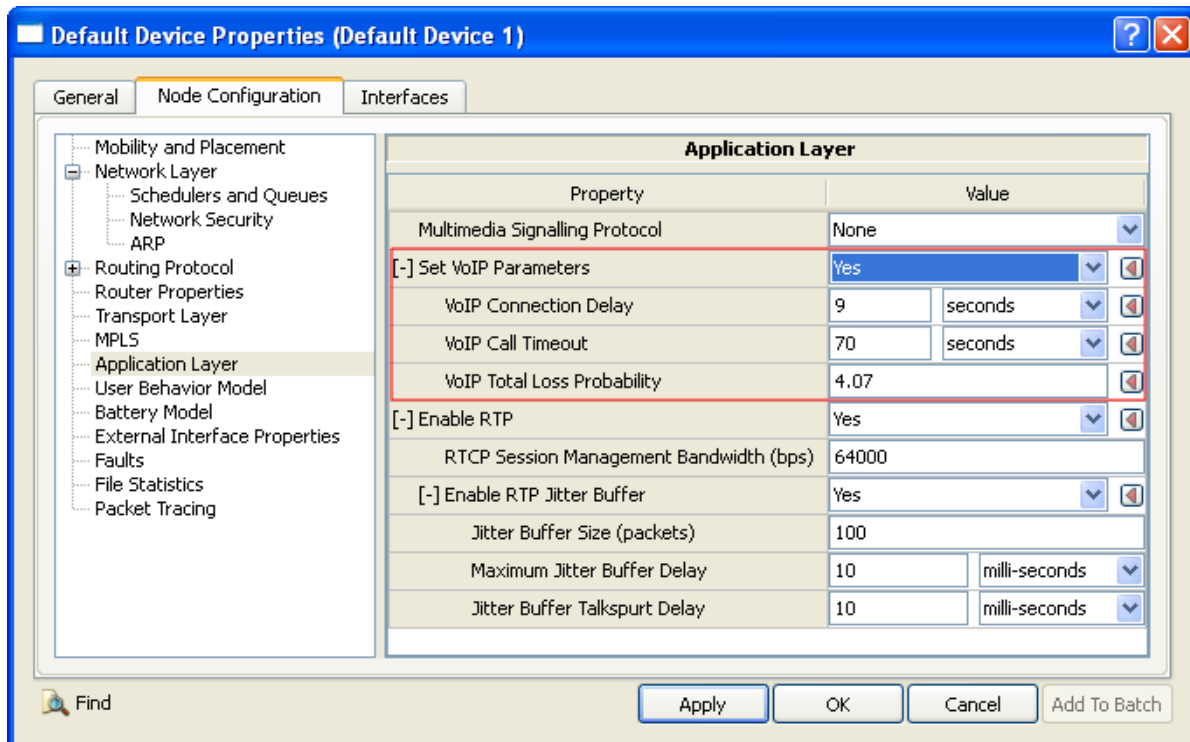4. For nodes 1 and 4, set **Set VoIP Parameters** to *Yes* and set the VoIP parameters as shown in Figure 8-17.

FIGURE 8-17.   Setting VoIP Parameters

5. For nodes 1 and 4, set **Multimedia Signalling Protocol** to *H323* and set the H323 parameters as shown in Figure 8-18.
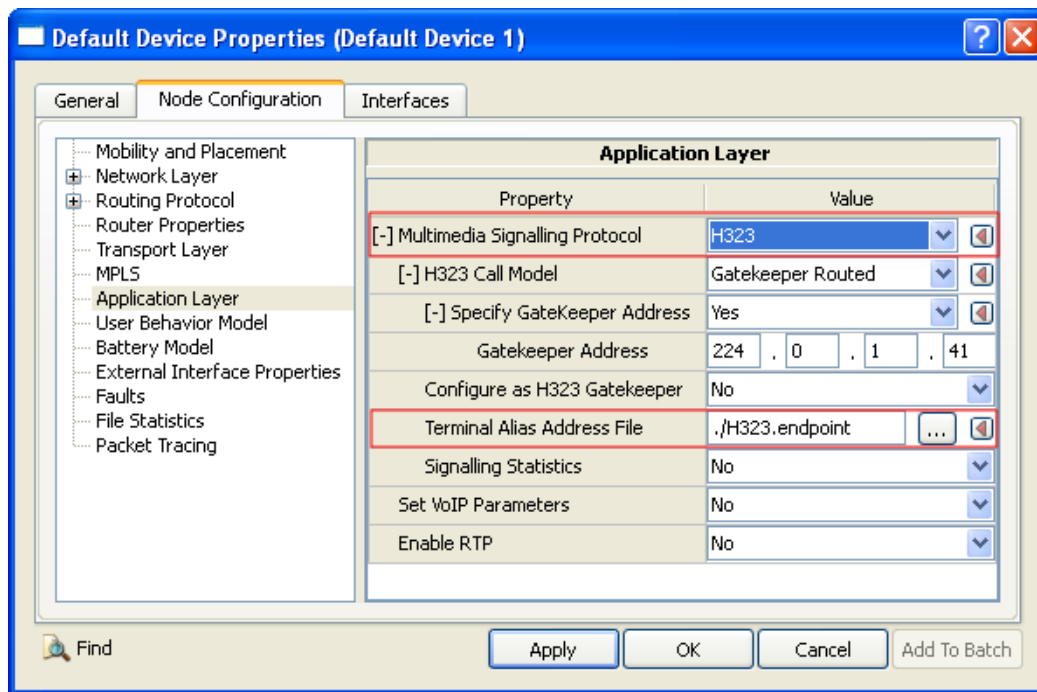

FIGURE 8-18.   Setting Multimedia Signalling Protocol

6. For nodes 1 and 4, set **Enable RTP** to *Yes* and set the RTP Jitter Buffer parameters as shown in Figure 8-19.
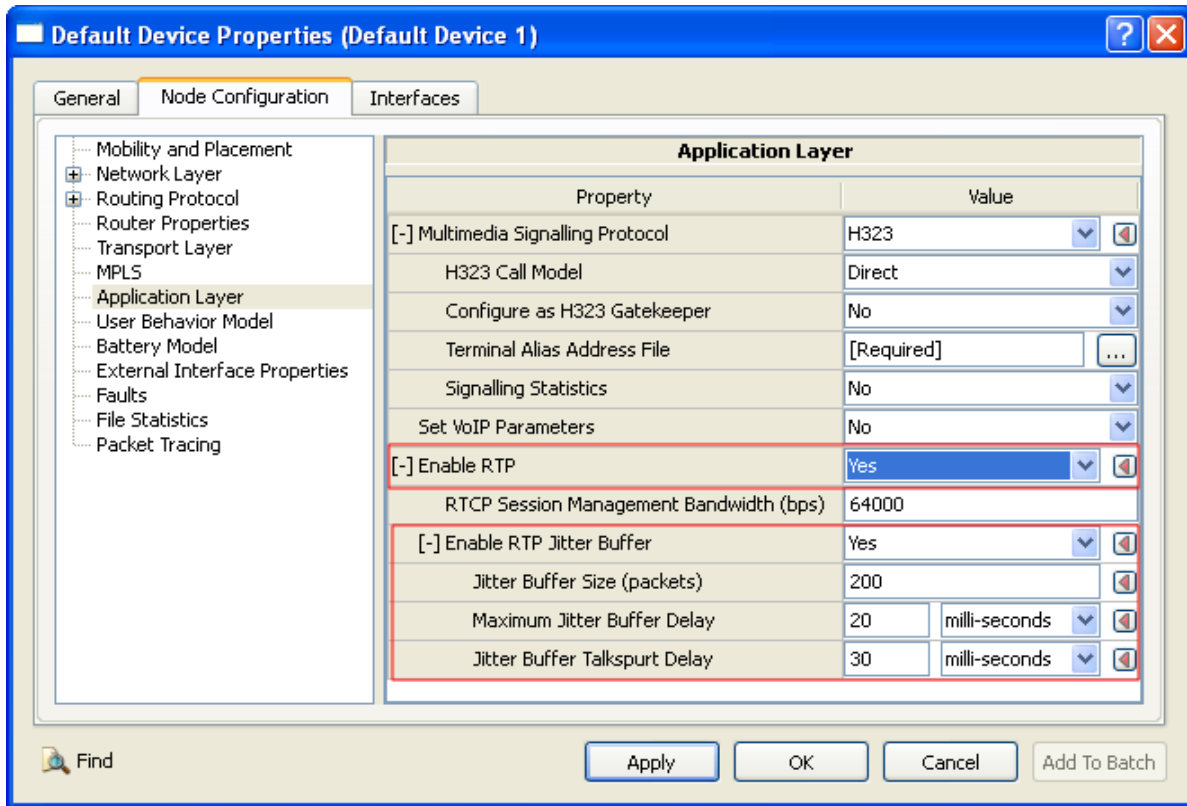

FIGURE 8-19.   Setting Jitter Buffer Parameters

8.4.6 Scenarios Included in QualNet

The QualNet distribution includes several sample scenarios for the VoIP model. All scenarios are located in the directory QUALNET_HOME/scenarios/multimedia_enterprise/voip. Table 8-25 lists the sub-directory where each scenario is located.

TABLE 8-25.   VoIP Scenarios Included in QualNet

Scenario	Description
h323/diff-encoding-scheme	Shows whether VOIP application with Jitter Buffer runs perfectly with the support of different encoding scheme and can make H323 call signaling direct from initiator to receiver.
h323/jitter-multiple-gatekeeper-direct	Shows whether VOIP application with Jitter buffer runs perfectly with the support of multiple gatekeepers and can make H323 call signaling direct from initiator to receiver.
h323/jitter-single-gatekeeper-direct	Shows whether VOIP application with Jitter Buffer can run perfectly with the support of one gatekeeper and make H323 call signaling direct from initiator to receiver.
h323/jitter-two-gatekeeper-direct	Shows whether VOIP application with Jitter Buffer runs perfectly with the support of two gatekeepers and can make H323 call signaling direct from initiator to receiver.

TABLE 8-25.   VoIP Scenarios Included in QualNet (Continued)

Scenario	Description
h323/multiple-gatekeeper-direct	Shows whether VOIP application with Jitter Buffer runs perfectly with the support of multiple gatekeepers and can make H323 call signaling direct from initiator to receiver.
h323/multiple-gatekeeper-gr	Shows whether VOIP application with Jitter buffer runs perfectly with the support of multiple gatekeepers and makes H323 call signaling through gatekeeper from initiator to receiver.
h323/no-gatekeeper	Shows whether VOIP application without Jitter Buffer runs perfectly without the support of gatekeeper.
h323/single-gatekeeper-direct	Shows whether VOIP application without Jitter Buffer can run perfectly with the support of one gatekeeper and make H323 call signaling direct from initiator to receiver.
h323/two-gatekeeper-direct	Shows whether VOIP application without Jitter Buffer runs perfectly with the support of two gatekeepers and can make H323 call signaling direct from initiator to receiver.
h323/two-gatekeeper-gr	Shows whether VOIP application without Jitter Buffer runs perfectly with the support of two gatekeepers and can make H323 call signaling through gatekeeper from initiator to receiver.
sip/multi-domain-2	Shows proper call set up and release between a set of nodes belonging to two domains.
sip/multi-domain-4	Shows proper call set up and release in multiple domains when calls are made concurrently and across several domains. The test is made here for a scenario involving 4 domains.
sip/singledomain-direct-normal	Shows normal call set up and release using VOIP in single domain scenario. The test is made for direct call mode.
sip/singledomain-direct-reject	Shows what happens if REJECT is selected for a VOIP session, that particular session should not execute but other sessions should continue normally. The test is made here for proxy routed call mode.
sip/singledomain-proxy-routed-normal	Shows normal call set up and termination in a single domain with the scenario run in proxy routed mode.
sip/singledomain-proxy-routed-timeout	Shows proper handling of call time out values and see if the call times out properly if no answer comes within the set time. The test is made here for proxy routed call mode.