Cisco Configuration Assurance Solution Audit and Analysis Flow Analysis User Guide for IT Sentinel

Software Release 11.0

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-7583-01

Cisco Configuration Assurance Solution
Audit and Analysis
Flow Analysis User Guide for IT Sentinel

Copyright

Document Copyright

Title: Flow Analysis User Guide for IT Sentinel
Part Number: D00186
Version: 13

Software Copyright

Product Name: IT Sentinel
Product Release: 11.0

Documentation Conventions

OPNET documentation uses specific formatting and typographic conventions to present the following types of information:

- Objects, examples, and system I/O
- Object hierarchies, notes, and warnings
- Computer commands
- Lists and procedures

Objects, Examples, and System I/O

- Directory paths and file names are in plain Courier typeface:

  `opnet\release\models\std\ip`

- Function names in body text are in italics:

  op_dist_outcome()

- The names of functions of interest in example code are in bolded Courier typeface:

```
/* determine the object ID of packet's creation module */
src_mod_objid = op_pk_creation_mod_get (pkptr);
```

- Variables are enclosed in angle brackets (< >):

  `<opnet_user_home>/op_admin/err_log`

Object Hierarchies, Notes, and Warnings

Menu hierarchies are indicated by right angle brackets (>); for example:

Open File > Print Setup > Properties...

Attribute hierarchies are represented by angled arrows (◢) that indicate that you must drill down to a lower level of the hierarchy:

Attribute level 1 ➘ Attribute level 2 ➘ Attribute level 3

Note—Notes are indicated by text with the word Note at the beginning of the paragraph. Notes advise you of important supplementary information.

WARNING—Warnings are indicated by text with the word WARNING at the beginning of the paragraph. Warnings advise you of vital information about an operation or system behavior.

Computer Commands

These conventions apply to Windows systems and navigation methods that use the standard graphical-user-interface (GUI) terminology such as click, drag, and dialog box.

- Key combinations appear in the form "press **<button>+x**"; this means press the **<button>** and **x** keys *at the same time* to do the operation.
- The mouse operations *left-click* (or *click*) and *right-click* indicate that you should press the left mouse button or right mouse button, respectively.

Lists and Procedures

Information is often itemized in bulleted (unordered) or numbered (ordered) lists:

- In bulleted lists, the sequence of items is not important.
- In numbered lists, the sequence of items is important.

Procedures are contained within procedure headings and footings that indicate the start and end of the procedure. Each step of a procedure is numbered to indicate the sequence in which you should do the steps. A step may be followed by a description of the results of that step; such descriptions are preceded by an arrow.

Procedure FM-1 Sample Procedure Format

1 Procedure step.

➥ Result of the procedure step.

2 Procedure step.

End of Procedure FM-1

For more information about using and maintaining OPNET documentation, see the OPNET IT Sentinel Documentation Guide.

Document Revision History

Release Date	Product Version	Chapter	Description of Change
August 2004	11.0	All	• Chapters reorganized to reflect new combined interface for IP and ATM flow analysis.
January 2004	10.5	Overview	• Added flow_analysis_network_mode preference.
		IP Reports	• Results Viewer section moved to User Guide manual.
		IP Report List	• Contents of appendix moved to IP Reports chapter.
September 2003	10.0	Revision History	• Section added to this manual.

Contents

List of Figures

List of Tables

List of Procedures

1 Overview

What is the Flow Analysis Module?

The Flow Analysis module lets you analyze IP, ATM, Frame Relay and Circuit-Switched networks. In analyzing a network, Flow Analysis considers the traffic flows in the network as well as OPNET's detailed models for network addressing and routing protocol implementation. These models are based on published standards and vendor implementations. Network planners, traffic engineers, and network operations staff can use Flow Analysis to help diagnose current network problems or help predict future network performance. Flow Analysis enables you to conduct

- Routing analysis
- Failure impact analysis
- Demand performance analysis
- Link performance analysis
- Capacity planning

With Flow Analysis, you can view the effects of traffic volume, traffic types, equipment failure, or device configuration on the operation of the network.

- By running flow analyses, you can do routing-related studies that let you visualize the route taken by each virtual circuit or traffic flow and the resulting traffic loads on the links.
- By running failure impact analyses, you can run multiple failure scenarios to identify risks such as unroutable traffic, and insufficient or incorrectly configured backup resources that can lead to congestion.
- By selectively failing network objects—manually with flow analysis or programatically with failure impact analysis—you can test the fault tolerance and quality-of-service characteristics of the network design.
- By running capacity planning analysis, you can determine if a network can deliver services in accordance with established or proposed service levels.

Failure impact analysis lets you do comparative failure studies to compare the performance of the network without failures to its performance under a variety of failure scenarios. When creating failure scenarios, you can select a set of network objects to fail one-by-one, in pairs, or all at once; or you can fail all the objects in the network one-by-one or in pairs. Using iterative techniques, the Flow Analysis module can help you answer network failure questions quickly.

After you complete an analysis, you can assess the impact of high network usage or failed network objects by studying comprehensive reports that contain information about the aggregate network and individual network objects.

Flow Analysis reports provide quick access to

- Utilization and performance statistics for each network object
- Performance reports that provide a detailed breakdown by component
- End-to-end routing for each flow or VC
- Steady-state delay estimates for each flow or VC
- Routing tables for each configured IP routing protocol on each router
- IP forwarding tables for each router
- Detailed protocol configuration and network inventory reports

Supported Technologies and Protocols

The Flow Analysis module can analyze network models that use the following technologies:

- Packet Switched (IP, ATM, and Frame Relay)
- Circuit Switched

IP Protocol Support

IP Flow Analysis supports the following:

- IP routing protocols
  - BGP—Unlimited peering between up to 30 iBGP speakers. (SP Guru and SP Sentinel have no limit to the number of iBGP speakers). Support for EBGP peers is unlimited.
  - EIGRP
  - IGRP
  - IS-IS
  - OSPF
  - RIP
- MPLS
  - Layer-2 and Layer-3 VPNs
  - VPLS
  - Juniper Fast Reroute
- Multiple processes for IGRP, EIGRP, OSPF, and IS-IS
- IP Multicasting
- Route redistribution
- Access, distribute, and prefix lists
- Route maps and route filters
- Policy routing
- Tunnel modeling
- Transparent bridging
- HSRP
- Layer-2 analysis (VLAN)
- Layer-3 aggregation
- EtherChannel

ATM Protocol Support

Flow Analysis supports the following:

- Routing protocols:
  - Distance Vector
  - PNNI
  - VNN
- PVP

Frame Relay Support

Flow Analysis supports FRF .8.

Circuit Switch Support

Flow Analysis supports N.E.T. Promina TDN.

How This User Guide is Organized

This user guide contains the following topics.

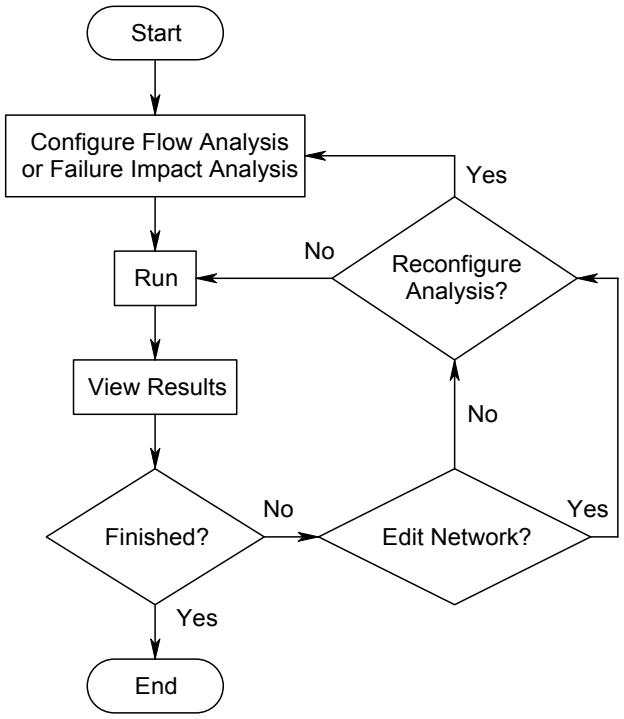
Table 1-1 User Guide Contents

Item	Description	Reference
Chapters		
Overview	Gives general information about the functions and features of Flow Analysis	Overview on page FA-1-1
Using Flow Analysis	Gives information about the menus and procedures for configuring, running, and viewing the results of flow analysis for an IP, ATM, or Frame Relay network	Using Flow Analysis on page FA-2-1
Using Failure Impact Analysis	Gives information about the procedures for configuring, running, and viewing the results of failure impact analysis for an IP, ATM, or Frame Relay network	Using Failure Impact Analysis on page FA-3-1
Using Capacity Planning	Gives information about the procedures for configuring, running, and viewing the results of capacity planning analysis	Using Capacity Planning on page FA-4-1
End of Table 1-1		

Workflow for Flow Analysis and Failure Impact Analysis

The Flow Analysis menu is accessible from the main menu of the Project Editor. You can run a flow analysis or failure impact analysis on any IP, ATM, or Circuit Switched network model that contains the supported protocols. Regardless of the supported technology or protocol your network model uses, the workflow for running a flow analysis or failure impact analysis is the same, as shown in Figure 1-1.

Figure 1-1 The Flow Analysis and Failure Impact Analysis Workflow



After you run a flow analysis or failure impact analysis, you can view the results as follows:

1) Use the Route Browser to view details about the flow or circuit paths—such as the number and order of hops or the IP address of the source node and destination node of each hop.

2) Visualize or animate link utilization and throughput in the Project Editor workspace.

3) View, print, or export the results in user-selectable, predefined reports.

4) View the results of user-selected node and link statistics in graphs.

5) Create a web report that you can view in any browser

6) Combine flow analysis or failure impact analysis with discrete event simulation.

Before You Begin…

To make sure that your working environment is set up correctly and that you have some hands-on experience before you start working with Flow Analysis, review the following sections:

- Adding and activating a Flow Analysis license
- Flow Analysis tutorials

Adding and Activating a Flow Analysis License

If you installed SP Guru, the Flow Analysis module is a standard component of the application and all necessary licenses were installed automatically.

If you are an IT Guru or Modeler user and want to use Flow Analysis, you must make sure that the Flow Analysis module is installed. You were given the choice of installing the Flow Analysis module when you installed OPNET. If you did not choose to install Flow Analysis at that time, run the installation program again (see the original installation notes) and answer “Yes” when the program prompts you to install the Flow Analysis module.

Adding a License

After the Flow Analysis module is installed, make sure that it is activated by using the Product Modules menu item in the License menu to enable the Flow Analysis module. You need to restart OPNET before this choice takes effect.

Procedure 1-1 Adding a License

1. Start OPNET.
2. In the main OPNET window, choose License > License Management.
   ➥ The License Manager window opens with information about the license server of the application you are running.
3. Click the Add License button.
   ➥ The Transaction Method window opens with a list of options by which you can complete the transaction.
4. Click on the button of the transaction method you want to use, then follow the instructions to get the license.

End of Procedure 1-1

Activating the License

Procedure 1-2 Activating the License

1. In the main OPNET window, choose License > Product Modules.
   ➥ The Select Product Modules window opens.
2. Make sure the Flow Analysis box is checked, then click OK.
3. Restart OPNET for the changes to take effect.

End of Procedure 1-2

You can get more information about licenses in License Manager on page AG-3-1.

Flow Analysis Tutorials

Two tutorials demonstrate how the Flow Analysis module works and some of its capabilities. Choose Help > Tutorials to open the Tutorial menu, then select a tutorial.

Preferences

Flow Analysis adds the following preference to IT Sentinel.

flow_analysis_network_mode

Specifies the Flow Analysis network mode, either Packet-Switched (for IP and ATM networks) or Circuit-Switched. Set this preference to the Flow Analysis mode that you use most often.

Type	string
Default Value	Packet-Switched
Constraints	Packet-Switched, Circuit-Switched

2 Using Flow Analysis

With the Flow Analysis module, you can do three types of analysis:

- Flow analysis
- Failure impact analysis
- Capacity planning

Flow analysis provides the routes, utilizations, and other performance information for a specific static scenario. The procedure for running a flow analysis on a network is in Configuring and Running a Flow Analysis on page FA-2-4.

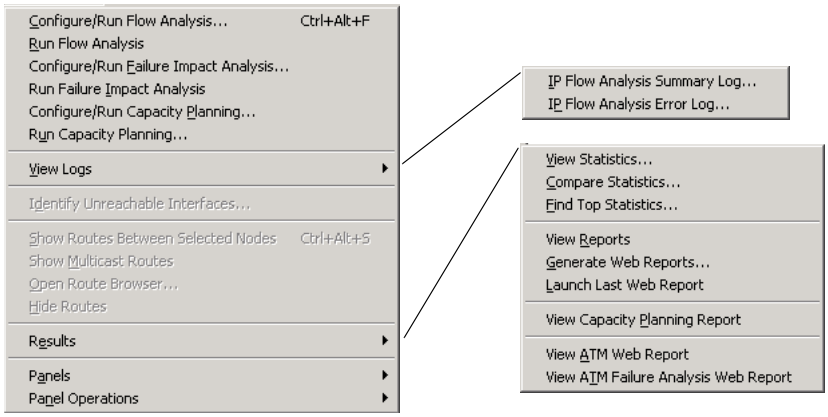
The Flow Analysis Menu

From the Flow Analysis menu, you can:

- Configure, run, and view the results of a flow analysis
- Find unreachable nodes
- Show routes between nodes

Some menu items are unavailable when you first open the Flow Analysis menu; most of these options appear dimmed because they are not available until after you have run a flow analysis.

Figure 2-1 Flow Analysis Menu



The following table describes the operations of the Flow Analysis menu.

Table 2-1 Flow Analysis Menu (Part 1 of 2)

Menu Item	Purpose
Configure/Run Flow Analysis…	Opens a dialog box from which you can set parameters for and run a flow analysis
Run Flow Analysis	Runs a flow analysis using the most-recently defined configuration
Configure/Run Failure Impact Analysis…	Opens a dialog box from which you can set parameters for and run a failure impact analysis
Run Failure Impact Analysis	Runs a failure impact analysis using the most-recently defined configuration
Configure/Run Capacity Planning...	Opens a dialog box from which you can set parameters for and run a capacity planning analysis
Run Capacity Planning...	Run a capacity planning analysis using the most-recently defined configuration

Table 2-1 Flow Analysis Menu (Part 2 of 2)

Menu Item	Purpose
View Logs > Flow Analysis Summary Log	Opens the log for the last flow analysis run on this scenario
View Logs > Flow Analysis Error Log	Opens the error log for the last flow analysis run on this scenario
Identify Unreachable Interfaces…	Generates a report that lists the unreachable interfaces in the network. You can limit the report to check interfaces of existing demands only or expand the report to include all connected interfaces that can be a source of a demand. This menu item is unavailable until after a flow analysis run.
Show Routes Between Selected Nodes	Displays routes between selected nodes in the Project Editor workspace. This menu item is not active until after a flow analysis run.
Show Multicast Routes	Displays the routes used for multicast applications in the Project Editor workspace. This menu item is not active until after a flow analysis run.
Open Route Browser…	Opens the Route Browser window so you can select network nodes to see the routes between them. This menu item is unavailable until after a flow analysis run.
Hide Routes	Unmarks routes that were selected and marked using the Show Routes… command or the Route Browser. This menu item is unavailable until after a flow analysis run.
Results > View Reports	Opens the Flow Analysis Tables in the View Results dialog box. From this window, you can select and view reports.
Results > Generate Web Reports...	Opens a dialog box from which you can create a customized report in HTML format
Results > Launch Last Web Report	Opens the last web report you created in the default web browser
Results > View Capacity Planning Report	Opens the last capacity planning report you created in the default web browser
Results > View ATM Web Report	Opens the last ATM Flow Analysis Report
Results > View ATM Failure Analysis Web Report	Opens the last ATM Failure Analysis Report
End of Table 2-1	

Configuring and Running a Flow Analysis

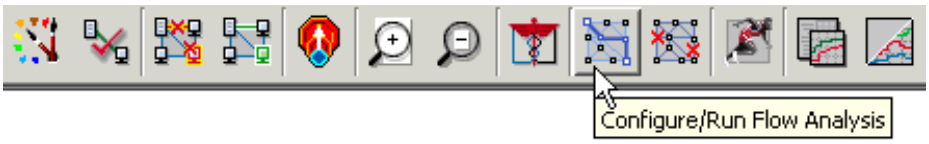
Before you run a flow analysis on a network for the first time, you should configure the parameters that Flow Analysis uses to analyze the network and collect results. You only need to configure Flow Analysis once; Flow Analysis retains the configuration settings of each scenario and uses them in subsequent runs.

You can also configure your network with failed objects and use Flow Analysis to do a manually configured (and static) failure impact analysis. This provides you with access to more detailed results of the failure condition. You must mark objects failed before you run the analysis. For information, see Failing and Recovering Network Objects on page FA-3-4.

Procedure 2-1 Configuring Flow Analysis

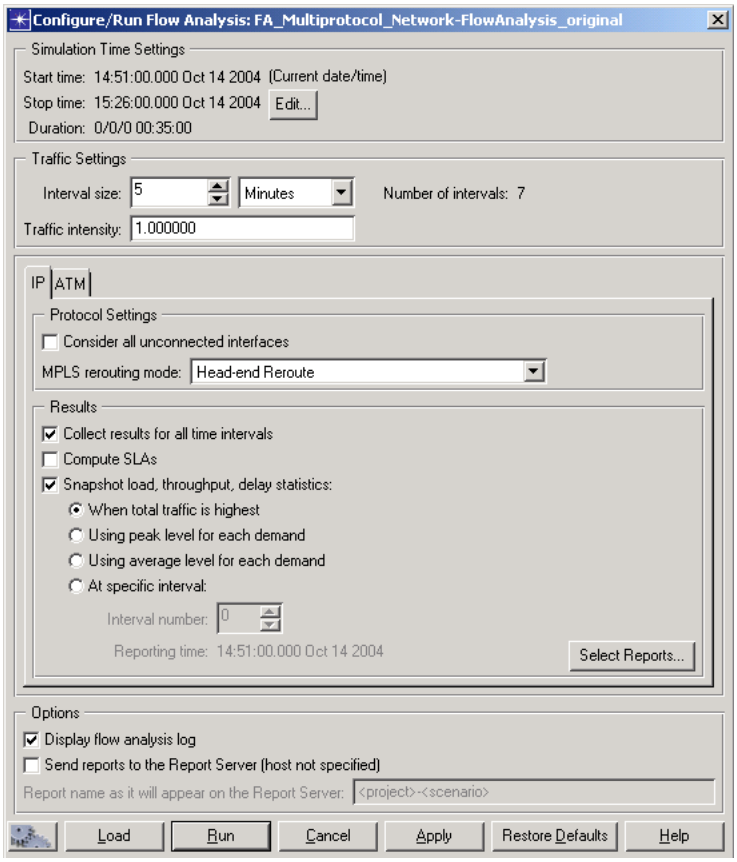
1 Click the Configure/Run Flow Analysis toolbar button. Alternatively, you can use the menu–choose Flow Analysis > Configure/Run Flow Analysis…

Figure 2-2 Configure/Run Flow Analysis Toolbar Button



➥ The Configure/Run Flow Analysis dialog box opens.

Figure 2-3 Configure/Run IP Flow Analysis Dialog Box



2 Set the parameters for the simulation in the dialog box. Changes affect only the current scenario. IP parameters appear on the IP tab and ATM parameters appear on the ATM tab. See Table 2-2, Table 2-3, and Table 2-4 for a description of the parameters.

3 Save the configuration by selecting one of the following options:

- To save and run a flow analysis immediately, click Run
- To save for a later flow analysis, click Apply and close the dialog box

End of Procedure 2-1

Table 2-2 lists the general options in the Configure/Run Flow Analysis dialog box. These flow analysis options apply to all types of networks. Options for IP and ATM networks appear in Table 2-3 and Table 2-4.

Table 2-2 Parameters in the Configure/Run Flow Analysis Dialog Box

Item Name	Description	Default
Start time	The start time of the first flow analysis interval. This value is set automatically.	Network Start Time[1]
Stop time	Sets the stop time of the last flow analysis interval; uses the format: hh:mm:ss.sss MMM DD YYYY. The Stop time is based on the data definition of the last traffic flow.	Auto-calculated
Interval size	Sets the size of the flow analysis time interval in the following selectable units: Seconds, Minutes, Hours, Days, or Weeks. Interval size is based on the intervals in the flow data. The calculated number of intervals is the smallest value that generates 100 or fewer intervals.	Auto-calculated
Traffic Intensity	Sets the traffic intensity scale factor that is applied to all traffic flows.	1.000000
Display flow analysis log	Displays the Flow Analysis Summary Log automatically after each run.	Enabled
Send reports to the Report Server	Sends a copy of the flow analysis report to the Report Server. Requires a Report Server module license.	Disabled
Report name	File name of the report sent to the Report Server. You can use two variables (“<project>” and “<scenario>”) in this field. Thus, you could enter the following string: “Mary’s <project>/<scenario>”. If you run a report from project Corporate and scenario Internetwork, the resulting report will be named “Mary’s Corporate/Internetwork”. This option is available only when the “Send reports to...” option is selected.	<project>-<scenario>
End of Table 2-2		

1. If the Network Start Time is not configured, the current time is used.

Table 2-3 describes the options available on the IP tab of the Configure/Run Flow Analysis dialog box.

Table 2-3 IP Parameters in the Configure/Run Flow Analysis Dialog Box (Part 1 of 2)

Item Name	Description	Default
Consider all unconnected interfaces	When this option is enabled, flow analysis also includes unconnected interfaces in its analysis.	Disabled
MPLS Rerouting Mode	This option configures how Flow Analysis reroutes an LSP if a node or link fails. Select an option only if you have configured MPLS in the network. • Full Reroute (All LSPs) clears the routes computed before the failure and recomputes routes for all LSPs in the network. • Head End Reroute keeps the routes that did not travel across the failed node or link and recomputes the routes that did. • Fast Reroute keeps all routes after a failure, even those that travelled across a failed node or link. The part of the route that is affected by the failure is modified to go around (and not through) the failed node.	Head-end Reroute
Collect results for all time intervals	Saves the flow analysis results for link utilization and throughput graphs and node throughput graphs.	Enabled
Compute SLAs	Enables SLA calculation during the flow analysis run for demands with SLAs	Disabled

Table 2-3 IP Parameters in the Configure/Run Flow Analysis Dialog Box (Part 2 of 2)

Item Name	Description	Default
Snapshot load, throughput, delay statistics	Sets the value on which the results of the analysis will be displayed in reports, route browsing, and link utilization: • When total traffic is highest—Flow Analysis reports on one interval within the specified time period: the interval during which the overall network traffic is heaviest. For each traffic flow, Flow Analysis calculates the average utilization over the interval. • Using peak level for each demand—for each traffic flow, Flow Analysis calculates the maximum peak rate during the specified time period. This is a "worst-case scenario," in which every traffic flow operates at its peak rate regardless of when the peak rate occurred within the specified time period (Start Time to Stop Time). • Using average level for each demand—for each traffic flow, Flow Analysis calculates the average utilization during the specified time period (Start Time to Stop Time). • At specific interval—Flow Analysis reports on the interval that you specify by setting the Interval Number. For each traffic flow, Flow Analysis calculates the average utilization over the interval. The reports generated by flow analysis cover only one interval. This parameter specifies how flow analysis chooses the interval to report on.	When total traffic is highest
Interval number	Sets the interval number to use in computing the report if At Specific interval is chosen as the value for the Measure load, throughput, delay statistics parameter. The time that corresponds to this interval is displayed as the Reporting time.	0
Select Reports...	Opens a dialog box in which you can select the reports to generate during the flow analysis. Selecting Reports on page FA-2-9.	All except node connections, forwarding table, and routing table reports
End of Table 2-3		

Table 2-4 describes the options available on the ATM tab of the Configure/Run Flow Analysis dialog box.

Table 2-4 ATM Parameters in the Configure/Run Flow Analysis Dialog Box

Item Name	Description	Default
Routing protocol	Sets the ATM protocol running in the network.	PNNI / VNN
CAC algorithm	Sets the CAC algorithm that flow analysis should use.	Built-in CAC
Circuit rerouting mode		Incremental (Affected Circuit Only)
View analysis results in web report	Generates a web report of the flow analysis results.	Disabled
Use baseline reservations from network model		Enabled
Save reservation results to network model as baseline		Disabled
End of Table 2-4		

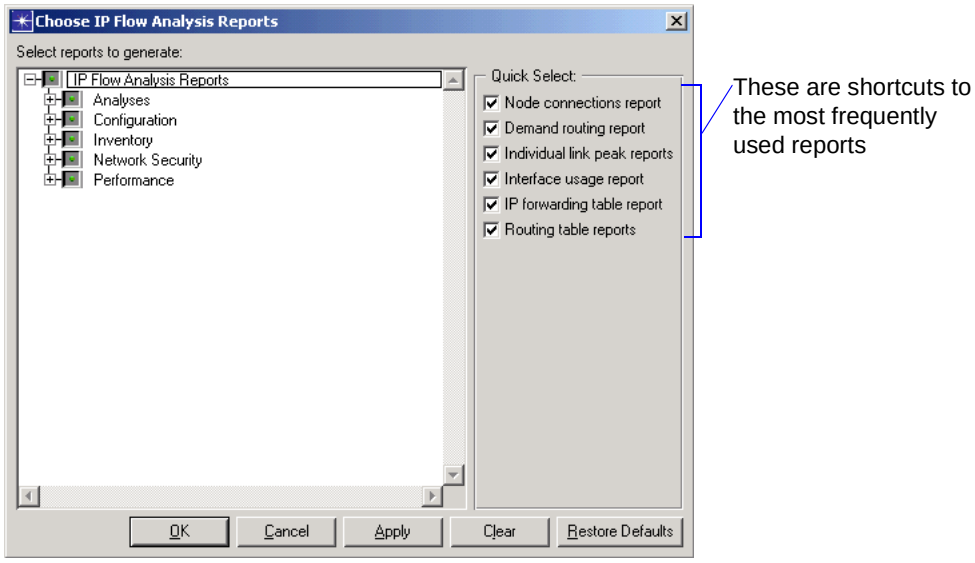
Selecting Reports

Flow Analysis does not automatically collect all possible reports and results during a simulation. By default, Flow Analysis collects all reports except the following:

- Node connections
- IP forwarding tables
- Routing tables

If you do not want to use the default selection, you can choose which reports to include when configuring the flow analysis. The Choose Flow Analysis Reports dialog box opens when you click Select Reports... on the IP tab in the Configure/Run Flow Analysis dialog box.

Figure 2-4 Choose Flow Analysis Reports Dialog Box



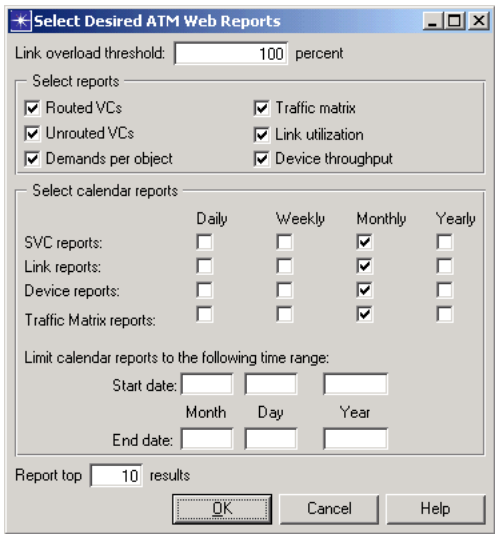
The most frequently selected reports appear in the Quick select pane on the right. To see the report(s) included in a quick selection, click Clear to remove all selections, then check the box next to the Quick select report. The included reports will be checked in the left pane.

To generate reports not included in the Quick select pane, use the treeview in the left pane to select additional reports. For a list and description of all reports, see Available IP Reports on page FA-2-19.

Selecting Detailed ATM Reports

The Select Reports button on the IP tab of the Configure/Run Flow Analysis lets you choose high-level ATM reports in addition to IP reports. You can also select detailed ATM reports by clicking on the Settings button next to the View analysis results in a web report checkbox on the ATM tab. Doing this opens the Select Desired ATM Web Reports dialog box.

Figure 2-5 Select ATM Reports Settings



In this dialog box, you can configure the following report parameters:

Table 2-5 ATM Web Report Parameters (Part 1 of 2)

Parameter	Description
Link Overload Threshold	Type the link utilization threshold percentage (default is 100). Link utilizations exceeding this threshold are reported in the Overloaded Links report in a failure impact analysis.
Select reports	Select the checkbox next to each type of report you want to generate (default is all): Routed VCs, Unrouted VCs, Flows per Object, Traffic Matrix, Utilization, and Throughput
SVC reports	Select the check box next to the time period(s) within the specified time range for which an SVC report will be generated (default is Monthly): Daily, Weekly, Monthly, Yearly
Link reports	Select the check box next to the time period(s) within the specified time range for which a Link report will be generated (default is Monthly): Daily, Weekly, Monthly, Yearly
Device reports	Select the check box next to the time period(s) within the specified time range for which a Device report will be generated (default is Monthly): Daily, Weekly, Monthly, Yearly

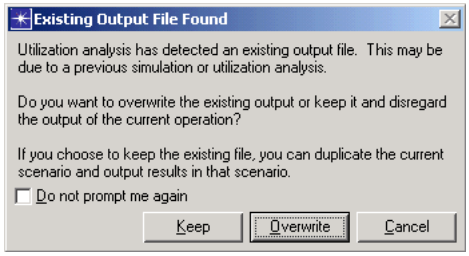
Table 2-5 ATM Web Report Parameters (Part 2 of 2)

Parameter	Description
Traffic matrix reports	Select the check box next to the time period(s) within the specified time range for which a Traffic Matrix report will be generated (default is Monthly): Daily, Weekly, Monthly, Yearly
Limit calendar reports to the following time range	Type the Start date: and End date: in the format mm/dd/yyyy (default is blank; this defines the time from the start of the earliest VC until 500 seconds after the end of the latest SVC. If there are no SVCs, the end of the range is 500 seconds after the start of the latest PVC.)
Report Top Results	Specify the number of top results for OPNET to display in the report (default is 10). Top results are the items that best match the primary sort criterion.
End of Table 2-5	

Running Flow Analysis

You can start a flow analysis from the Configure/Run IP Flow Analysis dialog box or from the Flow Analysis menu. With each run, Flow Analysis overwrites the results of the previous flow analysis on the scenario. If the Generate graph results option is checked in the current configuration, you might see the message shown in Figure 2-6. By clicking a button at the bottom of the dialog box, you can choose to overwrite the existing file, keep the existing file, or cancel the operation.

Figure 2-6 Existing Output File Found Dialog Box

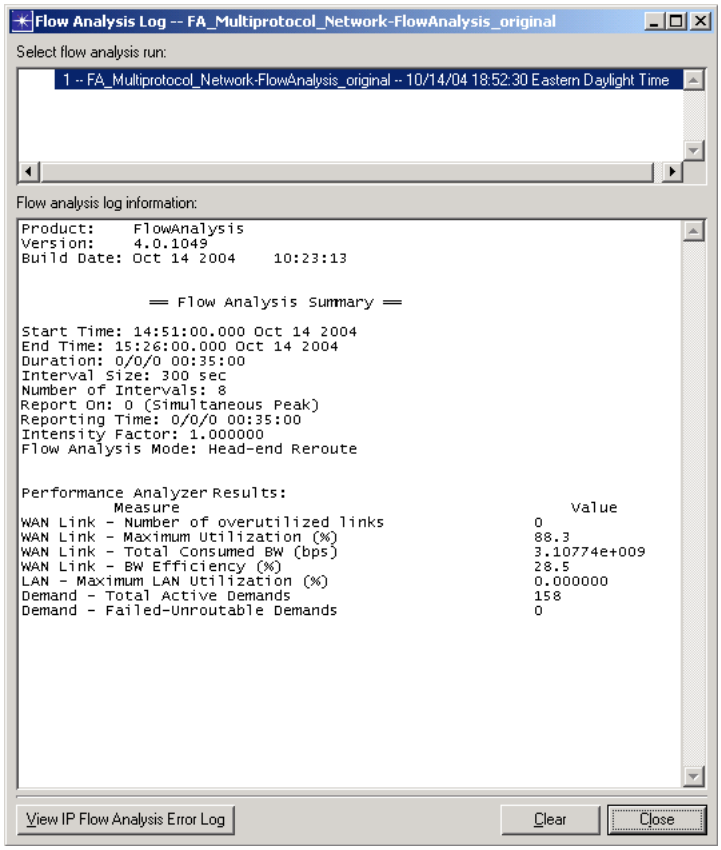


Unless you check the Do not prompt me again checkbox, this message appears each time you run a flow analysis.

Note—An environment attribute, ip_flow_analysis_out_file_preservation, determines whether or not this dialog box opens. The default setting is “Prompt.”

When the Display flow analysis log option is checked in the Configure/Run Flow Analysis dialog box, the Flow Analysis Summary Log window opens when the run is finished.

Figure 2-7 IP Flow Analysis Summary Log



This window contains the name and time of the flow analysis run that just finished, a pane with the summary log information, and a navigation button at the bottom of the window that enables you to view the Flow Analysis error log.

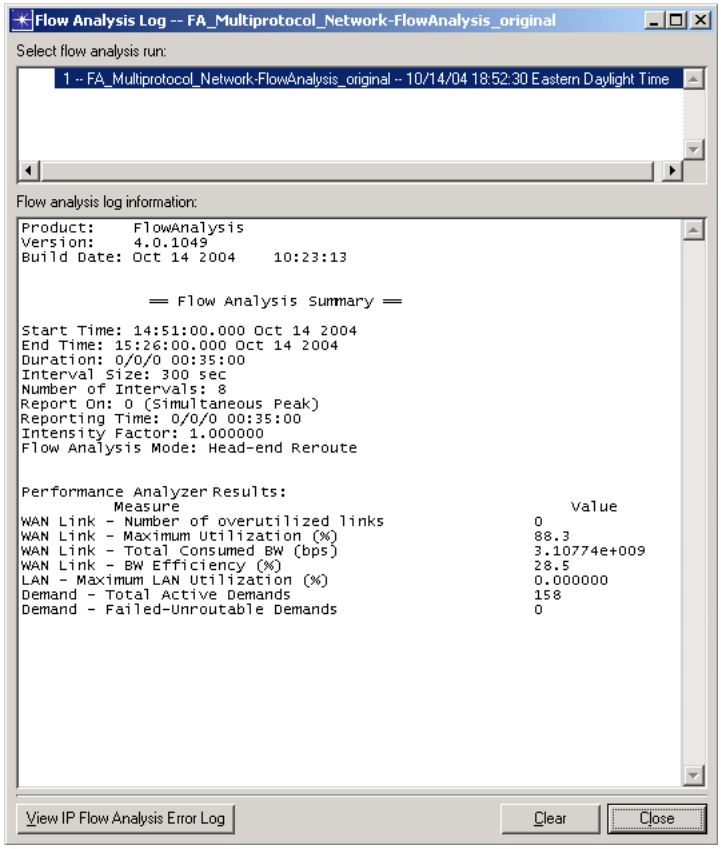
Note—For IP networks, if Flow Analysis is configured to report “At a specific interval,” each time you change the interval and click the Apply button, the selected performance measures are computed for that interval and written to the IP Flow Analysis summary log.

For more information, see Viewing the Flow Analysis Summary Log on page FA-2-14.

Viewing the Flow Analysis Summary Log

At the end of each flow analysis or failure impact analysis run, the Flow Analysis Summary Log window is available for viewing.

Figure 2-8 Flow Analysis Summary Log



There are two ways to access the Flow Analysis Summary Log within OPNET:

- Automatically—Make sure that Display flow analysis log is checked in the Configure/Run Flow Analysis dialog box; this setting opens the log window at the end of each flow analysis run.
- Manually—Choose Flow Analysis > View Logs > Flow Analysis Summary Log… from the main menu any time during a session.

The IP Flow Analysis Summary Log window contains the following information on a per-scenario basis for each flow analysis and failure impact analysis:

- The sequence and name of each run applied to the current project. Each entry contains a sequence number, the name of the project and scenario, and the date (mm/dd/yyyy) and time (hh:mm:ss time_zone) that the analysis was run.

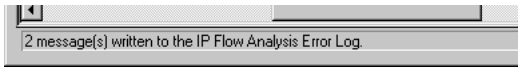
- The Flow Analysis Summary (or Failure Impact Analysis Summary) section of the log lists the configuration values that were set before the flow analysis or failure impact analysis run.
- The Performance Analyzer Results section of the log lists some of the performance results that were selected for reporting. A Flow Analysis Summary contains one set of Performance Analyzer Results. A Failure Analysis Summary contains multiple Performance Analyzer Results sections—one for the baseline scenario followed by one for each failed object or failed object pair.

Viewing the Flow Analysis Error Log

If any errors or warnings are generated during the flow analysis, IT Sentinel records them in a file named flan_error_log in the op_admin directory.

At the end of a flow or failure impact analysis operation, a message displays in the status line of the Project Editor to report the number of messages that were written to the log.

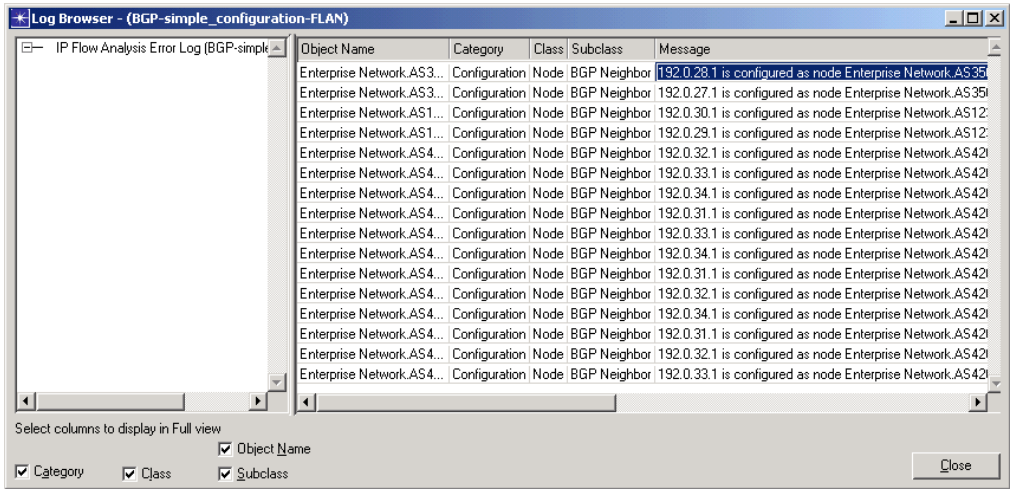
Figure 2-9 IP Flow Analysis Error Log Status Message



There are two ways to view the error log:

- From the menu, choose Flow Analysis > View Logs > Flow Analysis Error Log….
- From the IP Flow Analysis Summary Log, click View Flow Analysis Error Log.

Figure 2-10 Flow Analysis Error Log



The messages in the error log are collected according to the following rules:

- OPNET overwrites the log each time a flow or failure impact analysis is run. To save the current error log, choose File > Save As… and rename the error log before you run flow analysis or failure impact analysis; if you do not specify another directory, OPNET saves the file in the op_admin directory.
- Errors are categorized by object, category, class, and subclass.
- Switching scenarios or changing projects does not affect the contents of this log.
- Keeping the error log open during an operation that writes to the log does not refresh the open log. You must close then reopen the log to see the new entries.

After you run flow analysis or failure impact analysis, you can view results in the Results Viewer by loading selected reports from the Performance and Analyses categories. For flow analysis, you can also view utilization and throughput graphs if you selected the Save Results for Graphs option in the Configure/Run Flow Analysis dialog box before you ran the analysis.

For information about viewing reports for ATM-based networks, see Viewing ATM Web Reports on page FA-2-27.

Viewing Flow Analysis Results

This section describes the various types of results that are available after you run a flow analysis.

Flow Analysis includes the following types of results:

- Viewing Graphs on page FA-2-16
- Viewing Reports on page FA-2-17
- Viewing Network Information on page FA-2-36
- Viewing ATM Web Reports on page FA-2-27

Viewing Graphs

After a flow analysis, you can view the utilization and load statistics for the nodes and links in the network graphically. Graph data is collected by default, however, you can turn off this feature for any flow analysis by disabling the Generate graph results checkbox in the Configure/Run Flow Analysis dialog box.

Note—If you view graphs after running a failure impact analysis, you will be viewing the results of the baseline run.

On the Flow Analysis Graphs page of the View Results dialog box, you can select and show the statistics in time-varying graphs.

Procedure 2-2 Viewing Graphs of Utilization and Load Statistics for a Link

1. Choose Flow Analysis > Results > View Statistics. Alternatively, you can click on the View Results toolbar button then click on the Flow Analysis Graphs tab.

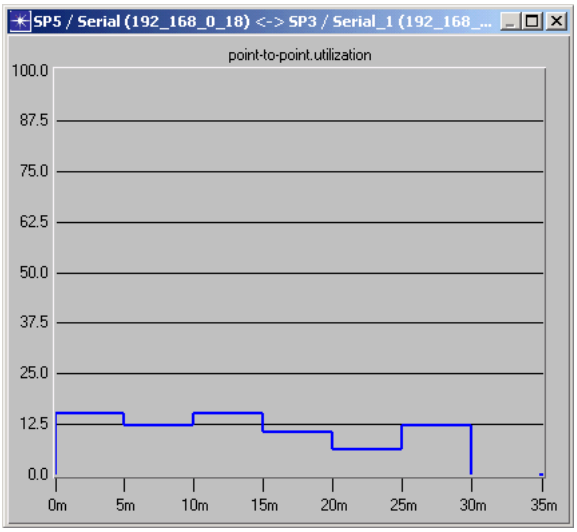
   ➥ The View Results dialog box opens to the Flow Analysis Graphs page.

2. Use the treeview to select the statistic(s) you want to see.

3. Click Show.

   ➥ The graph opens in a new window.

Figure 2-11 Graph Window



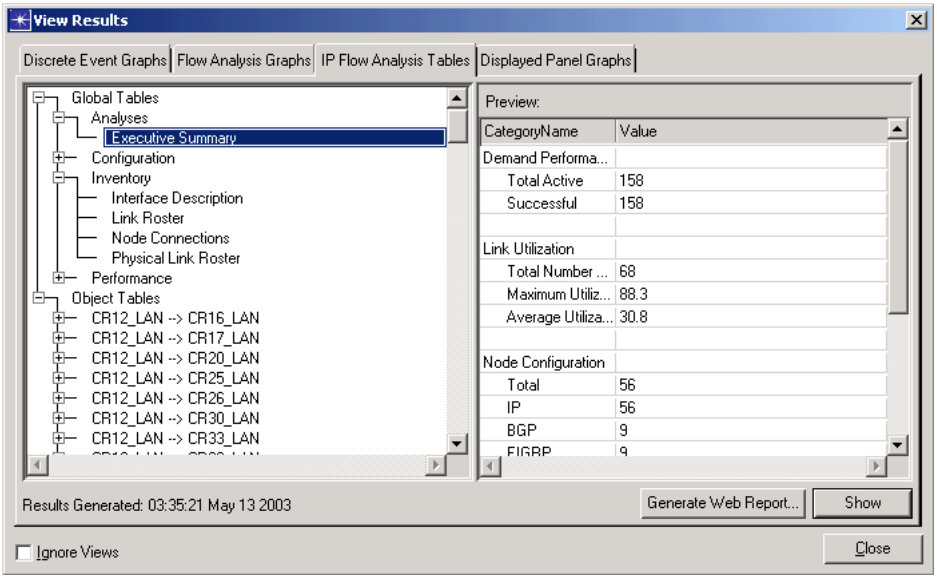
End of Procedure 2-2

Viewing Reports

This section provides an overview of the reports generated by a Flow Analysis operation. After you run an IP Flow Analysis, you can view detailed results in over 100 generated reports.

The IP Flow Analysis Tables page in the View Results dialog box lets you view any available table-based data. It lists all the available reports in the treeview in the left pane.

Figure 2-12 Flow Analysis in the View Results Dialog Box



Procedure 2-3 Viewing an IP Flow Analysis Report

1. Select Flow Analysis > Results > View Reports.

   ➥ The View Results dialog box opens at the Flow Analysis Tables tab.

2. Select the table you want to view in the treeview on the left.

3. Double-click on the report in the treeview, or click the Show button in the lower right corner.

End of Procedure 2-3

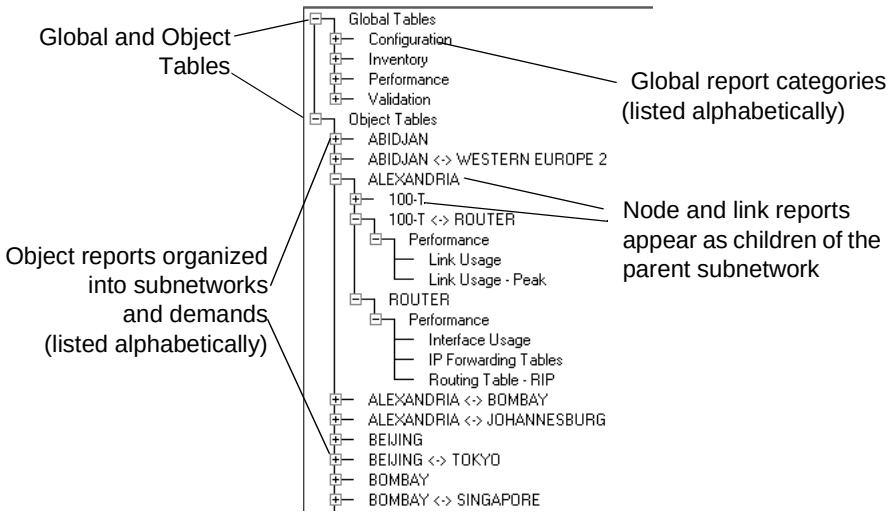
Report Categories

Flow Analysis can generate over 100 IP reports. The names of all the available reports are organized in the treeview of the View Results dialog box (Flow Analysis > Results > View Reports). The reports are divided into categories by their primary function.

The View Results dialog box organizes the reports into two major categories:

- *Global tables* that report on the entire network
- *Object tables* that report on a specific node, link, or demand. The Object Tables list all demands and subnetworks in the scenario; links and nodes are listed within each subnetwork; see Figure 2-13.

Figure 2-13 IP Report Categories in the View Results Dialog Box



Each report is registered to one category based on its primary function. The categories are defined in the following table.

Table 2-6 IP Report Categories

Category Name	Report Contents
Analyses	Reports for various automated analyses produced by SP Guru.
Configuration	Reports that contain configuration data about devices in the modeled network. Generally, these reports contain inputs used during a flow analysis.
Inventory	Reports that list network objects. Normally, inventory reports do not contain configuration or performance data. The term roster applies to reports that list network elements. Rosters are usually inventory reports.
Performance	Reports that contain results of a flow analysis that was initiated directly by running Flow Analysis.
End of Table 2-6	

Available IP Reports

The tables below list the name, category, and purpose of each report you can view in the Flow Analysis Tables page of the Results Viewer.

There are two types of reports

- Menu-Selectable Reports
- Detailed (Drill-Down) Reports

You can pick the menu-selectable reports from the treeview under Global Tables or Object Tables. Clicking on a link in a report (designated by blue text) enables you to drill down to a detailed report.

Note—Only the reports selected in the flow analysis configuration can be viewed in the Results Viewer. If there is no link for a detailed report, make sure that it is selected in the flow analysis configuration then run the flow or failure impact analysis again.

Menu-Selectable Reports A Report name followed by an asterisk (*) indicates that the report contains links to drill-down reports.

Table 2-7 Menu-Selectable Reports (Part 1 of 6)

Report Name	Category	Purpose
BGP AS Connections	Configuration	Lists information about autonomous system (AS) connectivity in the flow analysis model.
BGP Interface Configuration*	Configuration	Lists information about the configurable BGP interface-level parameters of each router in the flow analysis model.
BGP Node Configuration*	Configuration	Lists information about the configurable node-level BGP parameters of each router in the flow analysis model.
BGP Peer*	Configuration	Lists information about the BGP parameters that can be configured for each BGP peer in the flow analysis model. Unlimited peering between up to 30 iBGP speakers is allowed. (SP Guru and SP Sentinel have no limit to the number of iBGP speakers). Support for EBGP peers is unlimited.
Bridging Configuration	Configuration	Lists the configuration of transparent bridges in the flow analysis model.
Cloud Summary	Configuration	Lists information about each cloud in the flow analysis model, including the model parameters and endpoints.
Configuration Summary*	Configuration	Lists a summary of the network configuration and gives access to detailed configuration reports.
Contained Links Summary	Performance	Lists information about the allocation of link bandwidth to other circuits. There is a row in this report for every link that has at least one virtual circuit routed over it.
Data Link Summary	Configuration	Lists information about the configuration of each data link service (at various interfaces configured with the data link service) in the flow analysis model.
Demand Performance	Performance	Gives a summary of top-level information about the performance of a demand in the flow analysis and has drill-down links to detailed reports.
Demand Roster*	Inventory	Lists the demands in the flow analysis model.

Table 2-7 Menu-Selectable Reports (Part 2 of 6)

Report Name	Category	Purpose
Demand Routing*	Performance	Lists the routes and delays for the most recent flow analysis.
Destinations Advertised	Performance	Lists information about the “destinations advertised” for routers in the network.
Failed Demands–SL Criteria	Performance	Lists all the demands that failed during flow analysis because they exceeded their Service Level (SL) criteria.
Failed Demands–SL Criteria (Avg Util)	Performance	Lists all the demands that traverse links on which the average utilization is higher than the value permitted by the SL criteria for the demand.
Failed Demands–SL Criteria (Peak Util)	Performance	Lists all the demands that traverse links on which the peak utilization is higher than the value permitted by the SL criteria for the demand.
Failed Demands–SL Criteria (Hop Count)	Performance	Lists all the demands whose routes traverse more hops than permitted by the SL criteria of the demands.
Failed Demands–Unroutable*	Performance	Lists the demands that failed during flow analysis and gives the reason for each failure.
Failed LSPs*	Performance	Lists the failed Label Switched Paths (LSPs) that could not be routed across the MPLS domain and gives the reason for each failure.
Fast Reroute Parameters	Configuration	Lists the fast reroute parameters for each LSP in the network. The parameters are specified on a per-LSP basis and determine the fast reroute behavior, which is the way that detours are set up for a protected LSP.
Frame Relay Policing	Performance	Lists statistics about the frames lost as a result of policing at the endpoints of the Frame Relay Permanent Virtual Circuits (PVCs).
Frame Relay POP Roster	Inventory	Lists information about each node that is as a Frame Relay Point-of-Presence (FR POP) in the flow analysis model.
Frame Relay PVC Performance	Performance	Lists performance measures for Frame Relay Permanent Virtual Circuits (PVCs) in the flow analysis model.
Frame Relay PVC Roster	Inventory	Lists each Frame Relay Permanent Virtual Circuit (FR PVC) in the flow analysis model.
Host Roster	Inventory	Lists each node in the flow analysis model that can perform ATM host service or IP host service.
HSRP Groups	Configuration	Lists information about the HSRP configuration in the network.
IGP Neighbors	Performance	Lists the neighbors—computed by flow analysis or manually configured—for the Interior Gateway Protocols (IGPs) modeled in IP Flow Analysis.
Interface Description	Inventory	Lists the interfaces configured on the nodes in the network model. For each interface, it lists subinterfaces, if any, and descriptive text.

Table 2-7 Menu-Selectable Reports (Part 3 of 6)

Report Name	Category	Purpose
Interface Statistics	Performance	Lists a summary of the performance of the output queues of the nodes in the flow analysis model.
Interface Usage*	Performance	Lists the physical interfaces and the demands that use them for all nodes in the flow analysis model. (Subinterface usage is described in the Subinterface Usage report.)
IP Access List Summary*	Configuration	Lists the access lists configured on each router in the flow analysis model.
IP Forwarding Tables	Performance	Lists the IP forwarding tables constructed during flow analysis.
IP Route Filters*	Configuration	Lists the route filters configured for Interior Gateway Protocols (IGPs) in the flow analysis model.
IP Route Map Summary*	Configuration	Lists the route map configured for each IP router in the flow analysis model.
IP Route Redistribution*	Configuration	Lists information about how IP route redistribution is configured on all IP routers in the flow analysis model.
IP Router Address	Configuration	Lists the Layer 3 addresses configured on each interface of each router in the flow analysis model.
IP Router Roster	Inventory	Lists each node in the flow analysis model that can provide IP router service.
IP Static Routes*	Configuration	Lists information about each IP router and host in the flow analysis model that has one or more static routes.
IP Subnets	Configuration	Lists information about each IP subnet in the flow analysis model and the addresses allocated within each subnet.
IP Tunnels	Configuration	Lists information about the tunnels configured on each node in the network.
IS-IS Area Configuration	Configuration	Lists each area configured on IS-IS routers and the configuration of those areas.
LAN Delay	Performance	Lists the queueing delay, transmission delay, and total delay for each LAN on the network.
LAN Summary	Configuration	Lists information about the configuration of each physical LAN in the flow analysis model.
LAN/Cloud Roster	Inventory	Lists the physical multipoint links (physical and virtual) in the flow analysis model.
LAN/Cloud Usage*	Performance	Lists the demands routed over multipoint links (physical and virtual) between any pair of endpoints.

Table 2-7 Menu-Selectable Reports (Part 4 of 6)

Report Name	Category	Purpose
Link Roster	Inventory	Lists information about each physical and virtual point-to-point link in the flow analysis model; does not include multipoint links, such as clouds or LANs.
Link Statistics	Performance	Lists performance measures for all links in the flow analysis model.
Link Usage*	Performance	Lists all the demands routed over physical and virtual point-to-point links in the forward and return directions.
Link Utilization	Performance	Lists the utilizations and baseline utilizations of all point-to-point links in the network.
Link Utilization–Individual Link Peaks	Performance	Lists the peak utilization for each link in the network.
LSP Configuration	Configuration	Lists the configuration of all Label Switched Paths (LSPs) in the network.
LSP Rerouting	Performance	Lists the Label Switched Paths (LSPs) with routes that changed from the previous simulation. This report is populated only when flow analysis is configured to run in Incremental LSP Routes mode.
LSP Routes	Performance	Lists the current routes of all Label Switched Paths (LSPs).
LSR Configuration*	Configuration	Lists the configurations of the Label Switched Routers (LSRs) in the network.
LSR Usage	Performance	Lists the Label Switched Paths (LSPs) that traverse each Label Switched Router (LSR).
Measure Summary	Performance	Lists results of general global performance statistics such as Max Utilization and Total Demands Routed.
Network Validation	Validation	Lists the results of various flow analysis model consistency and validity checks performed by IP Flow Analysis.
Node Connections	Inventory	Lists the physical and logical connections for each node in the flow analysis model—its interfaces and subinterfaces, the links attached to each interface and subinterface, and the other endpoints on the attached links.
Node Port Summary	Configuration	Lists information about the hardware associated with each node in the flow analysis model including device model and port types.
Node Processing	Performance	Lists the performance of nodes, including routing delays, as they process demands routed through them.
Node Roster	Inventory	Lists information about each profiled node in the flow analysis model plus basic, technology-neutral information.
OSPF Area Configuration	Configuration	Lists the areas and configuration details of OSPF routers.

Table 2-7 Menu-Selectable Reports (Part 5 of 6)

Report Name	Category	Purpose
OSPF Virtual Links	Configuration	Lists information about each OSPF virtual link in the flow analysis model.
Physical Link Roster	Inventory	Lists information about each point-to-point physical link (such as T1 and T3) in the flow analysis model; does not include multipoint links such as clouds and LANs.
Router Configuration–EIGRP	Configuration	Lists information about the node and interface parameters that control the operation of EIGRP in the flow analysis model.
Router Configuration–HSRP	Configuration	Lists information about the node and interface parameters that control the operation of EIGRP in the flow analysis model.
Router Configuration–IGRP	Configuration	Lists information about routers and interfaces configured for HSRP in the flow analysis model.
Router Configuration–IS-IS	Configuration	Lists information about routers and interfaces configured for IS-IS in the flow analysis model.
Router Configuration–OSPF	Configuration	Lists information about routers and interfaces configured for OSPF in the flow analysis model.
Router Configuration–RIP	Configuration	Lists information about the node and interface parameters that control the operation of IP RIP on routers in the flow analysis model.
Router Protocol Summary	Configuration	Lists information about the network and routing protocols configured on each router in the flow analysis model. Although routers can operate under many protocols, a protocol is active only if it is configured on the router.
Router Protocols By Link	Configuration	Lists the network and routing protocols active on the endpoints of a link. This report includes all physical and virtual links for which IP is active on at least one endpoint.
Routing Domains–BGP	Performance	Lists which routers can share BGP routing information (without explicit route redistribution).
Routing Domains–EIGRP	Performance	Lists which routers can share EIGRP routing information (without explicit route redistribution).
Routing Domains–IGRP	Performance	Lists which routers can share IGRP routing information (without explicit route redistribution).
Routing Domains–IS-IS	Performance	Lists which routers can share IS-IS routing information (without explicit route redistribution).
Routing Domains–OSPF	Performance	Lists which routers can share OSPF routing information (without explicit route redistribution).
Routing Domains–RIP	Performance	Lists which routers can share RIP routing information (without explicit route redistribution).
Routing Table–BGP	Performance	Lists the routing table of each router running BGP.

Table 2-7 Menu-Selectable Reports (Part 6 of 6)

Report Name	Category	Purpose
Routing Table–EIGRP	Performance	Lists the routing table of each router running EIGRP.
Routing Table–IGRP	Performance	Lists the routing table of each router running IGRP.
Routing Table–IS-IS	Performance	Lists the routing table of each router running IS-IS.
Routing Table–OSPF	Performance	Lists the routing table of each router running OSPF.
Routing Table–RIP	Performance	Lists the routing table of each router running RIP.
Security Demand Conformance	Network Security	Lists status information for security demands that conform to the expected security type, which is permit or deny.
Security Demand Summary	Network Security	Lists the status of all security demands in the network.
Security Demand Violations	Network Security	Lists status information for all security demands that violate (do not conform to) the expected security type, which is permit or deny.
Subinterface Usage*	Performance	Lists the subinterfaces of all nodes and the demands that use each subinterface.
Traffic Engineering Subscription	Performance	Lists the traffic engineering subscription for each holding priority level of each MPLS interface in the network.
Transaction Response Time	Performance	Lists the round-trip and end-to-end measures for demands.
VLAN Summary	Performance	Lists the results of the VLAN spanning tree computation for each domain.
End of Table 2-7		

Detailed (Drill-Down) Reports

Table 2-8 Detailed (Drill-Down) Reports (Part 1 of 2)

Report Name	Category	Purpose
Failed Demand	Performance	Access this report by clicking on an item in the Demands Failed column of the Failure Impact Analysis—Demand report. This report gives details of demands that cannot be rerouted.
Link Usage–Peak	Performance	Access this report by clicking on Details in the Peak Details column of the Link Utilization–Individual Link Peaks report. This report lists details about the link peak.
Policy Statement Details	Configuration	

Table 2-8 Detailed (Drill-Down) Reports (Part 2 of 2)

Report Name	Category	Purpose
Rerouted Demand	Performance	Access this report by clicking on an item in the Demands Rerouted column of the Failure Impact Analysis—Demand report. This report gives details of demands that can be rerouted successfully.
Route Map Detail	Configuration	Access this report by clicking on an item in the Route Map Name column of the IP Route Map Summary or IP Route Redistribution report. This report contains detailed information about the selected route map.
Security Demand Routing	Network Security	
End of Table 2-8		

Web Reports

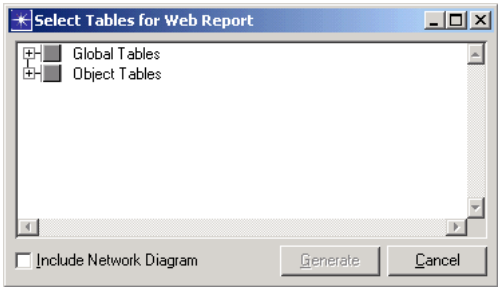
You can create a web report that contains one or more of the reports compiled in a flow or failure impact analysis.

Procedure 2-4 Generating a Flow Analysis Web Report

1. From the menu, select Flow Analysis > Results > Generate Web Reports.... Alternatively, click the Generate Web Report... button from the Flow Analysis Tables tab of the View Results dialog box.

   ➥ The Select Tables for Web Report dialog box opens.

   Figure 2-14 Select Tables for Web Report Dialog Box

2. Choose the reports you want included in the web report.

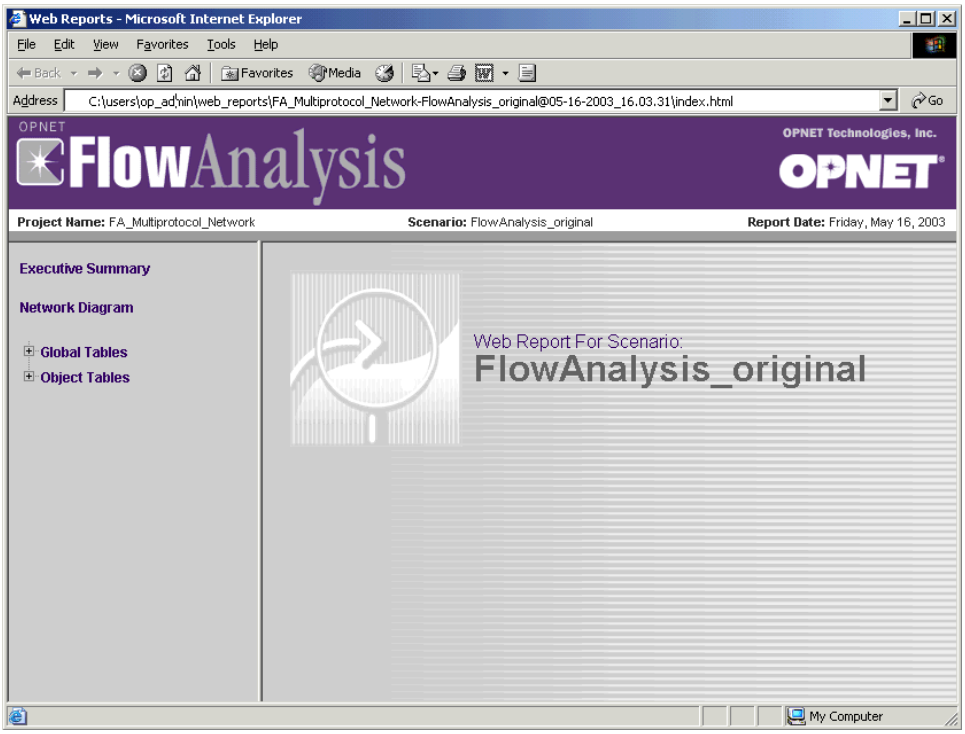
3. Check the Include Network Diagram checkbox if you want the web report to include a graphic of the network topology.

4. Click Generate.

5. Select a directory for the HTML files and click OK. The default directory is op_admin/web_reports/<project_name>-<scenario_name>@mm-dd-yyyy_hh.mm.ss.

   ➥ The web report is created and opens in the default web browser.

Figure 2-15 A Flow Analysis Web Report



End of Procedure 2-4

The web report contains links to all the reports you selected for inclusion and to an executive summary. The executive summary gives you an overview of the following categories:

- demand performance—number of routed and unroutable demands
- link utilization—average and maximum link utilization in the network
- security audit—number of successful security audits (requires the NetDoctor module)
- node configuration—breakdown of the protocols configured on nodes
- link configuration—breakdown of the protocols configured on interfaces

Viewing ATM Web Reports

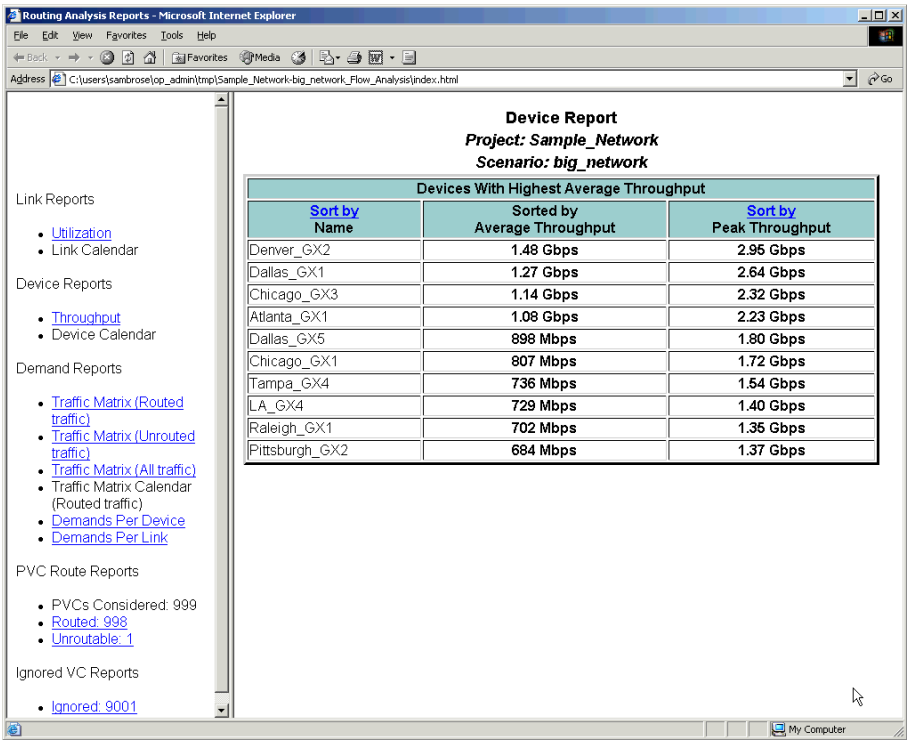
The Flow Analysis module produces web reports for ATM networks; you select the reports you want generated from the flow analysis and failure impact analysis configuration windows. For information about ATM web report parameters, see the following:

- Flow Analysis: Selecting Detailed ATM Reports on page FA-2-10
- Failure Impact Analysis: Configuring and Running a Failure Impact Analysis on page FA-3-1

After you run an analysis, the web report opens automatically in the browser with the information you selected. Each scenario retains the last flow analysis and failure impact analysis report that was generated. You can recall the last report by choosing Flow Analysis > Results > View ATM Web Report or View ATM Failure Analysis Web Report.

WARNING—If you do not enable a web report before running Flow Analysis, no report is created. If you use the Launch Last Report > Flow Analysis Report operation and a report opens, it was saved from a previous run and does not contain the current data.

Figure 2-16 Flow Analysis Report—Main Window



The main window shown in Figure 2-16 consists of two panes. The left pane has a menu of report types and the names of the reports that were created. Click on a report name to view the report in the right pane of the window. When the browser first opens, the right pane contains the Device Throughput report.

When a report displays in the right pane, the report title consists of the following information:

- Type of Report

- Project Name
- Scenario Name

When you configure flow analysis, you can specify the maximum number of links and devices to include in Link and Device reports (default is 10). For more information, see Selecting Detailed ATM Reports on page FA-2-10.

A third pane is below the report pane. It is normally empty when you open a report; if the report contains entries that are hypertext links (blue text), a detailed report opens in the third pane when you click on a link.

The data in reports is arranged in rows and columns. In some reports, you can select the column of data on which to sort. The words “Sort by” appear in blue in the headings of columns that you can sort.

In the column that is currently the sort key, the words “Sorted by” appear in black at the top of the column; a report can be sorted on only one column at a time. When you select another column, the sort label of the previously selected column changes to blue and becomes selectable again.

Figure 2-17 The Column Heading Indicates the Sort Key

Sorted by Average Utilization	Sort by Peak Utilization	Sort by Average Throughput	Sort by Peak Throughput
3.2 %	3.2 %	20.0 Mbps	20.0 Mbps
1.1 %	1.1 %	6.72 Mbps	6.72 Mbps
1.1 %	1.1 %	6.72 Mbps	6.72 Mbps

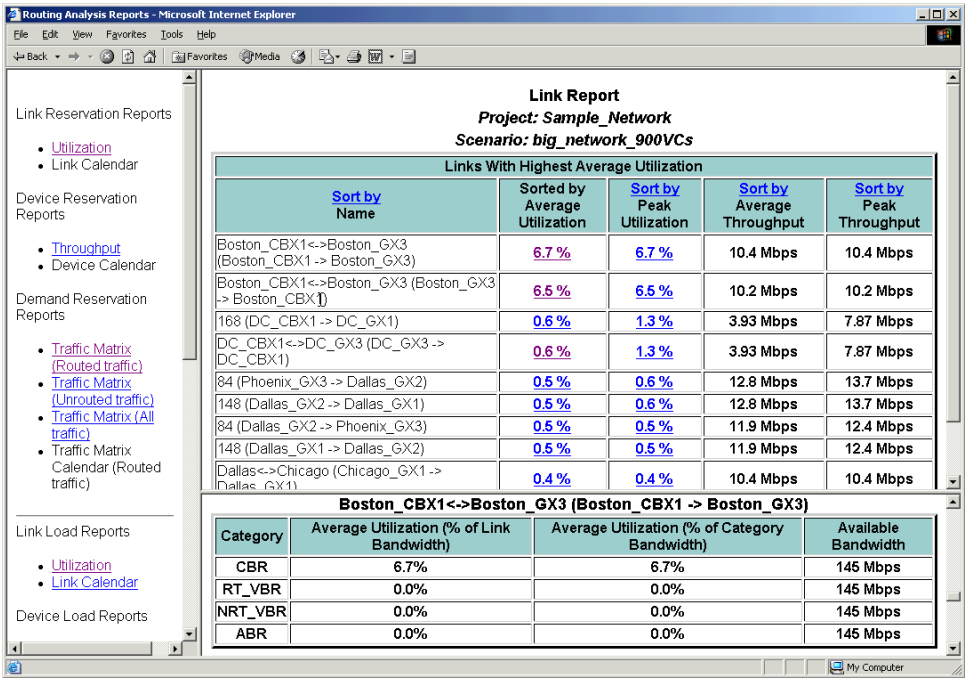
The data in a sorted column appears as follows:

- Alphabetic data is sorted in ascending order
- Numeric data is sorted in descending order

Note—The default sort order for alphabetic and numeric data cannot be changed.

When a report contains entries that are links, there is a third pane below the report. The third pane is normally empty when the report opens. By clicking on a link, you can view additional data in the detailed report that opens below the main report.

Figure 2-18 A Detailed Report Below the Main Report

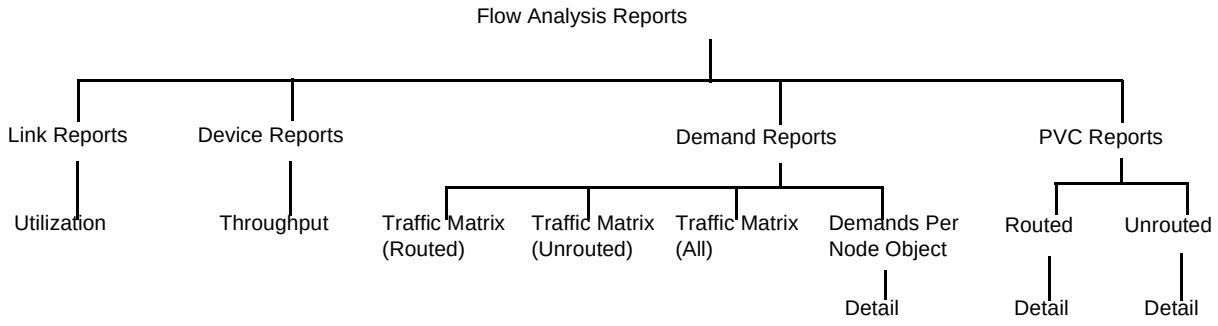


The left pane of the main window lists the types of flow analysis reports:

- Link Reports
- Device Reports
- Demand Reports
- PVC Reports

Figure 2-19 shows how the flow analysis reports are interrelated and how to navigate the report hierarchy to view the results:

Figure 2-19 Flow Analysis Report Hierarchy



Link Reports

The Link Report lists the name, utilization percentage, and throughput of the links in the network. The name of each link is derived from the two endpoints of the link; the arrows between the endpoints indicate the direction of the traffic flow: unidirectional (incoming or outgoing) or bidirectional (incoming and outgoing).

The title at the top of the table is defined by the option you selected in the Generate Flow Report dialog box: Average Utilization or Peak Utilization.

The default sort key is the Utilization column, which lists the utilization percentages of the links in descending numerical order.

Figure 2-20 Example: Sorting by Link Utilization

Link Report
Project: OPNET_Example
Scenario: ATM_reports_RECOVERED

Links With Highest Average Utilization

Sort by Name	Sorted by Average Utilization	Sort by Peak Utilization	Sort by Average Throughput	Sort by Peak Throughput
SantaClara_CA_2 -> SantaClara_CA_1	3.2 %	3.2 %	20.0 Mbps	20.0 Mbps
Cary_NC_1 -> Cary_NC_2	1.1 %	1.1 %	6.72 Mbps	6.72 Mbps
Cary_NC_2 -> Cary_NC_1	1.1 %	1.1 %	6.72 Mbps	6.72 Mbps
SANTA CLARA <-> BETHESDA (Bethesda_MD_3 -> SantaClara_CA_2)	0.5 %	0.5 %	12.4 Mbps	12.4 Mbps
CARY <-> BETHESDA (Bethesda_MD_3 -> Cary_NC_2)	0.5 %	0.5 %	12.4 Mbps	12.4 Mbps
CARY <-> BETHESDA (Cary_NC_2 -> Bethesda_MD_3)	0.5 %	0.5 %	12.4 Mbps	12.4 Mbps
SANTA CLARA <-> BETHESDA (SantaClara_CA_2 -> Bethesda_MD_3)	0.5 %	0.5 %	12.4 Mbps	12.4 Mbps
SantaClara_CA_1 -> SantaClara_CA_2	0.2 %	0.2 %	1.00 Mbps	1.00 Mbps
SantaClara_CA_2 -> SantaClara_CA_3	0.0 %	0.0 %	0.00 bps	0.00 bps
SantaClara_CA_4 -> SantaClara_CA_2	0.0 %	0.0 %	0.00 bps	0.00 bps

Device Reports

The Device Report lists the name and throughput of each device (node) in the network. You can sort this two-column report by device name or throughput; the default sort key is Throughput when the report is created.

Figure 2-21 Device Report

Device Report
Project: OPNET_Example
Scenario: ATM_reports_RECOVERED

Devices With Highest Average Throughput

Sort by Name	Sorted by Average Throughput	Sort by Peak Throughput
Bethesda_MD_3	47.8 Mbps	47.8 Mbps
SantaClara_CA_2	45.9 Mbps	45.9 Mbps
Cary_NC_2	38.3 Mbps	38.3 Mbps
SantaClara_CA_1	21.0 Mbps	21.0 Mbps
Cary_NC_1	13.4 Mbps	13.4 Mbps
Bethesda_MD_4	0.00 bps	0.00 bps
Bethesda_MD_1	0.00 bps	0.00 bps
Bethesda_MD_2	0.00 bps	0.00 bps
SantaClara_CA_3	0.00 bps	0.00 bps
SantaClara_CA_4	0.00 bps	0.00 bps

Demand Reports

There are four types of demand reports:

- Traffic Matrix (Routed Traffic)
- Traffic Matrix (Unrouted Traffic)

- Traffic Matrix (All Traffic)
- Demands Per Network Object

The Traffic Matrix reports show the aggregate demands between pairs of network nodes. These three-column reports give the Source Name, Destination Name, and Average Traffic flow for each node pair. You can choose the column you want to be the sort key; all three columns can be sorted. Average Traffic is the default sort key.

Figure 2-22 Traffic Matrix (Routed Traffic)

Aggregation of Demands (Routed Traffic)

Sort by Source Name	Sort by Destination Name	Sorted by Average Traffic
SANTA CLARA.SantaClara_CA_2	SANTA CLARA.SantaClara_CA_1	20.0 Mbps
BETHESDA.Bethesda_MD_3	CARY.Cary_NC_2	11.4 Mbps
BETHESDA.Bethesda_MD_3	SANTA CLARA.SantaClara_CA_2	11.4 Mbps
CARY.Cary_NC_2	BETHESDA.Bethesda_MD_3	11.4 Mbps
SANTA CLARA.SantaClara_CA_2	BETHESDA.Bethesda_MD_3	11.4 Mbps
CARY.Cary_NC_2	CARY.Cary_NC_1	6.72 Mbps
CARY.Cary_NC_1	CARY.Cary_NC_2	6.72 Mbps
CARY.Cary_NC_2	SANTA CLARA.SantaClara_CA_2	1.00 Mbps
SANTA CLARA.SantaClara_CA_1	SANTA CLARA.SantaClara_CA_2	1.00 Mbps
SANTA CLARA.SantaClara_CA_2	CARY.Cary_NC_2	1.00 Mbps

Figure 2-23 Traffic Matrix (Unrouted Traffic)

Aggregation of Demands (Unrouted Traffic)

Sort by Source Name	Sort by Destination Name	Sorted by Average Traffic
Bethesda_MD_4	Bethesda_MD_3	17.0 Mbps
Bethesda_MD_3	Bethesda_MD_4	17.0 Mbps
Bethesda_MD_1	Bethesda_MD_3	9.00 Mbps
Bethesda_MD_3	Bethesda_MD_1	9.00 Mbps
Bethesda_MD_3	Bethesda_MD_2	9.00 Mbps
Bethesda_MD_2	Bethesda_MD_3	9.00 Mbps

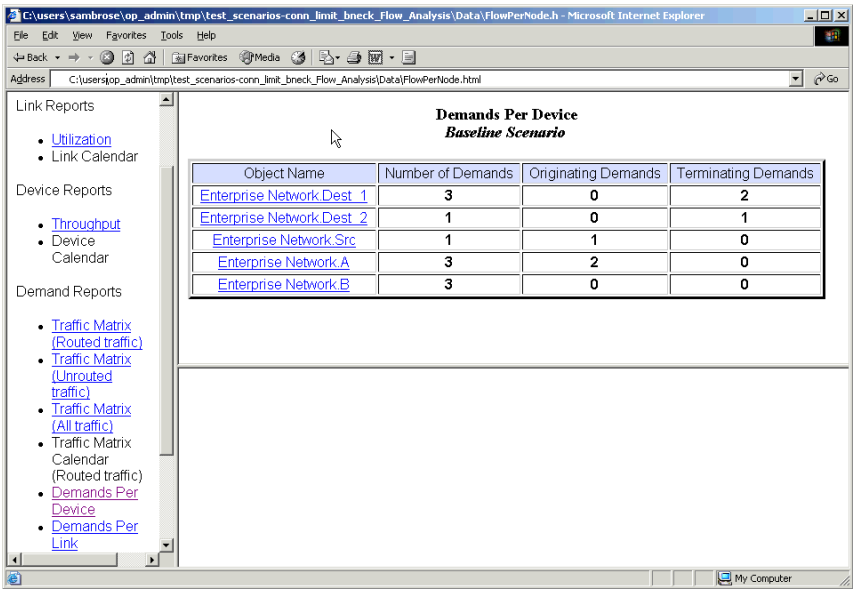
Figure 2-24 Traffic Matrix (All Traffic)

Aggregation of Demands (All Traffic)

Sort by Source Name	Sort by Destination Name	Sorted by Average Traffic
SANTA CLARA.SantaClara_CA_2	SANTA CLARA.SantaClara_CA_1	20.0 Mbps
Bethesda_MD_4	Bethesda_MD_3	17.0 Mbps
Bethesda_MD_3	Bethesda_MD_4	17.0 Mbps
CARY.Cary_NC_2	BETHESDA.Bethesda_MD_3	11.4 Mbps
SANTA CLARA.SantaClara_CA_2	BETHESDA.Bethesda_MD_3	11.4 Mbps
BETHESDA.Bethesda_MD_3	SANTA CLARA.SantaClara_CA_2	11.4 Mbps
BETHESDA.Bethesda_MD_3	CARY.Cary_NC_2	11.4 Mbps
Bethesda_MD_1	Bethesda_MD_3	9.00 Mbps
Bethesda_MD_2	Bethesda_MD_3	9.00 Mbps
Bethesda_MD_3	Bethesda_MD_1	9.00 Mbps
Bethesda_MD_3	Bethesda_MD_2	9.00 Mbps
CARY.Cary_NC_2	CARY.Cary_NC_1	6.72 Mbps
CARY.Cary_NC_1	CARY.Cary_NC_2	6.72 Mbps
CARY.Cary_NC_2	SANTA CLARA.SantaClara_CA_2	1.00 Mbps
SANTA CLARA.SantaClara_CA_1	SANTA CLARA.SantaClara_CA_2	1.00 Mbps
SANTA CLARA.SantaClara_CA_2	CARY.Cary_NC_2	1.00 Mbps

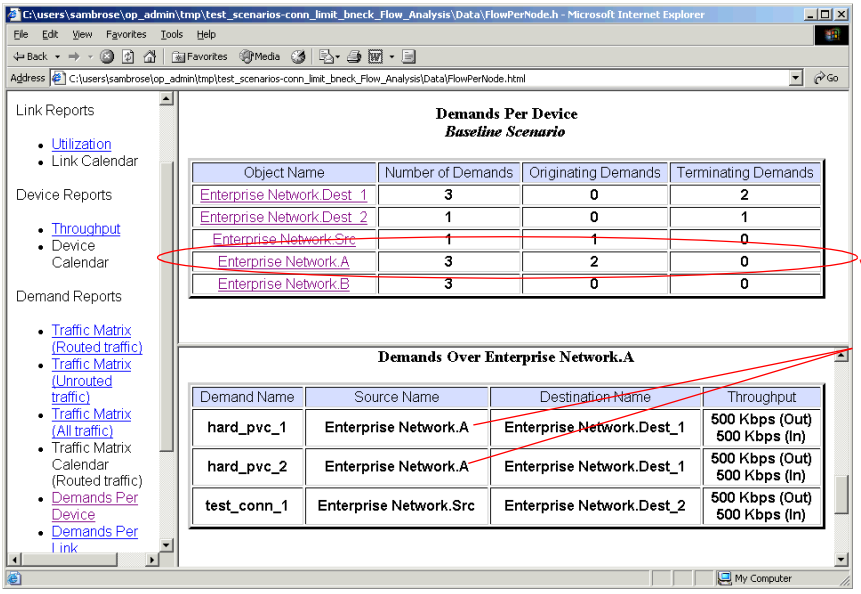
The Demands Per Device report shows a list of nodes, arranged in alphabetical order by device name, the corresponding number of demands that traverse, start at, or end at the node, the number of demands starting at the node, and the number of demands ending at the node.

Figure 2-25 Demands Per Device Report



Each device name is a link that opens a detailed report for that object when you click on it. The detailed report is a fixed-column table that lists the demand name, source name, destination name, and throughput of each demand of the selected object.

Figure 2-26 Demands Per Device—Detailed Report

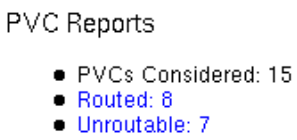


The details show that 2 demands start at this node and the third demand neither starts nor ends at the node.

Like the Demands Per Device report, the Demands Per Link report shows a list of links, arranged in alphabetical order by link name, with the corresponding number of demands that traverse the link. Clicking on a link name lists the demands that traverse the link.

PVC Route Reports

The PVC reports give information about routed and unroutable PVCs; the results summary opens under the PVC Reports heading in the left pane of the main window.



The PVCs Considered: field gives the total number of PVCs detected during flow analysis. This is for information only. The Routed: and Unroutable: fields indicate the number of PVCs detected in each category. If you click on either of these entries, the corresponding report for routed or unroutable PVCs opens in the right pane of the main window.

The title at the top of the table indicates the subject of the report—PVCs with Highest Throughput. This table has a 3-column, fixed format. It does not allow sorting on different columns.

The columns list the name of the PVC, the Hop Count, the Average Throughput, and the Peak Throughput.

Throughput is the subject of the table, so the Average Throughput column is the primary sort key; because the throughput data is numeric, it sorts in descending order. ATM demands can have different traffic specifications in each direction of the demand. The source-to-destination traffic specification is the throughput in the Out direction and the destination-to-source specification is the throughput in the In direction.

Figure 2-27 PVC Report

PVC Report

Project: Sample_Network

Scenario: demand_seq_by_bw

PVCs with highest average throughput				
Sort by Name	Sort by Connection ID	Sort by Hop Count	Sorted by Average Throughput	Sort by Peak Throughput
cbr10pcr (Enterprise Network.source -> Enterprise Network.dest)	N.A	2	10.0 Mbps (Out) 10.0 Mbps (In)	10.0 Mbps (Out) 10.0 Mbps (In)
cbr5pcr (Enterprise Network.source -> Enterprise Network.dest)	N.A	2	5.00 Mbps (Out) 5.00 Mbps (In)	5.00 Mbps (Out) 5.00 Mbps (In)
cbr4pcr (Enterprise Network.source -> Enterprise Network.dest)	N.A	2	4.00 Mbps (Out) 4.00 Mbps (In)	4.00 Mbps (Out) 4.00 Mbps (In)
cbr3pcr (Enterprise Network.source -> Enterprise Network.dest)	N.A	3	3.00 Mbps (Out) 3.00 Mbps (In)	3.00 Mbps (Out) 3.00 Mbps (In)
cbr2pcr (Enterprise Network.source -> Enterprise Network.dest)	N.A	3	2.00 Mbps (Out) 2.00 Mbps (In)	2.00 Mbps (Out) 2.00 Mbps (In)

You can see more information about each entry in the PVC column by clicking on the PVC name. When you click on a PVC name, a detailed report opens below the main report; the title of the detailed report is the link name of the PVC you selected.

The detailed report lists the name of each hop in the specified PVC and gives the node and interface names of the source node and destination node that are the endpoints of the PVC.

Figure 2-28 PVC Report—Detailed Report

cbr10pcr (Enterprise Network.source -> Enterprise Network.dest)

	Source Node		Destination Node	
Hop	Name	Link	Name	Link
1	Enterprise Network.source	source <-> node_41	Enterprise Network.node_41	source <-> node_41
2	Enterprise Network.node_41	node_41 <-> dest	Enterprise Network.dest	node_41 <-> dest

The report for Unroutable PVCs is a two-column list; each entry contains the PVC name followed by the source and destination endpoints of the circuit; the direction of the traffic flow (unidirectional or bidirectional) is indicated between the endpoints. The second column contains the Reason for Failure of the PVC.

Figure 2-29 Unroutable PVCs Report

PVC Report

Project: Sample_Network

Scenario: demand_seq_by_qos1

Unroutable PVCs			
Total Unroutable Throughput: 3.00 Mbps (Out) / 3.00 Mbps (In)			
PVC	QoS Category	Throughput	Reason For Failure
abr_1 (source -> dest)	ABR	1.00 Mbps (Out) 1.00 Mbps (In)	Insufficient Resources
abr_2 (source -> dest)	ABR	1.00 Mbps (Out) 1.00 Mbps (In)	Insufficient Resources
abr_3 (source -> dest)	ABR	1.00 Mbps (Out) 1.00 Mbps (In)	Insufficient Resources

Each entry in the Unroutable PVCs list is a link that opens a detailed report below the list when you click on it. The title of the detailed report is the link name of the unroutable PVC that you selected.

The detailed report has 2 columns that list the Possible Bottleneck and the Reason that the PVC could not be routed.

Figure 2-30 Unroutable PVCs—Detailed Report

abr_1

Possible Bottleneck	Reason
source <-> dest	At node source: ReqBW (1.00 Mbps) > AvBW (0.00 bps)
source <-> dest	At node dest: ReqBW (1.00 Mbps) > AvBW (0.00 bps)

Viewing Network Information

In addition to viewing results flow analysis results as a report in tabular format, you can also view certain flow analysis results in the project workspace.

Visualizing MPLS LSP Routes

When you use Flow Analysis on MPLS networks, you can view the routes computed for the LSPs in the Connections Browser.

Procedure 2-5 Viewing LSP Routes in the Connections Browser

1 Run Flow Analysis.

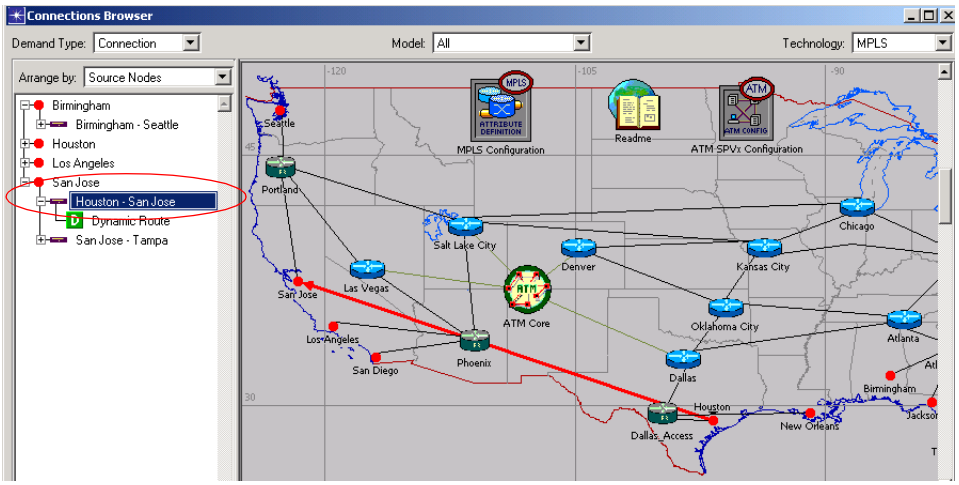
Note—An SP Guru license is needed to run a flow analysis on an MPLS network.

2 Open the Connections Browser (Topology > Open Connections Browser...).

3 Set the Technology to MPLS. This filters out other types of objects and makes it easier to find the LSPs.

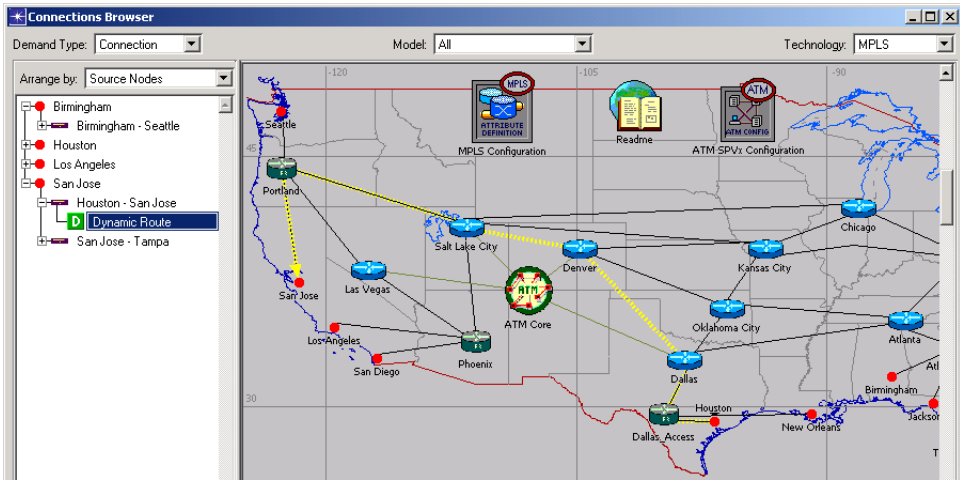
4 Click on an LSP in the treeview on the right.

➥ The LSP is displayed in the workspace.



5 Click on Dynamic Route under the LSP in the treeview.

➥ The route used by the LSP is drawn in the workspace.



End of Procedure 2-5

Visualize Link Loads

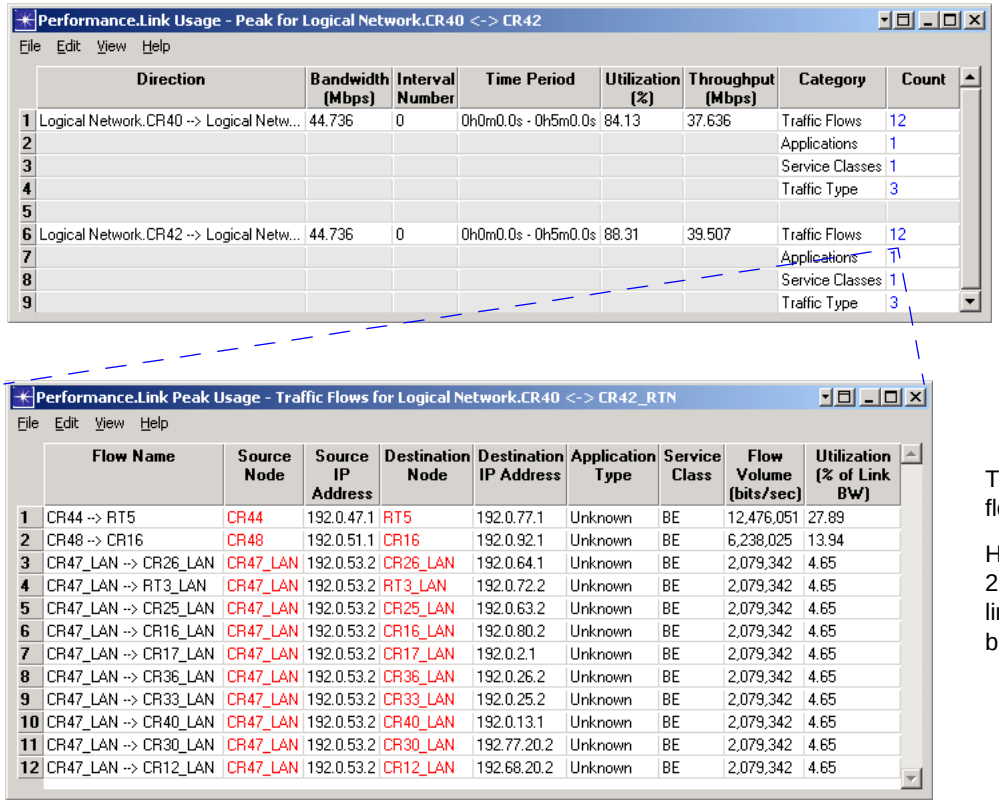
You can use the Visualize Link Loads feature to see overall link-load levels quickly and to pinpoint overloaded links. When link load visualization is turned on, colored arrows appear over the links. The line color indicates the load level (as a percentage of total capacity) in each direction; the line thickness indicates the total link capacity.

Link Usage Reports

You can view information about the traffic flowing across a link by looking at its usage report. This report is available by selecting View Link Peak Usage (Flow Analysis) from the link's object menu. The object menu is available when you right-click on a link.

The link usage report reports on the peak use of the link, when total traffic is highest. This is true even if another criterion was used for reporting during the flow analysis.

Figure 2-31 Link Usage Report



Performance.Link Usage - Peak for Logical Network.CR40 <-> CR42

File Edit View Help

	Direction	Bandwidth (Mbps)	Interval Number	Time Period	Utilization (%)	Throughput (Mbps)	Category	Count
1	Logical Network.CR40 --> Logical Netw...	44.736	0	0h0m0.0s - 0h5m0.0s	84.13	37.636	Traffic Flows	12
2							Applications	1
3							Service Classes	1
4							Traffic Type	3
5								
6	Logical Network.CR42 --> Logical Netw...	44.736	0	0h0m0.0s - 0h5m0.0s	88.31	39.507	Traffic Flows	12
7							Applications	1
8							Service Classes	1
9							Traffic Type	3

Performance.Link Peak Usage - Traffic Flows for Logical Network.CR40 <-> CR42_RTN

File Edit View Help

	Flow Name	Source Node	Source IP Address	Destination Node	Destination IP Address	Application Type	Service Class	Flow Volume (bits/sec)	Utilization (% of Link BW)
1	CR44 --> RT5	CR44	192.0.47.1	RT5	192.0.77.1	Unknown	BE	12,476,051	27.89
2	CR48 --> CR16	CR48	192.0.51.1	CR16	192.0.92.1	Unknown	BE	6,238,025	13.94
3	CR47_LAN --> CR26_LAN	CR47_LAN	192.0.53.2	CR26_LAN	192.0.64.1	Unknown	BE	2,079,342	4.65
4	CR47_LAN --> RT3_LAN	CR47_LAN	192.0.53.2	RT3_LAN	192.0.72.2	Unknown	BE	2,079,342	4.65
5	CR47_LAN --> CR25_LAN	CR47_LAN	192.0.53.2	CR25_LAN	192.0.63.2	Unknown	BE	2,079,342	4.65
6	CR47_LAN --> CR16_LAN	CR47_LAN	192.0.53.2	CR16_LAN	192.0.80.2	Unknown	BE	2,079,342	4.65
7	CR47_LAN --> CR17_LAN	CR47_LAN	192.0.53.2	CR17_LAN	192.0.2.1	Unknown	BE	2,079,342	4.65
8	CR47_LAN --> CR36_LAN	CR47_LAN	192.0.53.2	CR36_LAN	192.0.26.2	Unknown	BE	2,079,342	4.65
9	CR47_LAN --> CR33_LAN	CR47_LAN	192.0.53.2	CR33_LAN	192.0.25.2	Unknown	BE	2,079,342	4.65
10	CR47_LAN --> CR40_LAN	CR47_LAN	192.0.53.2	CR40_LAN	192.0.13.1	Unknown	BE	2,079,342	4.65
11	CR47_LAN --> CR30_LAN	CR47_LAN	192.0.53.2	CR30_LAN	192.77.20.2	Unknown	BE	2,079,342	4.65
12	CR47_LAN --> CR12_LAN	CR47_LAN	192.0.53.2	CR12_LAN	192.68.20.2	Unknown	BE	2,079,342	4.65

This table lists the individual flows that traverse the link.

Here, the first flow represents 27.89% of the traffic on the link, not 27.89% of the total bandwidth of the link.

Viewing Traffic Routes

After you run a flow analysis, you can view the routes between IP nodes graphically in the Project Editor two ways:

- Between two nodes–see Viewing Traffic Routes Between Two Selected Nodes on page FA-2-39
- Using the Route Browser–see Viewing Traffic Routes Using the Route Browser on page FA-2-40

You can also view a list of the routes computed for traffic flows in the Demand Routing report of the Results Viewer.

For ATM networks, the values that flow analysis reports as link utilizations are based on the link load or on the reservations for that link, depending on the option selected in the Configure/Run Flow Analysis dialog box.

For IP networks, the routes reported in the Demand Routing report are data plane routes whereas the routes computed using the two methods described in this section are control plane routes. Only demand routing reports account for policy routing configured in the network.

Viewing Traffic Routes Between Two Selected Nodes

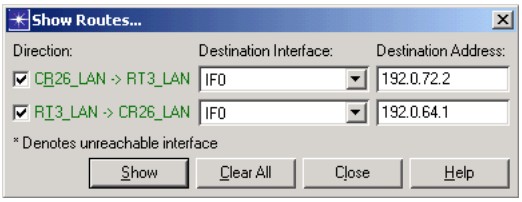
You can see the least-cost path(s) computed during the most recent flow analysis between two nodes quickly by using the Flow Analysis > Show Routes Between Selected Nodes menu operation. If you ran the flow analysis with objects marked as failed, you might want to see how traffic is routed between two objects in the presence of the marked failures.

Procedure 2-6 Showing the Routes Between Two Nodes

1. Hold down the Control key and select two nodes in the network.
2. Choose Flow Analysis > Show Routes Between Selected Nodes.

   ➥ The Show Routes dialog box opens.

Figure 2-32 Show Routes Dialog Box



3. Select the direction of the route you want to show. To show routes in both directions, select both checkboxes.
4. For each direction chosen in step 3, select the interface to route to from the pull-down menu. The route will be computed between the loopback interface of the source node to the destination interface you specify in this step.

   ➥ The address of the selected interface appears in the Destination Address field.
5. Click Show.

   ➥ The routes—which are computed according to the configured routing protocols—appear in the workspace as bold, dotted lines along the links between the selected nodes.

6 Click Clear All to remove the route visualization from the workspace. You can click Close or repeat steps 3-5 to show routes to other interfaces on the same nodes.

End of Procedure 2-6

Procedure 2-6 produces a unidirectional or bidirectional view of the routes between the two nodes you selected according to the view option that is set in the IP Flow Analysis Visualization dialog box.

- If route visualization is set to unidirectional, the route is shown in one direction (from A-to-B or from B-to-A); press Control+Shift+S to change the direction. If there are multiple least cost paths in any direction, they are all displayed.
- If visualization is set to bidirectional, the routes from A-to-B and B-to-A appear at the same time in two different colors. If there is more than one least-cost path in any direction, all are shown.

Viewing Traffic Routes Using the Route Browser

The Route Browser shows information about the routes between two specified nodes in the network. You can use the Route Browser to see information about the route taken: the number of hops the route takes, the names of intermediate nodes, and the IP addresses of the interfaces for each hop.

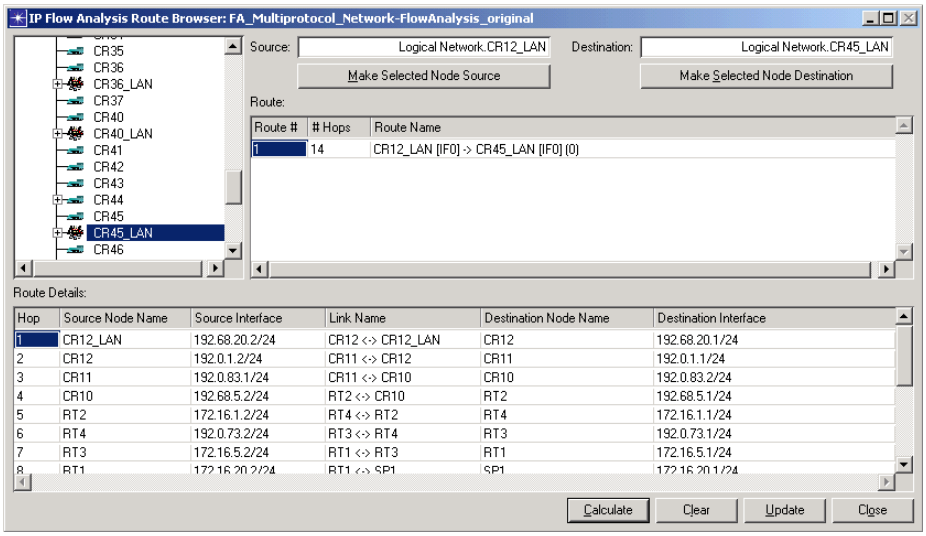
When the Route Browser calculates a route between two nodes, it displays the details of each hop in the Path Details area and draws the route in the Project Editor workspace at the same time.

Procedure 2-7 Viewing Traffic Routes

1 Choose Flow Analysis > Open Route Browser….

➥ The Flow Analysis Route Browser dialog box opens.

Figure 2-33 Flow Analysis Route Browser Window



2 In the Route Browser, select the node you want to be the source by clicking on the node name in the treeview, then clicking the Make Selected Node Source button. For IP networks, the nodes that you select as endpoints for a route must be IP-capable devices.

➥ The name of the selected node appears in the Source field.

Note—The nodes that you select as endpoints for a route must be IP-capable devices.

3 Select the node you want to be the destination by clicking on the node name in the tree view, then clicking the Make Selected Node Destination button.

➥ The name of the selected node appears in the Destination field.

4 Click Calculate to see a list of the least-cost paths between the selected source and destination nodes in the Path area.

5 Click on a route entry to show more detailed information in the Path Details area.

- The source node name and source interface for each hop
- The link traveled at each hop
- The destination interface for each hop

You can select each node and link in the path (listed in the Route Browser) to highlight the corresponding object in the Project Editor.

End of Procedure 2-7

You can keep the Route Browser open while you make changes to the network topology and do flow analysis runs. If you run a flow analysis while the Route Browser is open, you must click Update in the browser to load the routes from the last run.

3 Using Failure Impact Analysis

Failure impact analysis enables you to compare network performance measures over a set of user-defined failure scenarios. Failure impact analysis is also useful for determining which traffic flows are most sensitive to failure. The procedure for running a failure impact analysis on a network is in Configuring and Running a Failure Impact Analysis on page FA-3-1.

After you identify a failure scenario of interest, you can fail objects manually (see Failing and Recovering Network Objects on page FA-3-4) and drill down into more detail with a flow analysis run.

Configuring and Running a Failure Impact Analysis

When you run a failure impact analysis, OPNET runs a flow analysis first to establish a performance baseline against which to compare failure impact analysis results. This initial run is called the baseline run and consists of a flow analysis on the network without node failures. Next, objects are failed according to the way you configured the failure impact analysis.

Before you run failure impact analysis, configure flow analysis the way you want it; this configuration is used for the iterative flow analysis runs that make up the failure impact analysis. See Procedure 2-1 Configuring Flow Analysis on page FA-2-4 for details. For the failure impact analysis, you can also select additional performance measures for computation, turn some options on or off (such as turning on or off writing results for graphs).

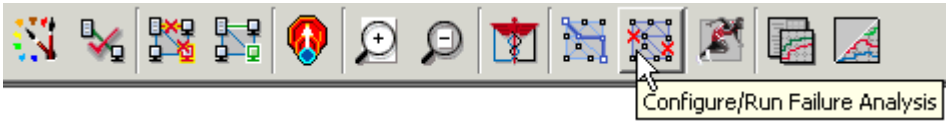
After you run a failure impact analysis, if you want to show routes or use the route browser, remember that you are acting on the results of the baseline run, not on any one of the failure scenarios. The reports for a failure impact analysis are stored under the Analysis category in the Results Viewer.

If you want to study a failure scenario in detail, configure it manually in the project editor then run a flow analysis.

Procedure 3-1 Configuring a Failure Impact Analysis

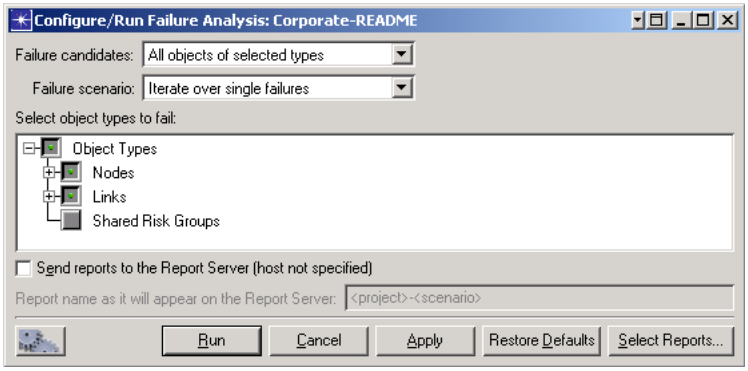
1 Click the Configure/Run Failure Impact Analysis button in the toolbar. Alternatively, you can use the menu–choose Flow Analysis > Configure/Run Failure Impact Analysis…

Figure 3-1 Configure/Run Failure Impact Analysis Toolbar Button



➥ The Configure/Run Failure Analysis dialog box opens.

Figure 3-2 Configure/Run Failure Analysis Dialog Box



2 Select the objects you want to fail from the Failure candidates pull-down menu:

- All Objects of Selected Types. Choosing this option enables the checkboxes in the Select Object Types to Fail list of the window so you can select the objects you want to fail.

  OPNET fails all objects of the selected object type one at a time—or one pair at a time depending on the Failure scenario option selected—then runs a flow analysis under the failure condition. For example, if Routers is selected as an object type to fail, OPNET iterates through all routers in the model.

- Failed Objects in Scenario. OPNET fails the objects that you marked as failure candidates one at a time—or one pair at a time depending on the Failure scenario options selected—and runs a flow analysis under the failure condition.

  To mark an object as a failure candidate in your current scenario use the Topology > Fail Selected Objects menu operation or the Fail Selected Objects toolbar button (see Failing and Recovering Network Objects on page FA-3-4).

  Choosing this option disables the checkboxes in the Select Object Types to Fail list of the window.

3 Select the mode you want OPNET to use when iterating over failure candidates by selecting from the Failure scenario pull-down menu:

- Iterate Over Single Failures—fail only one object at a time; count all single failures in the candidate set.
- Iterate Over Pairwise Failures—fail only pairs of objects at a time; count all pairwise failures in the candidate set.
- Fail All Candidates Simultaneously—fail all candidates at once and generate a comparison of this single-failure scenario with the baseline.

4 If you selected All Objects of Selected Types in the Failure candidates list, a tree directory is enabled in the Select Object Types to Fail pane. You can select the types of nodes and links you want to fail by clicking on the checkboxes next to the candidate object. In addition to nodes and links, you can also fail shared risk groups.

5 Save the configuration.

- To save and run a failure impact analysis immediately, click Run.
- To save without running a failure impact analysis, click Apply and close the dialog box.

End of Procedure 3-1

Failing and Recovering Network Objects

You can manually select network objects to fail during a flow analysis or a failure impact analysis. In both cases, you must mark the objects as failed before you run the analysis. However, a failed object is different for flow analysis than it is for failure impact analysis.

In flow analysis, all the marked objects are failed.

In failure impact analysis, all the marked objects are failed only if you have Failure candidates set to All Objects of Selected Types.

If Failure candidates is set to Failed Objects in Scenario, the objects marked as failed are NOT failed in the baseline run. (A baseline run is the initial failure impact analysis run that has no node failures.) The objects are failed only in failure scenarios according to the Failure Scenario mode set in the IP Failure Analysis window:

- Over Single Failures
- Over Pairwise Failures
- Fail All Candidates Simultaneously

For example, if you mark four objects as failed in the Project Editor, then run one or more analyses, you get the following results according to the type of analysis you run and how it is configured.

- If you run a flow analysis, all four objects are considered failed and the results reflect this.
- If you run a failure impact analysis with the Failure Candidates set to All Objects of Selected Types, the four objects are considered failed in the baseline and in all subsequent failure scenario runs. High-level performance measures for each failure scenario are available.
- If you run a failure impact analysis with the Failure Candidate set to Failed Objects in Scenario and the Failure Scenario set to Iterate over Single Failures, the four objects marked for failure are considered to be “failure candidates”. They are not failed in the baseline scenario; rather each of the objects is failed one at a time with a flow analysis run after each failure.

Selecting Objects to Fail

Procedure 3-2 Selecting Individual Objects to Fail

1. Click on each object in the network that you want to fail. Use shift-click to select multiple objects.

2 Click on the Mark Selected Node or Link as Failed toolbar button. 

➥ A red X appears on the selected objects to mark them as failed.

To add objects to the set, shift-click to select more objects—individually or as a group—then click the Fail Selected Objects toolbar button.

3 Configure and run flow analysis or failure impact analysis to generate results based on the failure of the selected objects.

End of Procedure 3-2

Recovering Failed Objects

Procedure 3-3 Recovering Failed Objects

1 Click on each object in the network that you want to recover. Use shift-click to select multiple objects.

2 Click on the Mark Selected Failed Node or Link as Recovered toolbar button. 

➥ The red X is removed from the failed objects you selected.

End of Procedure 3-3

To recover all the failed objects in a scenario at the same time, choose Edit > Select Objects…, select the Object Types and Search Scope that apply to the scenario, then click on the Mark Selected Failed Node or Link as Recovered toolbar button.

Available Failure Analysis Reports

The reports in Table 3-1 are available for viewing in the Results Viewer after a failure impact analysis.

Note—The visualization features on the View menu are not available after a failure analysis. You need to use flow analysis instead to access those operations.

Table 3-1 Failure Impact Analysis Reports

Report Name	Category	Purpose
Failure Impact–Baseline	Analyses	Compares the performance of the network under failure to the baseline network according to the failure mode used. With "Fail All Candidates Simultaneously," OPNET runs two flow analyses—a baseline and one with all candidates failed. With "Iterate Over Single Failures" or "Iterate Over Pairwise Failures," OPNET runs two or more flow analyses—the baseline followed by as many flow analysis runs needed to iterate through the selected failures.
Failure Impact–Demands	Analyses	Lists which demands failed in each failure event analyzed by failure impact analysis.
Failure Impact–DSI	Analyses	Lists a survivability index for each demand in the network under the failure scenarios analyzed by failure impact analysis.
Failure Impact–Links	Analyses	Lists which virtual links failed in each failure event analyzed by failure impact analysis.
Failure Impact–LSI	Analyses	Lists a survivability index for each virtual link in the network under the failure scenarios analyzed by failure impact analysis.
Failure Impact–NSI	Analyses	Lists network survivability indexes for demands and virtual links. These network-wide indexes are averages of the DSIs/LSIs over all the demands and virtual links in the network.
Failure Impact–Performance	Analyses	Lists the performance of the network under failure scenarios analyzed by failure impact analysis. Maximum, median, minimum, average and standard deviation measures are computed over all failure events for user-selected performance analysis measures.
Failure Impact–Overutilized Links	Analyses	Lists all the links whose average utilization exceeds the user-specified threshold.
End of Table 3-1		

4 Using Capacity Planning

Flow Analysis includes a capacity planning feature that lets you extend your analysis of a network into the future to see how a network will perform with time. IT Sentinel can look for trends in the traffic of the current network and forecast what the traffic levels will be later on.

The basic workflow of a capacity planning analysis involves the following steps:

1) Running a baseline flow analysis

2) Trending traffic into the future

3) Running flow analysis using trended traffic

4) Viewing reports

The capacity planning wizard automates and combines some of these steps. For example, when you use the wizard (Flow Analysis > Configure/Run Capacity Planning), the wizard automatically uses the most recent settings configured for flow analysis.

Configuring and Running Capacity Planning

This section describes how to configure and run a capacity planning analysis on a network.

Procedure 4-1 Running a Capacity Planning Analysis with Existing Traffic

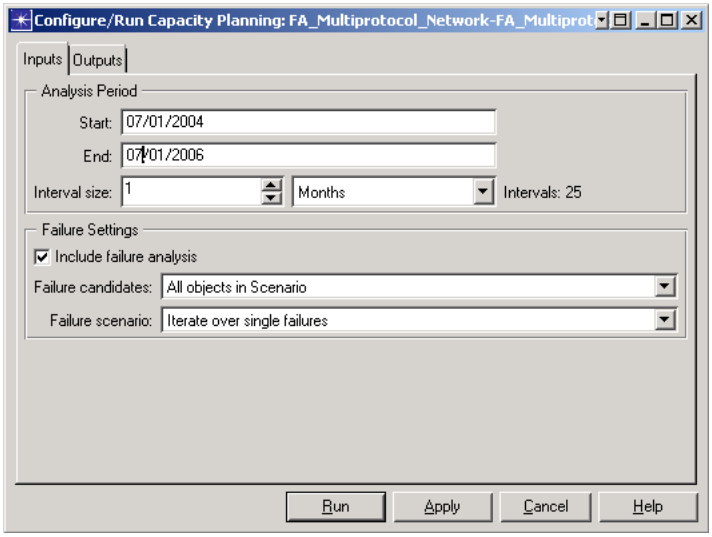
1 From the Flow Analysis menu, select Configure/Run Capacity Planning.

2 In the Capacity Planning dialog box, select Use Existing Traffic and click OK.

➥ The Configure/Run Capacity Planning dialog box opens.

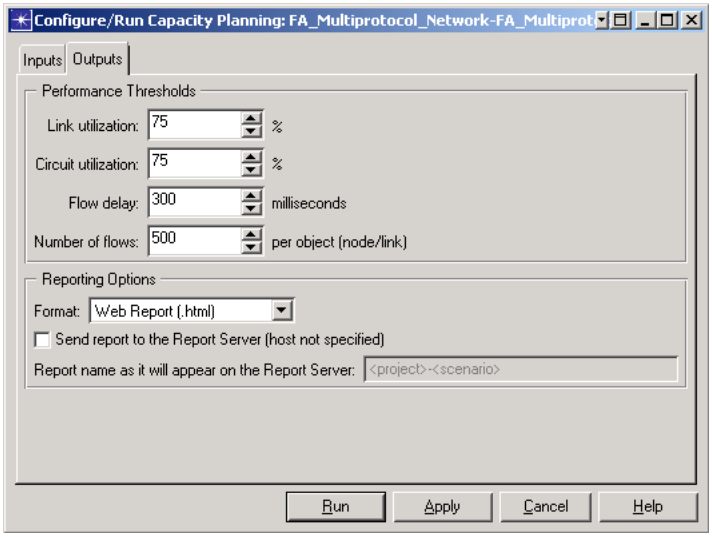
3 On the Inputs tab, configure the start and end times of the analysis and the interval size that you want to use for reporting. If would like to include failure scenarios in your analysis, select the Include failure analysis checkbox and specify which objects you want to fail.

Figure 4-1 Configure/Run Capacity Planning Dialog Box: Inputs



4 On the Outputs tab, configure the performance thresholds and specify the type of report you want to generate.

Figure 4-2 Configure/Run Capacity Planning dialog box: Outputs



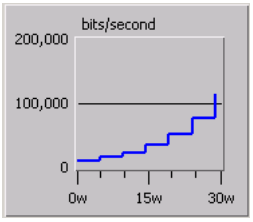
5 Click Run to start the analysis.

➥ The capacity planning analysis runs and generates a report in the format you specified. If you chose a web report, it opens when the analysis is complete.

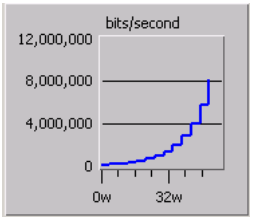
End of Procedure 4-1

The existing traffic data can be used to predict future traffic levels using well-known techniques. This process is called trending. When you trend traffic as part of a capacity planning analysis, IT Sentinel examines the traffic in the network and modifies each traffic profile so that it continues its current trend. Traffic profiles can represent link loads, circuit loads, or flow volumes.

Figure 4-3 Trended Traffic



Before Trending



After Trending

Notice that the two graphs are identical up to 30 weeks (30w).

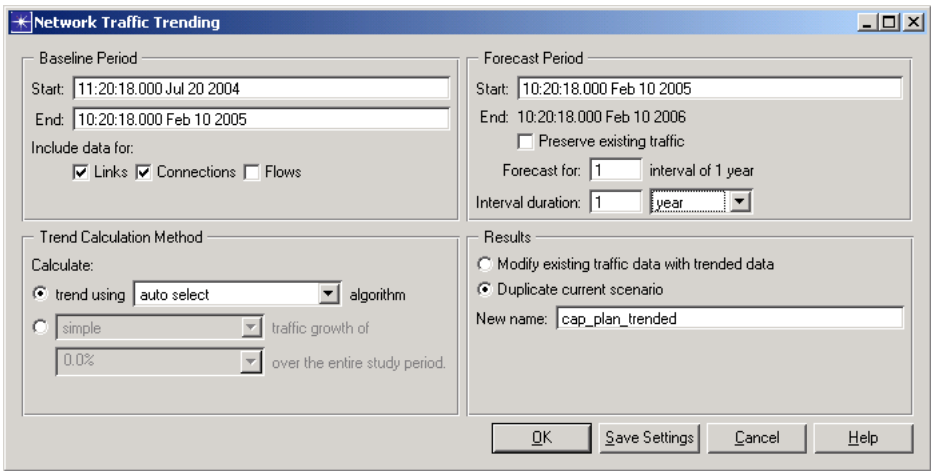
The second graph follows the trend seen in the first.

Procedure 4-2 Running a Capacity Planning Analysis with Trended Traffic

1. From the Flow Analysis menu, select Configure/Run Capacity Planning.
2. In the Capacity Planning dialog box, select Trend Current Traffic and click OK.

   ➥ The Network Traffic Trending dialog box opens.

Figure 4-4 Network Traffic Trending Dialog Box



3. Complete the following:
   - Baseline Period—The baseline period lets you specify the reference period that you want to use for trending traffic.
   - Forecast Period—The forecast period lets you specify the duration over which you want to trend the traffic. Ideally, the Start time should occur after the End time of the Baseline Period. The forecast end time is automatically calculated based on the duration specified.

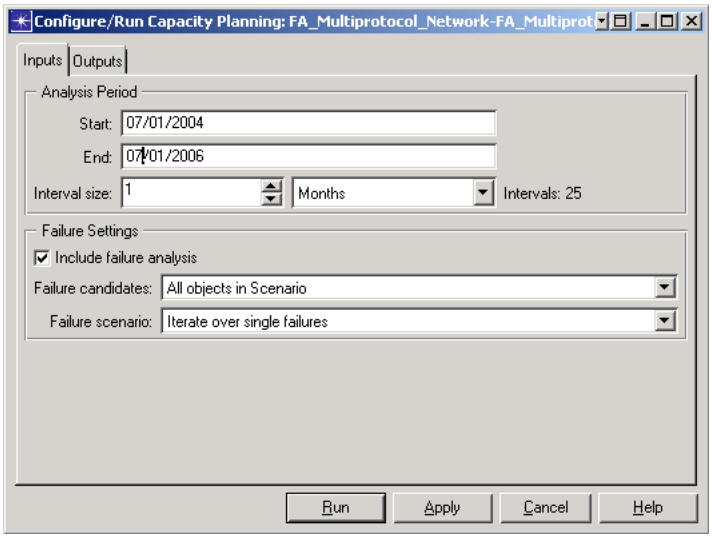
- Trend Calculation Method—Trend calculation lets you specify how to compute the traffic trends. The default, auto select algorithm, is suitable for most cases.
- Results—The trended traffic can be reflected in the current scenario or IT Sentinel can create a new scenario with the trended results.

4 Click OK.

➥ The trended traffic is added to the current or new scenario. The Configure/Run Capacity Planning dialog box opens.

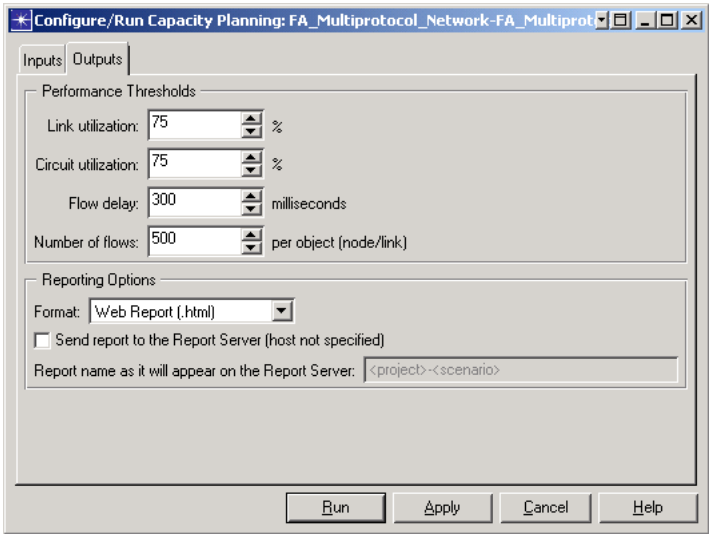
5 On the Inputs tab, configure the start and end times of the analysis and the interval size that you want to use for reporting. If would like to include failure scenarios in your analysis, select the Include failure analysis checkbox and specify which objects you want to fail.

Figure 4-5 Configure/Run Capacity Planning Dialog Box: Inputs



6 On the Outputs tab, configure the performance thresholds and specify the type of report you want to generate.

Figure 4-6 Configure/Run Capacity Planning dialog box: Outputs



7 Click Run to start the analysis.

➥ The capacity planning analysis runs and generates a report in the format you specified. If you chose a web report, it opens when the analysis is complete.

End of Procedure 4-2

Viewing Capacity Planning Reports

A capacity planning analysis generates a web report that opens automatically when the analysis completes. (You can also open the last report from the Flow Analysis > Results menu.) The report opens to the Executive Summary, which gives you a short overview of the report highlights. More detailed results are available by clicking on one of the links under Performance Metrics. Note that performance metrics are visible only after you select a scenario (baseline or failure) in the Network Performance section.

Figure 4-7 Capacity Planning Report

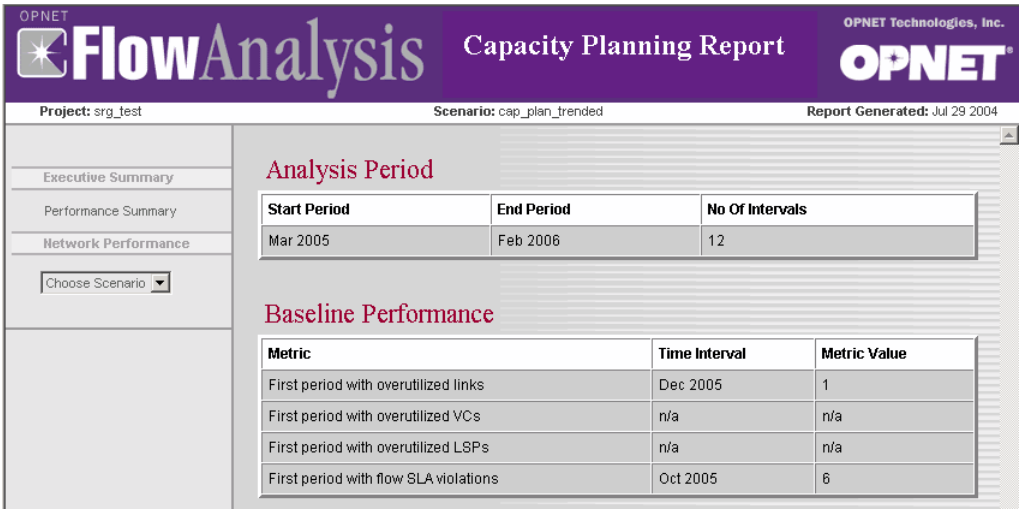
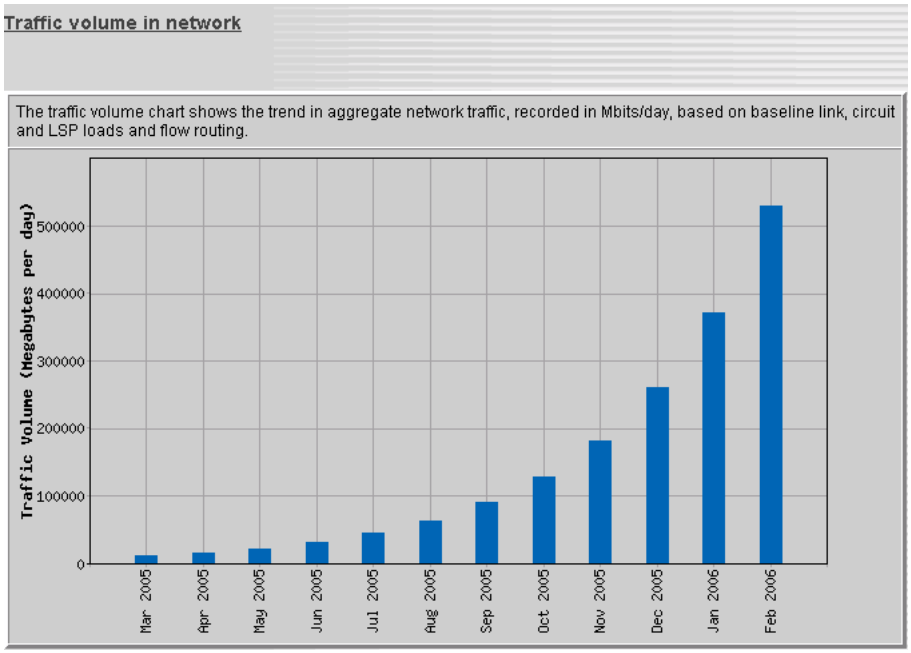


Figure 4-8 Network Traffic Volume Graph in a Capacity Planning Report



Capacity planning reports are stored in the following locations:

- MS Word reports:
  <op_admin>/flan_cap_plan_reports/<project>-<scenario>/rtf
- Web reports:
  <op_admin>/flan_cap_plan_reports/<project>-<scenario>/web

  The filename for the report is index.html.
- XML reports:
  <op_admin>/flan_cap_plan_reports/<project>-<scenario>/xml

IT Sentinel creates directories for all of the supported formats, but it only generates reports in the format specified during configuration. An XML report is also generated when the chosen format is web or MS Word.

Index

L

M

O

P

R

S

T

U

V

W