14 Failure Evaluation

When you run a network design operation, SP Guru Transport Planner supports recovery strategies that safeguard the routed traffic. Strategies include unprotected, 1+1 protection, shared path protection, restoration, and ring protection. Use these strategies to protect traffic against failures of the network elements. Apply different recovery strategies to different traffic demands according to the failures you expect and the grade of service. However, before you commit to a certain design, you need to know how a recovery action is supposed to work and what failures are recoverable.

SP Guru Transport Planner enables you to evaluate how a specific traffic demand—given a certain recovery action—responds to a set of failures. There are three types of evaluation:

- Service Availability—SP Guru Transport Planner considers all network failures you select. For each failure, it evaluates which part of the traffic can be recovered. The system correlates the data with the probability of each failure. This probability is calculated according to the specified failure rates of the equipment. If the evaluation has finished, the system reports availability for each selected connection. Also, it reports the expected loss of traffic of the entire traffic matrix, given the specified recovery method.
- Failure Analysis—You can use the Failure Analysis mode of SP Guru Transport Planner to evaluate how user-defined failures affect network traffic. The workflow consists of three general steps:
  a) Design the network for one or more traffic demands, with a designated recovery strategy for each traffic demand
  b) Specify one or more network elements that fail
  c) Inspect the effect of those failures on the traffic accommodated in the network: SP Guru Transport Planner determines which portion of the network traffic is lost and which can be recovered
- Failure Analysis Report—You can generate a comprehensive web report for all failures of a specific type. This enables you to identify the most critical failure in your network, and identify the lost and recovered connections for each of the considered failure scenarios.

Service Availability

You can use the Evaluate Availability operation to simulate link and node device failures. Given a set of routed connections and failure element, SP Guru Transport Planner calculates the expected availability (per capacity unit) and loss of traffic over the course of a year for each connection in the selected set.

Note—SP Guru Transport Planner can calculate the availability of OCH, DCL, and LOP connections.

Evaluating Service Availability: Workflow Description

Procedure 14-1 describes how to run an Evaluate Availability operation.

Procedure 14-1 Evaluating Service Availability

1 Before you evaluate availability, you must specify the failure probabilities of all equipment in the network. You do this in the Availability Settings dialog box (Network > Availability Settings) or by clicking the Availability Settings button in the Info > Evaluate Availability dialog box. For more information, see Availability Settings on page TrP-3-42.

2 Choose Info > Evaluate Availability to open the Evaluate Availability dialog box. (shown in Evaluate Availability Dialog Box on page TrP-14-6).

3 Select the Analysis Method. SP Guru Transport Planner can evaluate the service availability in an analytical way or by failure simulation. In the latter method, different failure scenarios (combining the selected failure elements) are simulated to inspect their impact on the selected traffic.

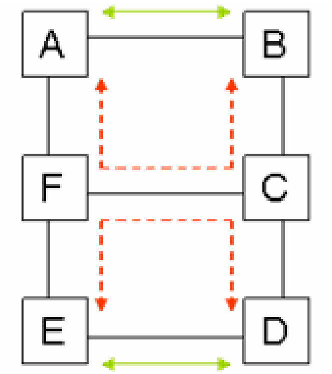
Note—The analytical method does not give exact results for traffic accommodated in the network with shared path protection or with restoration. In that case, the traffic is treated as unprotected traffic. This implies that the calculated value for the availability is a lower bound for the exact value.

4 Specify the Simulation Options. If you have selected the simulation method, some extra parameters must be set:

- Maximum Number of Simultaneous Failures—This parameter is used to limit the number of failure scenarios considered by the simulation method. For example, if this number is two, only failure scenarios with zero, single, and double failures are simulated to calculate the availability of the traffic. Thus, the higher this number is set, the more precise the calculated value for the availability will be. However, a higher number also increases the calculation time.
- Maximum Number of Simultaneous Failures to Restore for Shared Path Protection—This parameter is used to limit the number of failure scenarios in which shared path protection is considered. For example, if this number is set to two, the connection accommodated in the network with shared path protection are assumed to be unprotected in the failure scenarios with more than two simultaneous failures.

- Maximum Number of Simultaneous Failures to Restore for Link or Path Restoration—This parameter is used analogously to the previous parameter. This parameter is used to limit the number of failure scenarios in which link or path restoration is considered.
- Connection Order For Restoration —This parameter is used in case link or path restoration or shared path protection is applied in the network. This parameter prioritizes one connection above the other to use the protection capacity available in the network. Consider this example:

Figure 14-1 Connection Order for Restoration Example



In this example, two connections are accommodated with shared path protection in the network: a connection between node A and B and a connection between node E and D. Both protection paths are routed along the link between nodes F and C (marked in red in the figure above). The protection capacity on the link between C and F is shared among both connections. However, if the link between A and B and the link between E and D both fail, there is not enough protection capacity between F and C to restore both connections. In that case, the Connection Order for Restoration parameter determines which connection is restored. For example, assume the distance between A and B is higher than the distance between E and D. If the sorting order parameter is set to “Longest First,” the connection between A and B is restored, while the connection between E and D cannot be restored and is failing. However, if the sorting order is set to “Shortest First,” the connection between E and D is restored and the other connection fails.

5 Select the connections for which you want to calculate the availability in the Traffic To Analyze section. Only connections accommodated in the network are selectable.

Note—The connections part of an OCH or DCL traffic matrix that has been created by the grooming algorithm are not displayed in the Traffic To Analyze connection list.

6 Select failure elements in the Failure Elements To Analyze section. Only the selected failure elements are taken into account while calculating the availability. SP Guru Transport Planner supports the following failure elements.

- Cable Failures—Each OTS link in the network is displayed in this list. If a cable fails, traffic can no longer traverse this cable.

- OTS Node Failures—Each OTS node in the network is displayed in this list. If an OTS node fails, each switching device in this node fails. This implies that no traffic can be switched, added or dropped in each switching device present in this node (e.g. OXC, patch panel, DXC, TMs,…).
- OXC Failures—Each OXC present in the network is displayed in the list. If an OXC fails, it is no longer possible to switch, add or drop traffic in that OXC. Note that each node can contain one OXC at most.
- OADM Failures—Each OADM present in the network is displayed in the list. If an OADM fails, it is no longer possible to switch, add or drop traffic in this OADM. Note that a node can contain more than one OADM. An OADM is defined by its node name and the name of its incoming fiber(s).
- Patch Panel Failures—The list displays each patch panel present in the network. If a patch panel fails, it is no longer possible to switch, add or drop traffic in this patch panel. Note that each node can contain one patch panel at most.
- IXC Failures—This list displays each IXC present in the network. If an IXC fails, it is no longer possible to switch, add or drop traffic in this IXC. Note that each node can contain one IXC at most.
- DXC Failures—Each DXC present in the network is displayed in this list. If a DXC fails, it is no longer possible to switch, add or drop traffic in this DXC. Note that each node can contain one DXC at most.
- ADM Failures—Each ADM present in the network is shown in this list. If an ADM fails, traffic can no longer be added or dropped at this ADM. A node can contain more than one ADM. Each ADM is defined by its node and its ring name.
- SDH TM Failures—This list shows every SDH TM present in the network. If an SDH TM fails, DCL traffic can no longer be added or dropped at this TM. A node can contain more than one SDH TM. Each SDH TM is defined by its node name and the name of the incoming DCL trunk.
- LOP TM Failures—This list shows every LOP TM present in the network. If a LOP TM fails, LOP traffic can no longer be added or dropped at this LOP TM. A node can contain more than one LOP TM. Each LOP TM is defined by its node name and the name of its incoming DCL connection.
- In-line Regenerator Failures—If an in-line regenerator fails, traffic can no longer traverse the fibre attached to the in-line regenerator. Note that a fibre can contain more than one regenerator. However, one in-line regenerator failure is displayed per fibre in the In-line Regenerator Failures list. The availability of such failure equals: (availability of one in-line regenerator)^n (where n = number of in-line regenerators on the fibre).
- Optical Amplifier Failures—If an optical amplifier fails, traffic can no longer traverse the fibre attached to the optical amplifier. Note that a fibre can contain more than one optical amplifier. However, one optical amplifier failure is displayed per fibre in the Optical Amplifier Failures list. The availability of such failure equals: (availability of one optical amplifier)^n (where n = number of optical amplifiers on the fibre).
- Transponder Failures—If an LR transponder fails, each OCH connection path using this transponder fails. The LR transponders are displayed per OCH node and per path of an OCH connection. Note that the OCH connection can drop or add in the node, or can traverse the node. In the latter case, the path traverses two LR transponders. Therefore, the availability of such failure equals:

(availability of one LR transponder)[2]. In case of 1+1 protection, the number of transponders in an end node of a connection depends on the client protection option. If the connection is client protected, there are two LR (regular) transponders in each of its end nodes: one for the working path and one for the protecting path. However, in case of non-client 1+1 protection, only one LR (protection) transponder is present in each end node. If such a transponder fails, the working and the protecting path of the connection are failing (implying the connection fails).

7 After you have specified the analysis method, the simulation options (if applicable), the traffic and failure elements to analyze, click Evaluate.

➥ SP Guru Transport Planner evaluates your network and displays the results in the Availability Analysis report. This web report pops up automatically once the availability calculation has been finished.

End of Procedure 14-1

Evaluate Availability Dialog Box

Choose Info > Evaluate Availability to open the Evaluate Availability dialog box (Figure 14-2 and Table 14-1 on page TrP-14-6). For more information, see Procedure 14-1 Evaluating Service Availability on page TrP-14-2.

Figure 14-2   Evaluate Availability Dialog Box

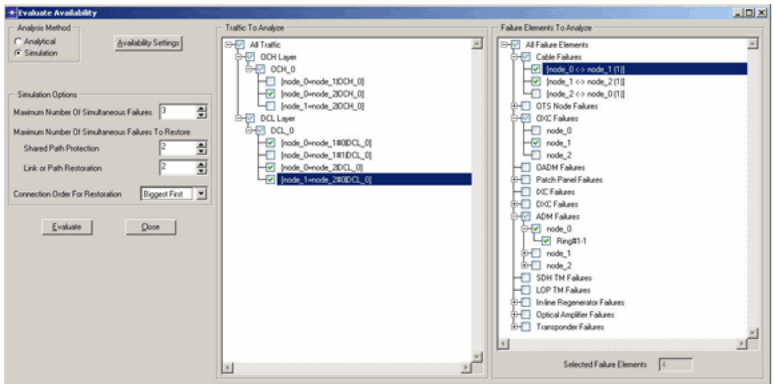


Table 14-1   Evaluate Availability Options/Fields

Item	Description
Analysis Method	Select the method to use. This is either the analytical or the simulation method.
Maximum Number of Simultaneous Failures	Determines the highest number of simultaneous failures that is considered in a failure scenario (only valid for the simulation method).
Maximum Number of Simultaneous Failures To Restore for Shared Path Protection	Determines the highest number of simultaneous failures for which shared path protection is considered in a failure scenario (only valid for the simulation method).
Maximum Number of Simultaneous Failures To Restore for Link or Path Restoration	Determines the highest number of simultaneous failures for which link or path restoration is considered in a failure scenario (only valid for the simulation method).
Connection Order for Restoration	Defines the sorting order to restore connections accommodated in the network with shared path protection or with link or path restoration.
Availability Settings	Opens the Availability Settings dialog box (for more information see Availability Settings on page WDM-3-38).
Traffic to Analyze	Determines the connections of which the availability is calculated. Only the routed connections are displayed in the list. To select all routed connection of a traffic matrix, just put a mark next to the traffic matrix name. Analogously, you can select all connections on a layer (e.g., “OCH Layer”), or all connections in the network (“All Traffic”).

Table 14-1 Evaluate Availability Options/Fields (Continued)

Item	Description
Failure Elements to Analyze	Determines the failure elements which are taken into account in the availability calculation. The failure elements are sorted per type. To select all failures of a certain type, just put a mark next to the failure type name (e.g., “DXC Failures”). You can select all failures by marking “All Failure Elements”.
Selected Failure Elements	Displays the number of failure elements selected (i.e., how high this number is, how long the evaluation will take)
Evaluate	Evaluates the availability of the selected connections taking into account the selected failure elements. If the calculation has been finished, a web report pops up displaying the availability and expected loss of traffic for the selected traffic.
End of Table 14-1	

Note—When you click the Evaluate button, a progress bar pops up. To interrupt the calculation, click Cancel on this progress bar.

Availability Analysis Report

The generated web report consists of two main parts. First, an overview of the availability analysis settings is shown. Next, an overview of the availability results is given per traffic matrix.

Figure 14-3 Availability Analysis Report—Analysis Settings

Analysis Settings

Analysis Method	Simulation		
Simulation Options	Maximum Number Of Simultaneous Failures		3
	Maximum Number Of Simultaneous Failures To Restore	Shared Path Protection	2
		Link or Path Restoration	2
	Connection Order For Restoration	Biggest First	
Selected Failure Elements	Cable Failures	[node_0 <-> node_1 (1)]	
		[node_1 <-> node_2 (1)]	
	OXC Failures	node_1	
	ADM Failures	node_0	Ring#1-1

This section gives an overview of the analysis options you can select. First, the analysis method is displayed. Next, the options for the simulation method are displayed: the maximum number of simultaneous failures, the maximum number of simultaneous failures to restore for shared path protection and for restoration, and the connection order for restoration. The report only shows these options if you have selected the simulation method. At the end, an overview of the selected failure elements is displayed. These failure elements are shown per failure type.

Figure 14-4 Availability Analysis Report—Availability Results

DCL_0

Summary

Average Availability	0.9999818997	
Expected Loss of Traffic	265.43	Gb/year
	0.48	STS-3 hours/year
Average Expected Loss of Traffic	88.48	Gb/year
	0.16	STS-3 hours/year

Connections meeting availability requirements

Connection	From	To	Protection Type	Minimal Availability	Estimated Availability	Maximal Availability	Required Availability
[node_0=node_1#0[DCL_0]	node_0	node_1	Ring	0.9999778496	0.9999778496	0.9999778496	0.9999500000
[node_1=node_2#0[DCL_0]	node_1	node_2	Ring	0.9999900000	0.9999900000	0.9999900000	0.9995000000

Connections failing to meet availability requirements

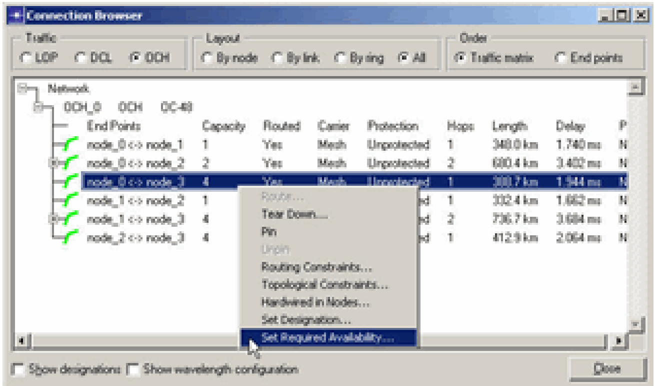
Connection	From	To	Protection Type	Minimal Availability	Estimated Availability	Maximal Availability	Required Availability
[node_0=node_2[DCL_0]	node_0	node_2	Ring	0.9999778496	0.9999778496	0.9999778496	0.9999990000

The Availability Analysis report shows the availability results per traffic matrix. You can view the result for a traffic matrix by clicking on the traffic matrix name at the left side of the report. The availability results per traffic matrix consists of three parts:

- An overview is given of the availability of the traffic matrix: the average availability, the expected loss of traffic, and the average expected loss of traffic. Note that only the connections you selected are taken into account to calculate these parameters.
- The “Connections meeting availability requirements” table is displayed. This table contains those connections for which the minimal calculated value for the availability is higher than or equal to the required availability set for the connection. This table shows, per connection, the connection name, the source and destination name, and the protection type. Also, the minimal, the estimated, and the maximal calculated value for the availability are shown.
- Next, the table shows the required availability of the connection. The minimal and maximal availability are respectively a lower-border and upper-border for the exact availability of the connection. Note that the estimated value is only displayed if the simulation method is selected. The equality of the minimal and maximal availability implies that this value is the exact value for the availability of the connection.
- At the end of the report, the “Connections failing to meet availability requirements” table is displayed and contains the connections for which the minimal value for the availability is lower than its required availability.

Note—The required availability of an LOP, DCL, or OCH connection can be specified by right-clicking on the connection in the Network > Connection Browser. This parameter should have a value between 0 and 1.

Figure 14-5 Connection Browser



Failure Analysis

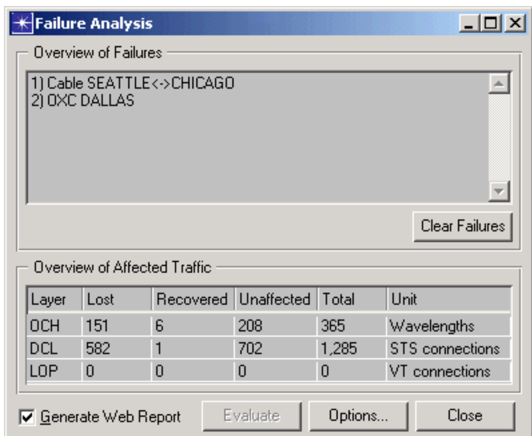
You can use SP Guru Transport Planner's Failure Analysis mode to evaluate how specific network failures affect traffic. Failure analysis determines how traffic currently routed in the network reacts to failures you define. After a failure, some traffic might be lost or rerouted. The following steps outline the workflow for running a Failure Analysis operation:

Procedure 14-2 Running a Failure Analysis

1 Choose Info > Failure Analysis.

➥ The Failure Analysis dialog box appears, and you are now in Failure Analysis mode.

Figure 14-6 Failure Analysis Dialog Box



2 Specify the objects that you want to fail, as described in Specifying Failures on page TrP-14-11.

3 Run the failure analysis by clicking Evaluate in the Failure Analysis dialog box.

4 Analyze the effects of the specified failures, as described in Evaluating the Impact of Failures on Traffic on page TrP-14-13.

5 If you want to run additional Failure Analysis operations, repeat steps 1 through 4. Otherwise, close the Failure Analysis dialog box to exit Failure Analysis mode. (You cannot run any network design operations such as routing or dimensioning while in Failure Analysis mode.)

End of Procedure 14-2

Specifying Failures

The Overview of Failures section of the Failure Analysis dialog box describes all the specified failures. You can generate the following failures at the different layers:

- OTS layer—Cable failure and complete node failure. A complete node failure means that the node fails at every network layer.
- OCH layer—OXC failure, IXC failure, OADM failure, patch panel failure, and complete node failure. Complete node failure applies only at the OCH layer.
- DCL layer—DXC failure, failure of all ADMs, and complete node failure. Complete node failure applies only at the DCL layer.

The Project Editor window shows red crosses to indicate user-defined failures, and marks as orange failures due to propagation toward higher layers and other objects that fail as a result of user-defined failures.

Keep in mind that any failures you specify during the evaluation process affect traffic only while you are in Failure Analysis mode. These effects do not persist in the network model after you exit this mode (by closing the Failure Analysis dialog box).

Procedure 14-3   Generating One Network Failure

1 Choose Info > Failure Analysis to open the Failure Analysis dialog box.

➥ You are now in Failure Analysis mode.

2 Place the mouse cursor over the specified network layer.

3 Right-click on the network object you want to fail.

4 Select the correct option from the popup menu, such as Fail This Link or Fail This Node.

➥ The list of failures appears in the Overview of Failures section of the Failure Analysis dialog box.

End of Procedure 14-3

Procedure 14-4   Removing One Network Failure

1 Choose Info > Failure Analysis to open the Failure Analysis dialog box.

➥ You are now in Failure Analysis mode.

2 Place the mouse cursor over the specified network layer.

3 Right-click on the failed network object.

4 Select the appropriate option from the popup menu, such as Repair This link or Repair This node.

End of Procedure 14-4

Procedure 14-5 Removing All Network Failures

1 Choose Info > Failure Analysis to open the Failure Analysis dialog box.

➥ You are now in Failure Analysis mode.

2 Click the Clear Failures button in the Failure Analysis dialog box.

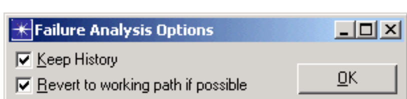
End of Procedure 14-5

Failure Analysis Options

When you specify an initial set of failures and click the Evaluate button, SP Guru Transport Planner considers all failures to be simultaneous failures. Click the Options button to specify the Failure Analysis Options. The options you select determine the behavior.

- Keep History—Select this option to make the new iteration take the result from the previous iteration as its starting point. This means the last iteration sets the current connection paths. However, the current paths might differ from the original paths because of rerouting on the protection or restoration path. This enables you to study the impact of a particular sequence of failures and repair actions. If Keep History is disabled, each time you click the Evaluate button, SP Guru Transport Planner considers the original connection paths before any failures and the current set of failures. Then it determines the affected connections and possible protection or restoration paths.
- Revert to working path if possible—SP Guru Transport Planner will restore a connection that was routed on its protection or restoration path to its original working path if the failures on this working path have been repaired.

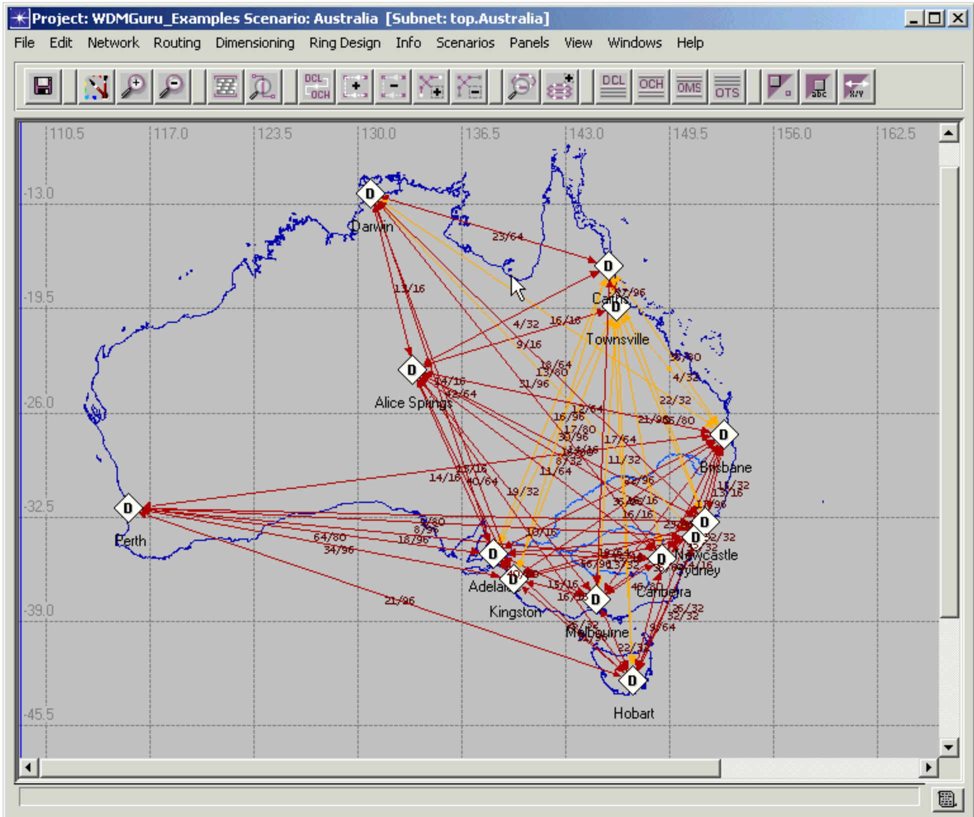
Figure 14-7 Failure Analysis Dialog Box



Evaluating the Impact of Failures on Traffic

After you fail one or more network elements, evaluate the impact of these failures by clicking the Evaluate button in the Failure Analysis dialog box. SP Guru Transport Planner starts at the OCH level by evaluating the connections affected by the failures. SP Guru Transport Planner tries to recover these connections. The recovery mechanism for each connection determines the recovery method. For example, if the working path of a 1+1 protected connection fails and the protection path is not affected by the failures, SP Guru Transport Planner switches to this path. Any connection not recovered at the OCH layer results in a failed DCL link. The DCL layer view marks the failing links in orange. SP Guru Transport Planner evaluates these link failures along with the other possible failures at the DCL layer to determine which DCL connections are affected.

Figure 14-8 Failure Analysis in DCL View



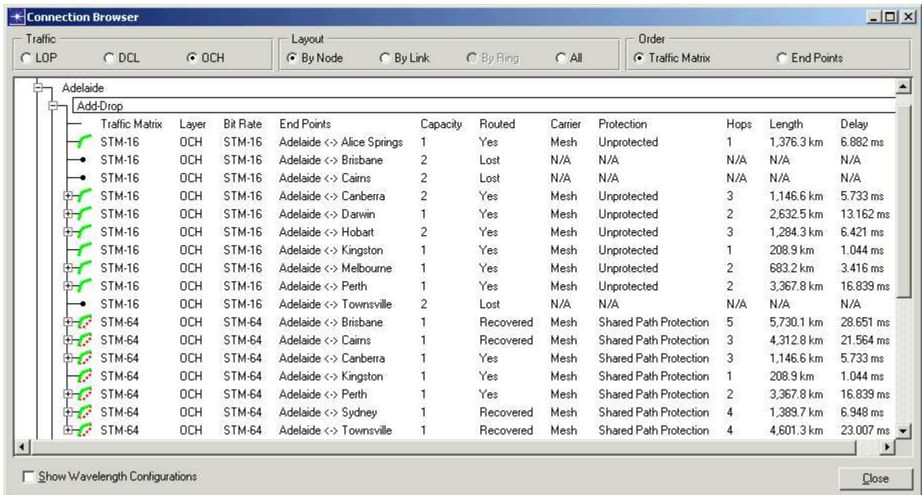
The Overview of Affected Traffic window in the Failure Analysis dialog box shows the amount of affected traffic recovered and lost in both the DCL and OCH layer.

In the Connection Browser (Network > Connection Browser), you can inspect the status of the individual connections. The Routed column indicates four possible states of a connection:

- No—Connection was not routed before the failure.

- Yes—Connection was routed and not affected by the failure.
- Recovered—Connection was routed, affected by the failure, but could be rerouted on its protection or restoration path.
- Lost—Connection was routed, affected by the failure, but was not protected or could not be rerouted on its protection or restoration path.

Figure 14-9   Failure Analysis Results in the Connection Browser



Traffic Matrix	Layer	Bit Rate	End Points	Capacity	Routed	Carrier	Protection	Hops	Length	Delay
STM-16	OCH	STM-16	Adelaide <-> Alice Springs	1	Yes	Mesh	Unprotected	1	1,376.3 km	6.882 ms
STM-16	OCH	STM-16	Adelaide <-> Brisbane	2	Lost	N/A	N/A	N/A	N/A	N/A
STM-16	OCH	STM-16	Adelaide <-> Cairns	2	Lost	N/A	N/A	N/A	N/A	N/A
STM-16	OCH	STM-16	Adelaide <-> Canberra	2	Yes	Mesh	Unprotected	3	1,146.6 km	5.733 ms
STM-16	OCH	STM-16	Adelaide <-> Darwin	1	Yes	Mesh	Unprotected	2	2,632.5 km	13.162 ms
STM-16	OCH	STM-16	Adelaide <-> Hobart	2	Yes	Mesh	Unprotected	3	1,284.3 km	6.421 ms
STM-16	OCH	STM-16	Adelaide <-> Kingston	1	Yes	Mesh	Unprotected	1	208.9 km	1.044 ms
STM-16	OCH	STM-16	Adelaide <-> Melbourne	1	Yes	Mesh	Unprotected	2	683.2 km	3.416 ms
STM-16	OCH	STM-16	Adelaide <-> Perth	1	Yes	Mesh	Unprotected	2	3,367.8 km	16.839 ms
STM-16	OCH	STM-16	Adelaide <-> Townsville	2	Lost	N/A	N/A	N/A	N/A	N/A
STM-64	OCH	STM-64	Adelaide <-> Brisbane	1	Recovered	Mesh	Shared Path Protection	5	5,730.1 km	28.651 ms
STM-64	OCH	STM-64	Adelaide <-> Cairns	1	Recovered	Mesh	Shared Path Protection	3	4,312.8 km	21.564 ms
STM-64	OCH	STM-64	Adelaide <-> Canberra	1	Yes	Mesh	Shared Path Protection	3	1,146.6 km	5.733 ms
STM-64	OCH	STM-64	Adelaide <-> Kingston	1	Yes	Mesh	Shared Path Protection	1	208.9 km	1.044 ms
STM-64	OCH	STM-64	Adelaide <-> Perth	1	Yes	Mesh	Shared Path Protection	2	3,367.8 km	16.839 ms
STM-64	OCH	STM-64	Adelaide <-> Sydney	1	Recovered	Mesh	Shared Path Protection	4	1,389.7 km	6.948 ms
STM-64	OCH	STM-64	Adelaide <-> Townsville	1	Recovered	Mesh	Shared Path Protection	4	4,601.3 km	23.007 ms

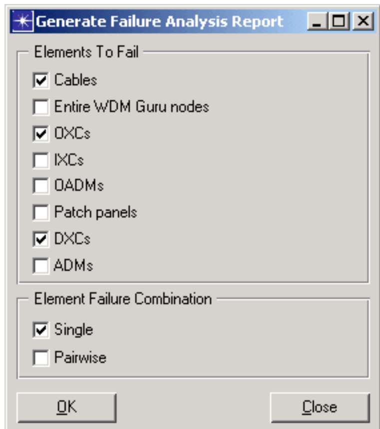
Failure Report

If the Generate Web Report option is selected, SP Guru Transport Planner generates a web report automatically when you click the Evaluate button in the Failure Analysis Dialog Box. The web report gives a detailed overview of the amount of traffic that is affected and recovered at each layer. For each traffic matrix, the web report lists the lost connections, recovered connections, and the new paths on which recovered connections are routed.

Failure Analysis Report

Within the Failure Analysis mode of SP Guru Transport Planner, you can study the impact of a specific set of failures and their effects on traffic at the different layers. Instead of defining the failures manually, you can also generate a web report with an overview of all specified failures and their impact. To generate this type of report, choose Info > Generate Web Report > Failure Analysis Report.

Figure 14-10 Generate Failure Analysis Report Dialog Box



The Generate Failure Analysis Report Dialog Box enables you to select the failure scenarios to include in the report. You can select the Elements To Fail, which list all the equipment types modeled in SP Guru Transport Planner. You can select one or more elements to fail; you can also select single or pairwise failures. When you click OK, SP Guru Transport Planner runs a failure analysis for each element (for single failures) or combination of elements (for pairwise failures) of a selected type.

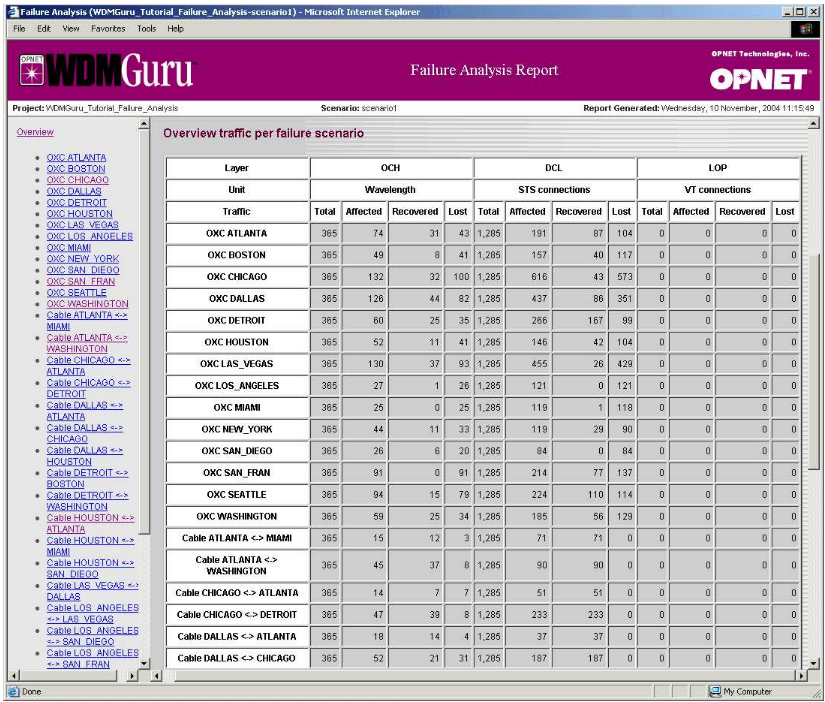
For example, suppose you select Cable and OXC elements (under Elements to Fail) and Single and Pairwise (under Element Failure Combination). In this case, the set of considered failure scenarios consists of:

- All single-cable failures
- All single-OXC failures
- All double-cable failures
- All double-OXC failures
- All failure scenarios with the simultaneous failure of one cable and one OXC

Note—An "Entire SP Guru Transport Planner node" failure implies the failure of all equipment elements in that node.

The resulting report includes an overview of lost and recovered connections for each of the considered failure scenarios, as well as an overview of all failure scenarios. The generated report contains an overview page, which includes an overview of the considered failure scenarios and the amount of lost and recovered traffic per failure scenario (as shown in Figure 14-11). This allows you to identify the most critical failure considered by the failure analysis.

Figure 14-11 Failure Analysis Web Report: Overview



Overview traffic per failure scenario

Layer	OCH				DCL				LOP			
Unit	Wavelength				STS connections				VT connections			
Traffic	Total	Affected	Recovered	Lost	Total	Affected	Recovered	Lost	Total	Affected	Recovered	Lost
OXC ATLANTA	365	74	31	43	1,285	191	87	104	0	0	0	0
OXC BOSTON	365	49	8	41	1,285	157	40	117	0	0	0	0
OXC CHICAGO	365	132	32	100	1,285	616	43	573	0	0	0	0
OXC DALLAS	365	126	44	82	1,285	437	86	351	0	0	0	0
OXC DETROIT	365	60	25	35	1,285	266	167	99	0	0	0	0
OXC HOUSTON	365	52	11	41	1,285	146	42	104	0	0	0	0
OXC LAS_VEGAS	365	130	37	93	1,285	455	26	429	0	0	0	0
OXC LOS_ANGELES	365	27	1	26	1,285	121	0	121	0	0	0	0
OXC MIAMI	365	25	0	25	1,285	119	1	118	0	0	0	0
OXC NEW_YORK	365	44	11	33	1,285	119	29	90	0	0	0	0
OXC SAN_DIEGO	365	26	6	20	1,285	84	0	84	0	0	0	0
OXC SAN_FRAN	365	91	0	91	1,285	214	77	137	0	0	0	0
OXC SEATTLE	365	94	15	79	1,285	224	110	114	0	0	0	0
OXC WASHINGTON	365	59	25	34	1,285	185	56	129	0	0	0	0
Cable ATLANTA <-> MIAMI	365	15	12	3	1,285	71	71	0	0	0	0	0
Cable ATLANTA <-> WASHINGTON	365	45	37	8	1,285	90	90	0	0	0	0	0
Cable CHICAGO <-> ATLANTA	365	14	7	7	1,285	51	51	0	0	0	0	0
Cable CHICAGO <-> DETROIT	365	47	39	8	1,285	233	233	0	0	0	0	0
Cable DALLAS <-> ATLANTA	365	18	14	4	1,285	37	37	0	0	0	0	0
Cable DALLAS <-> CHICAGO	365	52	21	31	1,285	187	187	0	0	0	0	0

You can click on each individual failure scenario listed in the left frame of the web report. Each failure-scenario page gives a detailed overview of the amount of traffic that is affected and recovered at each layer (as shown in Figure 14-12). Each failure-scenario page shows the lost connections, recovered connections, and the new paths on which the recovered connections are routed.

Figure 14-12 Failure Analysis Web Report: Individual Failure Scenario