CHAPTER 8

Simulating a LAN Failure

Overview

This tutorial provides an example on creating a new scenario in order to simulate a LAN segment failing along the path from one end system to another end system. The tutorial in "Round Trip IP Connectivity Requirements" is the basis for this tutorial. However, as this tutorial modifies router attributes to simulate a LAN failure, the *tutorial_baseline* scenario must be modified. Therefore, the *tutorial_baseline* scenario can *not* be used. A new scenario *must* be created.

The following tasks were performed and described in the previous tutorial:

- the *tutorial_baseline* baseline was opened and loaded
- a baseline topology was constructed
- end system connectivity requirements were created
- status of the new connectivity requirements was assessed
- the baseline connectivity round trip path was inspected

The following tasks are performed and described in this tutorial:

- a new scenario (*tutorial_baseline+*) for simulation is created
- simulation of the following occurs:
  - a LAN segment is disabled
  - a router interface is disabled
  - a router is disabled
- additional end system connectivity requirements are created and loaded for analysis
- status of the new connectivity requirements is assessed

Tutorial

Having proceeded through the steps of creating and opening the *tutorial_baseline* baseline, as described in the first tutorial, the Connectivity Tools window, shown in Figure 8-1, is displayed. See "Creating and Opening a Baseline" for information on how to create and open a baseline.

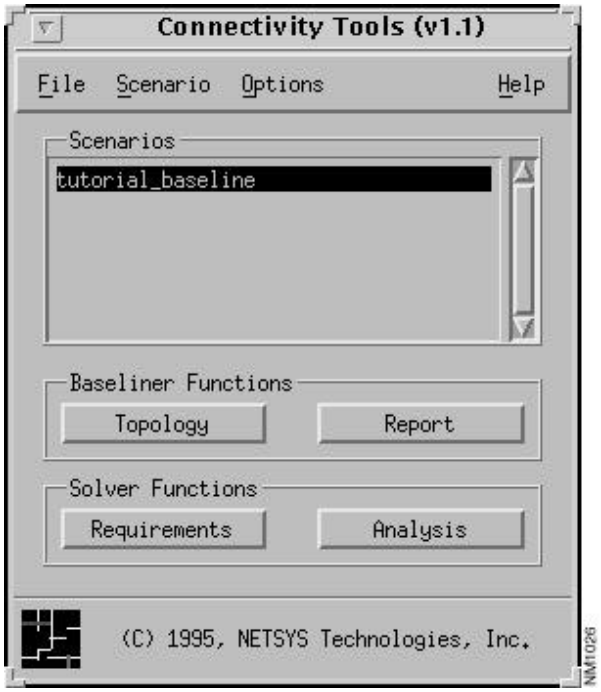

Figure 8-1 Connectivity Tools Window (Solver): Baseline Scenario Created

Step 1 Select the **Scenario>Create New** option.

The *tutorial_baseline+* scenario is created, selected, and displayed in the Connectivity Tools window, as shown in Figure 8-2. This newly created scenario can be used for simulation and analysis purposes.

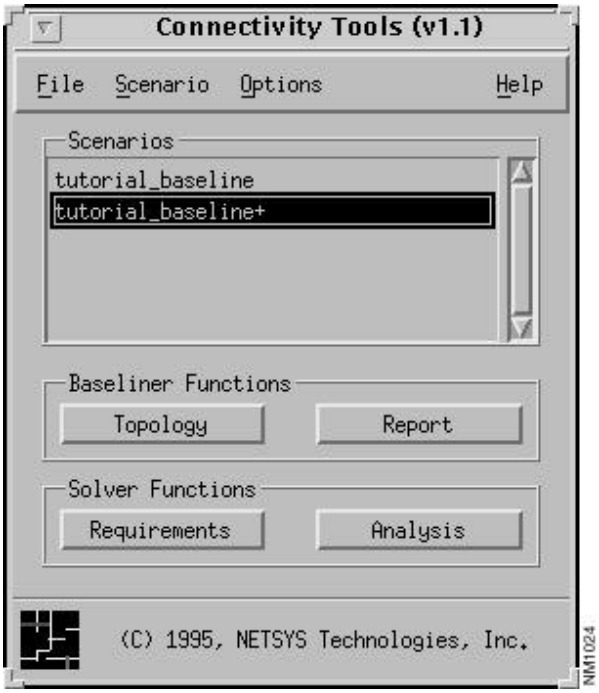

Figure 8-2 Connectivity Tools Window: New Scenario Created

Step 2 Click on the **Topology** button in the Connectivity Tools window.

A campus view of the *tutorial_baseline+* scenario's topology is displayed in the Topology window.

Step 3 Select the **View>Flat** and **Show>Router Labels** menu options in the Topology window.

The *tutorial_baseline+* topology, shown in Figure 8-3, is displayed in a flat, IP view with router labels displayed.

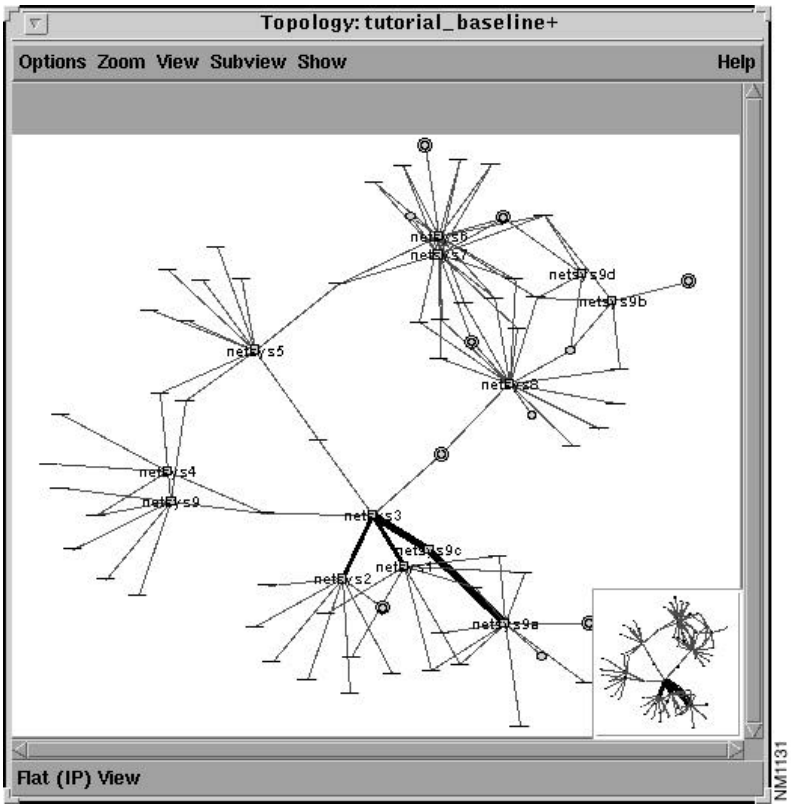

Figure 8-3 Topology Window: tutorial_baseline+ Scenario

Step 4 Click on the **Requirements** button in the Connectivity Tools window.

Clicking on the **Requirements** button allows you to create and load a set of connectivity requirements. The Requirement Sets window is displayed, as shown in Figure 8-4.

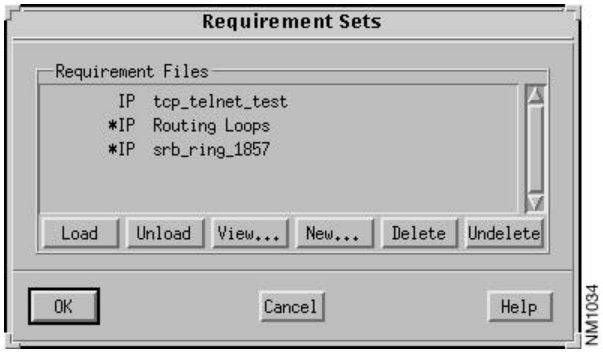

Figure 8-4 Requirement Sets Window

A list of existing requirement file sets is displayed in the **Requirement Files** list. A requirement file set contains network connectivity requirements for the baseline.

Requirement File entries preceded by an asterisk indicate connectivity requirements implicitly derived from the router configuration files. These connectivity requirement file sets can not be edited or deleted.

The implicitly derived **Routing Loops** requirement set is provided to find routing loops caused by IP redistribution. When you select the **Routing Loops** requirement set and then load it for analysis by clicking on the **Load** button followed by the **OK** button, a list of all the redistribution IP routing loops detected during analysis is displayed in the Requirements Analysis window. The results are a set of paths showing the identified routing loops. Each path displays a source address set to a port address of a router involved in the loop and a destination, which is a subnet or end point address, identifying the Routing Table destination involved in the routing loop. The path also shows a set of routers involved in a loop.

Load the previously created connectivity requirements found in the *tcp_telnet_test* requirement file set for analysis.

Step 5 Select the **`tcp_telnet_test`** file set from the **Requirement Files** list, then click on the **Load** button followed by the **OK** button.

The connectivity requirement file set loaded for analysis is prefixed by the identifier **LOAD** in the **Requirement Files** list. The results of the connectivity requirements are viewed from the Requirements Analysis window, partially shown in Figure 8-5. That is, the status of each connectivity requirement loaded for analysis, is viewable. One path was found providing the required connection between the source end system (**netsys9b**) and the destination end system (**netsys9a**).

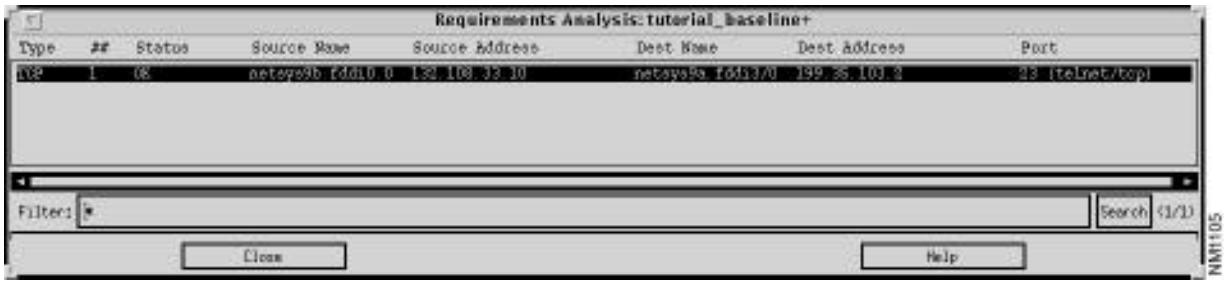

Figure 8-5 Requirements Analysis Window: tutorial_baseline+ Scenario

Step 6 Select the entry from this window to highlight the route between the two end systems in the Topology window, as shown in Figure 8-6.

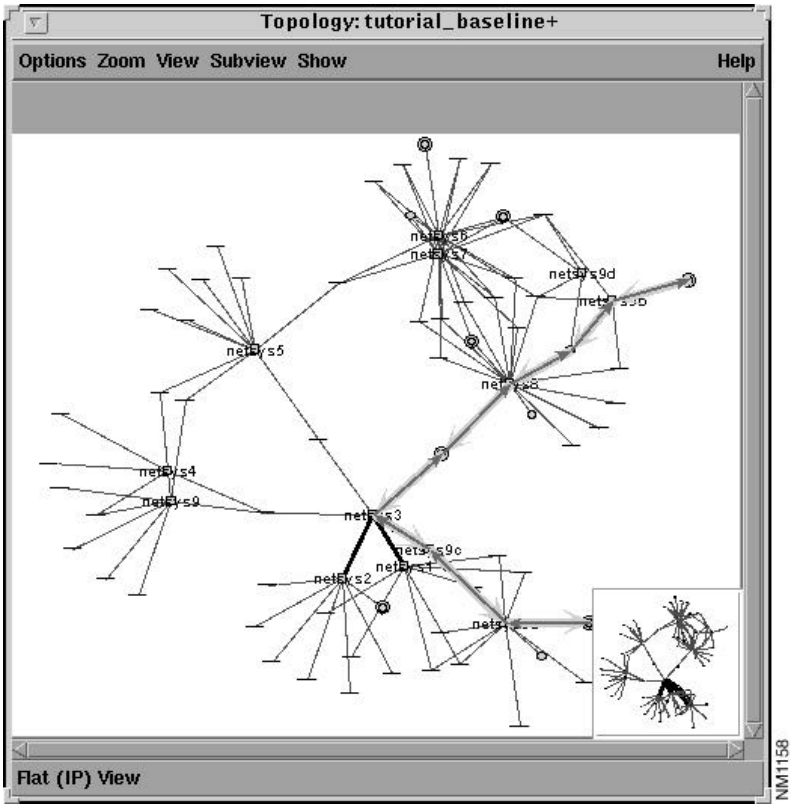

Figure 8-6 Topology Window: Round Trip Path Highlighted

The thicker highlighted line represents the route from the source router (**netsys9b**) to the destination router (**netsys9a**). The thinner highlighted line represents the return path from the destination router (**netsys9a**) to the source router (**netsys9b**).

Step 7 Double-click on the selected connectivity requirement entry in the Requirements Analysis window.

A corresponding Round Trip Path window is displayed, as shown in Figure 8-7. This window provides the end system names, addresses, and ports, the current status of the path, and a list of the devices and network elements that make up the path from the source end

system to the destination end system, and back. Based on this information and the information provided in the Topology window, the current connectivity requirements selected can be identified not only from a component standpoint, but visually as well.

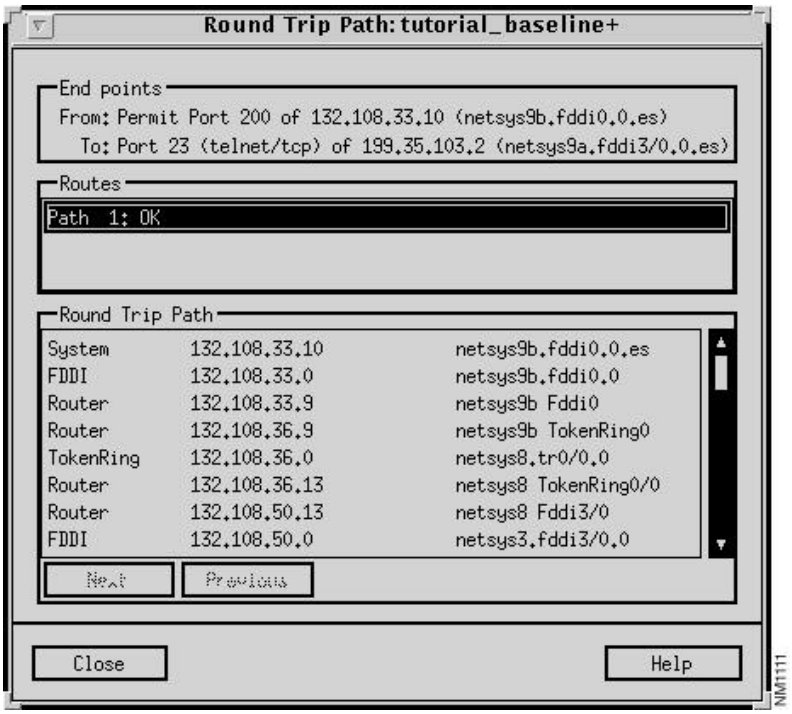

Figure 8-7 Round Trip Path Window: *tutorial_baseline+* Scenario

Step 8 Select the **`netsys3.fddi3/0.0`** (**`132.108.50.0`**) entry in the **Round Trip Path** list.

This LAN component is now highlighted in the Topology window.

Step 9 Double-click on the selected entry or on the highlighted **netsys3.fddi** icon in the Topology window to display the LAN Segment window as shown in Figure 8-8.

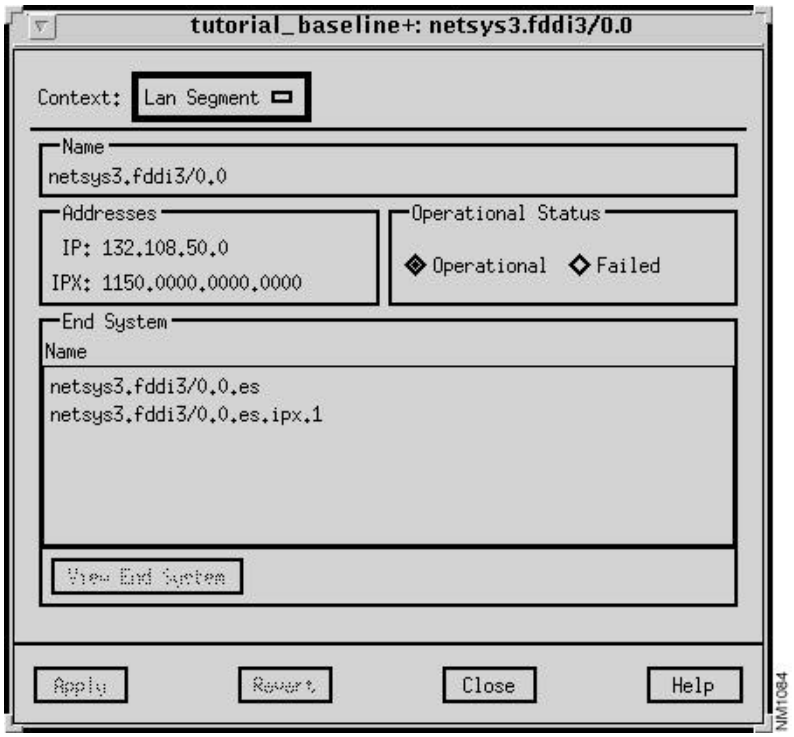

Figure 8-8 LAN Segment Window

Step 10 Click on the Operational Status **Failed** button, then click on the **Apply** button.

The `netsys3.fddi3/0.0` LAN segment is set to a failed state. Notice the `netsys3.fddi3/0.0` icon in the Topology window is red (indicating failure).

Step 11 Click on the **Analysis** button in the Connectivity Tools window.

Analysis of the *tutorial_baseline+* connectivity requirements is performed. Assess the status of the results. The *tutorial_baseline+* Requirements Analysis window is updated, as shown in Figure 8-9.

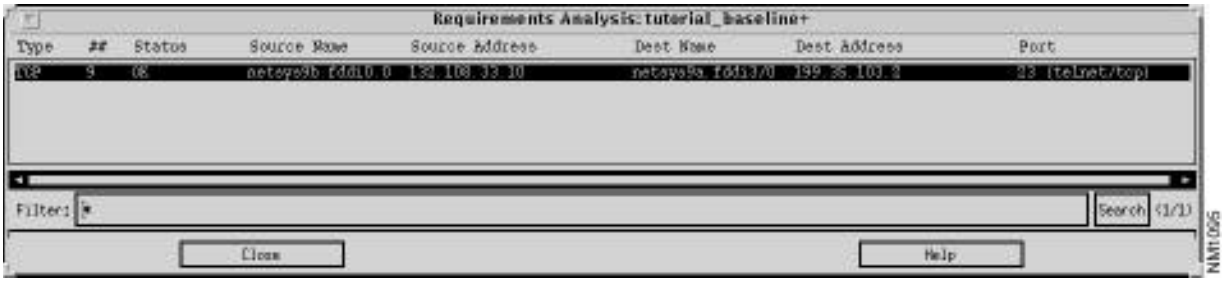

Figure 8-9 Modified Requirements Analysis Window: tutorial_baseline+ Scenario

Step 12 Select the connectivity requirements entry in the Requirements Analysis window.

A new path between the two end systems is highlighted, as shown in Figure 8-10. The new path reflects the route between the two end systems now that the `netsys3.fddi3/0.0` LAN segment is in a failed state (its icon is red).

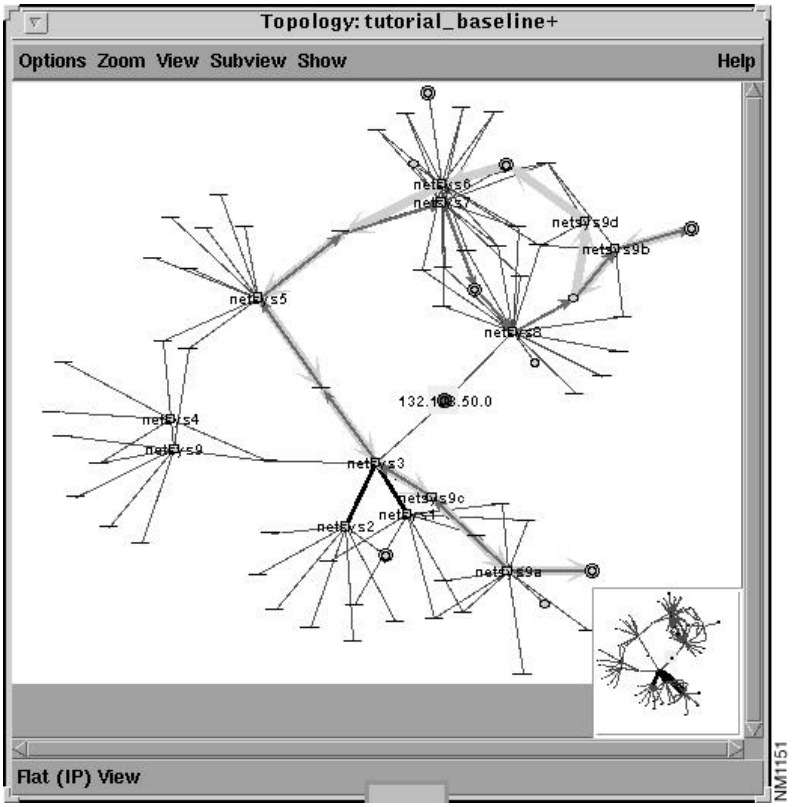

Figure 8-10 Topology Window with New Path Highlighted

Step 13 Double-click on the selected connectivity requirements entry.

The *tutorial_baseline+* Round Trip Path window is displayed, as shown in Figure 8-11. You can click on an entry in the **Routes** list to display the corresponding path in the Topology window.

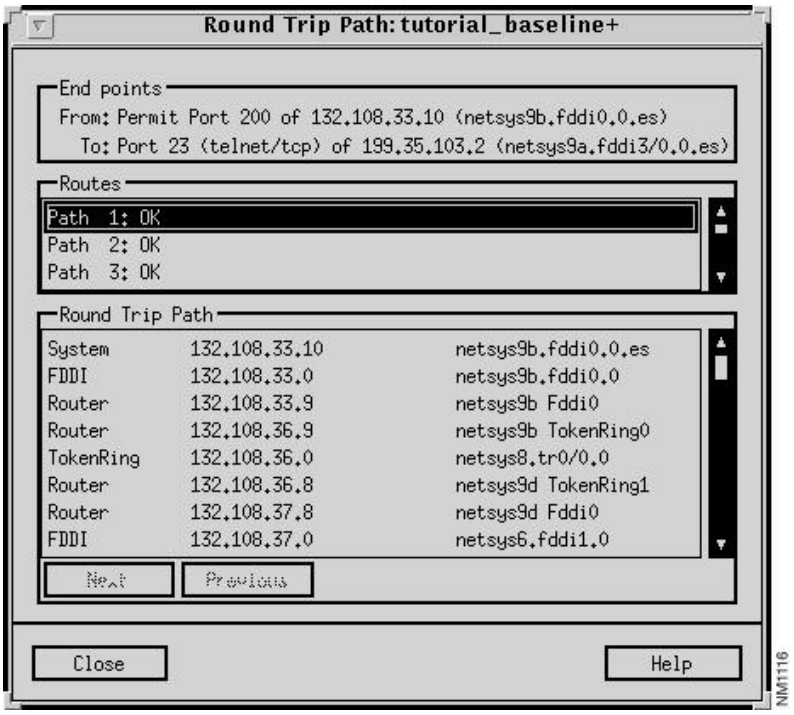

Figure 8-11 Roundtrip Path Window: New Path Displayed

Next, fail router **netsys8**'s incoming Token Ring interface (`132.108.36.13`), which is along the new path.

Step 14 Select the **`router 132.108.36.13 netsys8`** entry in the **Round Trip Path** list.

This router is highlighted in the Topology window.

Step 15 Double-click on this entry in the **Round Trip Path** list.

The **netsys8** Router Configuration window is displayed, as shown in Figure 8-12.

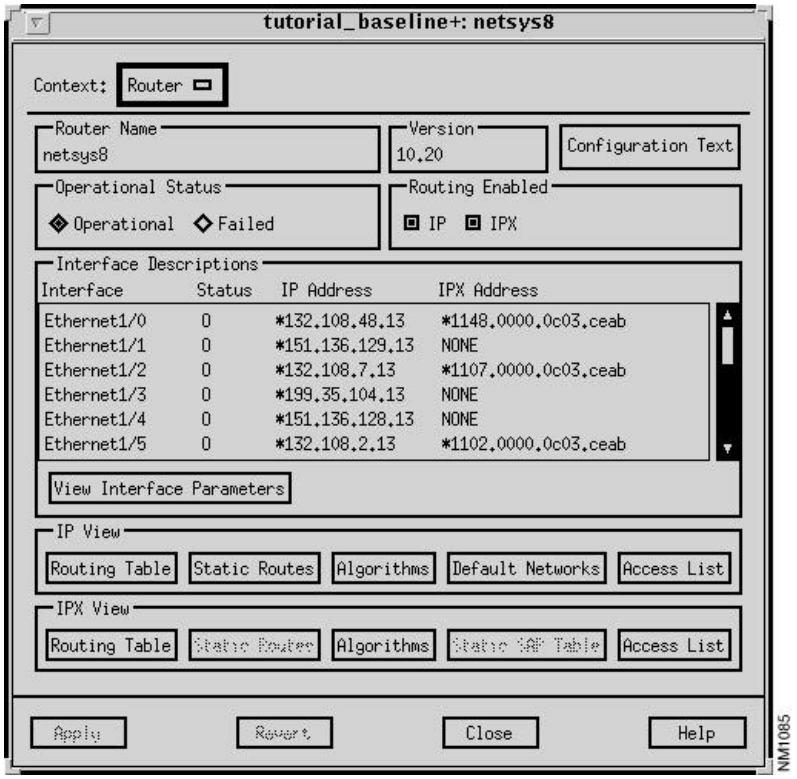

Figure 8-12 Router Configuration Window: netsys8 Router

Step 16 Select interface **`TokenRing0/0`** (**`132.108.36.13`**) from the **Interface Descriptions** list, then click on the **View Interface Parameters** button.

The Interface Parameters window is displayed, as shown in Figure 8-13.

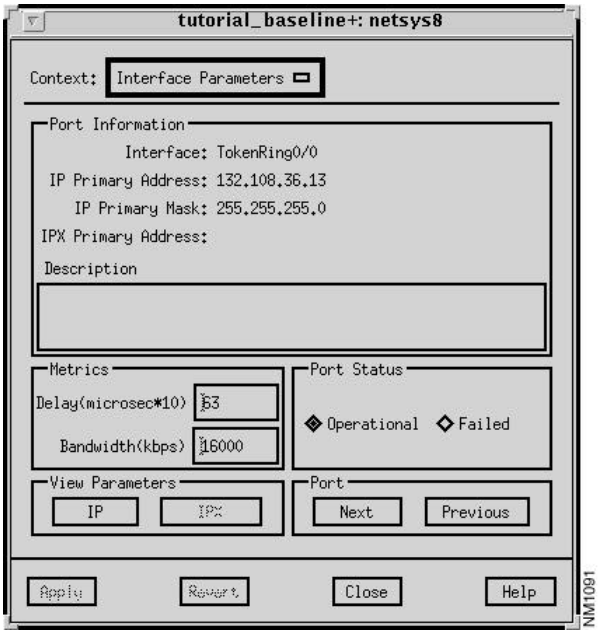

Figure 8-13 Interface Parameters Window: netsys8 TokenRing0/0

Step 17 Click on the Port Status **Failed** button, then click on the **Apply** button.

The `TokenRing0/0` (`132.108.36.13`) router interface status is set to failed (not operational.)

Step 18 Click on the **Analysis** button in the Connectivity Tools window.

Analysis of the new configuration is performed. The results are displayed in the Requirements Analysis window.

Step 19 Click on the connectivity requirements entry in the Requirements Analysis window.

The route taken from the source end system (**netsys9b**) to destination end system (**netsys9a**) and back, is highlighted in the Topology window, as shown in Figure 8-14. Notice the return path from the destination end system to the source end system has changed.

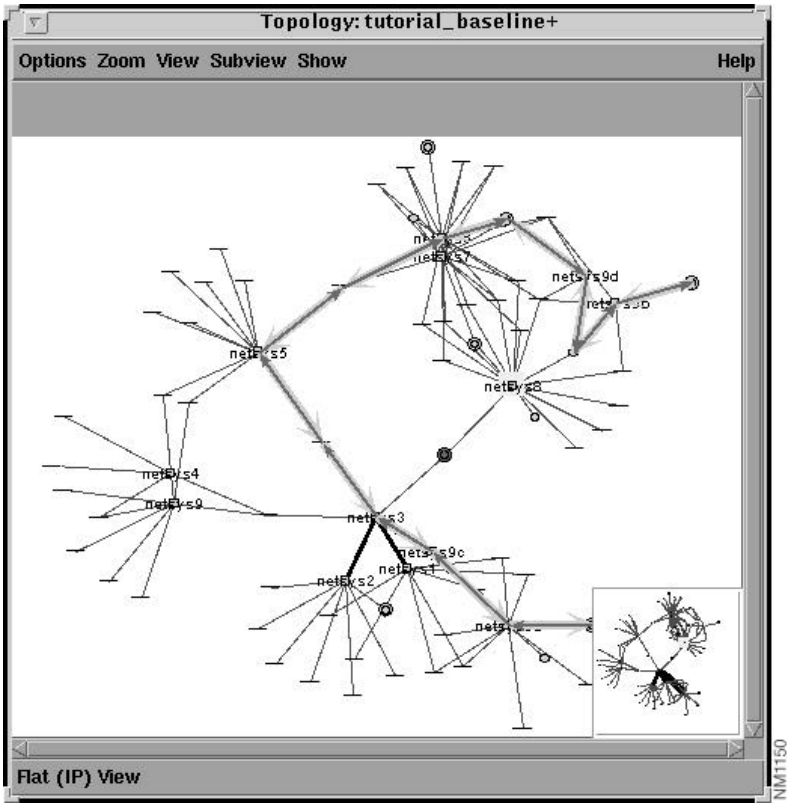

Figure 8-14 Topology Window: New Path Highlighted

Step 20 Double-click on the entry in the Requirements Analysis window.

Step 21 Select the **`router 132.108.36.9 netsys9b`** entry in the **Round Trip Path** list in the Round Trip Path window.

This router (**netsys9b**) is now highlighted in the Topology window.

Step 22 Double-click on this entry to display the **netsys9b** Router Configuration window.

Step 23 Click on the Operational Status **Failed** button, then click on the **Apply** button.

The **netsys9b** router operational status is set to failed. Notice the **netsys9b** router icon in the *tutorial_baseline+* Topology window is red (indicating failure).

Step 24 Click on the **Analysis** button in the Connectivity Tools window.

Analysis based on the modification is performed. Assess the status of the results. Notice the path from the source end system to the destination end system is now blocked, as partially shown in Figure 8-15.

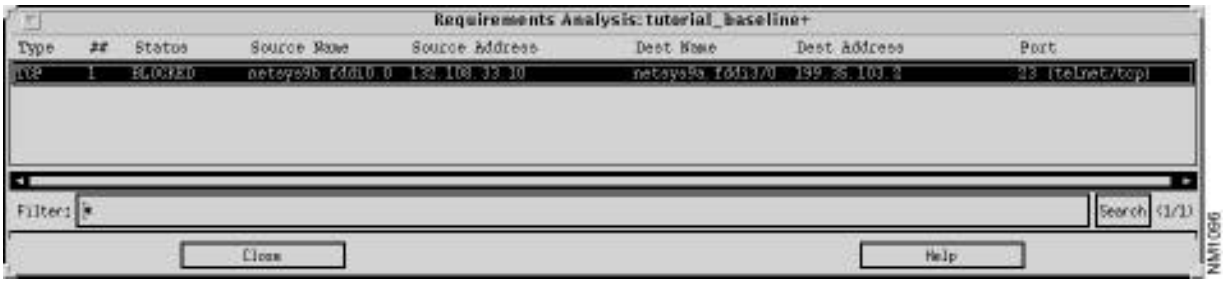

Figure 8-15 Requirements Analysis Window: Blocked Path

Step 25 Click on the **Operational** button in the **netsys9b** Router Configuration window, then click on the **Apply** button.

The status of the router is now back to operational. Notice the **netsys9b** router icon in the *tutorial_baseline+* Topology window is no longer red.

Step 26 Click on the **Analysis** button in the Connectivity Tools window.

Analysis of the new configuration is performed. The path's status is no longer blocked.

Step 27 Click on the **Requirements** button in the Connectivity Tools window.

Create another end system IP connectivity requirement set.

Step 28 Click on the **New** button in the Requirement Sets window.

Step 29 Name the new requirement file set *deny_test*, then click on the **OK** button in the New Requirement Set window.

The Requirements window is displayed.

Step 30 Click on the **Add** button in the Requirements window.

The Add IP Requirements window is displayed. Deny a FTP/TCP connection from port `220` of source end system `netsys8.ether1/2.0.es` (`132.108.7.14`) to port `21` of destination end system `netsys1.ether1/4.0.es` (`199.35.38.7`).

Step 31 Click on the **OK** button in the Add IP requirements window.

The Requirements window is displayed with the entry added to the *deny_test* requirement file set, as partially shown in Figure 8-16.

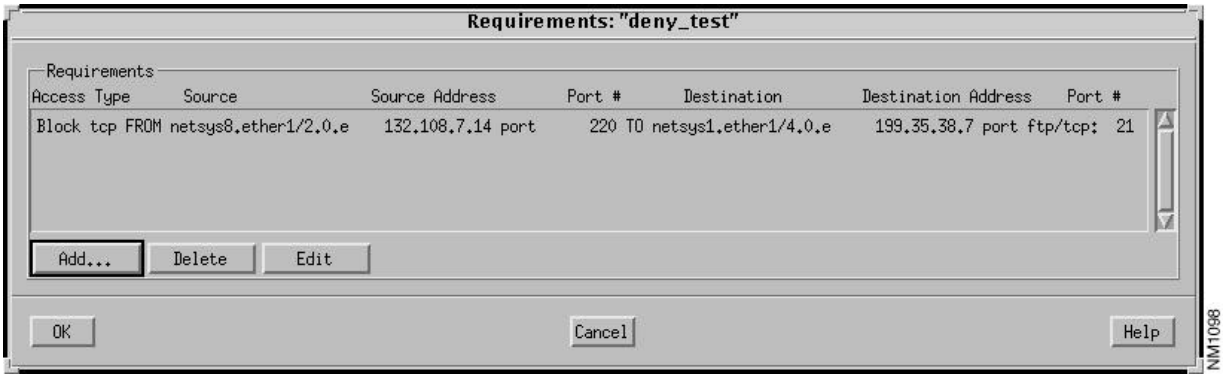

Figure 8-16 Requirements Window: deny_test Requirement Set Created

Step 32 Click on the **OK** button in the Requirements window.

The Requirements Set window is displayed. The *deny_test* requirement file set is displayed in the **Requirements File** list in the Requirement Sets window.

Step 33 Select the previously loaded requirements file (*tcp_telnet_test*) then click on the **Unload** button.

The *tcp_telnet_test* connectivity requirements are unloaded from analysis. Next load the *deny_test* connectivity requirements.

Step 34 Select the *deny_test* connectivity requirements file set from the **Requirements File** list, then click on the **Load** button followed by the **OK** button.

The *deny_test* set of connectivity requirements are loaded for analysis.

Step 35 Reanalyze the new connectivity requirements and inspect the results.

The results of the analysis on the *deny_test* connectivity requirements are displayed in the Requirements Analysis window, partially shown in Figure 8-17. A connectivity requirement entry with a SECURITY status indicates the connection is not permitted by an access list entry.

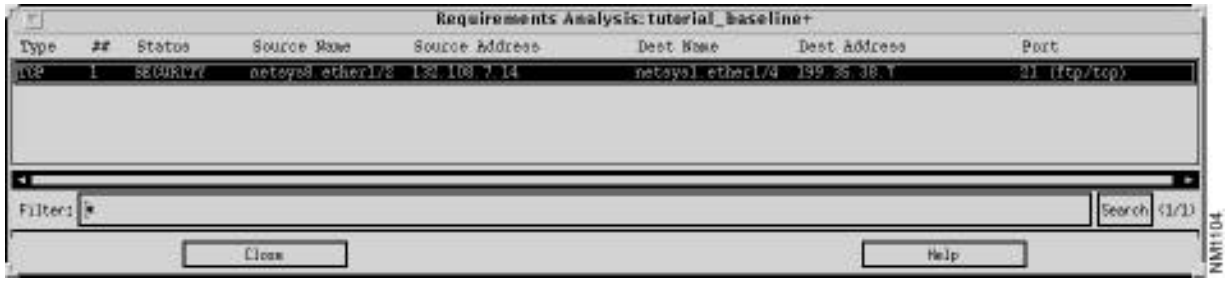

Figure 8-17 Requirements Analysis Window: Security Path