Security Labs in OPNET IT Guru

Enginyeria i Arquitectura La Salle

Universitat Ramon Llull

Barcelona 2004

Security Labs in OPNET IT Guru

Authors:

Cesc Canet

Juan Agustín Zaballos

Translation from Catalan:

Cesc Canet

Overview

This project consists in practical networking scenarios to be done with OPNET IT Guru Academic Edition, with a particular interest in security issues.

The first two parts are a short installation manual and an introduction to OPNET. After that there are 10 Labs that bring into practice different networking technologies. Every Lab consists in a theoretical introduction, a step-by-step construction of the scenario and finally Q&A referring to the issues exposed.

Lab 1: ICMP Ping, we study Ping traces and link failures.

Lab 2: Subnetting and OSI Model, we study tiers 1,2 and 3 of the OSI model, and the Packet Analyzer tool to observe TCP connections.

Lab 3: Firewalls, we begin with proxies and firewalls. We will deny multimedia traffic with a proxy, and study the link usage performance.

Lab 4: RIP explains the RIP routing protocol, and how to create timed link failures and recoveries.

Lab 5: OSPF compares RIP. We study areas and Load Balancing.

Lab 6: VPN studies secure non-local connections. A Hacker will try to access into a server that we will try to protect using virtual private networks.

Lab 7: VLAN creates user logical groups with Virtual LANs. Studies One-Armed-Router interconnections.

Lab 8: Dual Homed Router/Host, **Lab 9: Screened Host/Subnet. DMZ** and **Lab 10: Collapsed DMZ** explains the static routing tables, ACLs, proxies and internal vs. perimetric security. Lab 10 is 100% practical, we want you to create it on your own, a piece of cake if you did the other Labs!

Lab 4: RIP

The RIP Protocol (Routing Information Protocol) is, in a nutshell:

- Designed to reach a stable routing table with the less Administrator management as possible.
- The messages that routers send each other are sent to the multicast address to reduce the hosts processing load.
- It is a Intra-Domain and Vector-Distance protocol based in the Bellman-Ford algorithm.
- Uses the hop count metric.
- It is used in middle-size networks with no more than 15 hops.
- RIP messages are encapsulated inside UDP (port 520) and are sent once every 30 seconds, even if there are no changes in the network.
- No authentication is required.
- It was released in BSD Unix for the first time. The first version was RIPv1, a classful routing protocol. RIPv2 extended it using classless routing and other advantages.
- It is defined in RFC 1058 (RIPv1) and RFC 2453 (RIPv2). The RFC 2091 supports Triggered Extension.

All routers in the network have a routing table to indicate the link to forward IP packets . Every 30 seconds, all routers send UDP messages to the surrounding routers, indicating the distance, expressed in hops, to the other routers.
The router that receives the UDP message increases 1 unit the distance and will lookup in its tables if there's a shortest path to the destination. If there's no shorter link then the routing tables will be updated.

After several iterations the protocol will converge, and every router in the network will know how to route each IP packet it receives, and this route will be the shortest.

Lab Description

Four routers are connected each other in a ring topology. Each router has two LANs attached. We are going to design three scenarios: **NoFailure**, where all the links will work; **WithFailure**, with a specific link that is going to fail during the simulation and stops working in the future: **WithFailureAndRecovery**, where the link that failed is recovered later, and restarts working as before.
The purpose of this scenario is to represent with a bar chart the routing table updates and to see the evolution of the routing tables.

Creating the Scenario

1. Open a new project in OPNET IT Guru Academic Edition (**File→New Project**) with the following parameters (leave default values for the remainder):

    - **Project Name**: **<your_name>_RIP**
    - **Scenario Name**: **SenseFallida**
    - **Network Scale**: **Campus**

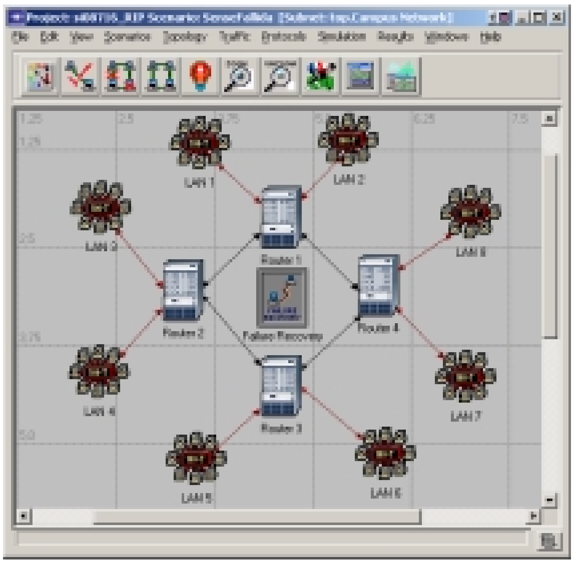
    Use the **Next** button in the Startup Wizard until the end. A new blank grid shall open in the Project Editor.

2. Deploying devices and controls upon the Grid:
    The following table summarizes all the nodes that have to be deployed in the scenario, and the Object Palette where can be found.

Qty	Component	Palette	Description
4	ethernet4_slip8_gtwy	internet_toolbox	Routers
8	100BaseT_LAN	internet_toolbox	LAN network model
1	Failure Recovery	utilities	Failure and Recovery Control
4	PPP_DS3	links	To connect the routers each other
8	100BaseT	internet_toolbox	To connect the routers with the LANs.

L4.1 Components list

Rename all the components as seen in picture L4.2. Hereinafter we will refer them by their name.



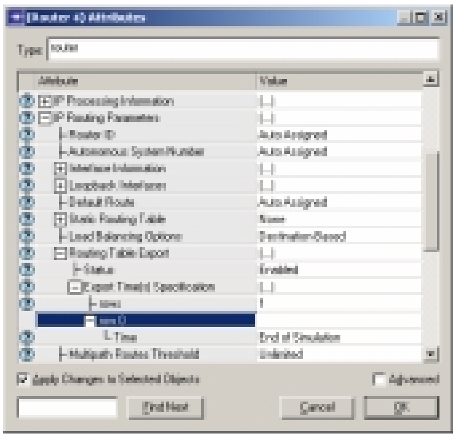
L4.2 The scenario with the names of the nodes

The fastest way to create the scenario is to create first **Router 1,LAN 1** and **LAN 2** with their names, and connect them with wires. After that, copy the whole structure and paste it three times. OPNET manages the name nodes to make a succession. Finally, connect the routers with **PPP_DS3**, deploy a Failure Recovery control and rename it.

3. Exporting routing tables to the Simulation Log:

   Select all the routers of the scenario, **right click** on any and **Edit Attributes**. Check the following options:

   - **IP Routing Parameters→Routing Table Export→**
   - **Status**: **Enabled**
   - **Export Time(s) Specification → row 0 → Time**: **End of Simulation**
   - **Apply Changes to Selected Objects** (To perform changes on all the routers of the scenario).



L4.3 Exporting the routing tables

4. Statistics:

From the Project Editor, **right click** on the Grid and **Choose Individual Statistics**. Select the following statistics in the **Choose Results** dialog. Click **OK**.

- **Global Statistics→RIP→Traffic Sent (bits/sec)**
- **Global Statistics→RIP→Traffic Received (bits/sec)**
- **Node Statistics→Route Table→Total Number of Updates**

5. Simulation configuration:

In the Project Editor, click on **configure/run simulation** , and use the following parameters:

- **Duration: 10 minute(s)**.
- On the **Global Attributes** tab,
    - o **IP Dynamic Routing Protocol**: **RIP**. This sets RIP protocol for all the routers in the scenario. We can do this also in the Project Editor doing **Protocols→IP→Routing→Configure Routing Protocols** and setting RIP in all interfaces.
    - o **IP Interface Addressing Mode**: **Auto Addressed / Export**
    - o **RIP Sim Efficiency**: **Disabled**. If this attribute is Enabled, the RIP protocol will stop after the "Stop Time". But instead of this, we want it to continue updating the routing tables when there are changes. This is precisely what we will do in the second scenario, by programming a controlled link failure to study routing changes.

- **RIP Stop Time**: **10000** will ensure that the tables won't stop updating during the simulation.
- **IP Routing Table Export/Import**: **Export**. This will export the routing tables to a file when the simulation ends.

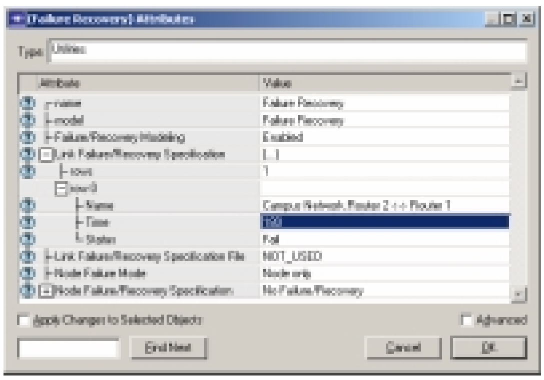
When finished, click **OK** (do not run the simulation yet).

Creating the second and third scenarios

In the scenario we just build up, the routers maintain their routing tables and are not going to be updated anymore if there are no network failures, so once all the routes are set, they won't change at all. We first want to study the effect of a router failure, to see how RIP can learn new routes.

1. In the Project Editor, **Scenario→Duplicate Scenario..** and call it **WithFailure**.

   Right click on the Failure object, and **Edit Attributes**, expand the **Link Failure/Recovery Specification** branch, set **rows**: **1** and unfold the branch of the new row. Use the following data:

   L4.4 Programming a link failure

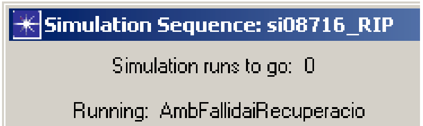
   We have established a failure for *Router 2 – Router 1* link, 180 seconds after the simulation start. Click **OK** to close the dialog.

2. Creating the third scenario:
   Now we create the third scenario: **WithFailureAndRecovery** with the same parameters as the second but 180 seconds after the link failure (i.e., 360 seconds after the simulation start), the link will recover. Repeat the steps as before but this time use **Status: Recovery**.

3. Run the simulation of the three scenarios at the same time:

   In the Project Editor, **Scenarios→Manage Scenarios**… Change values of column **Results** and click **<collect>** or **<recollect>** on every scenario.

   When we click **OK** now, the 3 simulations will run in sequence. Click on **Close** when the three simulations are over (wait for **Simulation runs to go** to be **0**).



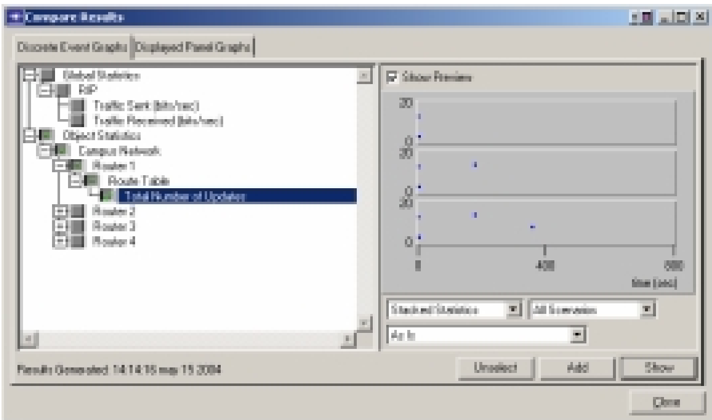
L4.5 Detail of Simulation sequence dialog

Results analysis

1. Compare the number of updates of the routing tables done by the RIP protocol (**Q1**).

   - In the Project Editor, **Results→Compare Results**.

     We can see in picture L4.6 that we have to choose **Stacked Statistics** and **All Scenarios** to show the graphics of all scenarios at the same time, but with overlaid charts to compare results.



L4.6 Compare Results

   - Select the statistic **Total Number of Updates** for Router1 and click on **Show**.
   - The two graphics appear now. **Right click** on each scenario and select **Draw Style→Bar**.

2. Obtaining the IP addresses of the interfaces (needed to study the routing tables). (**Q2**).

   The IP addresses of all the interfaces are generated automatically during the simulation. When we set **IP Interface Addressing Mode**: **Auto Addressed/Export** we made all this information to be able for analysis. We will export this data into a Generic Data File (gdf).

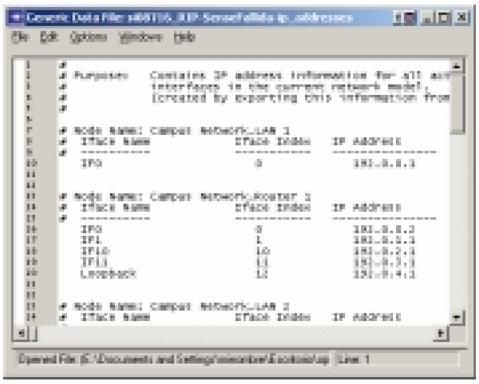
   - On the System window, choose **File→Model Files→Refresh Model Directories**. OPNET will search the models directory and update the file list.

L4.7 Refresh Model Directories

Don't forget that the System window can be open in the Project Editor if its closed (**Windows→System**).

   - In the System window: **File→Open**, and choose **Generic Data File**. Use the filename **<your_name>_RIP-NoFailure-ip_addresses**. This file is generated automatically during the simulation. Click **OK**.

An editor will pop up with the Generic Data File we choose. This contains the IP addresses of all the active interfaces in our network model.



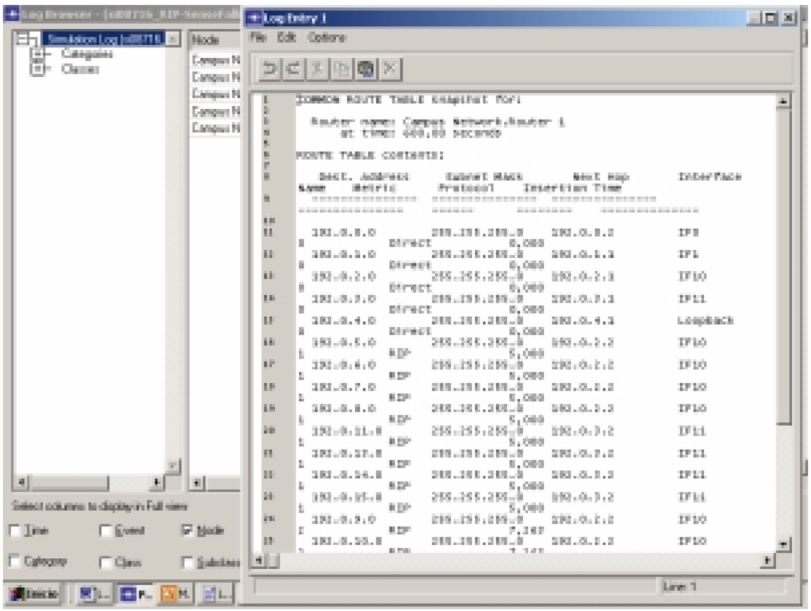
L4.8 Generic Data File with the IP addresses

3. Comparing the routing tables:

   Steps to visualize the routing tables of a router, for instance *Router 1*, for the two scenarios (**Q3**):

   - In the Project Editor, **Results→Open Simulation Log**.
   - Click on the **COMMON ROUTE TABLE** entry for the router.

   The routing tables export is not saved until the end, because we are using the *Once at End of Simulation* option.



L4.9 *Router 1* routing table

Questions

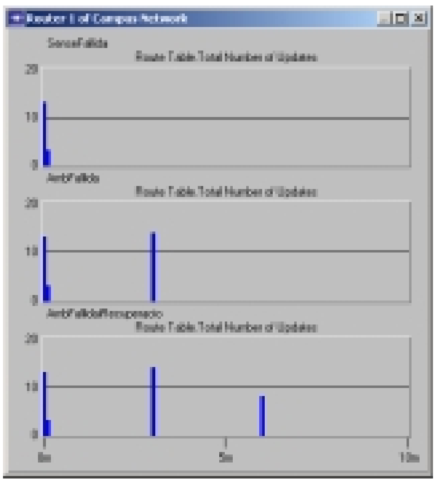
Q1 Create a routing table update bar chart for Router 1 throughout all 3 scenarios, and analyze it.

Q2 Write down the IP addresses for all interfaces on picture L4.2. They may differ depending on the creation order.

Q3 Compare the routing tables for Router 1 throughout all 3 scenarios. Routing tables are visible in the Simulation Log for all the scenarios (**Scenarios→Switch to Scenario** in the Project Editor). Compare the ingoing routes to LAN 3, LAN 4 and Router 2 loopback. Pay attention to these fields: Next Hop, Insertion Time and Metric.

Answers

Q1 Routing tables do not differ much during the simulation unless there are any changes, like a link failure or recovery.

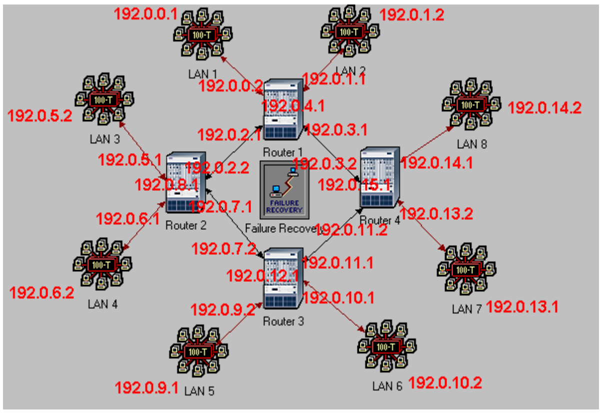


L4.10 Router 1 table updates

Q2 This is the .gdf file generated and the IP addresses for all interfaces on the network:

```
#
# Purpose:   Contains IP address information for all active
#            interfaces in the current network model.
#            (created by exporting this information from the model.)
#

# Node Name: Campus Network.LAN 1
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF0                     0             192.0.0.1        255.255.255.0    Campus Network.LAN 1 <-> Router 1


# Node Name: Campus Network.Router 1
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF0                     0             192.0.0.2        255.255.255.0    Campus Network.LAN 1 <-> Router 1
   IF1                     1             192.0.1.1        255.255.255.0    Campus Network.LAN 2 <-> Router 1
   IF10                    10            192.0.2.1        255.255.255.0    Campus Network.Router 2 <-> Router 1
   IF11                    11            192.0.3.1        255.255.255.0    Campus Network.Router 1 <-> Router 4
   Loopback                12            192.0.4.1        255.255.255.0    Not connected to any link.


# Node Name: Campus Network.LAN 2
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF0                     0             192.0.1.2        255.255.255.0    Campus Network.LAN 2 <-> Router 1


# Node Name: Campus Network.Router 2
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF1                     1             192.0.5.1        255.255.255.0    Campus Network.LAN 3 <-> Router 2
   IF2                     2             192.0.6.1        255.255.255.0    Campus Network.LAN 4 <-> Router 2
   IF10                    10            192.0.2.2        255.255.255.0    Campus Network.Router 2 <-> Router 1
   IF11                    11            192.0.7.1        255.255.255.0    Campus Network.Router 3 <-> Router 2
   Loopback                12            192.0.8.1        255.255.255.0    Not connected to any link.


# Node Name: Campus Network.LAN 3
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF0                     0             192.0.5.2        255.255.255.0    Campus Network.LAN 3 <-> Router 2


# Node Name: Campus Network.LAN 4
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF0                     0             192.0.6.2        255.255.255.0    Campus Network.LAN 4 <-> Router 2


# Node Name: Campus Network.LAN 5
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF0                     0             192.0.9.1        255.255.255.0    Campus Network.LAN 5 <-> Router 3


# Node Name: Campus Network.Router 3
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF0                     0             192.0.9.2        255.255.255.0    Campus Network.LAN 5 <-> Router 3
   IF1                     1             192.0.10.1       255.255.255.0    Campus Network.LAN 6 <-> Router 3
   IF10                    10            192.0.7.2        255.255.255.0    Campus Network.Router 3 <-> Router 2
   IF11                    11            192.0.11.1       255.255.255.0    Campus Network.Router 4 <-> Router 3
   Loopback                12            192.0.12.1       255.255.255.0    Not connected to any link.


# Node Name: Campus Network.LAN 6
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF0                     0             192.0.10.2       255.255.255.0    Campus Network.LAN 6 <-> Router 3


# Node Name: Campus Network.LAN 7
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF0                     0             192.0.13.1       255.255.255.0    Campus Network.LAN 7 <-> Router 4


# Node Name: Campus Network.Router 4
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF0                     0             192.0.13.2       255.255.255.0    Campus Network.LAN 7 <-> Router 4
   IF1                     1             192.0.14.1       255.255.255.0    Campus Network.LAN 8 <-> Router 4
   IF10                    10            192.0.11.2       255.255.255.0    Campus Network.Router 4 <-> Router 3
   IF11                    11            192.0.3.2        255.255.255.0    Campus Network.Router 1 <-> Router 4
   Loopback                12            192.0.15.1       255.255.255.0    Not connected to any link.


# Node Name: Campus Network.LAN 8
#  Iface Name           Iface Index   IP Address       Subnet Mask      Connected Link
#  ----------           -----------   ---------------  ---------------  ----------------
   IF0                     0             192.0.14.2       255.255.255.0    Campus Network.LAN 8 <-> Router 4
```

L4.11 Generic Data File (gdf)



L4.12 IP Addresses for all interfaces

Q3 The tables produced at the end of the simulation for the first 3 scenarios can be seen in picture below. Routes to networks 192.0.5.0/24, 192.0.6.0/24 and 192.0.8.0/24 appear in red color. They're the networks of the two LANs connected to Router 2. Router 1 has direct access (Metric = 1) when there's no link failure. When the link fails, however, access is granted though using another path, Metric and Next Hop. When the link is up once again, the routing table is identical as the first scenario, but the Insertion Time is delayed.

- NoFailure

COMMON ROUTE TABLE snapshot for:

Router name: Campus Network.Router 1
at time: 600,00 seconds

ROUTE TABLE contents:

Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol	Insertion Time
192.0.0.0	255.255.255.0	192.0.0.2	IF0	0	Direct	0,000
192.0.1.0	255.255.255.0	192.0.1.1	IF1	0	Direct	0,000
192.0.2.0	255.255.255.0	192.0.2.1	IF10	0	Direct	0,000
192.0.3.0	255.255.255.0	192.0.3.1	IF11	0	Direct	0,000
192.0.4.0	255.255.255.0	192.0.4.1	Loopback	0	Direct	0,000
192.0.5.0	**255.255.255.0**	**192.0.2.2**	**IF10**	**1**	**RIP**	**5,000**
192.0.6.0	**255.255.255.0**	**192.0.2.2**	**IF10**	**1**	**RIP**	**5,000**
192.0.7.0	255.255.255.0	192.0.2.2	IF10	1	RIP	5,000
192.0.8.0	**255.255.255.0**	**192.0.2.2**	**IF10**	**1**	**RIP**	**5,000**
192.0.11.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.13.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.14.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.15.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.9.0	255.255.255.0	192.0.2.2	IF10	2	RIP	7,263
192.0.10.0	255.255.255.0	192.0.2.2	IF10	2	RIP	7,263
192.0.12.0	255.255.255.0	192.0.2.2	IF10	2	RIP	7,263

L4.13

- WithFailure

COMMON ROUTE TABLE snapshot for:

Router name: Campus Network.Router 1
at time: 600,00 seconds

ROUTE TABLE contents:

Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol	Insertion Time
192.0.0.0	255.255.255.0	192.0.0.2	IF0	0	Direct	0,000
192.0.1.0	255.255.255.0	192.0.1.1	IF1	0	Direct	0,000
192.0.2.0	255.255.255.0	192.0.2.1	IF10	0	Direct	0,000
192.0.3.0	255.255.255.0	192.0.3.1	IF11	0	Direct	0,000
192.0.4.0	255.255.255.0	192.0.4.1	Loopback	0	Direct	0,000
192.0.11.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.13.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.14.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.15.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.5.0	**255.255.255.0**	**192.0.3.2**	**IF11**	**3**	**RIP**	**185,000**
192.0.6.0	**255.255.255.0**	**192.0.3.2**	**IF11**	**3**	**RIP**	**185,000**
192.0.7.0	255.255.255.0	192.0.3.2	IF11	2	RIP	185,000
192.0.8.0	**255.255.255.0**	**192.0.3.2**	**IF11**	**3**	**RIP**	**185,000**
192.0.9.0	255.255.255.0	192.0.3.2	IF11	2	RIP	185,000
192.0.10.0	255.255.255.0	192.0.3.2	IF11	2	RIP	185,000
192.0.12.0	255.255.255.0	192.0.3.2	IF11	2	RIP	185,000

L4.14

- WithFailureAndRecovery

COMMON ROUTE TABLE snapshot for:

Router name: Campus Network.Router 1
at time: 600,00 seconds

ROUTE TABLE contents:

Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol	Insertion Time
192.0.0.0	255.255.255.0	192.0.0.2	IF0	0	Direct	0,000
192.0.1.0	255.255.255.0	192.0.1.1	IF1	0	Direct	0,000
192.0.2.0	255.255.255.0	192.0.2.1	IF10	0	Direct	0,000
192.0.3.0	255.255.255.0	192.0.3.1	IF11	0	Direct	0,000
192.0.4.0	255.255.255.0	192.0.4.1	Loopback	0	Direct	0,000
192.0.11.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.13.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.14.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.15.0	255.255.255.0	192.0.3.2	IF11	1	RIP	5,000
192.0.9.0	255.255.255.0	192.0.3.2	IF11	2	RIP	185,000
192.0.10.0	255.255.255.0	192.0.3.2	IF11	2	RIP	185,000
192.0.12.0	255.255.255.0	192.0.3.2	IF11	2	RIP	185,000
192.0.5.0	**255.255.255.0**	**192.0.2.2**	**IF10**	**1**	**RIP**	**365,000**
192.0.6.0	**255.255.255.0**	**192.0.2.2**	**IF10**	**1**	**RIP**	**365,000**
192.0.7.0	255.255.255.0	192.0.2.2	IF10	1	RIP	365,000
192.0.8.0	**255.255.255.0**	**192.0.2.2**	**IF10**	**1**	**RIP**	365,000

L4.15