LAB 4

# VLANs: Virtual Local Area Networks

## Logically Partitioning a Physical Network into Several Separate LANs

### OBJECTIVES

The objective of this lab is to study how to divide a physical network into a number of separate logical networks using virtual local area networks (VLANs) with the benefit of decreasing collision domain and adding more security.

### OVERVIEW

Virtual LANs (VLANs) allow a single extended LAN to be partitioned into several seemingly separate LANs. Each virtual LAN is assigned an identifier (sometimes called a color), and packets can only travel from one segment to another if both segments have the same identifier. This has the effect of limiting the number of segments in an extended LAN that will receive any given broadcast packet. An attractive feature of VLANs is that it is possible to change the logical topology without moving any wires or changing any addresses.

In this lab, we will build a network for a university with two departments. Each department has three local area networks. One LAN is for the professors, the second is for the staff members, and the third is for the students. The university has three servers: one server is for research, the second is for human resources databases, and the third server is for online courses (e-learning). In the first scenario, the setting of the network allows all members of both departments to have access to all three servers. Even a hacker who plugs his or her computer into any of the network switches can also have access to the network servers.

The second scenario uses VLANs to allow access to the research server only by professors. The staff members are allowed to access only the human resources server. The students can only access the e-learning server. The VLANs settings will not allow a hacker to have access to any of the servers.

In the third scenario, a router is added to allow for communication between different VLANs. Here we will allow both the professors and students to communicate with each other and to have access to both the research and e-learning servers. The simulation results show us that VLANs also decrease the load on some of the links in the networks.

### PRE-LAB ACTIVITIES

📖 Read Section 3.1.4 from *Computer Networks: A Systems Approach*, 5*th Edition*.

## PROCEDURE

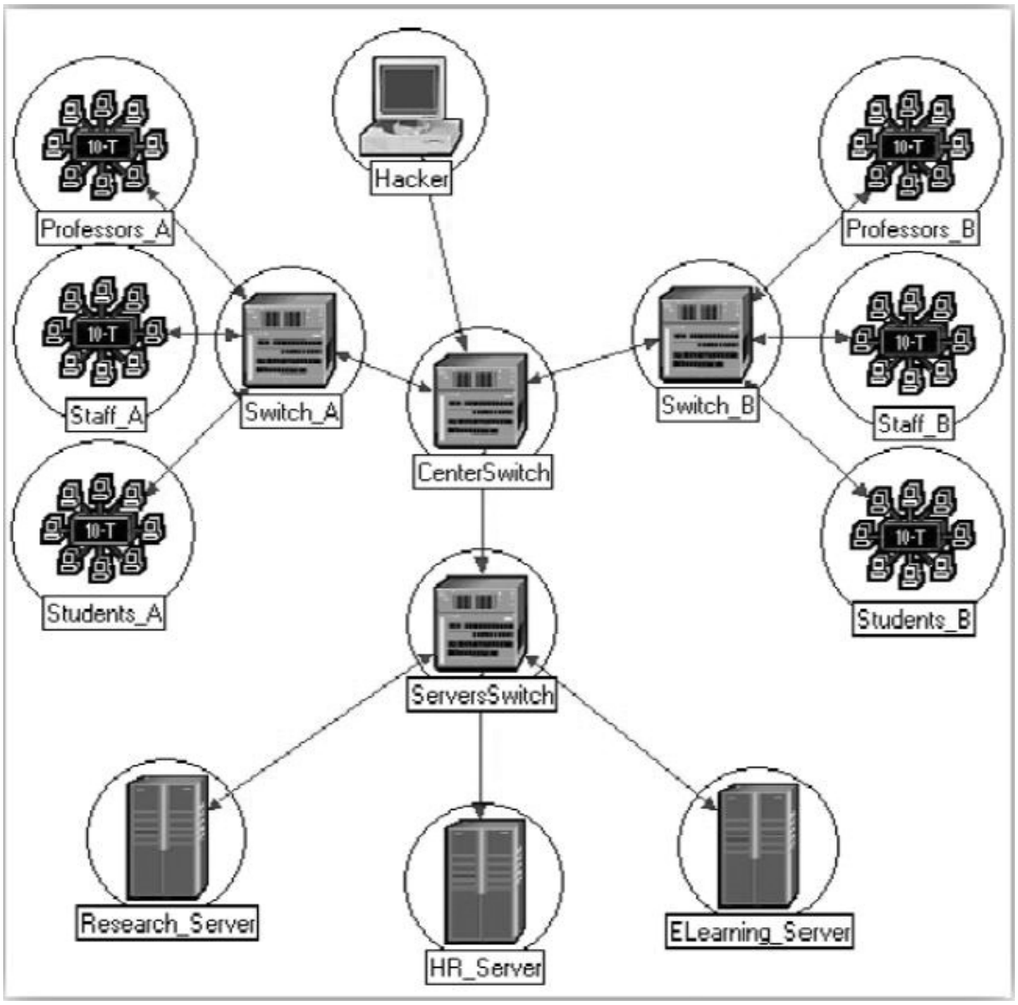
### Create a New Project

1. Start **OPNET IT Guru Academic Edition** → Choose **New** from the **File** menu.
2. Select **Project** and click **OK** → Name the project **<your initials>_VLAN**, and the scenario **NoVLAN** → Click **OK**.
3. In the ***Startup Wizard: Initial Topology*** dialog box, make sure that **Create Empty Scenario** is selected → Click **Next** → Choose **Campus** from the ***Network Scale*** list → In the ***Startup Wizard: Specify Size*** dialog box, assign the following: **Size** = **Kilometers**, **X Span** = **1**, and **Y Span** = **1** → Click **Next** two times → Click **OK**.

### Create and Configure the Network

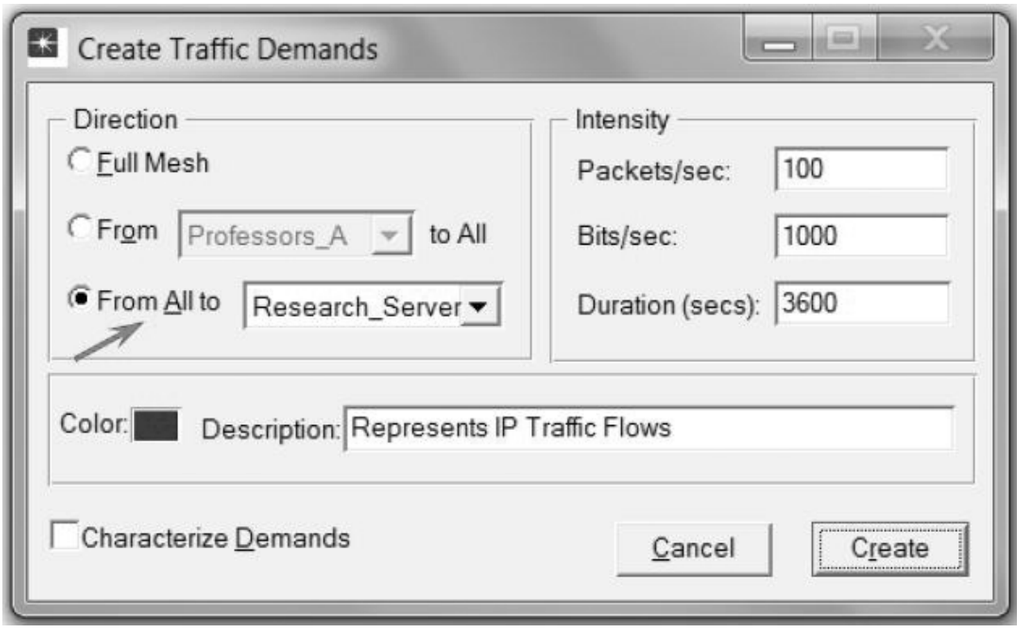
Network components:

1. Open the *Object Palette* dialog box by clicking  . Make sure that the **internet_toolbox** item is selected from the pull-down menu on the object palette. Add the following objects from the palette to the project workspace (see the following figure for placement):
   a. Six **10BaseT_LAN**, four **ethernet16_switch**, three **Ethernet_server**, and one **ethernet_wkstn**.
   b. Connect the objects using **100BaseT** links and *rename* them as shown.
2. **Save** your project.



Configure the traffic demands:

1. Simultaneously select the **Research_Server**, the **Hacker**, and all six **LANs** → Select the **Protocols** menu → **IP** → **Demands** → **Create Traffic Demands**.
2. Select **From All** to **Research_Server** as shown → Click **Create**.

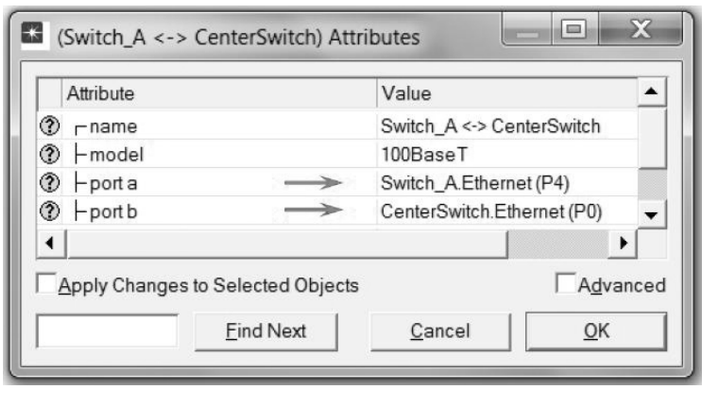





Here we have created traffic demands from all LANs and the Hacker to the Research_Server. Notice the dotted lines representing the demands.

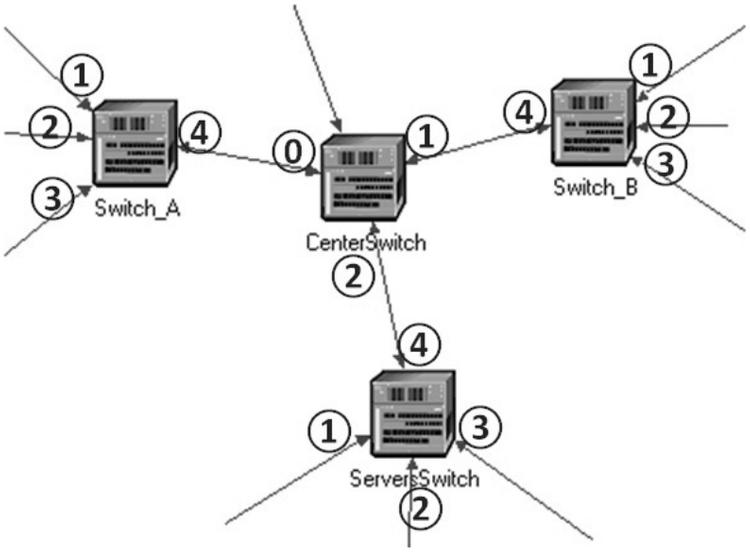
3. Repeat for the HR_Server: Simultaneously select the **HR_Server**, the **Hacker**, and all six **LANs** → Select the **Protocols** menu → **IP** → **Demands** → **Create Traffic Demands** → Select the **From All** to **HR_Server** → Click **Create**.
4. Repeat for the ELearning_Server: Simultaneously select the **ELearning_Server**, the **Hacker**, and all six **LANs** → Select the **Protocols** menu → **IP** → **Demands** → **Create Traffic Demands** → Select the **From All** to **ELearning_Server** → Click **Create**.
5. Press **Ctrl** + **Shift** + **M** to hide all traffic demands and **Ctrl** + **M** to show them again.
6. **Save** your project.

Configure the links ports:



1. Edit the attributes of the network links so that their ports connected to the switches have the numbers indicated in the following figure. The preceding figure shows an example of the ports assigned to the link connecting Switch_A with the CenterSwitch.

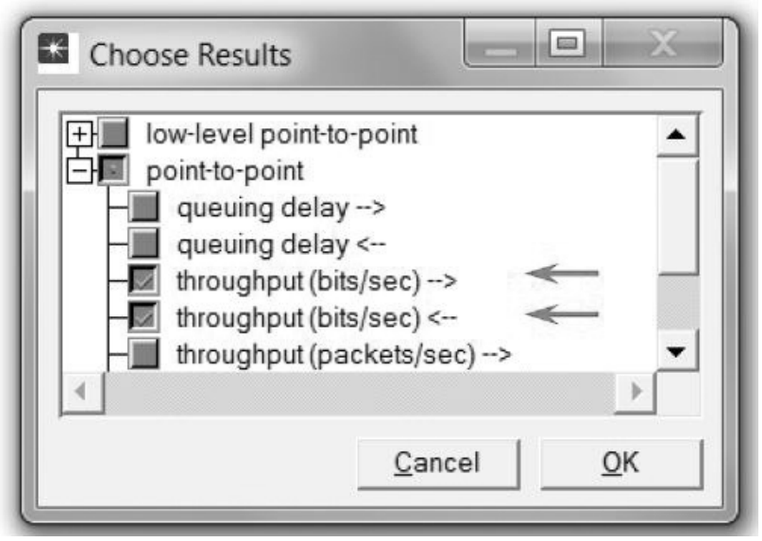
*Note:* If any one of the required ports is not available in the drop-down menu, pick another link to change first because you cannot choose a port that is already in use, and then go back to the previous link.






## Choose the Statistics

1. Right-click on the link connecting the **Research_Server** and the **ServersSwitch** → Select **Choose Individual Statistics** from the pop-up menu → Check the **throughput (bits/sec)** statistics as shown → Click **OK**.
2. Right-click on the link connecting the **CentralSwitch** and the **ServersSwitch** → Select **Choose Individual Statistics** from the pop-up menu → Check the **throughput (bits/sec)** statistics as shown → Click **OK**.
3. **Save** your project.

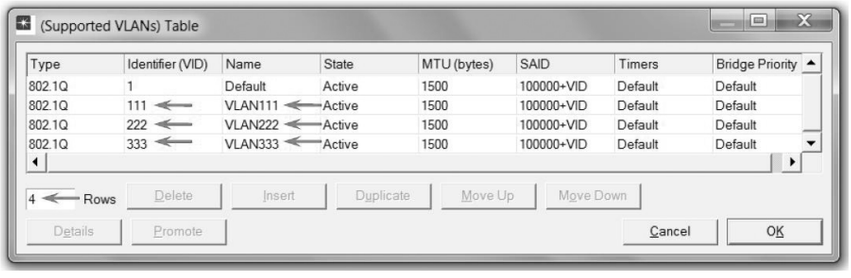


## The VLAN Scenario

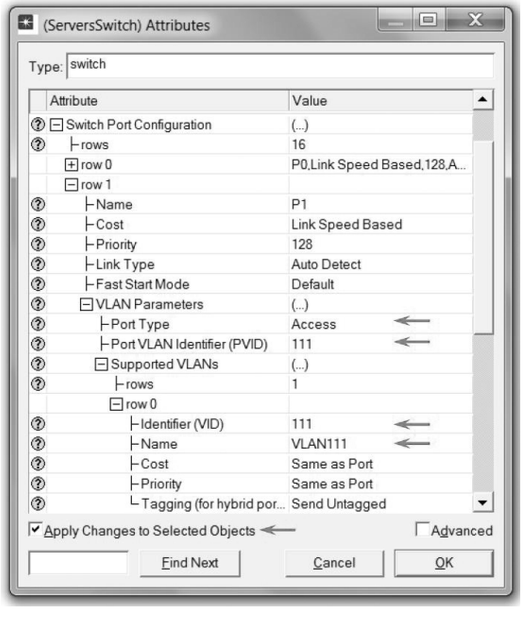
In the network we just created, the professors, students, staff, and even the hacker have access to the network of three servers. We need to create VLANs so that professors have access only to the Research_Server, staff members have access only to the HR_Server, and students have access only to the ELearning_Server. The hacker will not be granted access to any server. The following table shows the VLANs we plan to create and the members of each VLAN.

| VLAN Identifier (VID) | VLAN Members |
|---|---|
| 111 | Professors_A LAN, Professors_B LAN, and Research_Server. |
| 222 | Staff_A LAN, Staff_B LAN, and HR_Server. |
| 333 | Students_A LAN, Students_B LAN, and ELearning_Server. |

1. Select **Duplicate Scenario** from the **Scenarios** menu and name it **VLAN** → Click **OK**.
2. In the new scenario, select **Switch_A**, **Switch_B**, and **ServersSwitch** simultaneously → Right-click on any of them → Select **Edit Attributes** → Check the **Apply Changes to Selected Objects** check-box.
3. Expand the **VLAN Parameters** hierarchy → Assign **Port-Based VLAN** to the **Scheme** attribute → Edit the **Supported VLANs** attribute as shown in the following figure → Click **OK**.




4. Expand the **Switch Port Configuration** hierarchy.
5. Expand **row 1** hierarchy → Expand the **VLAN Parameters** hierarchy → Change the attributes for row 1 as shown in the following figure (recall that, in the selected switches, port 1 is connected to the members of VLAN 111):

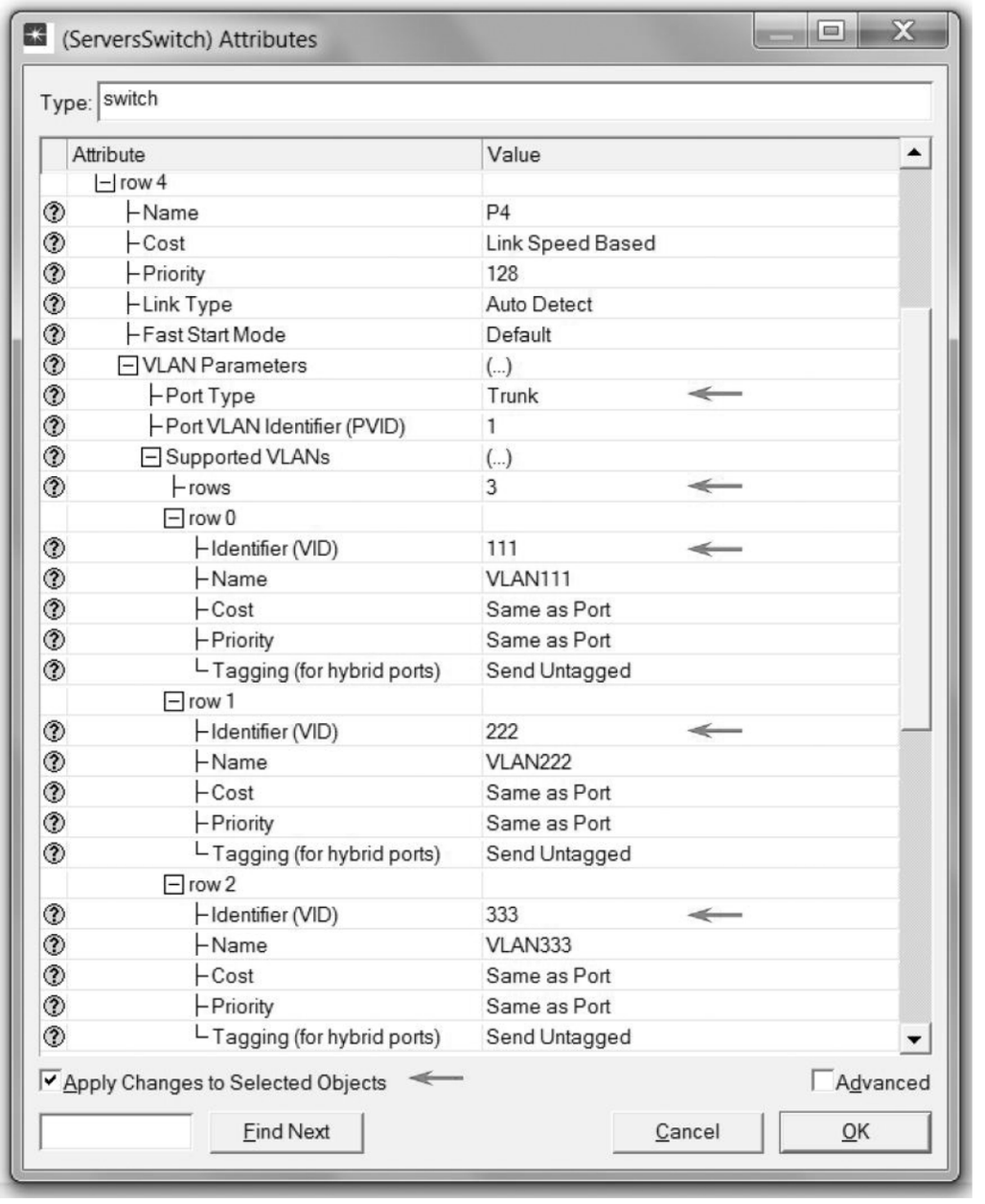



**Access** ports strip VLAN information from the packets before forwarding, while **trunk** ports always send packets VLAN-tagged, so they always contain VLAN information.

In typical configurations, access ports are used to connect end-nodes and VLAN-unaware nodes to the VLAN-aware bridged network, while trunk ports are used to connect the VLAN-ware bridges/switches of the bridged network to each other.

Regardless of their type, the ports can support as many VLANs as they want as long as these VLANs are supported by the surrounding node. Trunk ports are expected to support multiple VLANs, but they need to be configured under the sibling attribute "Supported VLANs" (i.e., they don't support all the VLANs by default).

6. Expand **row 2** hierarchy → Expand the **VLAN Parameters** hierarchy → Change the attributes for row 2 as we did for row 1 but assign VLAN 222 instead (recall that, in the selected switches, port 2 is connected to the members of VLAN 222).
7. Expand **row 3** hierarchy → Expand the **VLAN Parameters** hierarchy → Change the attributes for row 3 as we did for row 1 but assign VLAN 333 instead (recall that, in the selected switches, port 3 is connected to the members of VLAN 333).
8. Expand **row 4** hierarchy → Expand the **VLAN Parameters** hierarchy → Change the attributes for row 4 as shown in the following figure.
9. Click **OK** → **Save** your project.




10. Right-click on **CentralSwitch** only → Select **Edit Attributes**.

11. Expand the **VLAN Parameters** hierarchy → Assign **Port-Based VLAN** to the **Scheme** attribute → Edit the **Supported VLANs** attribute as in step 3 above → Click **OK**.
12. Expand the **Switch Port Configuration** hierarchy.
13. Change the attributes of **row 0**, **row 1**, and **row 2** exactly the same way we did in Step 8 with row 4 of the ServersSwitch.
14. Go to the **Protocols** menu → **VLAN** → **Visualize VLANs** → Take a note of the colors listed in the list → Click **OK**. Double check the following:
    a. All members to a VLAN have links with the same color.
    b. All trunk links have their assigned color.
    c. The hacker's link belongs to VID 1.

If you have any problem with the results of the visualization, go back and verify the steps of this configuring scenario.

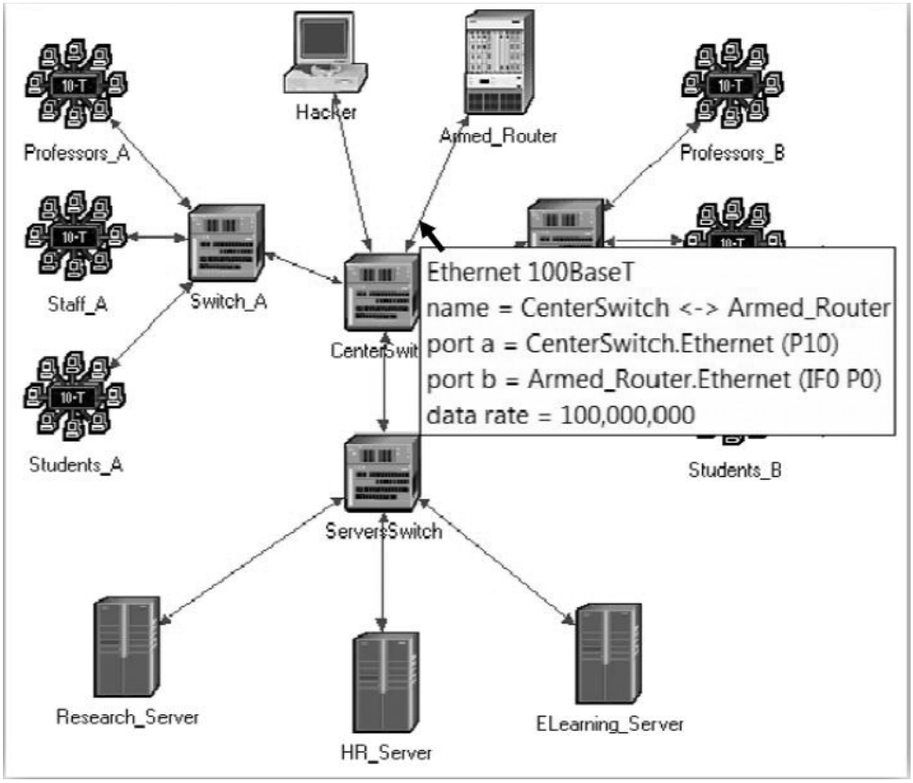
15. Click **OK** → **Save** your project.

## The VLAN_Comm Scenario

The VLAN scenario members of each VLAN are not allowed to communicate with members of any other VLAN. Assume that we need students to have access to the Research_Server and we need the professors to have access to the ELearning_Server. In this case, we need VLAN111 to communicate with VLAN333. This can be done on the IP layer by configuring a router to forward traffic between the two VLANs. Each VLAN will be assigned its own IP subnetwork.

1. While you are in the VLAN scenario, select **Duplicate Scenario** from the **Scenarios** menu and name it **VLAN_Comm** → Click **OK**.
2. Add to the project **ethernet_one_armed_router** from the **VLANs Palette** → Connect it to the **CenterSwitch** using **100BaseT** link → Click on the new link and record the port number in the CenterSwitch connected to it (it is P10 in the following figure).

The **one-armed router** node model represents an IP-based, one-armed router supporting one Ethernet interface. IP packets arriving on the interface are routed to the same interface. This gateway is typically used for inter-VLAN communication.



3. Right-click on **CentralSwitch** only → Select **Edit Attributes** → Expand the **Switch Port Configuration** hierarchy → Expand the row of the port you recorded in the previous step (in my project, it is **row 10**) → Change its **VLAN Parameters** and **Supported VLANs** the same way we did with row 0 in the same switch.
4. Click **OK** → **Save** your project.

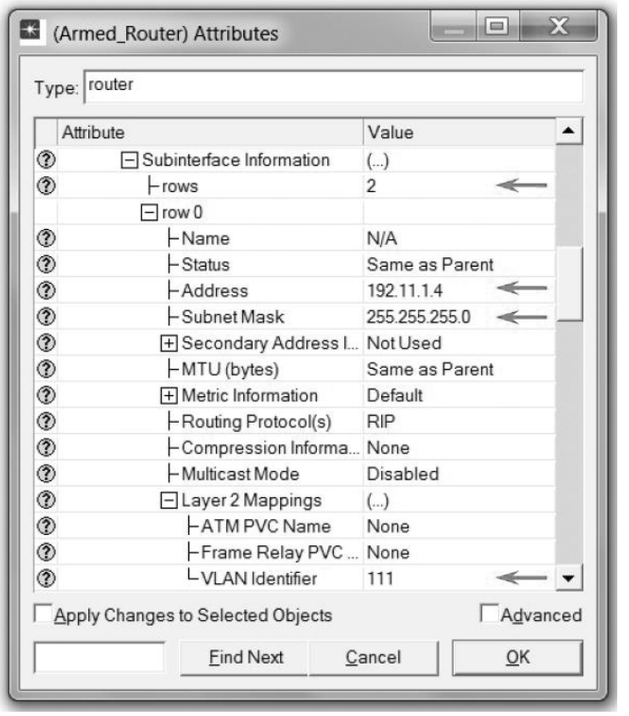
Now we need to assign the members of each VLAN to the same IP subnetwork, as shown in the following table.

| VLAN ID | VLAN Members | IP/Mask |
|---|---|---|
| 111 | Professors_A LAN | 192.11.1.1 / 255.255.255.0 |
| | Professors_B LAN | 192.11.1.2 / 255.255.255.0 |
| | Research_Server | 192.11.1.3 / 255.255.255.0 |
| 222 | Staff_A LAN | 192.22.2.1 / 255.255.255.0 |
| | Staff_B LAN | 192.22.2.2 / 255.255.255.0 |
| | HR_Server | 192.22.2.3 / 255.255.255.0 |
| 333 | Students_A LAN | 192.33.3.1 / 255.255.255.0 |
| | Students_B LAN | 192.33.3.2 / 255.255.255.0 |
| | ELearning_Server | 192.33.3.3 / 255.255.255.0 |

5. Right-click on each of the VLAN members in the previous table → **Edit Attributes** → **IP Host Parameters** → **Interface info** → Assign the **Address** and **Subnet Mask** shown in the previous table. (*Hint:* You can select multiple members and change their attributes at once, then revisit them one by one to edit the IP addresses to match those in the table.)
6. Right-click on the **Armed_Router** → **Edit Attributes** → **IP Routing Parameters** → **Interface Information** → **row 0** → Assign **Address = NO IP Address** → Expand the **Subinterface Information** hierarchy → Assign 2 to the rows.
7. Set the attributes of **row 0** as shown in the following figure:



**Layer 2 Mappings**: **VLAN Identifier** specifies the identifier of the VLAN to which this subinterface belongs. There should not be another subinterface of the same physical interface belonging to the same VLAN. In other words, within the domain of a physical interface, there has to be a 1:1 relation between the subinterfaces and the VLANs.



8. Set the same attributes for **row 1**, but assign 192.33.3.4 to the Address and 333 to the VLAN.
9. Click **OK** and **Save** your project.

## Run the Simulation

To run the simulation for the three scenarios simultaneously:

1. Go to the **Scenarios** menu → Select **Manage Scenarios**.
2. Change the values under the **Results** column to **<collect>** (or **<recollect>**) for the three scenarios. Set the **Sim Duration** to 0.5 hour, as shown in the following figure.




3. Click **OK** to run the three simulations. Depending on the speed of your processor, this process may take several seconds to complete.
4. After the three simulation runs complete, one for each scenario, click **Close**.

## View the Results

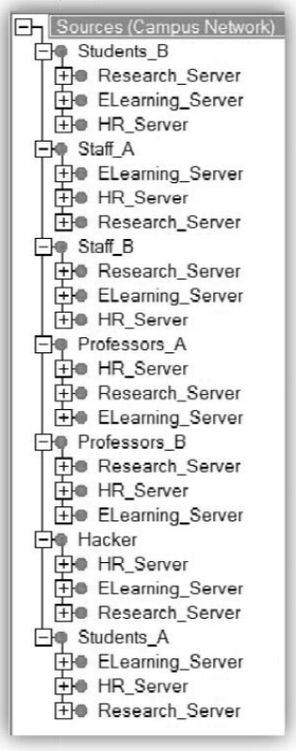
Compare the routes:

1. Go to the **NoVLAN** scenario → Select the **Protocols** menu → **IP** → **Demands** → **Display Routes for Configured Demands** → Click **OK**.
2. Repeat the previous step for the **VLAN** and **VLAN_Comm** scenarios.
3. Expand the routes hierarchies so that your results resemble those in the following figure. The demand route that is marked with a red bullet indicates an incomplete filtered route. The demand route that is marked with a green bullet indicates a complete route. Take note of which routes are complete and which ones are incomplete. You can click on a specific route and choose **Yes** under *Display* on the right pane. You can also click on **Show All Routes** to display all routes on the project workspace.

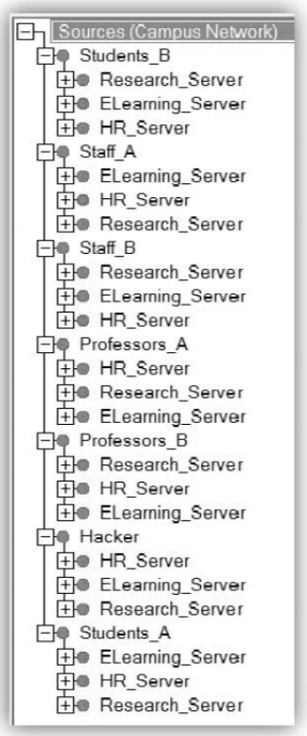
Compare the throughput:

1. Select **Compare Results** from the **Results** menu.
2. Show the results of the following two statistics:
   a. **Object Statistics → Campus Network → ServersSwitch <-> CenterSwitch → point-to-point → throughput (bits/sec)**. (Hint: Choose the throughput direction that brings results similar to the following one.)
   b. **Object Statistics → Campus Network → ServersSwitch <-> ResearchServer → point-to-point → throughput (bits/sec)**. (Hint: Choose the throughput direction that brings results similar to the following one.)

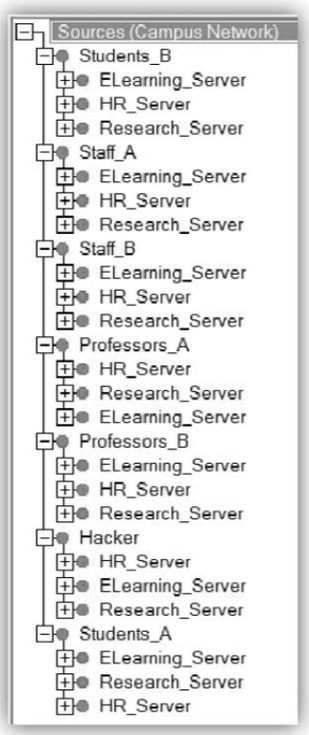
NoVLAN:




VLAN:

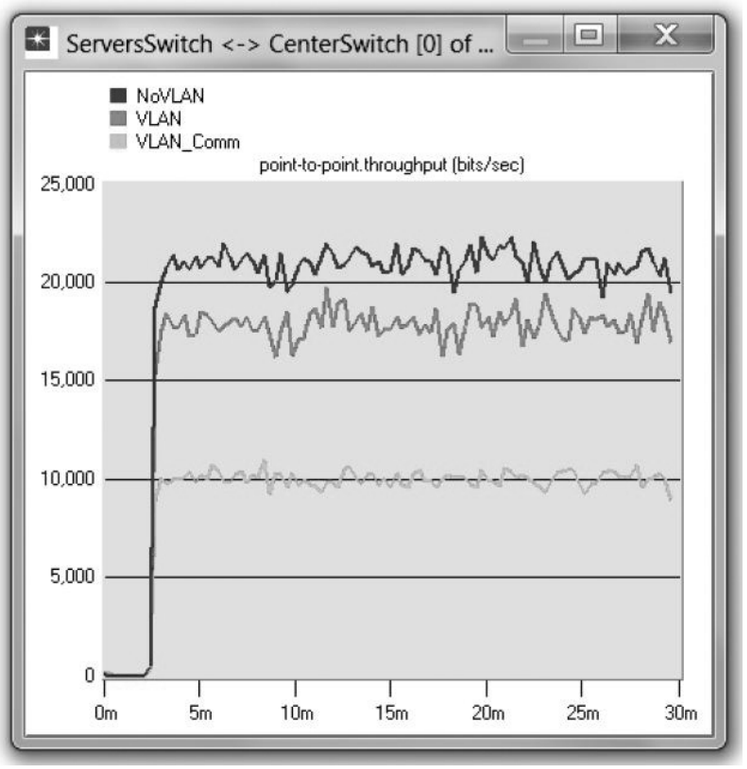


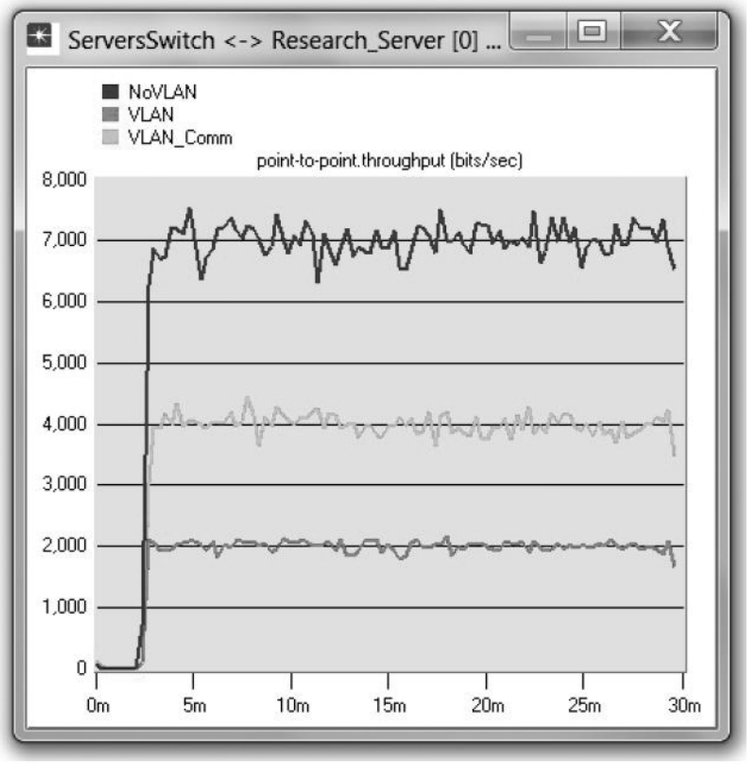

VLAN_Comm:






**3.** Your results should resemble the following figures:








## FURTHER READING

IEEE Standard for Virtual Bridged Local Area Networks (IEEE Std 802.1Q™-2005): http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf

## EXERCISES

1. On the results of the Routes for Configured Demands, elaborate on each route for the three scenarios, explaining why each is complete or incomplete.
2. In the graph showing the throughput of the link connecting the ServerSwitch and the CenterSwitch, explain why it is about 21,000 bits/sec, 18,000 bits/sec, and 10,000 bits/sec for the NoVLAN, VLAN, and VLAN_Comm scenarios, respectively.
3. In the graph showing the throughput of the link connecting the ServerSwitch and the Research_Server, explain why it is about 7000 bits/sec, 2000 bits/sec, and 4000 bits/sec for the NoVLAN, VLAN, and VLAN_Comm scenarios, respectively.
4. Create a new scenario called **VLAN_AllComm** as a copy from the **VLAN_Comm** scenario. Modify the new scenario so that all professors, staff members, and students have access to all three servers. The only one who is prevented from accessing the servers is the hacker.
   a. Display and comment on the **Routes for Configured Demands** for the new scenario.
   b. Compare the throughput of the links as in Exercises 2 and 3.

## LAB REPORT

Prepare a report that follows the guidelines explained in the Introduction Lab. The report should include the answers to the preceding exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.