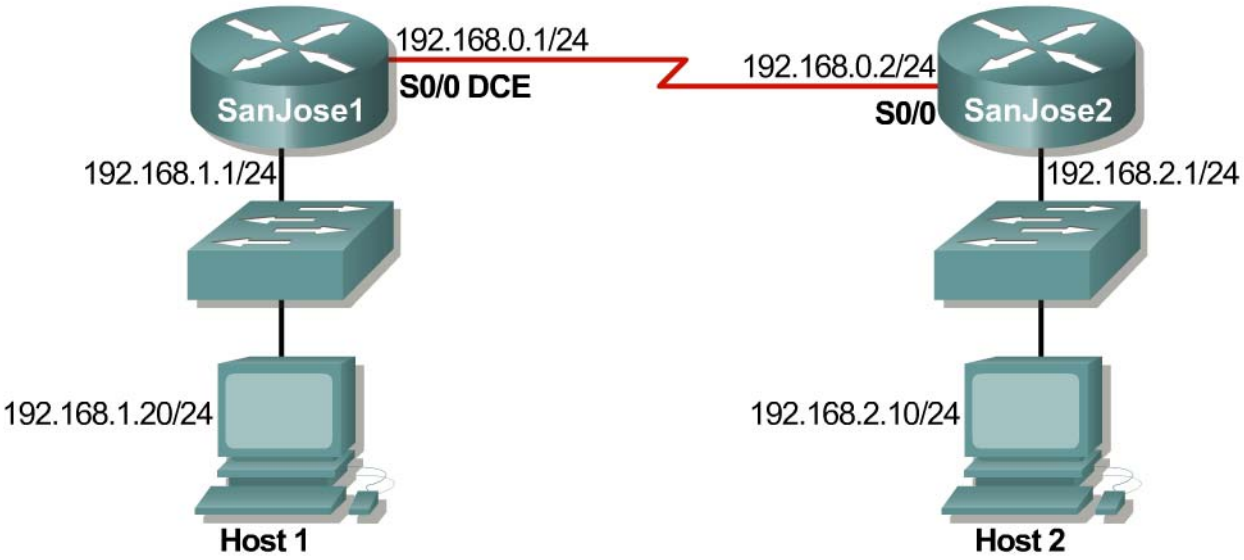
Lab 7.1.9a Introduction to Fluke Network Inspector – Instructor Version



Objective

This lab is a tutorial demonstrating how to use the Fluke Networks Network Inspector (NI) to discover and analyze network devices within a broadcast domain. This lab will demonstrate the key features of the tool that can be incorporated into various troubleshooting efforts in the remaining labs.

Background / Preparation

The Network Inspector software can distinguish workstations, servers, network printers, switches, and managed hubs, if they have been assigned a network address.

Options for conducting this lab.

1) Use Network Inspector in a small controlled LAN that is configured by the instructor in a closed lab environment as shown above. The minimum equipment should include a workstation, a switch, and a router.

2) Perform the steps in a larger environment such as the classroom or the school network to see more variety. Before attempting to run NI on the school LAN, check with the instructor and the network administrator.

The following is a list of points to consider:

1. Network Inspector detects the devices within a network subnet or VLAN. It does not search beyond a router. It will not inventory the entire network of the school unless it is all on one subnet.
2. Network Inspector is not a Cisco product nor is it limited to detecting just Cisco devices.

3. Network Inspector is a detection tool, but it is not a configuration tool. It cannot be used to reconfigure any devices.

The output in this lab is representative only, and output will vary depending on the number of devices, device MAC addresses, device hostnames, and which LAN is joined.

This lab introduces the Fluke Networks Network Inspector software, which may be useful in later troubleshooting labs and in the field. While the Network Inspector software is a valuable part of the Academy program, it is also representative of features available on other products in the market.

At least one host must have the Network Inspector software installed. If the lab is done in pairs, having the software installed on both machines means that each person can run the lab steps. Be sure to select both the Network Inspector and the Network Inspector Agent during installation.

The Console can be anywhere that has a valid IP path and security to allow the connection to an Agent. In fact, it might be an interesting exercise to have the Console reach across the serial link to load the database from the other Agent. The student can have the Console reading from a different database than the one that is currently in use by the Agent on the same PC.

Step 1 Configure the lab or attach the workstation to the school LAN

Option 1. If the closed lab environment is selected, cable the equipment as shown above and load the configuration files into the appropriate routers. These files might already be preloaded. If not, obtain them from the instructor. These files should support the IP addressing scheme as shown in the figure above and the table below.

Configure the workstation according to the specifications in the table below.

Host #1	**Host #2**
IP Address: 192.168.1.20	IP Address: 192.168.2.10
Subnet mask: 255.255.255.0	Subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1	Default Gateway: 192.168.2.1

Since the software discovers devices on the network, the more devices the better the demonstration.

If available, add additional hosts to both LANs.

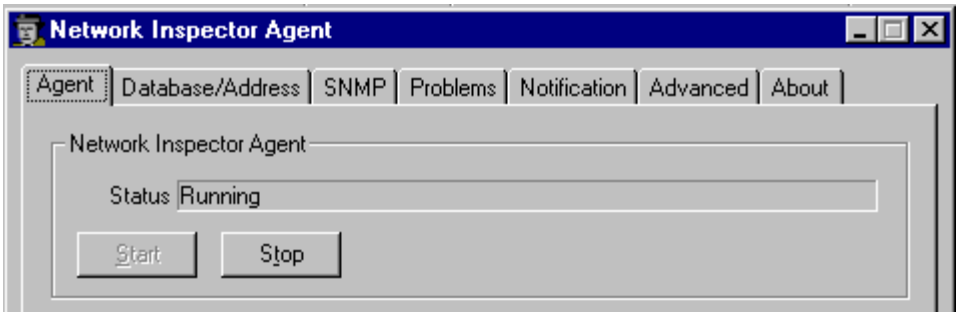
Option 2. If option 2, connect to school LAN, is selected, simply connect the workstation, with Network Inspector or Protocol Expert installed, directly to a classroom switch or to a data jack connected to the school LAN.

Step 2 Start Network Inspector and the Agent

From the Start menu, launch the Network Inspector Console. Click on the **Agent** button at the left end of the toolbar so that the Agent can be started.	

If necessary, select the **Agent** tab in the window, then click on the **Start** button and watch the **Status** box until it shows that the Agent is running as in the figure below. This process may take several minutes to start.

Notice the Agent status on the bottom of the Console window. Look closely and notice that the Agent has been running since 9:57 PM in the second graphic captured below that is in Step 3.

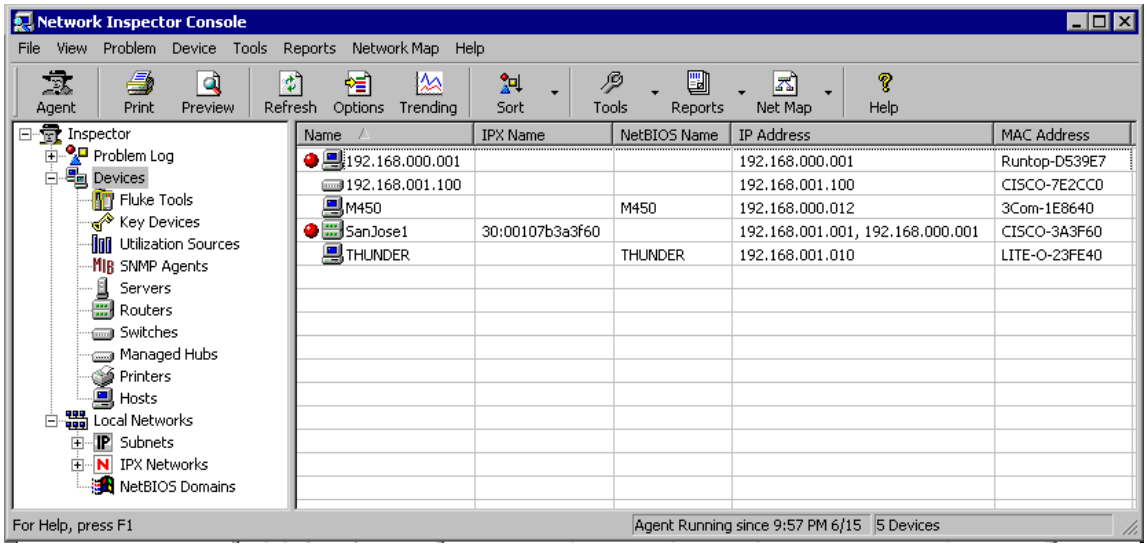


Use the **Close** button in the lower-right corner of the Agent window to send the Agent away. In some versions, this may be a **Hide** button. Do not use the **Stop** button or the discovery process will cease.

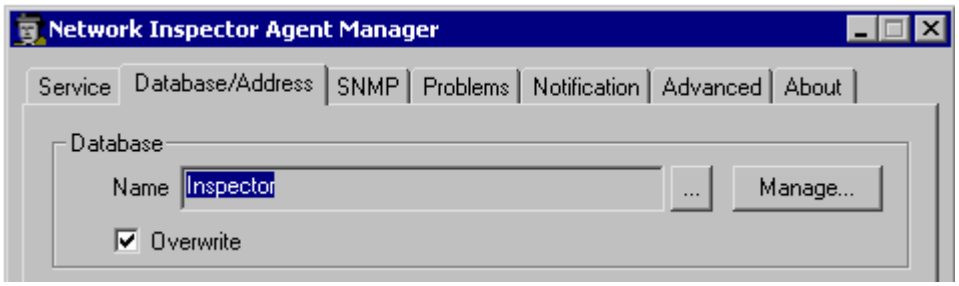
Step 3 Allow network discovery to occur

The Network Inspector software is designed to quietly, both passively and actively, collect network data. As such it takes time for devices to appear. This small network should be discovered in a minute or two. Active collection of statistical data is delayed for the first 10 minutes. An actual production network might take 30 minutes or more before most data is discovered.

After a few minutes, the Console window should start showing information about the network. In the following example**,** two additional workstations were added.



Note: Entries from previous sessions may be seen. It will take a few minutes for the entries to match the network. In the Agent window, under the **Database/Address** tab, there is a checkbox for **Overwrite**. If that box is checked, the current database content is discarded and a fresh data set is loaded as it is discovered when the Agent starts. Otherwise, any new data is integrated with the existing database as it is discovered.

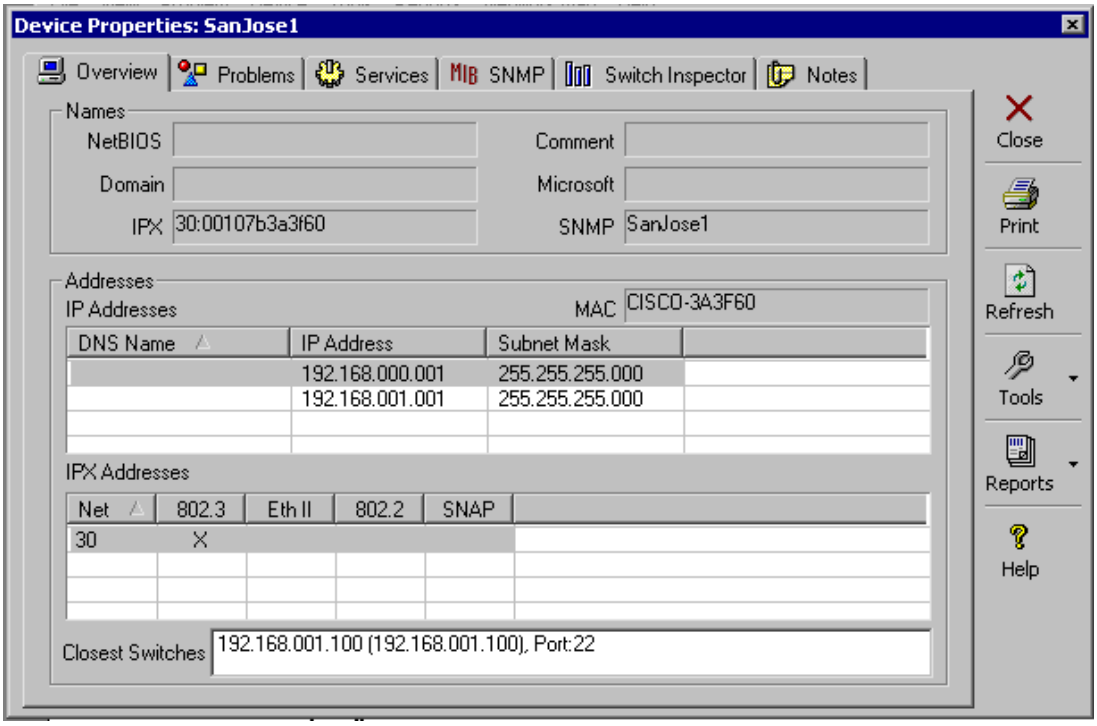


Notice the hostnames, which are M450, SanJose1 and Thunder, in the example above. PC hostnames will be different in student output. Also notice the IP addresses and MAC addresses for each discovered device. It should be obvious that both SanJose1 and SanJose2 have two IP addresses assigned to the LAN interface.

Notice that NI does not investigate beyond the router interface. It collects information only on the devices that share the same broadcast domain as the computer NIC.

Step 4 Investigate device properties

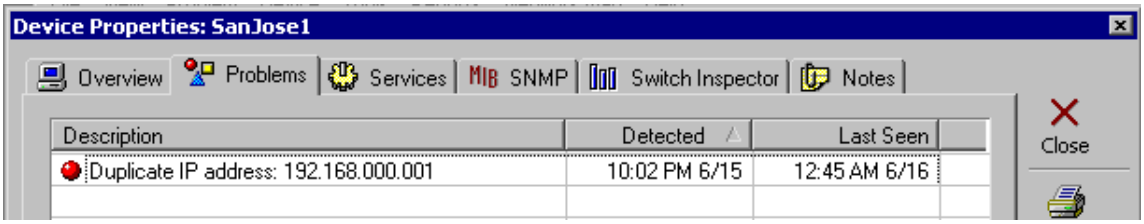
Double click on the router device name and look over the available Device Properties. Remember that results will depend on the devices included in the LANs subnet.



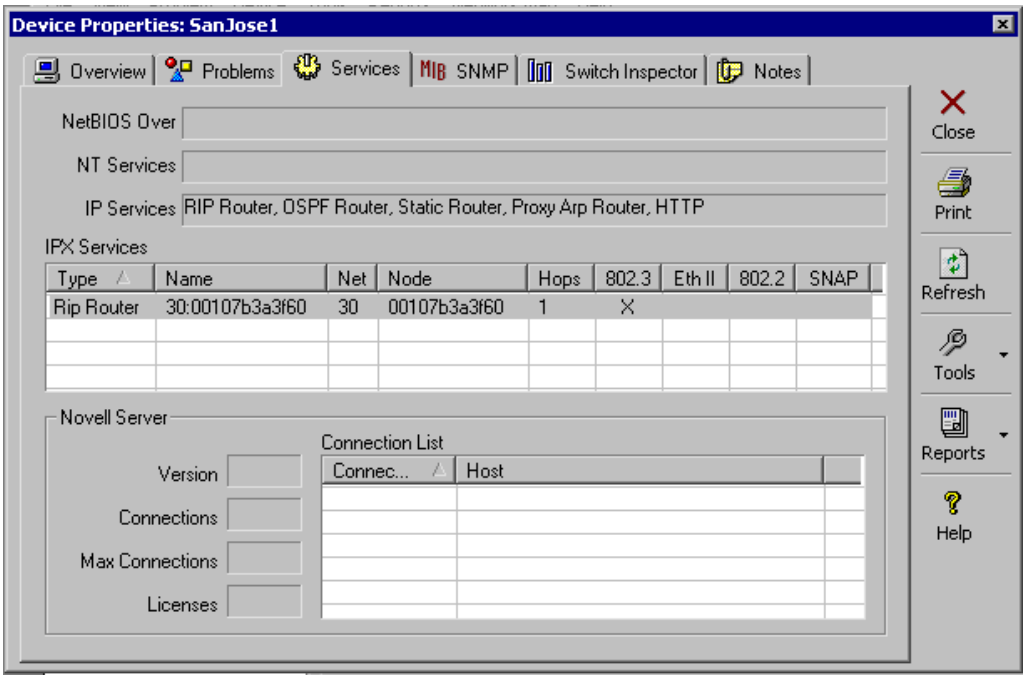
The **Overview** tab in the above graphic shows IP addresses, the IPX address, the IPX networks attached, the IPX data frame used (802.3 above), and the MAC address. Notice that the OUI has been converted to identify the manufacturer in the above example.

The closest switches will only appear if Network Inspector has been provided with a valid SNMP Community String for them.

The **Problems** tab reveals one of the IP addresses is duplicated within the network. This occurs if the student configured an optional host as defined in Step 1. The red ball to the left of the Description indicates a problem.



The **Services** tab reveals the IP and IPX Services running on the routers.

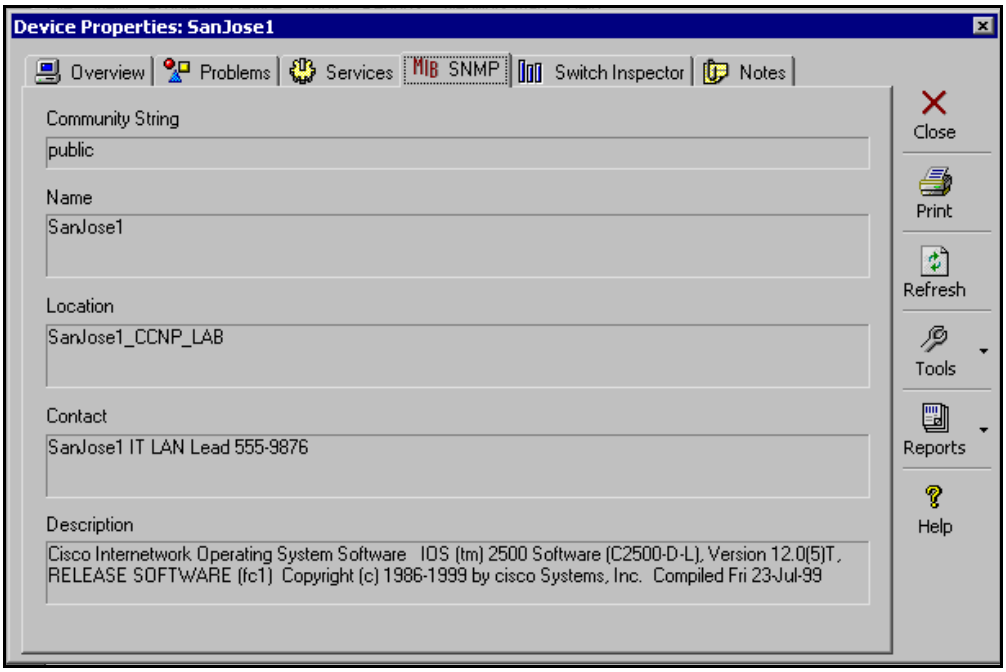


The IP Services example in the graphic above reveals that the **IP HTTP Server** service has been turned on. This means the router can be accessed via a Web browser.

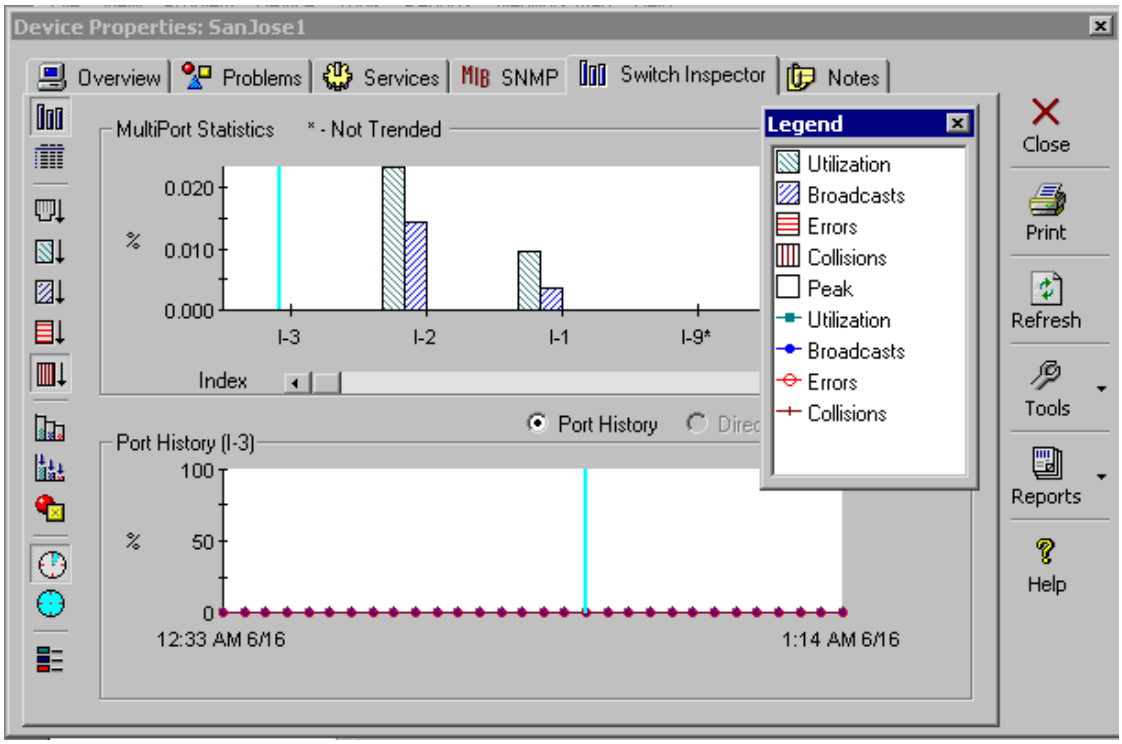
The IPX Services shows the IPX Network ID (30), the Node address (MAC), the frame type, and the fact that IPX RIP is running.

The bottom third of the window shows the information that would have been revealed if the device had been a Novell Server. A multi-homed server, which is one with more than one NIC (connection) in separate networks, is working as a router or bridge.

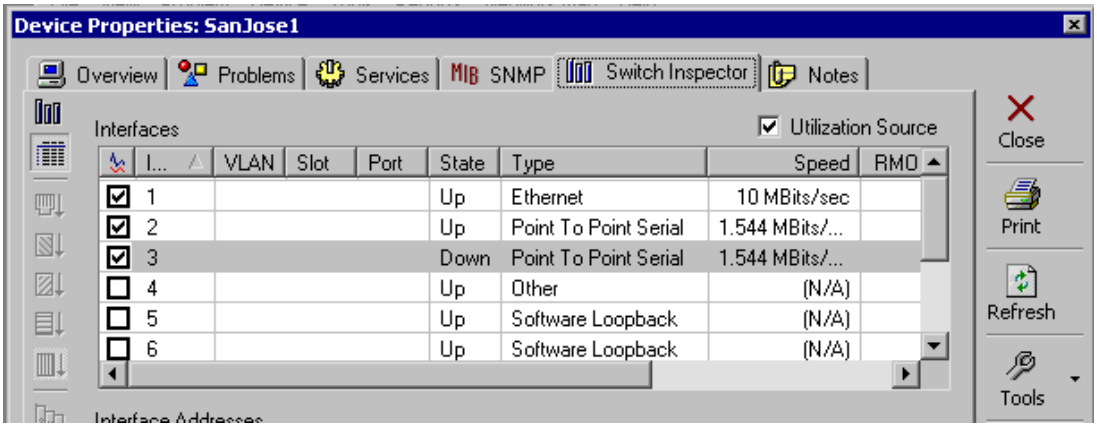
The **MIB SNMP** tab reveals SNMP information as well as the router IOS information.

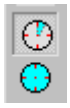


The **Switch Inspector** tab creates a variety of charts of the switch interface data for the selected device. This data is not collected during the initial 10-minute period. The Switch Inspector test provides basic utilization graphs for any SNMP enabled device. The level of information offered by this test depends on which MIBs are supported by the selected device. For example, since SanJose1 is a router, the student cannot display the address of any directly connected devices for a highlighted port. The buttons on the left side of the window change the chart format. The **Graph Legend**  button at the bottom-left corner displays the floating legend seen below.



The second button is the **TabularView**  , and selecting it details each interface on the selected device including whether the interface is up or down. The check box at the left of each line determines whether statistics are gathered for trending on that interface. Scrolling to the right reveals MTU and Description (FastEthernet0/0 or Token-Ring 0/1) details.

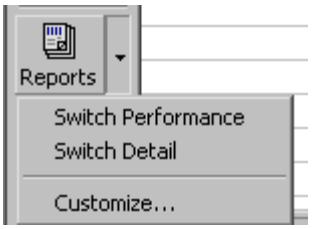




The two clock-like buttons switch between a one-hour or 24-hour history, which can create an interesting comparison if the NI has been running for an extended time. The results will be the same in this short exercise.

While in the Switch Inspector, the **Reports** button on the right side of the screen will expand to show two options. Select the **Switch Performance** choice and a multi-page report with various charts will appear on the screen. Look over the results.

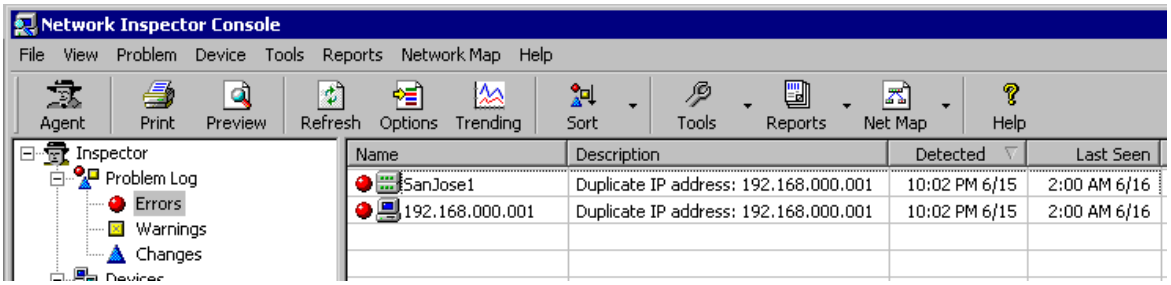
The **Switch Detail** option only works with a switch.



After looking over the Device Properties window, click on the **Close** button in the upper right corner to return to the Network Inspector Console.

Step 5 Explore the left panel options

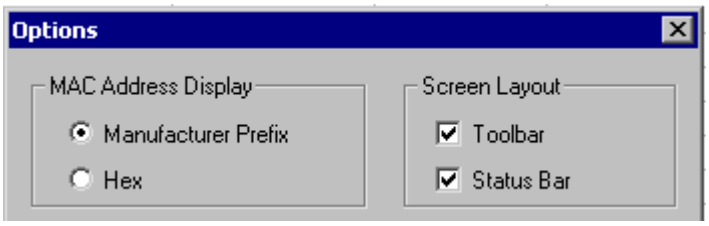
At the Network Inspector Console, experiment with expanding and contracting the choices in the left-side pane. As with the Explorer**,** if an item on the left side is selected, the right side will show the details. In the following example, expanding the Problems Log and selecting **Errors** shows the devices on the right side with errors. This makes it easy to spot the duplicate IP address device.



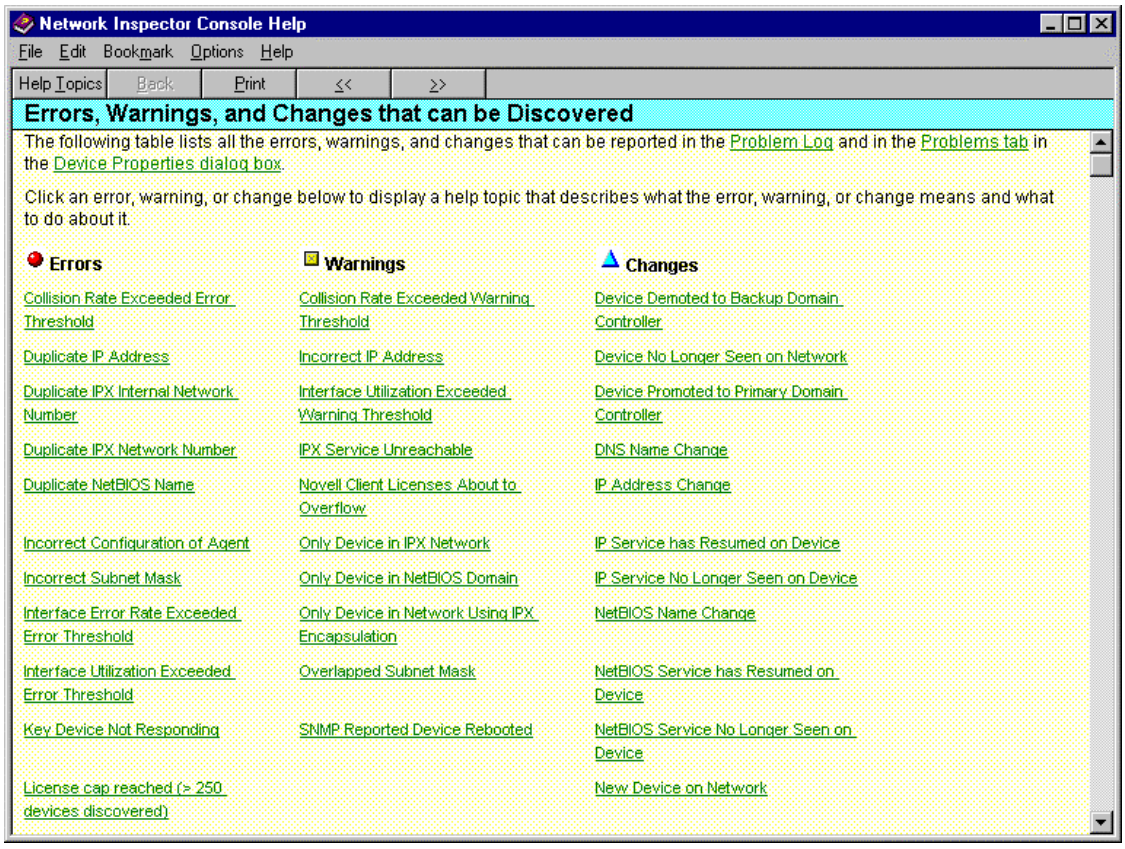
Try different options on the left pane and note the result in the right pane. Due to the limited number of devices**,** some will be empty. Try it later with a larger sample.

In the left pane, select **Devices** to show all devices in the right pane. Note the format of the MAC address.

Click on the **Options** button in the toolbar (or View > Options) and note that the student can choose between **Manufacturer Prefix** and **Hex**. Select the one that is not chosen, look over the other options, and then click on OK. Note the result.

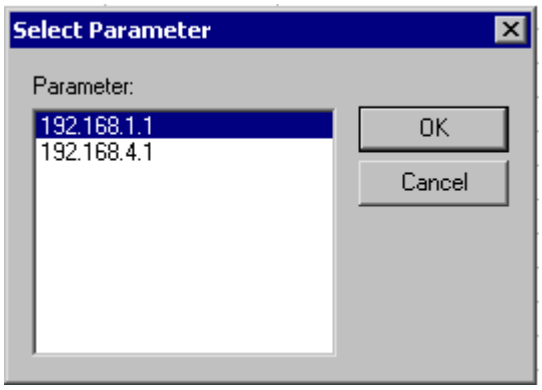


Getting Help. In the Console main screen, check that the **Problem Log** is selected, and that a device shown in the detail window has been highlighted. Press F1, which is the Help function key, to show a list of problems by category.



As an example, one of the problems created by the current Lab configuration in the above graphic is a duplicate IP address. To learn about duplicate IP addresses, what the symptoms are, and what can be done about them, select the hyperlink listing for **Duplicate IP Address** from the list. There is a wealth of information in the Help for this software.

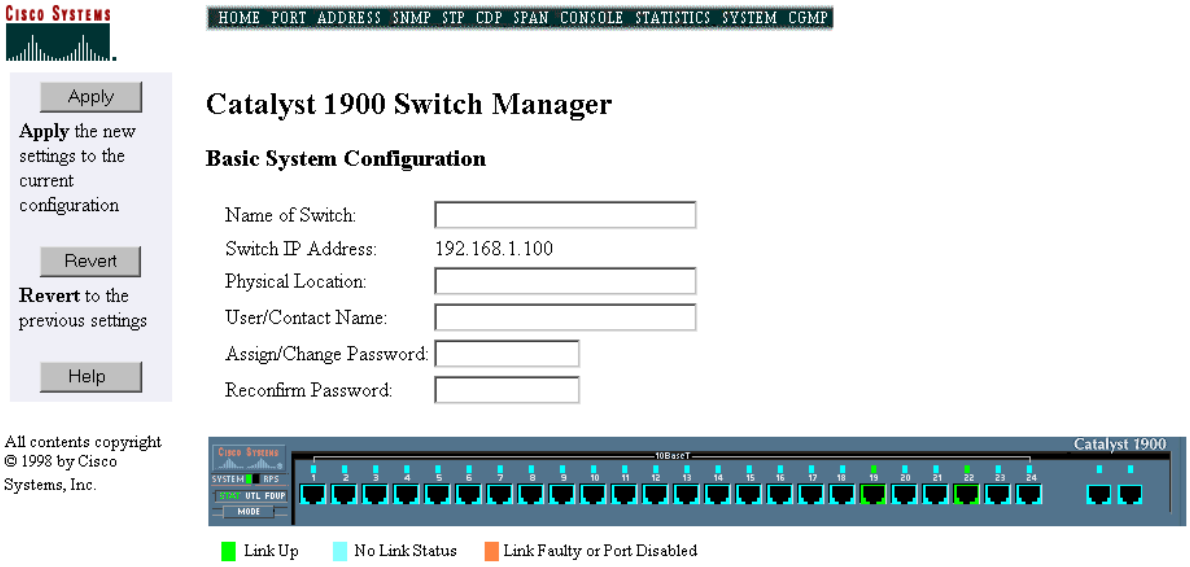
Take a minute and experiment with the **Preview**, **Sort**, and **Reports** buttons in the toolbar. The features should be obvious. Look particularly at the troubleshooting and documentation possibilities of the reports.

Select a host and then open the **Tools** button in the toolbar and pick **Ping**. The Select Parameter box will include the LAN IP addresses that the student can ping. Select one and click on OK. A command (MSDOS) window will appear to show the results. Type **exit** to close the new window when finished.	

Try using the **Telnet** and **Traceroute** options. Select a router or switch in the Console display and then choose Tools | Telnet and a window with a Telnet session open will appear. Trace works the same way.

The **Web** option on the **Tools** button will open a Web session with a device if the IP HTTP Server feature is turned on. If trying this, the username is the hostname, which is SanJose1 or SanJose2, and the password is cisco.

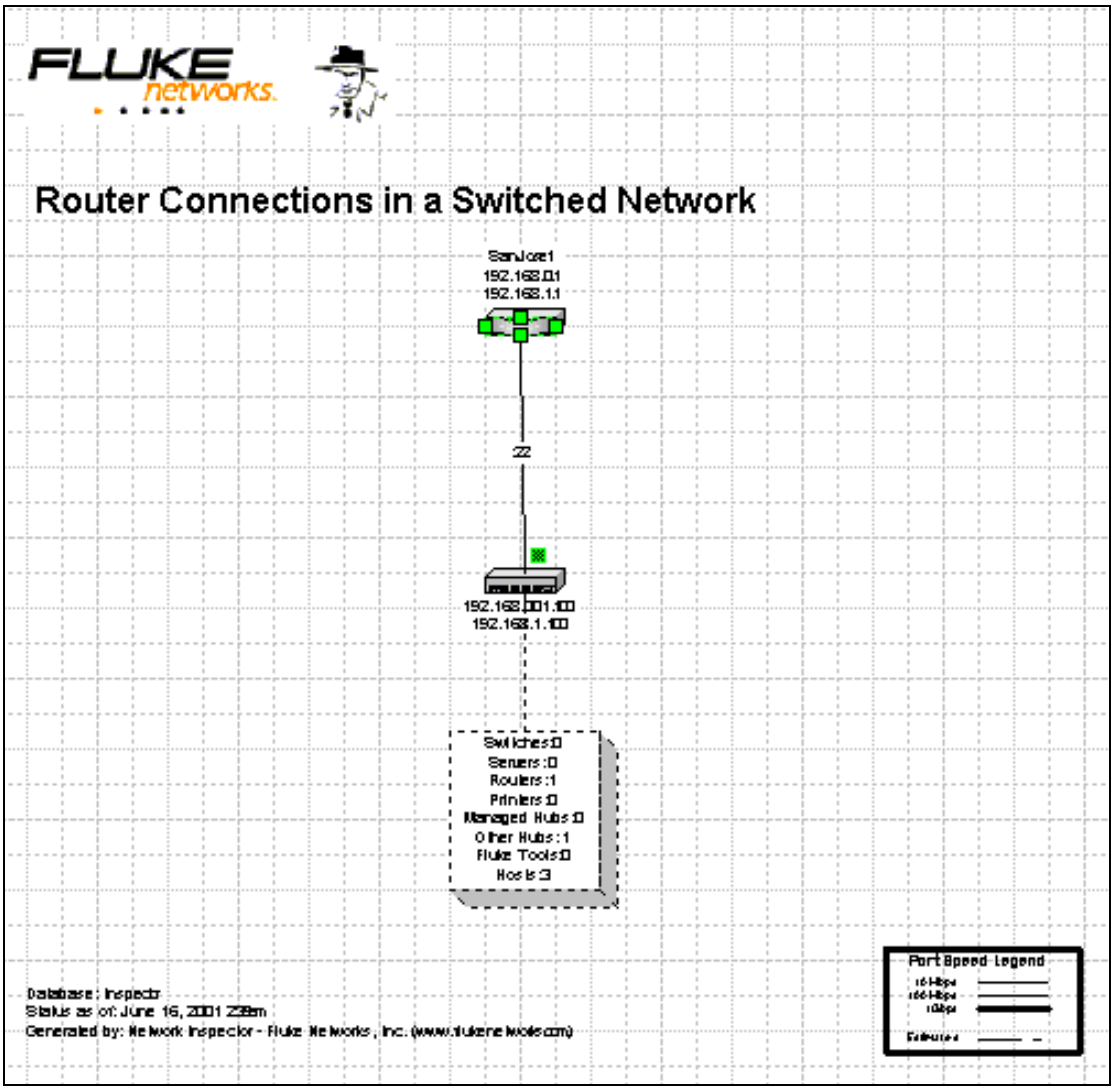
In the sample lab above**,** the switch is a Catalyst 1924 with an IP address assigned. Therefore, the following appears if the **Web** choice is selected while the switch is highlighted:



Experiment with the above toolbar options until comfortable with the features.

Step 6 Use Net Map and Visio to diagram the network

If Visio is installed on the workstation, the **Net Map** button on the toolbar will activate Visio and create a network map of the broadcast domain. The following example uses the “Router Connections in a Switched Network” on the Net Map button. It will draw the network whether or not a switch is included.



The Visio is fully integrated into NI. This means that double clicking one of the devices in the drawing will call up the Device Properties window that was used in Step 4.

Step 7 Document router information.

Using the skills covered earlier, select the router and document the following information where available:

a. What is the name of the device? SanJose1 or SanJose 2

b. What IP services is the device running? RIP Router, OSPF Router, Static Router, Proxy ARP Router, HTTP

c. What IPX services is the device running? Answers vary, most often, none.

d. What is the SNMP community string? public

e. What is the location? Answers will vary, but most likely San Jose.

f. Who is the contact? Answers will vary, usually it is the IT manager.

g. Which interfaces are available? Answers will vary on model of router.

h. Which interfaces are up? Serial 0/0 and Fa 0/0

i. List below any problem(s) that the software has discovered. Answers will vary.

Step 8 Observe device discovery

If possible, connect the two switches with a crossover cable and watch the NI output as new devices are discovered. If a crossover cable is unavailable, remove one of the switches and plug the host(s) and router into the second switch. While this would not usually be done in a production environment, do it now just to see how NI responds.

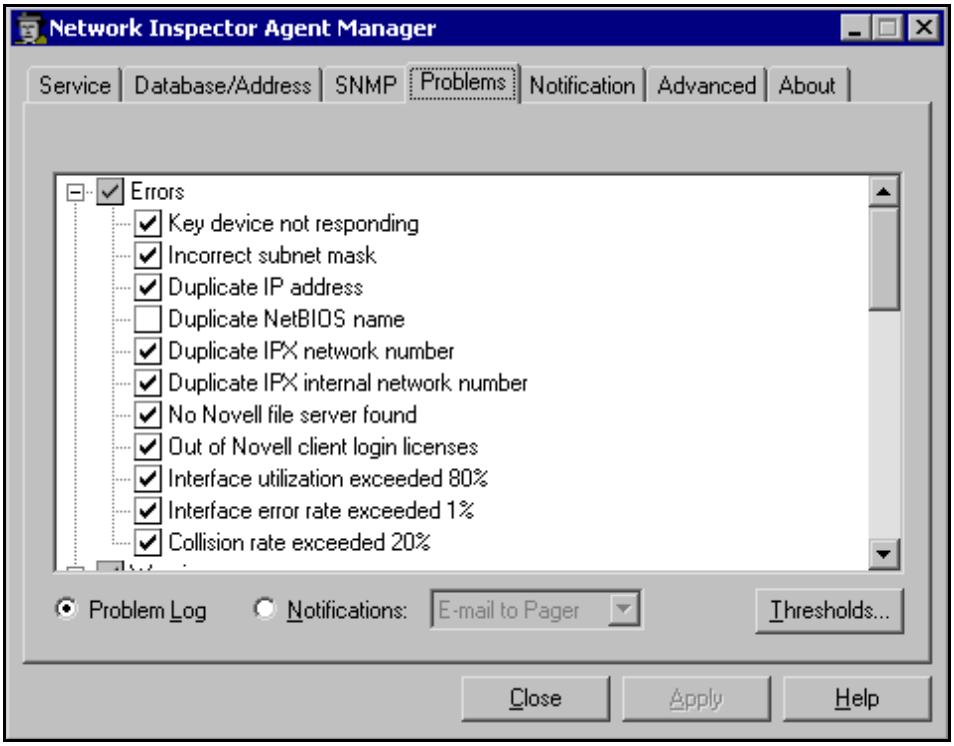
New devices should show up initially with blue triangles indicating they are newly discovered. Many should eventually get a yellow warning rectangle indicating a potential problem. Remember that this process could take 10 or more minutes.

Eventually, the other subnets and the second router should be seen.

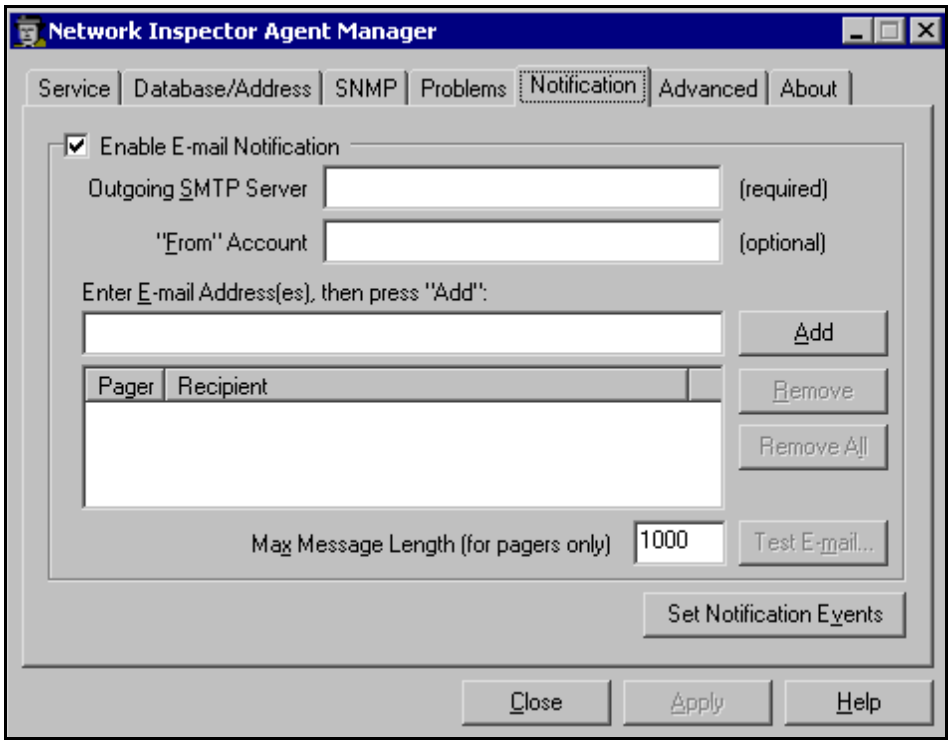
Step 9 Stop the capture and access the Problems and Notification tabs

Click on the **Agent** button in the toolbar. The Agent has been collecting data all this time. Click on the **Stop** button and then confirm intentions when prompted.

Look over the tabs to see the database options that can be set. Note the **Problems** tab and the choices for focusing the investigation.



On the **Notification**, notice that e-mail notifications can be sent out. To use this feature, the student would need the same information as that required to set up an Internet e-mail account or Outlook e-mail account.



If the student starts the Agent again, it may take a few minutes to detect any changes that occurred while the agent was off.

Step 10 Experiment with NI

Experiment with the NI tool by looking at the different devices.

If NI is installed on the classroom computers, investigate the devices on that larger network.

Reflection

How might this information be used in troubleshooting?

Answers vary. A typical response includes “Network Inspector will quickly find the problem at a specific workstation.”

What advantages over HyperTerminal might it have for troubleshooting documentation?

Answers vary. A typical response includes “Network Inspector is graphical and provides valuable information.”

