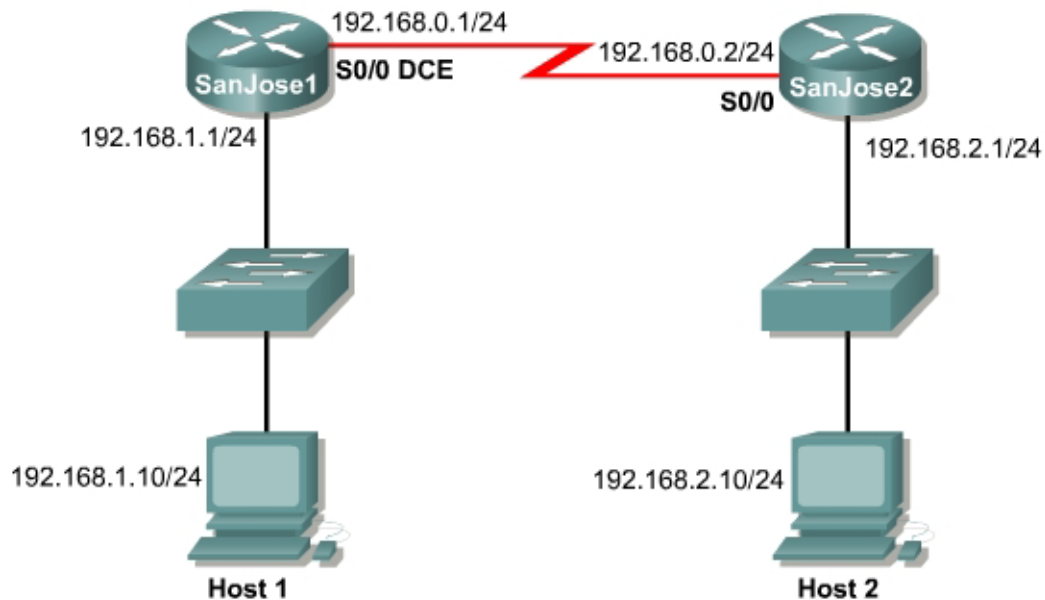


Lab 1.2.9.4 Introduction to Fluke Network Inspector



Objective

This lab is a tutorial demonstrating how to use the Network Inspector (NI) from Fluke Network to discover and analyze network devices in a broadcast domain.

This lab will demonstrate the key product features. However, the limited number of devices is an issue. The software can distinguish the following components if they have been assigned network addresses:

- Workstations
- Servers
- Network printers
- Switches
- Managed hubs

After performing the lab, consider repeating the steps in a larger environment like a classroom so that more variety can be seen. Before attempting to run NI on a school LAN, make sure it is okay with the instructor. Consider the following points:

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 and it is not limited to detecting only 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. The output will vary depending on factors such as the number of devices, device MAC addresses, device host names, the LAN that is joined, and protocols used.

Scenario

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

At least one host must have the Network Inspector software installed. If the lab is done in pairs, the software should be installed on both workstations so that each person can perform the lab steps.

Step 1

Cable and configure the devices as pictured in the network diagram. The switches pictured can be any catalyst switches that are used. Be sure to use the default switch configurations on these switches. If necessary, erase the configuration files on the switches.

The configurations required on the routers are as follows:

```
Router(config)#hostname SanJose1
SanJose1(config)#interface serial 0/0
SanJose1(config-if)#ip address 192.168.0.1 255.255.255.0
SanJose1(config-if)#clockrate 56000
SanJose1(config-if)#no shutdown
SanJose1(config-if)#interface FastEthernet 0/0
SanJose1(config-if)#ip address 192.168.1.1 255.255.255.0
SanJose1(config-if)#no shutdown
SanJose1(config-if)#exit
SanJose1(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.2
SanJose1(config)#exit
SanJose1#
```

```
Router(config)#hostname SanJose2
SanJose2(config)#interface serial 0/0
SanJose2(config-if)#ip address 192.168.0.2 255.255.255.0
SanJose2(config-if)#no shutdown
SanJose2(config)#interface FastEthernet 0/0
SanJose2(config-if)#ip address 192.168.2.1 255.255.255.0
SanJose2(config-if)#no shutdown
SanJose2(config-if)#exit
SanJose2(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1
SanJose2(config)#exit
SanJose2#
```

Since the software discovers devices on the network, the demonstration will improve as more devices are added to the network. Consider using a Cisco switch or a hub on each LAN instead of a crossover cable.

If available, add additional hosts to both LANs.

Verify connectivity between the hosts. Troubleshoot as necessary.

```
C:\WINDOWS\System32\cmd.exe

C:\Documents and Settings>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.10: bytes=32 time=22ms TTL=126
Reply from 192.168.2.10: bytes=32 time=20ms TTL=126
Reply from 192.168.2.10: bytes=32 time=20ms TTL=126

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 22ms, Average = 20ms

C:\Documents and Settings>
```

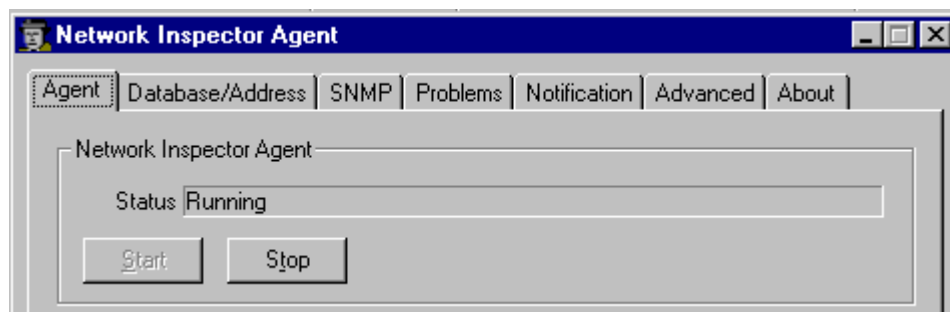
Step 2

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, click on the **Start** button, and watch the **Status** box until it says that the Agent is running. This process may take several minutes to start.



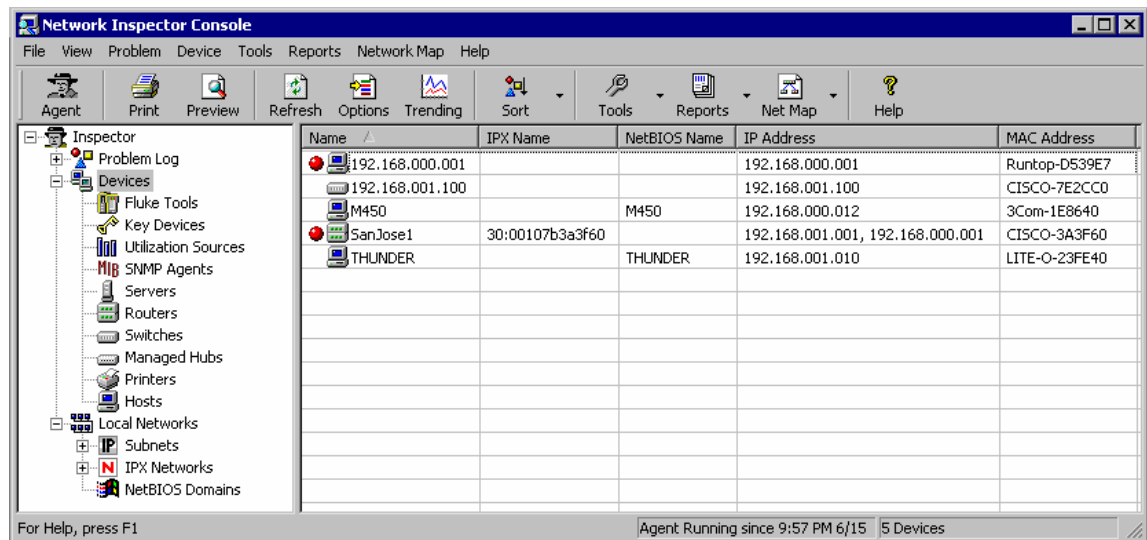
The Agent status can be seen on the bottom of the Console window. The first graphic in Step 3 indicates that the Agent has been running since 9:57 p.m.

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

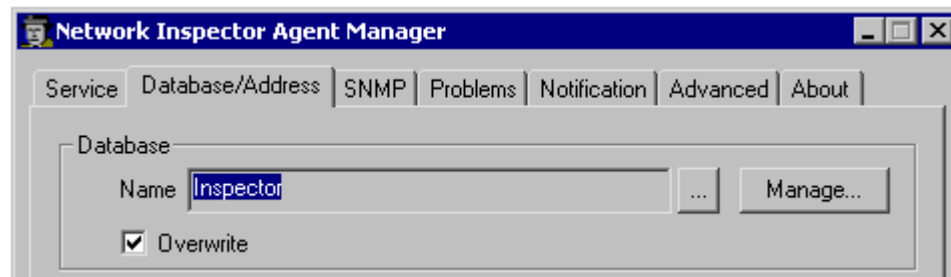
Step 3

The Network Inspector software is designed to quietly collect network data. This data collection can be performed either passively or actively. It takes time for the devices to appear. This small network should be discovered in a minute or two. Active collection of statistical data is delayed for the first ten minutes. An actual production network might take 30 minutes or more before most data is discovered.

After a few minutes, the **Console** window should display 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 discovered and loaded when the Agent starts. If the box is not checked, any new data is integrated with the existing database as it is discovered.



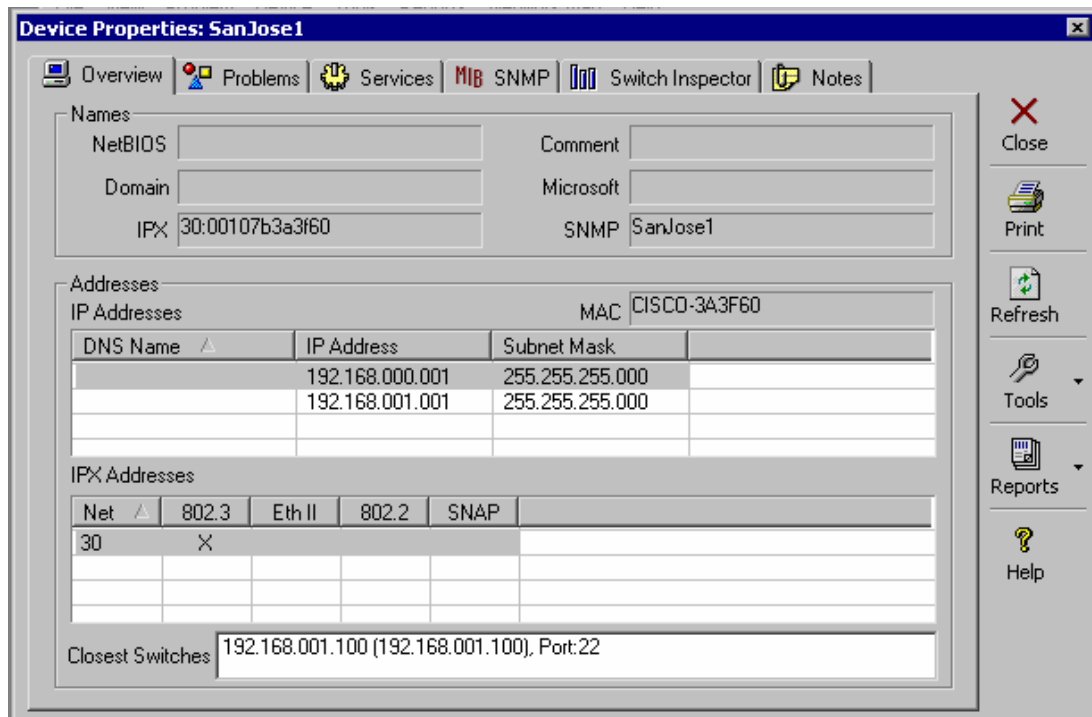
In the preceding sample output, the MAC address has been configured to interpret the first half of the 48-bit MAC address to show the vendor name. The **Options** button in the toolbar can be used to change this display.

The Network Inspector console in Step 3 lists M450, SanJose1, and THUNDER as the hostnames. Hostnames on PCs will be different. This window also lists the IP address and MAC address for each discovered device. SanJose1 and SanJose2 each have two IP addresses assigned to the LAN interface.

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

Step 4

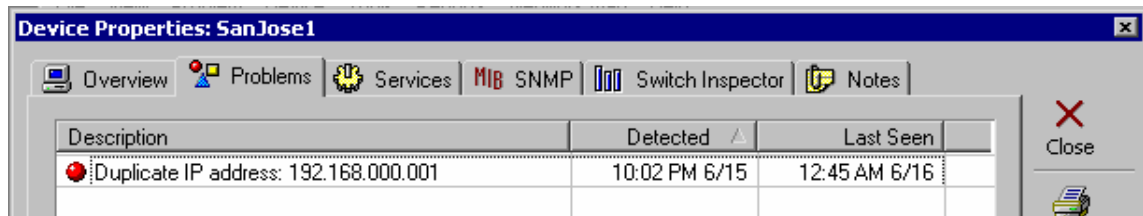
Double click on a device name. Choose a router if present and look over the available Device Properties. Remember that the results will depend on the devices included in the LAN subnet.



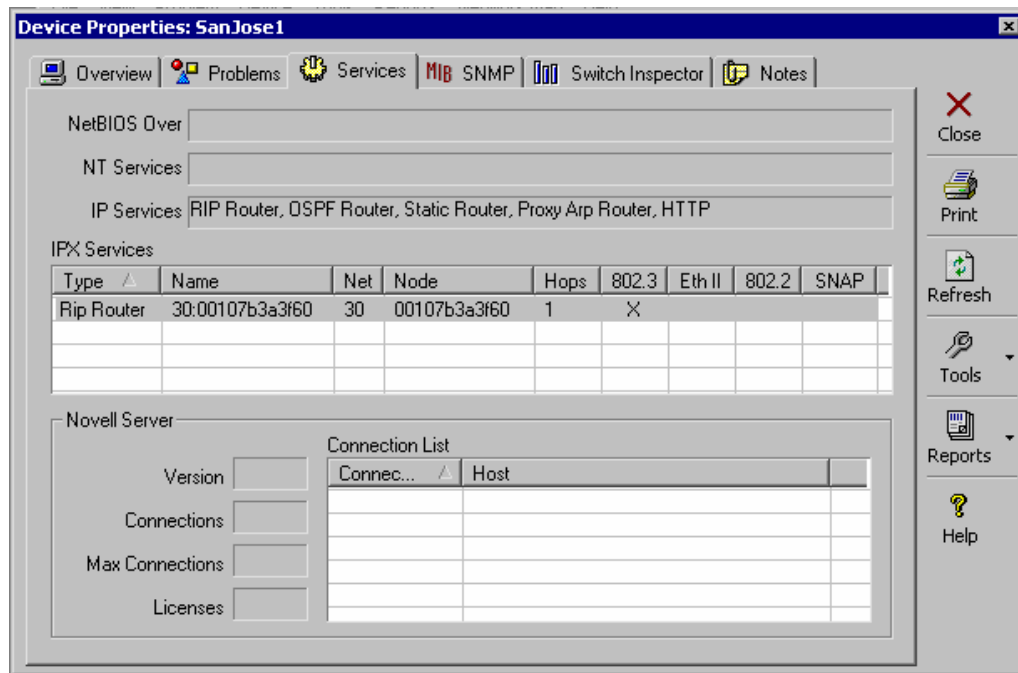
The **Overview** tab in the preceding graphic shows IP addresses, the IPX address, the IPX networks attached, the IPX data frame used for 802.3, and the MAC address. Notice that the OUI has been converted to identify the manufacturer in this example.

Closest switches will only appear if Network Inspector has been provided with a valid SNMP Community String for the switch.

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



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

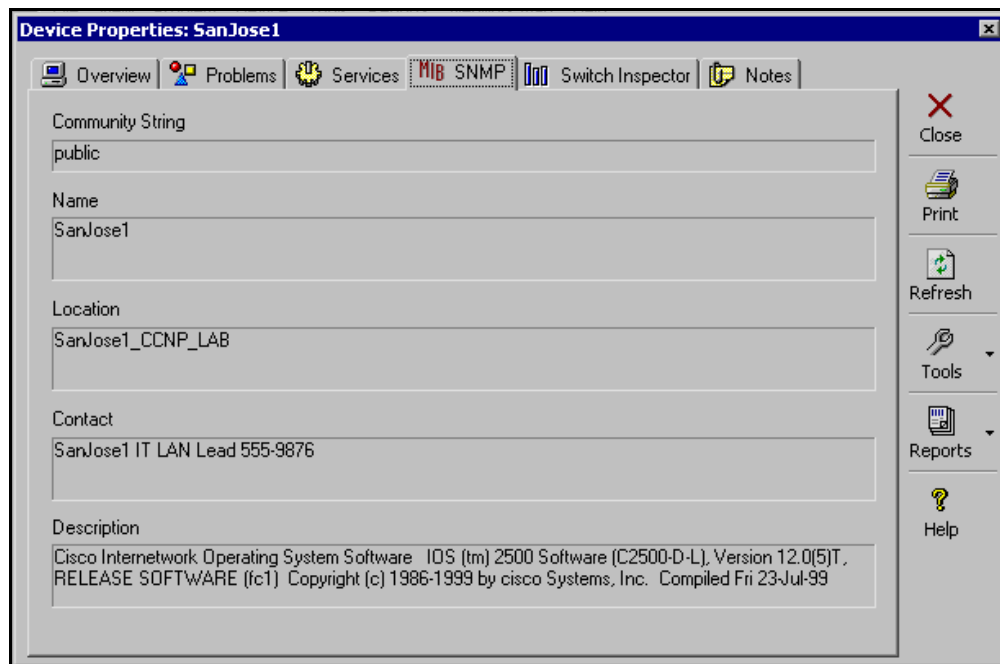


The preceding **IP Services** example reveals that the IP HTTP Server service has been turned on. This means the router can be accessed with a Web browser.


The IPX Services shows that the IPX Network ID is 30 and the Node address is MAC. It also indicates the frame type and the fact that IPX RIP is running.

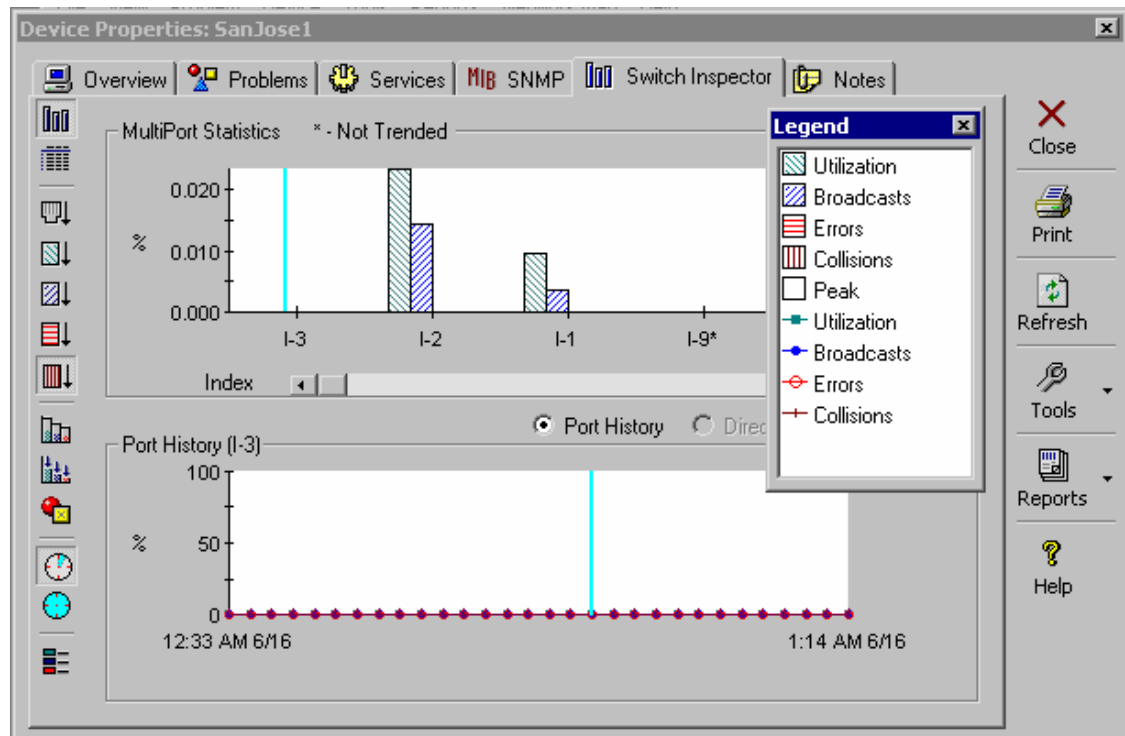
The bottom third of the window shows the information that would have been revealed if the device had been a Novell Server.


The **MIB SNMP** tab reveals SNMP information and the router IOS information.

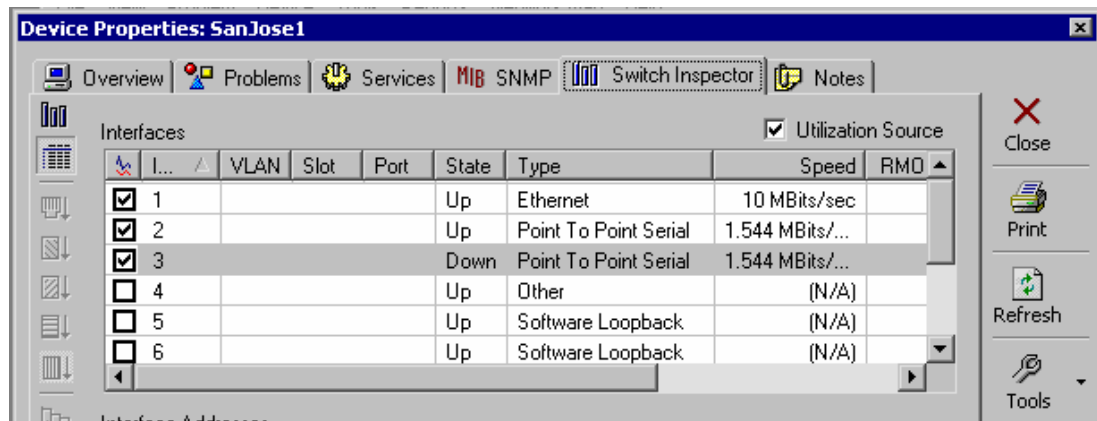


The **Switch Inspector** tab creates a variety of charts of the switch interface data for the selected device. This data is not collected during the initial ten-minute period. The **Switch Inspector** test provides basic utilization graphs for any SNMP-enabled device. The level of information offered by this test depends on which MIBs are supported by the selected device. For example, SanJose1 is a router that 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 in the following graphic.



The second button is the **Tabular View** . This option will detail each interface on the selected device 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 details such as Ethernet 0 or Token-Ring 0/1.



The screenshot shows the 'Device Properties: SanJose1' window with the 'Interfaces' table. The table lists interfaces 1 through 6, their states (Up or Down), types (Ethernet, Point To Point Serial, Other, Software Loopback), and speeds. A 'Utilization Source' checkbox is checked.

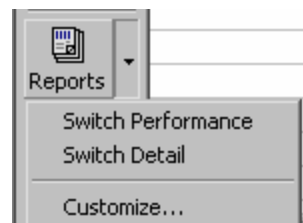
I...	VLAN	Slot	Port	State	Type	Speed	RMD
<input checked="" type="checkbox"/> 1				Up	Ethernet	10 MBits/sec	
<input checked="" type="checkbox"/> 2				Up	Point To Point Serial	1.544 MBits/...	
<input checked="" type="checkbox"/> 3				Down	Point To Point Serial	1.544 MBits/...	
<input type="checkbox"/> 4				Up	Other	(N/A)	
<input type="checkbox"/> 5				Up	Software Loopback	(N/A)	
<input type="checkbox"/> 6				Up	Software Loopback	(N/A)	



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.

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.

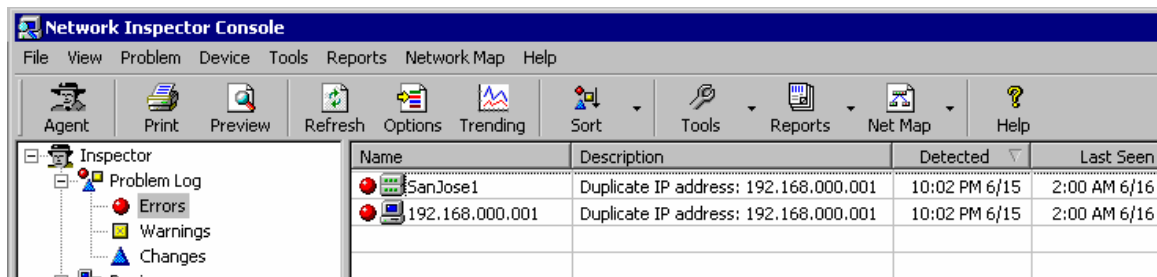
The **Switch Detail** option only works with a switch.



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

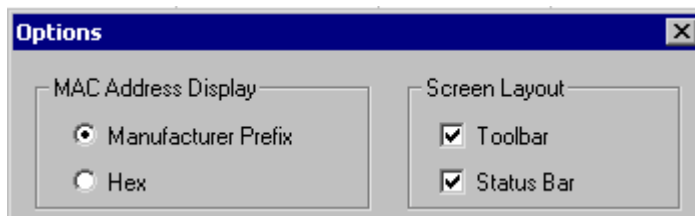
At the Network Inspector Console, experiment with expanding and contracting the choices in the left-side pane. As with the Explorer, if an item on the left side is selected, the right side will show the details. In the following example, expanding the **Problems Log** and selecting **Errors** shows the 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.

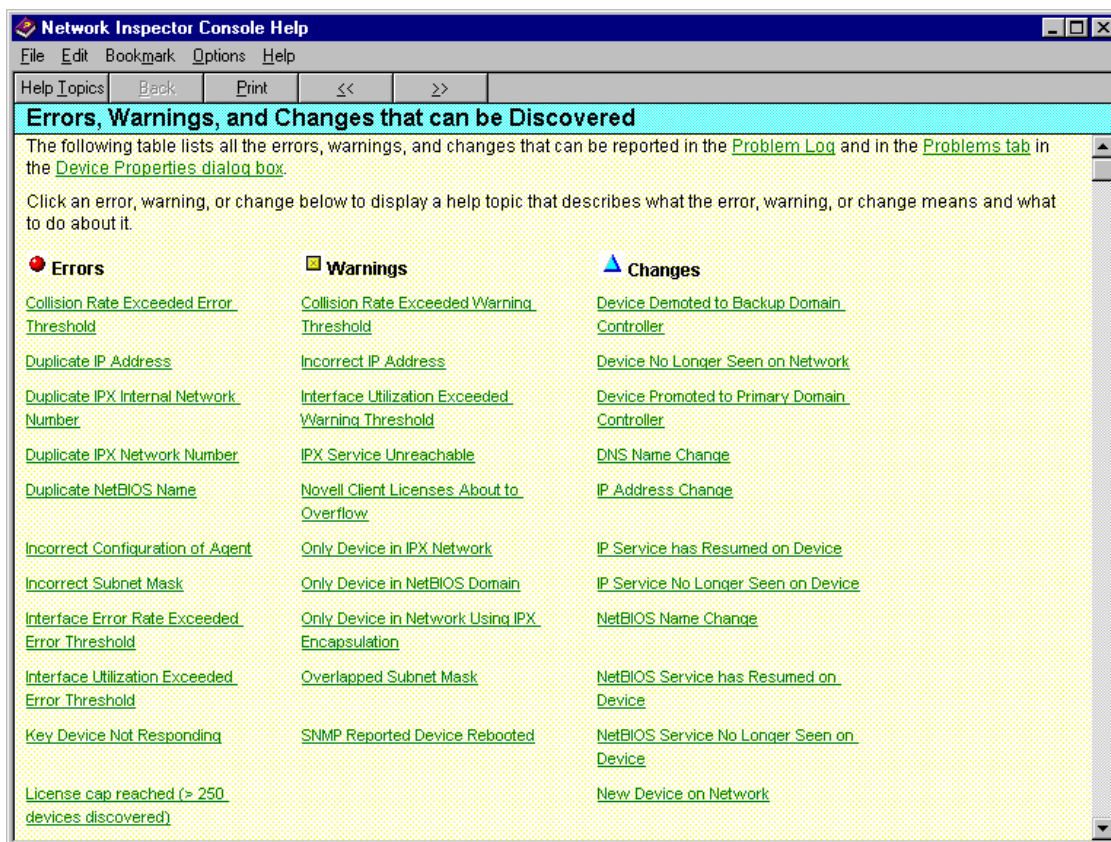
In the left pane, select **Devices** to show all devices in the right pane. Note the format of the MAC address.

Click on the **Options** button or **View > Options** in the toolbar. Note that there is a choice 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.



To get help in the Console main screen, check that the **Problem Log** is selected. Highlight a device shown in the detail window. Press the **F1** or the Help function key to show a list of problems by category.

If one of the problems created by the current lab configuration is a duplicate IP address, this can be viewed by providing a duplicate IP address for one of the devices. To learn about duplicate IP addresses, identify the symptoms, and determine what can be done about them, select the hyperlink listing for **Duplicate IP Address** from the list. There is a large amount of information in the **Help** window for this software.

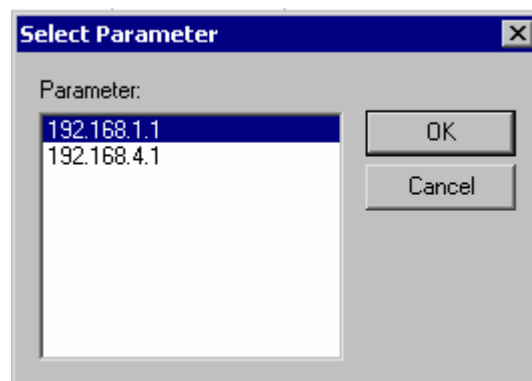


Experiment with the **Preview**, **Sort**, and **Reports** buttons in the toolbar. Focus on the troubleshooting and documentation possibilities of the reports.

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 can be pinged. Select one and click on **OK**.

A command or MSDOS window will appear to show the results.



Use the **exit** command to close the new window when finished.

Select a router or switch in the **Console** display and then choose **Tools > Telnet**. A window will appear with an open Telnet session. Traceroute 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.

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



HOME PORT ADDRESS SNMP STP CDP SPAN CONSOLE STATISTICS SYSTEM CGMP

Apply

Apply the new settings to the current configuration

Revert

Revert to the previous settings

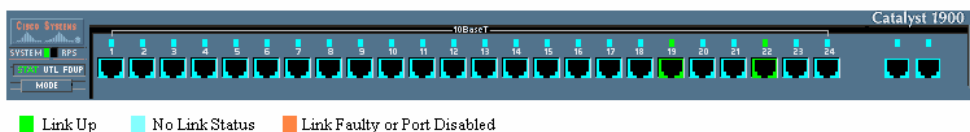
Help

Catalyst 1900 Switch Manager

Basic System Configuration

Name of Switch:
Switch IP Address: 192.168.1.100
Physical Location:
User/Contact Name:
Assign/Change Password:
Reconfirm Password:

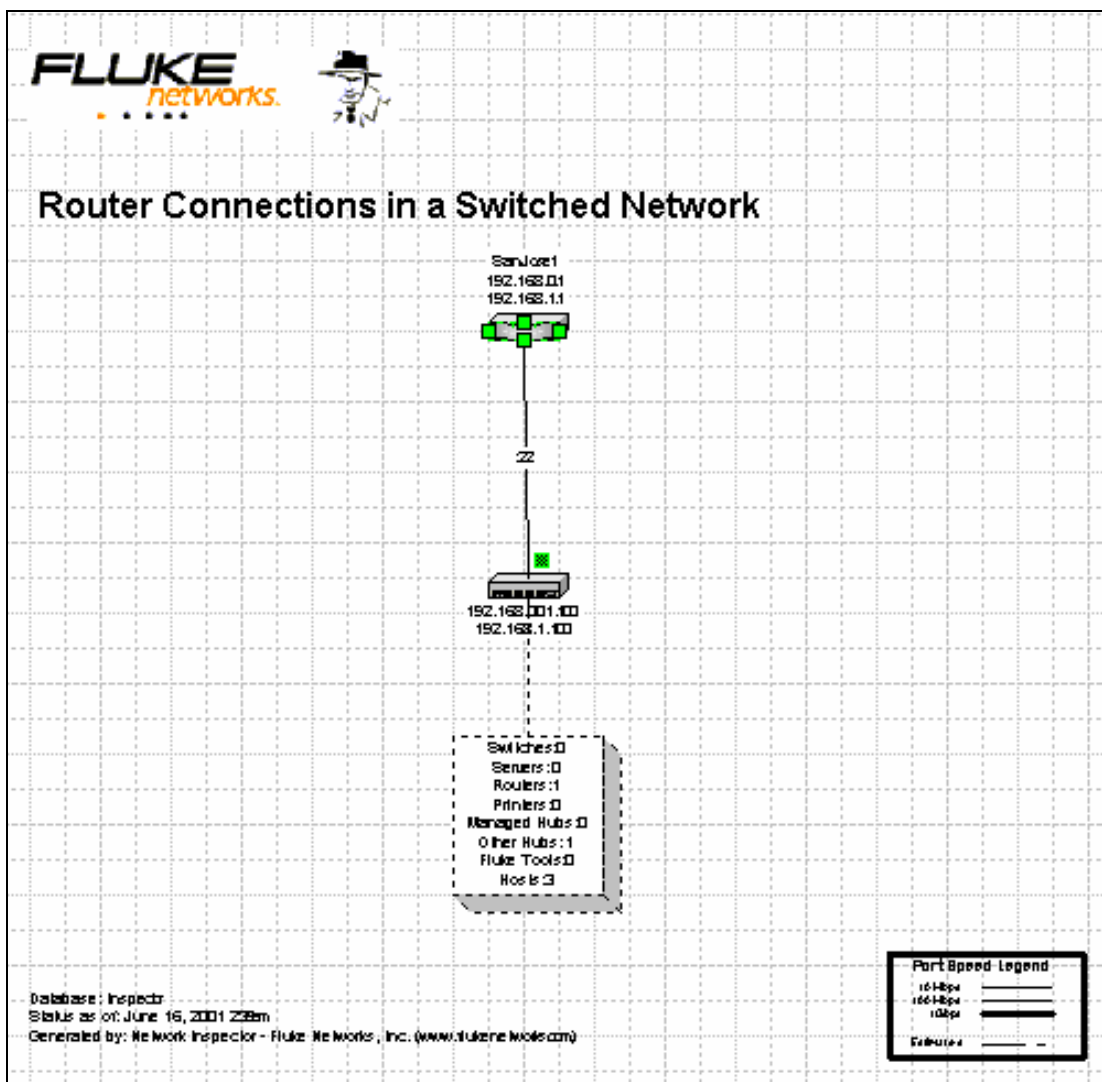
All contents copyright
© 1998 by Cisco
Systems, Inc.



Experiment with the toolbar options to become familiar with the features.

Step 6

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.



Visio is fully integrated into NI. Double clicking one of the devices in the drawing will display the **Device Properties** window that was in Step 4.

Step 7

Use the skills acquired in this lab to select the router and document the following information:

1. What is the name of the device?
2. What IP services is the device running?
3. What IPX services is the device running?
4. What is the SNMP community string?
5. What is the location?

6. Who is the contact?
7. Which interfaces are available?
8. Which interfaces are up?
9. List any problem that the software has discovered.

Step 8

Connect the two switches with a crossover cable and watch the NI output as new devices are discovered. If a crossover cable is not available, remove one of the switches and plug the host and router into the second switch. While this is not usually done in a production environment, students should see how the NI responds.

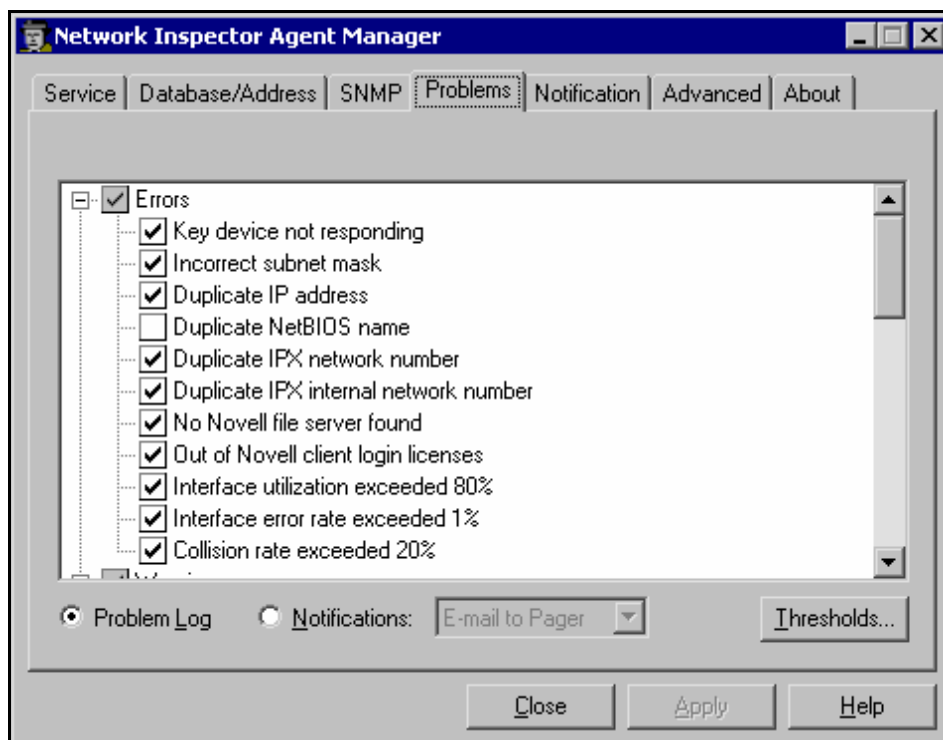
New devices should show up initially with blue triangles indicating they are newly discovered. Many should eventually get a yellow warning rectangle, which indicates a potential problem. This process could take ten or more minutes.

Eventually the other subnets and the second router will be seen.

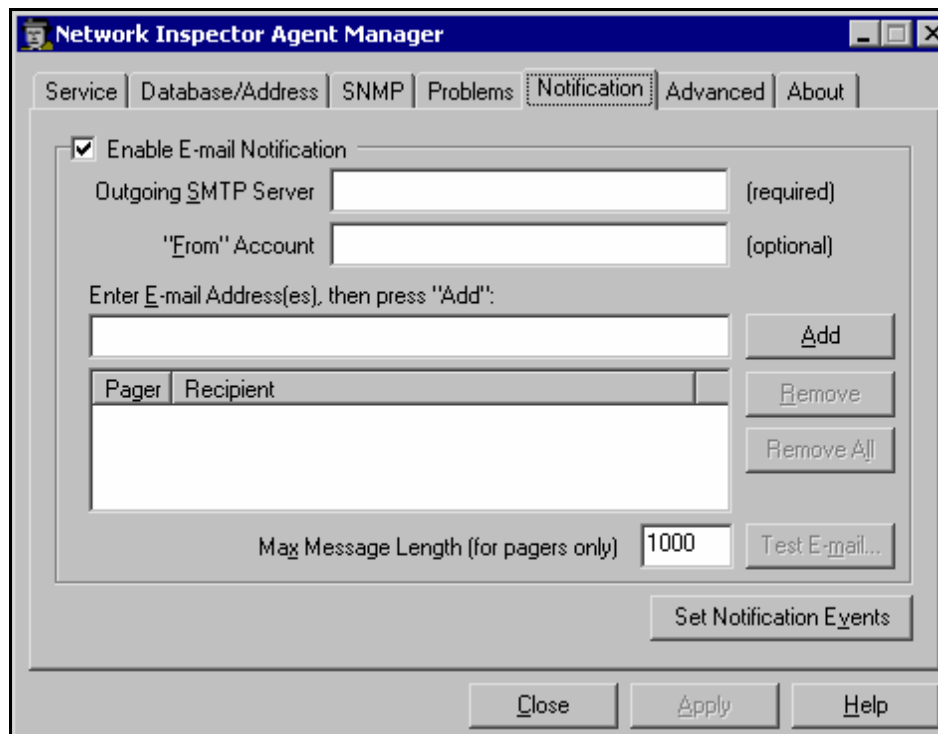
Step 9

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 what intentions there are 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** tab, notice that e-mail notifications can be sent out. To use this feature, it is necessary to have the same information that is required to set up an Internet or Outlook e-mail account.



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

Step 10

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

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

Reflection

How might this information be used in troubleshooting?

What advantages might NI have over HyperTerminal for troubleshooting documentation?