LABORATORY WORK NO. 10
NETWORK INSPECTOR

1. Objectives

The aim of this lab is to demonstrate how to use the Fluke Networks Network Inspector (NI) to discover and analyze network devices within a broadcast domain.

2. Theoretical consideration

2.1 Introduction

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.

Fluke Networks' Network Inspector is an application that runs under Windows (2k, NT 4.x, XP). It's an application for analyzing and monitoring Ethernet 10/100/1000 Networks. OPV-PE helps for monitoring networks.

This application is for network administrators and it permits monitoring, mapping and debugging of a segment of a Local Area network which can contain routers, servers, switches, clients etc. Network Inspector discovers most of the devices from a broadcast domain in about 10 minutes.

2.2 Overview of Network Inspector

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

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.

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 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.

2.2.1 Configure the lab (connect the workstation to the LAN)

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

If available, add additional hosts to both LANs.

Or you can 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.

2.2.2 Starting the 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.

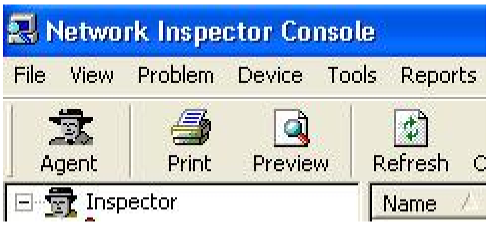
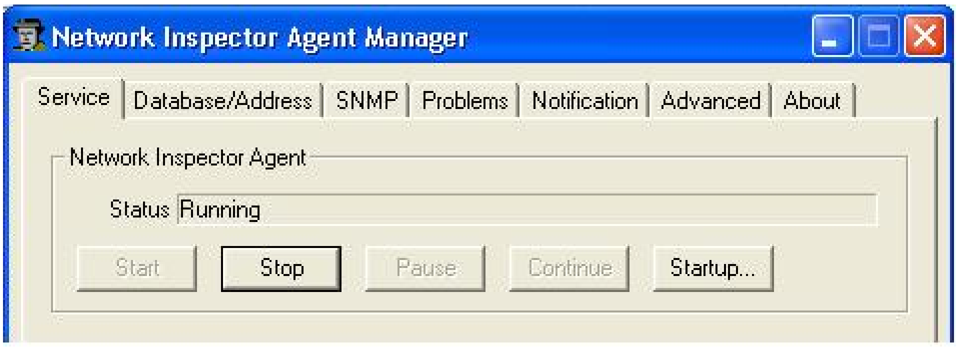


Figure 10.1

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.



Network Inspector Agent

Status Running

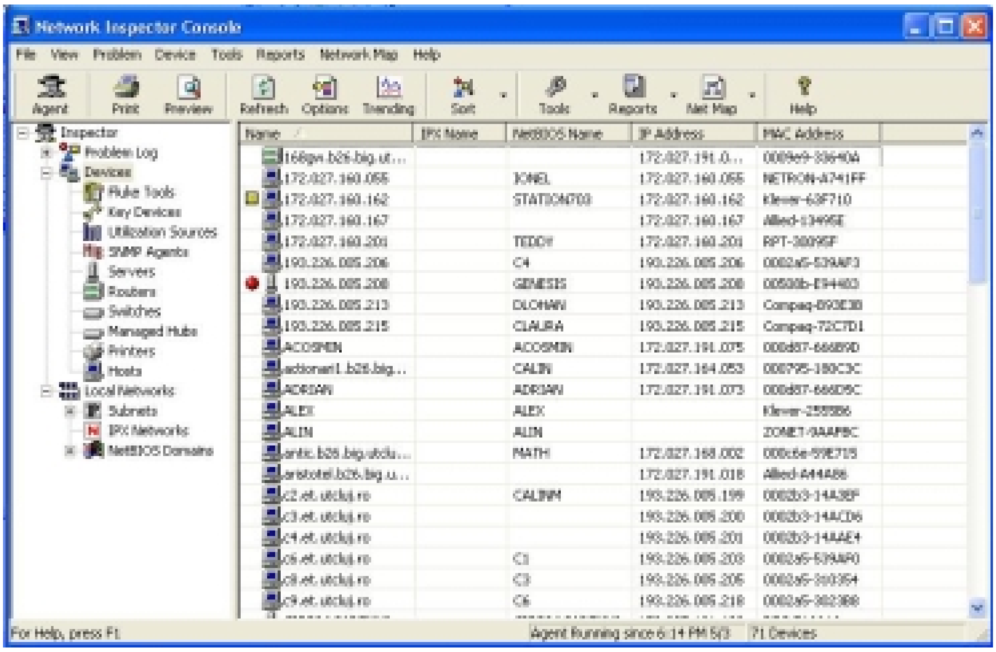
Figure 10.2

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.

2.2.3 Exploring the Network – quick view over the devices

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 as in the following example**.**



Name	IPX Name	NetBIOS Name	IP Address	MAC Address
168gw.b26.big.ut...			172.027.191.0...	0009e9-33640A
172.027.160.055		IONEL	172.027.160.055	NETRON-A741FF
172.027.160.162		STATION703	172.027.160.162	Klever-63F710
172.027.160.167			172.027.160.167	Allied-13495E
172.027.160.201		TEDDY	172.027.160.201	RPT-30095F
193.226.085.206		C4	193.226.085.206	0002a5-539AF3
193.226.085.208		GENESIS	193.226.085.208	00508b-E94403
193.226.085.213		DLOHAN	193.226.085.213	Compaq-893E38
193.226.085.215		CLAURA	193.226.085.215	Compaq-72C7D1
ACOSMIN		ACOSMIN	172.027.191.075	000d87-666B9D
actionar1.b26.big...		CALIN	172.027.164.053	000795-180C3C
ADRIAN		ADRIAN	172.027.191.073	000d87-666D5C
ALEX		ALEX		Klever-255586
ALIN		ALIN		ZONET-9AAF8C
antic.b26.big.utclu...		MATH	172.027.168.002	000c6e-59E715
aristotel.b26.big.u...			172.027.191.018	Allied-A44A86
c2.et.utcluj.ro		CALINM	193.226.085.199	0002b3-14A3EF
c3.et.utcluj.ro			193.226.085.200	0002b3-14ACD6
c4.et.utcluj.ro			193.226.085.201	0002b3-14AAE4
c6.et.utcluj.ro		C1	193.226.085.203	0002a5-539AF0
c8.et.utcluj.ro		C3	193.226.085.205	0002a5-3b0354
c9.et.utcluj.ro		C6	193.226.085.218	0002a5-3823B8

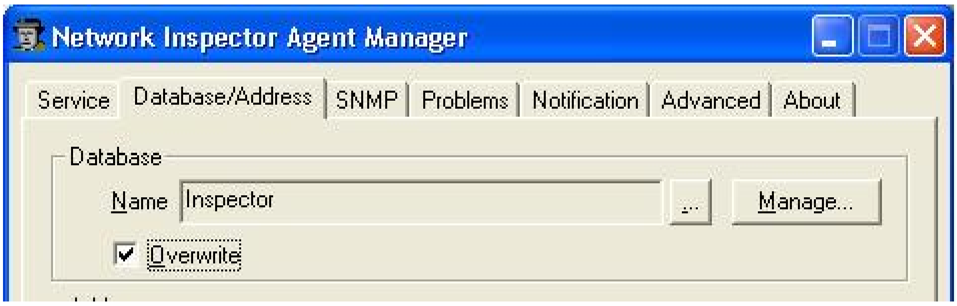
For Help, press F1

Agent Running since 6:14 PM 5/3

71 Devices

Figure 10.3

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.



Database

Name: Inspector

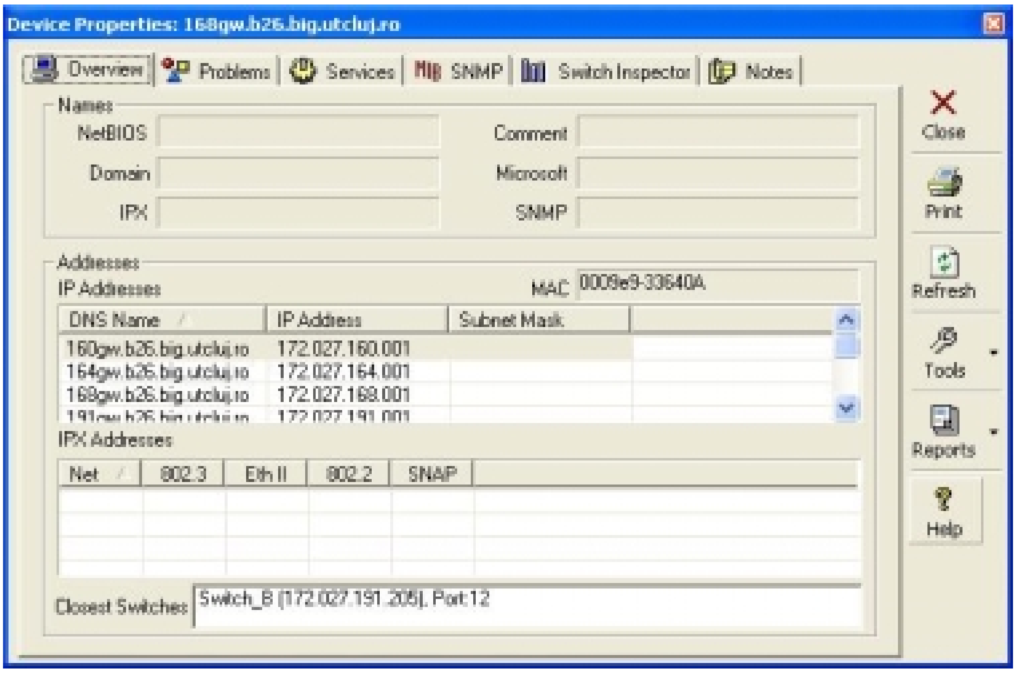
☑ Overwrite

Figure 10.4

The name of the devices will be different in this activity lab. Students will also notice IP and MAC addresses for each new device

2.2.4 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.



Device Properties: 168gw.b26.big.utcluj.ro

Names

NetBIOS

Domain

IPX

Comment

Microsoft

SNMP

Addresses

IP Addresses

MAC: 0009e9-33640A

DNS Name	IP Address	Subnet Mask
160gw.b26.big.utcluj.ro	172.027.160.001	
164gw.b26.big.utcluj.ro	172.027.164.001	
168gw.b26.big.utcluj.ro	172.027.168.001	
191gw.b26.big.utcluj.ro	172.027.191.001	

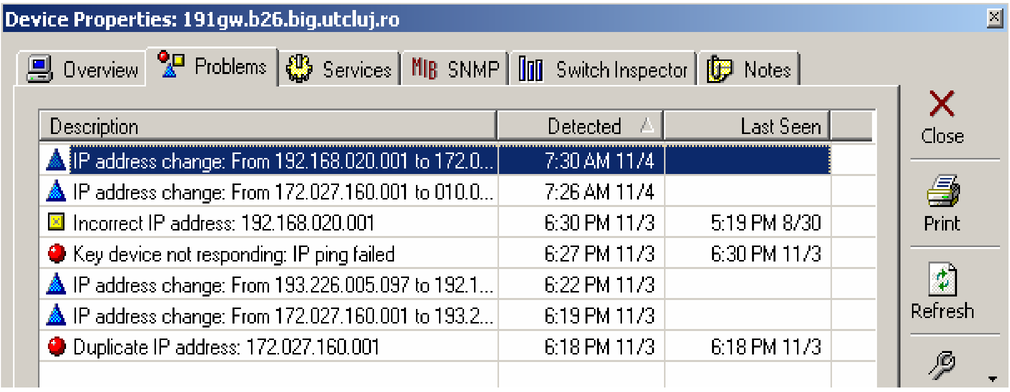
IPX Addresses

Net	802.3	Eth II	802.2	SNAP

Closest Switches: Switch_B [172.027.191.205], Port 12

Figure 10.5

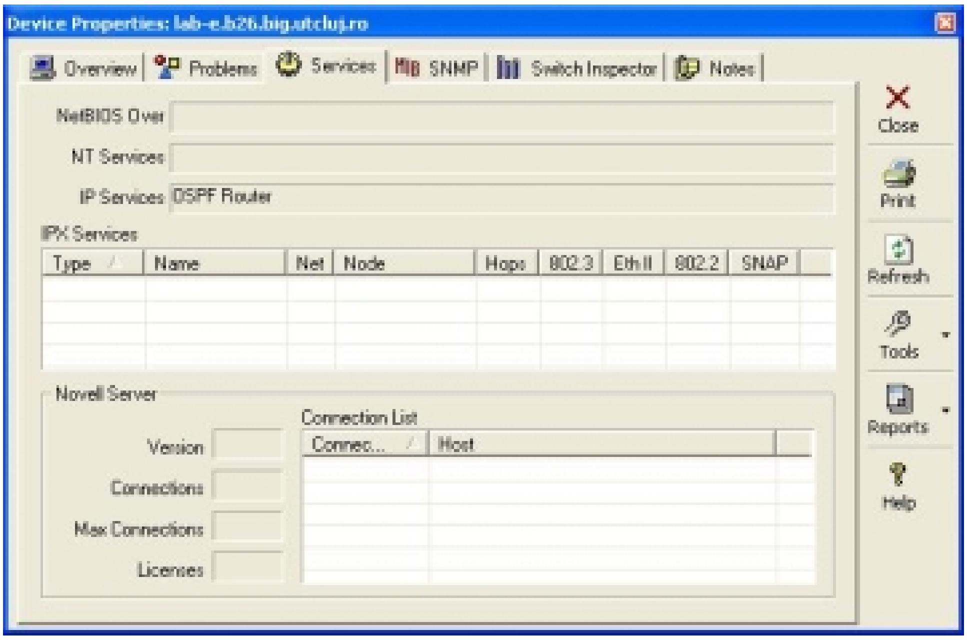
The **Overview** tab in the above graphic shows IP addresses, the IPX address, the IPX networks attached, the IPX data frame used and the MAC address. The closest switches will only appear if Network Inspector has been provided with a valid SNMP Community String for them. The **Problems** tab reveals one of the IP addresses is duplicated within the network. The red ball to the left of the Description indicates a problem.



Description	Detected	Last Seen
▲ IP address change: From 192.168.020.001 to 172.0...	7:30 AM 11/4	
▲ IP address change: From 172.027.160.001 to 010.0...	7:26 AM 11/4	
☒ Incorrect IP address: 192.168.020.001	6:30 PM 11/3	5:19 PM 8/30
● Key device not responding: IP ping failed	6:27 PM 11/3	6:30 PM 11/3
▲ IP address change: From 193.226.005.097 to 192.1...	6:22 PM 11/3	
▲ IP address change: From 172.027.160.001 to 193.2...	6:19 PM 11/3	
● Duplicate IP address: 172.027.160.001	6:18 PM 11/3	6:18 PM 11/3

Figure 10.6

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



NetBIOS Over

NT Services

IP Services OSPF Router

IPX Services

Type	Name	Net	Node	Hops	802.3	Eth II	802.2	SNAP

Novell Server

Version

Connections

Max Connections

Licenses

Connection List

Connec...	Host

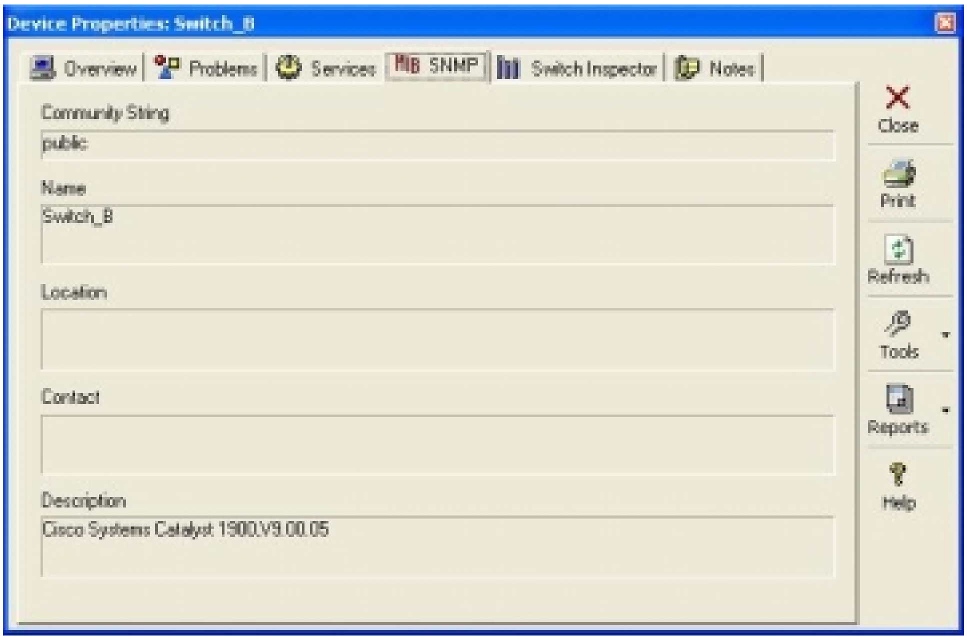
Figure 10.7

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.

From the example above you can see that the router uses the OSPF routing algorithm.

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.



Community String
public

Name
Switch_B

Location

Contact

Description
Cisco Systems Catalyst 1900.V9.00.05

Figure 10.8

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.. 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.

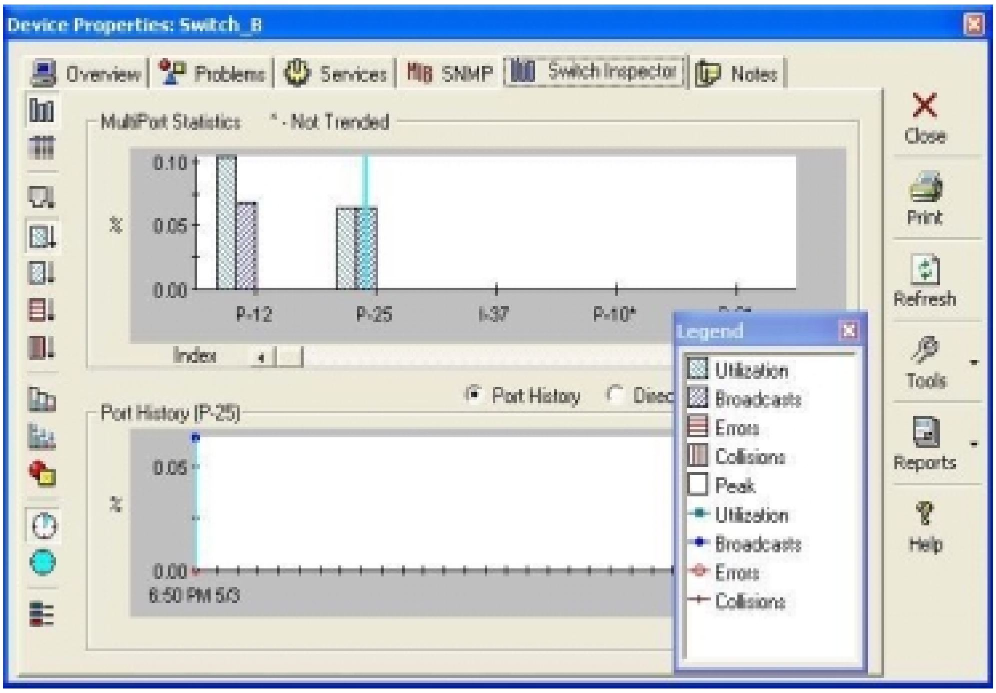
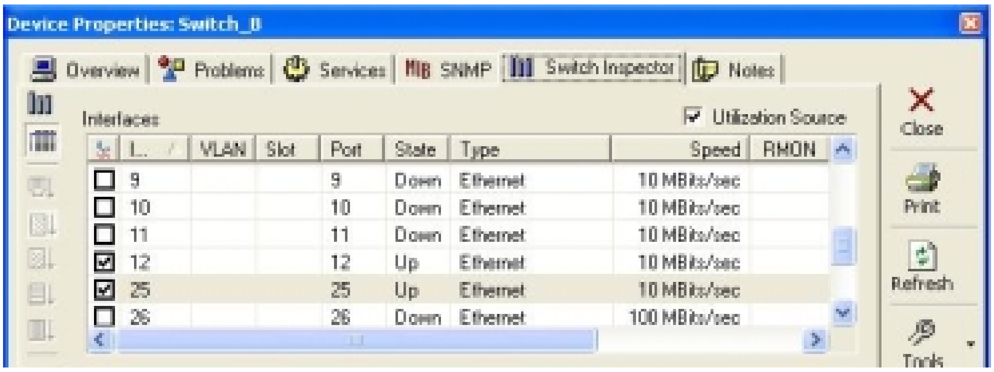


Figure 10.9

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.



Interfaces

☑ Utilization Source

	I...	VLAN	Slot	Port	State	Type	Speed	RMON
□	9			9	Down	Ethernet	10 MBits/sec	
□	10			10	Down	Ethernet	10 MBits/sec	
□	11			11	Down	Ethernet	10 MBits/sec	
☑	12			12	Up	Ethernet	10 MBits/sec	
☑	25			25	Up	Ethernet	10 MBits/sec	
□	26			26	Down	Ethernet	100 MBits/sec	

Figure 10.10

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. If the testing time is short the results will be the same.

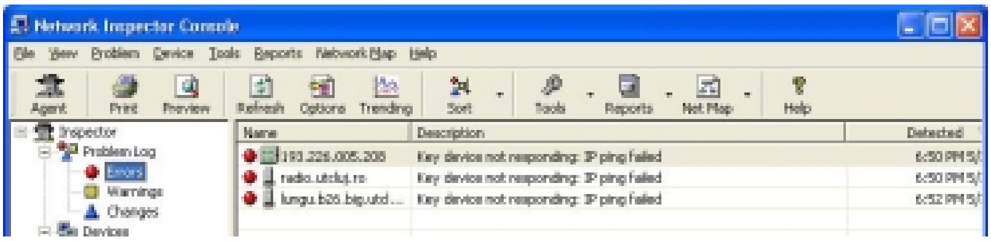
In the Switch Inspector window, the **Reports** button on the right side of the screen will expand to show two options. Select the **Switch Performance** choice and a multi-page report with various charts will appear on the screen. The **Switch Detail** option only works with a switch. After looking over the Device Properties window, click on the **Close** button in the upper right corner to return to the Network Inspector Console.

2.2.5 Explore the 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.

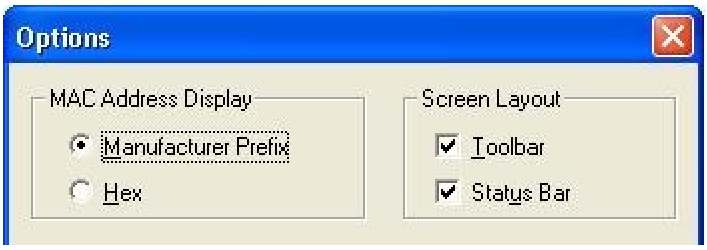
In the left pane, select **Devices** to show all devices in the right pane. Note the format of the MAC address.



Name	Description	Detected
193.226.005.208	Key device not responding: IP ping failed	6:50 PM 5/
radio.utcluj.ro	Key device not responding: IP ping failed	6:50 PM 5/
lungu.b26.big.utcl...	Key device not responding: IP ping failed	6:52 PM 5/

Figure 10.11

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.



MAC Address Display

● Manufacturer Prefix

○ Hex

Screen Layout

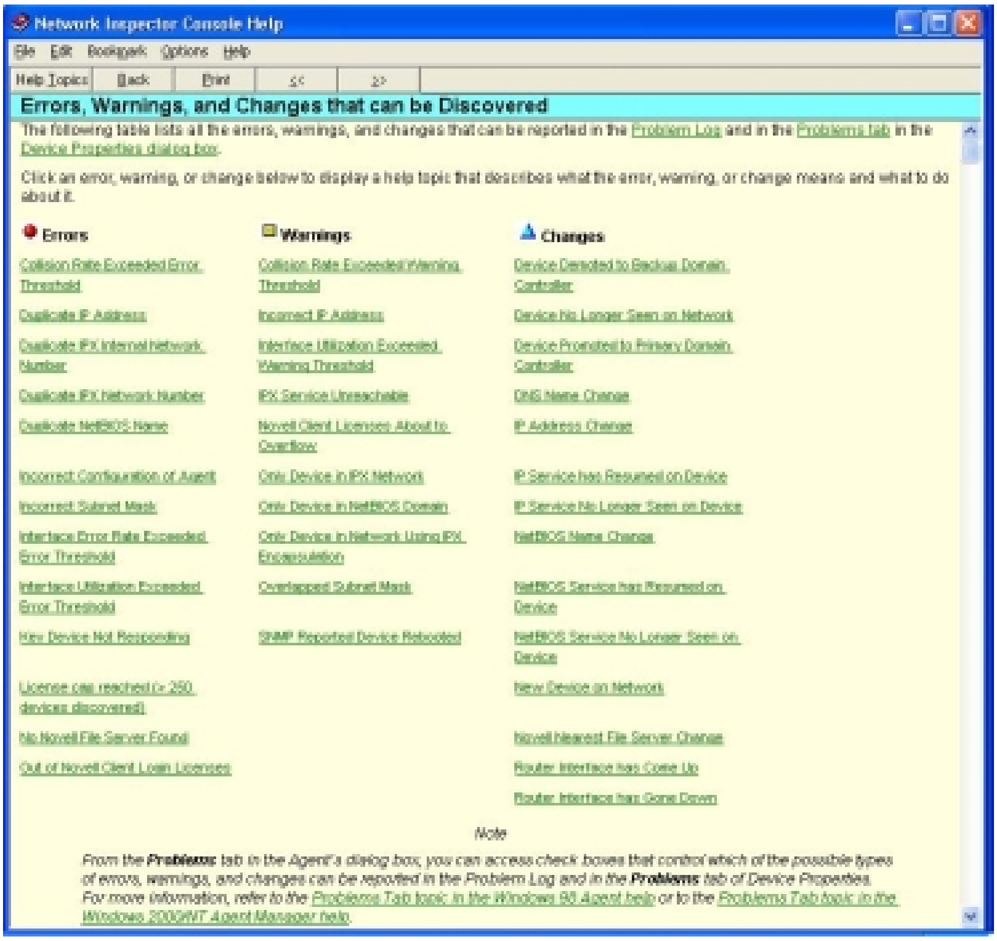
☑ Toolbar

☑ Status Bar

Figure 10.12

2.2.6 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.


Network Inspector Console Help
File Edit Bookmark Options Help
Help Topics Back Print << >>

Errors, Warnings, and Changes that can be Discovered

The following table lists all the errors, warnings, and changes that can be reported in the Problem Log and in the Problems tab in the Device Properties dialog box.

Click an error, warning, or change below to display a help topic that describes what the error, warning, or change means and what to do about it.

● Errors	Warnings	▲ Changes
Collision Rate Exceeded Error Threshold	Collision Rate Exceeded Warning Threshold	Device Demoted to Backup Domain Controller
Duplicate IP Address	Incorrect IP Address	Device No Longer Seen on Network
Duplicate IPX Internal Network Number	Interface Utilization Exceeded Warning Threshold	Device Promoted to Primary Domain Controller
Duplicate IPX Network Number	IPX Service Unreachable	DNS Name Change
Duplicate NetBIOS Name	Novell Client Licenses About to Overflow	IP Address Change
Incorrect Configuration of Agent	Only Device in IPX Network	IP Service has Resumed on Device
Incorrect Subnet Mask	Only Device in NetBIOS Domain	IP Service No Longer Seen on Device
Interface Error Rate Exceeded Error Threshold	Only Device in Network Using IPX Encapsulation	NetBIOS Name Change
Interface Utilization Exceeded Error Threshold	Overlapped Subnet Mask	NetBIOS Service has Resumed on Device
Key Device Not Responding	SNMP Reported Device Rebooted	NetBIOS Service No Longer Seen on Device
License cap reached (> 250 devices discovered)		New Device on Network
No Novell File Server Found		Novell Nearest File Server Change
Out of Novell Client Login Licenses		Router Interface has Come Up
		Router Interface has Gone Down

Note

*From the **Problems** tab in the Agent's dialog box, you can access check boxes that control which of the possible types of errors, warnings, and changes can be reported in the Problem Log and in the **Problems** tab of Device Properties. For more information, refer to the Problems Tab topic in the Windows 98 Agent help or to the Problems Tab topic in the Windows 2000/NT Agent Manager help.*

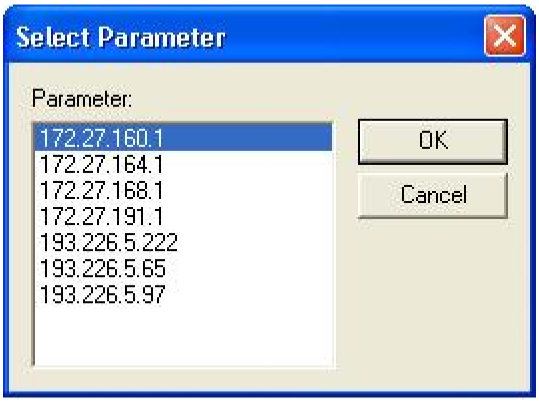
Figure 10.13

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.

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.



172.27.160.1
172.27.164.1
172.27.168.1
172.27.191.1
193.226.5.222
193.226.5.65
193.226.5.97

Figure 10.14

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.

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

2.2.7 Document router information

Select the router and document the following information where available:

a. What is the name of the device?
b. What IP services is the device running?
c. What IPX services is the device running?
d. What is the SNMP community string?
e. What is the location?
f. Which interfaces are available?
g. Which interfaces are up?
h. List below any problems that the software has discovered.

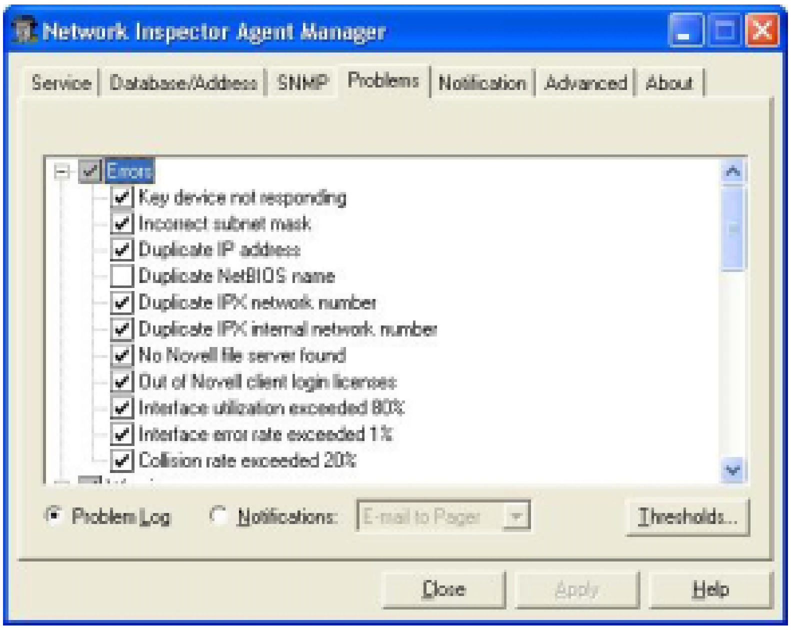
2.2.8 Observe discovered devices

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.

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.

2.2.9 Stopping the capture process and accessing the information table with detected problems

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.

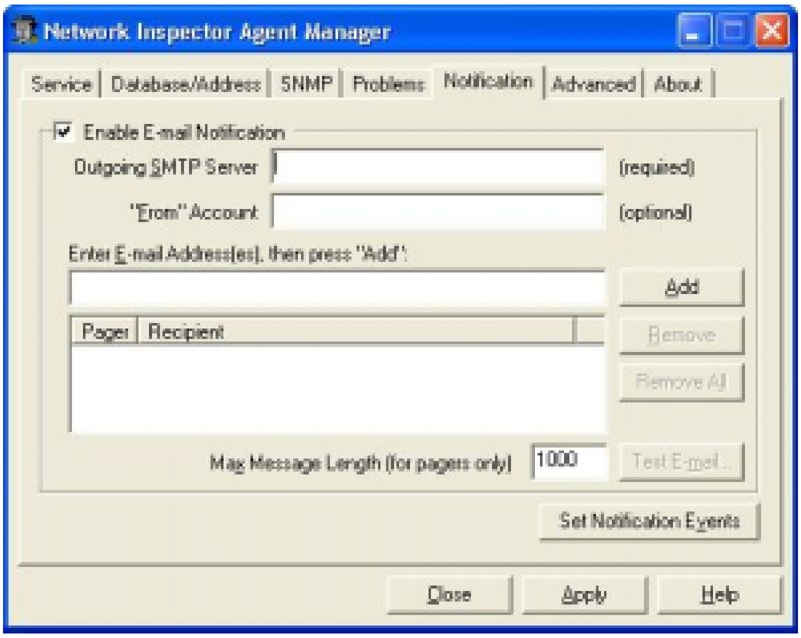


☑ Errors
- ☑ Key device not responding
- ☑ Incorrect subnet mask
- ☑ Duplicate IP address
- ☐ Duplicate NetBIOS name
- ☑ Duplicate IPX network number
- ☑ Duplicate IPX internal network number
- ☑ No Novell file server found
- ☑ Out of Novell client login licenses
- ☑ Interface utilization exceeded 80%
- ☑ Interface error rate exceeded 1%
- ☑ Collision rate exceeded 20%

● Problem Log ○ Notifications: E-mail to Pager

Figure 10.15

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



☑ Enable E-mail Notification

Max Message Length (for pagers only) 1000

Figure 10.16

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

3. Lab Activity

3.1 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.
Note: 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.
3.2 Because data from previous sessions may lead to network information inconsistence, activate the **Overwrite** checkbox under the **Database/Address** tab.
3.3 Double click the name of a router and select **Device Properties.**
3.4 Inspect the tabs from the **Device Properties** panel.

3.5 Select devices with problems (the ones marked with a red dot) if they exist and analyze the existent problems.

3.6 Select a switch and analyze the port statistics (the Switch Inspector, Tabular View, Graph View, and others), generate the reports. Execute a Ping and a Trace from the **Tools** button.

3.7 Inspect the **Problems Log.**

3.8 Activate the **Help** when a device with problems is selected by pressing the F1 key.

3.9 Document all the available information about a router.

3.10 Try to configure the agent to notify certain types of errors.

Notes