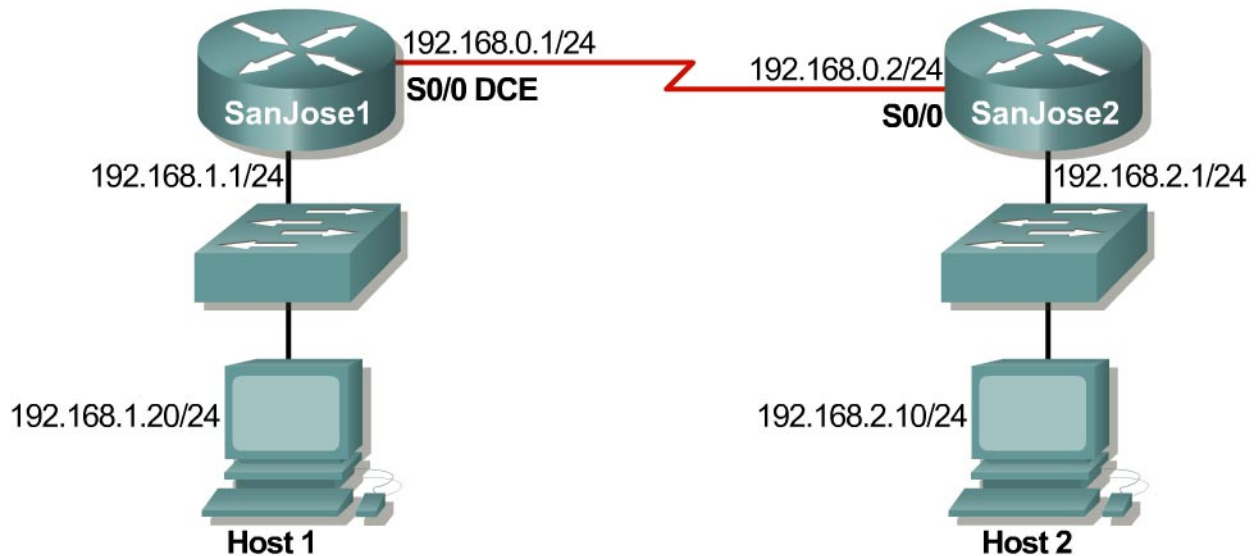


## Práctica de laboratorio 7.1.9a Introducción al Fluke Network Inspector



### Objetivo

Esta práctica de laboratorio es un tutorial que demuestra cómo usar el Fluke Networks Network Inspector (NI) para detectar y analizar los dispositivos de red en un dominio de broadcast. Esta práctica de laboratorio demuestra las características principales de la herramienta que se puede incorporar a varias tareas de detección de fallas en las próximas prácticas de laboratorio.

### Información básica / Preparación

El software Network Inspector puede distinguir estaciones de trabajo, servidores, impresoras de red, switches y hubs administrados, si se les ha asignado una dirección de red.

Opciones para llevar a cabo esta práctica.

- 1) Usar Network Inspector en una LAN pequeña controlada configurada por el instructor en un entorno de laboratorio cerrado como se muestra anteriormente. El equipo mínimo debe incluir una estación de trabajo, un switch y un router.
- 2) Realizar las tareas en un entorno de mayor tamaño, como la red del aula o de la escuela para ver mayor variedad de equipos. Antes de intentar de usar NI en la LAN de la escuela, consulte al instructor y el administrador de la red.

Se deben tener en cuenta los siguientes puntos:

1. Network Inspector detecta los dispositivos en una subred de red o VLAN. No busca más allá de un router. No realizará el inventario de toda la red de la escuela, a menos que toda ella esté incluida en una sola subred.
2. Network Inspector no es un producto de Cisco ni está limitado a detectar dispositivos de Cisco.

3. Network Inspector es una herramienta de detección, no de configuración. No se puede usar para reconfigurar dispositivos.

El resultado en esta práctica de laboratorio es únicamente representativo, y los resultados pueden variar según la cantidad de dispositivos, las direcciones MAC de los dispositivos, los nombres de host de los dispositivos y la LAN conectada.

Esta práctica presenta el software Fluke Networks Network Inspector, que resultará útil en prácticas de laboratorio posteriores sobre detección de fallas y en el campo. Si bien el software Network Inspector es una parte importante del programa de la Academia, también es representativo de las características de otros productos disponibles en el mercado.

Por lo menos un host debe tener el software Network Inspector instalado. Si la práctica se realiza en grupos de dos, ambas personas pueden ejecutar las tareas de la práctica de laboratorio si se instala el software en las dos máquinas. Seleccione Network Inspector y Network Inspector Agent durante la instalación.

La Consola puede estar en cualquier lado que tenga una ruta IP válida y la seguridad para permitir la conexión a un Agente. De hecho, puede ser un ejercicio interesante hacer que la Consola atraviese el enlace serial para cargar la base de datos desde el otro Agente. El estudiante puede hacer que la Consola lea una base de datos distinta de la que el Agente está usando en ese momento en el mismo PC.

## Paso 1 Configurar la red de laboratorio y conectar la estación de trabajo a la LAN de la escuela

**Opción 1.** Si se selecciona un entorno de laboratorio cerrado, realice el cableado del equipo como se muestra anteriormente y cargue los archivos de configuración en los routers correspondientes. Es posible que estos archivos ya estén precargados. En caso contrario, solicítelos al instructor. Estos archivos deben admitir el esquema de direccionamiento IP como se muestra en la figura anterior y la tabla siguiente.

Configure la estación de trabajo de acuerdo con las especificaciones de la tabla siguiente.

Host Nr. 1	Host Nr. 2
Dirección IP: 192.168.1.20	Dirección IP: 192.168.2.10
Máscara de subred: 255.255.255.0	Máscara de subred: 255.255.255.0
Gateway por defecto: 192.168.1.1	Gateway por defecto: 192.168.2.1

Como el software detecta dispositivos en la red, mientras haya más dispositivos, mejor será la demostración.

Si es posible, agregue hosts adicionales a ambas LAN.

**Opción 2.** Si se selecciona la opción 2, conectarse a la LAN de la escuela, basta con conectar la estación de trabajo, con Network Inspector o Protocol Expert instalado, directamente a un switch de un aula o un jack de datos conectado a la LAN de la escuela.

## Paso 2 Iniciar Network Inspector y el Agente

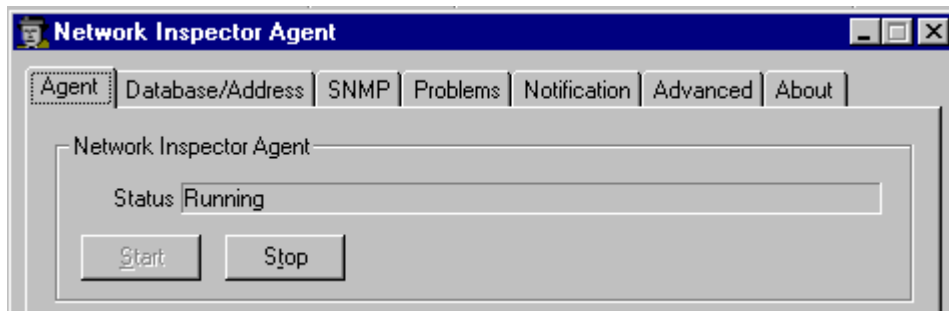
Desde el menú Inicio, abra "Network Inspector Console".

Haga clic en el botón **Agent** (Agente) en el extremo izquierdo de la barra de herramientas para que se pueda iniciar el Agente.



De ser necesario, seleccione la ficha **Agent** (Agente) en la ventana, y entonces haga clic en el botón **Start** (Inicio) y vea el cuadro **Status** (Estado) hasta que se muestre que el Agente está funcionando como se ve en la figura siguiente. Este proceso puede tardar varios minutos en empezar.

Observe el estado del Agente en la parte inferior de la ventana de la Consola. Observe cuidadosamente y vea que el Agente ha estado funcionando desde las 9:57 PM en el segundo gráfico a continuación, el cual fue capturado en el Paso 3.



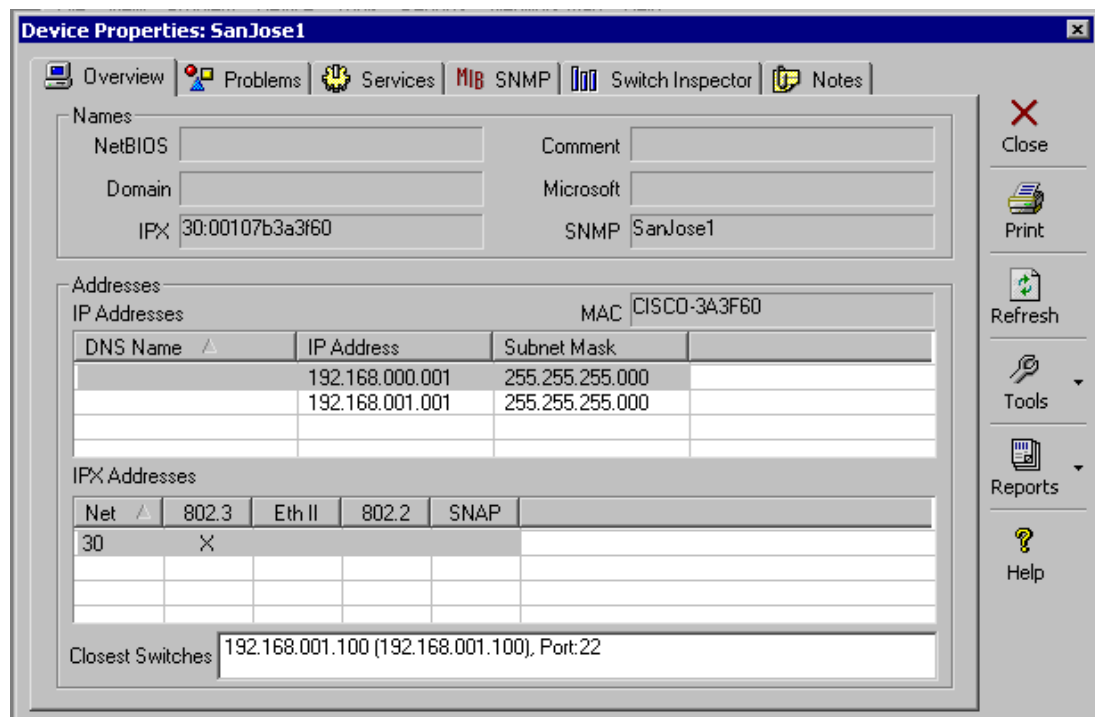
Use el botón **Close** (Cerrar) en la esquina inferior derecha de la ventana del Agente para que el Agente desaparezca. En algunas versiones, puede ser un botón **Hide** (Ocultar). No se debe usar el botón **Stop** (Detener), porque en ese caso el proceso de detección se interrumpirá.

## Paso 3 Permitir la detección en la red

El software Network Inspector está diseñado para reunir datos de la red sin interferir con su funcionamiento, de forma pasiva y activa. Por lo tanto, los dispositivos tardan en aparecer. Los dispositivos de una red pequeña deben aparecer en un par de minutos. La recopilación activa de datos estadísticos se demora durante los primeros 10 minutos. Una red de producción real puede tardar 30 minutos o más antes de detectar la mayoría de los datos.

Después de unos minutos, la ventana de la Consola debe empezar a mostrar información sobre la red. En el ejemplo siguiente, se agregaron dos estaciones de trabajo adicionales.

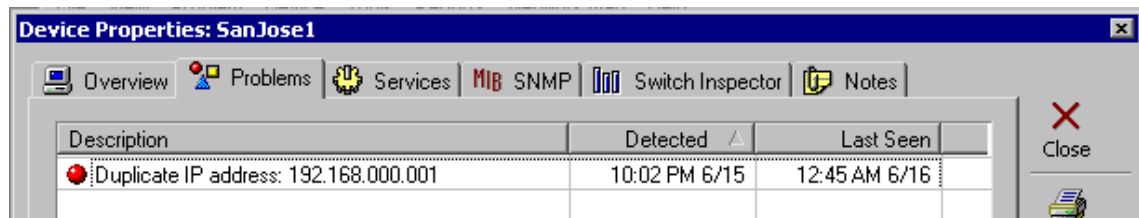




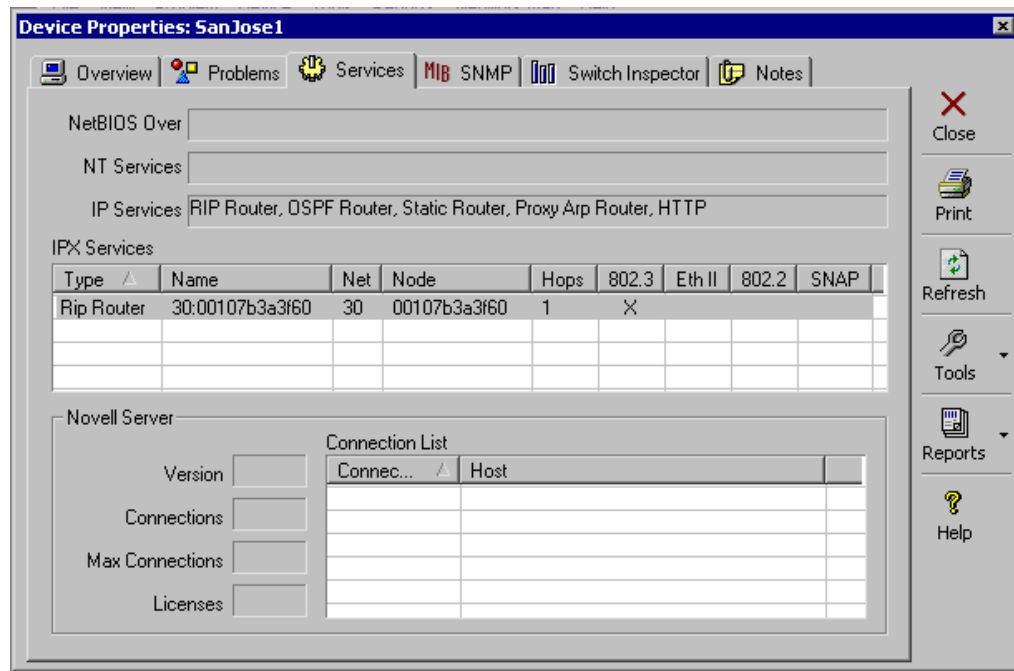
La ficha **Overview** (Descripción general) que aparece en el gráfico anterior muestra las direcciones IP, la dirección IPX, las redes IPX conectadas, la trama de datos IPX utilizada (802.3 en el anterior) y la dirección MAC. Observe que el OUI se ha convertido para identificar el fabricante en el ejemplo anterior.

Los switches más cercanos sólo aparecen si Network Inspector tiene una Cadena de Comunidad SNMP válida para ellos.

La ficha **Problems** (Problemas) revela que una de las direcciones IP está duplicada dentro de la red. Esto ocurre si el estudiante configura un host opcional tal como se define en el Paso 1. El círculo rojo a la izquierda de la Descripción indica un problema.



La ficha de **Services** (Servicios) revela los servicios IP y IPX que se ejecutan en los routers.

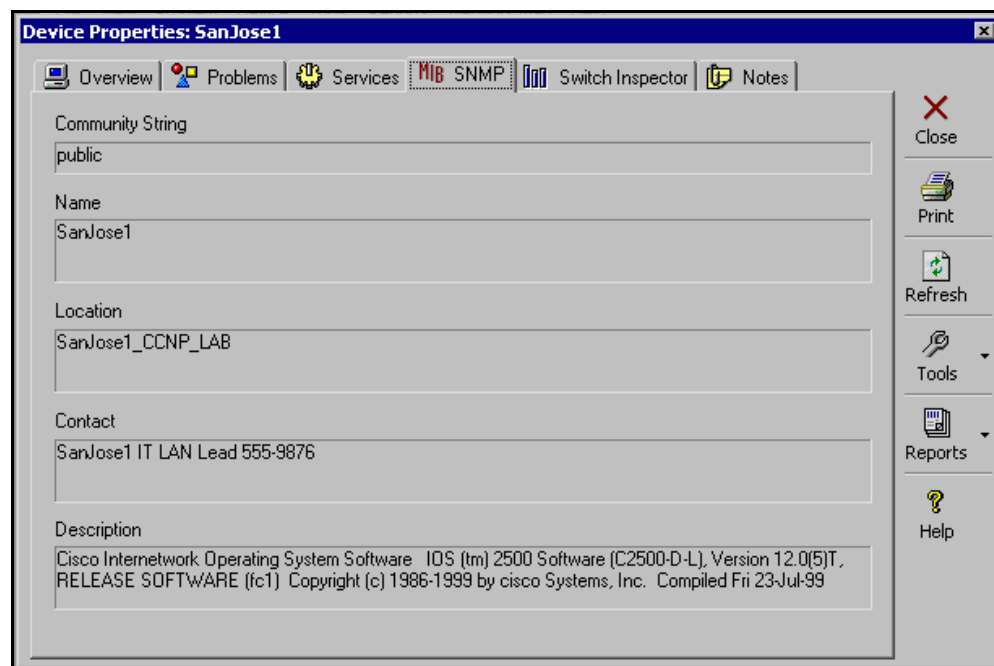


El ejemplo de los Servicios IP en el gráfico anterior muestra que se ha activado el servicio **IP HTTP Server** (Servidor HTTP IP). Esto significa que se puede acceder al router a través de un navegador de Web.


IPX Services (Servicios IPX) muestra el identificador de red IPX (30), la dirección de Nodo (MAC), el tipo de trama y el hecho de que se ejecuta RIP IPX.

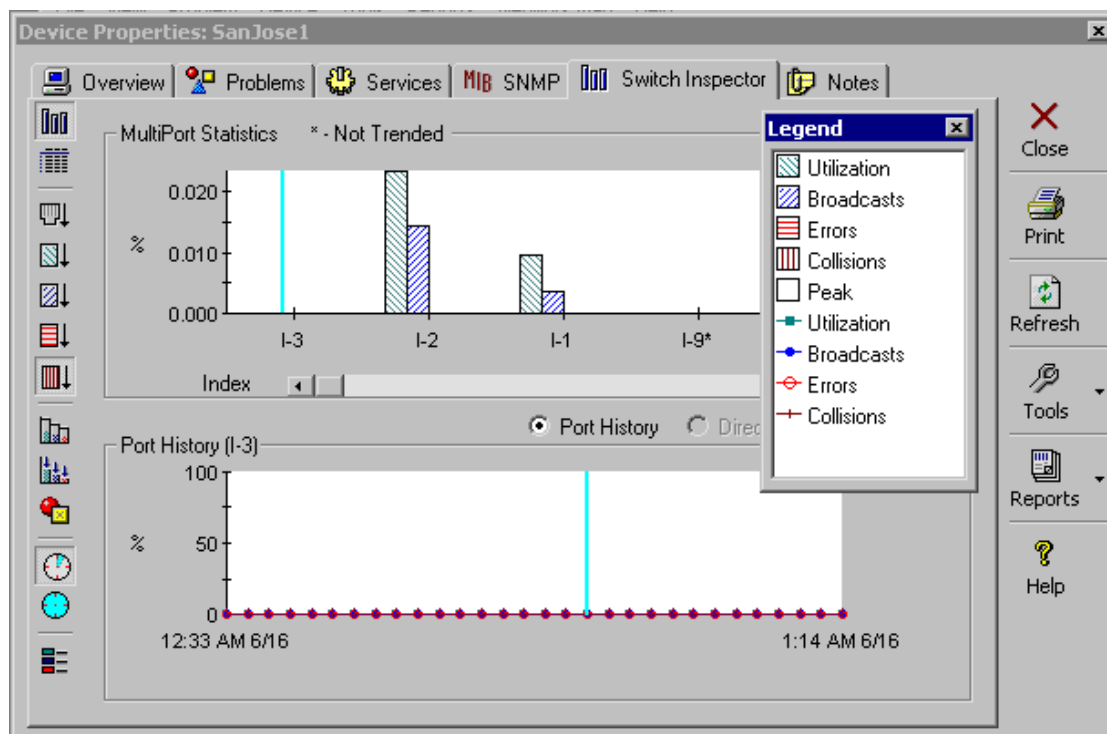
El tercio inferior de la ventana muestra la información que se revelaría si el dispositivo fuera un servidor de Novell. Un servidor con conexiones múltiples, que es uno que tiene más de una NIC (conexión) en redes diferentes, está funcionando como un router o puente.


La ficha **MIB SNMP** revela información de SNMP así como la información de IOS del router.

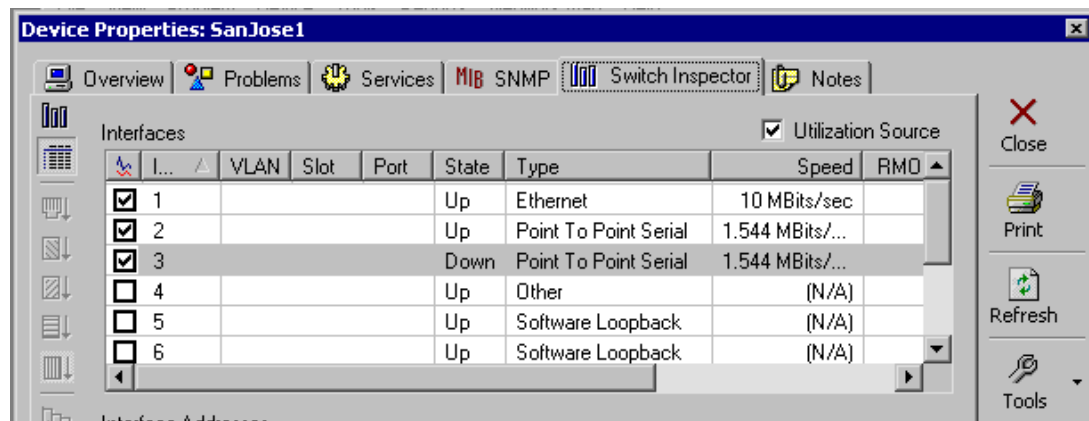


La ficha **Switch Inspector** (Inspector de switch) crea una serie de diagramas de los datos de interfaz del switch para el dispositivo seleccionado. Estos datos no se reúnen durante el período inicial de 10 minutos. La prueba Switch Inspector proporciona gráficos básicos de utilización para cualquier dispositivo con habilitación SNMP. El nivel de información ofrecido por esta prueba depende de qué MIB son admitidos por el dispositivo seleccionado. Por ejemplo, dado que SanJose1 es un router, el estudiante no puede mostrar la dirección de ningún dispositivo directamente conectado en un puerto destacado. Los botones del lado izquierdo de la ventana

cambian el formato del diagrama. El botón **Leyenda de gráfico**  que aparece en la esquina inferior izquierda muestra la leyenda flotante que se ve a continuación.

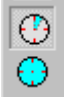


El segundo botón es **Vista tabular** , que al ser seleccionado, da detalles de cada interfaz en el dispositivo seleccionado incluyendo si la interfaz está activa o inactiva. La casilla de verificación a la izquierda de cada línea determina si las estadísticas se reúnen para detectar las tendencias de esa interfaz. Al desplazarse a la derecha aparecen los detalles de MTU y Description (Descripción) (FastEthernet0/0 o Token-Ring 0/1).



The screenshot shows the 'Device Properties: SanJose1' window with the 'Switch Inspector' tab selected. The 'Interfaces' table is displayed, showing details for each interface including its state, type, speed, and RMD. The 'Utilization Source' checkbox is checked.

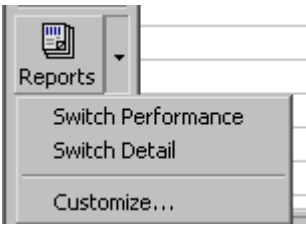
	I...	VLAN	Slot	Port	State	Type	Speed	RMD
<input checked="" type="checkbox"/>	1				Up	Ethernet	10 MBits/sec	
<input checked="" type="checkbox"/>	2				Up	Point To Point Serial	1.544 MBits/...	
<input checked="" type="checkbox"/>	3				Down	Point To Point Serial	1.544 MBits/...	
<input type="checkbox"/>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



Los dos botones que parecen relojes permiten seleccionar un historial de una hora o 24 horas, que pueden crear una comparación interesante si el NI ha estado funcionando por un período prolongado. En este ejercicio corto, los resultados serán iguales.

En el Switch Inspector, el botón **Reports** (Informes) a la derecha de la pantalla se expande para mostrar dos opciones. Al seleccionar la opción **Switch Performance** (Rendimiento del switch) aparece en pantalla un informe de varias páginas con diagramas. Vea los resultados.

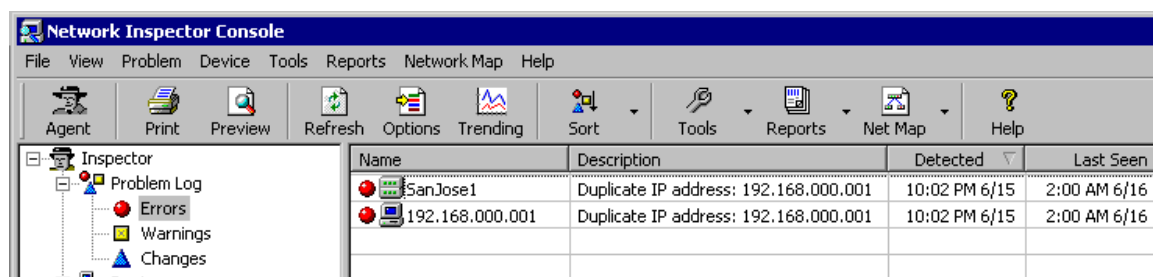
La opción **Switch Detail** (Detalle del switch) sólo funciona con un switch.



Después de ver la ventana Device Properties (Propiedades del dispositivo), haga clic en el botón **Close** (Cerrar) en la esquina superior derecha para volver a "Network Inspector Console".

### Paso 5 Explorar las opciones del panel izquierdo

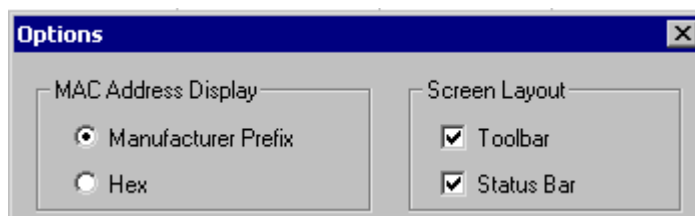
En la "Network Inspector Console", expanda y contraiga las opciones que aparecen en el panel de la izquierda. Como ocurre con el Explorador de Windows, si se selecciona un elemento en el lado izquierdo, el lado derecho muestra los detalles. En el ejemplo siguiente, al expandir el Problems Log (Registro de problemas) y seleccionar **Errors** (Errores) muestra en el lado derecho los dispositivos con errores. Esto facilita la detección de un dispositivo de dirección IP duplicada.



Pruebe con diferentes opciones en el panel de la izquierda y observe los resultados en el panel de la derecha. Debido a la cantidad limitada de dispositivos, algunos estarán vacíos. Pruebe más tarde con una muestra más grande.

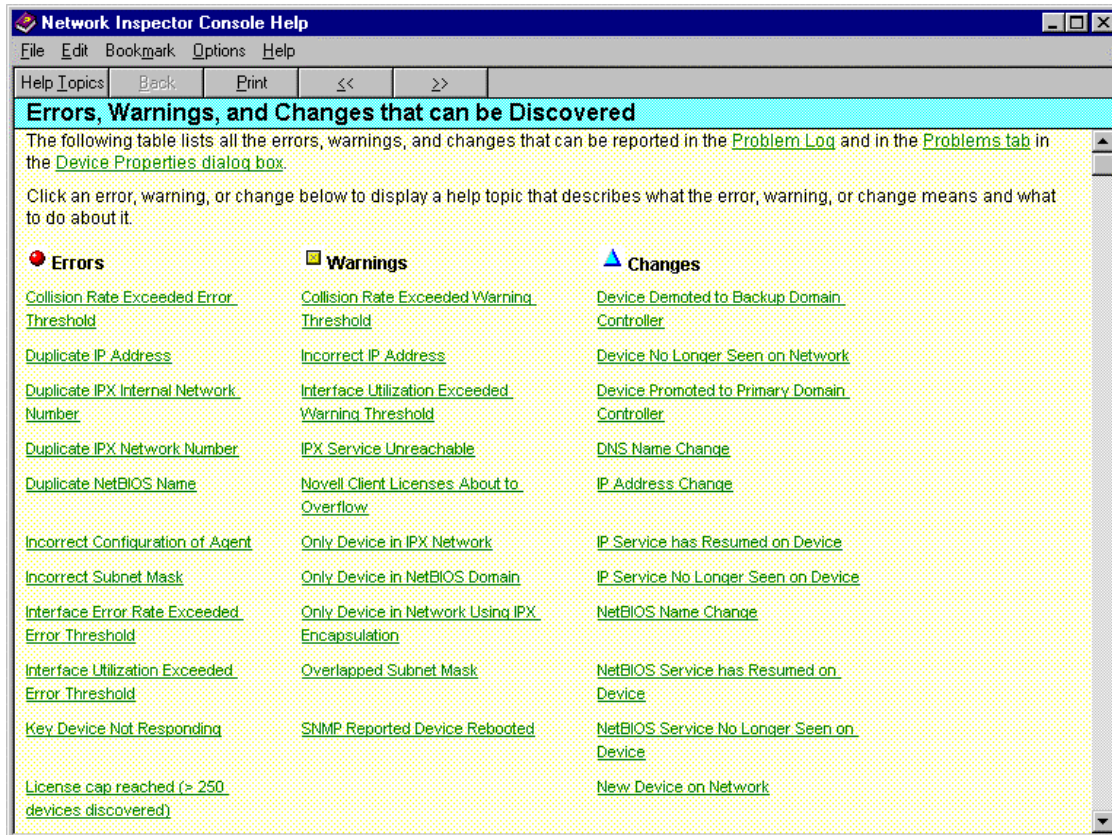
En el panel de la izquierda, seleccione **Devices** (Dispositivos) para que aparezcan todos los dispositivos en el panel derecho. Observe el formato de la dirección MAC.

Haga clic en el botón **Options** (Opciones) en la barra de herramientas (o **View > Options** (Ver > Opciones)) y observe que el estudiante puede elegir entre **Manufacturer Prefix** (Prefijo de fabricante) y **Hex** (Hexadecimal). Seleccione el que no aparezca elegido, vea las demás opciones y luego haga clic en **OK**. Observe el resultado.





**Ayuda.** En la pantalla principal de la Consola, verifique que esté seleccionado **Problem Log** (Registro de problemas), y que se haya resaltado un dispositivo de los que aparecen en la ventana de detalles. Presione F1, que es la tecla de función de Ayuda, para que aparezca una lista de problemas por categoría.



Como ejemplo, uno de los problemas creados por la configuración actual del Laboratorio en el gráfico anterior es una dirección IP duplicada. Para saber qué son las direcciones IP duplicadas, cuáles son los síntomas, y qué se puede hacer para resolver el problema, seleccione el hipervínculo de **Duplicate IP Address** (Dirección IP duplicada) de la lista. Hay abundante información en la Ayuda de este software.

Tómese un minuto y pruebe qué ocurre con los botones **Preview** (Vista preliminar), **Sort** (Clasificar) y **Reports** (Informes) en la barra de herramientas. La utilidad de estas funciones debe ser obvia. Observe especialmente las posibilidades de detección de fallas y documentación en los informes.

Seleccione un host y luego abra el botón **Tools** (Herramientas) en la barra de herramientas y seleccione **Ping**.

La casilla Select Parameter (Seleccione parámetro) incluye las direcciones IP de LAN al que el estudiante puede hacer ping. Seleccione una y haga clic en **OK**.

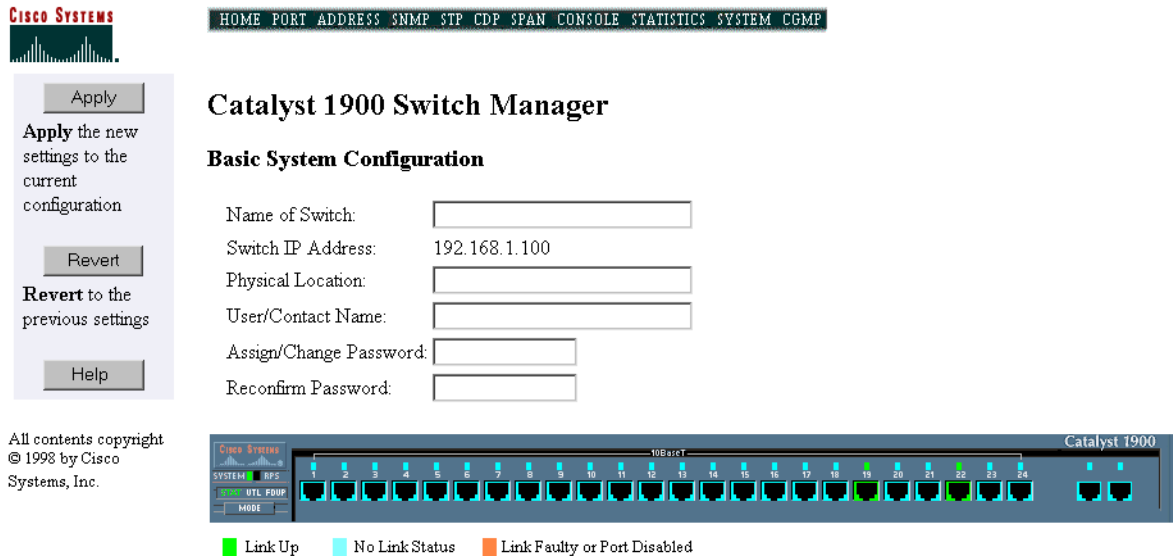
Aparece una ventana de comandos (MSDOS) para mostrar los resultados.

Escriba **exit** (salir) para cerrar la nueva ventana cuando termine.

Pruebe las opciones **Telnet** y **Traceroute**. Seleccione un router o switch en el visor de la Consola y luego seleccione Tools | Telnet (Herramientas | Telnet) y aparece una ventana con una sesión Telnet. El comando Trace funciona de la misma manera.

La opción **Web** del botón **Tools** (Herramientas) abre una sesión de Web con un dispositivo si la función IP HTTP Server (Servidor HTTP IP) está activada. Si intenta esto, el nombre de usuario es el nombre de host, que es SanJose1 o SanJose2, y la contraseña es cisco.

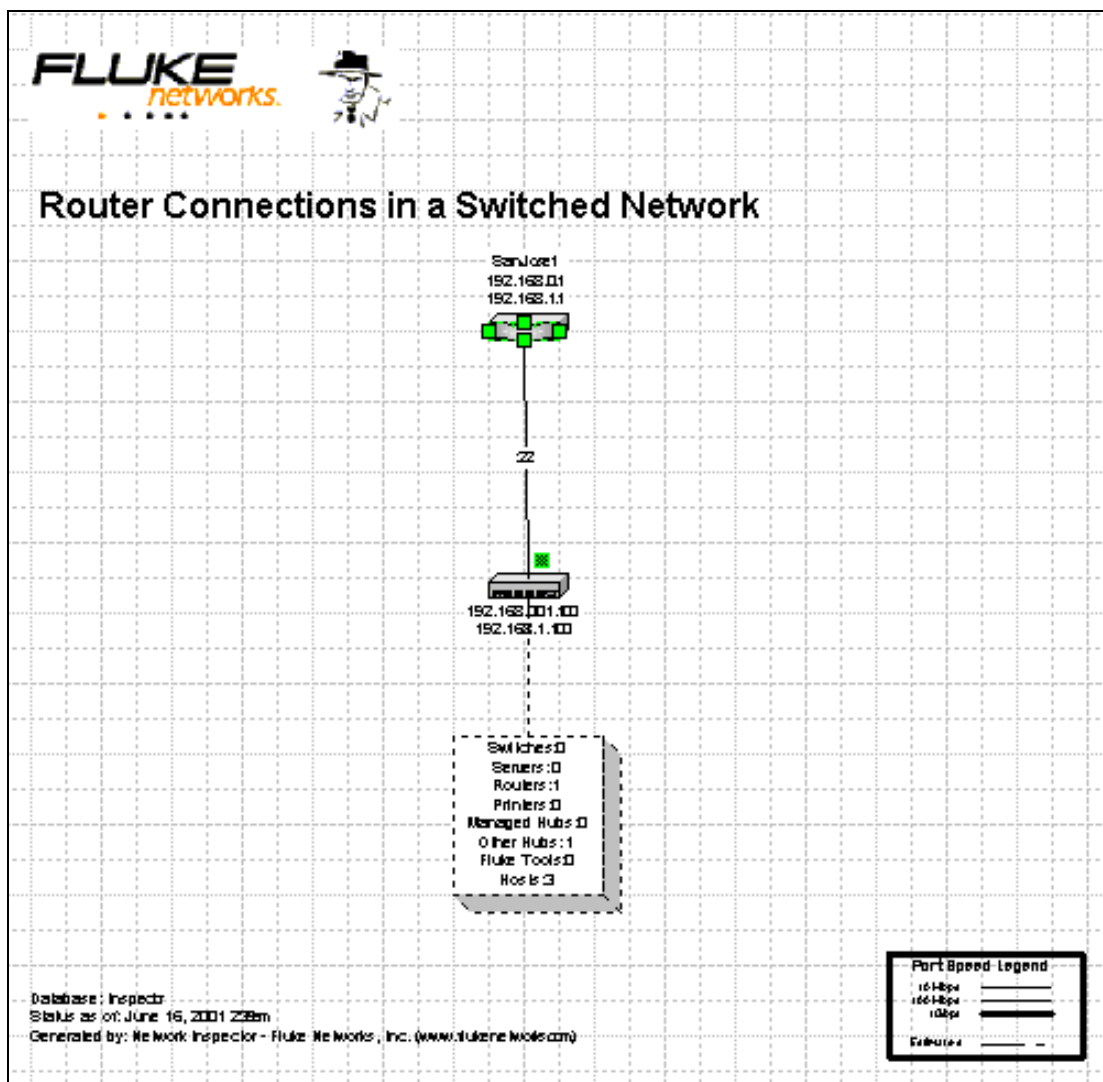
En la práctica de laboratorio de muestra anterior, el switch es un Catalyst 1924 con una dirección IP asignada. Por lo tanto, aparece lo siguiente si se selecciona la opción **Web** mientras el switch está resaltado:



Pruebe con las opciones anteriores de la barra de herramientas hasta que las conozca bien.

## Paso 6 Usar Net Map y Visio para diagramar la red

Si se ha instalado Visio en la estación de trabajo, el botón **Net Map** de la barra de herramientas activa Visio y crea un mapa de red del dominio de broadcast. El ejemplo siguiente usa "Router Connections in a Switched Network" (Conexiones de router en una red conmutada) en el botón Net Map. Hace un dibujo de la red, aunque no se incluya un switch.



Visio está totalmente integrado en NI. Esto significa que, al hacer doble clic en uno de los dispositivos del dibujo, aparece la ventana de Device Properties (Propiedades del dispositivo) que se usó en el Paso 4.

### Paso 7 Documentar la información del router

Aplicando las destrezas descritas anteriormente, seleccione el router y documente la siguiente información donde esté disponible:

a. ¿Cuál es el nombre del dispositivo?

\_\_\_\_\_

b. ¿Qué servicios IP ejecuta el dispositivo?

\_\_\_\_\_

c. ¿Qué servicios IPX ejecuta el dispositivo?

\_\_\_\_\_

d. ¿Qué es la cadena de la comunidad SNMP?

\_\_\_\_\_

e. ¿Cuál es la ubicación?

\_\_\_\_\_

f. ¿Quién es el contacto?

---

g. ¿Cuáles interfaces están disponibles?

---

h. ¿Cuáles interfaces están activas?

---

i. Enumere a continuación cualquier problema(s) detectado por el software.

---

---

---

## Paso 8 Observar los dispositivos detectados

De ser posible, conecte los dos switches con un cable de conexión cruzada y observe el resultado de NI a medida que se detectan nuevos dispositivos. Si no hay un cable de conexión cruzada disponible, elimine uno de los switches y conecte el host(s) y router en el segundo switch. Si bien esto no se hace normalmente en un entorno de producción, hágalo ahora para ver cómo responde NI.

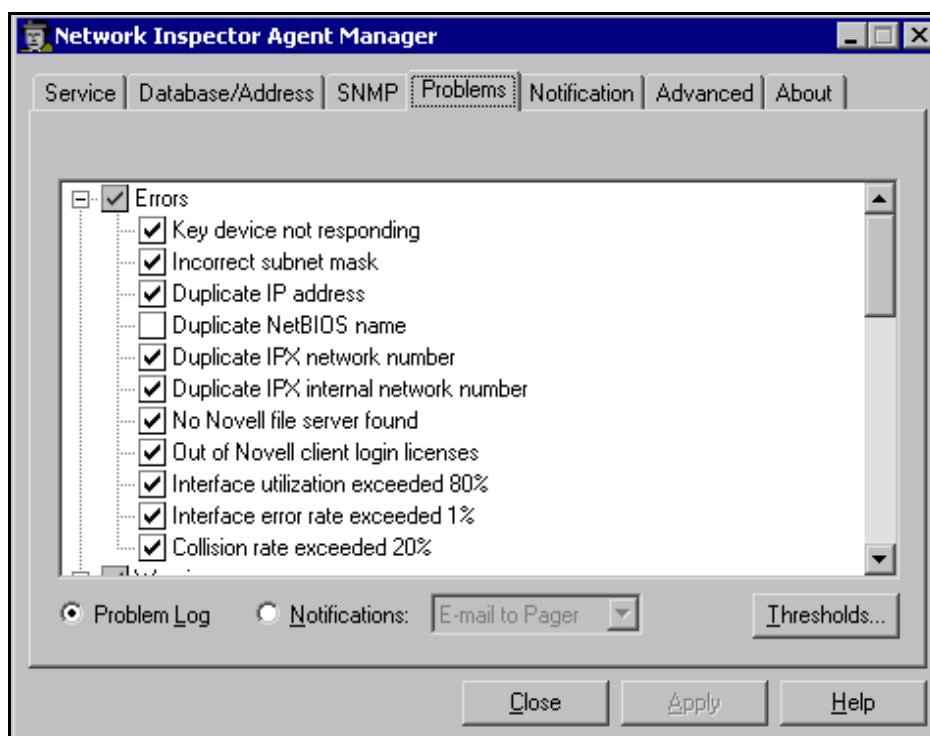
Los nuevos dispositivos deben aparecer inicialmente con triángulos azules que indican que acaban de ser detectados. Muchos aparecerán en su momento con un rectángulo amarillo de advertencia que indica un problema potencial. Recuerde que este proceso puede llevar 10 minutos o más.

Con el tiempo, se deberán ver las demás subredes y el segundo router.

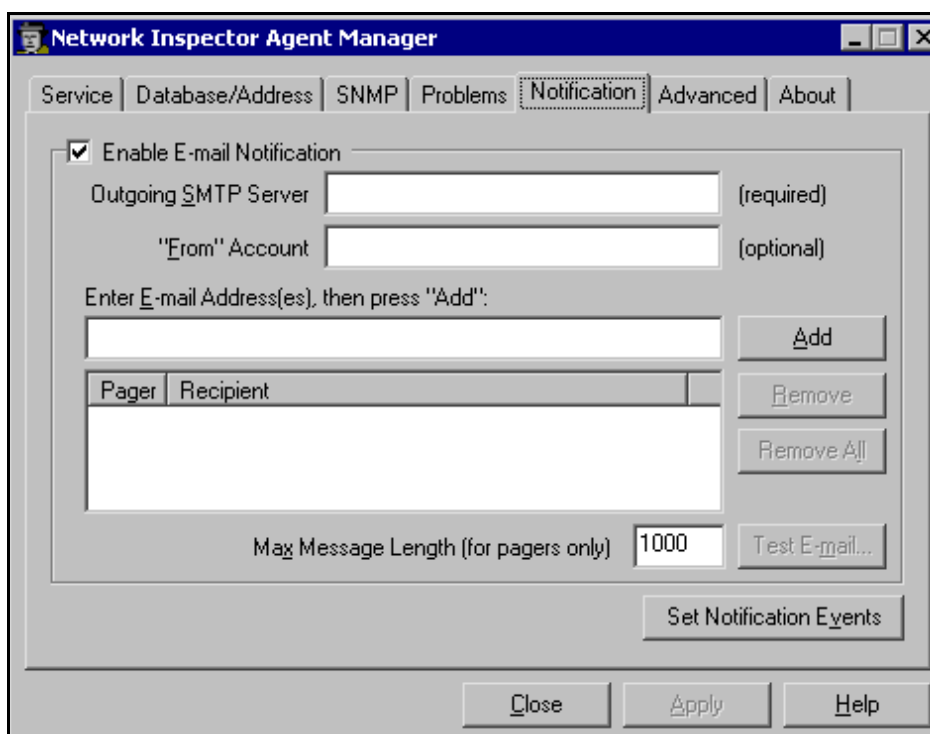
## Paso 9 Detener la captura y acceder a las fichas de Problemas y Notificación

Haga clic en el botón de **Agent** (Agente) en la barra de herramientas. El Agente ha estado reuniendo datos todo este tiempo. Haga clic en el botón **Stop** (Detener) y luego confirme su intención cuando se le pida que lo haga.

Observe las fichas para ver las opciones de base de datos que se pueden configurar. Observe la ficha **Problems** (Problemas) y las opciones para definir la investigación.



En la **Notification** (Notificación) observe que se pueden enviar notificaciones por correo electrónico. Para usar esta función, el estudiante necesita la misma información que la que se requiere para configurar una cuenta de correo electrónico de Internet o Outlook.



Si el estudiante inicia nuevamente el Agente, puede llevar unos pocos minutos para detectar los cambios ocurridos mientras el agente estaba inactivo.

## Paso 10 Experimentar con NI

Pruebe la herramienta NI mirando los diferentes dispositivos.

Si se instala NI en los computadores del aula, investigue los dispositivos en esa red más grande.

## Reflexión

¿Cómo se puede usar esta información en la detección de fallas?

---

¿Qué ventajas ofrece este programa para la documentación de la detección de fallas que no ofrece HyperTerminal?

---