# VISTA GLOBAL

## Capacidades Básicas Del Sniffer Pro

El Analizador de red sinffer pro de Network Associates es una poderosa herramienta de visibilidad para de redes. Consiste en un conjunto de funciones bien integradas que usted puede usar para:

- Capturar el tráfico de la red para un análisis detallado
- Diagnosticar problemas usando el Analizador Experto
- Monitorear la actividad de la red en tiempo real
- Recollectar la utilización detallada y estadísticas de error para estaciones individuales, conversaciones, o en cualquier porción de la red
- Guardar la utilización histórica e información de error para un análisis básico
- Generar alarmas en tiempo real visibles y audibles para notificar a los administradores de la red cuando se descubren problemas
- Prueba la red con herramientas activas para simular el tráfico, los tiempos de respuesta, contar puntos de conexión, y arreglar problemas

El sniffer pro está diseñado para aprovechar las características y ventajas de Windows 32-bits como multitarea. Usted puede ejecutar múltiples programas y sus herramientas individuales. El sniffer pro también puede correr conjuntamente con otras aplicaciones de Windows. la interface intuitiva de Windows hace al sniffer pro fácil aprender y de simple uso.

## Monitoreo En Tiempo Real

El monitor del sniffer pro guarda dimensiones estadísticas y cálculos sobre el tráfico de la red, mientras proporciona un cuadro exacto de la actividad de la red en tiempo real. Puede generar alarmas para notificarlo cuando se descubren errores. Puede guardar archivos históricos de la actividad de la red que usted puede usar después para el análisis del tráfico.

El monitor proporciona los siguientes tipos de información:

- Estadísticas de carga de la red, incluyendo el número de marcos/bytes del tráfico de la red por intervalo de tiempo, el porcentaje de utilización, y contadores broadcast y multicast
- Estadísticas de error de red, incluyendo,:

Para Ethernet, errores CRC, runt, paquetes demasiado grandes, jabbers, errores de alineación, cuenta de colisiones, y así sucesivamente,.

Para token ring, paquetes Ring purge, paquetes beacon, cambios NAUN, errores token, los errores soft, y así sucesivamente.

Para WAN/Synchronous, paquetes U-frame, paquetes S-frame, paquetes I-frames, paquetes LMI, y así sucesivamente,.

- Protocolo de uso estadístico
- Estadísticas por estación individual y de tráfico de conversación de pares
- Estadísticas de distribución de tamaño de paquete

La información colectada por el snifer pro lo ayuda a:

- Encontrar cargas excesivas de tráfico
- Solucionar "cuellos de botella"
- Localizar el equipo defectuoso
- Establecer la ejecución de la linea principal
- Planear para una expansión de la red
- Estructurar su red para una máxima eficacia
- Los datos recoletados por el monitor pueden ser un factor importante en la decisión de cómo asignar los recursos de su compañía para el mantenimiento de la red y actualizaciones.

NOTA:

Use los manejadores mejorados que están disponibles en el sniffer pro. Estos manejadores informan estadísticas de error de la red que los manejadores normales normalmente ignoran. los reportes de estadísticas de error del monitor dependen de haber instalado un manejador mejorado. Network Associates no soporta manejadores de otros vendedores.

## Monitor De Aplicaciones

Usted despliega los datos del monitor usando las aplicaciones del monitor. Las aplicaciones del monitor se listan bajo el menú del monitor y también están disponibles en la barra de herramientas. Cada aplicación del monitor se describe seguidamente.
Dashboard
matriz
tabla de host
historial
Distribución de protocolos
Estadísticas globales

## Base De Datos

El sniffer pro guarda las estadísticas generadas por las aplicaciones del monitor en tiempo real en un archivo de bases de datos Access de Microsoft. El archivo (netdb.mdb) se localiza en el directorio del programa sniffer pro. Por defecto, el sniffer pro actualiza el archivo de la base de datos para todas las estadísticas cada 60 minutos. Usted puede deshabilitar la colección de la base de datos para todos o las estadísticas específicas, puede cambiar el intervalo de actualización para las estadísticas, y puede anular todos o los archivos de la base de datos específicos. Usted también puede guardar el libro de direcciones del Sniffer pro.

## Alarmas

Las características de las alarmas del sniffer pro proporcionan un método comprensivo de descubrir y anotar los eventos anormales de la red (alarmas). hay dos fuentes para las alarmas:

- El sniffer Experto genera las alarmas durante la captura de los datos. Puede anotar un evento en la vitácora cuando descubre un síntoma o diagnóstico

- El administrador de alarmas del sniffer pro inicia automáticamente cuando usted inicia el sniffer pro. escribe un evento de alarma en la vitácora de alarmas cuando un límite de un parámetro especificado por el usuario se excede.

La vitácora de alarmas despliega información sobre alarmas que ocurrieron, incluso el estado de la alarma, el tipo de evento que ocurrió, el tiempo de ocurrencia, el nivel de severidad de la alarma, y una descripción del error. Ver la vitácora de alarmas, seleccione vitácora de alarmas de el menú monitor, o haga clic en el botón de la barra de heramientas.

Los eventos de red anormales pueden ser asignados a uno de los cinco niveles diferentes de severidad: Crítico, Mayor, Menor, Advertecia, e Informativo. Además, usted puede asociar cada nivel de severidad con cuatro acciones de notificación de alarma (por ejemplo, usted puede configurar el sniffer pro para enviar email cuando ocurre una alarma crítica o Mayor). las acciones de notificación de alarmas se pueden activar durante ciertos periodos de tiempo dentro de un día, o en ciertos días de la semana.

Modifique los Niveles de límites para la alarma

Notificación de Alarma automática

## Notificación De Alarma Automática

Usted puede configurar el sniffer pro para notificarlo cuando ocurre una alarma. El sniffer pro puede:

- Despertar un signo de alarma audible

- Enviar un email

- Llamar a un número de beeper

- Llamar a  un número de buscapersonas con el texto de alarma incluido

- Invocar un script de visual basic que a su vez puede lanzar otras aplicaciones o puede enviar una notificación de la alarma como un trap SNMP a una consola SNMP

Usted puede especificar las diferentes acciones de notificación de la alarma que dependan de la severidad de la alarma. Una alarma puede asignarse a uno de cinco niveles de severidad diferentes.

Cada nivel de severidad puede asociarse con cuatro acciones de notificación de alarma que pueden habilitarse para periodos de tiempo especificados dentro de un día, y en los días especificados de la semana.

Para configurar las acciones de notificación de la alarma, seleccione la pestaña de Alarma en la caja de dialogo Tools/Options.

NOTA:

Las alarmas expertas deben ponerse en (Tools/Expert Options/Alarms) para que la notificación tome efecto.

Defina las Acciones de Notificación de la Alarma

Asigne un Nivel de Severidad a un Tipo de Evento de Alarma

## Capturando Paquetes De La Red

Al contrario de la función monitoreo, la cual guarda dimensiones estadísticas y cálculos sobre el tráfico de la red, la función captura almacena paquetes actuales de su red y los descifra, mientras que proporciona información detallada sobre las transacciones de la red. Usted puede usar esta información para analizar la actividad de la red e identificar los problemas.

Panel captura

Use el panel Captura para controlar el proceso de captura del paquete. Plantear el panel Captura, selecione Capture/Capture Panel del la barra menú, o haga clic en el botón de la barra de herramientas.

Usando el panel Captura, usted puede:

- Iniciar y parar la captura
- Seleccionar un filtro de captura para usar mientras captura
- Accesar al dialogo  Define filte (definir filtro) para crear un nuevo filtro
- Muestra los resultados de una captura usando el Analizador Experto, muestra la decodificación, Mapa de Matriz, o una variedad de otros métodos

El panel Captura muestra el estado del proceso de la captura. La pestaña de graduación muestra el número de paquetes capturados y cómo está de lleno el buffer de captura (un porcentaje). La pestaña datalle muestras las estadísticas detalladas sobre el proceso de la captura actual.

Cuando usted empieza una captura, el sniffer pro abre su ventana Experta. En esta ventana usted puede supervisar la creación de objetos Expertos, y observa si hay cualquier indicación de problemas de la red.

Opción Docking (Conectarse)

El panel Captura es una ventana de conección. Usted puede conectarse en el escritorio del sniffer pro usando la caja de dialogo Tools/Options/Workspace, o haciendo clic con el botón derecho en el panel y seleccionando Docking View. Si no se conectó, es una ventana normal.

El buffer de captura

Los paquetes capturados se guardan en un buffer de captura. Usted puede desplegar los volúmenes actuales del buffer de captura, puede desplegar el análisis Experto, o puede guardar los paquetes capturados en el disco. Usted puede cargar y puede desplegar los archivos de la captura previamente guardados. Usted puede incluso hacer spool de los paquetes capturados de archivos en tiempo real, aumentando el tamaño de su buffer de captura eficazmente.

Opciones de buffer de captura

Para poner las opciones de buffer de Captura, seleccione Capture/Define Filter del menú principal, o haga clic en el ícono Define Filter en el panel de Captura, y seleccione la pestaña Buffer.

Usted puede configurar el tamaño del Buffer de captura de 256K bytes a 64 MB, dependiendo de cuánta memoria usted ha instalado en su computadora.

Usted puede guardar el paquete entero en el buffer de captura, o truncar cada paquete poniendo la opción de Packet Size (Tamaño de Paquete) definiendo un filtro de captura. Truncando los paquetes grandes, usted puede guardar más paquetes en el buffer de captura, mientras extendiende el tiempo cubierto por la captura y reduciendo el tamaño de los datos del archivo de datos de aptura, guardando espacio de disco (asumiéndo que se guarda en el buffer de captura del disco). En una red muy ocupada, marcos truncados pueden ayudar también ha evitar pérdidas de marcos, puesto que los marcos más grandes toman mucho más tiempo para ser almacenados.

Usted también puede especificar qué hacer cuando se llena el buffer de captura. Usted puede detener la captura automáticamente, o permitir la sobreescritura de datos.

## Desplegar Datos Capturados

Cuando usted empieza una captura, el sniffer abre la ventana experto en tiempo real. En cuadro de resumen Experto (cuadro superior izquierdo), usted puede observar los objetos de la red, síntomas, y diagnósticos que el analizador Experto crea mientras captura se desarrolla. Los síntomas y Diagnósticos son indicaciones Expertas de posibles problemas de la red. Usted puede navegar a través de varios cuadros en tiempo real de la ventana experta para mirar los items de interés.
Usted puede desplegar más información abriendo el Packet Display (Desplegar Paquete). Para abrirlo se debe:

- Hacer Clic en el icono de panel de Captura si una captura ha sido completada.

- Hacer clic en el icono de parar y Desplegar en el panel de Captura si usted está actualmente capturando datos.

- Hacer clic en File/Open y seleccionar un archivo para cargar y desplegar un archivo de captura previamente guardado.

Además de la ventana Experto, el Paquete desplegado proporciona vistas adicionales de los datos capturados en sus pestañas de Post Analysis (análisis posterior):

- Pestaña Decode (decodificar)
- Pestaña Matriz
- Pestaña tablade host
- Pestaña Distribución de Protocolo
- Pestaña de Estadísticas

(Para desplegar las pestañas de la Matriz, tabla de host, Distribución de Protocolo, y Estadísticas, selecione Display/Show de la pestaña Post analysis.)

El Despliegue de Paquete o Packet Display proporciona los controles para ayudarle en la investigación, vista, y filtrardo de los paquetes capturados desplegados en la pestaña Decode. haga clic en el item Display menu para acceder a estos controles.

Usted puede invocar las instancias múltiples del Packet Display para ver simultaneamente diferentes conjuntos de datos capturados, o para el conteniod actual del buffer con los archivos de la captura guardados.

También vea: pestañas Display

## Pestañas Display

Usted puede examinar los resultados de su captura en una variedad de formatos haciendo clic en una de las últimas pestañas de la ventana Packet Display. Las siguientes selecciones describen cada pestaña del formato de display.
Para una apreciación global de cada etiqueta (display) de despliegue , haga clic en un botón.

Pestaña expert
Pestaña decode
Pestaña Matrix
Pestaña host table
Pestaña protocol distribution
Pestaña Statistics

Tips:

- Para mostrar o esconder las pestañas post-analysis (Matrix, host Table, Protocol dsitribution, y Estadísticas) al fondo de Packet Display, seleccione las pestañas Display/Show / Hide Post Analysis del menú principal.

- Para mostrar o esconder la pestaña Expert Analysis, seleccione la pestaña Display/Show / Hide Expert análisis.

- Para evitar qen tiempo real que la ventana Expert se despliegue durante la captura, seleccione Tools/Expert Options/Objects y deschequee la caja de chequeo Expert durante la captura.

## Filtros

Hay dos categorías de filtros, filtros definidos y filtros automáticos.

Filtros definidos: Usted puede definir dirección, protocolo, y filtros de modelo de dato Booleano para seleccionar el tráfico particular que se necesita para su análisis de la red. Usando los filtros, usted se puede enfocar precisamente en los datos donde usted necesita arreglar los problemas de la red y minimizar el tamaño de archivos que recolecta para los archivos históricos.

Los Filtros automáticos: En algunos casos, son creados automáticamente por el sniffer pro cuando usted escoge ver la información seleccionada. Por ejemplo, usted puede individualizar una particular conversaciones de una estación usando el Filtro Visual en la Matrix map (despliegue de mapa de Matriz).

## Experto

En modo Experto, el sniffer pro observa el tráfico en los segmentos de la red, aprende sus características únicas, y automáticamente descubre una gran variedad de problemas, mientras escribe con precisión sus orígenes.
Cuando usted empieza una captura, el sniffer pro inmediatamente empieza a construir un banco de datos de objetos del tráfico de la red que éste ve. El sniffer pro usa sus intérpretes de protocolos para aprender sobre todas las estaciones de la red, ruteando nodos, subredes, y conexiones relacionadas a los marcos en el buffer de captura. Usando esta información, el sniffer pro descubre y lo alerta de problemas potenciales que pueden existir en la red. Estos problemas se categorizan en síntomas o diagnósticos.

## Triggers

La característica de el trigger le permite empezar y detener capturas basadas en fecha y tiempo, alarmas, y eventos de la red específicos. use los triggers para capturar los datos mientras el sniffer pro está sin vigilancia, tal como apagado en horas o fines de semana, o para empezar las capturas cuando ocurren los eventos específicos, como las condiciones de alarma.

Usted puede definir tres tipos de triggers - triggers de inicio, el cual empezará una sesión de captura, triggers de parada, los cuales pararán una sesión de captura, y triggers de inicio y parada, los cuales hacen ambas cosas. Una vez con un filtro, usted define un trigger y le da un nombre, usted puede usarlo siempre que sea apropiado.

Un trigger de inicio tiene dos elementos:

- Especificación de trigger- especifica que empezará una sesión de captura. Seleccione una especificación de trigger predefinido de una lista desplegable, o cree uno nuevo haciendo clic en el botón Define (definir).

- Especificación de filtro de captura- seleccione un filtro de captura para usar durante la captura. Seleccione uno de la lista Capture filter (Filtro de Captura).

Un trigger de parada tiene tres elementos:

- Especificación de trigger- especifica que detendrá una sesión de captura. Seleccione una especificación de trigger predefinido de una lista desplegable, o cree uno nuevo haciendo clic en el botón Define (Definir).

- Especificación retraso de trigger- especifica cuántos paquetes debe capturar después de que el evento de trigger de parada ocurre.

- Opción Restart - chequee esta caja para reiniciar automáticamente la captura después de que el evento de trigger de parada ocurre.

Vea Configuración de trigger de inicio y parada para Packet Capture para información adicional sobre configurar triggers.

## Libro De Direcciones

El libro de direcciones del sniffer pro permite asignar los nombres conocidos, reconocibles para sus nodos de red. El sniffer pro usa estos nombres simbólicos en lugar de direcciones de hardware de seis bytes o direcciones de red de capa IP en:

- Definicion de Filtros

- La captura decode display

- Visualización experto

- Visualización de tabla de host

- Visualización de la matriz

Para crear un libro de direcciones para mantener una tabla de nombres simbólicos para su propia red, usted puede:

- Entrar manualmente los nombres

- Importar una tabla de direcciones externas (formato CSV)

- Use la propiedad de autodescubrir del libro de direcciones

## Herramientas Activas

El sniffer pro incluye el siguiente conjunto de utilidades comues de IP que usted puede usar para identificar y arreglar los problemas de red de IP.

- Ping - Identifica la disponibilidad de un nodo host IP en la red
- Finger - visualiza la información sobre cada usuario conectado en red en un host especifico
- DNS Lookup - encuentra el nombre de dominio de una dirección IP, o viceversa
- Whois - Busca para un directorio TCP/IP un nombre de dominio registrado, el nombre de usuario, o ID del usuario
- Trace Route - Identifica todo router intermediario de una dirección IP entre su sniffer pro y un destino de host

Usted puede acceder a estas utilidades desde el menú Herramientas.

Usted también puede agregar sus propias herramientas al menú herramientas usando el itemmenú herramientas de usuario Tools/Customize. Para más información sobre agregar sus propias herramientas, vea la Adicionando herramientas al Menú Herramientas.

## Generador De Paquete

Use el Generador de Paquete para transmitir los paquetes de prueba en su red. transmitiendo los paquetes en la red le dan la habilidad de:

- Reproduce los problemas de la red para que usted puede arreglar y puede verificar los apuros de sus equipos de la red o aplicaciones
- Genera una carga de tráfico de red para que usted pueda simular las condiciones realistas de la red para probar su equipo o aplicaciones

El Generador de Paquete tiene dos vistas, una vista de animación y una vista de detalle.

- La vista de animación indica cuando están transmitiéndose los paquetes (animando cuando están enviándose los paquetes, aún cuando ningún paquete está enviándose).
- La vista de detalle muestra estadísticas detaladas del progreso de transmisión del paquete.

El Generador de Paquete tiene dos modos de acción, modo de paquete y modo buffer.

- El modo paqute transmite un solo paquete, cualquiera de los dos que usted ha creado o uno que usted ha capturado en la red.
- El modo buffer transmite los volúmenes enteros del buffer de captura.

Usted puede enviar paquetes en un solo tiempo, un número especificado de tiempos, o continuamente. Al enviar continuamente, usted puede especificar cuánto tiempo debe tardar entre cada paquete.

ADVERTENCIA:

Transmitiendo paquetes en una red real pueden causar resultados inesperados o dificultades. Asegúrese de transmitir sólo paquetes benignos a una red de producción, o aisle su red de la prueba de la red de producción antes de proceder con la generación del paquete.

El generador del paquete comparte los recursos de CPU con otras operaciones del sniffer pro. Usted puede generar tráfico, paquetes de captura, y puede supervisar la carga de la red al mismo tiempo. Note, sin embargo, ese funcionamiento los procesos múltiples pueden reducir la proporción a que pueden capturarse los paquetes en una red de gran velocidad simultáneamente.

También vea: Enviando un Solo Paquete, Revisando los Volúmenes del Paquete, reconstruyendo un Archivo de Captura,

# CÓMO HACER..

## USANDO SNIFFER PRO POR PRIMERA VEZ

### Invocando El Sniffer Pro

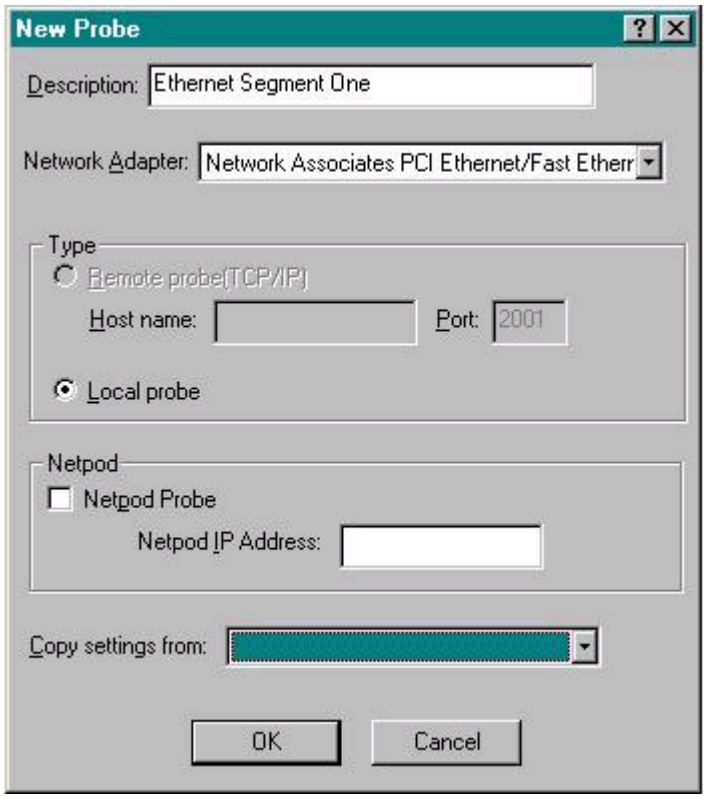
1. Click en el botón de inicio de Windows, y los seleccione Programas.

2. Click en el icono del programa sniffer pro para iniciarlo.

Si usted tiene más de un adaptador de red instalado en su sistema, una caja de diálogo de Adaptador le pedirá que seleccione un adaptador de red para el que sea supervisado por el sniffer pro.

### Seleccionando Una Prueba De Red O Adaptador

Si usted tiene más de un adaptador conforme con NDIS 3.1 instalado en su sistema, el sniffer Pro permite incluir el adaptador para su escojencia.
Para seleccionar un adaptador, vaya al menú Files y haga clic en Select Network Probe/Adapter. se abre el dialogo Select Network Probe/Adapter. Contiene las pruebas que usted ha definido para este sniffer pro PC. Usted puede seleccionar una prueba previamente definida para monitorear la red, o usted puede hacer clic en el botón New Proben para definir una nueva prueba para monitorear. Pulsando el botón en New Pobe despliega la caja de diálogo de New Probe.




- Use el campo Descripción para proporcionar un nombre descriptivo para este adaptador. Su descripción aparecerá en casos futuros en la caja de dialogo Select Network Probe/Adapter.

- Use el campo Adaptador de Red para seleccionar el adaptador. La lista incluye todos los adaptadores NDIS 3.1 actualmente instalados en el sniffer Pro PC.

- Use los campos Tipo para especificar si la prueba es Remota o Local. Para el sniffer pro, usted se limita a las pruebas Locales. Sólo se soportan las pruebas remotas para el sniffer pro Distribuído. Si usted está usando el sniffer pro Distribuído y usted selecciona una prueba Remota (es decir, una prueba que usted conecta encima de una red que usa TCP/IP), usted debe proporcionar el nombre del host y un número de puerto TCP usado para conectar la prueba remota.

- Habilite la caja de chequeo Netpod Probe si esta prueba se usará con una interface de red pod (así como Pod Full Duplex Ethernet de Network Associates). Cuando usted le habilita la caja de chequeo Netpod Probe, la dirección Netpod IP está automáticamente llena con una dirección IP incrementada por una dirección IP del sniffer pro PC. Por ejemplo, si la dirección IP del sniffer Pro PC es 206.129.112.24, la dirección IP Netpod proporcionada por el sniffer pro será 206.129.112.25.

NOTA:

Esta versión del sniffer pro sólo soporta conexiones locales para pods de red. Usted no puede conectar pods de red sobre la red.

- Use los conjuntos del campo Copy para usar los conjuntos de configuración de una prueba existente. La lista incluye todos las pruebas previamente definidas en el sniffer pro PC.

NOTA:

Varias opciones en el menús del sniffer pro cambiarán dependiendo del tipo de adaptador que usted ha seleccionado para la captura. Por ejemplo, habilitando un adaptador token ring habilitará diferentes opciones que habilitando un adaptador WAN.

Para más información sobre seleccionar una prueba de red o adaptador, vea Monitoreando Dos o Más actualmente Adaptadores de Red

## Usando Contexto De Menú

Un menú de contexto se invoca cuando usted aprieta el botón derecho del ratón. Es un atajo para acceder a algunos del la mayoría de comandos de menú usados.


El menú de contexto despliega una lista de comandos que usted puede usar para ejecutar operaciones en la ventana actual. Generalmente lista todos los comandos en el menú principal que son pertinentes al objeto, y unos atajos extras.

## ORGANIZAR VENTANAS

## Organizando Las Ventanas Dockable

Usted puede configurar el Dashboard, visualización de Paquete, y ventanas de Generador de Paquete para ser dockable o normal.
Una ventana dockable siempre se queda encima de otras ventanas, y será en todo momento visible. Cuando se arrastra y se incluye a el borde de la ventana principal.

1. Click en la raya pequeña entre el borde de la caja interior y el bordede la ventana dockable. Una caja rectangular negra se pondrá visible.

2. Mantenga el botón izquierdo del ratón presionado y saque la ventana de su posición.

Para cambiar una ventana dockable a una  ventana normal:

1. Posicione el cursor del ratón encima de la ventana.

2. Pulse el botón derecho del ratón para configurar el menú de contexto.

3. Deseleccione la vista Docking (quite la marca de chequeo).

Para poner el estado predefinido de las ventanas dockable, seleccione Tools/Options y haga clic en la pestaña Workspace. deschequee las ventanas que usted quiere convertir en ventanas normales.

# MONITOR ACTIVIDAD DE RED

## Vista Dashboard

El Dashboard visualiza la actividad de la red actual en el formato gráfico o tabular.
Para abrir el Dashboard, seleccione Dashboard del menú Monitor o haga clic en el botón de la barra de herramientas principal.

Una ventana abre mostrando el tráfico de red en tiempo real en un despliegue gráfico. El Dashboard despliega tres cuadrantes mostrando número de paquetes por segundo, porcentaje de utilización de red, y número de errores por segundo.
Para ver la carga de tráfico de red total acumulada desde el inicio del sniffer pro, haga clic en la pestaña Detail (Detalle) (Ethernet), las pestañas Llc o Mac (Token ring), o la pestaña WAN (WAN/Synchronous).

Para ver estadísticas promedio-por-segundo, pulse el botón derecho en Detail (Ethernet), Llc o Mac (token ring), o la pestaña WAN (WAN/Synchronous) y el selecione Show Average del menú de contexto.

TIP:

Si los números desplegados en el Detalle, Llc, Mac, WAN son truncados, ponga el indicador del ratón en el divisor vertical entre el item description y los números, entonces haga clic y arrastre la línea divisora a la izquierda para hacer un lugar para los números.

Visualización Ethernet Detail
Mostar token ring MAC y Llc

Pestañas Dashboard WAN

## Vista De Del Tamaño Del Paquete Y Distribución De Utilización

Monitorear el tamaño del paquete y distribución de utilización ayuda a entender los niveles de actividad global de la red, y para apuntar con precisión las cargas de tráfico de tamaño paquete grande y pequeña.
Para mostar el tamaño del paquete y la distribución de utilización:

1. Del menú de Monitor, seleccione Estadísticas Globales.

2. Click en la pestaña Utilización Dist. o Tamaño Dist. para mostrar el gráfico respectivo de la barra.

3. Click en el botón para ver la vista de gráfico de pastel.

## Vista De Estadísticas De Vínculo WAN

El monitor de estadísticas de vínculo WAN prorumpe por DTE y DCE para ayudarle a entender los niveles de actividad global nivela en la red, y para apuntar con precisión las cargas de tráfico de tamaño paquete grandes y pequeñas. Usted también puede comparar las cargas de tráfico en ambos lados del vínculo usando los despliegues gráficos.

Para visualizar las Estadísticas de vínculo WAN:

1. Del menú Monitor, seleccione las Estadísticas Globales.

2. Click en la pestaña del vínculo WAN.

Las siguientes estadísticas del vínculo WAN están proporcionadas:

Estadísticas WAN:

- Un gráfico rastrea la tasa de datos actuales en paquetes por segundo. Las tasas de datos son rastreados independientemente para DTE y DCE. Cada uno está graficado en un color por separado.

- Un gráfico rastrea el porcentaje actual de utilización del ancho de banda WAN total disponible. La utilización del porcentaje se rastrea independientemente para DTE y DCE. Cada uno es graficado en un color por separado.

- Un gráfico rastrea el número actual de errores por segundo en el vínculo WAN. los errores por segundo son rastreados independientemente para DTE y DCE. Cada uno es graficado en un color por separado.

Estadísticas Generales del vínculo WAN:

- La tabla de Red cuenta Paquetes, Bytes, Utilización, y Errores. Cada estadística se cuenta separadamente de DTE y DCE. Un total también se cuenta para cada estadística (DTE + DCE).

- La tabla de Error cuenta errores de aborto, errores de CRC, errores del Sobretamaño, y Fragmentos. Cada error se cuenta separadamente de DTE y DCE. Un total también se cuenta para cada estadística (DTE + DCE).

- La tabla de Distribución de Tamaño cuenta los marcos según varias ventanas de tamaño. El número de marcos visto en cada ventana del tamaño se cuenta separadamente de DTE y DCE. Un total también se cuenta para cada tamaño del marco (DTE + DCE).

## Recolectando Muestras De Historial

Para coleccionar las muestras del historial:

1. Seleccione History Sample del menú Monitor, o seleccione el botón de la barra de Herramientas.

ventana muestras del historial.

2. Es importante el icono para la muestra de la red usted quiere usar. Por ejemplo, para recolectar una muestra de historial muestra el número de paquetes por segundo en su red en un cierto periodo de tiempo, es importante el icono Packets/s.

3. Click el botón derecho del ratón para abrir el menú de contexto.

4. Selecione Properties para abrir la caja de diálogo History (historial).

5. En la pestaña General, entre el nivel de límite alto y bajo y el intervalo de prueba. (El sniffer pro mantiene un máximo de 3,600 muestras. Si usted especifica 15 segundos como intervalo de prueba, usted conseguirá 3,600 muestras en 15 segundos.)

6. Seleccione el tipo de gráfico que usted quiere usar: barra, Área, o Línea.

7. Click en la pestaña Color para escoger los colores para sobre lo Normal (límite), Normal, Primer plano, y colores del Fondo.

8. Click OK para guardar las configuraciones.

9. Doble click en el icono de muestra de red para empezar a monitorear.

Una ventana de la historia abre desplegando los procesos de muestra de datos de la red. Cuando un total de 3,600 muestras se ha grabado, monitoreando las paradas automáticamente. Usted también puede detener el monitor cerrando la ventana del Historial.

Cuando usted cierra la ventana monitoreando el historial, usted se obliga a aguardar los datos de la muestra a un archivo.

Para revisar las estadísticas guardadas del historial, seleccione Open del menú Archivo. en la caja de dialogo Open, seleccione el archivo guardado de estadísticas del historial, y pulse el botón OK.

NOTA:

Cuando usted ve los datos del historial en un gráfico de barras, el dato se despliega sobre el color Normal si excede el límite que usted puso.

Exportando los datos del historial a un archivo CSV o Excel

## Exportando Los Datos De Historial

Usted puede exportar los datos coleccionados en una Muestra del Historial a un archivo de texto en formato CSV, o a una hoja de cálculo de Excel.
Para exportar los datos de la muestra a un archivo de texto:

1. Click en el botón de la ventana del Historial. abre una caja de diálogo Export.

2. Entre el nombre del archivo, y pulse el botón (save) guardar.

Para exportar los datos de la muestra a Excel:

1. Selecciona la ventana del Historial los datos que usted quiere exportar pulsando el botón en cualquier parte dentro de la ventana.

2. Del menú Archivo, selecione Run Script.

3. Selecione hi2excel.bas (localizado en el directorio del Programa del sniffer pro), entonces pulse el botón Open.

El Averaje del programa abre con una nueva hoja de cálculo que muestra los datos de muestra de Historia actuales.

ADVERTENCIA:

Hi2excel.bas contiene una escritura Básica Visual usada por el Olfateador En pro de exportar los datos. No haga ninguna modificación a la escritura. Puede causar los resultados imprevisibles.

Usted debe tener un gráfico del Historial corriendo para exportar los datos a Excel.

## Visualización de Top Talkers (los que más conversan)

la gráfica de barras en la tabla de host muestra el tope-N de los los nodos del host más ocupados en tiempo real. Usted puede ver el tope-N del tráfico del host en MAC, IP, o IPX .
Para ver a los Top Talkers:

1. Del menú del Monitor, seleccione Host Table, o haga clic en el botón. La ventana de host table se abre.

2. Click en el botón en el lado izquierdo de la ventana host table.

3. Seleccione la capa de la red en la que usted quiere ver el tope-N de los talkers pulsando el botón de la pestaña apropiada en el fondo de la ventana de host table (por ejemplo, IP, IPX, SDLC, y así sucesivamente).

Por defecto, la visualización del tope-N se ordena por los bytes contados totales en la carga de tráfico y visualizada con los 10 primeros nodos de la red.

Para cambiar estas configuraciones:

1. Click para abrir la caja de dialogo de host table properties.

2. Seleccione la pestaña de gráfico tope-N.

3. Cambie el criterio de ordenamiento y el número del tope-N de los nodos a desplegar.

## Monitoreo del Volumen de Tráfico Nodos: matriz

Las estadísticas de la matriz proporcionan un análisis rápido del volumen de tráfico de conversación generado entre los pares de nodos de la red. Usted puede seleccionar la capa donde usted quiera ver el tráfico de la conversación haciendo clic en la pestaña apropiada al fondo de la ventana (por ejemplo, PVC, MAC, IP, IPX, y así sucesivamente)..
Las estadísticas de la matriz tienen cinco vistas diferentes: el mapa de tráfico, la tabla de detalle, tabla outline, grafica de barras o de pastel.

Para ver el tráfico de la Matriz:

1. Del menú del monitor, seleccione Matrix selecta o pulse el botón. La ventana Matriz se abre.

2. Clic:

En el  botón para ver desde arriba el modelo de tráfico de red.

3. En el botón para ver un resumen rápido de bytes totales y paquetes transmitidos entre los pares de nodos de la red.

4. En el botón para ver un resumen rápido del protocolo de la capa superior y su carga de tráfico transmitida entre los pares de nodos de la red.

5. En el botón para ver una gráfico de baras mostrando el tope-N de los pares de nodo de conversación más ocupados.

6. En el botón para ver un gráfico de pastel mostrando el tope-N el par de nodos de conversación más ocupados en su porcentaje relativo de carga de tráfico total del topN.

## Monitoreo de la Distribución de Protocolos de la red

La Distribución de protocolo informa el uso de la red basado en los protocolos de la capa de red - IPX/SPX, TCP/IP, NetBIOS, AppleTalk, DECnet, SNA, Banyan y otros - en tiempo real. También soporta la función de distribución de aplicaciones de TCP/IP que informa el porcentaje o carga acumulado de cada aplicación de TCP/IP como parte del tráfico de TCP/IP. El sniffer pro supervisará aplicaciones populares, como NFS, FTP, Telnet, SMTP, POP, HTTP (WWW), Gopher, NNTP, SNMP, y X-window.
También supervisa los protocolos IPX - NCP, SAP, RIP, NetBIOS, Diagnostic, Serialization, NMPI, NLSP, SNMP, y SPX. Los protocolos no listados están agrupados en otras categorías.

Para los adaptadores WAN, las pestañas están también proporcionadas para supervisar el uso de la red basado en los protocolos de la capa link - por ejemplo, por PVC para los circuitos frame relay. Las pestañas WAN disponibles dependen del protocolo de encapsulación actualmenteseleccionado en la caja de diálogo de Opciones.

Para iniciar el monitoreo de la Distribución de Protocolo:

1. Del menú del monitor, selecione la Distribución de Protocolo, o pulse el botón del icono. La ventana de Distribución de Protocolo se abre.

2. Usted puede desplegar la información en un gráfico de barras, de pastel o tabla pulsando el botón del lado izquierdo de la ventana de Distribución de Protocolo.

3. Usted también puede seleccionar la capa donde quiere ver la distribución de protocolo pulsando el botón en la pestaña apropiada al fondo de la ventana (por ejemplo, PVC, MAC, IP, IPX, y así sucesivamente).

## Aplicación de un Filtro al monitor

El sniffer pro le permite aplicar los filtros predefinidos al monitor. El filtro que usted aplica al monitor afecta todas las aplicaciones del monitor, Dashboard, tabla de host, tabla de Matriz, Historial y la Distribución de Protocolo.

Usando un filtro del monitor, usted puede mirar el tráfico de la red de varias vistas diferentes. Por ejemplo, definiendo y aplicando un filtro de dirección de hardware y de una router, usted puede contar la carga de tráfico fácilmente y de ese router. Usando el mismo filtro, la tabla de Matriz también mostrará que está hablando al router. Si usted abre la ventana de Distribución de Protocolos, mostrará el % de la carga de tráfico que atraviesa el router por los tipos de protocolo. Además, el gráfico del Historial trazará la carga de tráfico con respesto al tiempo del router.

Si usted quiere mirar la matriz y sólo las estadísticas de la tabla de host para trafico IP, usted puede definir y puede aplicar un filtro de protocolo IP. Si usted quiere se enfocar en otros tipos de protocolo, por ejemplo, IPX o AppleTalk, usted también puede definir los filtros para éstos.
Para aplicar un filtro al monitor:

1. Del menú del monitdor, escoja el Select Filter (seleccionar filtro).

2. Chequee Aplicar el filtro de monitor.

3. Seleccione un filtro de la lista.

4. Clic en OK.

También vea: Definir vista de Filtro

## USE LA BASE DE DATOS

## Desactivar Database Collection (Colección del Bases de datos)

Si usted no quiere guardar los datos coleecionados en tiempo real por el sniffer pro, usted puede desactivar la colección de la base de datos para todas las estadísticas o para estadísticas específicas (Estadísticas, host table, Matriz, y la Distribución de Protocolos).
Para desactivar la colección de la base de datos:

1. Seleccione las opciones del menú Database. se abre la caja de dialogo las opciones de Database.

2. Deschequee la caja en el área de Data Type para las estadísticas que usted no quiere guardar al archivo de la base de datos.

Si usted deschequea todas las cajas, ninguno de los datos se coleccionará en el archivo de la base de datos.

## Borrar los registros de la Base de datos

El sniffer Pro proporciona tres métodos para borrar los registros del banco de datos. Usted puede:

- Configure el sniffer pro para borrar automáticamente los registros de la base de datos después de cierto número de días.

- Borre todos los datos actuales del archivo de la base de datos.

- Borre todos los registros recolectados antes de una fecha específica.

Para Configurar el sniffer pro para borrar los registros de la base de datos automáticamente después de cierto número de días:

1. Seleccione Options del menú Database. La caja de dialogo de Opciones de la Base de datos se abre.

2. Chequee la caja Automatically delete records over (borrar Automáticamente los registros...) y especifique el tiempo (en días) en la caja del texto.

3. clic en OK.

Para borrar todos los datos actuales del archivo de la base de datos:

1. seleccione Purge del menú Database.

Para anular todos los archivos coleccionados antes de una fecha específica:

1. Seleccione Maintenance del menú Database. El diálogo de Mantenimiento de la Base de datos se abre.

2. Clic en la flecha al lado de la caja de texto para abrir el calendario.

3. Clic en el día del mes actual o pulse los botones de arriba del calendario para seleccionar un mes diferente.

4. Clic en OK.

## Cambio del Intervalo de Actualización de la base de datos

Usted puede cambiar cuan a menudo el sniffer pro actualize el archivo de la base de datos con las nuevas estadísticas en tiempo real:
Para cambiar el intervalo de actualización para las estadísticas del archivo de la base de datos:

1. Seleccione Opciones del menú Base de datos. la caja de dialogo del las Opciones de la Base de datos se abre.

2. Clic en la celda de Intervalo de Actualización (minutos) para los tipos de datos que usted quiere cambiar.

3. Seleccione la tasa de actualización de la lista desplegable.

4. Clic en OK.

## Guardar el Libro de Direcciones al Archivo de la Base de datos

Para guardar el libro de dirección al archivo del Banco de datos del sniffer pro, seleccione Save Address Book del menú Base de datos.

# CAPTURA DE PAQUETES

## Capturando Todos los Paquetes de la Red

1. Del menú Captura, selecione Capture Panel (panel decaptura). La ventana se abre.

2. Seleccione Valor por defecto de la lista desplegable de los filtros disponibles.

3. Clic para empezar la captura. El sniffer pro despliega la ventana Experto en tiempo real, y la captura muestra el estado de la captura en marcha.

4. La captura se detendrá cuando el buffer esté lleno (el tamaño predefinido de bytes es de 256K). Alternativamente, pulse el botón para detener la captura.

5. Si usted quiere hacer una pausa en la captura, haga clic.

Entonces pulse el botón para reasumir de nuevo la captura.

En La ventana de Captura se despliega el progreso de la captura actual de:

- El número de paquetes que capturó

- El porcentaje del espacio del buffer lleno

Usted puede ver los datos en forma gráfica o tabular pulse el botón de la pestaña Gauge o la de Detail (Detalle).

La ventana Expert despliega o muestra los objetos acumulados, síntomas y diagnósticos en el recuador de Expert Overview. Mientras la captura está en marcha, usted puede seleccionar los items en la ventana Expert para enfocar las estaciones particulares, protocolos, eventos.

TIP:

El perfil del filtro predefinido que viene con el sniffer Pro permite todos los marcos (ningún marco se filtra afuera), y el buffer de captura está fijo en 256KB. cuando el buffer se llena se Detiene la Captura. para Crear un nuevo filtro o modificar el filtro predefinido, vea Definir Filter Overview.

## Usar un Hot Link para Empezar la Captura

El sniffer pro soporta una función del hot link en el mapa de tráfico de Matriz, Matrix outline table, and Host outline table windows. Esta función le permite lanzar una sesión de captura de paquetes directamente para uno de los nodos seleccionados de estas ventanas. La función de hot link crea un filtro de dirección temporal para apuntar sólo a los nodos que usted selecciona de la pantalla.

El ejemplo muestras cómo lanzar una captura usando hot links para multiples direcciones de IP:

1. Desde el menú Monitor, seleccionando Matrix, o haciendo click en la barra de la herramienta. Una ventana Matriz es desplegada.

2. Clic en el botón Traffic Map (Mapa de Tráfico) (en el borde izquierdo de la ventana Matriz) para mostrar el tráfico de red actual.

3. Clic en la pestaña IP en el boton de la ventana Matriz para ver todo el trafico IP.

4. Para filtrar tráfico en uno o más nodos de la red, seleccione cada nodo. Para seleccionar más de un nodo, sostenga la tecla Ctrl abajo mientras selecciona.

5. Clic en el botón derecho del ratón para invocar el menú de contexto de Matriz.

6. Select Capture para iniciar la captura del paquete. Se capturarán sólo esas estaciones que usted ha seleccionado en el buffer de captura.

NOTA:

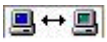
Si la dirección de nodo de red no es legible en el mapa de tráfico, usted puede usar el comando Zoom del menú del contexto (click en el botón derecho) para agrandar el mapa, o coloque el cursor sobre la dirección del objeto hasta que una reducida ventana despliega la dirección del nodo.

Si el icono Captura pernanece inactivo después de seleccionar un nodo, verifica dos veces que una sesión de captura ya no se empieza. Si una sesión de captura ya está en marcha, usted no podrá lanzar otra.

## Capturando Conversaciones sobre IP routers

1. Desde el panel de Captura, pulse el botón para abrir la caja de dialogo Define Filter.

2. Clic en el botón Profiles (Perfiles) para abrir la caja de dialogo Profiles, y haga click en Nuevo.
3. Entran en un nuevo perfil (filtro), por ejemplo, Mi Filtro de IP.
4. Clic OK.
5. Clic en el boton Done para cerrar la caja de diálogo Profile.
6. Seleccionan la pestaña Dirección
7. Seleccione IP desde el tipo de dirección de la caja.
8. Clic en el botón de elección Include.
9. Entre la primera dirección IP (por ejemplo, 192.44.81.128) en la primera Estación dominio 1.
10. Entrar la segunda dirección IP (por ejemplo, 192.55.90.133) en la primera Estación domonio 2.
11. Seleccione (ambas direcciones).



12. Clic OK.

Usted ha definido simplemente un nuevo filtro de la captura (Mi filtro IP) para capturar la conversación entre un par especificado de estaciones de IP.

Pulse el botón para empezar a capturaro usando este filtro.

NOTA:

Usando el Libro de Direcciones, usted puede asignar un nombre lógico a la dirección de IP para cada host o servidor en su red. Entonces usted puede localizar el nombre del host que usted desea usar del libro de direccines. Usted puede arrastrar los nombres a las pilas de la estación en el filtro de direcciones.

Si usted desea capturar todo el tráfico de una sola estación, entre la estación (nombre o dirección IP) en la Estación dominio 1 y arrastre cualquiera de las direcciones listadas en la estación dominio 2 .

Profile es otro nombre para la definición del filtro.

## Capturando Paquetes de un solo protocolo

Sniffer Pro tiene una habilidad única para capturar paquetes que equivalen a un protocolo en particular o tipo subalterno de protocolo.

Como un ejemplo, el procedimiento siguiente muestra cómo capturar paquetes IPX.

1. Desde la ventana Captura, pulse el botón Define Filter en la caja de dialogo.

2. Clic en el boton Profiles para abrir la caja de dialogo Profiles.
3. Clic en el botón Nuevo.
4. Entre el nuevo nombre del perfil - por ejemplo, mi filtro de IPX.
5. Clic OK.
6. Clic en el botón Done para cerrar la caja de dialogo Profiles.
7. Seleccione la pestaña Advanced.
8. Seleccione IPX de la lista de Protocolos Disponibles en la caja.
9. Clic OK.
10. Clic para empezar la captura.

NOTA:

Profile es otro nombre para la definición del filtro.

No todos los protocolos en la lista de los Protocolos Disponibles son apoyados por el Experto. Para una lista de protocolos actualmente apoyados para el Experto, vea a el Intérprete de Protocolos.

## Capturar Paquetes que corresponden a un Cierto Modelo del Datos

Sniffer Pro tiene una habilidad única para preparar un filtro para capturar paquetes que corresponden sólo a un cierto modelo del datos.

Como un ejemplo, el procedimiento siguiente ilustra cómo capturar paquetes IPX RIP.

1. Desde la ventana Captura, pulse el botón para abrir Define Filter en la caja de diálogo.

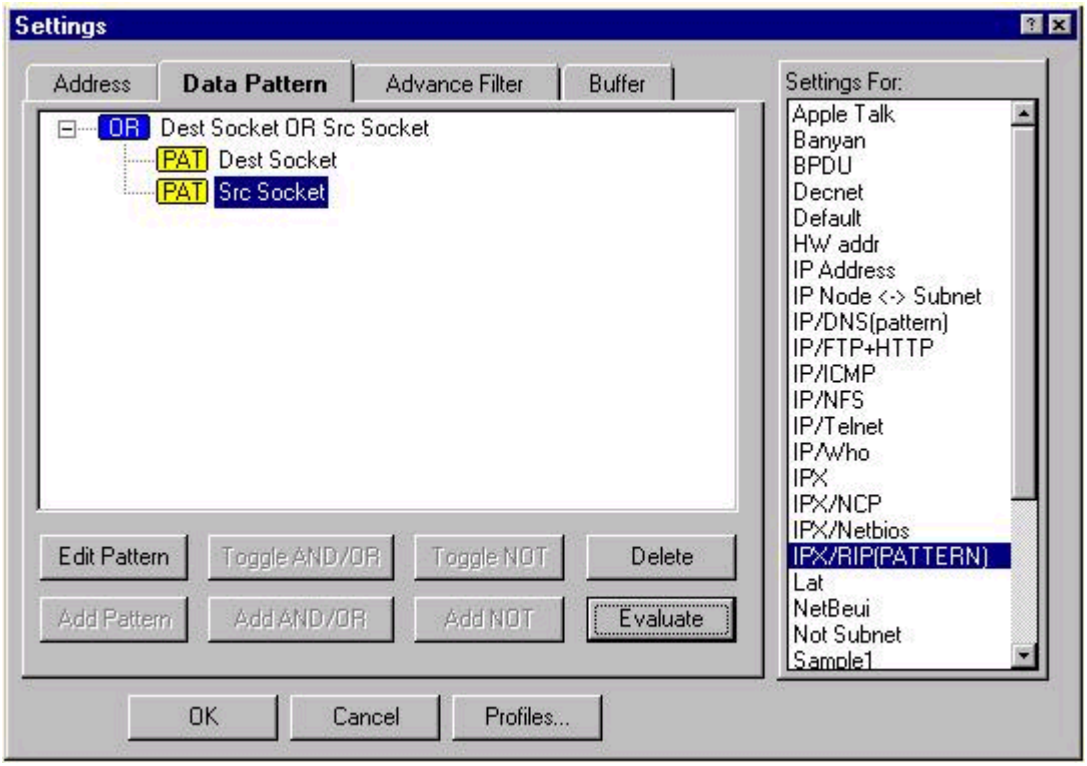
2. Clic en el boton Profiles para abrir la caja de diálogo Profile.
3. Clic en Nuevo.
4. Entran el nuevo nombre del perfil - por ejemplo, IPX/RIP(PATTERN).
5. Clic OK.
6. Clic en el botón cerrar la caja de diálogo Profile.
7. Clic en la pestaña Advanced.
8. Seleccione IPX de la lista de protocolos Disponibles en la caja.
9. Clic en la pestaña Data Patterm (Modelo de Datos). Se muestra un valor AND por defecto.
10. Clic en el botón de la Barra AND/OR para cambiar al operador OR.
11. Clic en el botón Add Patter (Agregar Modelo) para invocar la caja de dialogo con la edición de modelos.
12. Click en el botón From que despliega una caja con una lista que puede recorrer. Seleccione el Protocolo.
13. Entre 16 en el campo Offset (de Desplazamiento) (sugerencia: el campo Destination Socket es un desplazamiento de 16 bytes desde el principio del paquete IPX).
14. Entre 2 en el campo Len. Seleccione Hex (hexadecimal) desde el campo Format (Formato). Entre el número 04 hexadecimal en la columna 0 fila 1, ademas 53 en la columna 1 fila 1 (sugerencia: 0453 hexadecimal es el número del socket para IPX/RIP).
15. Entre un nombre simbólico en el campo Name - por ejemplo, Dest socket.
16. Clic OK. Un nuevo modelo del datos, Dest Socked, es creado y conectado al operador OR.
17. Clic en el nombre simbólico al lado del operador OR, en este ejemplo, Dest Socket. (Sugerencia: evite pulsar el botón del operador OR o cambiarlo a AND.)
18. Clic en el botón Add Patter para invocar otra caja de dialogo con edicion de modelos .
19. Clic en el botón From que despliega una caja con una lista que puede recorrer. Seleccione el Protocolo.
20. Entre 28 en el campo Offset (sugerencia: 28 bytes de desplazamiento desde el principio del paquete IPX son el campo Sourse Socket).
21. Entre 2 en el campo Len.
22. Seleccione Hex del campo del Format.
23. Entre el número 04 hexadecimal en la columna 0 fila 1, ademas 53 en la columna 1 fila 1. (sugerencia: 0453 hexadecimal es el número del socket para IPX/RIP).
24. Entre un nombre simbólico en el campo Name - por ejemplo, Src Socket.
25. Clic OK. Un nuevo modelo del datos, Src Socket, es creado y conectado al operador OR justo debajo del socket Dest.

26. Clic en el botón Evaluate

El resultado de la operación OR (Socket Dest OR Socket Src) se muestra después del operador OR.

27. Clic OK para guardar el filtro.

28. Clic para empezar la captura.




NOTA:

Usando el filtro de captura se requiere una CPU adicional que procesa para examinar cada paquete que corresponde al criterio. En una red con una carga de tráfico pesada, usted puede perder paquetes. Para evitar la perdida de paquetes, usted puede capturar todo el tráfico, además aplique un filtro para seleccionar los paquetes que usted quiere ver. Alternativamente usted puede usar el alto rendimiento de las targetas de red PCI .

Profile es otro nombre para la definición del filtro.

## Capturando Paquetes y haciendo Spooling a archivos en tiempo real.

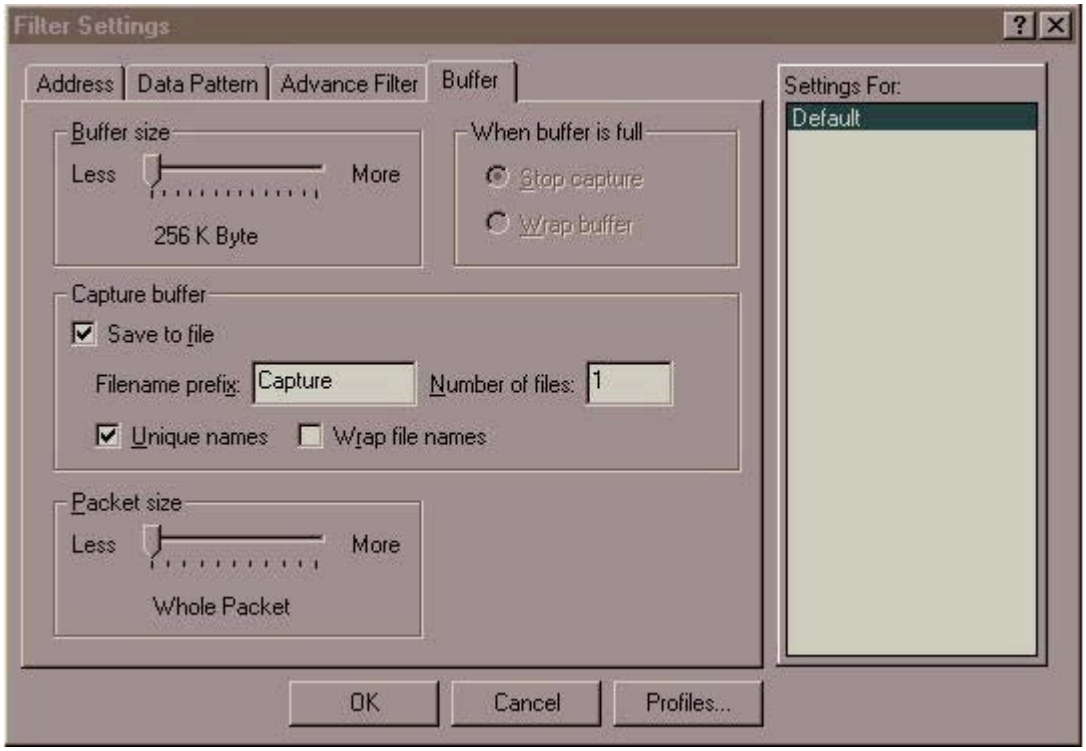
Sniffer Pro puede hacer Spooling a los paquetes capturados desde el buffer de captura a un archivo del disco en el tiempo real.
Coloque los parámetros para hacer spooling a los archivos en la pestaña Define Filter/Buffer.
Cuando el buffer está lleno, Sniffer Pro escribe el contenifo en un archivo. El tamaño de cada archivo se define de la misma forma que se define el tamaño del buffer de captura. Por ejemplo, si usted selecciona un tamaño de buffer de 4 MB , entonces cada archivo creado será de 4 MB. (El tamaño del último archivo puede ser más pequeño que 4 MB.)

Usted puede seleccionar la única opción de nombre de archivo para garantizar que el nombre de archivo creado por la captura de paquetes es único dentro de un directorio. Ésta es una opción útil cuando usted usa spoolling en la captura del paquete junto con el desencadenande de captura en modo repetitivo. Varias secuencias de capturas de paquetes pueden guardarse preferiblemente con nombre únicos de archivo separados en lugar de tener cada conjunto de archivos sobreescribiendolos.

Seleccionando en el wrap la opción file, la captura continuará haciendo spool y sobreescribiendo el primer archivo después de escribir el último archivo. Por otra parte, la captura se detendrá cuando alcanza el extremo final del archivo.

Definir la captura del paquete a archivar:

1. Clic en el botón panel de Captura de Paquete, despues haga click en la pestaña Buffer en la cja de dialogo Definir filtro.




2. Guarde para Archivar la caja de chequeo, y entre en un prefijo del nombre del archivo. El prefijo del nombre del archivo le ayudará a identificar qué archivos se escribieron a su disco duro.

3. Especifique el número de archivos que usted quiere escribir. El número máximo de archivos permitido es 99,999.

4. Opcionalmente, especificar otros parámetros del filtro.

5. Clic OK.

Para empezar la captura y ver los resultados, siga estos pasos:

1. Para empezar la captura, pulse el botón Start Capture. Si usted quiere ver el archivo al que le está haiendo spooling en una barra de progreso, pulse la pestaña Detail (Detalle) del panel de Captura. Un resumen del estado de la captura se desplegara para mostrarle el archivo en el cual actualmente están los paquetes capturados a los que se les ha hecho spooling, y si los archivos se encapsulan.


2. Para detener la captura y ver los resultados, pulse el botón stop and Display (Parar el despliegue) Seleccione el archivo capturado que usted quiere abrir.

NOTA:

Usted puede ordenar la lista por columna Modificada en el archivo abierto de la caja de diálogo para ver qué archivo es el más recientemente escrito.

3. Seleccione un archivo, y pulse el botón Open. Se despliegan el contenido del archivo en la ventana Esperta, y está disponible de cualquiera de las pestañas de Despliegue de Paquete.

NOTA:

Al hacer spooling al disco, el rendimiento de la captura de paquete depende del throughput del disco duro, así como de la carga de la red y la velocidad de CPU.

## Capturar y Filtrar Paquetes de error.

Usando los drivers escritos y apoyados por Network Associates, Sniffer Pro es capaz de capturar un rango de paquetes de error, por ejemplo CRC, runt, fragment, oversize, y jabber en una red Ethernet. Usted también puede capturar y desplegar filtros para seleccionar uno o más tipos de paquetes de error. El tipo de paquetes de error que usted puede seleccionar depende de su tipo de red. Por ejemplo, en una red Token Ring, usted puede seleccionar errores CRC y errores FC. En una red WAN\Synchronous, usted puede seleccionar los errores CRC, errores de aborto, y errores del sobrecarga, entre otros.

Contactar el soporte tecnico de Network Associates para obtener la última lista de tarjetas NIC soportadas por sniffer Pro mejora los drivers.

Para definir un filtro de paquete de error:

1. Clic el botón del panel de Captura

2. Clic en el boton Profiles para crear un nuevo filtro.
3. En la caja de dialogo Capture Profiles, pulse el botón Nuevo y entre en un nuevo nombre del perfil, por ejemplo, Errores de Ethernet.
4. Clic Done.
5. Clic en la pestaña Advanced.
6. Asuma el l tipo del paquete como Normal y cualquier otro tipo de paquete de error que usted quiere excluir. Deje el checkmarks en los que usted quiere capturar.
7. Clic OK.

## Capturar y Filtrar Tipos de Marco en una WAN espicifica

Al usar un adaptador de WAN\Synchronous (el LM2000 o el adaptador HSSI), Sniffer Pro puede capturar y puede filtrar una gran variedad de tipos de marco WAN.

Para definir un filtro para capturar los tipos del marco WAN específicos:

1. Clic el botón del panel de Captura

2. Clic en el botón Profails para crear un nuevo filtro.
3. En la caja de dialogo Capture Profiles, pulse el botón Nuevo y entre en un nuevo nombre del perfil, por ejemplo, Errores de Ethernet.
4. Clic Done.
5. Cuando usted está capturando desde un adaptador WAN, el ambiente del filtro en la caja de dialogo contiene una pesña WAN (SDLC, X.25, Frame Relay o HDLC) que corresponde al protocolo de encapsulación actualmente seleccionado en las opciones de la caja de diálogo . Pulse el botón en la pestaña WAN.

6. Aparece una lista de los tipos de marco que corresponden al protocolo seleccionado. Por ejemplo, si Frame Relay es el protocolo del encapsulación actualmente seleccionado, usted puede filtrarse marcos con el FECN bit, BECN bit, o DE bit . Seleccione el tipo de marco que usted quiere incluir o excluir verificando sus cajas.

7. Clic OK.

## DESPLIEGUE Y GUARDE LOS PAQUETES DE LA CAPTURA

### Desplegar Los Paquetes Capturados

De la ventana Capture, pulse el botón (Stop and Display)

o el botón (Despliegue) para plantear la ventana de Despliegue de Paquete.

NOTA:

Mientras la captura del paquete está en marcha,

El botón solo está activo.

### Guardar los paquetes capturados a un archivo

Para guardar los paquetes capturados a un archivo:

1. Desde la ventana Capture, pulse el botón (Stop and Display)

o el botón (Despliegue) para abrir la ventana de Despliegue de Paquete.

2. Del menú Archivo seleccione Guardar como. La caja de dialogo Guardar como se abre.

3. Entran un nombre del archivo para su archivo capturado.

4. Clic OK.

NOTA:

Usted también puede guardar automáticamente los archivos de la captura usando la opción Guardar en la pestaña Buffer de la caja de dialogo Define Filter. Vea la pestaña Buffer de Define Filter para mas información.

## Guardar los paquetes capturados en formato comprimido.

Sólo pueden guardar archivos en formato comprimido desde la ventana de Packet Display. (Cuando a los paquetes se les ha hecho spooling automaticamente a un archivo, ellos no se guardan en un formato de archivo comprimido.)

Para guardar paquetes en formato comprimido:

1. De la ventana Capture, pulse el botón (Stop and Display)

o el botón (Despliegue) para abrir la ventana de Despliegue de Paquete.

2. Del menú Archivo, seleccione Guardar Como. La caja de dialogo Guardar Como se abre.

3. Entre el nombre del archivo para su archivo de captura. Entre la extensión del archivo como .CAZ, al formato comprimido.

4. Clic OK.

## Seleccionar Paquetes para verlos por separado.

Para seleccionar paquetes para desplegarlos en una ventana Packet Display separada:

1. Para cada paquete que usted quiere seleccionar, pulse en la caja el botón que está delante de su número del índice.

2. Clic el botón derecho del ratón para abrir el menú de contexto.

3. Seleccione Save Select.

Una nueva ventana de Despliegue de Paquete se muestra con sólo los paquetes seleccionados.

Usted puede guardar los paquetes seleccionados para revisarlos más tarde usando File/Save As.

## Desplegar paquetes desde un archivo de captura.

1. Del menú Archivo, seleccione Open. El Archivo de la caja del diálogo se abre.

2. Entre el nombre del archivo para su archivo de captura. Especifique una carpeta o localización, si es necesario. Usted puede abrir archivos guardados con Sniffer Pro, ademas de muchos tipos de archivos guardados con Network associate´s (anteriormente Network General´s) el Analizador de Red Expert Sniffer y el producto LANalyzer de Novell.

3. Clic OK. La ventana Packert Display se abre desplegando los paquetes en el archivo.

## DEFINA UNA SEÑAL DE CAPTURA

## Configurar señales de Arranque y Culminación para la Captura del Paquete

Esta función suministra un medio para empezar y detener las capturas del paquete basado en un evento de señales.

Al definir un evento de la señal, usted puede incluir:

- Fecha y hora
- Carga de tráfico o alarmas de umbral de error
- Eventos de filtros

Usted puede seleccionar cualquiera o todos éstos eventos para empezar o detener una captura. Si cualquiera de stos eventos seleccionados ocurre, la señal se activará.

Active las Opciones

Usted puede especificar el filtro de captura para usar cuando el evento de la señal ocurre. Usted puede seleccionar actualmente que filtro definir. (También vea: Vision general para definir un filtro, Especificando un Filtro de Captura para una señal)

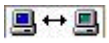
La Parada gatillo retraso opción determina si la captura del paquete detiene inmediatamente cuando el gatillo de la parada se descubre, o después de que un número especificado de paquetes se captura. Poniendo un retraso, usted puede examinar los paquetes que siguen el gatillo de la parada.

La función de la señal también puede reiniciarse automáticamente. Cuando el reinicio automatico es usado junto con el spooll de la captura para archivar la función, Sniffer Pro puede capturar multiples instancias del tráfico de red que equivale a la señal sin intervención manual.

Los Filtros de evento

Si usted quiere usar un filtro de evento en una definición de una señal, este debe definirse primero. Definir un filtro de evento es similar a definir una captura o un filtro del despliegue. A un filtro de evento siempre se da un nombre del perfil. (También vea: Visión general de la definicion de un filtro)

Por ejemplo, si usted quiere empezar una captura activada por una dirección de IP particular, usted puede lograr esto definiendo un filtro de una dirección IP con su dirección IP conocida en el campo Estación 1 y cualquiera en el campo Estación 2 , con el Dir set to. Use este filtro como el filtro de evento para la señal de salida.



Para colocar una señal de captura de paquete:

1. Define cómo usted quiere la señal para controlar la captura del paquete. - use la señal de salida, detenga la señal, el retraso después de la señal, repita (la vuelta) el modo en cualquier combinación.

2. Decida que evento(s) - el date/time, umbral de alarma, o filtro de evento - para usar como la señal(s).

3. Si usted usará un nuevo filtro de evento, defina el perfil de filtro de evento que usa la caja de dialogo Define Filter.

4. Invoque el panel de señal, y establesca la señal según su definición. Despues aplique la señal.

NOTA:

Experimente con la función de señal para ponerse hábil antes de aplicarlo con el localizador en mundo real.

Para determinar si una señal se habilita o no, vaya al menú Capture. Si la opción Cancel Trigger es visible, entonces la señal se habilita. Si la opción Tigger setup es visible, entonces la señal no se habilita.

Para desactivar una señal, seleccione la señal Capture\Cancel .

También vea: Trigger Example

## PERSONALICE Y USE EL DESPLIEGUE DEL PAQUETE

### Desplegar paquetes

Packet Display despliega los paquetes en trescuadros separados:Resumen, Detalle, y Hex. Cada cuadro puede ser cambiado de tamaño pulsando el botón y arrastrando la barra del separador entre los cuadros. Cada hoja de vidrio contiene scroll bars que lo permitieron usan el ratón para manipular la posición viendo en el cuadro.

Usted también puede usar las teclas de control para mantener el enfoque del cuadro en una forma similar.

NOTA:

Para aumentar al máximo la eficacia examinando los paquetes detalladamente, siga estas sugerencias:

Ajuste el tamaño de Despliegue de Paquete, y el cuadro individual para aumentar al máximo el área viendo lo que le interesa en particular.

Selecione el paquete de arranque de interés haciendo click sobre el en el cuadro de resumen.

Click en el cuadro Detalle para obtener el enfoque. El movimiento del cursor y las teclas de control PgUp / PgDn se refieren ahora al cuadro Detalle.

Use la tecla F7 para dirigirse al paquete anterior. Use la tecla F8 para dirigirse al próximo paquete.

Si usted quiere mover el área viendo en el cuadro Detalle, use el cursor y las teclas de controlPgUp / PgDn.

## Fijar un Campo Seleccionado en la Ventana Detalle

Pulsando el botón en un campo seleccionado o en la línea del resumen de protocolos para resaltarlo, usted ha fijado ese campo a ser desplegado en el cuadro detalle. Sniffer Pro recuerda el campo resaltado en cada paquete, y siempre pondrá ese campo en las ventanas del cuadro Detalle.

Fijando un campo en el cuadro Detalle le permite navegar entre varios paquetes sin tener que reposicionar el cuadro Detalle usando scroll bar.

## Usar el Resumen de Protocolos en linea en la Ventana Detalle

Por defecto, Sniffer Pro amplia detalles del protocolo de la capa en el cuadro Detalle. Usted puede guardar viendo el espacio pulsando el botón del signo menos (-) delante de la línea de protocolo de subacapa. Los campos detalle de ese protocolo de capa seran contraidos dentro de una unica linea de despliegue solamente con un resumen de la información. Para extender el despliegue del protocolo de nuevo, pulse el botón del signo mas (+) .

La expanción o contracción de cada campo de subprotocolo es "memorizada" por el Packet Display. El mismo estado para ese subprotocolo se mantendrá, cuando usted ve el próximo paquete o el paquete anterior. Por ejemplo, suponga usted alquila los servicios del protocolo de capa RIP en un decodificador IPX . viendo subsecuentemente otros paquetes IPX RIP mostrará el protocolo RIP desplegado en una línea a modo de resumen.

La longitud de un paquete se mostrará en la columna Len del cuadro Resumen, la cual será de cuatro bytes más de lo que se indica en el cuadro Detalle y el cuadro Hex. El cuadro Detalle y el cuadro Hex no incluyen cuatro-bytes CRC.

El modo valor por defecto del cuadro Detalle puede personalizarse. Para cambiar la contraccion inicial o vista extendida de cada subprotocolo individual, siga estos pasos:

1. Desde el menú de Despliegue, seleccione el Display Setup. Una caja de dialogo con Opciones de propiedades aparece.

2. Seleccione la pestaña Protocol Expand.

3. Clic en la caja de chequeo para cambiar esos tipos de protocolos que se ven en el estado inicial. Una marca del chequeo indica la vista extendida;dechequeado indica la vista contraída.

4. Usted también puede pulsar el botón Expand All para poner todas las capas protocolares a la vista totalmente extendida. Pulsando el botón Callapse All pondrán todas las capas protocolares a la vista contraída.

5. Cuando usted está satisfecho con la selección, pulse el botón OK.

## Establecer un resaltador de protocolo

Los paquetes en el cuadro Resumen pueden ser reslatados, basandose en su tipo de protocolo. Este rasgo le ayuda visualmente a identificar paquetes de un protocolo particular.

Para establecer un resaltador de protocolo:

1. Del menú Display, seleccione Display setup.

2. Seleccione la pestaña Protocol Color.

3. Seleccione el tipo de protocolo que usted quiere modificar.

4. Seleccione el color del Texto que usted quiere. El color del protocolo es cambiado para reflejar su selección.

5. Cuando usted está satisfecho con la selección , pulse el botón OK.

# REALICE ANÁLISIS POST EN EL DESPLIEGUE DEL PAQUETE

## Mostrar el Mapa de Tráfico

El mapa de tráfico es una herramienta poderosa que le da una vista superficial de los modelos de tráfico de red capturados en el buffer del paquete. Da una presentación gráfica completa del modelo de tráfico entre los nodos de la red, así como el tipo de protocolo usado para las comunicaciones.
Para ver el mapa de tráfico del Despliegue del Paquete:

1. Seleccione la pestaña Matriz en el fondo de la ventana de Despliegue de Paquete. Si usted no ve la pestaña Matriz, asegurese que la opción de la pestaña Show Post Analysis en el menú del Despliegue está habilitada.

2. Clic en el botón de mapa de tráfico. Un mapa de tráfico muestra una conversación y el tipo protocolo es desplegado.

Para ver el tráfico a una capa diferente:

1. Abra la lista desplegable en la esquina izquierda superior del mapa de tráfico.

2. Seleccione la capa  a que usted quiere ver el tráfico (por ejemplo, PVC, IP o IPX). Un mapa de trafico se mostrando una conversación y el tipo de protocolo seleccionado es desplegado.

## Usar un Filtro Visual en el Mapa de Tráfico

El mapa de tráfico puede usarse para definir un filtro automáticamente. Usted puede seleccionar las estaciones y los protocolos particulares que serán desplegados en el mapa de tráfico y Sniffer Pro  configurará un filtro automáticamente para relacionar sus selecciones.

Para usar el Mapa de Tráfico para definir un filtro:

1. Seleccione la pestaña Matriz en el fondo de la ventana de Despliegue de Paquete. Si usted no ve la pestaña Matriz, asegurese de que la opción de la pestaña Show Post Analysis en el menú del Despliegue está habilitada.

2. Al minimizar la ventana , seleccione la colección de protocolos. En la columna izquierda, seleccione uno o más subprotocolos para desplegar.

3. Destacar cualquier nodo(s) de la red que usted quiere filtrar. Para seleccionar más de un nodo, sostenga la tecla Ctrl  presionada mientras usted selecciona los nodos adicionales.

4. Clic. Esto plantea una nueva ventana de Despliegue de Paquete. La nueva ventana de Despliegue de Paquete ya se filtra, basado en el nodo de la red y en las selecciones del protocolo que usted hizo.

## Usar el Mapa de la Matriz para Identificar Otro Tipo de Protocolos

La capacidad del mapa de tráfico de crear un filtro visual proporciona una manera ideal de investigar Otros tipos de protocolos en el buffer de captura. Otros son protocolos que no entran en las categorías de protocolos predefinidos por Sniffer Pro.

Para definir un filtro para seleccionar Otros paquetes del protocolo para desplegar en la ventana de Despliegue de Paquete:

1. Selecciona la pestaña Matriz en el fondo de la ventana de Despliegue de Paquete.

2. Deschequee todos los protocolos listados en el mapa de tráfico excepto la caja  Otros

3. Clic. Esto plantea una nueva ventana de Despliegue de Paquete. La nueva ventana de Despliegue de Paquete ya se filtra, basado en los Otros protocolos seleccionados.

## Mostrar el Top-N de Pares en  Conversación

La barra Matriz revela en el top-N el par de nodos en conversación más ocupados en el buffer de captura de paquete. Usted puede ver en el top-N las conversaciones de varias capas de la red.
Para ver en el top-N la conversación de pares IP:

1. Selecciona la pestaña Matriz en el fondo de la ventana de Despliegue de Paquete. Si usted no ve la pestaña Matriz, asegurese de que la opcion de la pestaña Show  Post Analysis en el menú de Despliegue está habilitada.

2. Clic en el botón diagrama de barras.Sniffer Pro despliega un diagrama de barras que muestra el Top-N de pares en conversación.

3. Abra la lista desplegable  en la esquina izquierda superior del diagrama de barra.

4. Seleccione IP . El mapa de tráfico mostrará ahora en el top-N los pares IP en conversación.

## Identificación del protocolo de aplicación TCP/IP Usado por Cada Host

La tabla Host en linea proporciona un resumen rápido del  total de bytes y paquetes transmitido entre los pares de nodos de la capa MAC capturados en el buffer del paquete. Seleccionando MAC, IP, o  IPX, usted puede ver un resumen de tráfico instantáneamente en cada capa de la red. La vista extendida de la tabla revela cada tipo de protocolo usado por el nodo y sus cargas de tráfico asociadas.
Para identificar el protocolo de aplicación TCP/IP usado:

1. Seleccione la pestaña Host Table al fondo de la ventana de Despliegue de Paquete. Si usted no ve la pestaña Host Table, asegurese de que la opción de la pestaña Show  Post Analysis en el menú del Despliegue está habilitada.

2. Clic el botón Outline. Una tabla de contorno se despliega.

3. Abra la lista desplegable en la esquina izquierda superior de la tabla de contorno y seleccione IP

4. Clic en siguientel símbolo de la columna de Dirección para extender o colapsar el despliegue.

## Mostrar la distribución del protocolo IPX

El Resumen de Protocolos proporciona un análisis rápido de las estadísticas de la distribución de protocolos coleccionada en el buffer de captura de paquete. Usted puede ver la distribución de los protocolos en ls capas mas bajas (por ejemplo, MAC o PVC), o selectivamente ve sólo la distribución de los protocolos IP o IPX.
Para ver la distribución del protocolo IPX

1. Seleccione la pestña Protocol Dist en el fondo de la ventana de Despliegue de Paquete. Si usted no ve la pestaña Protocol Dist, asegurese de que la opción de la pestaña Show Post Analysislisis en el menú del Despliegue está habilitada.

2. Clic el botón de diagrama de pastel. Un mapa del pastel que muestra (%) la distribución de los protocolos de la capa MAC se despliega.

3. Abra la lista desplegable en la esquina izquierda superior del mapa de la barra.

4. Seleccione IPX . La distribución de los protocolos muestra ahora la carga de trasporte IPX de la capa.

## DEFINA UN FILTRO

### Defina la apreciación global del filtro

Todos los filtros son definidos usando la caja de dialogo Filters Settings. Usted puede seleccionar Define Filter desde Monitor, Capture, o menú de Despliegue,
o pulsar el botón Define Filter en el icono del panel de captura, o en la Tabla Hots o en la matris de despliegue.

El diálogo de Filter Setting tiene las siguientes pestañas:

- Use la etiqueta Resumen para repasar las escenas actuales en la caja de dialogo Filter Setting.
- Use la pestaña de Dirección para especificar los diez pares de dirección para filtrar.
- Use la etiqueta de Modelo de Datos para especificar una expresión Booleana de un modelo de datos para filtrar.
- Use la etiqueta Avanzada para especificar uno o más protocolos de la red o uno o más tipos de error para filtrar.
- Use la pestaña buffer para especificar el tamaño del buffer de captura y definir qué hacer cuando el buffer está lleno.

- Para los adaptadores WAN, use SDLC, X.25, Frame Relay , o HDLC para especificar varios paquetes WAN para filtrar. La pestaña exacta disponible dependerá del ambiente de la opción de encapsulación en las opciones de la caja de diálogo.

También vea:

Capturando Todos los Paquetes de la Red, las Conversaciones Capturadoras sobre los routers IP, Capturando paquetes de un unico Protocolo, Capturando paquetes que corresponden a un Modelo del Datos, Capturando y Filtrándo paquetes de error Ethernet, Usando un Filtro de Despliegue, Definiendo un filtro de Captura, Capturando y Filtrándo Tipos del Marco WAN específicos

## Copiar un Perfil Existente

Sniffer Pro viene con un juego predefinido de muestras de filtros que usted puede copiar al crear las nuevas definiciones del filtro. Además, usted puede copiar un filtro existente que usted ha definido, y usted puede compartir definiciones del filtro creadas en otros sistemas.

Mover Perfiles de Filtro de Un Sistema a Otro.

Sniffer Pro mantiene una muestra de filtro ubicada en el archivo NXSAMPLE.CSF, y el filtro actual ubicado aparte en el archivo SNIFFER.CSF.

Para usar filtros de la muestra creados por otros:

1. Guarde NXSAMPLE.CSF bajo otro nombre

2. Haga una copia del filtro actual en SNIFFER.CSF y renombrela NXSAMPLE.CSF.

3. Renombre el archivo de la muestra que otros crearon como SNIFFER.CSF.

Para copiar un filtro desde un perfil del filtro existente:

1. Traer la caja dialogo Define Filter. Usted puede hacer esto haciendo click en la ventana Capture , o desde la barra del menú pulsando el botón Monitor/Define Filter, Capture/Define Filter, o Display/Define Filter

2. Clic en el botón Profile para plantear la caja de diálogo Profile.

3. Clic en el botón Nuevo para plantear el dialogo Nuevo Perfil de Captura,

4. Entrar un nuevo nombre del perfil, por ejemplo, Mi Filtro IPX.

5. Clic el botón apropiado que depende de si usted quiere copiar del Perfil Existente o del Perfil de la Muestra.

6. Clic para abrir la lista desplegable. escoja un filtro para copiar.

7. Clic OK.

8. Clic en Done para volver a la caja de dialogo Define Filter.

9. Haga cualquier cambio que usted quiera personalizando filtro para su propósito particular.

10. Clic OK para terminar.

## APLIQUE UN FILTRO

### Especificar un Filtro del Despliegue de protocolos

Un filtro de despliegue le permite filtrarse afuera los paquetes no deseados cuando usted despliega el contenido del buffer de captura. El perfil definido para un filtro de captura también puede usarse para filtrar afuera los paquetes del Despliegue de Paquete. El procedimiento para definir un filtro de despliegue es idéntico al procedimiento para un filtro de captura.

Crear o cambiar un filtro de despliegue:

1. En el menú Despliegue, seleccione Define Filter.

2. Seguir el procedimiento Define Filter. Los enlases a temas que describen cómo crear los varios filtros de captura son aplicables al definir un filtro de despliegue.

3. Del menú Despliegue, escoja el Select Filter para aplicar su nuevo filtro al despliegue actual.

### Aplicar un Filtro de Despliegue

Para aplicar un filtro de despliegue:

1. Del menú Despliegue, escoja el Selec Filter.

2. Seleccionan un filtro previamente definido en la lista.

3. Clic OK.

Una nueva ventana de Despliegue de Paquete se despliega con los paquetes que corresponden al criterio del filtro que usted ha especificado. Si ningún paquete ecorresponde al criterio, un mensaje de indicación se despliega.

Usted puede ver ahora o puede guardar el contenido en el Packet Display.

## USE AL EXPERTO

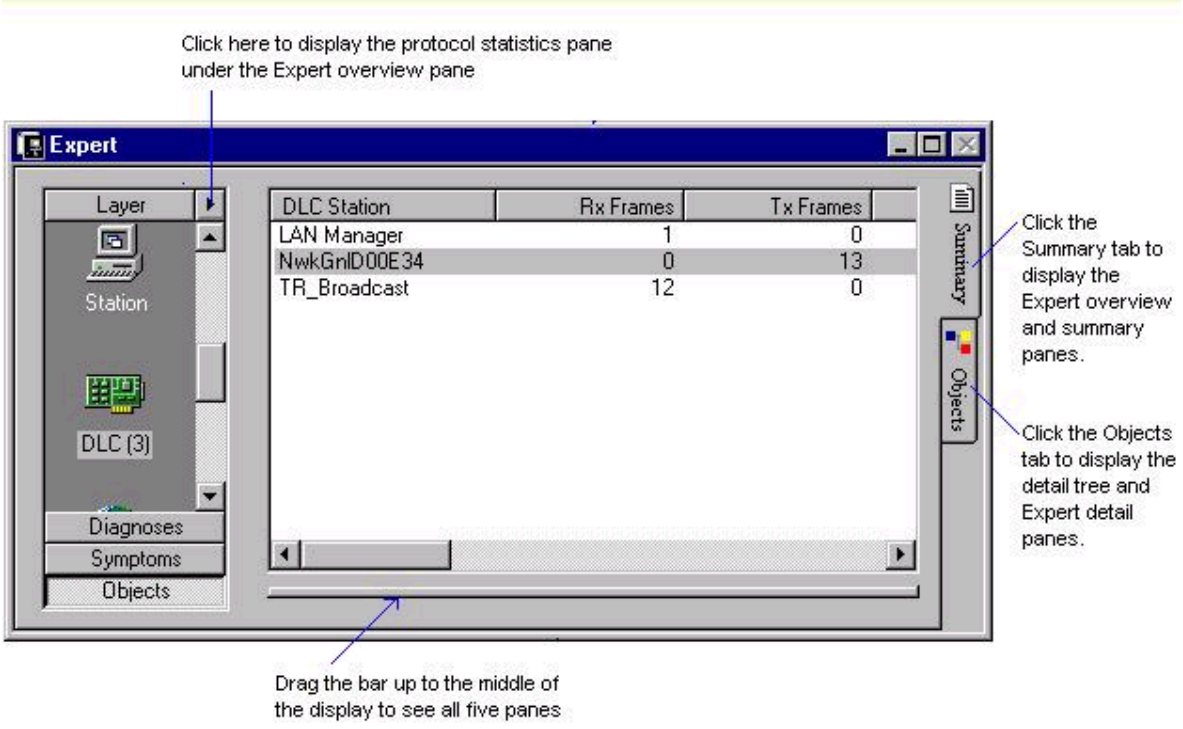
### Colocar el Despliegue Experto

La pewstaña Expert y la ventana esperta en tiempo real desplegada durante la captura puede mostrar los resultados del análisis Experto en cinco cuadros,Expert overview, Expert summary, protocol statistics, detail

tree, y Expert detail . Estos cuadros funcionan juntos para que usted pueda seleccionar la información del análisis Experto en todos los niveles en forma detallada.
Usted puede cambiar el despliegue para satisfacer sus necesidades . Usted puede desplegar:

- Todas los cinco cuadros al mismo tiempo.
- La apreciación global de los cuadros Expert overview y Expert summary(con o sin el cuadrode estadisticas de protocolo). Ésta es la vista predefinida.
- Los cuadros detail tree y Expert detail

La figura debajo de las muestras el despliegue Experto predefinido y demuestra cómo cambiar las vistas.






## Codificar el umbral de alarma experto

IMPORTANTE: Se han calculado cuidadosamente los umbrales predefinidos proporcionados con el Experto para garantizar el sintoma con exactitud y proporcionar el diagnostico. Antes de cambiar cualquiera de los umbrales, asegurese de que usted entiende su red.

Para modificar un umbral de alarma Experto:

1. Seleccione la pestaña Alarms desde las opciones de menú Tools/Expert .

2. Seleccione el signo mas (+) al lado de una capa experta para desplegar la lista de alarmas quecontiene. (Usted también puede hacer click en el 1 en la primera columna de la tabla para expandir todas las capas y desplegar todas las alarmas.)

Todas las alarmas que tienen un umbral despliegan un valor en la columna de la tabla.

3. Extienda la alarma en la columna de Descripción haciendo doble click o pulsando el botón con el signo + a la derecha de la alarma.

4. Cambie el ambiente del umbral en el valor de la columna , entonses haga click en Apply.

Umbrales de Alarma expertos

## Asignar niveles de seguridad a alarmas expertas

Para asignar un nivel de seguridad a una alarma Experta:

1. Seleccione la pestaña Alarms de las opciones del menú Tools/Expert

2. Seleccione el signo más (+) al lado de una capa Experta para desplegar la lista de alarmas que contiene. (Usted también puede hacer click en 1 en la primera columna de la tabla para extender todas las capas y desplegar todas las alarmas.)

el valor en la columna al lado de la descripción de la alarma muestra el estado actual de la alarma.

3. Extienda la alarma en la columna de Descripción haciendo doble-click en el botón alarma o haciendo click en el signo mas (+) al lado derecho de la alarma.

4. Clic en la celda de Valor para la Seguridad y seleccione el nivel de seguridad de la lista desplegable. Usted puede escoger Critical/Diagnosis, Major, Minor, Warning, Informational, or Disabled.

5. Clic Apply.

Una alarma no se graba en Sniffer Pro a menos que la Alarma de ambiente en la vitacora se ponga a SÍ. La alarma debe grabarse en la vitacora de la alarma para que una acción de notificación tenga lugar. (Usted puede preparar las acciones de notificación en el menú Tools / Option.)

## Desplegar archivos de explicación experta

El Experto mantiene las explicaciones detalladas de cada síntoma y el diagnóstico generado.
Para desplegar una explicación detallada de un síntoma o diagnóstico:

1. Selecciona el síntoma o diagnóstico en el cuadro Expert summary. El cuadro Expert detail muestra los detalles sobre el síntoma / el diagnóstico.

2. Clic en el signo de interrogación (?) a la derecha de la descripción del síntoma / diagnóstico en el cuadro Expert detail. (Usted tiene que recorrer a la derecha el cuadro para ver el ?.)

El Experto también proporciona descripciones de los campos en los cuadros Expert overview, Expert summary, protocol statistics, detail tree, y Expert detail . Pulse el botón dentro del cuadro en que usted necesita información y presione F1.

La pestaña Expert

## Configurando el experto

Para configurar las opciones Expertas, seleccione Expert Options del menú de Herramientas para abrir la caja de dialogo con las Propiedades Expertas.

La caja de dialogo de las propiedades Expertas contiene cuatro pestañas: Objects, Alarms, Subnet Masks, y RIP Options.

## USE LAS ALARMAS

## Definiendo una Alarma Audible

Definir una alarma audible:

1. Seleccione la pestaña Alarm del menú Tools/Options.

2. Selecione Once or Repeat de la lista de Sonidos.

3. El sonido predefinido es un beep del portavoz de un PC. Si usted prefiere otro sonido para su alarma, reemplace el pitido normal por un archivo de sonido .WAV. Entre el camino y nombre del archivo legítimo (.WAV), o seleccione el botón browse para hojear el archivo.

4. Clic OK.

NOTA:

Para usar un archivo .WAV para una alarma audible, su sistema debe tener una tarjeta de sonido y un altavoz

## Definición de la notificación de la alrma SMTP Mail

Para configurar Sniffer Pro para enviar la notificación del email cuando una alarma ocurre:

1. Selecciona la etiqueta de la Alarma del menú de Tools/Options.

2. Clic en el botón Define Actions para abrir la caja de dialogo Alarm Action.

3. Clic en el botón Add, entre en un nuevo nombre de Acción de Alarma y seleccione los SMTP en el botón de radio. Alternativamente, usted puede copiar las escenas de una acción predefinida. Pulse el botón OK. El asistente de información de correo se abre.

4. Entre el nombre del servidor, su número de puerto, y el nombre del destinatario del correo y la dirección de email en los campos proporcionados. Pulse el botón siguiente para continuar.

5. Establesca el horario de notificación de alarma. Siempre seleccione si usted quiere habilitar la acción de la alarma en todo momento, o seleccionar el Horario si usted quiere habilitar la acción de la alarma durante ciertos periodo de tiempo. Entre en el periodo de tiempo y seleccione qué días usted quiere la acción habilitada. Si esta en apuros encienda el botón de la acción de la alarma durante ese día. Usted puede pulsar el botón Todos los días, dias de la semana, o fin de semana para que se encienda esos días automáticamente. Pulse el botón siguiente par acontinuar

6. Evalue la Nueva Configuración para enviar un mensaje de email de prueba al destinatario del correo. Pulse el botón Finalizar.

7. Clic OK para completar la definición de acción de alarma.

NOTA:

Después de que usted completa la definición de acción de alarma, usted debe asignar un nivel de seguridad a la acción de la alarma. Una acción de notificación sólo ocurrirá si usted asigna un nivel de seguridad de alarma.

## Definir la notificación de la alarma Alpha Pager

Para configurar Sniffer Pro para enviar una notificación del pager cuando una alarma ocurre:

1. Selecciona la pestaña Alarm del menú Tools/Options.

2. Clic el el boton Define Actions para invocar la caja de dialogo Alarm Action

3. Clic en el boton Add, entre en un nuevo nombre de Acción de Alarma, y seleccione los Pager en el boton de radio. Alternativamente, usted puede copiar la configuracion de una acción existente. Pulse el botón OK. El asistante de información de pager se abre.

4. Entre el número del teléfono, una contraseña opcional, y su numero PIN para el pager en los campos proporcionados. click en siguiente para continuar.

5. Entre el puerto de comunicación y la información de configuración para su módem. Pulse el botón siguiente para continuar.

6. Establesca el horario de notificación de alarma. Siempre seleccione si usted quiere habilitar la acción de la alarma en todo momento, o seleccione el Horario si usted quiere habilitar la acción de la alarma durante ciertos periodo de tiempo. Entre el periodo de tiempo y seleccione qué días usted quiere la acción habilitada. Si esta en apuros encienda el botón de la acción de la alarma durante ese día. Usted puede pulsar el botón Todos los días, Días de la semana, o fin de semana para que se encienda esos días automáticamente. Pulse el botón siguiente para continuar.

7. Evalue las nuevas configuraciones para enviar un mensaje de la prueba al pager. Pulse el botón Finalizar.

8. Clic OK para completar la definición de acción de alarma.

NOTA:

Dos o más acciones de alarma pager o una combinación de beeper y alarmas del pager no pueden llamarse al mismo tiempo para especificar una seguridad a menos que se usan los módems diferentes.

Después de que usted complete la definición de acción de alarma, usted debe asignar la acción de alarma a un nivel de rigor. Una acción de notificación sólo ocurrirá si usted lo asigna a un nivel de rigor de alarma.

## Definiendo beeper (localizador) para la notificación de alarma.

Para configurar el Sniffer pro para enviar la notificación a un beeper (localizador) cuando una alarma ocurre:

1. Selecciona la etiqueta Alarma del menú de Tools/Options.

2. Click en el botón Define Actions para abrir la caja de diálogo Acción de alarma.

3. Click en el botón Add, para entrar un nuevo nombre de Acción de Alarma y seleccione el botón Beeper radio. Alternativamente, usted puede copiar el ambiente de una acción existente. Pulse el botón OK. La información del localizador para ayudar al usuario aparece.

4. Entre el número del teléfono, el periodo de retraso para su localizador particular, el mensaje numérico, la cadena final para el mensaje, y el valor de retraso para colgar en los campos proporcionados. El mensaje numérico normalmente es el número del teléfono del módem, pero también puede ser el número del código en un esquema mensaje-codificado. Pulse el botón Net para continuar.

5. Entrar a la información de la configuración del puerto de comunicaciones para su módem. Pulse el botón Next para continuar.

6. Establezca el cronograma de notificación de alarma. Siempre seleccione on si usted quiere habilitar la acción de alarma en todo momento, o seleccione Schedule si usted quiere habilitar la acción de la alarma durante ciertos periodo de tiempo. Entre el periodo de tiempo y seleccione qué días usted quiere la acción habilitada. Presione el botón encendido para la acción de la alarma durante ese día. Usted puede pulsar el botón todos los día, Días de la semana, o fin de semana para encender esos días automáticamente. Pulse el next para continuar.

7. Pruebe el nuevo ambiente para enviar un mensaje de la prueba al beeper. Pulse el botón Finish.

8. click en OK para completar la definición de acción de alarma.

NOTA:

Dos o más beeper(localizadores) de acciones de alarma o una combinación de beeper y buscadores de alarmas no pueden llamarse al mismo tiempo para una gravedad específica a menos que se usen módems diferentes.

Después de que usted completa la definición de acción de alarma, usted debe asignar la acción de la alarma a un nivel de gravedad. Una notificación de acción sólo ocurrirá si usted asigna éste a un nivel de gravedad de alarma.

## Definiendo el Script de Notificación de Alarma

Para configurar el Sniffer pro para invocar un Script de visual Basic cuando una alarma ocurre:

1. Seleccione la etiqueta  Alarma del menú de Tools/Options.

2. click en el botón Define actions para abrir la caja de diálogo Acción de alarma.

3. click en el botón Add, entre un nuevo nombre de Acción de Alarma y seleccione el botón Script radio. Alternativamente, usted puede copiar el ambiente de una acción existente. Pulse el botón OK. La información de Script para ayuda al usuario abre.

4. Entre la ruta y nombre de su archivo del Script de visual Basic, o pulse el botón para examinar su archivo. Pulse el botón next para continuar.

5. Establezca el cronograma para la notificación de alarma. Siempre seleccione on si usted quiere habilitar la acción de la alarma en todo momento, o seleccione el cronograma si usted quiere habilitar la acción de la alarma durante ciertos periodo de tiempo. Entre el periodo de tiempo y seleccione qué días usted quiere la acción habilitada. Presione el botón encendido para la acción de la alarma durante ese día. Usted puede pulsar el botón Todos los días, Días de la semana, o fin de semana para encender esos días automáticamente. Pulse el botón next para continuar.

6. Pruebe el nuevo ambiente para Script. Pulse el botón Finish.

7. click OK para completar la definición de acción de alarma.

Un Script es un programa de visual Basic que construye el Sniffer pro Basic, él interpreta, entiende y ejecuta una tarea específica que usted define. El Sniffer incluye  un programa de muestra, ALARM.BAS;  que muestra cómo invocar un programa externo y desplegar un mensaje de alarma. Siguiendo el programa de muestra, usted puede escribir un programa para realizar otras tareas para ocuparse de una notificación de alarma.

NOTA:

Después de que usted completa la definición de acción de alarma, usted debe asignar la acción de la alarma a un nivel de gravedad. Una acción de notificación sólo ocurrirá si usted asigna ésta a un nivel de gravedad de alarma.

## Asignando Las Acciones de  Alarma

Después de que usted completa la definición de una acción de la alarma, usted debe asignar la acción de la alarma a un nivel de gravedad. Una acción de la notificación sólo ocurrirá si usted asigna ésta a un nivel de gravedad de alarma.

Para asignar las acciones de la alarma a los niveles de gravedad (severidad):

1. Seleccione la etiqueta Alarma del menú de Tools/Options.

2. click en la celda de la tabla dónde usted quiere asignar una nueva acción de la alarma. Hay cuatro celdas subsecuentemente para cada nivel de severidad, pulse el botón en la celda en blanco numerada más baja.

3. click en flecha abajo para desplegar una lista de acciones definidas y seleccionar la acción usted quiere.

4. Repita los pasos 2 y 3 para asignar más acciones de alarma en los espacios proporcionados.

5. Pruebe y habilite la Nueva Alarma para habilitar la notificación de alarma.

6. click OK.

## Asignando un Nivel de Severidad a un Tipo de Evento de Alarma

Alarmas expertas
Alarmas supervisoras

## Modificando un Nivel de Umbral de Alarma

Alarmas expertas
Alarmas supervisoras

## Alarm Log (Anotación de las Actividades que se producen en una alarma)

El Sniffer pro descubre los eventos de la red anormales durante una supervisión y durante una captura en el modo Experto. Estos eventos, llamados alarmas, son grabados en un log (anotaciones de actividades) de Alarma.

Para ver el alarm log, seleccione Alarm Log del menú Monitor, o pulse el icono en el toolbar.

El Alarm log lista las alarmas con la más reciente primero. Usted puede ordenar las entradas de alarma por sus encabezados de columna. Para ordenar ascendentemente, pulse el botón encabezado de columna deseado. Pulse el botón encabezado de columna para ordenar descendentemente otra vez.

Usted puede marcar una alarma como se había aceptado. Usted reconocería una entrada de alarma, por ejemplo, si ésta fuese asignada a un localizador de problemas de la red.
Para reconocer las alarmas:

1. Seleccione Alarm log del menú monitor, o pulsa el icono en el toolbar.

2. Haga Click derecho en alarm log, o en una alarma particular que usted haya seleccionado.

3. Seleccione Acknowledge All del menú de contexto para reconocer todas las alarmas en el alarm log, o acknowledge para reconocer la alarma particular que usted seleccionó.

4. Usted puede limpiar el log, individualmente o todos ellos de una sola vez.

Para limpiar las entradas de alarmas en el alarm log:

1. Seleccione alarm log del menú monitor, o pulsa el icono en el toolbar.

2. Seleccione una alarma en particular si usted quiere quitarla del alarm log. Click derecho en el botón alarm log, o seleccione una alarma particular y click derecho botón en ella.

3. Seleccione Remove All o Remove del menú de contexto para quitar todas las entradas del alarm log o simplemente la entrada que usted seleccionó.

## ADMINISTRAR LA LISTA DE DIRECCIONES.

### Entradas en la lista de direcciones

La lista de direcciones le permite definir sus nodos de la red en nombres simbólicos más legibles. El Sniffer pro usa la lista de direcciones en la definición de filtros, la captura visualiza la decodificación, el Expert visualiza, y el fichero que contiene direcciones numéricas conocidas como anfitriones (host table) reemplaza el 6 byte de la dirección del hardware o dirección del nodo de la red con su nombre simbólico respectivo.
Una entrada en la lista de direcciones contiene:

- Nombre
- La dirección de Hardware
- La Dirección IP
- la Dirección IPX
- El tipo de nodo
- Descripción

El Sniffer pro usa sólo la direcciones de hardware o direcciones de IP/IPX. Los otros campos sólo son informativos. (Ellos pueden usarse en las versiones futuras del Sniffer pro)

El tipo de selecciones son Workstation, Host Computer, Server, File Server, Printer Server, Router, Bridge, and Hub.

El campo de Descripción es un campo de texto en que usted puede escribir su propia descripción o notas sobre el nodo.

Administrando la lista de direcciones

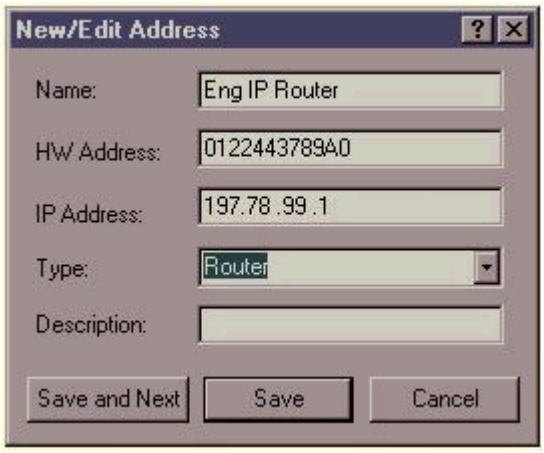
Para abrir la lista de direcciones, seleccione Address Book del menú de Herramientas, o pulsa el icono en el toolbar.

Cuando la lista de direcciones abre, pulse el botón derecho del Morse para desplegar un menú de contexto. Usted puede crear, puede modificar, o puede anular una entrada. Usted también puede deshacer o reconstruir un cambio en la entrada. Usted puede acceder a las mismas funciones de los botones de la barra de herramienta en el borde izquierdo de la caja de diálogo lista de direcciones.

### Crear una Entrada

Para crear una entrada en la lista de direcciones:

1. Seleccione Tools/Address Book para desplegar la lista de direcciones.
2. click en el botón derecho del mouse para desplegar el menú de contexto.
3. click en New Adrress para abrir la caja de diálogo New/Edit Address.

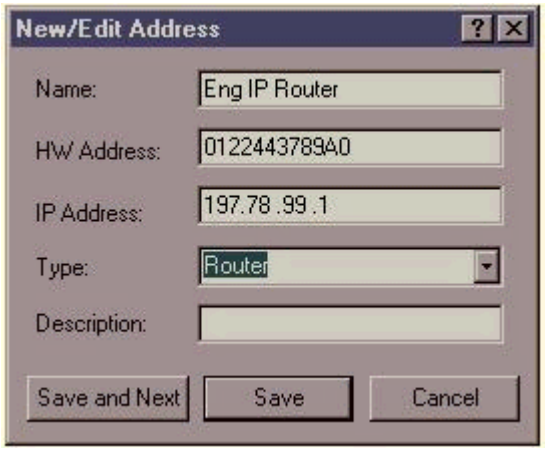



4. Entre el Nombre, HW Address, IP Address y/o IPX address. Si la entrada es un router, seleccione router. (esto previene duplicar las direcciones de alarmas durante un autodescubrimiento de direcciones) Otras entradas son usadas solo para referencias. El Sniffer pro no las interpreta.
5. click en Save para agregar la nueva entrada a la lista de direcciones. Alternativamente, pulse el botón Save y Next para guardar está entrada y agregar otra entrada.

## Modificar una Entrada

Para modificar una entrada en la lista de direcciones:

1. Seleccione Tools/Address Book para visualizar la lista de direcciones
2. Seleccione la entrada de su opción señalando y pulsando la fila para resaltar la selección.
3. Click en el botón derecho del mouse para desplegar el menú de contexto.
4. click en edit address para abrir la caja de diálogo New/Edit Address.




5. Entrar el Nombre, HW Address, IP Address y/o IPX address. Si la entrada es un router, seleccione router. (Esto previene duplicar las direcciones de alarmas durante un autodescubrimiento de direcciones) Otras entradas sólo son para la referencia del usuario. El Sniffer pro no las interpreta.

6. click en Save para guardar la entrada modificada en la lista de direcciones.

## Anular una Entrada

Para anular una entrada en la lista de direcciones:

1. Seleccione Tools/Address Book para desplegar la lista de direcciones.

2. Seleccione la entrada que usted quiere anular.

3. Click en el botón derecho del mouse para desplegar el menú de contexto.

4. click en delete address.

## Importar Tablas de direcciones

El Sniffer pro permite importar tabla de direcciones otras aplicaciones (como NetXRay y WebXRay) y del local host files en la lista de direcciones del Sniffer Pro. Las tablas de direcciones deben estar separadas por el formato comma-separated-value (CSV) y puede importarse la lista de direcciones usando scripts de visual Basic que proporciona el directorio del Sniffer Pro:

- Use el script xray2xray.bas para NetXRay, WebXRay, y tablas de direcciones Sniffer Pro.
- Use el script ImpIPAddrTable.bas para las tablas de direcciones IP
- Use el script ImpIPHosts.bas para local hosts files TCP/IP
- Use el script ImpNovAddr.bas para archivos que contienen nombres de servicio de directorio de Novell Netware 4.0.

NOTA:

Usted puede tener unas 5,000 entradas en la lista de direcciones.

Para importar una tabla de direcciones:

1. Seleccione Run Script del menú archivo (file).

2. Seleccione el script apropiado del directorio Programa del Sniffer Pro Programa directorio, y entonces pulsa el botón Abrir (open).

3. De la caja del diálogo, seleccione un archivo .CSV y pulse el botón open.

## Autodescubrimiento de direcciones de red y Nombres de Dominio

El Sniffer pro proporciona una característica de autodescubrimiento, que aprende lo siguiente: nombres y direcciones automáticamente y los guarda en la lista de direcciones.

- Una dirección IP de un nodo de una red, su dirección de hardware asociada, y nombre del dominio
- Un NetBIOS de un nodo de la red, nombre y hardware (dirección MAC)
- Un usuario Netware de un nodo de la red IPX, nodo y hardware (dirección MAC)

TIP:

Si su red usa asignaciones dinámicas de direcciones IP, el auto-Descubrimiento no es útil porque las direcciones IP para un nodo de la red de vez en cuando puede cambiar.

IMPORTANTE:

Antes de usar la característica autodescubrimiento, asegúrese que especifica los routers usados en su red para prevenir las entradas de dirección duplicadas en el alarm log.

Para usar la característica autodescubrimiento:

1. Seleccione Address Book del menú Opciones.

2. click en el botón address book en toolbar para abrir la caja de diálogo Opciones de Descubrimiento.

3. click en uno de los botones:

Para determinar los nombres del dominio de direcciones de IP específicas, pulse el botón Rango (direcciones IP), entonces entre la dirección subnet y el rango de dirección de nodo en los campos proporcionados.

Para determinar el nombre del dominio de cualquier nodo IP que tiene el tráfico en el subnet, pulse alguna dirección IP en la red.

Para determinar el nombre NetBIOS nombran de algún nodo que tiene el tráfico en el subnet, pulse algún dirección NetBios en la red.

Para determinar un nombre de usuario Netware de algún nodo IPX que tiene el tráfico en el subnet, pulse alguna dirección Novell en la red.

4. clic OK. Una caja de diálogo pequeña muestra el autodescubrimiento en marcha. Cada vez el sniffer Pro ve una nueva dirección, intenta aprender el nombre del dominio asociado con él. Si el nombre no se encuentra, la dirección de IP no es cargada y no entra en la lista de direcciones.

NOTA:

Durante el autodescubrimiento de nombre de usuario de Netware y direcciones MAC, usted debe iniciar la sesión en un Servidor de Netware desde una ventana de DOS y debe teclear userlist /a. Este procedimiento habilita al Sniffer Pro para extraer el nombre del usuario conectado y direcciones del hardware.

Para detener el descubrimiento, pulse el botón Cancelación en la caja de diálogo de progreso.

## ORGANIZANDO EL FORMATO DE VISUALIZACIÓN HOST TABLE

### Ordenando los contenidos de un contador de campo

Usted puede ordenar las entradas del host table por los contenidos de un contador particular. Para ordenar el host table en orden descendente, el host table da un vistazo de cuales nodos son los más activos transmitiendo o recibiendo ciertos tipos de paquetes.

- Haciendo click en los encabezados de columna ordenarán la tabla en orden descendente basado en los contenidos del campo seleccionado.
- Haciendo Click en el encabezado de columna ordenarán la tabla en orden ascendente otra vez

Nota

- El orden predefinido del campo de dirección es el reverso del contador de campo - pulsando un encabezado de campo de dirección ordenarán ascendentemente.

## USE LAS HERRAMIENTAS ACTIVAS DEL SNIFFER PRO

### Ping

Use el Ping para identificar la disponibilidad de un nodo host IP en la red.
El Ping utiliza el protocolo ICMP obligatorio datagrama ECHO REQUEST como respuesta a un ICMP ECHO RESPONSE de un host una entrada de la red que usted especifica.
Para Invocar Ping, seleccione Tools/Ping del menú principal.

- Si el host responde, el Ping imprime y contesta de xx.xx.xx.xx bytes=xx time=xx ms TTL=xx en el Ping log window.
- Si no hay ninguna respuesta para el periodo definido tiempo-fuera, el Ping imprime Error xx.xx.xx.xx: Pida la Interrupción en la log window.

El periodo predefinido tiempo-fuera es 300 milliseconds. Usted puede ajustarlo a un valor apropiado para sus condiciones de red.

TIP:

- Usted puede resaltar un host IP en el host table y con click derecho en ping puede acceder a otras herramientas activas en el menú contexto.

## Finger

Use finger para desplegar la información sobre cada usuario conectado en un host especifico. Usted puede entrar el nombre del host o su dirección IP.
Para Invocar la herramienta finger, seleccione Tools/Finger del menú principal.

Para preguntar por un usuario particular, entre un username en el campo de Pregunta. Para ver a todos los usuarios, deje el espacio en blanco de campo de Pregunta.
Finger visualiza los resultados de su pregunta en la ventana log finger.

TIP:

- Usted puede resaltar un host IP de un host table haciendo click derecho en finger para acceder a otras herramientas activas en el menú contexto.

## DNS LOOKUP

Use DNS Lookup para encontrar el nombre del dominio de una dirección IP, o viceversa. DNS Lookup envía una pregunta al host DNS y despliega el resultado de la pregunta en la ventana log DNS Lookup.
Para Invocar la herramienta DNS Lookup, seleccione Tools/DSN Lookup del menú principal.

TIP:

Usted puede resaltar un host IP del host table y con el click derecho en DNS lookup puede acceder a otras herramientas activas en el menú contexto.

## Whois

Use Whois (como en, quién es...?) para buscar un entrada de directorio TCP/IP para un nombre del dominio registrado, el nombre de usuario, o usuario ID.

Para inicializar la herramienta Whois, seleccione Tools/Whois del menú principal.

Para Usted entrar el nombre del dominio registrado en el campo Host name:

- Entre name.dom para un dominio, por ejemplo, netscape.com

- Entre Firstname Lastname o Lastname, Firstname para un usuario registrado, por ejemplo, Mary Smith o Smith, Mary,
- Entre el userid para un usuario ID, por ejemplo, el eric_hua

Opcionalmente, usted puede entrar en el nombre de un servidor Whois particular en el campo Servidor si usted desea restringir la búsqueda a un servidor particular.

Se despliegan los resultados de la búsqueda en la ventana Whois log.

TIP:

Usted puede resaltar un host IP del host Table y con click derecho en Whois puede acceder a otras herramientas activas en el menú contexto.

## Trace Route

Use Trace route para identificar toda las direcciones IP de routers intermedios y retrasos de tiempo de acceso entre su Sniffer pro y un host destino.

Para Invocar la herramienta de Trace Route, seleccione Tools/Trace del menú principal.

Especifique la dirección IP de su host destino y el intervalo de tiempo-fuera (el valor por defecto es 300 milliseconds).El rastreo de la ruta manda los paquetes ICMP Trace route. Los routers adjuntan camino de regreso, y construyen ruta y despliegan un Trace Route Log.

Una vez el rastreo de la ruta se ha completado, Trace Route emite un DNS Lookup y despliega el resultado en Trace route log. Usted también puede desplegar la información de Trace route en una tabla o gráfico. Pulse la etiqueta tabla o gráfico en la barra de estado.

TIP:

Usted puede resaltar un host IP del Host table y con click derecho en Trace Route puede acceder a otras herramientas activas en el menú del contexto.

# PERSONALICE EL MENÚ DE LAS HERRAMIENTAS

## Agregue Herramientas al Menú de las Herramientas

Además del conjunto normal de herramientas de IP, usted puede agregar sus propias herramientas al menú de las Herramientas. La herramienta puede ser alguno de Windows o archivo ejecutable DOS archivo ejecutable instalado o accesible a su máquina.

Para agregar una herramienta:

1. Seleccione Tools/Customize User tools del menú principal.

2. click en add. El programa agregará (la nueva herramienta) a la lista de la herramienta.

3. Edit en el Menú Text Field. Reemplace (la nueva herramienta) con el nombre usted quiere ver en el menú.

4. Especifique la línea de comando, los parámetros de línea de comando, e inicialice el directorio que necesite cargar para su programa.

5. Opcionalmente, asigne una combinación de teclas (Alt + t, letter). para hacer esto, ponga un carácter ampersand (&) delante de la letra apropiada en el campo de Texto de Menú. (Además, el programa asigna un Alt automáticamente + la combinación número, visible al derecho del ítem del menú cuando usted despliega el menú de las Herramientas.)

6. Opcionalmente, use los botones Move Up y Move Down en la caja de diálogo personalizar herramientas de usuario para cambiar el orden de herramientas desplegado en el menú.

7. clic OK. La nueva herramienta aparecerá en el menú de las Herramientas.

## Quitar Herramientas del Menú Herramientas

Para quitar una herramienta listada en el menú de las Herramientas:

1. Seleccione Tools/Customize User Tools del menú principal.

2. Seleccione la herramienta que usted quiere quitar.

3. Click en Remove.

4. Clic OK.

# GENERAR TRÁFICO DE RED

## Enviando un Solo Paquete

El generador del paquete le da la habilidad de enviar los paquetes de datos a la red. Puede usarse para producir los paquetes para proveer su aplicación para probar, o para generar una carga de tráfico hacia la red.

Para enviar un solo paquete usando el generador del paquete:

1. Del menú de las Herramientas, seleccione Packet generator. Una ventana Packet generator se despliega.

2. click en Enviar 1 Marco. Una caja de diálogo de envío de un marco se despliega.


3. click en el botón del Tamaño para ajustar el tamaño de su paquete.

4. Usted puede opcionalmente editar el contenido del paquete en la ventana Hex

5. Escoja entre Enviar continuamente, o Enviar un numero de veces.

6. Seleccionan el tiempo de retraso en milliseconds.

7. clic OK para empezar la generación del paquete.

8. click en la etiqueta Anim para ver el progreso del generador de paquete en el modo gráfico animado. (La proporción de la pelota pequeña que pasa por la conexión de red no refleja la velocidad de transmisión.) Usted también puede pulsar la etiqueta Detalle para ver la proporción de la transmisión real.

9. click en el botón, si usted quiere detener la transmisión de paquetes.

## Editando el contenido del paquete

Al usar el Generador del Paquete, usted puede enviar un solo paquete que usted crea o modifica usando la caja de diálogo send new frame.
Pueden modificarse el contenido del paquete en el campo hex de la caja de diálogo de enviar nuevo paquete

1. Mueva el cursor al campo hex y pulse el botón izquierdo del mouse.

2. Use la tecla del cursor para posicionar el cursor en los datos que usted quiere cambiar.

3. Escriba los datos en hex. Usted puede entrar dígitos 0 a 9 y A a F.

## Reconstruir un Archivo de Captura

Al usar el Generador del Paquete, usted puede enviar los contenidos de un archivo de captura previamente guardado usando el botón Send Current Buffer

1. Del menú de las Herramientas, seleccione Packet Generator. Una ventana de generador de paquete se despliega.

2. Seleccione Archivo de la barra menú y pulse el botón Open (abrir). Una caja de diálogo abrir Archivo se despliega.

3. Seleccionan su archivo de captura y pulsan el botón Abrir. Una ventana de Despliegue de Paquete se visualiza.

4. Click en Send Current Buffer. Una caja de diálogo Send Current Buffer se despliega.

5. Escoge entre Enviar continuamente, o Enviar varias veces.

6. Clic OK para empezar la generación del paquete.

7. Click en  la etiqueta Anim para ver el progreso de generador de paquete en el modo gráfico animado. Por favor note que la proporción de la pelota pequeña que pasa por el eslabón de la red no refleja la velocidad de transmisión. Usted también puede pulsar el botón la etiqueta de Detalle para ver la proporción de la transmisión real.

8. Click en el botón, si usted quiere detener la transmisión de paquetes.

TIP:

Usted también puede seleccionar un paquete del Packet display puede pulsar el botón para revisar y enviar un solo paquete del archivo de captura.

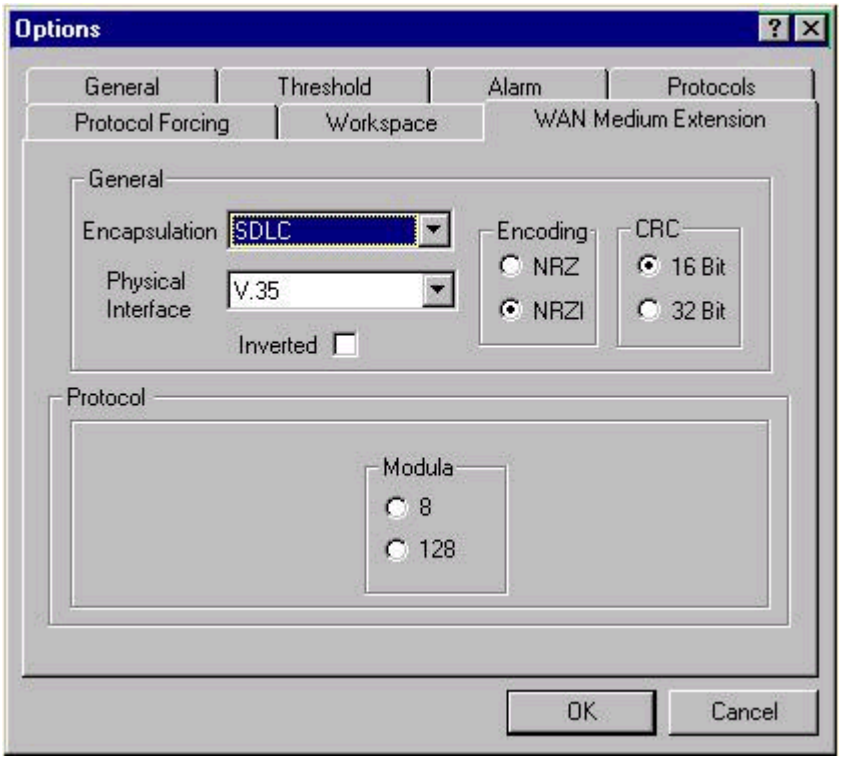
## EL CONJUNTO DE OPCIONES PRECAPTURE PARA LOS ADAPTADORES WAN HSSI

### Opciones de  Extensión Medio

Las específicas opciones Capture  al adaptador HSSI se encuentran en la etiqueta extensión media HSSI de la caja de diálogo Opciones del Sniffer. Usted despliega la etiqueta extensión media HSSI seleccionando Opciones del menú de Herramientas y pulsando en la etiqueta extensión media HSSI en la caja de diálogo que aparece.

NOTA:

La etiqueta extensión media HSSI sólo está disponible si el adaptador de HSSI es el adaptador actualmente seleccionado. Usted puede cambiar el adaptador actualmente seleccionado usando Network  Probe\Adapter, comando en el menú Archivo.




## Opciones Encapsulation

Cuando se captura de un circuito HSSI, usted necesita especificar los protocolos de bajo nivel usados por la conexión síncrona. Usted usa las lista dropdown Encapsulation en la etiqueta extensión media HSSI para especificar el tipo del marco (encapsulation) usado para transmitir marcos a través de la WAN. Los métodos de encapsulation siguientes están disponibles:

- SDLC
- X.25
- Frame Relay
- HDLC/ROUTER/BRIDGE

Los protocolos de encapsulation no afectan los protocolos de nivel superior empotrados dentro de sus marcos.

De estos protocolos, los el más ampliamente usamos somos SNA (Arquitectura de Red de Sistema), SDLC en las instalaciones de IBM, y X.25 en HDLC los cuales están extendidos en Europa y se usa cada vez más en los Estados Unidos. El tipo de marco Frame Relay se usa ampliamente para la interconectividad de LAN, como versiones propietarias de HDLC (decodificado por la opción de HDLC/Router/Bridge)..

Acerca de la Opción HDLC/Router/Bridge

La opción HDLC/Router/Bridge permite el analizador descifrar versiones propietarias de HDLC durante la captura. Muchas interredes que usan líneas arrendadas usan versiones propietario de HDLC. El Sniffer Pro puede reconocer y puede interpretar los datos dentro de muchas versiones de HDLC. Éstos incluyen el Punto a punto (PPP) los estándares formatos de marco router/bridge, también otras variedades, incluso las versiones propietario de HDLC de los siguientes router/bridge:

- Wellfleet (Versiones 3.1, 3.3, y 3.7).

Full support - Post-análisis más todas las estadísticas y distribución del protocolo para la captura de tiempo real y despliegue del post-análisis.

- CISCO

Full Support - Post-análisis más todas las estadísticas y distribución del protocolo para la captura de tiempo real y despliegue del post-análisis.

- VITALINK

Full Support - Post-análisis más todas las estadísticas y distribución del protocolo para la captura de tiempo real y despliegue del post-análisis.

- PROTEON

post-análisis

- IBM source routing bridges (Versiones 2.2 y 2.3, token ring solo)

post-análisis.

- MICROCOM

post-análisis.

- Ungermann-bass

post-análisis.

- ACC

post-análisis

- BANYAN VINES

post-análisis

- CROSSCOM

post-análisis

- RETIX

post-análisis

- DEC

post-análisis

- NETRONIX

post-análisis

- ATT

post-análisis

IMPORTANTE: Cuando Encapsulation es colocada en HDLC/Router/Bridge, el Sniffer pro automáticamente deduce el tipo de HDLC en uso en la línea de comienzo de la captura. Si durante una sesión de captura usted reconfigura algún link WAN(por ejemplo, rebooting el router, o cambia el protocolar ejecutado por el router), usted debe detener y debe reiniciar la sesión de la captura actual. Al reiniciar la sesión de la captura permite el analizador re-descubrir el tipo de tráfico WAN en la conexión.

Opciones de La Velocidad de la Línea (bps)

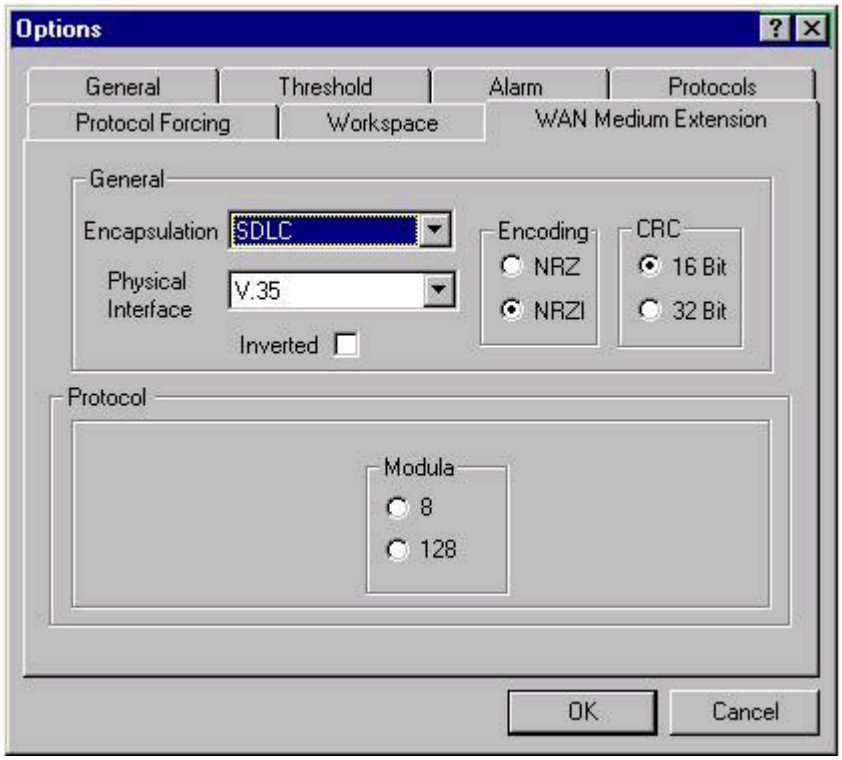
Use la opción Line Speed para especificar la velocidad del circuito HSSI a ser supervisado.

Opciones CRC

El Sniffer puede descifrar 16-bit CRC y 32-bit CRC para la detección del error entre dos routers. El valor por defecto es 16-bit CRC. Usted puede cambiar entre 16-bit y 32-bit seleccionando la opción apropiada en la etiqueta extensión media HSSI de la caja de diálogo de Opciones.

Opciones de Extensión media WAN

Las específicas opciones Capture del adaptador LM2000 se encuentran en la etiqueta Extensión media WAN de la caja de diálogo Opciones del Sniffer Pro. Usted despliega la etiqueta extensión media WAN seleccionando Opciones del menú Herramientas y pulsando en la etiqueta extensión media WAN en la caja del diálogo que aparece.
Nota: La etiqueta Extensión media WAN sólo está disponible si el adaptador LM2000 es el adaptador actualmente seleccionado. Usted puede cambiar el adaptador actualmente seleccionado que usa Selecionando Network Probe\Adapter, comando en el menú Archivo.



Opciones Encapsulation

Cuando capturar de un circuito HSSI, usted necesita especificar los protocolos de bajo nivel usados por la conexión síncrona. Usted usa las listas dropdown Encapsulation en la etiqueta de extensión media HSSI para especificar el tipo de marco (encapsulation) usado para transmitir marcos a través de la WAN. Los métodos de encapsulation siguientes están disponibles:

- SDLC
- X.25
- Frame Relay
- HDLC/ROUTER/BRIDGE

Los protocolos del encapsulation no afectan los protocolos de nivel superior empotrados dentro de sus marcos.

De estos protocolos, los el más ampliamente usamos somos SNA (Arquitectura de Red de Sistema), SDLC en las instalaciones de IBM, y X.25 de HDLC el cual está extendido en Europa y se usa cada vez más en los Estados Unidos. El tipo de marco Frame Relay se usa ampliamente para la interconectividad de LAN, como es versión propietario de HDLC (se descifra por la opción HDLC/Router/Bridge)..

Acerca de la Opción Router\Bridge

La opción Router/Bridge permite el analizador descifrar versiones propietario de HDLC durante la captura. Muchos interredes que arriendan líneas usan versiones propietario de HDLC. El Sniffer Pro puede reconocer y puede interpretar los datos dentro de muchas versiones de HDLC. Éstos incluyen el Punto a punto (PPP) los formato de marco estándares router/bridge y también una otras variedades, incluso las versiones propietario de HDLC de los siguientes router/bridges:

- Wellfleet (Versiones 3.1, 3.3, y 3.7).

Full Support - Post-análisis más todas las estadísticas y distribución de protocolo para la captura de tiempo real y despliegue del post-análisis.

- CISCO

Full support - Post-análisis más todas las estadísticas y distribución de protocolo para la captura de tiempo real y despliegue del poste-análisis.

- VITALINK

Full support - el Post-análisis más todas las estadísticas y distribución de protocolo para la captura de tiempo real y despliegue del post-análisis.

- PROTEON

post-análisis

- IBM source routing bridges (Versiones 2.2 y 2.3, solo token ring)

post-análisis

- MICROCOM

post-análisis

- Ungermann-bass

post-análisis

- ACC

post-análisis

- BANYAN VINES

post-análisis

- CROSSCOM

post-análisis

- RETIX

post-análisis

- DEC

post-análisis

- NETRONIX

post-análisis

- ATT

post-análisis

IMPORTANTE: Cuando Encapsulation es conjunto de HDLC/Router/Bridge, el Sniffer pro automáticamente deduce el tipo de HDLC en uso en la línea al empezar la captura. Si durante una sesión de captura usted reconfigura alguna conexión WAN (por ejemplo, rebooting el router, o cambiando el protocolo que ejecuta el router), usted debe detener y debe reiniciar la sesión de la captura actual. Reiniciando la sesión de captura permite el analizador re-descubrir el tipo de tráfico WAN en la conexión.

Opciones de Interfase Físicas

Antes de que usted pueda capturar del circuito WAN usando una tarjeta LM2000, usted debe especificar el tipo de interface física al que la tarjeta LM200 se conecta. Usted usa la lista dropdown de Interfaces Físicas en la etiqueta Extensión media WAN para especificar la interface física. Las interfaces físicas siguientes están disponibles:

- Interface RS-232 a través de un cable DB-25

- Interface RS-422 a través de un cable DB-15

- Interface RS-423 a través de un cable DB-15
- Interface V.10 a través de un cable DB-15
- Interface V.11 a través de un cable DB-15
- Interface V.35 a través de un cable DB-15

Opciones de Codificación

Para descifrar correctamente los datos transmitidos, especifique el método de codificación usado por su red. Los dos métodos de codificación más comunes para SDLC y HDLC son NRZ (Non-return to zero) y NRZI (Non-return to zero inverted). Click en la opción apropiada para su red.

Opciones CRC

El Sniffer Pro puede decodificar 16-bit CRC y 32-bit CRC para la detección de error entre dos routers. El valor por defecto es 16-bit CRC. Usted puede cambiar entre el 16-bit y 32-bit seleccionando el apropiado.

Opción "Invertido"

Algunas redes WAN/Synchronous invierten los bit de datos cuando ellos se cae el cableado (cambios binario 0 a 1, y viceversa). En casos así, usted debe habilitar la opción Invertido en la etiqueta Extensión media WAN de la caja de diálogo de Opciones, para permitir al analizador leer los datos correctamente.

Opción Protocolo

Dependiendo de la selección del protocolo de encapsulation, diferentes opciones protocolo-específicas (como el método para generar la numeración de secuencia de números de los marcos) puede configurarse en el área Protocolo de la etiqueta Extensión media WAN. Estas opciones se describen debajo.

Generando La Enumeración de Secuencia de Marco

Si usted ha seleccionado entre SDLC, X.25, o HDLC/Router/Bridge como el protocolo de encapsulation, usted también puede especificar el método a usar para generar la numeración de sucesión de marco. Hay dos métodos para generar la numeración de sucesión de marco. El método a usarse en una red particular no está aparentemente claro sólo por inspección. Un método usa tres bits (Modulo 8), y se usa ampliamente en los Estados Unidos y en Europa. El otro método usa siete bits (Modulo 128), y se usa a menudo en Japón y en las conexiones de satélite internacionales.

El valor por defecto es Modulo 8.

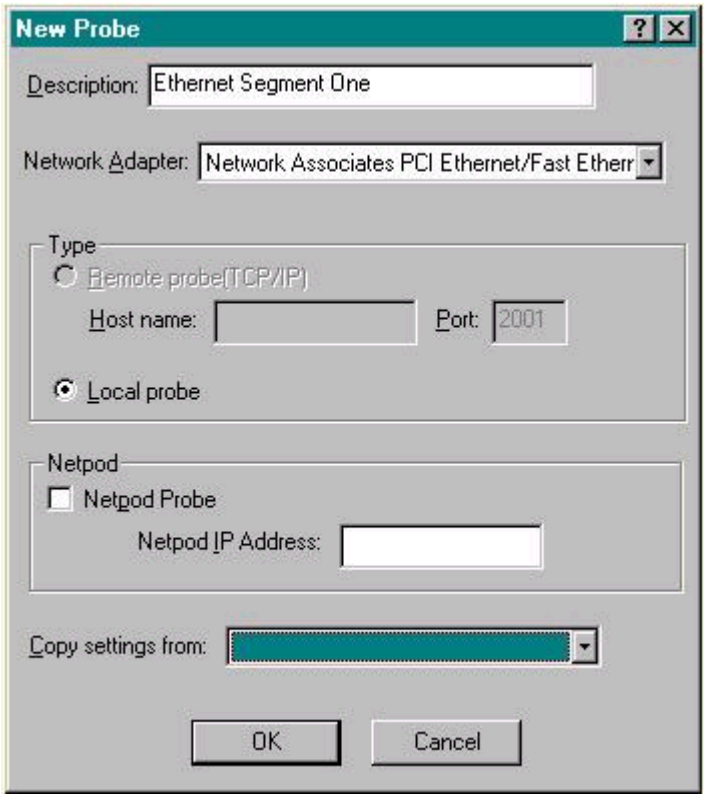
## ASPECTOS DE USO AVANZADO DEL SNIFFER PRO.

### Supervisando Dos o Más Adaptadores de la Red al mismo tiempo

Si usted tiene múltiples adaptadores de red instaladas en su sistema, usted puede iniciar un programa en múltiples instancias del Sniffer pro, con cada uno supervisando a través de un adaptador separado. En cada caso Sniffer Pro es llamado es llama una exploración.
Para crear una nueva exploración en Sniffer Pro:

1. Vaya al menú Archivo y click en Select Network Probe\Adapter.

2. Click en el botón New Probe para abrir una caja de diálogo de nueva exploración.




- Use el campo de Descripción para proporcionar un nombre descriptivo para este adaptador. Su descripción aparecerá en las instancias futuros de la caja de diálogo Select Network Probe/Adapter
- Use el campo de Adaptador de Red para seleccionar el adaptador. La lista dropdown incluye todo los adaptadores conformes a NDIS 3.1 actualmente instalados en el Sniffer Pro. Seleccione un adaptador que no este supervisado por otra exploración de Sniffer Pro

- Use el campo tipo para especificar si la exploración es Remota o Local. Para el Sniffer Pro, usted está limitado a las exploraciones Locales. Sólo se soportan las exploraciones remotas para el Sniffer Pro Distribuido. Si usted está usando el Sniffer Pro distribuido y selecciona una exploración Remota (es decir, una exploración en la cual usted se conecta a otra red usandoTCP/IP), usted debe proporcionar el nombre del host y el número del puerto TCP usado para conectarse en la exploración remota

- Habilite el Netpod Probe checkbox si esta exploración se usará con una interface de red pod (como la Network Associates Full Duplex Ethernet Pod). Cuando usted le permite el Netpod Probe checkbox, la dirección Netpod IP se llena automáticamente con una dirección IP incrementada por una dirección IP de PC del Sniffer Pro Por ejemplo, si la dirección IP de PC de Sniffer Pro es 206.129.112.24, la dirección Netpod IP proporcionada por el Sniffer Pro será 206.129.112.25.

NOTA: Este descargo del Sniffer Pro sólo soporta las conexiones locales network pods. Usted no puede conectar network pods encima de la red.

- Use el ambiente de Copia de campo para usar las escenas de configuración de una exploración existente. La lista dropdown incluye previamente todas las exploraciones definidas en el Sniffer Pro PC

- Una nueva exploración es creada para supervisar el adaptador de la red seleccionado.

TIP:

Una vez usted ha creado múltiples exploraciones locales, usted puede iniciar un programa nuevo la sesión de Sniffer Pro sin crear nuevas exploraciones otra vez.

## Manteniendo múltiple archivos en Sniffer Pro

Si usted es una persona que mantiene su red soportando sitios múltiples, la característica de múltiple exploración del Sniffer Pro le permite convenientemente mantener una lista de direcciones separada, y otro ambiente, para cada sitio. Cada vez usted crea una nueva exploración, el Sniffer Pro establece un directorio separado para mantener otra copia de la lista de direcciones, las escenas de filtro de captura, las opciones de

Despliegue de Paquete, la actualización de la frecuencia, y los umbrales de la alarma. Usted puede crear una nueva exploración local a la que le ponen el nombre de cada sitio que usted maneja.

Para crear una nueva exploración local:

1. Del menú Archivo, escoja Select Network Probe/Adapter para extraer la caja de diálogo Adaptador.

2. click en New Probe para abrir una Nueva caja de diálogo de exploración.

3. Entre una descripción, seleccione el botón Local Probe Radio, y entonces pulse el botón OK. Alternativamente, usted puede copiar un ambiente workspace para la nueva exploración de las exploraciones existentes. Abra la caja que contiene la lista y seleccione una exploración existente como la fuente a copiar. El ambiente workspace exploración incluye la lista de direcciones, las escenas de filtro de captura, las opciones de Despliegue de Paquete, actualización de la frecuencia, y umbrales de la alarma.

4. Seleccione un adaptador, entonces pulse el botón OK.

Para usar la escena particular para un sitio:

1. Del menú Archivo, escoja Select Network Probe/Adapter para extraer la caja de diálogo Adaptador.

2. Abra la exploración local (Sitio) de su opción pulsando el botón(+), señalando delante el nombre de la exploración

3. Seleccionan un adaptador, entonces pulse el botón OK.

El Sniffer Pro cambiará a las escenas que se definieron previamente para ese sitio.

## Capturando De un Archivo

Usted puede usar le modo Loopback del Sniffer Pro para simular una captura de un archivo desde un rastreo de marcos guardados. Simulando una captura pueden ser útiles para instruir propósitos.

Para capturar de un archivo desde un rastreo de marcos guardados:

1. En el menú Archivo del Sniffer Pro, habilite la opción Loopback Mode.
2. Del menú Herramientas, seleccione Packet generator. Una ventana de generador de paquete abre.
3. Seleccione su rastreo de archivo y click en open. Una caja de diálogo File Open se visualiza.
4. Seleccionan su rastreo de archivo pulse el botón open. Una ventana de Despliegue de Paquete abre.
5. click en Send Current Buffer. Una caja de diálogo aparece.
6. Escoja entre Enviar continuamente, o Enviar varias veces.
7. click en OK para empezar la generación del paquete.
8. Para empezar a capturar seleccione Start del menú Captura.
9. El panel de captura actualiza las capturas del Sniffer Pro desde el rastreo de archivo seleccionado

Si usted es una persona de soporte de red que mantiene múltiples sitios, el Sniffer Pro múltiple-sonda le permite convenientemente mantener un libro separado de direcciones, y otras escenas para cada sitio. Cada vez usted crea una nueva sonda, el Sniffer Pro monta un directorio separado para mantener otra copia del libro de direcciones, Despliega el paquete de opciones, actualiza la frecuencia, y umbrales de la alarma. Usted puede crear una nueva sonda local después de cada sitio que se maneja.

Para crear una nueva sonda local:

1. Del menú del Archivo, escoja la Select Network Probe/Adapter para plantear la caja de diálogo de Adaptador.
2. Pulse el botón New Probe para abrir una caja de diálogo New Probe.
3. Entre en una descripción, seleccione el botón Local Probe radio, y entonces pulse el botón OK. Alternativamente, usted puede copiar un workspace que coloca para la nueva sonda de las sondas existentes. Abra Combo list box y seleccione una sonda existente como el camino a copiar. El workspace de una sonda enviada incluye el libro de direcciones, captura los filtros enviados, las opciones de Despliegue de Paquete, actualiza la frecuencia, y umbrales de la alarma.
4. Seleccione un adaptador, entonces pulse el botón OK.

Para usar la escena particular para un sitio:

1. Del menú del Archivo, escoja la Select Network Probe/Adapter para plantear la caja de diálogo de Adaptador.
2. Abra la Sonda Local (el Sitio) de su opción pulsando el botón (+) la señal delante del nombre de la sonda.
3. Seleccione un adaptador, entonces pulse el botón OK.

Sniffer Pro cambiará a las escenas que se definieron previamente para ese sitio.

Captura De un Archivo

Usted puede usar el Modo de Loopback del Sniffer Pro para simular una captura de un archivo de los frame grabados.

Para capturar de un archivo la pista de frames grabados:

1. En el menú del Archivo de Sniffer Pro, habilite la opción Loopback Mode.
2. Del menú de las Herramientas, seleccione Packet Genrator. Un Packet generator se abre en la pantalla.
3. Seleccione Archivo de la barra del menú y pulsa el botón Abrir. Una caja de diálogo de abrir archivo se despliega.
4. Seleccione su pista del archivo y pulse el botón Abrir. Una ventana de Despliegue de Paquete se abre.

5. Pulse el botón Send Current Buffer. Se abre una caja de diálogo Send current buffer.
6. Escoja entre Enviar continuamente, o Enviar varias veces.
7. Pulse el botón OK para empezar la generación del paquete.
8. Inicie captura para seleccionar Iniciar del menú Captura.
9. El tablero de captura se actualiza como el Sniffer Pro captura la pista del archivo seleccionado.

# REFERENCIAS DEL SNIFFER PRO

## ESTADÍSTICAS GLOBALES

### Vista gráfica

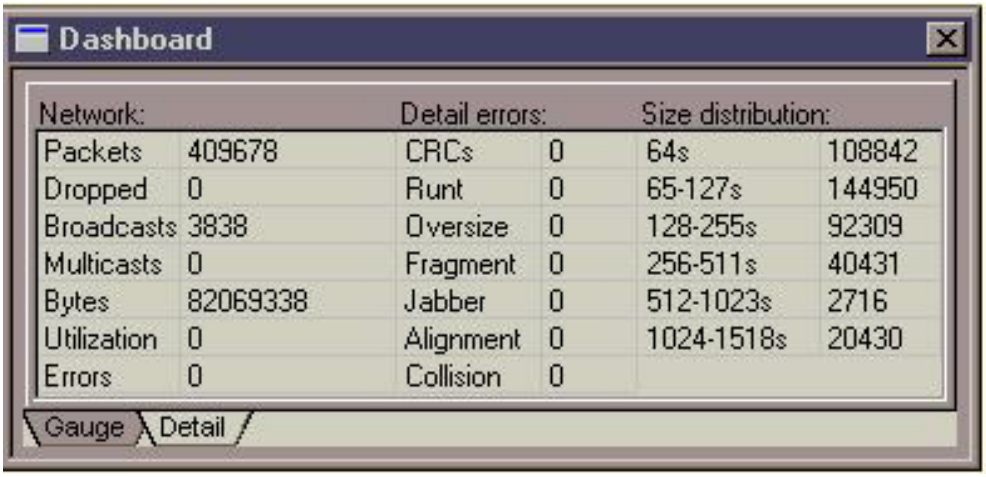
Sniffer Pro empieza coleccionando las estadísticas del segmento de red inmediatamente a la salida. Permite ver las estadísticas de la red en el tiempo real, Seleccione del menú del Monitor Dashboard. La ventana de Dashboard abre.

La ventana de Dashboard despliega las estadísticas de carga de la red en tiempo real, incluso el número de paquetes por segundo, la proporción de utilización como un porcentaje, y el número de errores por segundo.

La zona roja desplegada en cada indicador de Dashboard muestra el nivel de actividad de la red sobre el umbral alto que pone para esa medida. Coloca el umbral alto para estas tres variables, seleccione Opciones del menú de Herramientas, entonces pulse el botón Threshold.

### Resumen Detallado de Ethernet

Para ver el resumen detallado, pulse el botón Detail del Dashboard.




Las estadísticas detalladas de Red Ethernet son mostrados en tres grupos:

1. La red

· Número total de todos los paquetes

· Número total de paquetes que se dejaron caer

· Número total de paquetes de la transmisión

· Número total de paquetes multicast

· Número total de bytes

· Porcentaje Actual de la utilización de la red

· Número total de errores

2. Detalle de los Errores

· Número total de errores de los paquetes CRC

· Número total de paquetes de pequeño tamaño

· Número total de paquetes de gran tamaño

· Número total de fragmentos del paquete

· Número total de paquetes de texto

· Número total de paquetes con errores de alineación

· Número total de paquetes colisionados

3. Distribución del tamaño

· Total de paquetes cuyo tamaño es de 64 bytes

· Total de paquetes cuyo tamaño es de 65 a 127 bytes

· Total de paquetes cuyo tamaño es de 128 a 255 bytes

· Total de paquetes cuyo tamaño es de 256 a 511 bytes

· Total de paquetes cuyo tamaño es de 512 a 1023 bytes

· Total de paquetes cuyo tamaño es de 1024 a 1518 bytes

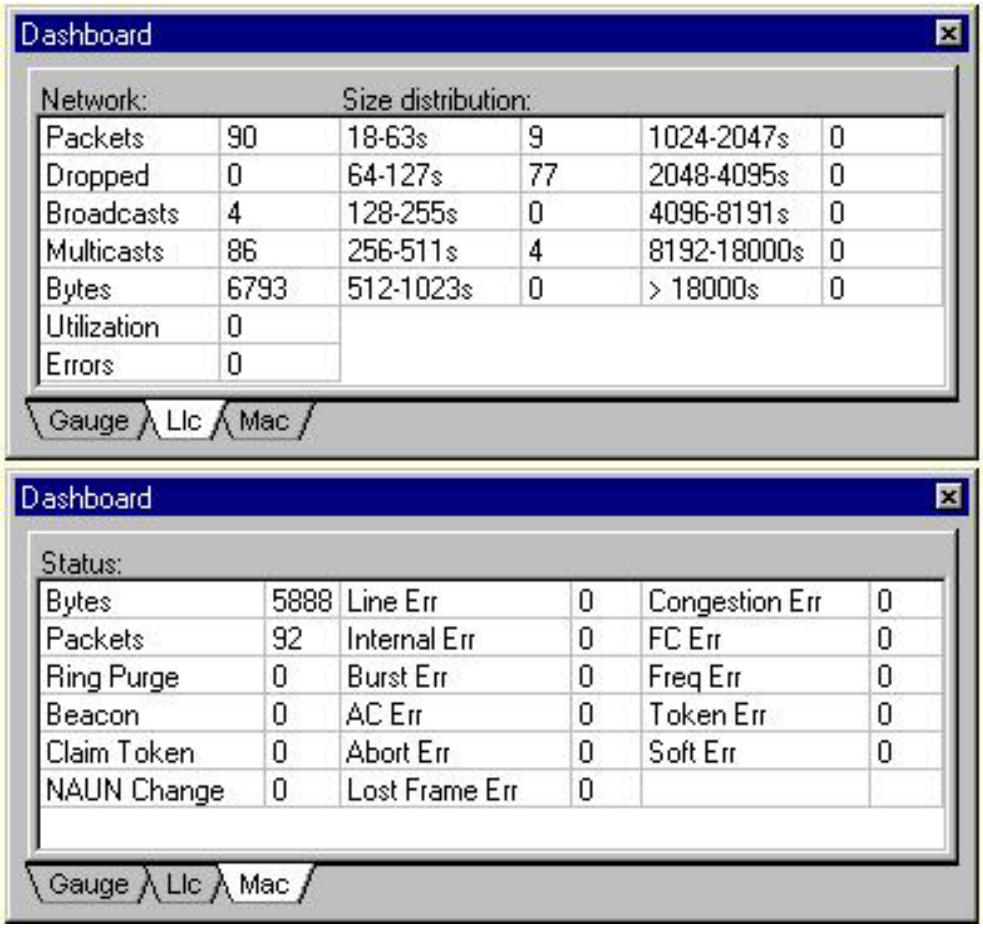
Nota:

· Los Tamaños del paquete definidos aquí incluyen 4 bytes de CRC.

· La versión actual del NDIS 3.1 especifica que no apoya al contar fragmentos y paquetes de texto. Ciertamente las tarjetas de drives NIC no pueden apoyar la detección de CRC y errores de colisión. Usando tales drivers, Sniffer Pro despliega estas estadísticas como ceros. Para el reporte total estadístico de errores, instale el Sniffer Pro reforzado a drivers de NDIS proporcionados con el producto.

## Token Ring MAC y Resumen de L1c

Para ver las estadísticas acumuladas en un formato tabular, pulse el botón el Llc del Dashboard o etiqueta Mac.
Los detalles son despliegados en dos grupos: Llc y Mac.




La etiqueta de Llc despliega la siguiente información:

- El Número total de todos los paquetes
- El Número total de paquetes que se dejaron caer
- El Número total de paquetes de la transmisión
- El Número total de paquetes del multicast
- El Número total de bytes
- Porcentaje Actual de la utilización de la red

- El Número total de errores de los paquetes
- El Número total de paquetes de tamaño de 18 a 64 bytes
- El Número total de paquetes de tamaño de 65 a 127 bytes
- El Número total de paquetes de tamaño de 128 a 255 bytes
- El Número total de paquetes de tamaño de 256 a 511 bytes
- El Número total de paquetes de tamaño de 512 a 1023 bytes
- El Número total de paquetes de tamaño de 1024 a 2047 bytes
- El Número total de paquetes de tamaño de 2048 a 4095 bytes
- El Número total de paquetes de tamaño de 4096 a 8191 bytes
- El Número total de paquetes de tamaño de 8192 a 18000 bytes
- El Número total de paquetes de tamaño mayor que 18000 bytes

La etiqueta de MAC despliega la información siguiente:

- El total bytes de la capa MAC
- El total paquetes de la capa MAC
- El total de paquetes de purga de anillo
- El total #de paquetes de la almenara
- El total #de paquetes de ficha de demanda
- El Número total de cambios de NAUN
- El Número total de errores de la línea
- El Número total de errores internos
- El Número total de errores del estallido
- El Número total de errores del CA
- El Número total de errores de la interrupción
- El Número total de errores del marco perdidos
- El Número total de errores de congestión
- El Número total de errores de FC
- El Número total de errores de frecuencia

· El Número total de errores de la ficha

· El Número total de errores sencillos

## Resumen de WAN Dashboard

Cuando una prueba de la red WAN (por ejemplo, el adaptador de LM2000 o el adaptador de HSSI) es seleccionado por monitoreo o captura, el Dashboard contiene etiquetas adicionales que corresponden al protocolo del encapsulación WAN especificadas en la caja de diálogo de Opciones. Las posibles etiquetas WAN en el Dashboard incluyen:

· **WAN**

La Etiqueta WAN en el Dashboard

Para ver las estadísticas acumuladas WAN en un formato tabular, pulse el botón de la etiqueta WAN del Dashboard. La etiqueta WAN está disponible para todos los protocolos de encapsulación WAN.

La etiqueta WAN despliega la información siguiente:

· El Número total de todos los paquetes

· El Número total de paquetes que se dejaron caer

· El Número total de bytes

· Porcentaje Actual de la utilización de la red

· El Número total de paquetes con error

· El Número total de errores abortados

· El Número total de errores de CRC

· El Número total de errores de gran tamaño

· El Número total de errores del Fragmento

· El Número total de paquetes de tamaño de 1 a 32 bytes

· El Número total de paquetes de tamaño de 33 a 64 bytes

· El Número total de paquetes de tamaño de 65 a 127 bytes

· El Número total de paquetes de tamaño de 128 a 255 bytes

· El Número total de paquetes de tamaño de 256 a 511 bytes

· El Número total de paquetes de tamaño de 512 a 1023 bytes

· El Número total de paquetes de tamaño de 1024 a 1500 bytes

· El Número total de paquetes de tamaño mayor que 1501 bytes

· El Estado de la línea

Etiqueta de Estado de línea en el Dashboard

Usted puede pulsar el botón la etiqueta de Estado de Línea para ver el estado de la línea conectada que usa los indicadores de RS-232 normales RxC, TxC, RxD, TxD, CTS, RTS, DSR, DTR, y Reloj. La condición de cada indicador se muestra con una la flecha hacia arriba (para un lógico 1), una flecha hacia abajo (para un lógico 0), o una flecha que apunta para mostrar de arriba abajo que el estado del indicador ha cambiado en el último segundo. Una arremetida al lado del indicador del Reloj significa que los relojes están ausentes (por ejemplo, cuando la línea no se conecta).

· SDLC

Etiqueta de SDLC en el Dashboard

Usted puede pulsar el botón de la etiqueta de SDLC del Dashboard para ver las cuentas para varios tipos de marcos SDLC. SDLC es la versión de IBM de HDLC. Es el protocolo de capa de enlace para los servicios de capa de red de IBM proporcionados en el SNA. La etiqueta de SDLC está disponible que cuando Encapsulation es colocado a SNA encima de SDLC en la caja de Diálogo Opciones.

La etiqueta de SDLC despliega la información siguiente:
SDLC:

· El Número total de Marcos I

· El Número total de Bytes I

· El Número total de Marcos S

· El Número total de Bytes S

· El Número total de Marcos U

· El Número total de Bytes U

El S-marco:

· El Número total de S-marcos de RR

· El Número total de S-marcos de RNR

· El Número total de S-marcos de REJ

· U-marco

Etiqueta del U-marco en el Dashboard

Usted puede pulsar el botón en la etiqueta del U-marco del Dashboard para ver las cuentas para los diferentes tipos del U-marco. La etiqueta del U-marco está disponible cuando la Encapsulation se coloca en SNA sobre SDLC o enrutador/Puente en la caja de diálogo Opciones.

La etiqueta del U-marco despliega la siguiente información:

· El Número total de U-marcos de SABM (sólo Enrutador/Puente)

· El Número total de U-marcos de SABME (Sólo Enrutador/puente)

· El Número total #de U-marcos del DISCO

· El Número total de U-marcos de DM

· El Número total de U-marcos de UA

· El Número total de U-marcos de FRMR

· El Número total de U-marcos de RD

· El Número total de U-marcos del RIM

· El Número total de U-marcos de UI

· El Número total de U-marcos de UP

· El Número total de U-marcos de TEST

· El Número total de U-marcos de XID

· El Número total de U-marcos de SIM

· El Número total de U-marcos de SNRM

· El Número total de U-marcos de SNRME

· El Número total de U-marcos de SARM (sólo Enrutador/Puente)

· El Número total de U-marcos de SARME (sólo enrutador/puente)

· El Número total de U-marcos de RSET (sólo enrutador/puente)

· El Número total de U-marcos de CFGR

· El Número total de U-marcos de BCN

· LAPB

Etiqueta LAPB en el Dashboard

Usted puede pulsar el botón de la etiqueta de LAPB del Dashboard para ver las cuentas para varios tipos de marcos LAPB. LAPB es un subconjunto de HDLC. Es el protocolo de capa de enlace para el protocolo de la capa de X.25. La etiqueta de LAPB está disponible cuando la Encapsulation se pone a X.25 en la Caja de diálogo Opciones.

La etiqueta de LAPB despliega la siguiente información:

LAPB:

· El Número total de Marcos I

· El Número total de Bytes I

· El Número total de Marcos S

· El Número total de Bytes S

· El Número total de Marcos U

· El Número total de Bytes U

El S-marco:

· El Número total de S-marcos de RR

· El Número total de S-marcos de RNR

· El Número total de S-marcos de REJ

El U-marco

· El Número total de U-marcos de SABM

· El Número total de U-marcos de SABME

· El Número total de U-marcos del DISC

· El Número total de U-marcos de DM

· El Número total de U-marcos de UA

· El Número total de U-marcos de FRMR

· Parada del marco

Etiqueta de Parada de marco en el Dashboard

Usted puede pulsar el botón en la etiqueta de Parada de Marco del Dashboard para ver las cuentas de los diferentes Marco Parada, marcos de tipos. La etiqueta de Parada de Marco está disponible cuando la Encapsulation se coloca en el Marco de Parada en la caja de diálogo de Opciones.

La etiqueta de Parada de Marco despliega la siguiente información:

LMI:

· Marcos LMI

· Bytes LMI

· Enquiries enviado

· Enquiries recibidos

· El estado de Los Mensajes Enviados

· El estado de los mensajes recibidos

· actualizaciones Enviadas

· actualizaciones Recibidas

Indicadores de congestión:

· FECNs

· BECNs

· DEs

· HDLC

Etiqueta de HDLC en el Dashboard

Usted puede pulsar el botón en la etiqueta de HDLC del Dashboard para ver las cuentas para varios tipos de marcos HDLC. HDLC es el protocolo del nivel de enlaces lógicos de la norma ISO para sincronizar las comunicaciones de los datos. La etiqueta de HDLC está disponible cuando la Encapsulation se coloca en el enrutador/puente de la caja de diálogo Opciones.

La etiqueta de HDLC despliega la siguiente información:

HDLC:

· El Número total de Marcos I

· El Número total de Bytes I

· El Número total de Marcos S

· El Número total de Bytes S

· El Número total de Marcos U

· El Número total de Bytes U

El S-marco:

· El Número total de S-marcos de RR

· El Número total de S-marcos de RNR

· El Número total de S-marcos de REJ

## Tamaño del paquete y Distribución de Utilización de Red

Estas estadísticas le permiten al manejador de la red a entender bien la actividad global de los niveles en la red y para calcular con precisión la carga de tráfico de paquetes de tamaños grande y pequeños cada uno de los cuales pueden tener un efecto diferente en la actuación de la red global y su disponibilidad.
Al desplegar Distribución se muestra el consumo del ancho de Banda de la Red distribuido como 0-10%, 11%-20%, 21%-30%, y más adelante.

Para desplegar el gráfico de utilización,

1 Seleccione las Estadísticas Globales del menú del Monitor.

2 Pulse el botón la Utilización Dist. o Tamaño Dist. para mostrar la respectiva barra del gráfico.

3 Pulse el botón el icono de mapa de pastel si usted quiere ver el pastel trazar la vista.

4 Si usted está usando el LM2000 o el adaptador de HSSI, usted también puede pulsar el botón en la etiqueta de enlace WAN para mostrar los gráficos y tablas que resumen la actividad en el Enlace WAN.

## Personalizando el Protocolo de Distribución TCP

TCP/UDP la Aplicación de  paquetes con números del puerto no listados en la lista del protocolo predefinida son agrupados juntos y contados en las otras categorías. Usted puede agregar los números del puerto en la aplicación específica en la lista protocolar para que ellos desplieguen como artículos separados.

Para asignar aplicación de números de puerto TCP/UDP a la lista del protocolo:

1 Del menú de las Herramientas, seleccione Opciones.

2 Seleccione la etiqueta de Protocolo.

3 Colocar cada nombre deseado y el número del puerto que usted desea al monitor como un ítem separado en la lista. Usted puede entrar hasta 3 números del puerto para cada nombre de la aplicación. Entre 0 en las localizaciones del puerto no usadas.

4 Pulse el botón OK.

Nota:

· Sniffer Pro puede sólo cargar las pistas del protocolo que son basadas o bien conocidas y fijar los números del puerto. Si usted tiene una aplicación que asigna y usa número de puertos dinámicamente TCP/UDP, ellos se agruparán en la categoría Otros.

# ESTADISTICAS DE ESTACION

## Ver la tabla de host -  Adaptadores LAN

La tabla de host proporciona un análisis rápido de las estadísticas de tráfico recolectada para cada nodo host en tiempo real. Sus adaptadores LAN pueden ver el tráfico del host en la capa MAC, o sólo ver selectivamente el tráfico de la red en las capas IP o capas de IPX.
La tabla de host tiene cuatro vistas diferentes - tabla outline, tabla de detalle, gráfica de columnas, o de pastel.

ver tabla outline

Proporciona un resumen de los bytes totales y paquetes transmitidos dentro y fuera de cada nodo de la red en tiempo real. Seleccionando la pestaña MAC, IP, o IPX, usted puede ver el resumen de tráfico en cada capa de la red.
nota: La información desplegada en la pestaña de MAC depende de su topología:
Estadísticas Ethernet MAC
Estadísticas token ring MAC

El ancho de la columna de la tabla de host puede ser ajustada para encajar en su vista. Usted puede pulsar el botón y puede arrastrar el divisor de la columna a la izquierda o puede estrechar o ensanchar la anchura de la columna.

Para acceder a los comandos adicionales, apriete el botón derecho del ratón en ver tabla de host para plantear el menú de contexto:

Pause update (pausar actualización) suspende tabla de host contadora de actualización temporalmente.
Refresh (refresco) se Refresca la pantalla inmediatamente.
Reset borra todos los contadores en la tabla de host.

Capture Starts capture(captura de Salidas). Está configurado para capturar cualquier paquete enviado y de la estación seleccionada.
Define Filter (Definir Filtro) Abre la caja de diálogo de definir Filtro. El par de dirección de hardware es configurado automáticamente con la dirección de cualquier estación de hardware puesta.
Export (exportar) guarda los datos de la tabla de host en un archivo de extensión CSV.
Properties (propiedades) Abre una caja del diálogo para cambiar la opciones de vista de la tabla de host. Usted puede mostrar cualquier dirección del hardware de la estación o nombre simbólico.
Active Tools (Herramientas activas) Proporcionan el acceso para hacer Ping, trazo de ruta, DNS Lookup, finger y Whois.

ver detalle de tabla

La vista de detalle de proporciona un resumen rápido del tipo de protocolo la capa más alta y su carga de tráfico transmitida dentro y fuera de cada nodo de la red en el tiempo real. Seleccionando la pestaña MAC, IP, o IPX, usted puede ver un resumen del tráfico en cada capa de la red.

ver gráfico de barras

Revela el tope-N de los nodos del host más ocupados en tiempo real. Usted puede ver el tope-N de tráfico del host de la MAC, IP, o IPX.

nota: Por defecto, la tabla de host muestra los 10 nodos más ocupados en la red. Para cambiar la escena predefinida, pulse el botón TopN de la pestaña Chart.

Ver de gráfico pastel

Revela el tope-N de los nodos de host más ocupados por medio de porcentajes relativos de la carga total del tope-N de tráfico.

También vea:
Ver tabla de host - Adaptadores WAN



## Ver tabla de host - adaptadores WAN

La tabla de host proporciona un análisis rápido de las estadísticas de tráfico recolectado para cada nodo de host en el tiempo real. Para los adaptadores WAN (adaptador LM2000 o el adaptador HSSI), usted puede ver el tráfico a la capa link. El nombre exacto de la capa link cambiará dependiendo del protocolo de encapsulación seleccionado en las opciones de la caja de diálogo.

· Si usted habilita SNA de SDLC, usted puede ver el tráfico por direcciones SDLC.

· Si usted habilita X.25, usted puede ver el tráfico por los Números de Llamada Lógica (LCNs).

· Si usted habilita Frame Relay, usted puede ver el tráfico por los Circuitos Virtuales. Usted también puede ver selectivamente sólo el tráfico de capa de red en las capas IP o IPX.

· Si usted habilita Router/Bridge, usted puede ver el tráfico por direcciones HDLC.

La tabla de host tiene cuatro vistas diferentes - tabla outline, tabla detallada, gráficos de barras, o gráfico de pastel.

ver tabla outline

Mantiene varias estadísticas para cada nodo de la red en tiempo real. La información desplegada en la tabla de outline depende del protocolo de encapsulación actualmente seleccionado en las opciones de la caja de diálogo.

· pestaña SDLC

· pestaña LCN

· pestaña Virtual Circuits (Circuitos Virtuales)

· pestaña HDLC

El ancho de la columna de la tabla de host puede ser ajustada para encajar en su vista. Usted puede pulsar el botón y puede arrastrar el divisor de la columna a la izquierda o puede estrechar o ensanchar la anchura de la columna. Para acceder a los comandos adicionales, apriete el botón derecho del ratón en ver tabla de host para plantear el menú de contexto:

Pause update (pausar actualización) suspende tabla de host contadora de actualización temporalmente. Refresh (refresco) se Refresca la pantalla inmediatamente. Reset borra todos los contadores en la tabla de host. Capture Starts capture(captura de Salidas). Está configurado para capturar cualquier paquete enviado y de la estación seleccionada. Define Filter (Definir Filtro) Abre la caja de diálogo de definir Filtro. El par de dirección de hardware es configurado automáticamente con la dirección de cualquier estación de hardware puesta. Export (exportar) guarda los datos de la tabla de host en un archivo de extensión CSV. Properties (propiedades) Abre una caja del diálogo para cambiar la opciones de vista de la tabla de host. Usted puede mostrar cualquier dirección del hardware de la estación o nombre simbólico. Active Tools (Herramientas activas) Proporcionan el acceso para hacer Ping, trazo de ruta, DNS Lookup, finger y Whois.

ver tabla detallada

Proporciona un resumen rápido del tipo de protocolo de la capa más alta y su carga de tráfico transmitida dentro y fuera de cada nodo de la red en el tiempo real.

ver gráfico de barras

Revela el tope-N de los nodos del host más ocupados en tiempo real.
nota: Por defecto, la tabla de host muestra los 10 nodos más ocupados en la red. Para cambiar la escena predefinida, pulse el botón TopN en la etiqueta Chart.

ver gráfico de pastel

Revela el tope-N de los nodos del host más ocupados por medio de porcentajes relativos de la carga total de tráfico de tope-N.

También vea:

· ver tabla de Host - Adaptadores LAN



## Clasificación de la Tabla de host

Una vista de una tabla de host clasificada despliega estaciones que están más o menos activas en una cierta categoría de estadísticas de la red.
Haciendo clic en encabezamiento de una columna de un campo contador selecciona la variable en la llave clasificada , y causará la clasificación de la entrada de la tabla de host en orden descendente. Pulsando el botón de nuevo clasificará la tabla en orden ascendente.
La tabla de host es actualizada cada diez segundos. Se reordena cada 60 entradas. Para cambiar estos parámetros, pulse el botón Properties (Propiedades) y entre los nuevos valores.



## Ver la matriz

Las matriz de estadísticas proporciona un análisis rápido de las estadísticas de tráfico de conversación recolectado en el tiempo real.
Para el trafico en LAN, usted puede ver el tráfico de la conversación en la capa MAC, o selectivamente ve sólo los IP o IPX.
Para los adaptadores WAN (adaptador LM2000 o el adaptador HSSI), usted puede ver el tráfico en la capa link. El nombre exacto de la capa link cambiará dependiendo del protocolo de encapsulación actualmente seleccionado en las opciones de la caja de diálogo.

· Si usted habilita SNA de SDLC, usted puede ver el tráfico por direcciones SDLC.

· Si usted habilita X.25, usted puede ver el tráfico por los Números de Llamada Lógica (LCNs).

· Si usted habilita Frame Relay, usted puede ver el tráfico por Circuitos Virtuales. Usted también puede ver selectivamente sólo el tráfico de capa de red en los IP o IPX.

· Si usted habilita Router/Bridge, usted puede ver el tráfico por direcciones HDLC.

La matriz de estadísticas tienen cinco vistas diferentes - mapa de tráfico, la tabla de contorno, la tabla de detalle, gráfico de barras y de pastel.

Mapa de tráfico

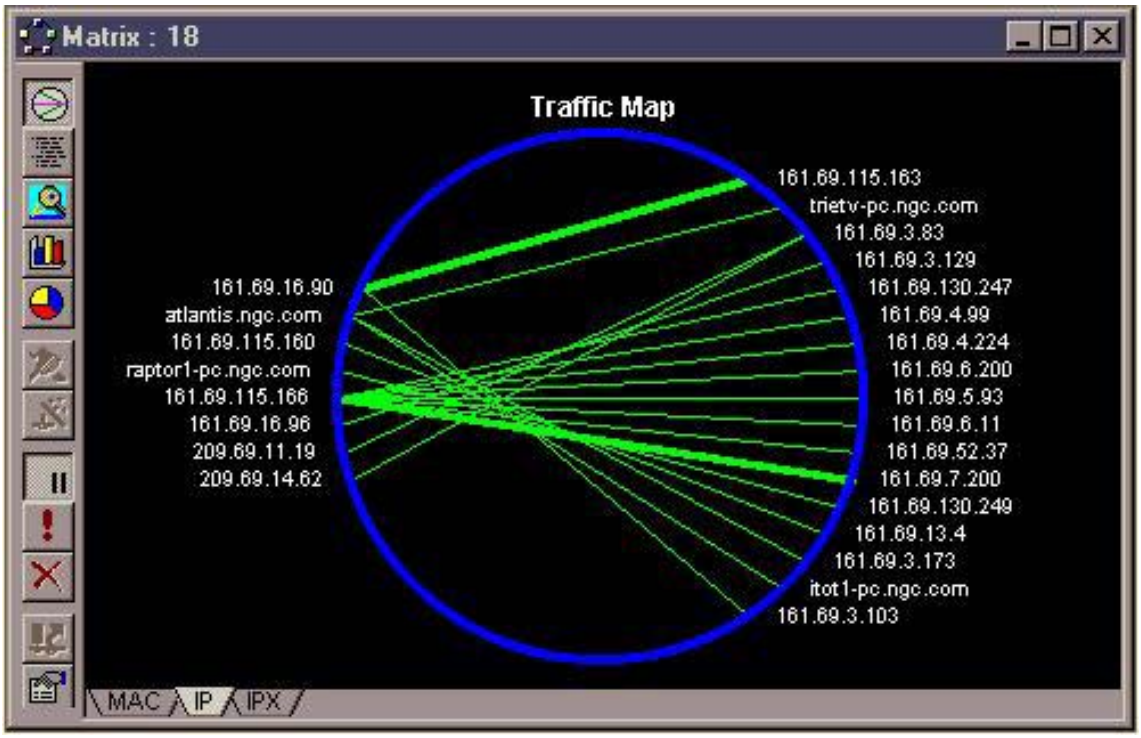
Muestra los modelos de tráfico de red en tiempo real. Da una presentación gráfica completa del modelo de tráfico entre los nodos de la red.

Además, usted puede filtrar fuera el tráfico no deseado seleccionando los nodos de la red de su interés.

El ejemplo siguiente muestra cómo usted puede desplegar el mapa de tráfico completo, entonces aisle el tráfico transmitido y los nodos de red de particulares.

Para mostrar el mapa de tráfico, pulse el botón en la ventana de Matrix (Matriz),

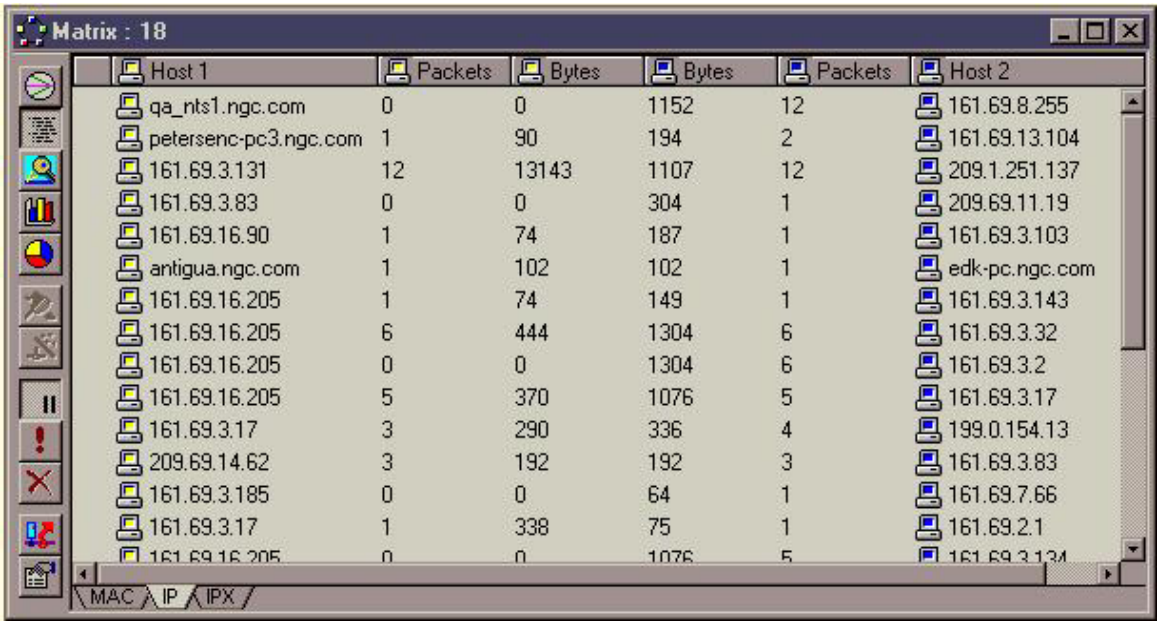
Para ver sólo la conversación o tráfico en tiempo real sólo en las capas IP o IPX, seleccione la pestaña apropiada en la ventana matrix (matriz). Un ejemplo del mapa de trafico de conversación por IP se muestra debajo,




Para ver el tráfico de conversación entre ciertos nodos, resalte el nodo de la red en el mapa de tráfico usando el botón izquierdo del ratón. Para seleccionar más de un nodo, mantenga oprimido la tecla Ctrl, y haga clic en los nodos adicionales. Pulse el botón derecho del ratón para invocar el menú de contexto de matriz, y seleccione el comando para mostrar el nodo seleccionado. El mapa de tráfico de matriz se muestra con sólo esos nodos seleccionados, y su conversación por modos.

ver la tabla outline

Proporciona un resumen rápido del total de bytes y paquetes transmitidos entre los pares de nodos de la red en tiempo real. Seleccionando MAC, IP, o IPX, usted puede ver el resumen de tráfico en cada capa de la red.



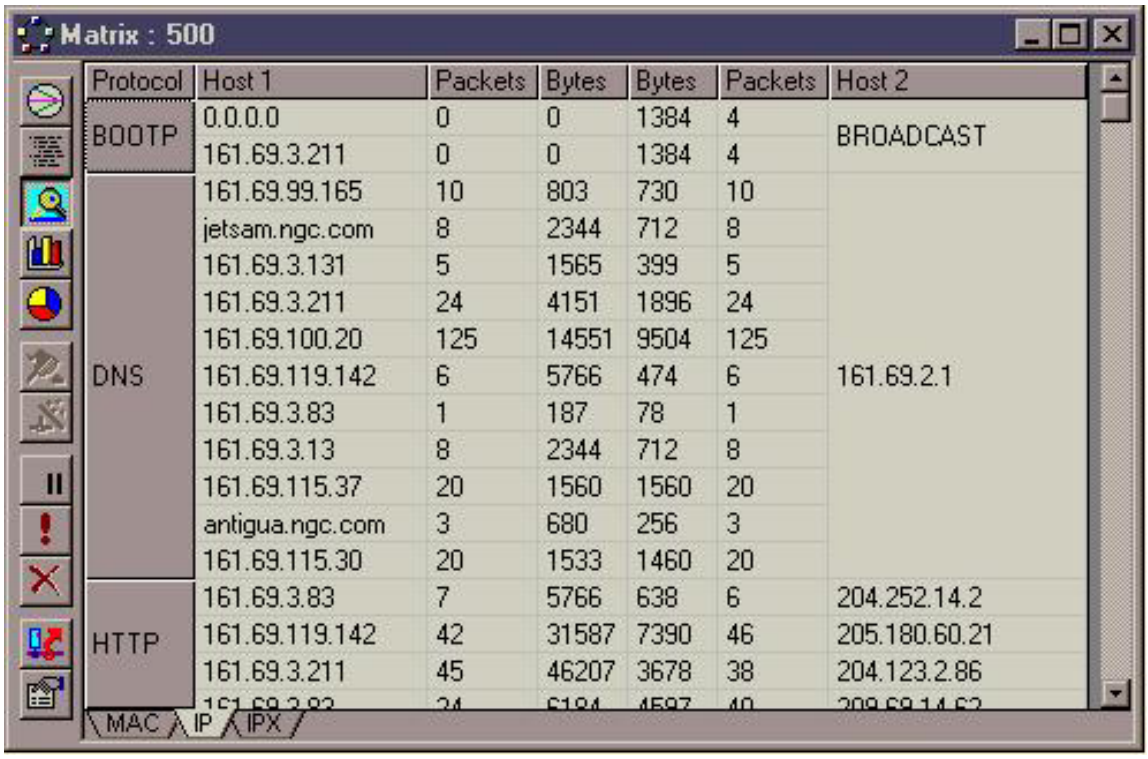

Para ver los mayores "habladores", simplemente pulse el botón del encabezado de la columna de los Paquetes de la tabla. Las columnas de Paquetes y Bytes de la izquierda de la tabla muestra el tráfico total enviado de la Estación Fuente a la Estación Destino, mientras las columnas en la derecha muestra el flujo de volumen de tráfico del Destino a la Fuente.

Para acceder a los comandos adicionales, haga clic en el botón derecho del ratón en la vista de tabla outline del menú del contexto:

Pause Update (Actualización) suspende la actualización de la tabla de Matriz contadora temporalmente.
Refresh Refresca la pantalla inmediatamente.
Reset borra todos los contadores en la tabla de Matriz.
Capture starts filtra cualquier paquete enviado de un par de direcciones de estación seleccionadas.
Define filter (Definir el Filtro) Abre la caja de diálogo definir Filtro.
Export (exportar) guarda los datos de la tabla de Matriz en un archivo de formato CSV.
Properties (propiedades) Abre una caja del diálogo para cambiar las opciones de vista de la tabla de matriz. Usted puede mostrar la dirección del hardware de la estación o el nombre simbólico de estación.

Ver tabla detallada

Proporciona un resumen rápido de tipo de protocolo de la capa más alta y su carga de tráfico transmitida dentro y fuera de cada par de nodos en conversación en tiempo real. Seleccionando el MAC, IP, o IPX, usted puede ver el resumen de tráfico por cada capa de la red. El ejemplo siguiente muestra una vista de la tabla de matriz detallada IP.




| Protocol | Host 1 | Packets | Bytes | Bytes | Packets | Host 2 |
|---|---|---|---|---|---|---|
| BOOTP | 0.0.0.0 | 0 | 0 | 1384 | 4 | BROADCAST |
| | 161.69.3.211 | 0 | 0 | 1384 | 4 | |
| DNS | 161.69.99.165 | 10 | 803 | 730 | 10 | |
| | jetsam.ngc.com | 8 | 2344 | 712 | 8 | |
| | 161.69.3.131 | 5 | 1565 | 399 | 5 | |
| | 161.69.3.211 | 24 | 4151 | 1896 | 24 | |
| | 161.69.100.20 | 125 | 14551 | 9504 | 125 | |
| | 161.69.119.142 | 6 | 5766 | 474 | 6 | 161.69.2.1 |
| | 161.69.3.83 | 1 | 187 | 78 | 1 | |
| | 161.69.3.13 | 8 | 2344 | 712 | 8 | |
| | 161.69.115.37 | 20 | 1560 | 1560 | 20 | |
| | antigua.ngc.com | 3 | 680 | 256 | 3 | |
| | 161.69.115.30 | 20 | 1533 | 1460 | 20 | |
| HTTP | 161.69.3.83 | 7 | 5766 | 638 | 6 | 204.252.14.2 |
| | 161.69.119.142 | 42 | 31587 | 7390 | 46 | 205.180.60.21 |
| | 161.69.3.211 | 45 | 46207 | 3678 | 38 | 204.123.2.86 |

gráfico de barras

Revela el tope-N del par de nodos en conversación más ocupados en tiempo real. Usted puede ver tope-N del tráfico en MAC, IP, IPX.

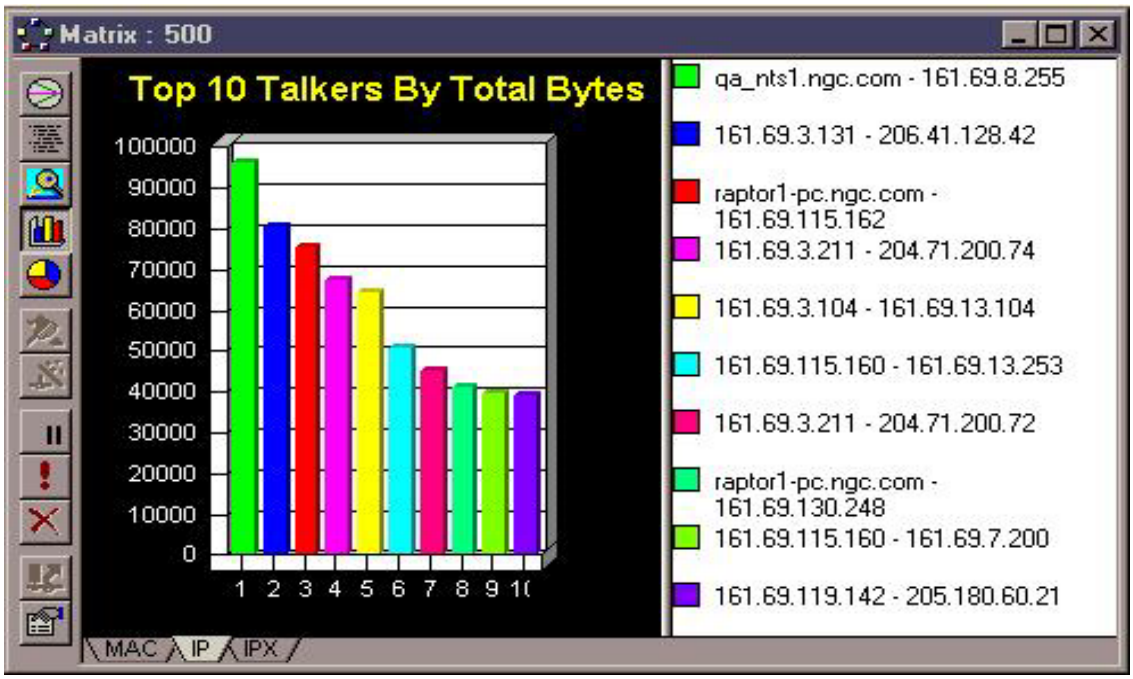
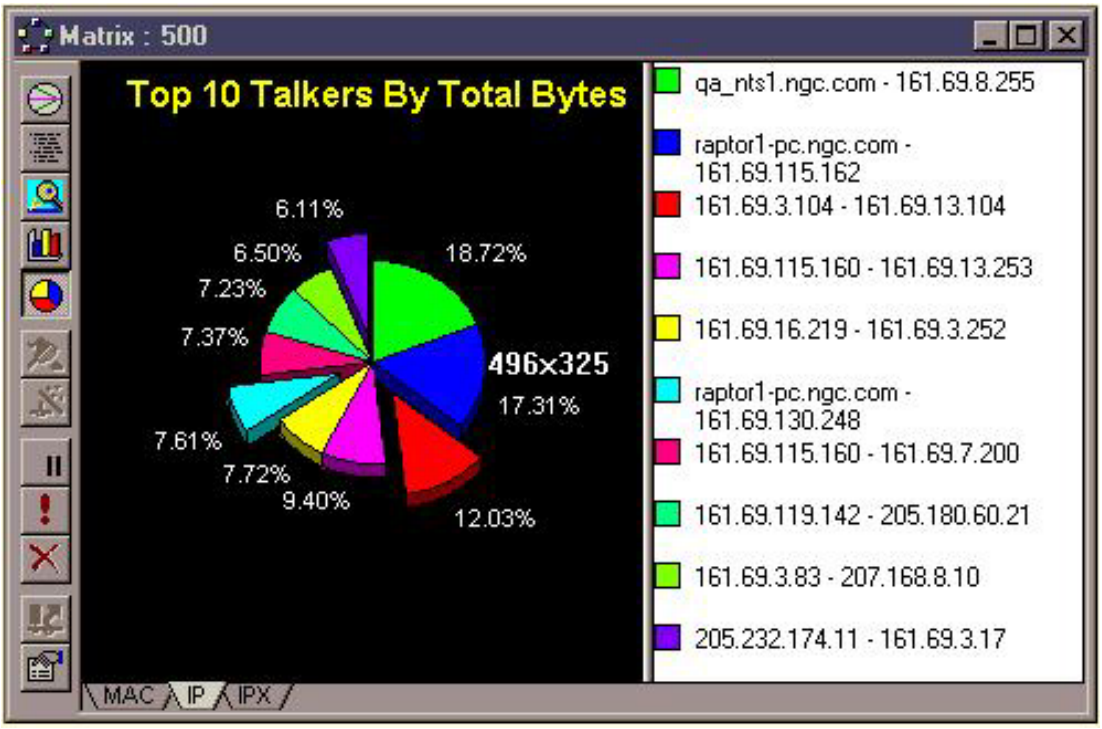


Gráfico de pastel

Revela el tope-N del par de nodos en conversación más ocupados en su carga de porcentaje relativa del total de tráfico de tope-N.






## HISTORIAL DE ESTADISTICAS

### Vista rápida del historia

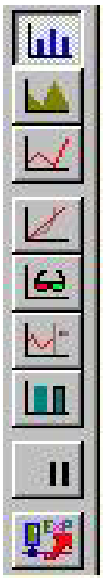
El historial graba las actividades de la red durante un período de tiempo. Usted puede usar los datos grabados para establecer una red de ejecución de línea principal, la cual lo ayuda a ubicar los umbrales para activar las alarmas cuando las actividades de la red son fuera de lo normales. El historial muestra datos que también son usados para determinar los cambios a largo plazo en la red o para que usted pueda planear una expansión de la red en un futuro.
Usted puede monitorear concurrentemente 10 actividades de la red. Las estadísticas del historial múltiple pueden iniciarse para la misma actividad de la red, para que los dos puedan grabarse a un corto término simultáneamente.

Los eventos de la red disponen del historial que muestra el monitoreo acorde con el tipo de adaptador que usted ha seleccionado en la caja de diálogo adapter (Adaptador). Por ejemplo, al supervisar una red token ring, usted puede monitorear el historial de varios tipos de marcos de token ring, mientras que al monitorear una red frame relay, usted puede supervisar un historial de varios tipos de marcos frame relay (como los marcos LMI). Los exactitud de los eventos varía de un adaptador a otro.

## Personalizando la Vista de Muestras del Historial

Cada ventana de muestra de Historial contiene una barra de herramientas que le permite cambiar el despliegue de la muestra de Historial. Usted puede mostrar los datos de la muestra en una barra, línea, o mapa del área. Usted puede desplegar el mapa en 3D o 2D, con o sin una leyenda, y con o sin un borde.
Use la barra vertical para ajustar la escala vertical del mapa del gráfico. Use la barra horizontal para ver los datos del historial capturados más temprano o más tarde.

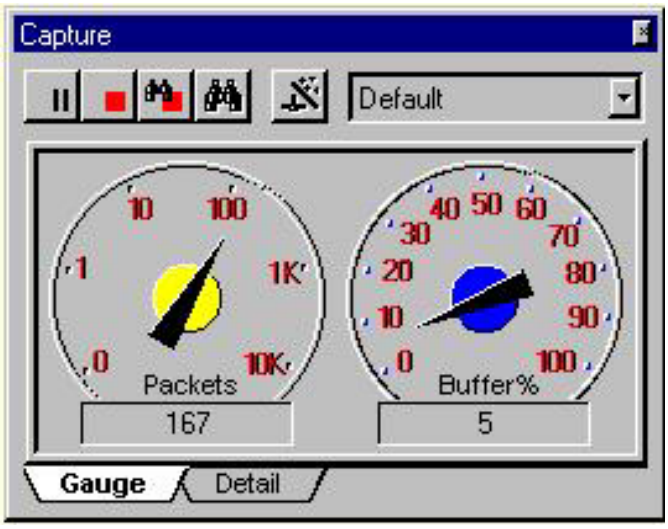




## CAPTURA DE PAQUETES

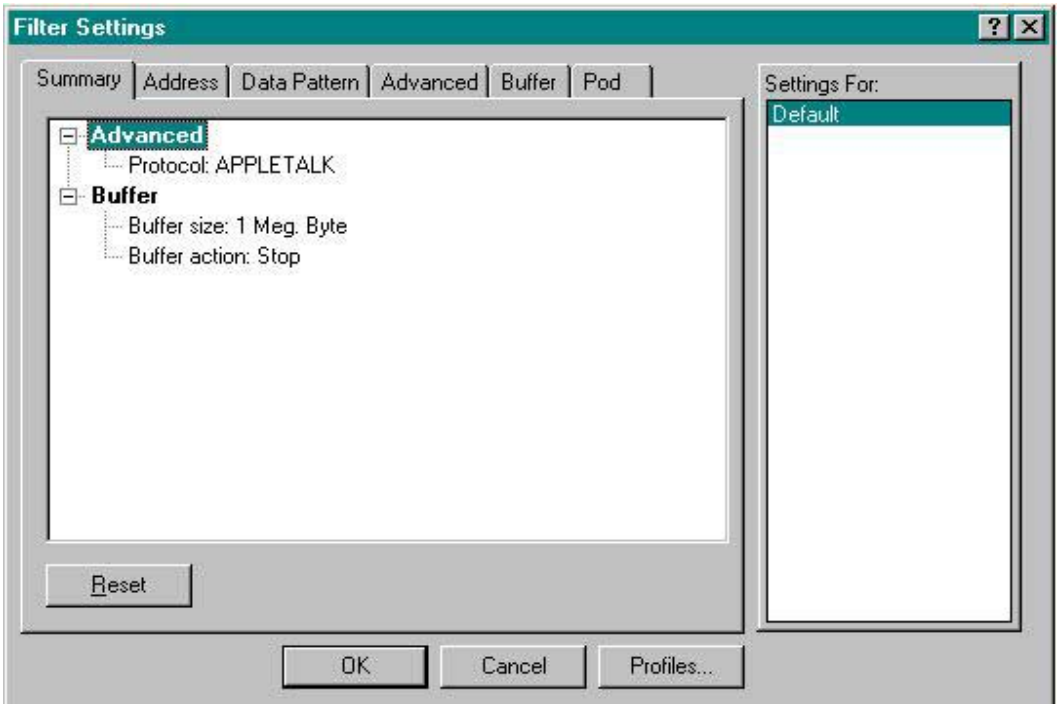
## Ventana de panel de captura

La Captura del paquete le permite capturar los paquetes y guardarlos en la memoria, y puede detener la captura del paquete a su discreción. Después, usted puede desplegar estos paquetes y puede examinar su contenido. Pulsando el botón Defina el Filtro, usted también puede definir o puede cambiar el criterio de la captura.




## Definiendo los filtros de captura

Pulse el botón  Defina el Filtro para abrir las la caja de diálogo Escenas del Filtro. La caja de diálogo Escenas del Filtro le permite definir los filtros de la captura para coleccionar la información específica de la red. Cuando usted abre primero la caja de diálogo Escenas del Filtro, la etiqueta de resumen aparece, listando las escenas actuales en las otras etiquetas de la caja de diálogo Escenas del Filtro.



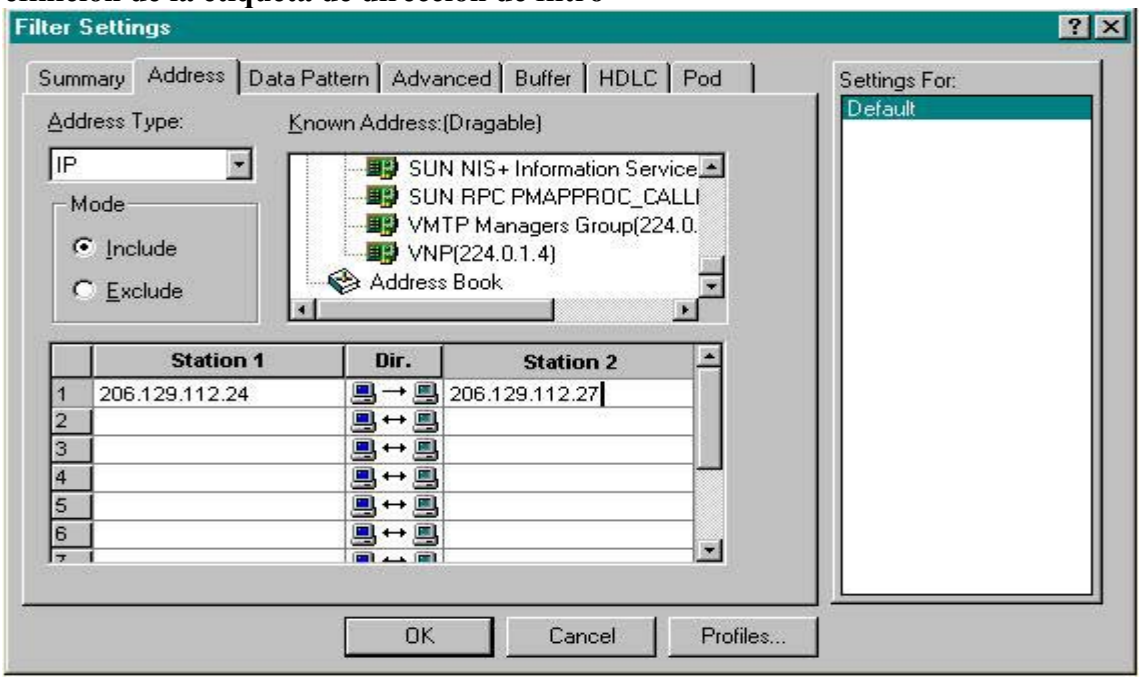
La caja de diálogo Escenas del Filtro incluye las siguientes etiquetas adicionales:
- La etiqueta de Dirección que le permite definir los filtros para capturar datos transmitidos entre los nodos de la red (o pares de dirección)
· La etiqueta de Modelo de Datos que le permite definir filtros que capturan marcos que emparejan las reglas de modelos de datos unidos por AND/OR/NOT los operadores lógicos
· La etiqueta Avanzada, que le permite definir filtros que capturan marcos que pertenecen a uno o más grupo(s) de protocolos. También le permite poner los filtros para marcos que toman un rango de tamaño especificado y los varios tipos de marco de protocolo-específicos (por ejemplo, paquetes del habla en una red de Ethernet).
· La etiqueta de buffer que le permite poner varias opciones globales que relacionan al tamaño del buffer de la captura y qué acciones deberían tomar cuando el tamaño máximo del buffer de la captura llega al máximo.
· Las varias etiquetas WAN (SDLC, X.25, Frame Relay, o HDLC) permiten definir filtros que capturan los tipos del marco WAN protocolo-específicos. Las etiquetas WAN sólo están disponibles cuando usted está capturando de un adaptador WAN (el adaptador de LM2000 o el adaptador de HSSI). El nombre exacto de la etiqueta WAN cambiará según el protocolo del encapsulacion especificado en la caja de diálogo de Opciones.
· La etiqueta POD sólo es pertinente si usted está acostumbrando a una interfase de red POD externa para capturar de una red (por ejemplo, la Network Associates Full Duplex Ethernet POD). Le permite especificar qué acción debe tomarse cuando el buffer de la captura interior del POD está lleno.

Los filtros de modelo de datos proporcionan un método genérico de definir y documentar condiciones del filtro que no pueden definirse por la dirección y los filtros protocolares.

Cuando usted define un filtro que requiere más de un tipo del filtro, por ejemplo, la dirección y los filtros protocolares, hay una operación Booleana AND implícito en la definición del filtro. Es decir, un paquete debe contener la dirección y la especificación del filtro de protocolo antes de que se capturara.

Cada escena de la captura puede darse y puede nombrarse y puede ahorrarse en un perfil. El Sniffer pro da los apoyos y salva los múltiples perfiles. Usted puede recuperar y aplicar un perfil de captura previamente definido antes de que usted active la captura.

## Definición de la etiqueta de dirección de filtro



Usted usa la caja de diálogo Escenas del Filtro, etiqueta de Dirección para definir los filtros para capturar datos transmitidos entre los nodos de la red especificados (o pares de dirección). para colocar los filtros de dirección, pulse el botón en la caja de diálogo Escenas del Filtro, etiqueta de direcciones.

Para poner un filtro de Dirección:
1. Use el campo Tipo de Dirección para especificar el tipo de dirección que usted quiere filtrar.
2. Use el campo Modo para especificar si usted quiere incluir o excluir el tráfico especificado.
3. La caja de Dirección Conocida ya incluye direcciones conocidas al Sniffer pro (incluyendo aquellos en su Libro de Dirección). Usted puede pulsar el botón y puede arrastrar las direcciones de la caja de Dirección en los campos Estación 1 o Estación 2 para filtrar en estas direcciones. Si usted no quiere pulsar el botón y arrastrar las direcciones conocidas, usted también puede agregar manualmente las direcciones poniendo su cursor en el apropiado campo y tecleando.
4. Una vez usted ha especificado el par de direcciones en que usted quiere filtrar, pulse el botón en el botón de dir. para especificar en que direcciones usted quiere capturar el tráfico (de Estación 1 para Estación 2, de Estación 2 para Estación 1, o en ambas direcciones).
5. 5 En la figura sobre, nosotros hemos puesto un filtro de dirección para capturar el tráfico de la estación IP 206.129.112.24 a la dirección IP 206.129.112.27, pero no en la dirección inversa.

## Definición de la etiqueta filtro modelo de datos

Invoque la etiqueta Filtro Modelo de Datos pulsando la caja de diálogo etiqueta de Modelo de Datos. Usted puede definir un filtro de modelo de datos para capturar sólo esos paquetes que emparejan el criterio de modelo de datos que usted especifique.
Un filtro de modelo de datos puede crearse de un solo modelo de datos o de definiciones de modelo de datos múltiples que se conectan juntos por AND/OR/NOT operadores Boléanos. Un filtro complejo puede contener no más de 20 operadores Boleanos y modelos de datos.

Un modelo de datos se define por una sucesión particular de pedazos, la longitud de estos pedazos, y la posición del desplazamiento del modelo dentro del paquete. Usted tiene la opción de especificar el desplazamiento del principio del paquete lleno o del primer límite de nivel de protocolo. La longitud de modelo de datos máxima es 32 octetos.
La situación de octeto de principio de un límite de protocolo del paquete puede variar, dependiendo del tipo de medios de comunicación, (Ethernet, Token ring), o los formatos DLC (Ethernet II, 802.2, 802.2 SNAP) que usa. El protocolo de IPX es un ejemplo bueno. Empieza el desplazamiento en el byte 14 en un paquete tipo Ethernet II, pero en el byte 17 en un paquete del tipo 802.2. Desde que el Sniffer reconoce que existen varios tipos de formatos DLC, él puede marcar el límite protocolar correctamente, mientras usa el límite de la capa protocolar como una situación de arranque para calcular el desplazamiento, le permite capturar los paquetes protocolares con un filtro modelo de los diferentes medios de red o con diferentes formatos DLC.

Facilita la definición de un modelo de datos, el Sniffer le permite a usted 'copiar' el modelo de datos que ha escogido de un paquete conocido. Al hacer esto, usted debe en el paquete visualizar la decodificación, y ha seleccionado un paquete particular antes de que usted lo invoque Defina el filtro profiler. Use Add Pattern/Set Data en la etiqueta de Modelo de Datos, copiar un campo de dato conocido del paquete descifrado en los campos de modelo de datos. Esto calculará el desplazamiento y longitud automáticamente, llenará el modelo de datos, y hará pensar en un nombre del campo predefinido.

Use AND/OR/NOT operadores de Boleanos para construir un filtro de modelo de datos complejo. El resultado se despliega en un árbol-como un diagrama que muestra las relaciones lógicas.
La mejor manera de aprender a construir un filtro Boleano de modelo de datos es empezar de un filtro de modelo de datos simple. El primer paso es apuntar las relaciones lógicas en una ecuación Boleana. Luego, clarificar la anterioridad del funcionamiento Boleano usando el paréntesis, para que la última ecuación que usa un diagrama del binario-árbol pueda construirse.

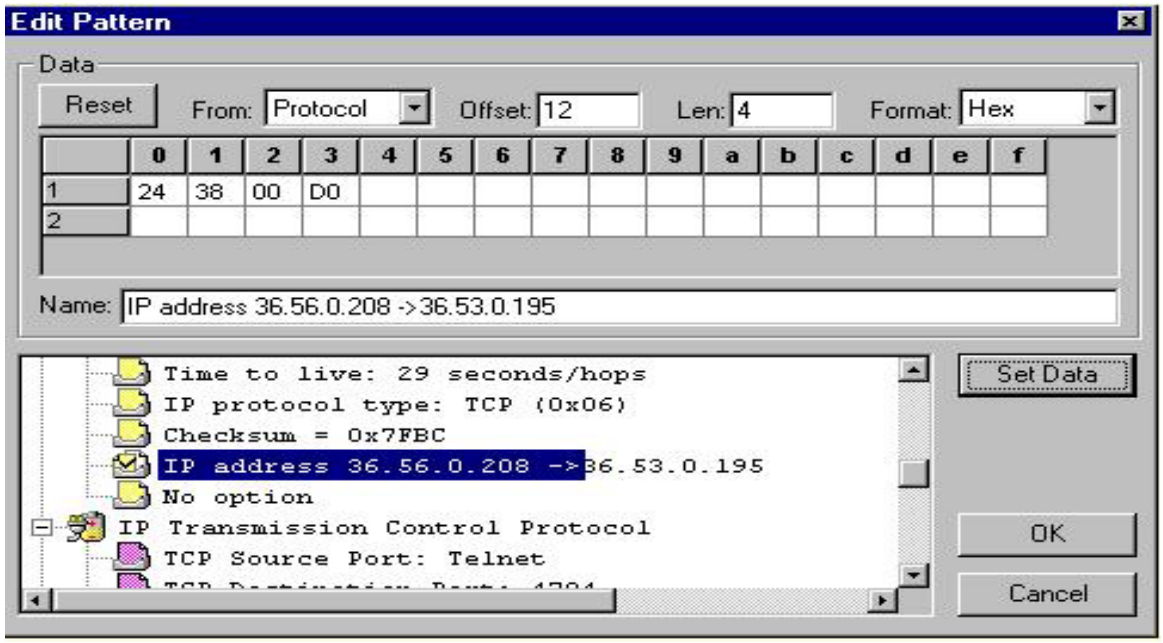
El ejemplo siguiente demuestra cómo construir el filtro de la muestra, Mi Subnet. (My Subnet is also listed in the sample Boolean Data Pattern filters supplied in Sniffer Pro capture profiles.)
Suponga que usted quiere capturar todo el tráfico IP excepto el tráfico de subnet 36.56.0. El primer paso es apuntar un modelo de datos ecuación Boleana que representa este funcionamiento:

Not (Src Subnet 36.56.0 OR Dest Subnet 36.56.0)

Si usted ya tiene un archivo capturado que contiene esta dirección subnet, usted debe abrir este archivo y debe seleccionar el paquete que contiene la fuente de dirección subnet 36.56.0. Esto aliviará substancialmente después el funcionamiento de entrada de datos, cuando usted define el modelo de los datos para el subnet 35.56.0.
Luego, comience la definición del filtro de modelo de datos siguiendo estos pasos:

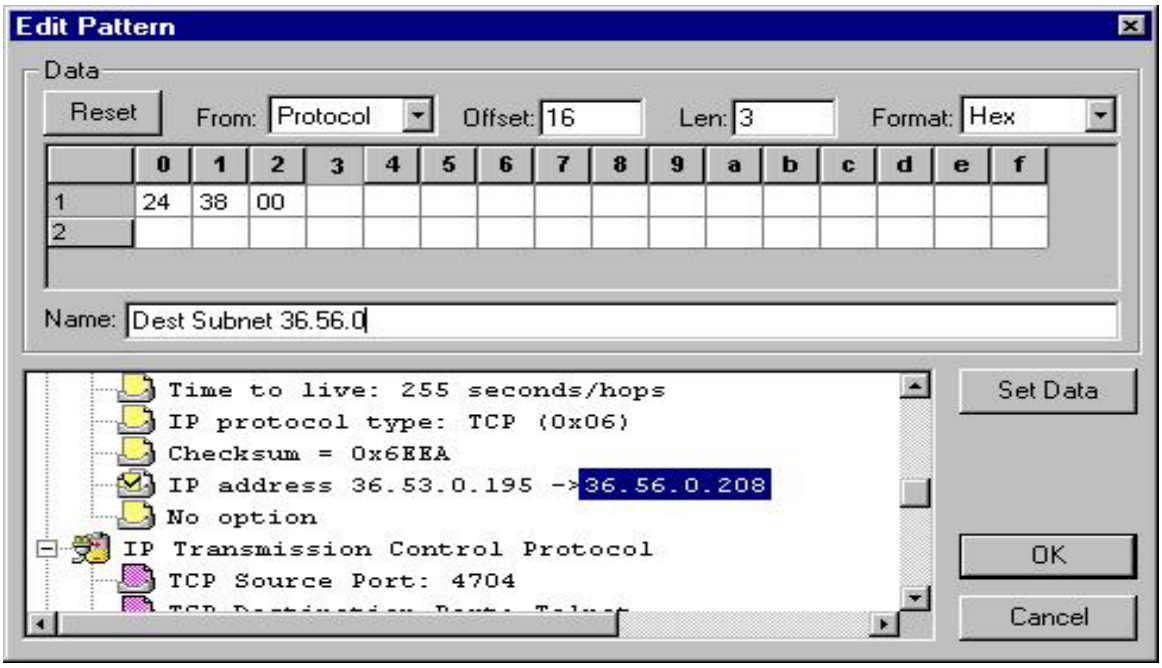
1. de la ventana de la Captura, click para abrir la caja diálogo Escenas del Filtro.

2. click en el botón Perfiles para abrir la Caja de diálogo Perfiles de la Captura.
3. click en el botón Nuevo. Entre en el nuevo nombre del perfil - por ejemplo, Mi Subnet. Pulse el botón OK.
4. click en el botón hecho para cerrar la caja de dialogo perfiles de la captura.
5. click la etiqueta Avanzada.
6. Seleccione IP de la lista de protocolos Disponibles. Esto se filtrará fuera cualquier paquete non-IP que podría tener el mismo modelo de los datos.
7. click en la etiqueta de Modelo de Datos. Un valor por defecto, operador AND se despliega.
8. click en el botón Añadir NOT para crear un operador NOT.
9. de la línea recientemente creada, pulse el botón el Añadir AND/OR para crear un nuevo operador AND unido al operador NOT.
10. click en el botón AND/OR para cambiar el ANSD a OR.
11. e la línea OR, pulse el botón Agregue Modelo para invocar el editor de la caja de diálogo del Modelo.
12. Desplace línea a línea el detalle para ver la ventana para localizar la dirección fuente IP que contiene subnet 35.56.0 y resaltar el campo.
13. Seleccione Protocolo en la lista. Esto le dirá al Sniffer pro que calcule la dirección fuente IP empezando del paquete de datos del protocolo IP.
14. click en el botón Conjunto de datos para decirle al Sniffer pro que complete el campo en la dirección fuente IP. En la caja de diálogo de Modelo aparecerá:

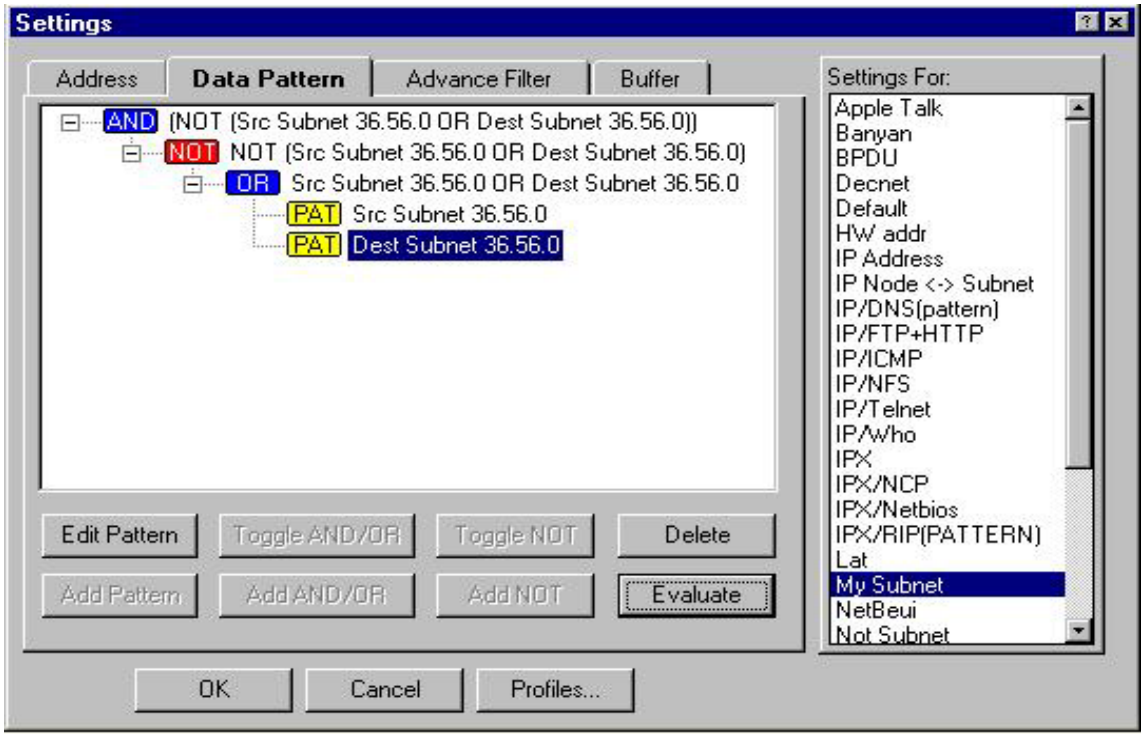



15. Cambiar Len (la longitud de subnet) de 4 a 3, y anular el 4 octeto del campo de modelo de datos.
16. Editar el nombre del campo a Src Subnet 36.56.0.
17. click OK. Un nuevo modelo del datos Src Subnet 36.56.0 se crea y es conectado al operador de OR.
18. click en el operador OR de nuevo para seleccionarlo.
19. click en el botón agregar Modelo para invocar otro editor de la caja de diálogo de Modelo.
20. click en el botón Conjunto de datos para decirle al Sniffer En pro que rellene un modelo de datos mudo (un placeholder) para el Dest Subnet y click OK.
21. click OK en la caja de diálogo Escenas de filtro de nuevo para salvar el filtro.
22. seleccionar el próximo paquete, incluyendo la dirección destino subnet IP del Paquete visualizado.
23. de la ventana de Captura, pulse el botón para llevar la propiedad de la caja de diálogo Defina Filtro para Mi Subnet.

24. click en la etiqueta de Modelo de Datos para desplegar el filtro de Modelo de Datos definido hasta ahora.
25. Momento culminante la segunda PAT (éste era el placeholder creado previamente) y pulsa el botón editar el Modelo para invocar la caja de diálogo editor de Modelo.
26. Desplace línea a línea el detalle para ver la ventana para localizar la dirección destino IP que contiene subnet 35.56.0. Resalte el campo.
27. seleccione Protocolo en la lista. Esto dirá al Sniffer pro que calcule la dirección destino IP empezando del paquete de datos del protocolo IP.
28. click en el botón conjunto de datos para decirle al Sniffer pro que complete el campo de dirección fuente IP.
29. cambiar Len (la longitud de subnet) de 4 a 3, y anula el 4 octeto del campo de modelo de datos.
30. revisar el nombre del campo, para que le muestra Dest Subnet 36.56.0. El Revisa la caja de diálogo de Modelo que aparecerá:




31. click OK. Un segundo modelo de los datos en Dest Subnet 36.56.0 se crea y conectó al operador de OR.
32. click en botón evaluar. La operación resultante No (Src Subnet 36.56.0 OR Dest Subnet 36.56.0) se muestra en la línea de la cima. En la etiqueta de filtro de modelo de datos aparecerá:

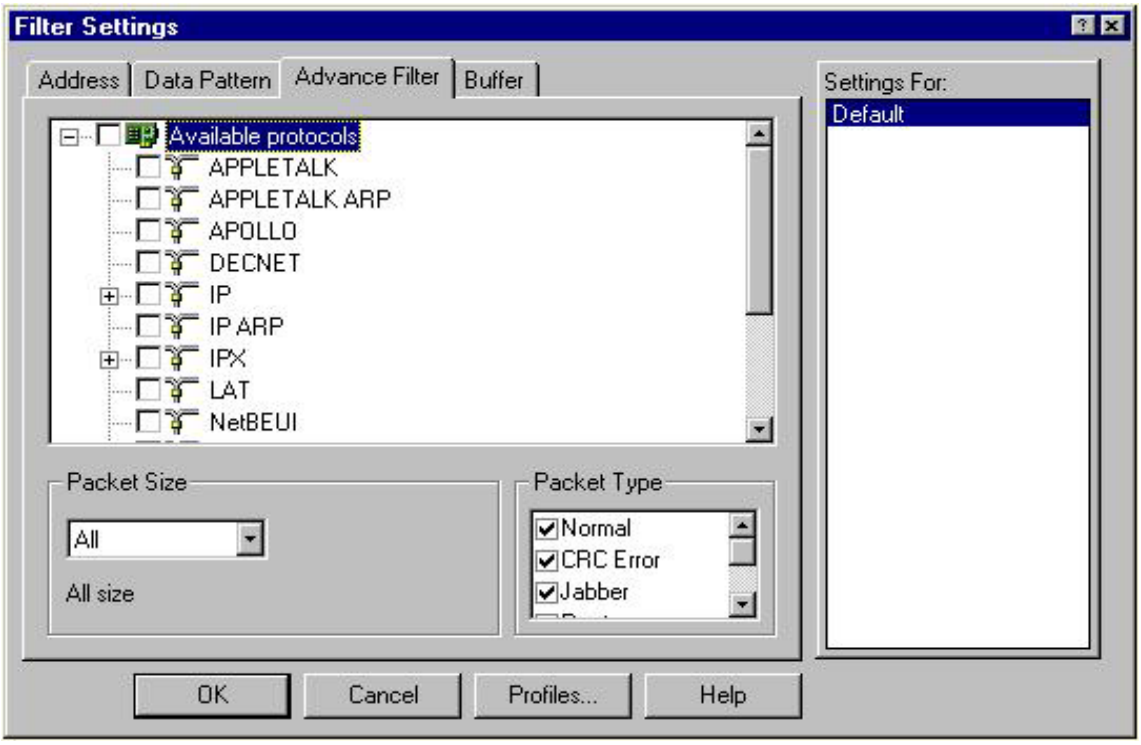



33. clic OK para salvar el filtro.

## Definición de la etiqueta de filtro avanzado

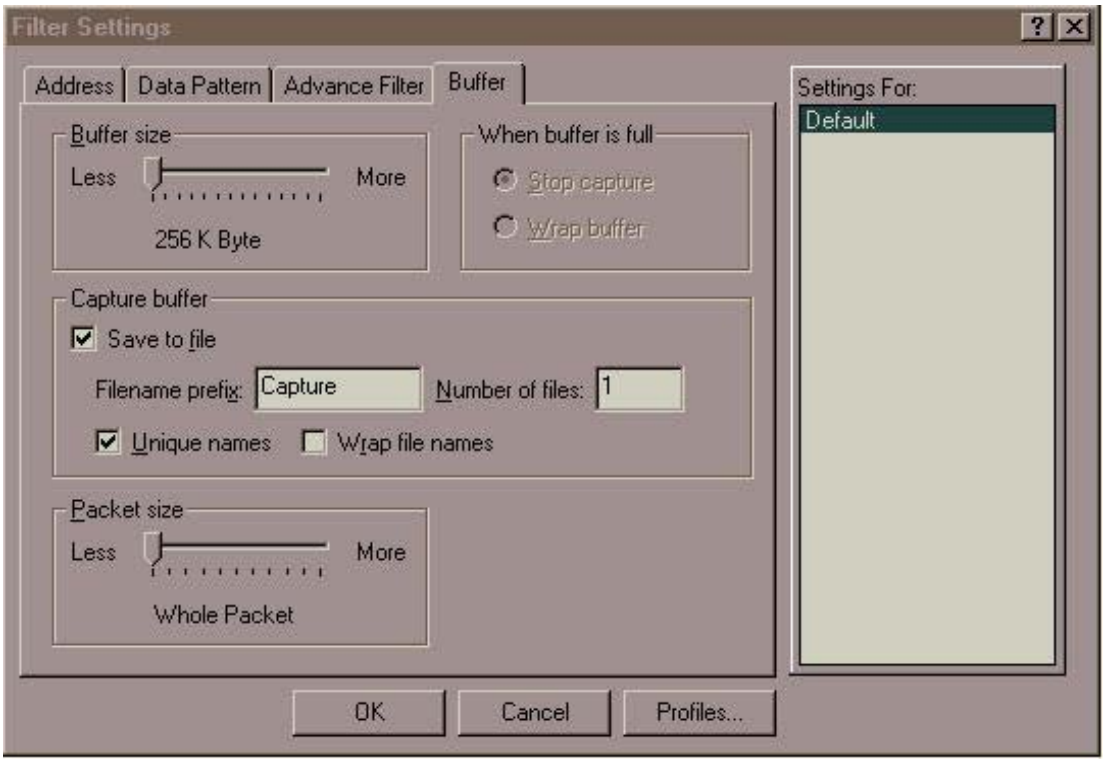
La etiqueta de filtro avanzado puede invocarse pulsando el botón el botón Defina Filtro, en la etiqueta Avanzada.
Usted puede seleccionar uno o más (primero) - o protocolos (segundo-nivel) para filtrar. Si un paquete corresponde a uno de los tipos protocolares seleccionados, se capturará en el buffer de la captura.
Usted también puede especificar un filtro de tamaño de paquete. Usted puede capturar paquetes basados en tamaño del paquete Igual, Mayor que, menos que, entre, o no entre ciertos rangos.
El filtro Protocolar para IP incluye los protocolos de capa de transporte TCP, UDP, ICMP, IGMP, ISO-TP4, Hello, IP-VINES, OSPF, GGP, EGP, IGRP, así como TCP y UDP, protocolos de la capa de aplicación FTP, REXEC, RLOGIN, RSH, PRINTER, SMTP, Telnet, DNS, GOPHER,POP, HTTP, NNTP, NetBIOS, NFS, RPC, el X-WINDOW, BOOTP, TFTP, SNMP, BIFF, WHO, SYSLOG, RIP, y GDP.

El filtro Protocolar para IPX incluye los sub-protocolos como RIP,SAP, NCP, SPX, NBIOS, Diagnostic, Serialization, NMPI, NLSP, y SNMP.




## Definición de la etiqueta filtro buffer

Invocando la etiqueta Definición de Filtro, en la etiqueta Buffer




Tamaño del buffer

Usted puede seleccionar un tamaño del buffer para acomodar la montaña de tráfico de la red que usted desea capturar. Mueva el deslizador para seleccionar el tamaño de memoria para el buffer de captura.

Tips:
· Cuando usted cambia el tamaño del buffer, usted puede experimentar un retraso cuando el Sniffer asigna la memoria para el Buffer, sobre todo si usted especifica un buffer grande.

· Evitar especificar un buffer más grande que la cantidad de RAM disponible en su sistema.
La acción para buffer lleno

Escoja qué acción para tomar cuando el buffer de memoria está lleno. Usted puede elegir dejar de capturar o permitir que los datos se enrollen en el buffer. Cuando los datos se enrollan en el buffer, los paquetes más viejos se sobrescriben por los nuevos datos.

Salvar archivo

Usted puede poner los prefijos Filename. El número máximo de archivos permitido es 99,999.

Cada archivo es del tamaño como el buffer de captura lo ha definido. Por ejemplo, si usted selecciona los 4 MB el tamaño de buffer, cada archivo creado será 4 MB en el tamaño. (El último tamaño del archivo puede ser más pequeño que 4 MB.) Poniendo el tamaño del buffer entre 8 y 12 MB mejorará el acto de captura.

Usted puede seleccionar la Única opción de los nombres para garantizar que los nombres del archivo creado por la captura del paquete es único a guardarse en el mismo directorio. Pueden ahorrarse varias sucesiones de captura de paquete sin borrar las sucesiones más tempranas.

Por otra parte, la captura se detendrá una vez que alcanza el extremo del último archivo.

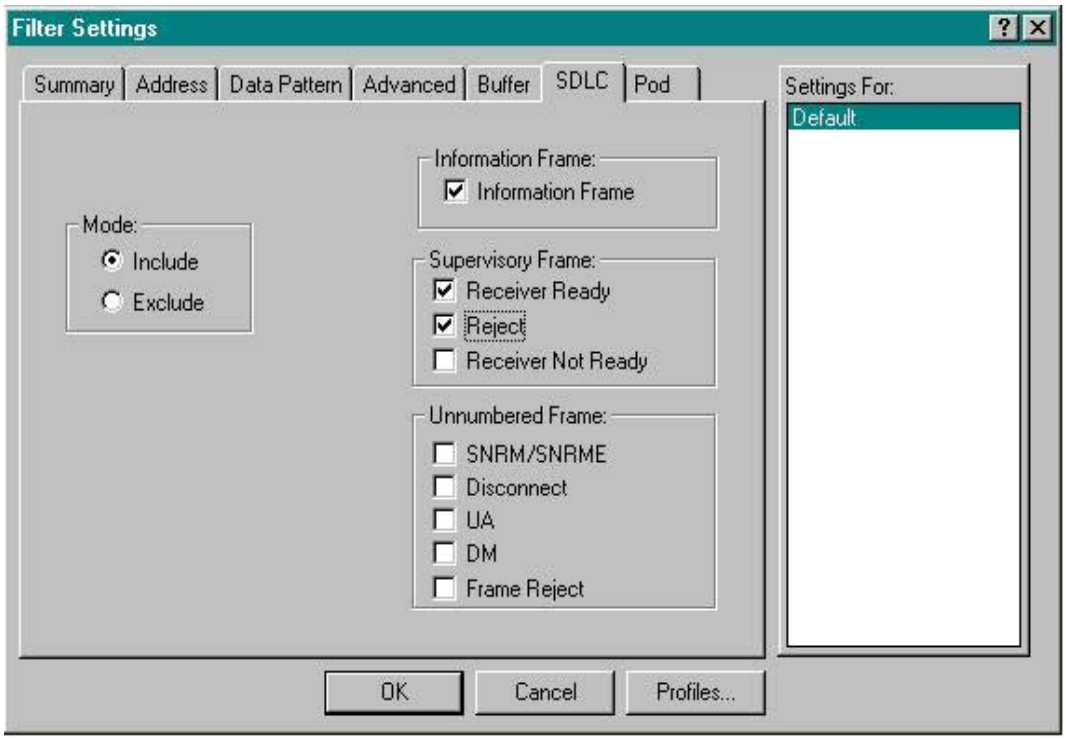
El tamaño del paquete

Seleccionando un tamaño del paquete más pequeño le permite ahorrar el espacio en el buffer, e ignora los datos innecesarios.

Mueva el deslizador para seleccionar el tamaño del paquete a ser capturado y guárdelo en el buffer. Un tamaño de paquete de datos mayor que el tamaño especificado se truncará. Usted puede seleccionar paquete Entero, 64, 128, 256, 512, 1024, 4096, 8192, o 16384 octetos.

## Pestaña Definición del Filtro SDLC

La pestaña SDLC permite especificar en la caja de dialogo varios tipos de marco SDLC que usted quiere incluir o excluir de la captura. La etiqueta SDLC está disponible cuando la Encapsulación se pone como SNA de SDLC en las Opciones de la caja de dialogo.




Usted puede incluir o puede excluir los siguientes tipos de marcos SDLC:
Marcos de información (I frames)

· Marcos de Información

Marcos de supervisión (S Frames)

- Receiver Ready (RR)
- Reject (REJ)
- Receiver Not Ready (RNR)

Unnumbered Frames (U Frames)

· SNRM /SNRME

· Disconnect

· UA

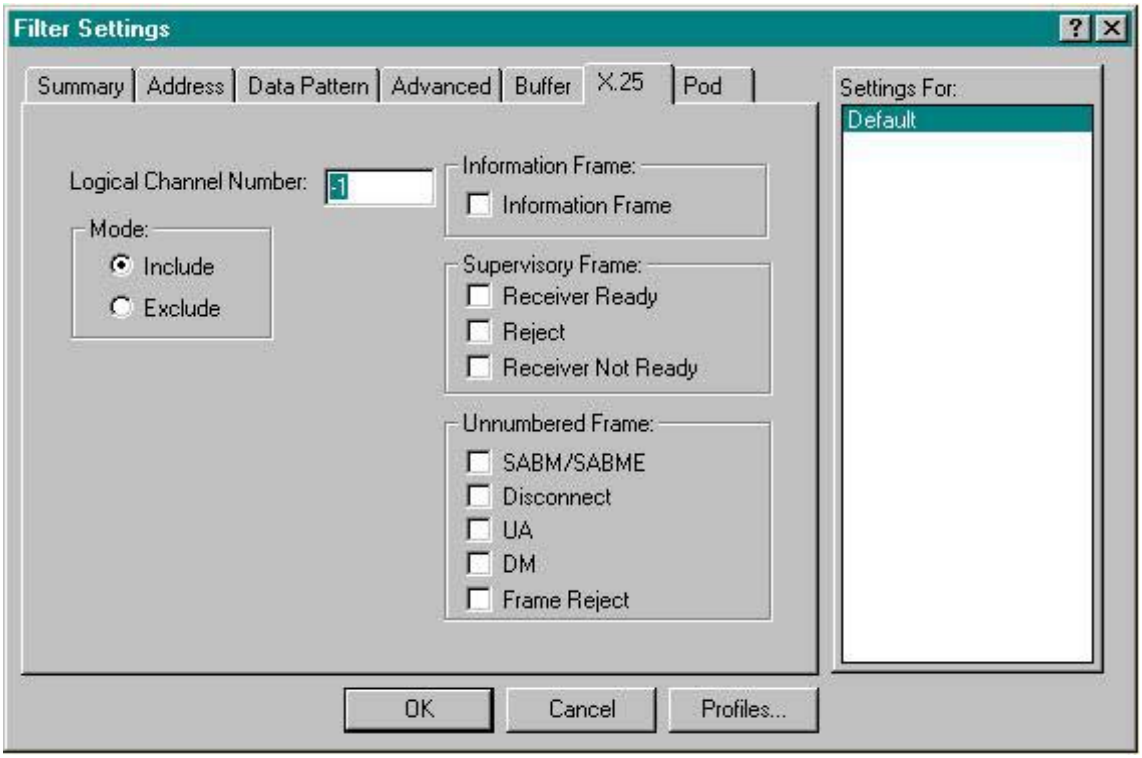
· DM

· Frame Reject



## Pestaña de Definición del Filtro X.25

La pestaña X25 permite especificar en la caja de dialogo varios tipos de marcos LAPB que usted quiere o incluir o excluir de la captura. La pestaña X.25
Está disponible cuando la Encapsulación se pone a X.25 en las Opciones de la caja de dialogo.




Antes de que usted especifique que marco quiere incluir o excluir, usted debe primero especificar el número del canal lógico en que usted quiere filtrar el tráfico en el campo de Número de Canal Lógico. Usted puede incluir o puede excluir los siguientes marcos tipo LAPB en el Número del Canal Lógico especificado.

Information Frames (I Frames)

- Information Frames

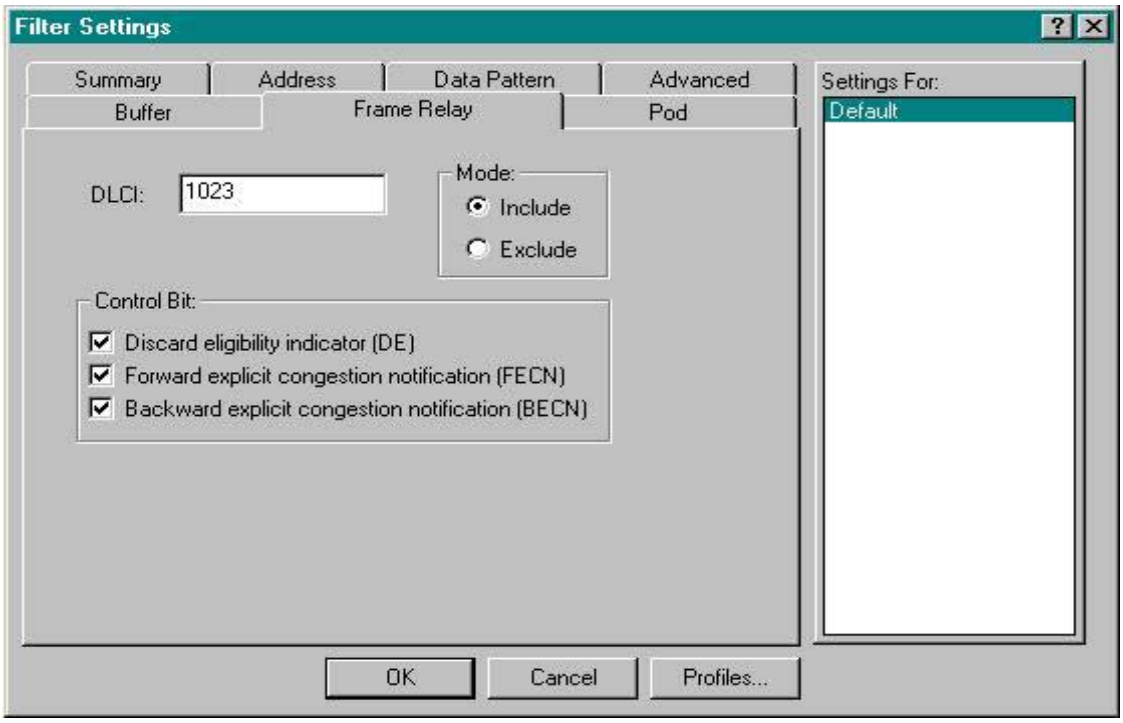
Supervisory Frames (S Frames)
- Receiver Ready (RR)
- Reject (REJ)
- Receiver Not Ready (RNR)

Unnumbered Frames (U Frames)
- SABM /SABME
- Disconnect
- UA
- DM
- Frame Reject



## Pestaña definir filtro Frame Relay

La pestaña de Frame Relay permite especificar en la caja de dialogo varios tipos de Marcos Frame Relay que usted quiere o incluir o excluir de la captura. La pestaña de Frame Relay está disponible cuando la Encapsulación se pone para Frame Relay en las opciones de la caja de diálogo.




Antes de que usted especifique que marco quiere incluir o excluir, usted debe especificar primero el DLCI en que usted quiere filtrar el tráfico en el campo de DLCI. Usted puede incluir o puede excluir los siguientes tipos de marco en el DLCI especificado.

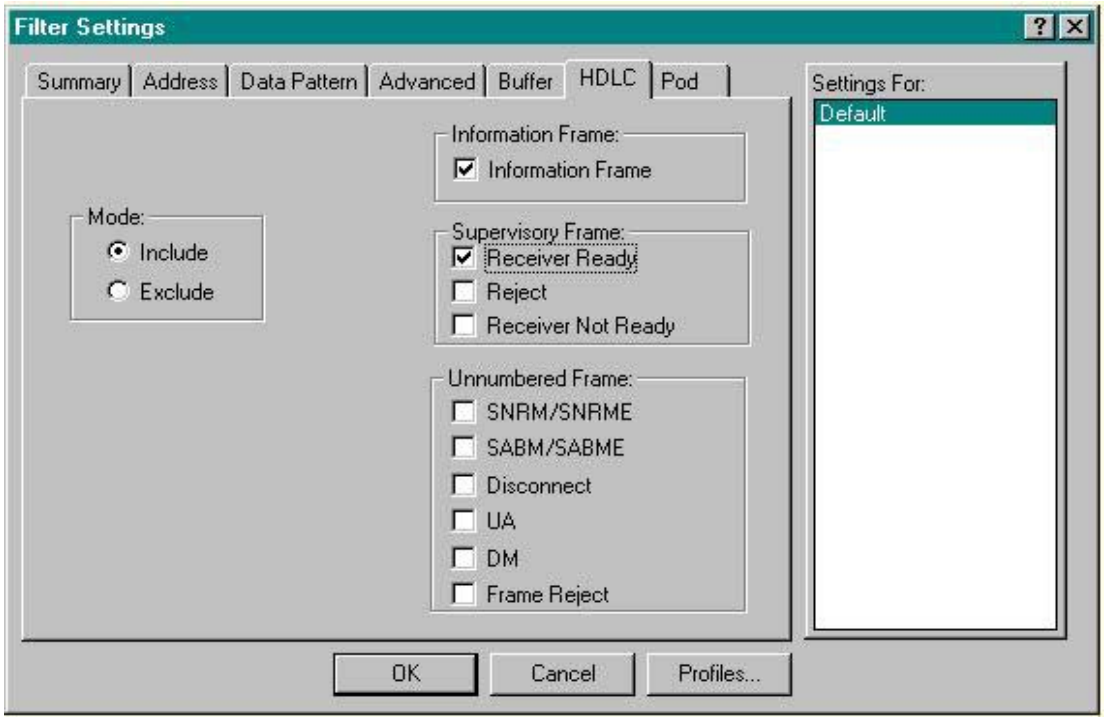
·Frames with the DE bit set to true.
·Frames with the FECN bit set to true.

·Frames with the BECN bit set to true.



## Pestaña Definir el Filtro HDLC

La pestaña HDLC permite especificar en la caja de dialogo  varios tipos de marcos HDLC que usted quiere o incluir o excluir de la captura. La etiqueta de HDLC está disponible cuando la encapsulación se pone a Router/Bridge en las Opciones de la caja de dialogo.




Usted puede incluir o puede excluir los siguientes tipos de marcos HDLC:

Information Frames (I Frames)
- Information Frames

Supervisory Frames (S Frames)
- Receiver Ready (RR)
- Reject (REJ)
- Receiver Not Ready (RNR)

Unnumbered Frames (U Frames)
- SNRM /SNRME
- SABM /SABME
- Disconnect
- UA
- DM
- Frame Reject

## Pestaña Definir Pod

La pestaña Pop permite especificar en la caja de dialogo qué acción debe tomarse cuando el buffer está lleno. Usted puede elegir para dejar de capturar, permitir que los datos sean capturados en el buffer de memoria, o dar una sugerir al usuario por una acción. Cuando los datos son capturados en el buffer, los paquetes más viejos se sobreescriben por los nuevos datos.
La pestaña Pop sólo es pertinente si usted está usando una interface Pop externa de red para capturar desde una red (por ejemplo, la Red Associates Full Duplex Ethernet Pod).



# DESPLEGAR EL PAQUETE

## Apreciación global de Packet Display

El Display del Paquete abre cuando usted detiene captura y despliega el BUFFER de la captura, o cuando usted abre un archivo de la captura. Usted puede abrir casos múltiples del Displaydel Paquete.

El Displaydel Paquete Descifra la etiqueta contiene tres hojas de vidrio separadas, Resumen, Detallan, y Hex.

La hoja Sumary muestra todos los paquetes en un línea-por-línea resumió formato con la información siguiente:

· Paquete Sucesión Número
· Paquete Estado
· Fuente Dirección
· Destino Dirección
· que la Capa Protocolar más Alta Interpretó
· la Información Sumary para la Capa Protocolar
- Longitud de · del Paquete (incluyendo 4-byte CRC)
· Time Relativo (de la salida del periodo de la captura)
- Delta de · Time (tiempo pasó del marco anterior)
· Time Absoluto (tiempo y fecha)

La hoja Detalle despliega los campos de detalle de capa protocolares interpretados en cada capa para el paquete actualmente resaltado.

La hoja de Hex muestra el paquete entero en Hex, y el ASCII respectivo, y vistas de EBCDIC.

Usted cambia resize verticalmente cada hoja pulsando el botón y arrastrando la barra del separador entre las hojas .

Usted puede realizar análisis estadístico en los datos en el buffer de la captura. Estas funciones se resumen debajo:

· Usted puede ver estadísticas de lamatrix en el MAC, IP, y niveles de IPX. Usted puede desplegar los resultados en un mapa de tráfico, la mesa del contorno, mesa de detalle, obstruye mapa, o mapa del pastel.

· El mapa de tráfico dematrix proporciona una vista del pájaro-ojo de conversaciones de la red, vista por carga de tráfico y el tipo protocolar.

· El Filtro Visual en el mapa de tráfico dematrix proporciona un método poderoso para filtrarse rápidamente fuera tráfico no deseado.
· Usted puede ver estadísticas del organizador para los datos en el MAC, IP, y niveles de IPX. Usted puede desplegar los resultados en una mesa del contorno, mesa de detalle, obstruya mapa, o mapa del pastel.

· Usted puede ver estadísticas de la distribución protocolares en el MAC, IP, y niveles de IPX. Usted puede desplegar los resultados en una mesa, obstruya mapa, o mapa del pastel.

· Usted puede ver información de la estadística sumary.

## Uso del teclado

Los apoyos de Displayde Paquete las llaves siguientes para navegar el buffer de la captura:

Page up A Vista la página anterior en la hoja activa
Page Down Abajo Vista la próxima página en la hoja activa
Cursor up Vista la línea anterior en la hoja activa
Cursor down Vista la próxima línea en la hoja activa
F2 búsqueda el próximo seleccionó (marcado) el paquete en la hoja Sumary
Shift+F2 búsqueda el anterior seleccionó (marcado) el paquete en la hoja Sumary
Control+F2 barra traviesa el paquete seleccionado entre seleccionó y estado del unselected
F3 búsqueda para el próximo caso de un del texto, modelo de los datos, o estado
Alt+F3 abren la Búsqueda Paquete diálogo caja
F4 in/out del zoom de un Decode pane.
F7 vista el paquete anterior en la hoja Sumary
F8 vista el próximo paquete en la hoja Sumary
Para aumentar al máximo la eficacia de examinar paquetes para detalles, nosotros recomendamos que usted:

1 ajusta el tamaño de Displayde Paquete, y hoja individual para aumentar al máximo el área viendo para sus intereses particulares.

2 seleccionan el paquete de arranque que usted quiere ver en la hoja pulsando el botón en él.

3 pulsan el botón la hoja de Detalle y usan al movimiento del cursor y Botones **Up/Page Abajo** las llaves para mover a través del buffer.

4 uso F7 para mover al paquete anterior. Acostumbre F8 al próximo paquete.

## Buscando paquetes

Usted puede buscar por paquetes en el Decodificador ventana por una cadena de texto, un cierto modelo de los datos, o adelanto a un paquete particular especificando su número.
Para buscar un paquete que empareja una cadena de texto:

1.seleccione FIND FRAME del menú DISPLAY o del menú del contexto (pulse el botón derecho del raton), para abrir y buscar los marcos de la caja de dialogo.

2 seleccionan la etiqueta del TEXT. Rellene la información, incluso el cordón del texto, el descifre campo para investigar en, y otros parámetros de la búsqueda.

3 pulsan el botón OK para empezar la búsqueda.

Si el cordón se encuentra, el paquete que contiene el modelo se desplegará en el Descifre Despliegue. Apriete F3 para buscar el próximo paquete.

Buscar y localizar un paquete que empareja un campo de los datos en un paquete conocido:

1 localiza y resalta un campo protocolar o un modelo de los datos en la hoja de Detalle del Descifre Despliegue.

2 selecione del menú Find Frame del menú display o contexto (vía un derecho-ratón pulse el botón), para abrir la Hallazgo Marco diálogo caja.

3 seleccionan la etiqueta de los Data. Abra el De la caja de la lista y selecciona Don ' t Care. Pulse el botón los Datos Fijos abrochan para abrir el detalle descifre vista del paquete.

4 seleccionan un modelo de los data o campo y pulsan el botón Set Data. El nuevo datos se pone en el área de modelo de datos. Ajuste los datos y la longitud si necesario, y pulsa el botón OK para empezar la búsqueda.

Si del modelo se encuentra, el paquete que contiene el modelo se desplegará en el Descifre Despliegue. Apriete F3 para buscar el próximo paquete.

Para buscar un paquete con un modelo de los datos conocido sin localizar el paquete primero, siga estos pasos:

1 Marco del Hallazgo Select del menu display, o del menú del contexto (vía un derecho-ratón pulse el botón), para abrir la Hallazgo Marco diálogo caja.

2 cambio el desplazamiento, clasifique según tamaño, o el campo de los datos si necesario, y pulsa el botón OK para empezar la búsqueda.

Si usted sabe el número del paquete, usted puede adelantar al paquete seleccionando Va Go To Frame del menú del Display, o del menú del contexto (vía un ratón correcto pulse el botón). Entre en el número del paquete, entonces pulse el botón OK.

## Usando un Filtro del Display

Un filtro del displayle permite filtrarse fuera los paquetes no deseados del buffer de la captura. Usted puede acostumbrar un filtro del displaya sólo ver:

Los Paquetes de · transmitieron entre los nodos de la red (o pares de dirección),

Paquetes de · que pertenecen a uno o más de un group(s protocolares),

· el paquete LIVIDO Específico teclea correspondiendo al protocolo del encapsulation LIVIDO actualmente seleccionado (SDLC, X.25, Parada del Marco, o HDLC),

Paquetes de · que los fósforos un modelo de los datos definido, o

Paquetes de · que emparejan varios combinación de las especificaciones anteriores

El perfil definido para un filtro de la captura, filtro del amonestador, o filtro de evento también puede usarse por filtrarse paquetes del Displaydel Paquete.

Para crear un nuevo filtro, seleccione Define Filter del menu display. Usted define filtros del Displayde la misma manera que usted define filtros de la captura. Vea el tema de los Filtros Definiendo.

Para aplicar un filtro, escoja Filtro Select del menu display. Escoja un filtro pre-definido y pulse el botón OK.

## Imprimir paquetes decodificados

Usted puede imprimir los paquetes de los datos descifrados en el Descifre Despliegue. Usted puede imprimir una lista del línea-por-línea de los paquetes en la hoja Sumary, una lista de campos protocolares en la hoja de Detalle, los datos del hex en la hoja del Hex.
Impresión selecta del menú del Archivo. En el área de Rango de Impresión, seleccione el rango de paquetes que usted quiere imprimir. En el área del Formato, seleccione qué hojas de vidrio (Resumen, Detalle, Hex) usted quiere imprimir.
Si usted quiere al rendimiento los paquetes de los datos descifrados a un archivo, la Impresión del cheque para Archivar.

Use el Aborte Imprimiendo toolbar abroche o File/Abort Printing la selección del menú para abortar el trabajo de la impresión actual.

## Seleccionando Paquetes para vistas separadas o como Marcas del Libro

El Profesional del snifer permite seleccionar paquetes individuales, o un grupo de paquetes, en la hoja sumary del Descifre Despliegue, y entonces sálvelos en un separado descifre ventana.
Para seleccionar paquetes individuales, pulse el botón la caja del cheque delante del número del índice del paquete.
Para seleccionar un grupo de paquetes:

1 pulsa el botón el botón del ratón correcto, y selecciona Select Range.

2 pulsan el botón el botón de radio de Rango y entran en el rango del paquete de su opción.

3 pulsan el botón el botón Select

Para aclarar todas las marcas:

1 pulsa el botón el botón del ratón correcto y selecciona Select Range.

2 pulsan el botón el All nnn Packetsradio botón.

3 pulsan el botón el botón de Deselect.

Para seleccionar todos los paquetes excepto unos:

1 pulsa el botón el botón del ratón correcto y selecciona Select Range.

2 pulsan el botón el All nnn Packetsradio botón.

3 pulsan el botón el botón Select

4 pergamino la hoja sumary para localizar paquetes del undesired. Pulse el botón la caja del cheque delante de cada paquete del undesired al deselect él.

Una vez usted ha seleccionado los paquetes, usted puede:

· Save los paquetes seleccionados en un nuevo descifre ventana seleccionando Ahorre Seleccionado del menú del contexto (pulsando el botón el botón del ratón correcto)

· Use los paquetes seleccionados como Libro de ‘Marcan '. Use F2 para adelantar de uno seleccionó marco a otro

Notas:

· Cuando usted selecciona y excepto los paquetes en una ventana separada, el tiempo relativo del paquete al paquete se mantiene propiamente.

## Importando un Archivo de Captura para terceros

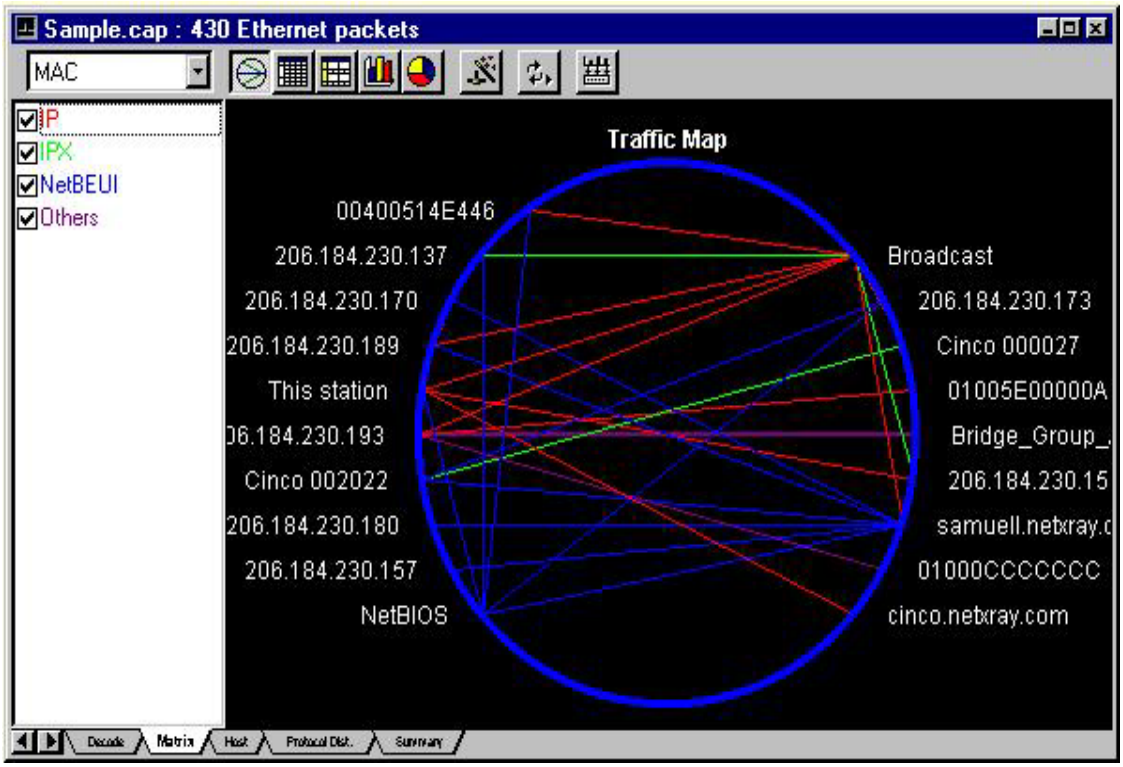
El Profesional del sniffer reconoce muchos archivos de la captura creados por General de la Red (ahora los Socios de la Red) el Analizador de Red de Sniffer Especialista.
Novell LANalyzer para los Windows captura archivos (.TR1) también puede ser desplegado por Sniffer En pro de.
Cargue estos archivos que usan la File/Open menú selección. Seleccione el tipo de archivo para cargar usando los Files of type: campo.

## Usando la matrix de  Mapa de Tráfico en la decodificación de paquetes

El mapa de tráfico en Paquete Descifra es una herramienta poderosa que le proporciona una vista del pájaro-ojo de los modelos de tráfico de red capturada en el buffer del paquete. Da una presentación gráfica completa del modelo de tráfico entre los nodos de la red, así como el tipo de protocolo usó.
Además, usted puede filtrarse fuera tráfico no deseado por unchecking ciertos protocolos, o seleccionando nodos de la red específicos para desplegar.
El ejemplo siguiente muestra cómo usted puede desplegar el mapa de tráfico completo, IP trafican, y el tráfico transmitió a y de un nodo de IP particular.

Para desplegar el mapa de tráfico, seleccione la etiqueta de lamatrix en el fondo de la ventana de Displayde Paquete, y pulse el botón el botón del Mapa.

Nota: Si usted no ve la etiqueta de lamatrix, asegúrese ese Muestra Poste Análisis Etiquetas en el menú del se habilita.




El gota-baje lista en la esquina izquierda superior de la ventana de mapa de tráfico le permite ver el mapa de tráfico de las varias capas (como PVC, MAC, IP, o IPX). Los checklist protocolares en el lado izquierdo de la ventana cambiarán dependiendo de la capa usted escoge. Por ejemplo, si usted selecciona IP del gota-baje lista, el mapa de tráfico desplegará sólo IP capa conversaciones.

Cada línea de conexión entre dos nodos de la red se colora para indicar el protocolo usado en la comunicación. Si más de uno el protocolo se graba entre dos nodos, la línea que une se irrumpirá en los segmentos coloreados, con cada representar colorido un protocolo diferente. La longitud de cada segmento colorido representa la proporción de tráfico para el protocolo indicado.
Llevar más allá aislan tráfico a y de un nodo particular, resalte el nodo, derecho-pulse el botón para desplegar el menú del contexto, y pulse el botón la Muestra Seleccionó Nodos.

## Definiendo un Filtro de despliegue con la matriz de Mapa de Tráfico

El mapa de tráfico dematrix puede usarse para definir un anuncio hoc el filtro del display(llamó un filtro visual) para seleccionar paquetes que emparejan la dirección de mapa de tráfico actual y el criterio protocolar.

Para usar el mapa de tráfico para definir un filtro visual, seleccione los protocolos usted quiere filtrarse para y resaltar el node(s de la red) usted quiere filtrarse para en el mapa de tráfico. Para seleccionar más de un nodo, sostenga los Ctrl codifican abajo y pulsan el botón nodos adicionales.
Para aplicar el filtro visual, pulse el botón, y una nueva ventana de Displayde Paquete abre para mostrar sólo

paquetes que emparejan el nodo seleccionado se dirige y las especificaciones protocolares.

Tip:

· El número de la sucesión de cada paquete en el buffer de la captura original se retiene. A veces es útil a la referencia los paquetes filtrados al paquete lleno puesto en el buffer. Sin embargo, si el juego del paquete filtrado se ahorra a un archivo, los paquetes se renumerarán cuando recargó en el buffer y desplegó.

## HERRAMIENTAS ACTIVAS

## Ping

Use Ping para identificar la disponibilidad de un IP organizador nodo en la red.
Ping utiliza el datagram de DEMANDA de ECO obligatorio del protocolo de ICMP para sacar una ICMP ECO CONTESTACION de un organizador o entrada de la red que usted especifica.
Invocar la herramienta de Ping, Tools/Ping selecto del menú principal.

· Si el organizador responde, Ping imprime Reply from xx.xx.xx.xx  bytes=xx time=xx ms  TTL=xx

EN el Ping anote ventana.

· Si no hay ninguna contestación para los definieron tiempo-fuera el periodo, Ping imprime Ping xx.xx.xx.xx Error: Pida Interrupción en la ventana del leño.

El predefinido tiempo-fuera el periodo 300 milliseconds está. Usted puede ajustarlo a un valor apropiado por sus condiciones de la red.

Tip:

· Usted puede resaltar a un organizador de IP del Anfitrión Table y puede derecho-pulsar el botón para acceder Ping y otras herramientas activas en el menú del contexto.

## Finger

Use Dedo para desplegar información sobre cada uno anotado-en usuario en un organizador especificado.
Usted puede entrar en el nombre del organizador o su dirección de IP.
Invocar la herramienta Digital, Tools/Finger selecto del menú principal.
Para preguntar para un usuario particular, entre en un username en el campo de la Pregunta Query

Para ver a todos los usuarios, deje el espacio en blanco de campo de Pregunta Query

Despliegues del dedo los resultados de su pregunta en la ventana del leño Digital.

Tip:

· Usted puede resaltar a un organizador de IP del Anfitrión Table y puede derecho-pulsar el botón para acceder Dedo y otras herramientas activas en el menú del contexto.

## DNS Lookup

Use DNS Lookup para encontrar el nombre del dominio de una dirección de IP, o viceversa. DNS Lookup envía una pregunta al organizador de DNS y a despliegues el resultado de la pregunta en el DNS Lookup anote ventana.
Invocar el DNS la herramienta de Lookup, Tools/DSN Lookup selecto del menú principal.

Tip:

· Usted puede resaltar a un organizador de IP del Anfitrión Table y puede derecho-pulsar el botón para acceder DNS Lookup y otras herramientas activas en el menú del contexto.

## Whois

Use Whois (como en, quién es...?) para buscar una TCP/IP directorio entrada para un nombre del dominio registrado, el nombre de usuario, o usuario ID.
Empezar la herramienta de Whois, Tools/Whois selecto del menú principal.
Usted entra en el nombre del dominio registrado en el campo de Nombre de Organizador:

· Enter name.dom para un dominio, por ejemplo, netscape.com

· Enter Firstname Lastname o Lastname, Firstname para un usuario registrado, por ejemplo, Mary Smith o Smith, Mary,

· Enter el userid para un usuario ID, por ejemplo, eric_hua

Opcionalmente, usted puede entrar en el nombre de un servidor de Whois particular en el campo del Servidor si usted desea restringir la búsqueda a un servidor particular.

Se despliegan los resultados de la búsqueda en la Whois leño ventana.

Tip:

· Usted puede resaltar a un organizador de IP del Anfitrión Table y puede derecho-pulsar el botón para acceder Whois y otras herramientas activas en el menú del contexto.

## Trace Route

Use Ruta del Rastro para identificar toda la route del intermedio IP se dirige y retrasos de tiempo de acceso entre su Sniffer En pro de y un organizador del destino.

Invocar la herramienta de Ruta de Rastro, Tools/Trace Route selecto del menú principal.
Especifique los IP se dirigen de su organizador del destino y un tiempo-fuera el intervalo (el valor por defecto es 300 milliseconds). la Ruta del Rastro manda ICMP Rastro Ruta paquetes. Las routes informan por el camino atrás, y figuras de Ruta de Rastro y despliegues un leño de Ruta de Rastro.
Una vez el rastro de la ruta se ha completado, problemas de Ruta de Rastro un DNS Lookup y despliegues el resultado en el leño de Ruta de Rastro. Usted también puede desplegar la información de ruta de rastro en una mesa o mapa. Pulse el botón en la Mesa o etiqueta del Mapa sobre la barra de estado.

Tip:

· Usted puede resaltar a un organizador de IP del Anfitrión Table y puede derecho-pulsar el botón para acceder Ruta del Rastro y otras herramientas activas en el menú del contexto.

## Herramientas agregando al Menú de las Herramientas

Además del juego normal de herramientas de IP, usted puede agregar sus propias herramientas al menú de las Herramientas. La herramienta puede ser actualmente cualquier Windows o DOS archivo ejecutable instalado o accesible a su máquina.
Para agregar una herramienta:

5 Tools/Customize User tools selectas del menú principal.

6 pulsan el botón el Add botón. El programa agregará (nuew tool) a la lista de la herramienta.

7 revisan el campo de menu Text. Reemplace (nueva herramienta) con el nombre usted quiere ver en el menú.

8 especifican la línea del orden, parámetros de línea de orden, y firman con iniciales salida-a el directorio como necesitó empezar su programa propiamente.

9 opcionalmente, asigne una llave del atajo (Alt + t, carta). para hacer esto, ponga un carácter del ampersand (&) delante de la carta apropiada en el campo de Menú Text. (Además, el programa asigna un Alt automáticamente + el atajo del número, visible al derecho del artículo del menú cuando usted despliega el menú de las Herramientas.)

10 opcionalmente, use el Movimiento A y Instálese Abajo los botones el Personalice las Herramientas del Usuario dialogan caja para cambiar el orden de herramientas desplegado en el menú.

11 pulsan el botón OK. La nueva herramienta aparecerá en el menú de las Herramientas.

## Herramientas quitando del Menú de las Herramientas

Para quitar una herramienta listada en el menú de las Herramientas:

1 Tools/Customize Usuario tools selectas del menú principal.

2 seleccionan la herramienta que usted quiere quitar.

3 pulsan el botón Quite.

4 pulsan el botón OK.

# EXPERT

## Capas especialistas

El Experto categoriza problemas de la red según la capa Especialista a la que ellos ocurren. Durante la captura, los usos Especialistas su real-tiempo los intérpretes protocolares para trazar la información empotrada en cada marco hacia su propio modelo de capas de la red.

El modelo del Experto de capas de la red se muestra debajo.

NOTA: La estructura de layering de red del Experto es similar al modelo de OSI. Sin embargo, los dos esquemas no siempre trazan en una uno-a-uno base.

CAPAS de OSI la CAPA ESPECIALISTA
El ApplicationPresentation ApplicationThe Experto une las dos capas de OSI superiores en uno porque los relativamente pocos protocolos existen a la capa de la presentación. También, los límites entre estas capas son inciertos–muy a menudo las aplicaciones pueden acceder la capa de transporte (por ejemplo, TCP) sin usar los servicios a la capa de la presentación.
Sesión SessionThe los cheques Especialistas para problemas relacionados a la administración y seguridad.
Transporte ConnectionThe los cheques Especialistas para problemas relacionados a la eficacia de comunicaciones del extremo-a-extremo y recuperación del error.
Red StationThe los cheques Especialistas para la red dirigiéndose y derrotando problemas. También interpreta tráfico entre los subnets y medidas la distancia entre el subnets en términos de brincos.
LinkPhysical de los datos el Experto de DLCThe une las dos capas más bajas porque no realiza una gama amplia de diagnósticos en las características físicas de la red como voltaje eléctrico y el Experto de current.The se preocupa por el traslado real de datos por la red (por ejemplo, guarda la huella del número de marcos de la transmisión y el número de bytes transmitida durante un intervalo del predefined para descubrir carga excesiva de la red). también se descubren errores Físicos como los errores de CRC y marcos que son demasiado cortos.
Además de las cinco capas Especialistas, el Experto cuenta también Síntomas Globales, Dirija, y Información de Subnet. Los Síntomas globales son síntomas que no residen a cualquier capa particular, como Tormentas de la Transmisión. Dirija que la Información proporciona información sobre todos comunicando subnets que el Experto descubre.

## Intérpretes protocolares

El Experto de Profesional de Sniffer puede procesar marcos en un Ethernet red segmento, un anillo de la ficha, o un eslabón LIVIDO.
Los Protocolos actualmente disponible para el análisis Especialista se muestra debajo:

Protocolo los Protocolos del Elector Familiares
TCP/IP ARP, IP, que ICMP, IGRP, RASGAN, TCP, UDP, RPC, NGCP,
X-ventana, POP3, HTTP,NNTP, NFS, RPC, TELNET, FTP, TFTP, RLOGIN, SMTP, NIS,,,
Sybase TDS/SQL
Oráculo TNS, SQL,

## Ventana especialista

La ventana Especialista es dividido en cinco hojas de vidrio: Apreciación global especialista, estadísticas sumarys, protocolares Especialistas, árbol de detalle, detalle Especialista. La información mostrada en cada hoja se describe debajo.

Apreciación global especialista

Apreciación global

Resumen especialista

Resumen del síntoma
Resumen del diagnóstico
La aplicación Objeta Resumen
La sesión Objeta Resumen
La conexión Objeta Resumen
Resumen de Objetos de estación
DLC Objects el Resumen
Resumen de los Objetos global
Resumen de Objetos de ruta
Subnet Pair el Resumen de los Objetos

Estadísticas protocolares

Estadísticas protocolares

Arbol de detalle

El árbol de detalle muestra una inscripción jerárquica de todas las capas a o debajo de aquéllos seleccionados en la apreciación global Especialista y Experto las hojas de vidrio sumarys.

Detalle especialista

Detalles de Objeto de aplicación: POP3 detalles, HTTP Details, FTP Details, TFTP Details, NNTP Details, Telnet Details, que el Oráculo Detalla, TDS Details, NFS Details, SMTP Details, NIS Details, Detalles de RLOGIN,,
Detalles de Objeto de sesión: X Windows Detalles, TNS Details, RPC Details, Detalles de NGCP,

Detalles de Objeto de conexión: UDP Details, Detalles de TCP,
Detalles de Objeto de estación: IP Details
DLC Object los Detalles: Ethernet Details, Detalles de Anillo de Ficha,
Detalles del Objeto globales
Detalles de Objeto de ruta
Subnet Pair los Detalles del Objeto

## Opciones especialistas

Para configurar opciones Especialistas, seleccione Opciones Especialistas del menú de las Herramientas abrir las Propiedades Especialistas dialoge caja.

Las Propiedades Especialistas dialogan que la caja contiene cuatro etiquetas: Objetos, Alarmas, Subnet Masks, y Opciones de la RASGADURA.

## Umbrales de la Alarma especialistas

Ciertas alarmas Especialistas tienen umbrales que determinan cuando un síntoma o el diagnóstico se genera. IMPORTANTE: Se han calculado los umbrales predefinidos proporcionados con el Experto cuidadosamente para asegurar síntoma exacto y informativo y descubrimiento del diagnóstico. Antes de cambiar cualquiera de los umbrales, se asegura que usted entiende su red.

Umbrales de DLC

Proporción alta de errores Físicos
Proporción alta de errores del line/burst
Proporción alta de errores de congestión de receptor
Demasiados ingresos
Síntoma de purga de anillo
Proporción alta de diagnóstico de purga de anillo
Demasiados quita

Estacione Umbrales

Routes Remotas múltiples
Routes Locales múltiples

Umbrales de conexión

Time ocioso (Esté ocioso Demasiado Largo)
Retransmission rápido (Ack Demasiado Largo)
Ponga a cero Ventana (Ventana Demasiado Largo)
Ponga a cero Ventana (Ventana Helada)
Retransmission rápido
Contestación Time, la Contestación Lenta (Servidor Lento)
Ninguna Contestación (Estación No-sensible)
Retransmissions (demasiados Retransmission)

Umbrales de la sesión

Xfer local (KB/s), Xfer Remoto (KB/s) (Throughput Bajo)
Fíltrese Time (ms) (Vueltas en misma demanda)
Min appl req, Vuelta% (demasiadas vueltas en misma demanda)
Archivo lento Xfer% (demasiados Archivo Retransmissions)
Archivo lento Xfer% (Archivo Lento)
Cuenta negada (la Demanda Negó)
Cuenta negada, Min appl req, la Demanda Negada% (las demasiadas Demandas Negaron)

La Conexión del oráculo Falló (TNS Connect se Negó a)
Oráculo Lento Conecte Time (TNS Slow Conectan)
Oráculo Seguridad Brecha Esfuerzo (TNS Seguridad Brecha Esfuerzo)
Oráculo la Contestación del Servidor Lenta Time (TNS la Contestación del Servidor Lenta)
Oráculo la Cuenta de Contestación de Servidor Lenta, Oráculo Servidor Contestación Intervalo (TNS el Diagnóstico del Servidor Lento)

Umbrales de la aplicación

FTP Connect las Pruebas (FTP Login Esfuerzos)
FTP Connect Time (FTP Slow Conectan)
FTP Login Time (FTP Slow Primero la Contestación)
FTP Interframe Time (FTP la Contestación Lenta)
FTP Interframe Cuenta, FTP Interframe Intervalo (FTP el Diagnóstico del Traslado Lento)
Telnet Connect (Telnet la Contestación Lenta a Login)
SMTP Slow Conectan Time
NNTP Slow Conectan Time (NNTP la Contestación Lenta Time)

POP3 lento Conecte Time
La Conexión de DB Falló (DB Connect la Demanda Negó)
DB Seguridad Brecha Esfuerzo
DB la Contestación del Servidor Lenta Time
DB Slow Conectan Time
DB la Cuenta de Contestación de Servidor Lenta, DB el Intervalo de Contestación de Servidor Lento (DB el Diagnóstico de Contestación de Servidor Lento)

Umbrales globales

Tormenta de la Transmisión menor (Broadcast/Multicast Storm)
Tormenta de la Transmisión mayor (Tormenta de Broadcast/Multicast Diag)
LAN Overload excesivamente% (LAN Overload excesivamente)
LAN Overload excesivamente (intervalo) (LAN Overload excesivamente el porcentaje)
Colisión (Colisiones encima del umbral)

# GENERADOR DE PAQUETE

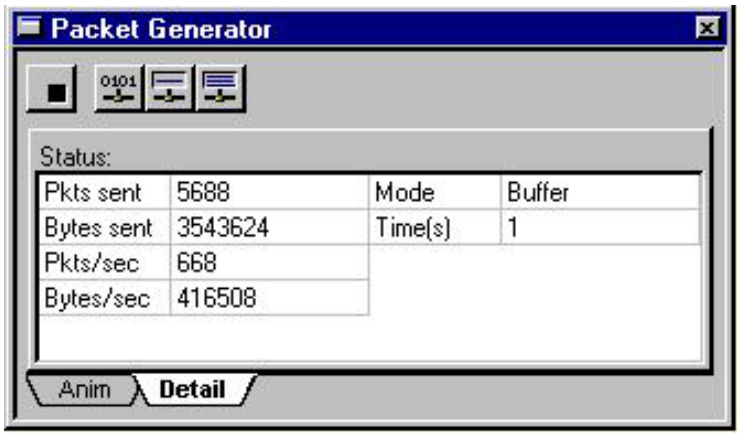
## Apreciación global de Generador de paquete

Los paquetes transmitiendo hacia la red le dan la habilidad a:

· Reproduce los problemas de la red así que usted puede arreglar y puede verificar apuros que usted ha hecho a sus equipos de la red o aplicaciones.

· Generate el tráfico de la red para probar condiciones sus equipos de la red deben poder manejar.

Para invocar el Generador del Paquete, escoja Generador del Paquete del menú de las Herramientas. Una ventana de Generador de Paquete se despliega.




Para ver el paquete que transmite estado, pulse el botón la etiqueta de Detalle.

Advirtiendo:

· Transmitting los paquetes a una red real pueden producir resultados inesperados. Asegúrese que usted ha aislado su red de la prueba de la red de la producción antes de proceder con comprobación de carga de red.

## Transmitiendo un Solo Paquete

Para transmitir un solo paquete, pulse el botón el Send New Packet,


o pulse el botón

el Envía botón del Paquete Actual cuando un archivo capturado o el buffer se despliega en Displaydel Paquete.
Usted puede cambiar el paquete siguiente envía parámetros:

· Send #de tiempos, o continuamente

· Delay tiempos en milliseconds entre el paquete envían

· Paquete tamaño

· Paquete volúmenes

El Envía el modelo de datos de hex a los Paquete diálogo caja despliegues para el nuevo o actualmente seleccionó paquete. Usted puede revisar los datos del hex del paquete poniendo el cursor en la ventana del hex, usando el cursor codifica para mover el cursor a la situación deseada, y tecleando en los nuevos valores.

Ponga el tiempo de Retraso para poner a cero milliseconds para producir la proporción del máximo de transmisiones del paquete. La proporción de transmisión depende del tamaño del paquete, el los CPU de PC aceleran, y la velocidad de su tarjeta de interface de red. Para lograr la proporción de transmisión de máximo, use un PC rápido y un PCI alto rendimiento conectan una red de computadoras tarjeta de la interface.

Puesto que el Profesional del | se diseña para correr en el Windows 95 ambiente del multitasking, el tiempo de retraso usado en transmisión del paquete no puede controlarse con precisión. Puede variar, dependiendo del tipo de aplicaciones usted están corriendo concurrentemente en el PC. Para la actuación óptima, cierre todos los otros programas activos.

## Transmitiendo un Archivo Capturado Entero

Pulse el botón para invocar el Envía función del Buffer Actual, cuando un archivo capturado o el buffer se despliega en el Displaydel Paquete.
Usted puede enviar el buffer entero #de tiempos, o continuamente.
Se calcula el retraso de tiempo entre cada paquete del tiempo de retraso original guardado en el buffer de la captura. El tiempo de retraso no puede ser exactamente reproducible porque el Windows 95 cronómetro del sistema tiene un granularity mínimos de 1 millisecond. Además, el tiempo de retraso puede variar dependiendo del tipo de aplicaciones usted grandemente está corriendo concurrentemente con Sniffer En pro de. Para la actuación óptima, cierre todos los otros programas activos.

# MODO LOOPBACK

## Captura de un Archivo

Usted puede usar el Modo de Loopback de Sniffer Pro's para simular una captura de una traza de un archivo de marcos salvados. La simulación de una captura puede ser útil para sus propósitos de práctica.

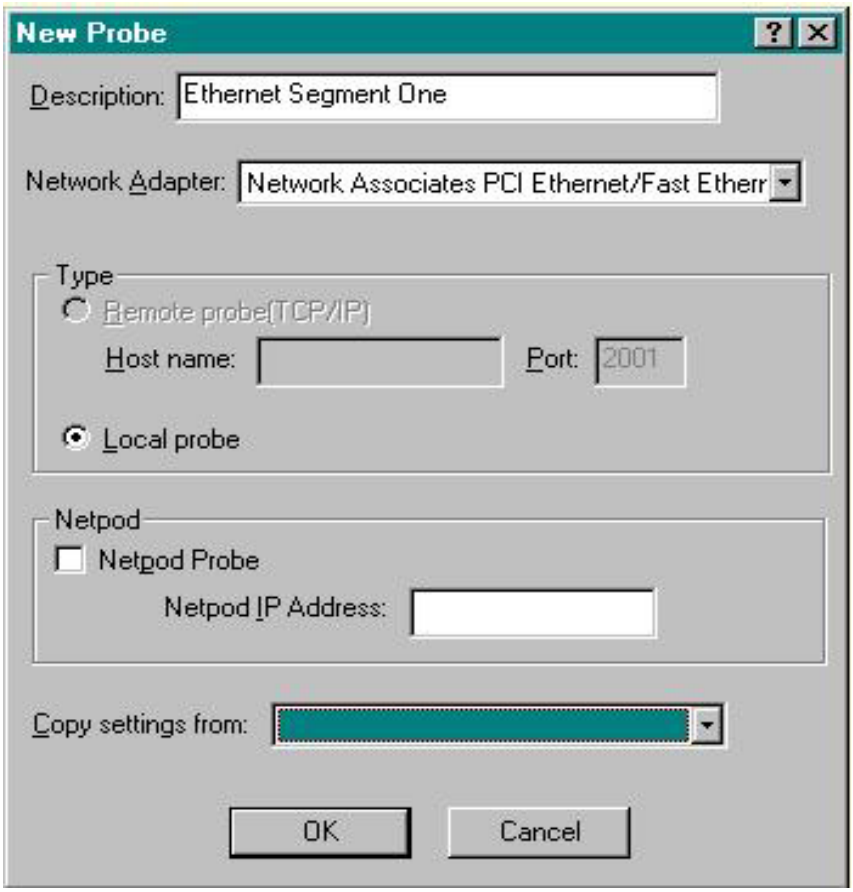
Para capturar la traza de un archivo de marcos salvados:

1 En el menú File (Archivo) del Sniffer Pro's, habilite la opción Modo Loopback.
2 El menú Tools (Herramientas), seleccione Packet Generator (Generador de Paquetes). Una ventana del Generador de Paquetes se abrirá.
3 Seleccione File (Archivo) de la barra del menú y pulse el botón Open (Abrir). Los archivo abiertos se despliegan en
una caja de diálogo.
4 Seleccione su archivo de traza y pulse el botón Open (Abrir). Una ventana de despliegue de Paquetes se abrirá.
5 Pulse el botón Send Current Buffer (Buffer de envío actual). Una caja de diálogo del Buffer de envío actual se abre.
6 Escoja entre Envíar continuamente, o Envíar un número de veces.
7 Pulse el botón OK para empezar la generación de paquetes.
8 Inicie la captura seleccionando Start (Iniciar) del menú Capture (Capturar).
9 El tablero de captura actualiza como el Sniffer Pro captura los archivos de traza seleccionados.

**MULTIPLES ADAPTADORES DE RED**

## Seleccione el Adaptador de Red.

Si usted tiene más de un adaptador obediente NDIS 3.1 instalado en su sistema, Sniffer Pro le permite vincular el adaptador de su preferencia.
Para seleccionar un adaptador, vaya al menú Files (Archivos) y pulse el botón Select Network Probe/Adapter (Seleccionar Sondeo/Adaptador de Red). Se abre una caja de diálogo de selección de Sondeo/Adaptador de Red. Contiene las pruebas que usted ha definido para este PC con Sniffer Pro. Usted puede seleccionar cualquier prueba previamente definida como la red objetivo del monitor Sniffer Pro, o usted puede pulsar el botón New Probe (Nueva Prueba) para definir una nueva prueba a ejecutar. Pulsando el botón New Probe (Nueva Prueba) se mostrará una caja de diálogo de New Probe (Nueva Prueba).




Use el campo Description (Descripción) para proporcionar un nombre descriptivo para su adaptador. Su descripción aparecerá en los casos futuros de la caja de diálogo Select Network Probe/Adapter (Seleccionar Sondeo/Adaptador de Red).

Use el campo Network Adapter (Adaptador de Red) para seleccionar el adaptador. La lista desplegable incluye todos los adaptadores obedientes NDIS 3.1 que está instalados actualemente en el PC con Sniffer Pro.

Use los campos Type (Tipo) para especificar si la prueba es Remota o Local. Para el Sniffer Pro usted se limita a Local Probes (Pruebas Locales). Las pruebas remotas son sólo soportadas por el Distribuídor Sniffer Pro. Si usted está usando el Distribuídor Sniffer Pro y selecciona Remote Probe (Prueba Remota), es decir,

una prueba en la cual usted se conecta encima de una red que usa TCP/IP, usted debe proporcionar el nombre del host y el número de puerto TCP usado para conectar a la prueba remota.

Habilite la caja de chequeo Netpod Probe(Prueba de Encapsulamiento de Red) si esta prueba será usada con una red de interface de encapsulamiento. Cuando usted habilita la caja de chequeo Netpod Probe, la Netpod IP Address (Dirección IP encapsulada) es automáticamente ocupada con una dirección IP incrementada en uno de la dirección IP del PC Sniffer Pro. Por ejemplo, si la dirección IP del PC Sniffer Pro es 206.129.112.24, la dirección IP encapsulada proporcionada por el Sniffer Pro será 206.129.112.25.

NOTA: Esta versión del Sniffer Pro sólo soporta conexiones locales para redes encapsuladas. Usted no puede conectarse a una red encapsulada sobre la red.

Use las escenas Copy del campo para usar las escenas de configuración de una prueba existente. La lista desplegable incluye todas las pruebas previamente definidas en el PC Sniffer Pro.

NOTA: Varias opciones en los menús del Sniffer Pro cambiarán dependiendo del tipo de adaptador que usted haya seleccionado para la captura. Por ejemplo, habilitando un adaptador Token Ring se habilitarán opciones diferentes que al habilitar un adaptador WAN.

# USANDO EL SNIFFER PRO CON UN ADAPTADOR WAN

## La apreciación global de la WAN Sniffer Pro

La Network Associates proporciona varios adaptadores WAN para el uso de Sniffer Pro:

Adaptador LM2000. El adaptador LM2000 permite conectar Sniffer Pro para las interfaces de red RS-232, RS-422, RS-423, V.10, V.11, y V.35.
Adaptador HSSI. El adaptador de HSSI permite conectar Sniffer Pro a interfaces seriales de alta velocidad.

El manual Sniffer Pro: Instalación, Conección, y Configuración de Hardware WAN describe cómo instalar estos adaptadores en el PC Sniffer Pro y conectarlos a la red.

Antes de que usted pueda usar estos adaptadores para captura en la red, debe configurar el analizador para usarlos.

Use la etiqueta HSSI Medium Extension (Extensión Intermedia HSSI) en la caja de diálogo Options (Opciones) para fijar las opciones de configuración para el adaptador HSSI.

Use la etiqueta WAN Medium Extension (Extensión Intermedia WAN ) en la caja de diálogo Options (Opciones) para fijas las opciones de la configuración para el adaptador LM2000.

## Fijar la opciones WAN

Antes de que usted pueda capturar o puede supervisar la red que usa un adaptador WAN (el LM2000 o el adaptador de HSSI), usted debe configurar el Sniffer Pro para usar el adaptador. Esto incluye las opciones fijadas como el protocolo del encapsulamiento usado en el enlace WAN.

Use la etiqueta HSSI Medium Extension en la caja de diálogo Options para fijar las opciones de configuración para el adaptador HSSI.

Use la etiqueta WAN Medium Extension en la caja de diálogo Options para fijar las opciones de configuración para el adaptador LM2000.