White Paper de las mejores prácticas del proceso de línea de base

Contenido

Introducción

Este documento describe los conceptos y los procedimientos del establecimiento de líneas de base para redes de alta disponibilidad. Incluye los factores de éxito críticos para que el establecimiento de líneas de base de red y del umbral ayude a evaluar el éxito. También proporciona gran cantidad de detalle para los procesos de la línea de base y el umbral y la implementación que siguen las pautas de prácticas recomendadas identificadas por el equipo HAS (High Availability Services) de Cisco.

Este documento le toma paso a paso con el proceso del baselining. Algunos Productos del sistema de administración de la red actual (NMS) pueden ayudar a automatizar este proceso, sin embargo, el proceso del baselining sigue siendo lo mismo si usted utiliza las herramientas automatizadas o manuales. Si usted utiliza estos productos NMS, usted debe ajustar los establecimientos del umbral predeterminados para que haya su entorno de red única. Es importante tener un proceso para elegir inteligente esos umbrales de modo que estén significativos y correctos.

Línea de base

¿Qué es una línea de base?

Una línea de fondo es un proceso para estudiar la red a intervalos regulares para asegurarse de que la red está trabajando según lo diseñado. Es más que un solo informe que detalla la salud de la red en cierta punta a tiempo. Siguiendo el proceso de línea de base, usted puede obtener la siguiente información:

- Gane la información valiosa en la salud del hardware y software
- Determine los usos de recurso de la red actuales
- Tome las decisiones precisas sobre los umbrales de la alarma de red
- Identifique los problemas de la red actual
- Prediga los problemas futuros

Otra manera de mirar la línea de fondo se ilustra en el diagrama siguiente.

La línea roja, el punto de interrupción de la red, es el punto en el que se interrumpirá la red el cual está determinado a través del conocimiento de cómo se ejecutan el hardware y el software. La línea verde, la carga de la red, es la progresión natural de carga en la red cuando se agregan nuevas aplicaciones y existen otros factores similares.

El propósito de una línea de fondo es determinar:

- Donde está su red en la línea verde
- Cómo rápidamente la carga de la red está aumentando
- Esperanzadamente prediga en qué punta a tiempo entrecruzarán los dos

Realizando una línea de fondo en las bases normales, usted puede descubrir al estado actual *y* extrapolar cuando los errores ocurrirán y se prepararán para ellos por adelantado. Esto también lo ayuda a tomar decisiones más informadas sobre cuándo, dónde y cómo gastar dinero del presupuesto en actualizaciones de la red.

¿Por qué una línea de base?

Un proceso de línea de base le ayuda a identificar y a planear correctamente para los problemas de la limitación de los recursos críticos en la red. Estos problemas se pueden describir como los recursos de plano del control o recursos de plano de los datos. Los recursos de plano del control son únicos a la plataforma y a los módulos específicos dentro del dispositivo y pueden ser afectados por varios problemas incluyendo:

- Utilización de los datos
- Características habilitadas
- Diseño de red

Los recursos de plano del control incluyen los parámetros por ejemplo:

- Utilización de la CPU
- Utilización de la memoria
- Utilización del almacén intermedio

La cantidad de tráfico afectan solamente el tipo y e incluyen a los recursos de plano de los datos la utilización del vínculo y la utilización de backplane. Por la utilización de recursos del baselining para las áreas críticas, usted puede evitar los problemas graves de rendimiento, o peor, un que SE funda la red.

Con la introducción de las aplicaciones susceptibles a la latencia, como voz y video, el establecimiento de líneas de base es ahora más importante que antes. Las aplicaciones tradicionales del Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP) están perdonando y permiten una determinada cantidad de retardo. La Voz y el vídeo son User Datagram Protocol (UDP) basado y no permiten las retransmisiones o la congestión de red.

Debido a la nueva mezcla de aplicaciones, el baselining le ayuda a entender los problemas de la utilización de los recursos de plano del avión y de los datos del control y dinámico a planear para que los cambios y las actualizaciones aseguren el éxito continuo.

Las redes de datos han estado alrededor durante muchos años. Hasta hace poco, mantener las redes funcionando era un proceso bastante indulgente, con algún margen de error. Con la aceptación cada vez mayor de aplicaciones sensibles a la latencia, como Voz sobre IP (VoIP), la tarea de operar una red es cada vez más difícil y requiere mayor precisión. Para ser más exacto y dar a un administrador de la red las bases sólidas sobre las cuales manejar la red, es importante tener cierta idea de cómo la red se está ejecutando. Para ello, debe seguir un proceso denominado línea de base.

Objetivo de línea de base

El objetivo de una línea de fondo está a:

1. Determine el estado actual de dispositivos de red
2. Compare ese estatus a las guías de consulta del rendimiento estándar
3. Configure los umbrales para que le avisen cuando el estado excede aquellas pautas.

Debido a una gran cantidad de los datos y a la cantidad de tiempo que toma para analizar los datos, usted debe primero limitar el alcance de una línea de fondo para hacerla más fácil aprender el proceso. El lugar más lógico y, a veces, más beneficioso, para comenzar es el núcleo de la red. Esta parte de la red es generalmente la más pequeña y requiere la mayoría de la estabilidad.

Por la simplicidad, este documento explica cómo al Management Information Base muy importante del protocolo administración de red simple de la línea de fondo una (SNMP MIB): cpmCPUTotal5min. el cpmCPUTotal5min es la media de decaimiento del minuto cinco de la Unidad de procesamiento central (CPU) de un router Cisco, y es un indicador de rendimiento del avión del control. La línea de base será realizada en un router de la serie 7000 de Cisco.

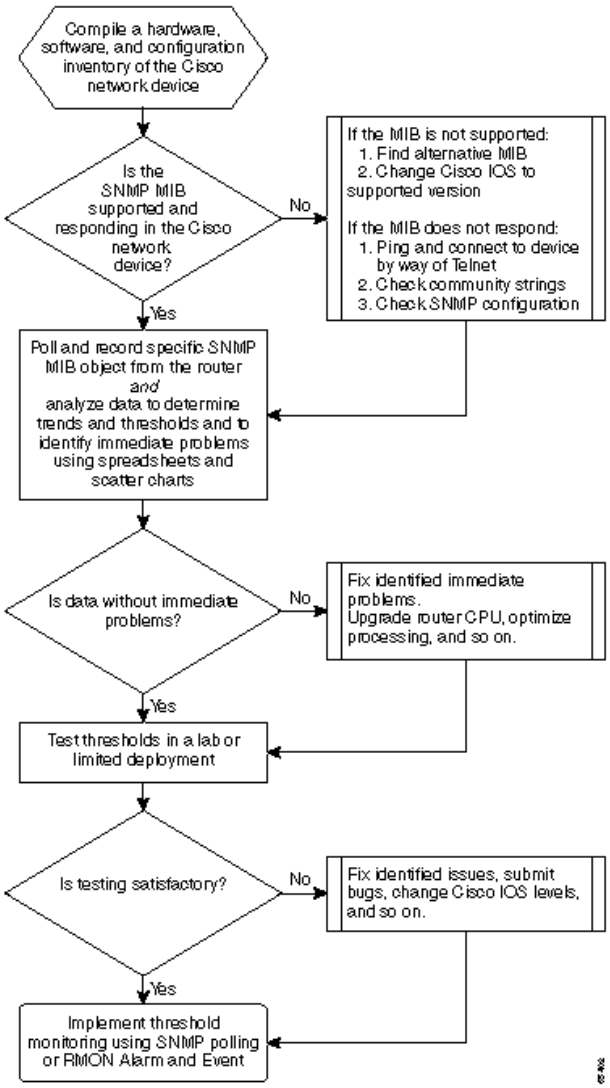
Una vez que ha aprendido el proceso, puede aplicarlo a todos los datos disponibles en la amplia base de datos SNMP que está disponible en la mayoría de los dispositivos de Cisco, como:

- Uso del Integrated Services Digital Network (ISDN)

- Pérdida de celda del Asynchronous Transfer Mode (ATM)
- Memoria de sistema libre

Diagrama de flujo de línea de base del núcleo

El siguiente diagrama de flujo muestra los pasos básicos del proceso de línea de base central. Mientras que los Productos y las herramientas están disponibles realizar algunos de estos pasos para usted, tienden a tener intervalos en la flexibilidad o la facilidad de empleo. Incluso si usted planea utilizar las herramientas del sistema de administración de la red (NMS) para realizar el baselining, esto sigue siendo un buen ejercicio en estudiar el proceso y la comprensión de cómo su red trabaja realmente. Además, este proceso puede develar algunas incógnitas sobre cómo funcionan algunas herramientas NMS, dado que la mayoría de las herramientas realizan básicamente las mismas tareas.



Procedimiento de línea de base

Paso 1: Compile un soporte físico, un software, y un inventario de la configuración

Es extremadamente importante que usted compila un inventario de soporte físico, de software, y de configuración por varias razones. Primero, el MIB de Cisco SNMP es, en algunos casos, específico al Cisco IOS Release que usted está ejecutando. Algunos objetos MIB son reemplazados por nuevos objetos o, en ocasiones, eliminados completamente. El inventario del hardware es muy importante una vez que recolectaron los datos, ya que los umbrales que se deben configurar después de la línea de base inicial muchas veces dependen del tipo de CPU, cantidad de memoria, etcétera, en los dispositivos Cisco. El inventario de la configuración también es importante para asegurarse de que conoce las configuraciones actuales: Usted puede querer cambiar las configuraciones del dispositivo después de que su línea de fondo para ajustar los buffers, y así sucesivamente.

La forma más eficiente de llevar a cabo esta parte de la línea de base para una red Cisco es utilizar Aspectos esenciales de gestión de recursos de CiscoWorks2000 (Essentials). Si este software está instalado correctamente en la red, el esencial debe tener los inventarios actuales de todos los dispositivos en su base de datos. Simplemente necesita ver los inventarios para consultar si hay problemas.

La siguiente tabla es un ejemplo de un informe de inventario de software de clase de router de Cisco, exportado de Essentials y luego editado en Microsoft Excel. De este inventario, note que usted tiene que utilizar los datos del SNMP MIB y los identificadores de objeto (OID) encontraron en las versiones del Cisco IOS 12.0x y 12.1x.

Nombre del dispositivo	Tipo de router	Versión	Versión del software

field-2.500a.embu-mlab.cisco.com	Cisco 2511	M	12.1(1)
qdm-7200.embu-mlab.cisco.com	Cisco 7204	B	12.1(1)E
voip-3640.embu-mlab.cisco.com	Cisco 3640	0x00	12.0(3c)
wan-1700a.embu-mlab.cisco.com	Cisco 1720	0x101	12.1(4)
wan-2500a.embu-mlab.cisco.com	Cisco 2514	L	12.0(1)
wan-3600a.embu-mlab.cisco.com	Cisco 3640	0x00	12.1(3)
wan-7200a.embu-mlab.cisco.com	Cisco 7204	B	12.1(1)E
172.16.71.80	Cisco 7204	B	12.0(5T)

Si el esencial no está instalado en la red, usted puede utilizar la línea de comando unix **snmpwalk de la** herramienta de una estación de trabajo Unix para encontrar la versión de IOS. Esto se muestra en el siguiente ejemplo. Si usted no está seguro cómo este comando trabaja, teclee el **man snmpwalk** en el prompt UNIX para más información. La versión de IOS será importante en cuanto comience a elegir cuales MIB OID se establecerán como líneas de base, ya que los objetos MIB dependen del IOS. También note que conociendo al tipo del router, usted puede hacer más adelante las determinaciones en cuanto a lo que deben ser los umbrales para el CPU, los buffers, y así sucesivamente.

```
nsahpov6% snmpwalk -v1 -c private 172.16.71.80 system
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JS-M), Version 12.0(5)T, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 23-Jul-2001 23:02 by kpma
system.sysObjectID.0 : OBJECT IDENTIFIER:
.iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.cisco7204
```

Paso 2: Verifique que SNMP MIB se admita en el router

Ahora que usted tiene un inventario del dispositivo que usted quiere sondear para su línea de fondo, usted puede comenzar a elegir los OID específicos usted quiere sondear. Guarda mucha frustración si usted verifica, antes de tiempo, que los datos que usted quiere estén realmente allí. El objeto cpmCPUTotal5min MIB se encuentra en CISCO-PROCESS-MIB (Base de información para la administración de procesos de Cisco).

Para encontrar el OID que desea sondear, necesita una tabla de conversión que esté disponible en el sitio Web de CCO de Cisco. Para acceder a este sitio web desde un navegador web, vaya a la página Cisco MIBs y haga clic en el enlace OIDs.

Para ingresar a este sitio Web desde un servidor FTP, escriba ftp://ftp.cisco.com/pub/mibs/oid/. De este sitio, usted puede descargar el MIB específico que ha sido decodificado y clasificado por los números OID.

El siguiente ejemplo se extrae de la tabla CISCO-PROCESS-MIB.oid. Este ejemplo muestra que el OID para el cpmCPUTotal5minMIB es .1.3.6.1.4.1.9.9.109.1.1.1.1.5.

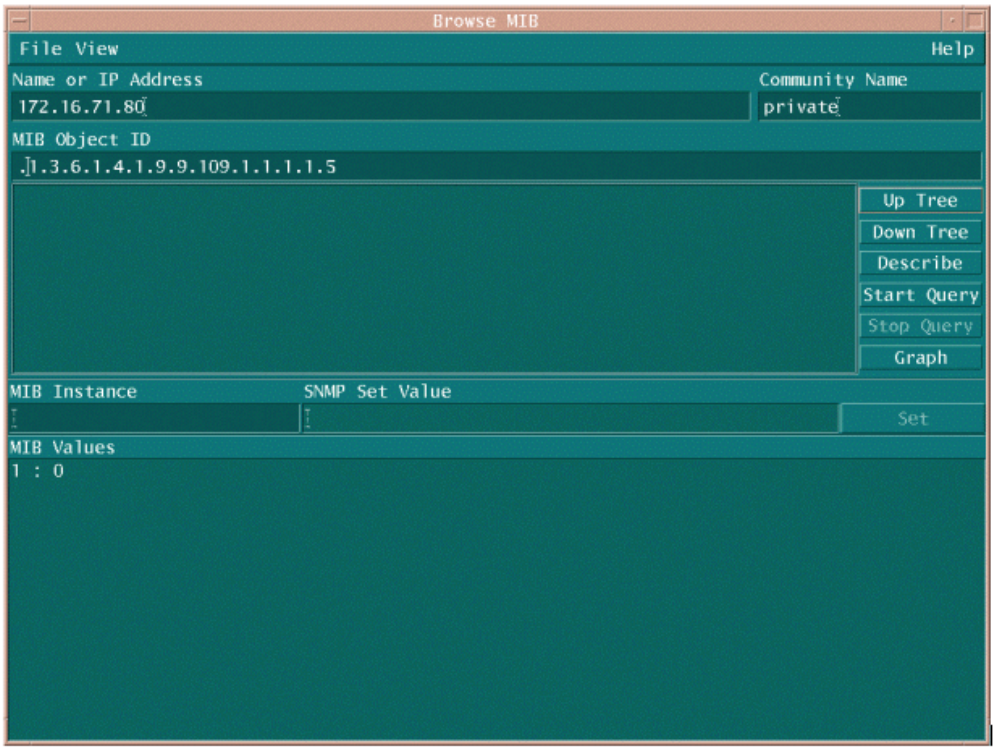
Nota: No olvide agregar "." al principio del OID o del usted conseguirá un error cuando usted intenta sondearlo. Es necesario agregar un ".1" al final del OID para implementarlo. Esto dice a dispositivo el caso del OID que usted está buscando. En algunos casos, los OID tienen más de un caso de un tipo determinado de datos, por ejemplo cuando un router tiene CPU múltiples.

```
ftp://ftp.cisco.com/pub/mibs/oid/CISCO-PROCESS-MIB.oid
### THIS FILE WAS GENERATED BY MIB2SCHEMA
"org" "1.3"
"dod" "1.3.6"
"internet" "1.3.6.1"
"directory" "1.3.6.1.1"
"mgmt" "1.3.6.1.2"
"experimental" "1.3.6.1.3"
"private" "1.3.6.1.4"
"enterprises" "1.3.6.1.4.1"
"cisco" "1.3.6.1.4.1.9"
"ciscoMgmt" "1.3.6.1.4.1.9.9"
"ciscoProcessMIB" "1.3.6.1.4.1.9.9.109"
"ciscoProcessMIBObjects" "1.3.6.1.4.1.9.9.109.1"
"ciscoProcessMIBNotifications" "1.3.6.1.4.1.9.9.109.2"
"ciscoProcessMIBConformance" "1.3.6.1.4.1.9.9.109.3"
"cpmCPU" "1.3.6.1.4.1.9.9.109.1.1"
"cpmProcess" "1.3.6.1.4.1.9.9.109.1.2"
"cpmCPUTotalTable" "1.3.6.1.4.1.9.9.109.1.1.1"
"cpmCPUTotalEntry" "1.3.6.1.4.1.9.9.109.1.1.1.1"
"cpmCPUTotalIndex" "1.3.6.1.4.1.9.9.109.1.1.1.1.1"
"cpmCPUTotalPhysicalIndex" "1.3.6.1.4.1.9.9.109.1.1.1.1.2"
"cpmCPUTotal5sec" "1.3.6.1.4.1.9.9.109.1.1.1.1.3"
"cpmCPUTotal1min" "1.3.6.1.4.1.9.9.109.1.1.1.1.4"
"cpmCPUTotal5min" "1.3.6.1.4.1.9.9.109.1.1.1.1.5"
```

Hay dos maneras comunes de sondear el MIB OID para aseegurarlo es disponible y funcionamiento. Es una buena idea hacer esto antes de que usted comience la colección de datos en bloque de modo que usted no pierda la interrogación del tiempo algo que no está allí y termine para

arriba con las bases de datos vacías. Una manera de hacer esto es utilizar un MIB Walker de su plataforma NMS tal como HP OpenView Network Node Manager (NNM), o el CiscoWorks Windows, y ingresa el OID que usted quiere marcar.

A continuación se presenta un ejemplo desde OpenView SNMP MIB walker.



Otra forma sencilla de sondear el MIB OID es utilizar el **snmpwalk del** comando unix tal y como se muestra en del siguiente ejemplo.

```
nsahpov6% cd /opt/OV/bin
nsahpov6% snmpwalk -v1 -c private 172.16.71.80 .1.3.6.1.4.1.9.9.109.1.1.1.1.5.1

cisco.ciscoMgmt.ciscoProcessMIB.ciscoProcessMIBObjects.cpmCPU.cpmCPUTotalTable.cpmCPUTotalEntry.cpmCPUTotal5min.1 :
```

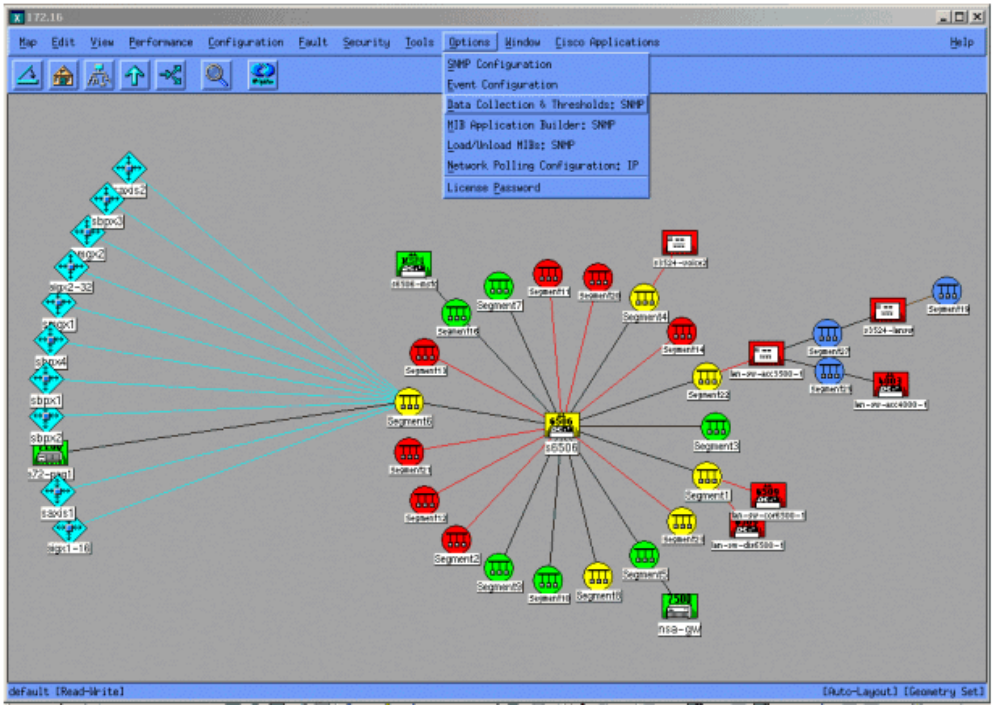
En ambos ejemplos, el MIB volvió un valor de 0, significando que para ese ciclo de sondeo el CPU hizo un promedio de 0 utilizaciones de porcentaje. Si usted tiene dificultad que consigue el dispositivo para responder con los datos correctos, intente hacer ping el dispositivo y acceder el dispositivo por Telnet. Si usted todavía tiene un problema, marque la configuración SNMP y las cadenas de comunidad SNMP. Usted puede necesitar encontrar una alternativa MIB u otra versión del IOS para hacer este trabajo.

Paso 3: Consultar y registrar objetos MIB del SNMP específicos del router

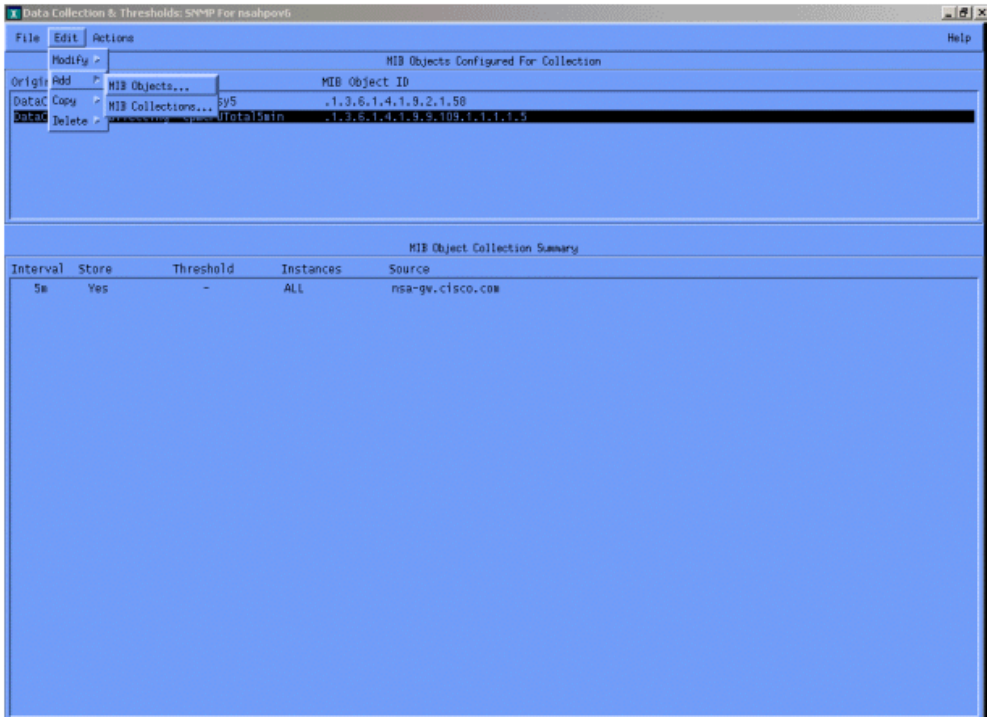
Hay varias maneras de sondear los objetos de MIB y de registrar la salida. Los Productos, los productos gratuitos, los scripts, y las herramientas disponibles del vendedor están disponibles. Todas las herramientas frontales utilizan el SNMP **consiguen el** proceso para obtener la información. Las principales diferencias residen en la flexibilidad de la configuración y en la forma en la que se registran los datos en una base de datos. Una vez más mirada en el procesador MIB para ver cómo estos diversos métodos trabajan.

Ahora que usted sabe el OID se soporta en el router, usted necesita decidir cuantas veces sondearlo y cómo registrarlo. Cisco recomienda que el CPU MIB esté sondeado en los intervalos del minuto cinco. Un intervalo más bajo aumentaría la carga en la red o el dispositivo, y puesto que el valor MIB es un promedio de cinco minutos de todos modos no sería útil sondearlo más a menudo que el valor hecho un promedio. Se recomienda también generalmente que el sondeo de línea de base tiene por lo menos un periodo de dos semanas de modo que usted pueda analizar por lo menos dos ciclos comerciales semanales en la red.

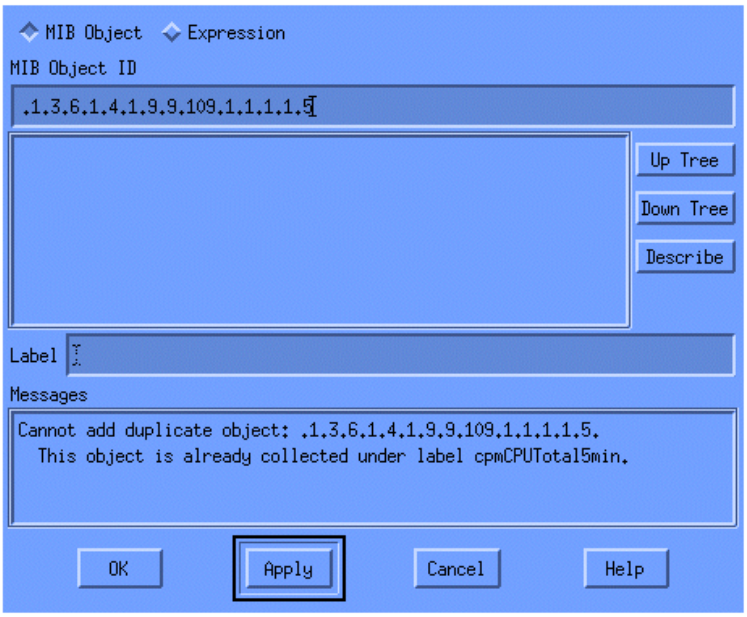
Las siguientes pantallas muestran cómo agregar objetos MIB en la versión 6.1 del OpenView Network Node Manager de HP. De la pantalla principal, seleccione las **opciones > la obtención de datos y los umbrales**.



Entonces seleccione el **Edit (Edición) > Add (Agregar) > MIB Objects (Objetos MIB)**.

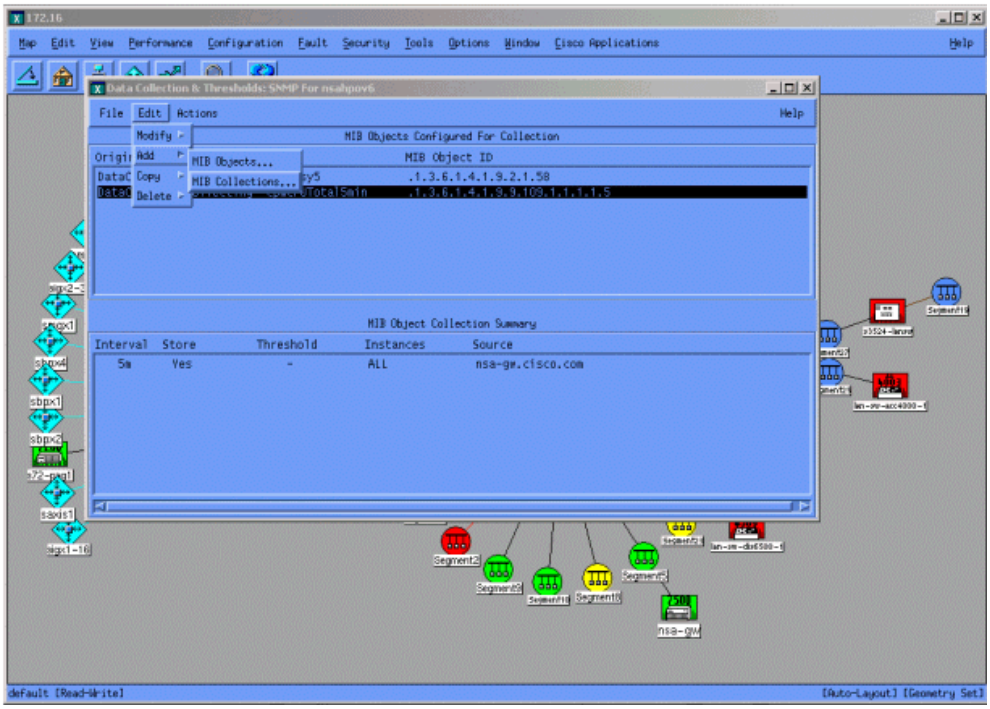


Del menú, agregue la cadena OID y el tecleo **se aplica**. Ahora ingresó el objeto de MIB en una plataforma OpenView de HP para que pueda ser consultado.



Luego debe permitir que HP OpenView conozca el router a interrogar para este OID.

Del menú de la obtención de datos, seleccione el **Edit (Editar) > Add (Agregar) > MIB Collections (Recolecciones MIB)**.

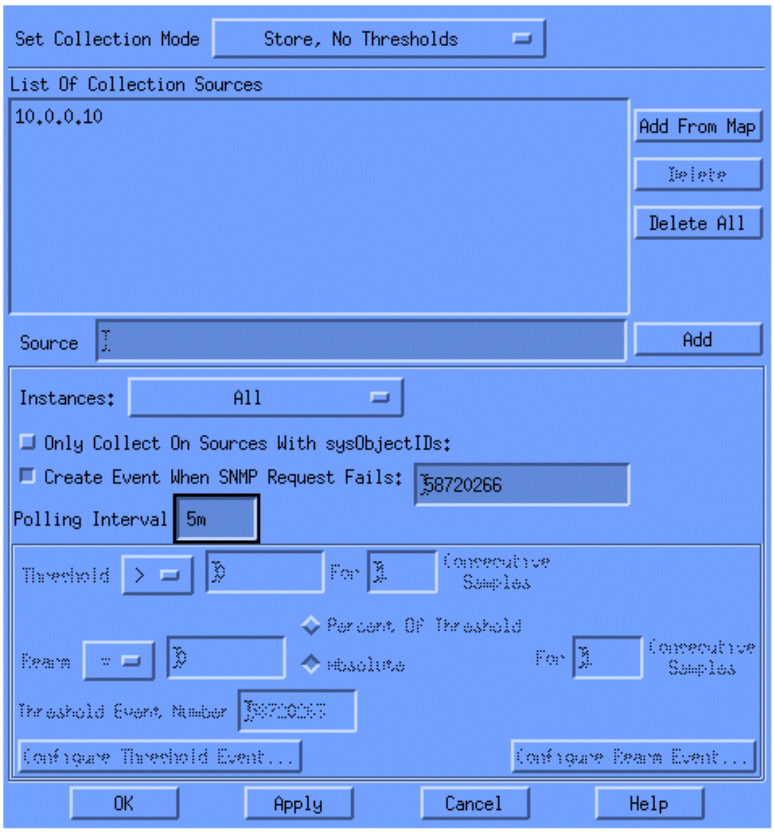


En el campo de fuente, ingrese el nombre del Domain Naming System (DNS) o el IP Address del router que se sondeará.

Seleccione Store (Almacenar), No Thresholds (Sin umbrales) desde la lista Set Collection Mode (Configurar modo de colección).

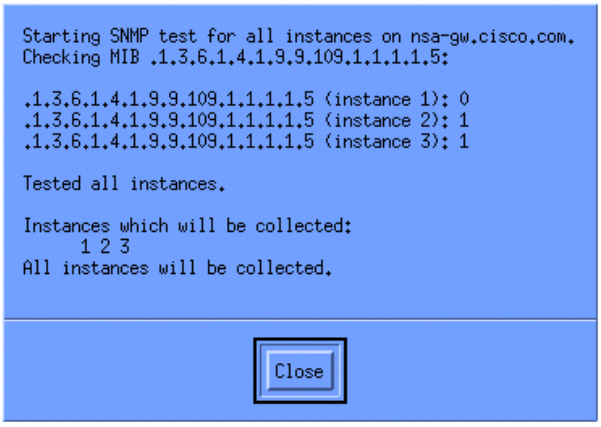
Fije el intervalo de sondeo hasta los **5m**, para cinco intervalos minuciosos.

Haga clic en Apply (Aplicar).



Usted debe seleccionar el **File (Archivo) > Save (Guardar)** para que los cambios tomen la influencia.

Para verificar que la colección esté configurada correctamente, resalte la línea sumaria de la colección para el router y seleccione las **acciones > la prueba SNMP**. Esto verifica si la identificación de comunidad es correcta y realizará el sondeo de todas las instancias de OID.



Haga clic **cerca**, y deje la colección ejecutarse por una semana. En el final del periodo semanal, extraiga los datos para analizarlos.

Los datos se analizan más fácilmente si los descarga en un archivo ASCII y lo importa a una herramienta para hojas de cálculo como Microsoft Excel. Para hacer esto con el NNM HP OpenView, puede usar la herramienta de línea de comando, snmpColDump. Cada colección configurada escribe a un archivo en el directorio de /var/opt/OV/share/databases/snmpCollect/.

Extraiga los datos a un archivo ASCII llamado **testfile** con el siguiente comando:

```
snmpColDump /var/opt/OV/share/databases/snmpCollect/cpmCPUTotal5min.1 > testfile
```

Nota: cpmCPUTotal5min.1 es el archivo de base de datos que el HP OpenView NNM creado cuando el sondeo de OID comenzó.

El archivo de prueba generado es similar al ejemplo siguiente.

```
03/01/2001 14:09:10 nsa-gw.cisco.com 1
03/01/2001 14:14:10 nsa-gw.cisco.com 1
03/01/2001 14:19:10 nsa-gw.cisco.com 1
03/01/2001 14:24:10 nsa-gw.cisco.com 1
03/01/2001 14:29:10 nsa-gw.cisco.com 1
03/01/2001 14:34:10 nsa-gw.cisco.com 1
03/01/2001 14:39:10 nsa-gw.cisco.com 1
03/01/2001 14:44:10 nsa-gw.cisco.com 1
```

```
03/01/2001 14:49:10 nsa-gw.cisco.com 1
03/01/2001 14:54:10 nsa-gw.cisco.com 1
03/01/2001 14:59:10 nsa-gw.cisco.com 1
03/.....
```

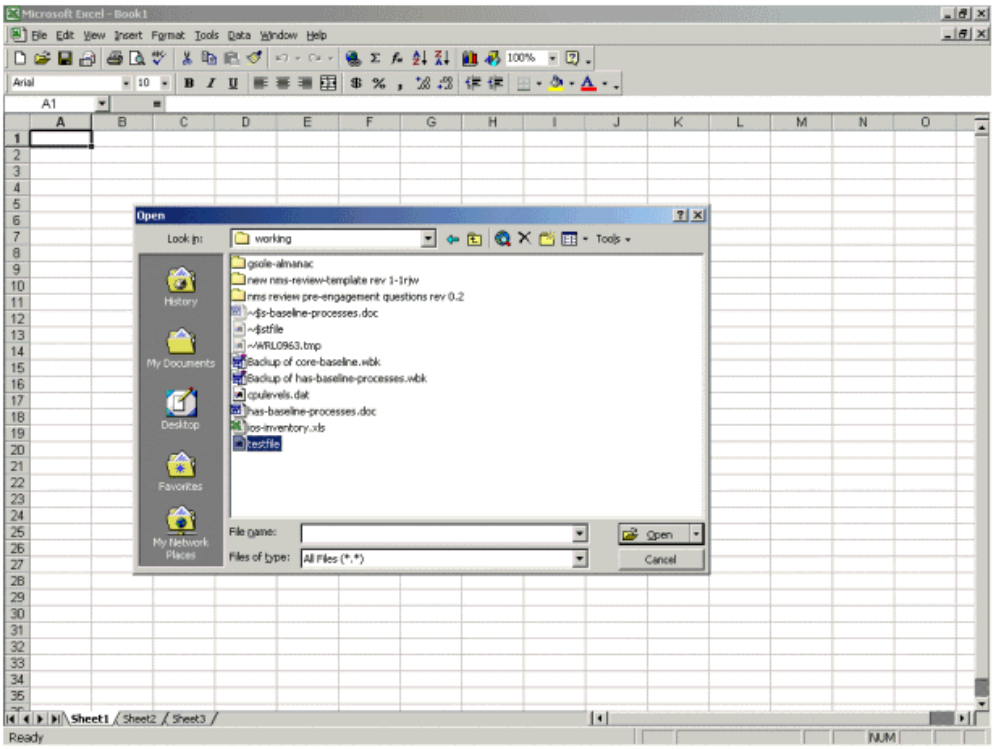
Una vez que el resultado del archivo de prueba está en su estación UNIX, puede transferirla a la PC mediante el Protocolo de transferencia de datos (FTP).

También puede recopilar los datos mediante sus propias secuencias de comandos. Para hacer esto, realizar un **snmpget** para el CPU OID cada cinco minutos y vaciar los resultados en un .csv clasifía.

Paso 4: Analice los datos para determinar los umbrales

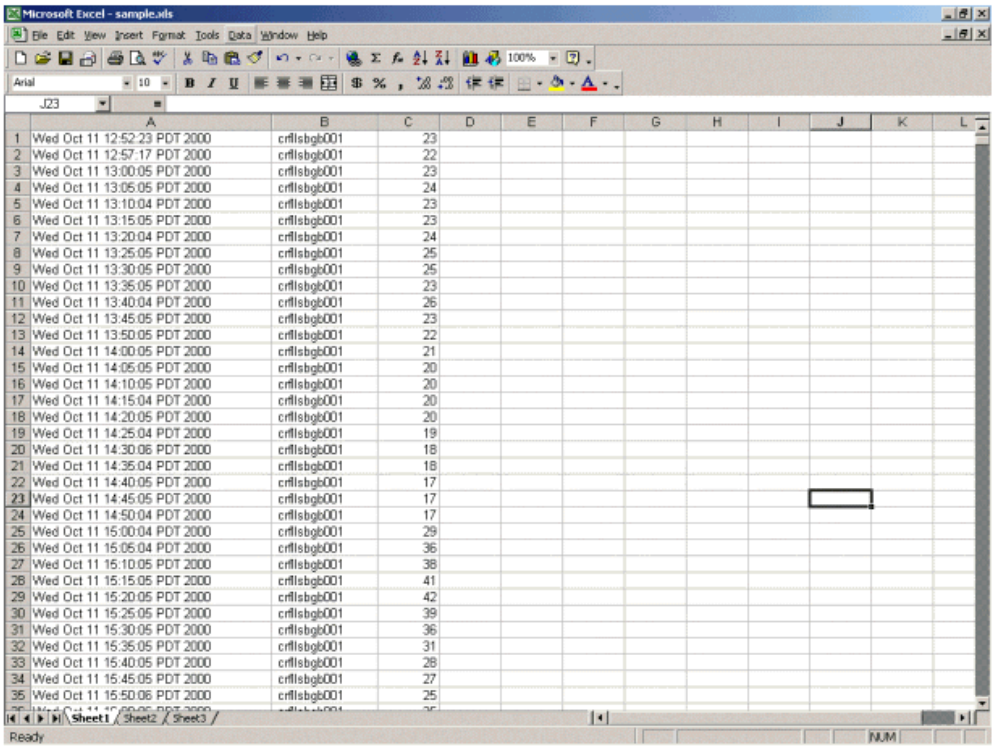
Ahora que usted tiene ciertos datos, usted puede comenzar a analizarlo. Esta fase de la línea de base determina las configuraciones del umbral que puede utilizar que son una medida precisa de rendimiento o falla y que no activará demasiadas alarmas cuando encendamos el monitoreo de umbral. Una de las formas más sencillas para hacer esto consiste en importar los datos en una hoja de cálculo como por ejemplo Microsoft Excel y hacer un cuadro de dispersión. Este método hace muy fácil considerar cuántas veces habría creado un dispositivo determinado una alerta de la excepción si usted la monitoreaba para cierto umbral. No es recomendable girar los umbrales sin hacer una línea de fondo, puesto que éste puede crear las tormentas alertas de los dispositivos que han excedido el umbral que usted ha elegido.

Para importar los archivos de prueba en una hoja de cálculo de Excel, Excel abierto y un **File > Open** selecto y seleccionar su archivo de datos.



La aplicación de Excel entonces le solicita que importe el archivo.

Una vez terminado, el archivo importado debería lucir parecido a la pantalla siguiente.

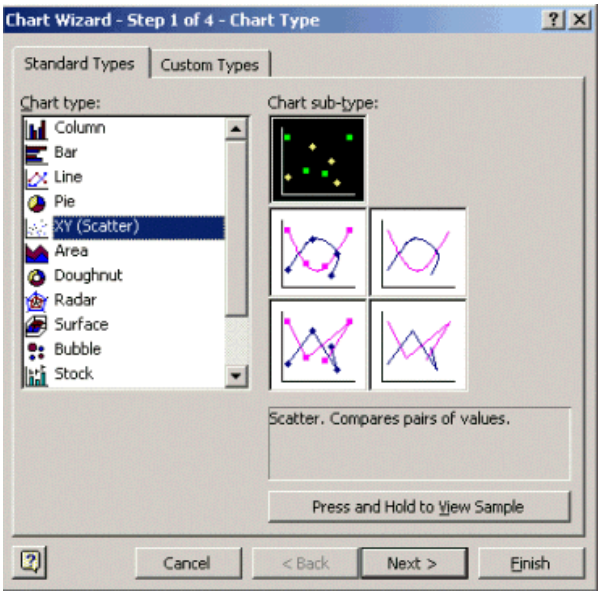


	A	B	C
1	Wed Oct 11 12:52:23 PDT 2000	crfllsbgb001	23
2	Wed Oct 11 12:57:17 PDT 2000	crfllsbgb001	22
3	Wed Oct 11 13:00:05 PDT 2000	crfllsbgb001	23
4	Wed Oct 11 13:05:05 PDT 2000	crfllsbgb001	24
5	Wed Oct 11 13:10:04 PDT 2000	crfllsbgb001	23
6	Wed Oct 11 13:15:05 PDT 2000	crfllsbgb001	23
7	Wed Oct 11 13:20:04 PDT 2000	crfllsbgb001	24
8	Wed Oct 11 13:25:05 PDT 2000	crfllsbgb001	25
9	Wed Oct 11 13:30:05 PDT 2000	crfllsbgb001	25
10	Wed Oct 11 13:35:05 PDT 2000	crfllsbgb001	23
11	Wed Oct 11 13:40:04 PDT 2000	crfllsbgb001	26
12	Wed Oct 11 13:45:05 PDT 2000	crfllsbgb001	23
13	Wed Oct 11 13:50:05 PDT 2000	crfllsbgb001	22
14	Wed Oct 11 14:00:05 PDT 2000	crfllsbgb001	21
15	Wed Oct 11 14:05:05 PDT 2000	crfllsbgb001	20
16	Wed Oct 11 14:10:05 PDT 2000	crfllsbgb001	20
17	Wed Oct 11 14:15:04 PDT 2000	crfllsbgb001	20
18	Wed Oct 11 14:20:05 PDT 2000	crfllsbgb001	20
19	Wed Oct 11 14:25:04 PDT 2000	crfllsbgb001	19
20	Wed Oct 11 14:30:06 PDT 2000	crfllsbgb001	18
21	Wed Oct 11 14:35:04 PDT 2000	crfllsbgb001	18
22	Wed Oct 11 14:40:05 PDT 2000	crfllsbgb001	17
23	Wed Oct 11 14:45:05 PDT 2000	crfllsbgb001	17
24	Wed Oct 11 14:50:04 PDT 2000	crfllsbgb001	17
25	Wed Oct 11 15:00:04 PDT 2000	crfllsbgb001	29
26	Wed Oct 11 15:05:04 PDT 2000	crfllsbgb001	36
27	Wed Oct 11 15:10:05 PDT 2000	crfllsbgb001	38
28	Wed Oct 11 15:15:05 PDT 2000	crfllsbgb001	41
29	Wed Oct 11 15:20:05 PDT 2000	crfllsbgb001	42
30	Wed Oct 11 15:25:05 PDT 2000	crfllsbgb001	39
31	Wed Oct 11 15:30:05 PDT 2000	crfllsbgb001	36
32	Wed Oct 11 15:35:05 PDT 2000	crfllsbgb001	31
33	Wed Oct 11 15:40:05 PDT 2000	crfllsbgb001	28
34	Wed Oct 11 15:45:05 PDT 2000	crfllsbgb001	27
35	Wed Oct 11 15:50:06 PDT 2000	crfllsbgb001	25

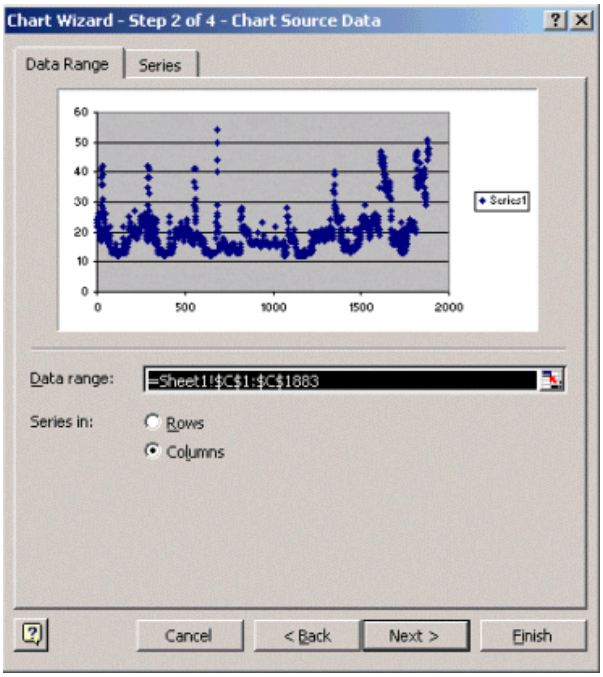
Una carta de la dispersión le permite a visualiza más fácilmente cómo los diversos establecimientos del umbral trabajarían en la red.

Para crear el gráfico de dispersión, resalte la columna C en el archivo importado y luego haga clic en el icono del asistente para gráficos. Siga los pasos del Chart Wizard (Asistente para la creación de cuadros) para crear un cuadro de dispersión.

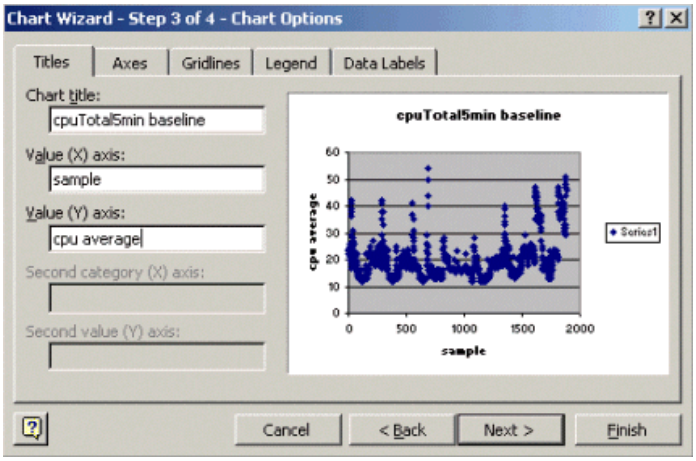
En el paso del Asistente para gráficos 1, como se muestra abajo, seleccione la lengueta **estándar de los tipos**, y seleccione el tipo **XY de la** carta **(de la dispersión)**. Luego haga clic en Next (Siguiente).



En el paso del Asistente para gráficos 2, como se muestra abajo, seleccione la lengueta del **rango de datos** y seleccione el rango de datos y **opción Columns (Columnas)**. Haga clic en Next (Siguiente).



En el paso del Asistente para gráficos 3, como se muestra abajo, ingrese los valores del título de la carta y del eje X y Y, y después haga clic **después**.



En el paso del Asistente para gráficos 4, seleccione si usted quiere la carta de la dispersión en una nueva página o como objeto en la página existente.

Clic en Finalizar para poner la carta en su ubicación deseada.

"Qué si?" Análisis

Ahora puede utilizar el gráfico de dispersión para realizar un análisis. Sin embargo, antes de proceder, usted necesita hacer las preguntas siguientes:

- ¿Qué recomienda el proveedor (en este ejemplo el proveedor es Cisco) como umbral para esta variable MIB?

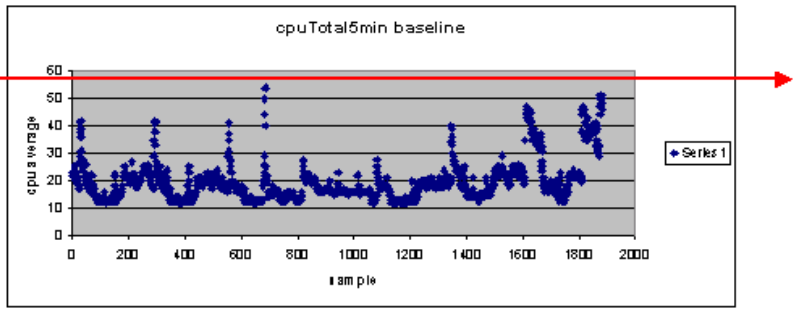
  Cisco recomienda generalmente que un router del núcleo no excede la utilización de la CPU media del 60 por ciento. El sesenta por ciento fue elegido porque un router necesita un ciertos gastos indirectos en caso de que experimenten el problema o la red tiene algunos errores. Cisco estima que un router del núcleo necesita aproximadamente 40 porcentaje de la CPU por encima en caso de que un Routing Protocol tenga que recalcular o reconverge. Estos porcentajes varían en función de los protocolos que utiliza y la topología y estabilidad de la red.
- ¿Qué ocurre si utilizo un 60% como establecimiento del umbral?

  Si usted drena una línea a través de la carta de la dispersión horizontalmente en 60, usted verá que ningunos de los puntos de datos exceden 60 por ciento de uso de la CPU. Un umbral del conjunto 60 en sus estaciones del sistema de administración de la red (NMS) no habrá fijado tan de una alarma de umbral durante el período del sondeo. Un porcentaje de 60 es aceptable para este router. Sin embargo, aviso en la carta de la dispersión que algunos de los puntos de datos están cercanos a 60. Sería agradable saber cuando un router está acercando al umbral del 60 por ciento así que usted puede saber antes de tiempo que el CPU se está acercando al 60 por ciento y tener un plan para que lo que haga cuando alcanza esa punta.
- ¿Qué si fijé el umbral al 50 por ciento?

  Se estima que este router alcanzó la utilización de porcentaje 50 cuatro veces durante este ciclo de sondeo y habría generado una alarma de umbral cada vez. Este proceso llega a ser más importante cuando usted mira a los *grupos de Routers* para ver lo que harían los diversos

establecimientos del umbral. Por ejemplo, “qué si fijé el umbral en el 50 por ciento para la red del núcleo entera?” Es muy difícil elegir sólo un número.

Umbral de la CPU “qué si” análisis



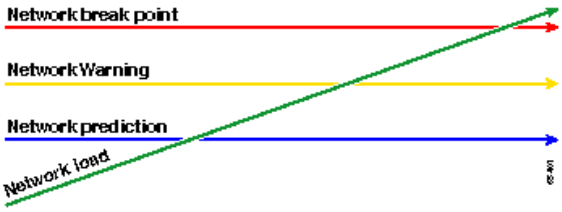
Una estrategia que usted puede utilizar para hacer este más fácil está la lista, conjunto, va metodología de umbral. Esta metodología utiliza tres números sucesivos de umbral.

- Ready (Listo)—el umbral que estableció como indicador de qué dispositivos quizá necesiten atención en el futuro
- Set—el umbral que se usa como un indicador previo que le avisa que comienza la planificación para una reparación, actualización o nueva configuración.
- Vaya — el umbral que usted y/o el vendedor creen es una condición de falla y requiere una cierta acción repararla; en este ejemplo es el 60 por ciento

La siguiente tabla muestra la táctica de la estrategia Ready, Set, Go (listo, preparado, ya).

Umbral	Acción	Resultado
45 por ciento	Investigue más lejos	Lista de opciones para los planes de acción
el 50 por ciento	Formule el plan de acción	Lista de pasos en el plan de acción
60 por ciento	Implemente el plan de acción	El router ya no supera los umbrales. De nuevo al modo listo

La metodología Listo, Preparado, Ya cambia el gráfico de línea de base tratado anteriormente. El siguiente diagrama muestra el cuadro cambiado de línea de base. Si usted puede identificar los otros puntos de intersección en la carta, usted ahora tiene más tiempo para planear y para reaccionar que usted hizo antes.



Note que en este proceso, la atención está centrada en las excepciones en la red y no referida a los otros dispositivos. Se asume que mientras los dispositivos estén debajo de los umbrales, están muy bien.

Si usted hace estos pasos pensar hacia fuera desde el principio, usted estará bien preparado para mantener la red sana. La ejecución de este tipo de hojas de operación (planning) es también extremadamente útil para la planificación del presupuesto. Si usted conoce qué **van** sus cinco superiores al Routers, sus routeres medios listos, y son sus **routeres preparados** inferiores, usted puede planear fácilmente en cuánto presupuesto usted necesitará para las actualizaciones basadas en qué clase de Routers son y cuáles son sus opciones del plan de acción. La misma estrategia se puede utilizar para los links o cualquier otro MIB OID del Red de área ancha (WAN).

Paso 5: Problemas inmediatos identificados arreglo

Esta es una de las partes más sencillas del proceso de la línea de base. Una vez que haya identificado qué dispositivos exceden el paso del umbral, es recomendable que confeccione un plan de acción para devolver esos dispositivos dentro del umbral.

Usted puede abrir un caso con el Centro de Asistencia Técnica (TAC) de Cisco o entrar en contacto a su técnico para las opciones disponibles. Usted no debe asumir que eso conseguir a las cosas el umbral inferior posterior costará le a dinero. Algunos problemas de CPU pueden ser solucionados cambiando la configuración para asegurar que todos los procesos se estén ejecutando de la manera más eficaz. Por ejemplo, algún Listas de control de acceso (ACL) puede hacer CPU del router para ejecutar mismo el elevado debido a la trayectoria los paquetes para tomar a través del router. En algunos casos, usted puede implementar el Switching de Netflow para cambiar la trayectoria de conmutación de conjunto de bits y para reducir el impacto del ACL en el CPU. Más allá del problema, es necesario que todos los routers vuelvan a estar bajo el umbral en este paso para que usted pueda implementar los umbrales más tarde sin correr el riesgo de inundar las estaciones NMS con demasiadas alarmas de umbral.

Paso 6: Monitoreo del umbral de prueba

Este paso implica evaluar los umbrales en el laboratorio mediante las herramientas que usará en la red de producción. Existen dos enfoques comunes para la supervisión de umbrales. Debe decidir qué método es el mejor para su red.

- Sondee y compare el método usando la plataforma SNMP o la otra herramienta de supervisión SNMP

  Este método utiliza más ancho de banda de la red para el tráfico de sondeo y toma los ciclos de procesamiento en su plataforma SNMP.
- Use configuraciones de alarmas y eventos RMON (Monitoreo remoto) en los routers de modo que envíen una alarma sólo cuando se exceda un umbral.

  Este método reduce el uso del ancho de banda de la red, pero también aumenta el uso de la memoria y de la CPU en los routers.

Implementar un umbral usando el SNMP

Para configurar el método SNMP usando el HP OpenView NNM, las **opciones** selectas **> la obtención de datos y umbrales** como usted lo hizo cuando usted configura el sondeo inicial. Esta vez, sin embargo, en el menú de colecciones seleccione Store (tienda), Check Thresholds (comprobar umbrales) en lugar de Store, No Thresholds (sin umbrales). Después de que usted configure el umbral, usted puede aumentar la utilización de la CPU en el router enviándole los ping múltiples y/o el SNMP múltiple recorre. Tendrá que disminuir el valor del umbral si no puede hacer que la utilidad de la CPU sea lo suficientemente alta como para cruzar el umbral. En todo caso, usted debe asegurarse de que el threshold mechanism esté trabajando.

Una de las limitaciones de usar este método es que no se pueden implementar umbrales múltiples en forma simultánea. Necesitará tres plataformas SNMP para establecer tres umbrales diferentes simultáneamente. Las herramientas tales como Integridades de la red Concord y TENDENCIA Trinagy permiten los umbrales múltiples para el mismo caso OID.

Si su sistema puede dirigir solamente un en un momento del umbral, usted puede considerar el listo, conjunto, va estrategia en la moda serial. Esto es, cuando se alcanza en forma continua el umbral ready (listo), comience su investigación y eleve el umbral para al nivel set (preparado) establecido para ese dispositivo. Cuando se alcanza el nivel “set” de manera continua, comience a formular su plan de acción y eleve el umbral hasta el nivel “go” para ese dispositivo. Luego el go threshold se alcanza continuamente, implemente su plan de acción. Esto debería funcionar tan bien como el método de tres umbrales simultáneos. Apenas tarda un poco más tiempo que cambia los establecimientos del umbral de la plataforma SNMP.

Implementar un umbral usando la alarma RMON y el evento

Mediante el uso de las configuraciones de alarma RMON y de sucesos, puede hacer que el router se monitoree a sí mismo para varios umbrales. Cuando el router detecta una condición que excede el umbral, envía una trampa de SNMP a la plataforma SNMP. Debe tener un receptor de trampa SNMP establecido en la configuración de su router para que la trampa sea reenviada. Existe una correlación entre alarma y evento. La alarma marca el OID para el umbral dado. Si se alcanza el umbral, el proceso de la alarma enciende el proceso del evento que puede cualquiera enviar un mensaje de trampa SNMP, crea una entrada de registro RMON, o ambas. Para más detalle en este comando, vea la alarma RMON y los Comandos de configuración de eventos.

Los siguientes comandos de configuración de router tienen el monitor del router cpmCPUTotal5min cada 300 segundos. Encenderá el evento 1 si el CPU excede el 60 por ciento y encenderá el evento 2 cuando el CPU recurre al 40 por ciento. En ambos casos, un mensaje de trampa SNMP será enviado a la estación NMS con la cadena del soldado de la comunidad.

Para usar el método Listos, preparados, ya, use todos los siguientes enunciados de configuración.

```
rmon event 1 trap private description "cpu hit60%" owner jharp
rmon event 2 trap private description "cpu recovered" owner jharp
rmon alarm 10 cpmCPUTotalTable.1.5.1 300 absolute rising 60 1 falling 40 2 owner jharp


rmon event 3 trap private description "cpu hit50%" owner jharp
rmon event 4 trap private description "cpu recovered" owner jharp
rmon alarm 20 cpmCPUTotalTable.1.5.1 300 absolute rising 50 3 falling 40 4 owner jharp

rmon event 5 trap private description "cpu hit 45%" owner jharp
rmon event 6 trap private description "cpu recovered" owner jharp
rmon alarm 30 cpmCPUTotalTable.1.5.1 300 absolute rising 45 5 falling 40 6 owner jharp
```

El siguiente ejemplo muestra el resultado del comando show rmon alarm que fue configurado por los enunciados anteriores.

```
zack#sh rmon alarm
Alarm 10 is active, owned by jharp
Monitors cpmCPUTotalTable.1.5.1 every 300 second(s)
Taking absolute samples, last value was 0
Rising threshold is 60, assigned to event
1
Falling threshold is 40, assigned to event
```

```
2
On startup enable rising or falling alarm
Alarm 20 is active, owned by jharp
Monitors cpmCPUTotalTable.1.5.1 every 300 second(s)
Taking absolute samples, last value was 0
Rising threshold is 50, assigned to event
3
Falling threshold is 40, assigned to event
4
On startup enable rising or falling alarm
Alarm 30 is active, owned by jharp
Monitors cpmCPUTotalTable.1.5.1 every 300 second(s)
Taking absolute samples, last value was 0
Rising threshold is 45, assigned to event
5
Falling threshold is 40, assigned to event
6
On startup enable rising or falling alarm
```

El siguiente ejemplo muestra el resultado del comando show rmon event.

```
zack#sh rmon event
Event 1 is active, owned by jharp
Description is cpu hit60%
Event firing causes trap to community
private, last fired 00:00:00
Event 2 is active, owned by jharp
Description is cpu recovered
Event firing causes trap to community
private, last fired 02:40:29
Event 3 is active, owned by jharp
Description is cpu hit50%
Event firing causes trap to community
private, last fired 00:00:00
Event 4 is active, owned by jharp
Description is cpu recovered
Event firing causes trap to community
private, last fired 00:00:00
Event 5 is active, owned by jharp
Description is cpu hit 45%
Event firing causes trap to community
private, last fired 00:00:00
Event 6 is active, owned by jharp
Description is cpu recovered
Event firing causes trap to community
private, last fired 02:45:47
```

Pruebe ambos métodos para decidir cuál se adecua mejor a su entorno. Incluso puede encontrar que una combinación de métodos funciona sin problemas. En todo caso, la prueba se debe hacer en un ambiente de laboratorio para asegurarse de que todo trabaja correctamente. Después de probar en el laboratorio, una instrumentación limitada en un pequeño grupo de Routers permitirá que usted pruebe el proceso de enviar las alertas a su centro de operaciones.

En este caso, usted tendrá que bajar los umbrales para probar el proceso: El intentar aumentar artificial el CPU en un router de producción no se recomienda. También debe asegurarse de que cuando llegan las alertas a las estaciones NMS en el centro de operaciones, hay una política de escalada que le permite estar seguro de que se le informa sobre los dispositivos que excedieron los umbrales. Estas configuraciones se han probado en un laboratorio con Cisco IOS Versión 12.1(7). Si usted encuentra cualesquiera problemas, usted debe marcar con Cisco que dirige o los técnicos para ver si usted tiene un bug en su versión de IOS.

Paso 7: Implemente el monitoreo de umbral que usa el SNMP o el RMON

Una vez que usted haya testeado cuidadosamente el umbral del monitoreo en el laboratorio y en un despliegue limitado, estará listo para implementar el umbral a lo largo del núcleo de la red. Ahora puede implementar sistemáticamente este proceso de línea de base para otras variables MIB importantes en su red, como búfers, memoria libre, errores de verificación de redundancia cíclica (CRC), pérdida de celdas ATM y demás.

Si usted utiliza la alarma RMON y las configuraciones de evento, usted puede ahora parar el sondear de su estación NMS. Esto disminuirá la carga en su servidor NMS y la cantidad de datos de sondeo en la red. Sistemáticamente pasando con este proceso para los indicadores de estado de la red importante, usted podría venir fácilmente a la punta que el equipo de red se está monitoreando usando la alarma RMON y el evento.

MIB adicionales

Después de que usted haya aprendido este proceso, usted puede querer investigar el otro MIB a la línea de fondo y monitorear. Las siguientes subsecciones presentan una breve lista de algunas OID y descripciones que le pueden resultar útiles.

MIB del router

Las características de la memoria son muy útiles en determinar la salud de un router. Un router saludable debe casi siempre tener espacio del búfer disponible con el cual trabajar. Si el router comienza a ejecutarse fuera del espacio del búfer, el CPU tendrá que trabajar más difícilmente para crear los nuevos buffers y para intentar encontrar los buffers para entrante y los paquetes de salida. Un debate en detalle de los buffers está fuera del alcance de este documento. Sin embargo, como regla general, un router saludable debe tener pocas o incluso ningúas faltas del buffer y no debe tener ningunas fallas del almacén intermedio, o una condición de cero memoria libre.

Objeto	Descripción	OID (ID del objeto)
ciscoMemoryPoolFree	La cantidad de bytes del agrupamiento de memoria que no se utilizan actualmente en el dispositivo administrado	1.3.6.1.4.1.9.9.48.1.1.1.6
ciscoMemoryPoolLargestFree	El número más grande de bytes contiguos del agrupamiento de memoria que son Currently Unused	1.3.6.1.4.1.9.9.48.1.1.1.7
bufferElMiss	Cantidad de omisiones de elementos de memoria intermedia	1.3.6.1.4.1.9.2.1.12
bufferFail	Cantidad de fallas de asignación de memorias intermedias	1.3.6.1.4.1.9.2.1.46
bufferNoMem	La cantidad de memoria intermedia genera fallas debido a que no hay memoria libre	1.3.6.1.4.1.9.2.1.47

Catalyst Switch MIBs

Objeto	Descripción	OID (ID del objeto)
cpmCPUTotal5min	Porcentaje de ocupado de la CPU total en el periodo de cinco minutos más pasado. Este objeto desaprueba el objeto avgBusy5 de OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5
cpmCPUTotal5sec	Porcentaje de ocupado de la CPU total en el período de cinco segundos más pasado. Este objeto hace que el objeto busyPer de OLD-CISCO-SYSTEM-MIB se vuelva obsoleto	1.3.6.1.4.1.9.9.109.1.1.1.3
Tráfico del sistema	El porcentaje de uso del ancho de banda para el intervalo de consultas previo	1.3.6.1.4.1.9.5.1.1.8
sysTrafficPeak	El valor de medidor de tráfico máximo desde la última vez que los contadores del puerto se borraron o que se inició el sistema.	1.3.6.1.4.1.9.5.1.1.19
sysTrafficPeaktime	El tiempo (en centésimos de un segundo) desde que ocurrió el valor del medidor de tráfico pico	1.3.6.1.4.1.9.5.1.1.20
portTopNUtilization	Utilización del puerto en el sistema	1.3.6.1.4.1.9.5.1.20.2.1.4
portTopNBufferOverFlow	La cantidad de sobrecargas en memoria intermedia del puerto en el sistema	1.3.6.1.4.1.9.5.1.20.2.1.10

MIB de link serial

Objeto	Descripción	OID (ID del objeto)
locIfInputQueueDrops	La cantidad de paquetes perdidos porque la cola de entrada estaba completa	1.3.6.1.4.1.9.2.2.1.1.26
locIfOutputQueueDrops	La cantidad de paquetes perdidos porque la cola de salida estaba completa	1.3.6.1.4.1.9.2.2.1.1.27
locIfInCRC	Cantidad de paquetes de entrada que presentaron errores de suma de comprobación por redundancia cíclica	1.3.6.1.4.1.9.2.2.1.1.12

Comandos de configuración de evento y alarma RMON

Alarmas

Las alarmas RMON pueden configurarse dentro de la siguiente sintaxis:

```
rmon alarm number variable interval {delta | absolute} rising-threshold value
          [event-number] falling-threshold value [event-number]
          [owner string]
```

Elemento	Descripción
número	El número de la alarma, que es idéntico al valor de alarmIndex de la tabla alarmTable, en la MIB de RMON.
Variable	La MIB se opone al control lo que se traduce en la alarmVariable utilizada en la alarmTable de la MIB de RMON.
intervalo	El tiempo en segundos en que la alarma controla la variable MIB, que es idéntico al alarmInterval que se usó en la alarmTable de la MIB de RMON.
delta	Prueba el cambio entre las variables MIB, que afecta al alarmSampleType en el alarmTable del MIB DE RMON.
absoluto	Prueba cada variable MIB directamente, lo que afecta el alarmSampleType en la alarmTable de la MIB de RMON.
valor de umbral ascendente	El valor en el cual se acciona la alarma.
event-number	(Opcional) el número de evento a accionar cuando el levantamiento o el umbral descendente excede su límite. Este valor es idéntico al alarmRisingEventIndex o al alarmFallingEventIndex en la tabla de alarma del RMON MIB.
valor de umbral descendente	Valor en el que se reinicia la alarma.
La cadena owner	(Opcional) Especifique un propietario para la alarma, que sea idéntico al alarmOwner en la Tabla de la alarma del MIB de RMON.

Eventos

Los eventos RMON pueden configurarse dentro de la siguiente sintaxis:

```
rmon event number [log] [trap community] [description string]
          [owner string]
```

Elemento	Descripción
número	Número de evento asignado, que es idéntico al eventIndex en el

	eventTable en el MIB DE RMON.
registro	(Opcional) Genera una entrada de registro RMON cuando se activa un evento y configura eventType en la RMON MIB en registro o en registro y trampa.
comunidad de trampa	(Opcional) Cadena de comunidad SNMP utilizada para esta trampa. Configura la configuración del eventType en el MIB DE RMON para esta fila como SNMP-desvío o registro-y-desvío. Este valor es idéntico al eventCommunityValue en el eventTable en el MIB DE RMON.
description string	(Opcional) Especifica una descripción del evento que es idéntica a la que figura en la tabla de eventos de la MIB de RMON.
La cadena owner	(Opcional) Propietario de este evento, que es idéntico al eventOwner en la tabla eventTable de la MIB de RMON.

Alarma RMON e implementación de eventos

Para información detallada sobre la implementación de eventos y alarma de RMON, lea por favor la sección de implementación de eventos y alarma de RMON del White Paper de las *mejores prácticas de los sistemas de administración de red*.

Información Relacionada

- **Technology White Paper**

Fecha de Generación del PDF: 24 Agosto 2015

http://www.cisco.com/cisco/web/support/LA/102/1025/1025763_HAS_baseline.html