White Paper dos melhores prática do processo de linha de base

Índice

Introdução

Este documento descreve os conceitos fundamentais e os procedimentos para redes de alta disponibilidade. Inclui fatores críticos ao sucesso para a de sucessão crítica para que a avaliação comparativa e o limite de rede ajude a avaliar o sucesso. Ele também fornece detalhes significativos processos para de linha de base e limites e a implementação que segue as diretrizes de práticas recomendadas identificadas pela equipe da Cisco de High Availability Services (HAS).

Este documento toma-o ponto por ponto com o processo de linha de base. Algum Produtos do sistema de administração da rede atual (NMS) pode ajudar a automatizar este processo, contudo, o processo da linha de base permanece o mesmo se você usa ferramentas automatizadas ou manuais. Se você usa estes produtos de NMS, você deve ajustar as configurações de limiar do

padrão para seu ambiente de rede exclusiva. É importante ter um processo para escolher inteligentemente aqueles pontos iniciais de modo que estejam significativos e corretos.

Linha de base

O que é uma linha de base?

Uma linha de base é um processo para estudar a rede em intervalos regulares para assegurar-se de que a rede esteja trabalhando como projetado. É mais do que um único relatório que detalha a saúde da rede em algum ponto a tempo. Seguindo o processo de linha de base, você pode obter a informação seguinte:

- Ganhe a informação valiosa na saúde do hardware e software
- Determine as utilizações de recurso de rede atuais
- Faça decisões precisas sobre pontos iniciais do alarme de rede
- Identifique problemas da rede atual
- Preveja problemas futura

Uma outra maneira de olhar a linha de base é ilustrada no seguinte diagrama.

A linha vermelha, o ponto de ruptura de rede, é o ponto em que a rede será interrompida, o que é determinado pelo conhecimento do desempenho do hardware e do software. A linha verde, a carga da rede, é a progressão natural de carga na rede à medida que novos aplicativos são adicionados e outros fatores.

A finalidade de uma linha de base é determinar:

- Onde sua rede está na linha verde
- Como rapidamente a carga de rede está aumentando
- Preveja esperançosamente em que ponto a tempo os dois cruzarão

Executando uma linha de base numa base regular, você pode encontrar o estado atual *e* extrapolá-lo quando as falhas ocorrerão e se prepararão para eles adiantado. Isso também o ajuda a tomar decisões mais informadas sobre quando, onde e como gastar o dinheiro do orçamento em atualizações de rede.

Por que uma linha de base?

Um processo de linha de base ajuda-o a identificar e planejar corretamente para edições da limitação dos recursos críticos na rede. Estas edições podem ser descritas como recursos de plano do controle ou recursos de plano dos dados. Os recursos de plano do controle são originais à plataforma e aos módulos específicos dentro do dispositivo e podem ser impactados um número de incluir das edições:

- Utilização dos dados
- Características permitidas

- Projeto de rede

Os recursos de plano do controle incluem parâmetros como:

- Utilização CPU
- Utilização de memória
- Utilização do buffer

Os recursos de plano dos dados são impactados somente pelo tipo e pela quantidade de tráfego e incluem a utilização do enlace e a utilização de backplane. Pela utilização de recurso da linha de base para áreas crítica, você pode evitar problemas graves de desempenho, ou mais ruim, uma sobrecarga de rede.

Com a introdução de aplicativos sensíveis à latência, como de voz e vídeo, uma avaliação comparativa se faz mais imprescindível do que nunca. Os aplicativos tradicionais do Protocolo de Controle de Transmissão/Protocolo de Internet (TCP/IP) estão perdoando e permitem uma certa quantidade de atraso. A Voz e o vídeo são User Datagram Protocol (UDP) baseado e não permitem retransmissões ou congestionamento de rede.

Devido à mistura nova de aplicativos, a linha de base ajuda-o a compreender edições da utilização dos recursos de plano do plano e dos dados do controle e a planeá-las dinamicamente para que as mudanças e as elevações assegurem o sucesso continuado.

As redes de dados estiveram ao redor por muitos anos. Até recentemente, manter as redes em execução era um processo bastante complacente, com alguma margem de erro. Com a aceitação cada vez maior de aplicativos sensíveis à latência, como VoIP (Voice over IP, Voz sobre IP) o trabalho de funcionamento da rede está cada vez mais difícil e exige mais precisão. A fim ser mais preciso e dar a um administrador de rede uma base sólida em cima de que para controlar a rede, é importante ter alguma ideia de como a rede está sendo executado. Para fazer isso, você deve percorrer um processo chamado linha de base.

Objetivo da linha de base

O objetivo de uma linha de base está a:

1. Determine o status atual dos dispositivos de rede
2. Compare esse estado às diretrizes do desempenho padrão
3. Defina limiares que alertem você quando o status exceder essas diretrizes.

Devido à grande quantidade de dados e da quantidade de tempo que toma para analisar os dados, você deve primeiramente limitar o espaço de uma linha de base para facilitá-la aprender o processo. O local mais lógico e, às vezes, mas vantajoso para começar é o centro da rede. Este parte da rede é geralmente o menor e exige a maioria de estabilidade.

Para a simplicidade, este documento explica como ao Management Information Base muito importante do protocolo administración de red simple da linha de base uma (SNMP MIB): cpmCPUTotal5min. o cpmCPUTotal5min é a média de deterioração do cinco minutos da unidade de processamento central (CPU) de um roteador Cisco, e é um indicador de desempenho do plano do controle. A linha de base será executada em um Cisco 7000 Series Router.

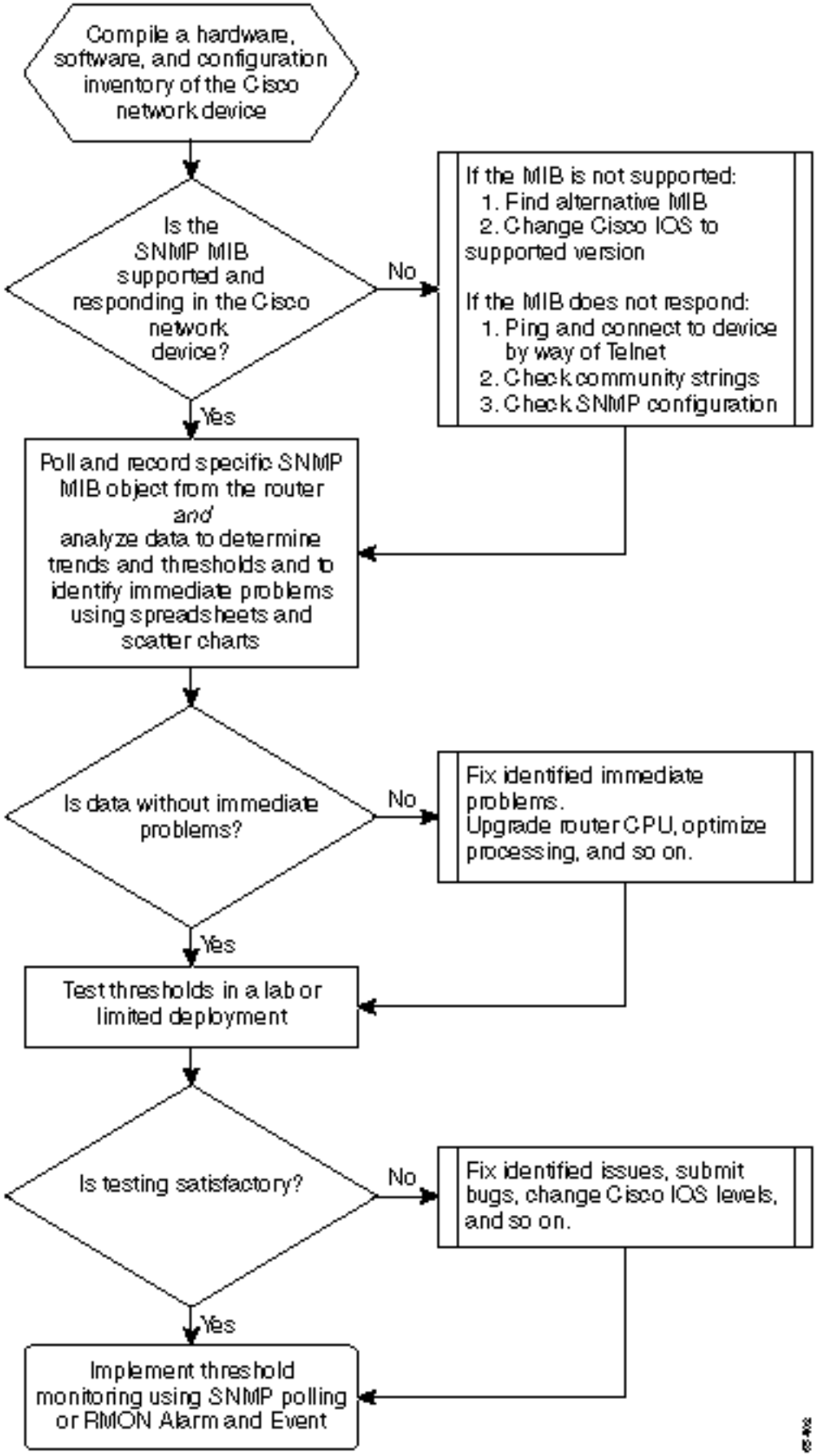
Depois de conhecer o processo, você pode aplicá-lo a qualquer dado disponível no vasto banco de dados SNMP, que está disponível na maioria dos dispositivos Cisco, tais como:

- Uso do Integrated Services Digital Network (ISDN)

- Perda de célula do Asynchronous Transfer Mode (ATM)
- Memória de sistema gratuito

Fluxograma da linha de base central

O seguinte fluxograma mostra as etapas básicas do principal processo de linha de base. Quando o Produtos e as ferramentas estiverem disponíveis para executar algumas destas etapas para você, tende a ter diferenças na flexibilidade ou na acessibilidade. Mesmo se você planeia usar ferramentas de sistema de gerenciamento de rede (NMS) para executar a linha de base, este é ainda um bom exercício em estudar o processo e em compreender como sua rede trabalha realmente. Esse processo pode ser também o mistério de como algumas ferramentas NMS funcionam uma vez que a maioria das ferramentas faz essencialmente as mesmas coisas.



Procedimento de linha de base

Passo 1: Compile um hardware, um software, e um inventário da configuração

Éextremamente importante que você compila um inventário do hardware, do software, e da configuração por vários motivos. Primeiramente, o MIBs de Cisco SNMP é, em alguns casos, específico ao Cisco IOS Release que você está executando. Alguns objetos MIB são substituídos por novos e, às vezes, são completamente eliminados. O inventário de hardware é muito importante depois que os dados são coletados, pois os limiares que você precisa configurar após a linha de base inicial são, com freqüência, baseados no tipo de CPU, na quantidade de memória etc. dos dispositivos Cisco. O inventário de configuração também é importante para garantir que você tenha as configurações atuais: Você pode querer mudar configurações de dispositivo depois que sua linha de base para ajustar bufferes, e assim por diante.

A maneira mais eficaz de fazer com que isto seja parte da linha de base de uma rede Cisco é usar o CiscoWorks2000 Resource Manager Essentials (Essentials). Se este software é instalado corretamente na rede, os fundamentos devem ter os inventários atuais de todos os dispositivos em seu base de dados. Basta observar os estoques para ver se existem problemas.

A tabela a seguir é um exemplo de relatório de inventário do software Cisco Router Class, exportado do Essentials e, em seguida, editado no Microsoft Excel. Deste inventário, observe que você tem que usar dados do SNMP MIB e os identificadores de objeto (OID) encontraram no Cisco IOS 12.0x e 12.1x se liberam.

Nome de dispositivo	Tipo de roteador	Versão	Versão de software
field-2500a.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	I	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)

Se os fundamentos não são instalados na rede, você pode usar a linha de comando unix **snmpwalk da** ferramenta de uma estação de trabalho Unix para encontrar a Versão do IOS. Isso é mostrado no seguinte exemplo: Se você não é certo como este comando trabalha, datilografe o **man snmpwalk na** alerta Unix para mais informação. A versão IOS será importante quando a escolha de qual MIB OIDs para a linha de base começar, porque os objetos dependem do IOS. Igualmente observe que conhecendo o tipo de roteador, você pode mais tarde fazer determinações a respeito do que os pontos iniciais devem ser para o CPU, bufferes, e assim por diante.

```
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
```

Passo 2: Verifique se o SNMP MIB é suportado no roteador

Agora que você tem um inventário do dispositivo que você quer votar para sua linha de base, você pode começar a escolher os OID específicos você quer votar. Salvar muita frustração se você verifica, adiantadamente, que os dados que você quer são realmente lá. O objeto MIB cpmCPUTotal5min está em CISCO-PROCESS-MIB.

Para descobrir para qual OID você deseja efetuar a apuração, é necessária uma tabela de conversão disponível no site de CCO da Cisco. Para acessar este site em um navegador da Web, vá para a página MIBs da Cisco e clique no link OIDs.

Para acessar esse site da Web de um servidor FTP, digite ftp://ftp.cisco.com/pub/mibs/oid/. Deste local, você pode transferir o MIB específico que foi descodificado e classificado por números OID.

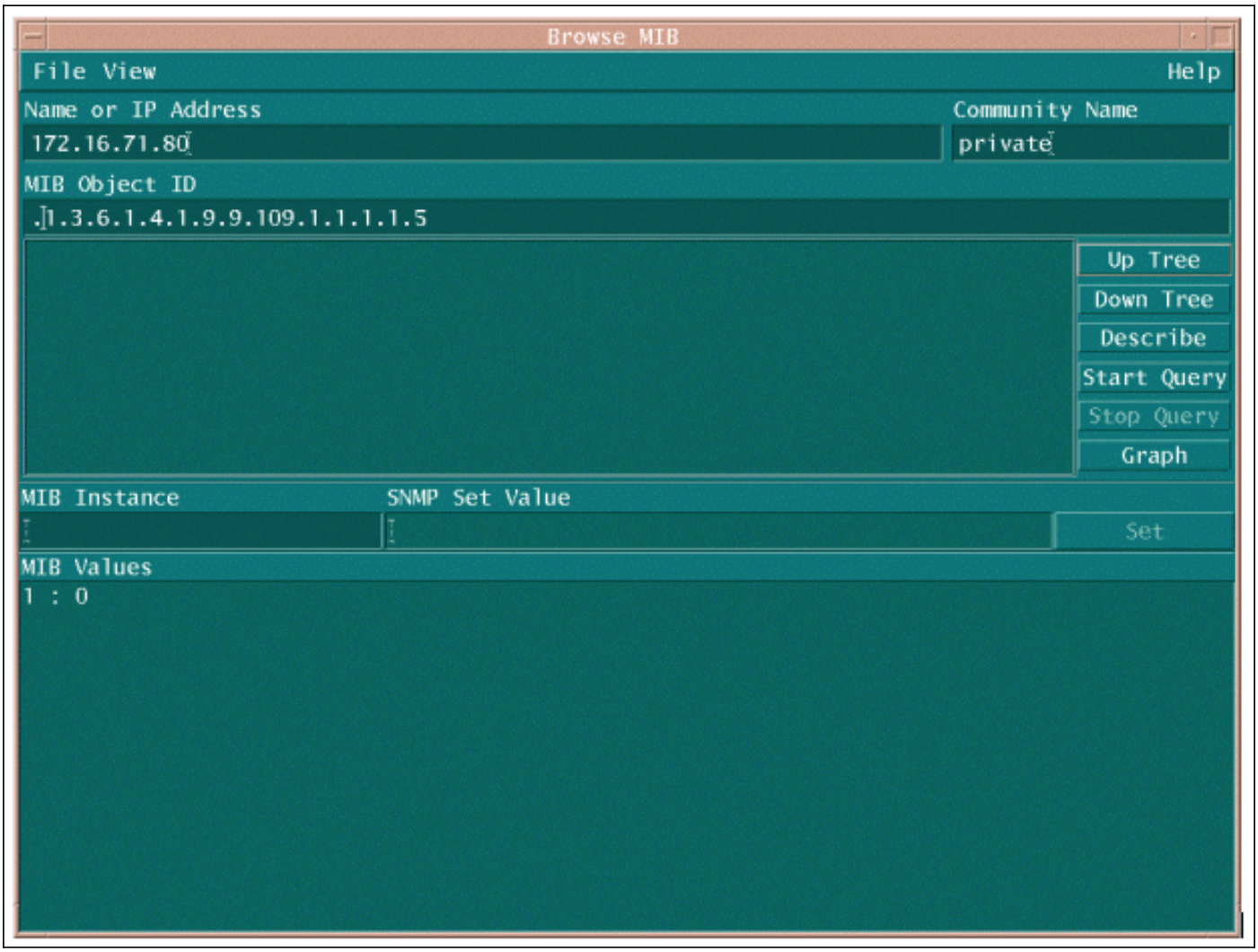
O exemplo seguinte é extraído da tabela CISCO-PROCESS-MIB.oid. Este exemplo mostra que o OID para o cpmCPUTotal5minMIB é .1.3.6.1.4.1.9.9.109.1.1.1.1.5.

Note: Não esqueça adicionar “.” ao começo do OID ou do você obterá um erro quando você tenta o votar. Talvez você precise também adicionar ".1" no final da OID para instanciá-la. Isto diz ao dispositivo o exemplo do OID que você está procurando. Em alguns casos, os OID têm mais de um exemplo de um tipo particular de dados, como quando um roteador tem CPU múltiplos.

```
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"
```

Há duas formas comum votar o MIB OID para certificar-se que é disponível e funcionar. É uma boa ideia fazer isto antes que você comece o levantamento de dados maioria de modo que você não desperdice a votação do tempo algo que não está lá e a termine acima com um base de dados vazio. Uma maneira de fazer isto é usar um MIB móvel de sua plataforma do NMS tal como o HP OpenView Network Node Manager (NNM), ou o CiscoWorks Windows, e incorpora o OID que você quer verificar.

A seguir está um exemplo do HP OpenView SNMP MIB walker.



Uma outra maneira fácil votar o MIB OID é usar o **snmpwalk do** comando unix segundo as indicações do exemplo seguinte.

```
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"
```

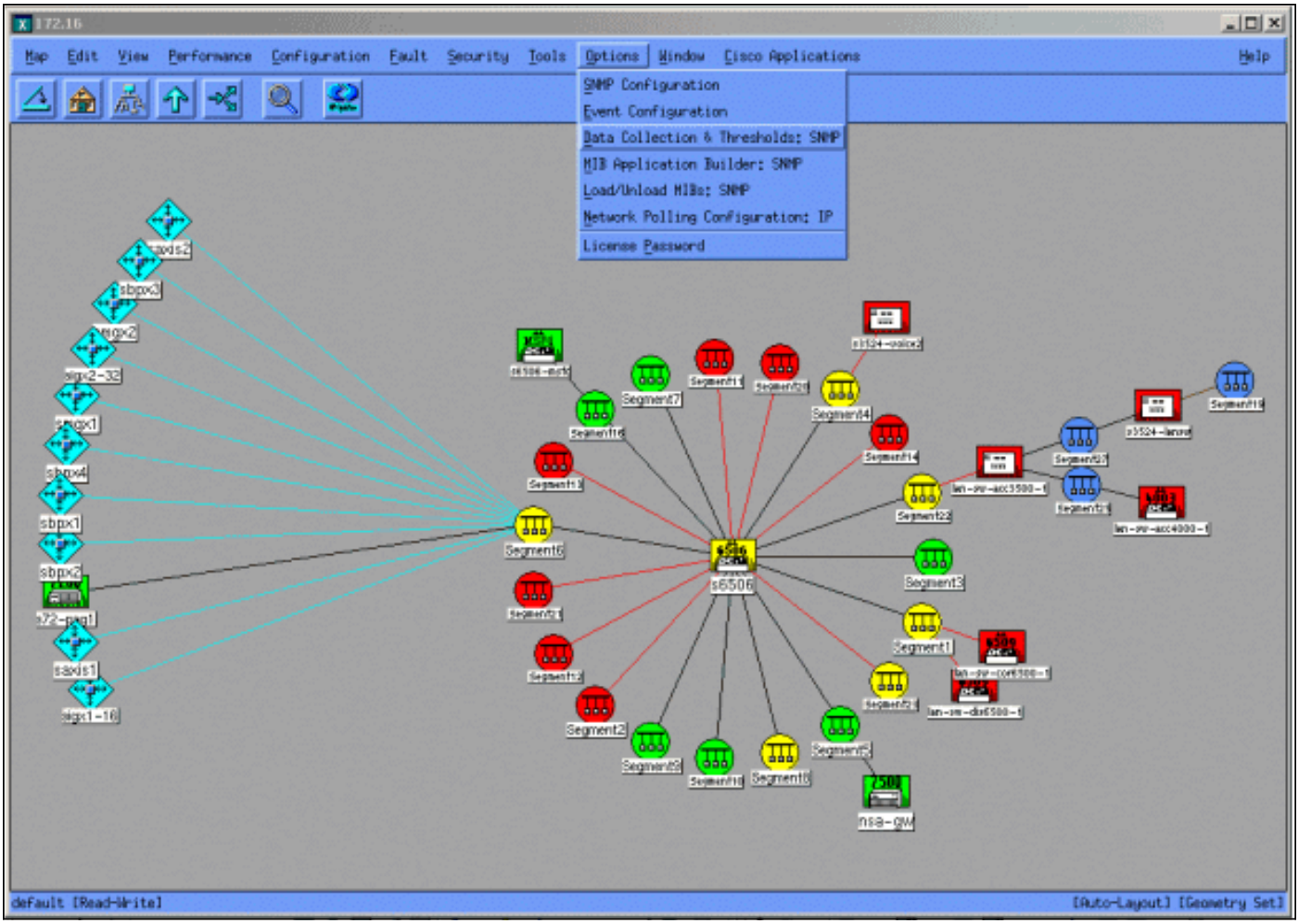
Em ambos os exemplos, o MIB retornou um valor de 0, significando que para esse ciclo de polling o CPU calculou a média de 0 porcentagens de utilização. Se você tem a dificuldade que consegue o dispositivo responder com os dados corretos, tente sibilar o dispositivo e alcançar o dispositivo pelo telnet. Se você ainda tem um problema, verifique a configuração de SNMP e as séries de comunidade snmp. Você pode precisar de encontrar uma alternativa MIB ou uma outra versão de IOS para fazer este trabalho.

Passo 3: Reúna e registre o objeto SNMP MIB específico do roteador

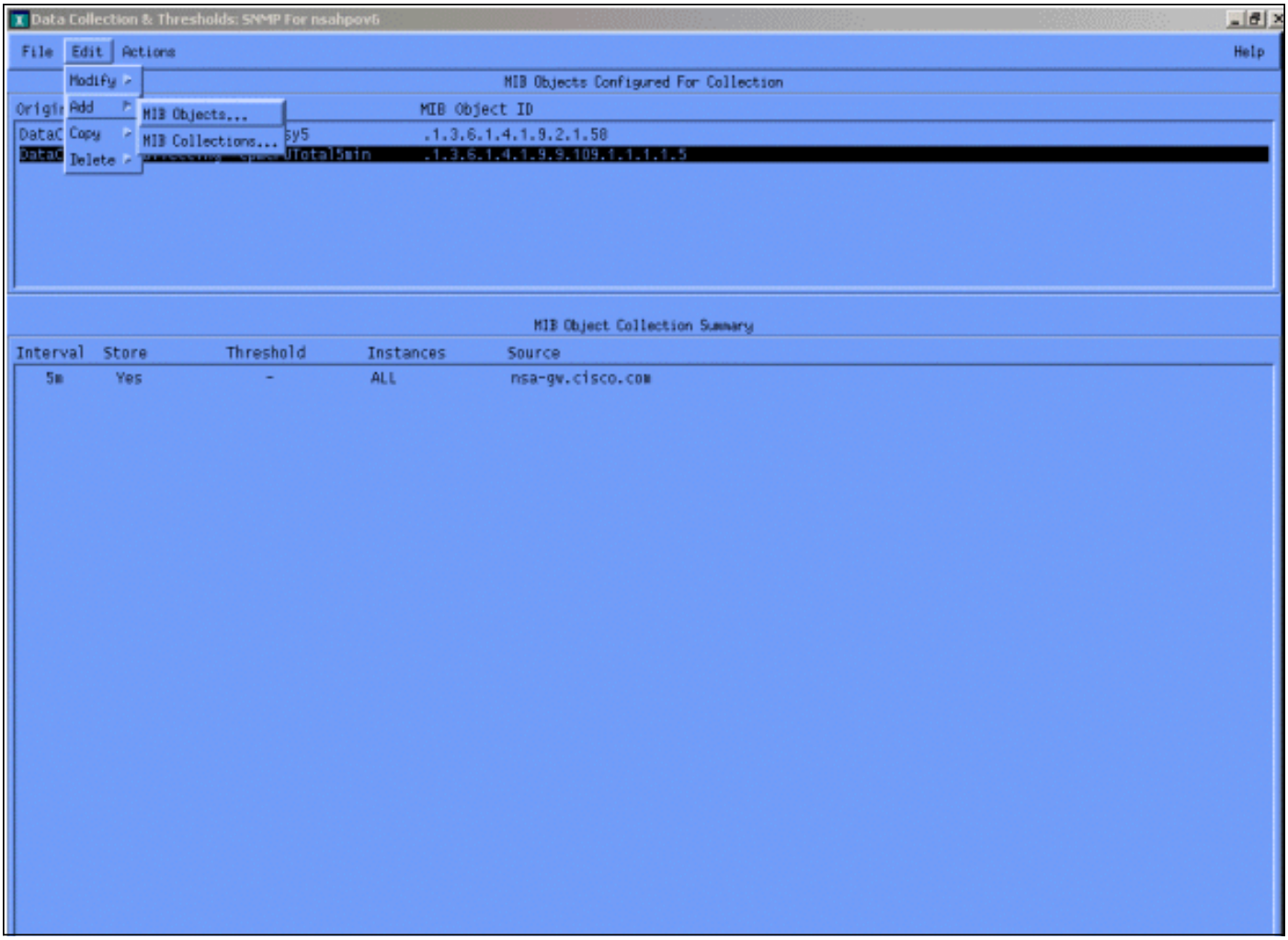
Há diversas maneiras de votar objetos MIB e gravar a saída. O Produtos, os produtos shareware, os scripts, e as ferramentas disponíveis imediatamente do vendedor estão disponíveis. Todas as ferramentas da parte frontal usam o SNMP **conseguem o** processo obter a informação. As principais diferenças estão na flexibilidade da configuração e na maneira na qual os dados são registrados em um banco de dados. Além disso, olhar no processador MIB para ver como estes vários métodos trabalham.

Agora que você sabe o OID está apoiado no roteador, você precisa de decidir frequentemente como votá-lo e como gravá-lo. Cisco recomenda que o CPU MIB esteja votado em intervalos do cinco minutos. Um intervalo mais baixo aumentaria a carga na rede ou no dispositivo, e desde que o valor MIB é uma média de cinco minutos de qualquer maneira não seria útil votá-la mais frequentemente do que o valor calculado a média. Igualmente recomenda-se geralmente que o polling de linha de base tem pelo menos um período de duas semanas de modo que você possa analisar pelo menos dois ciclos de negócios semanais na rede.

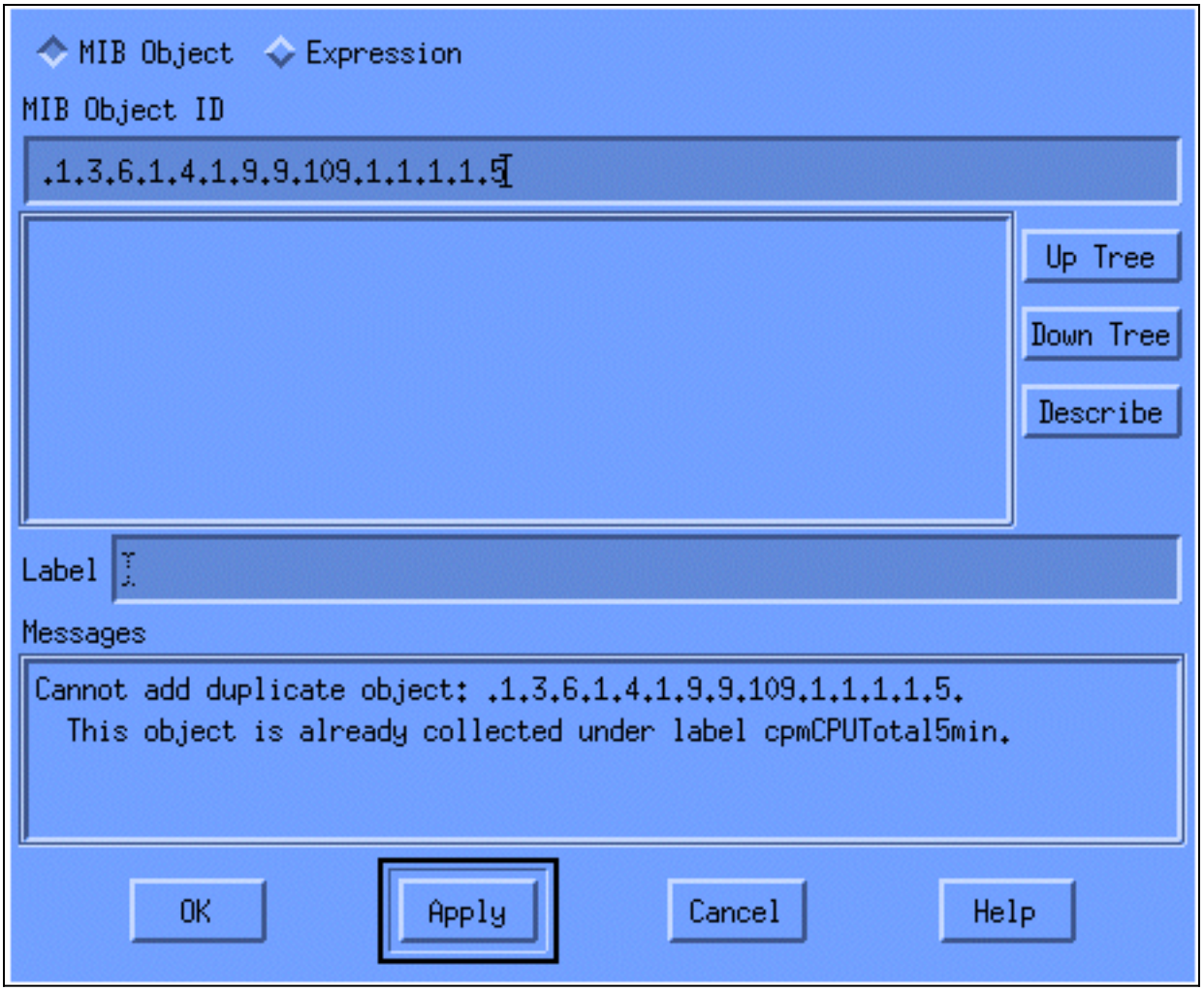
As telas a seguir mostram como adicionar objetos MIB ao HP OpenView Network Node Manager version 6.1. Da tela principal, selecione **opções > levantamento de dados & pontos iniciais**.



Selecione então o **Editar > adicionar > objetos de MIB**.

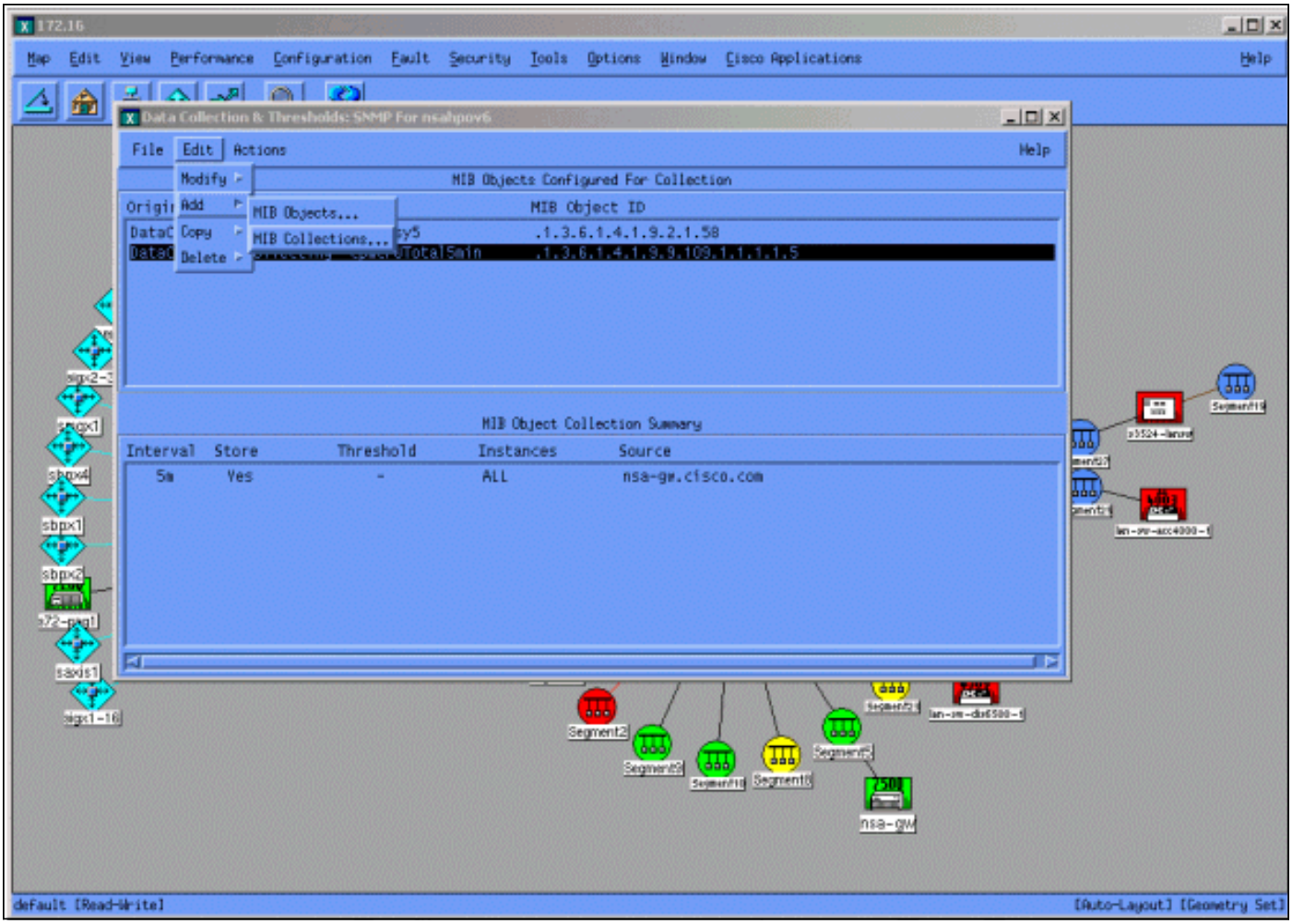


Do menu, adicionar a corda OID e o clique **aplica-se**. Agora você introduziu o objeto MIB na plataforma HP OpenView para que ele possa ser interrogado.



Em seguida, você deve informar ao HP OpenView qual roteador deve ser consultado para este OID.

Do menu do levantamento de dados, selecione **Edit > Add > coleções MIB**.

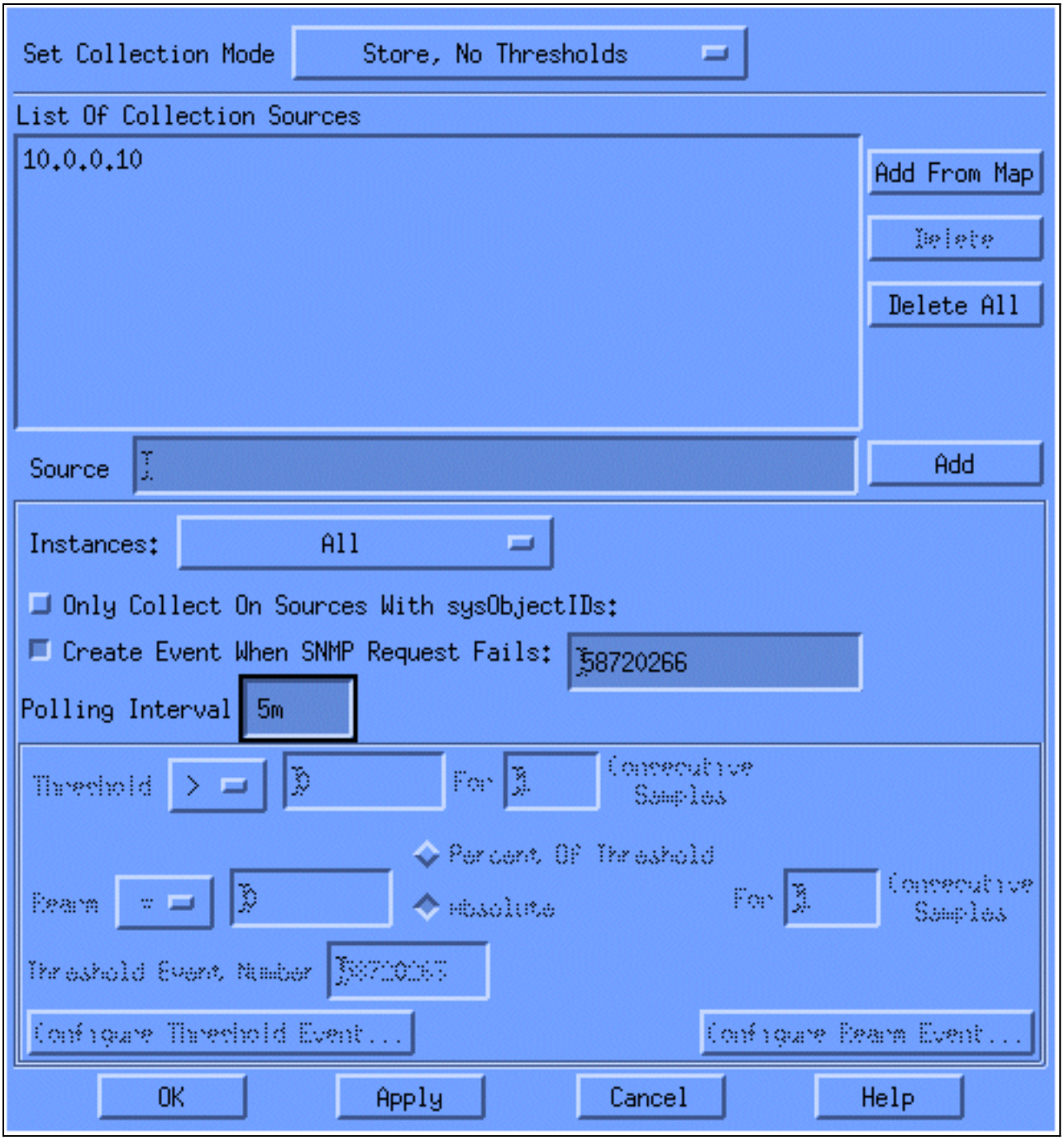


No campo de fonte, incorpore o nome do Domain Naming System (DNS) ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do roteador a ser votado.

Selecione Store (Armazenamento), No Thresholds (Sem Limites) na lista Set Collection Mode (Definir Modo de Coleta).

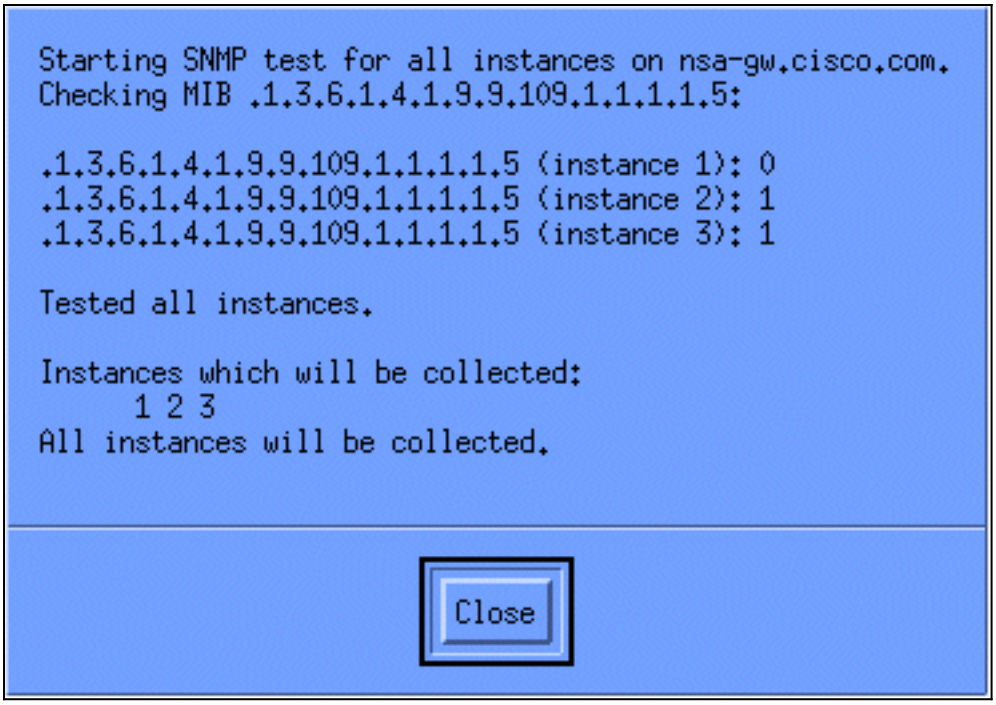
Ajuste o intervalo de polling a **5m**, para cinco intervalos minutos.

Clique em Apply.



Você deve selecionar o **arquivo > salvar** para que as mudanças tomem a influência.

Para verificar que a coleção se estabelece corretamente, destaque a linha sumária da coleção para o roteador e selecione as **ações > o teste SNMP**. Isso verifica se a série de comunidade está correta e interrogará todas as instâncias do OID.



Clique **perto**, e deixe a coleção ser executado por uma semana. No fim do período semanal, extraia os dados para a análise.

Os dados serão analisados mais facilmente se você copiá-los parcialmente para um arquivo ASCII e importá-los para uma ferramenta de planilha, como o Microsoft Excel. Para fazer isso com o HP OpenView NNM, você pode usar a ferramenta de linha de comando snmpColDump. Cada coleção configurada escreve a um arquivo no diretório de /var/opt/OV/share/databases/snmpCollect/.

Extraia os dados a um arquivo ASCII chamado **testfile** com o comando seguinte:

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

Note: cpmCPUTotal5min.1 é o arquivo da base de dados que o HP OpenView NNM criado quando o polling OID começou.

O arquivo de teste gerado é semelhante ao do exemplo a seguir.

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

Depois que a saída do arquivo de teste estiver na estação UNIX, você poderá transferi-la para o PC utilizando o FTP (Protocolo de Transferência de Arquivos).

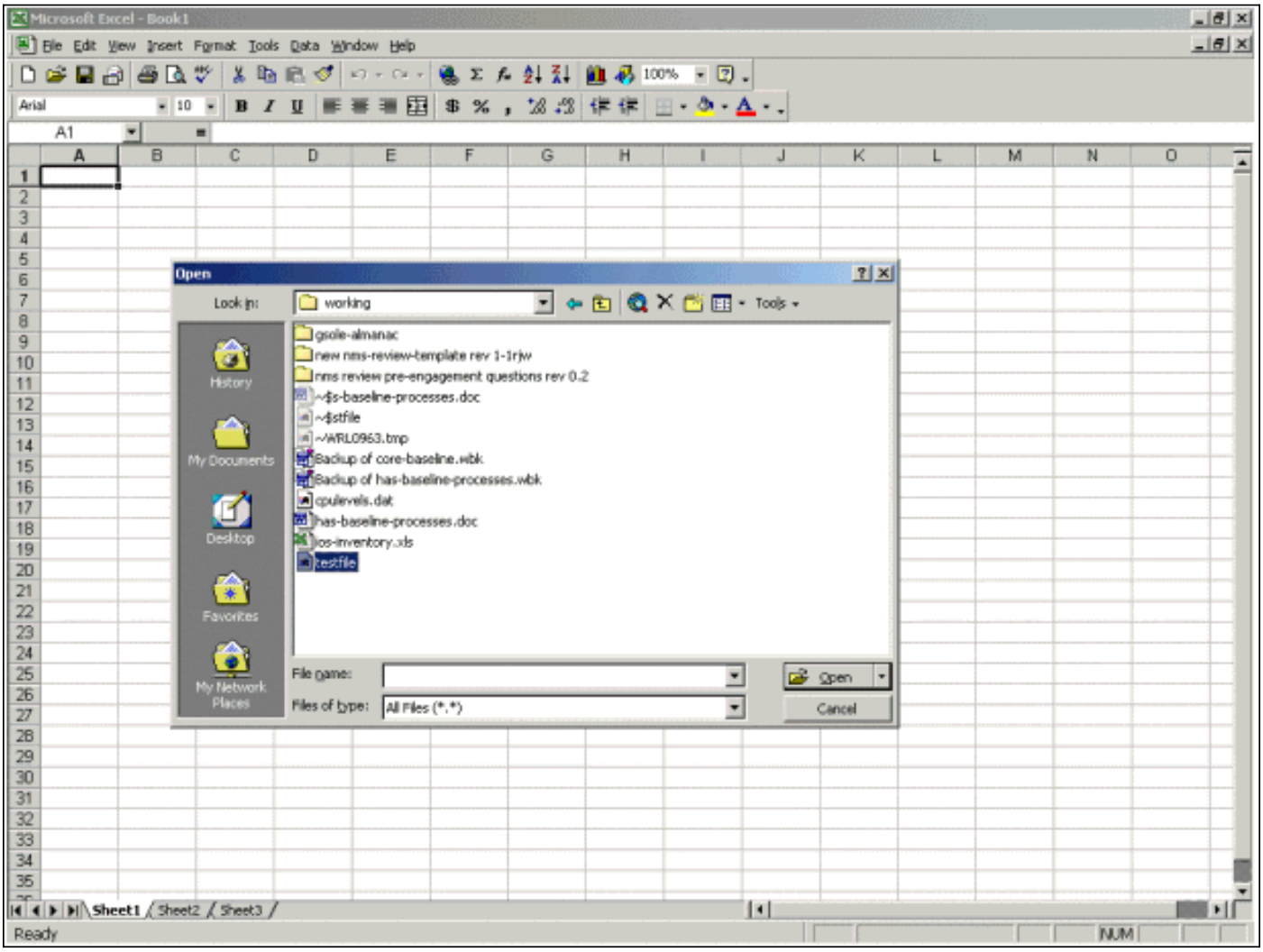
Também é possível coletar os dados usando seus próprios scripts. Para fazer isto, execute um **snmpget** para o CPU OID cada cinco minutos e despeje os resultados em um arquivo .csv.

Passo 4: Analise dados para determinar pontos iniciais

Agora que você tem alguns dados, você pode começar a analisá-la. Essa fase da linha de base determina as configurações de limiar que podem ser usadas e que são uma medida precisa do desempenho ou da falha e que não irão disparar muitos alarmes quando você ativar o

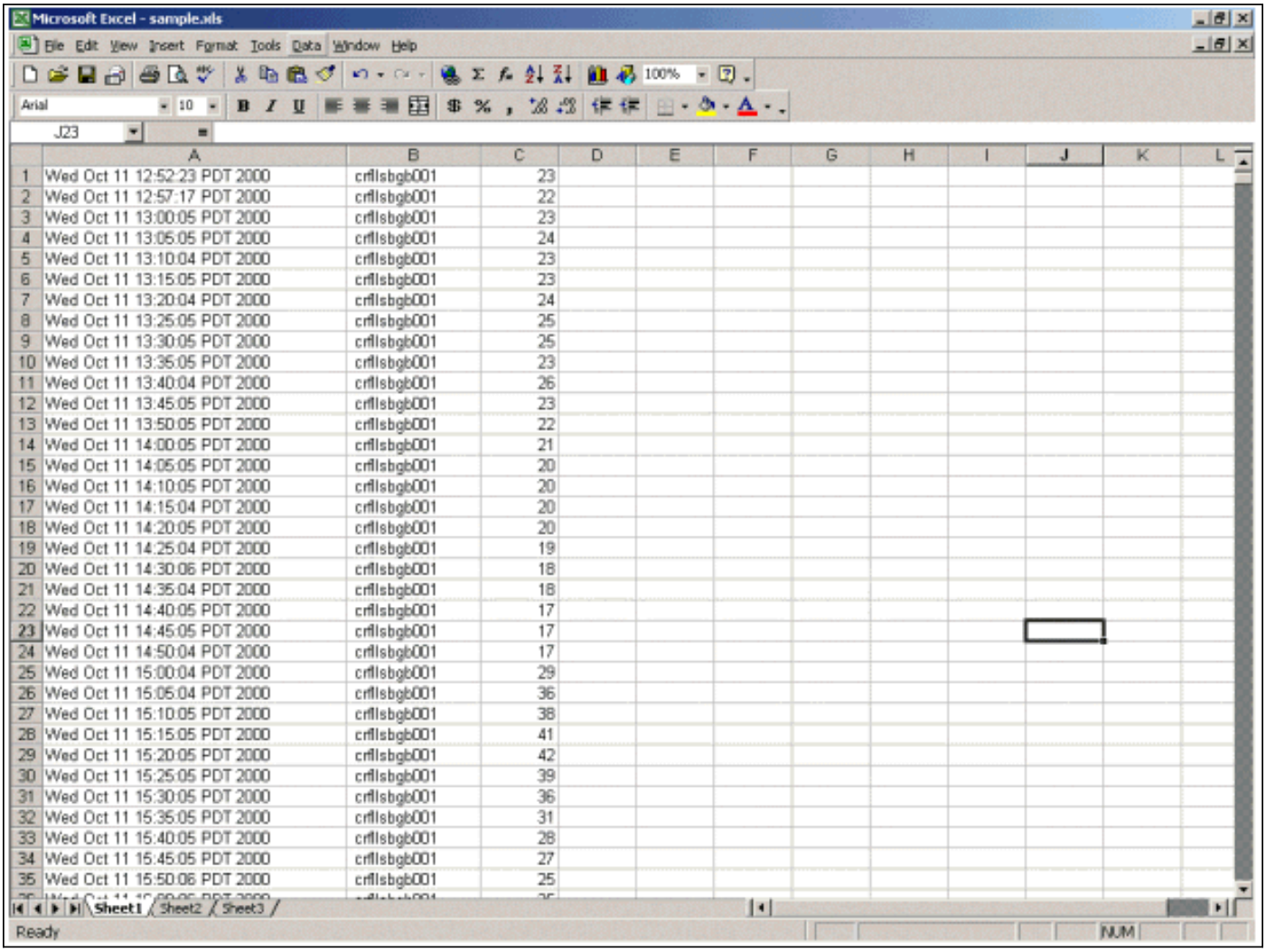
monitoramento de limiares. Uma das maneiras mais fáceis de fazer isso é importar os dados para uma planilha como as do Microsoft Excel e esboçar um gráfico disperso. Este método fá-la muito fácil de ver quantas vezes um dispositivo particular criaria um alerta da exceção se você o monitorava para um determinado ponto inicial. Não é aconselhável girar sobre pontos iniciais sem fazer uma linha de base, desde que este pode criar tempestades alertas dos dispositivos que excederam o ponto inicial que você escolheu.

Para importar o arquivo de teste em uma planilha excel, em Excel aberto e em um **File > Open** seleto e selecionar seu arquivo de dados.



O aplicativo Excel, então, orienta você durante toda a importação do arquivo.

Quando concluído, o arquivo importado deve ser semelhante à tela a seguir.

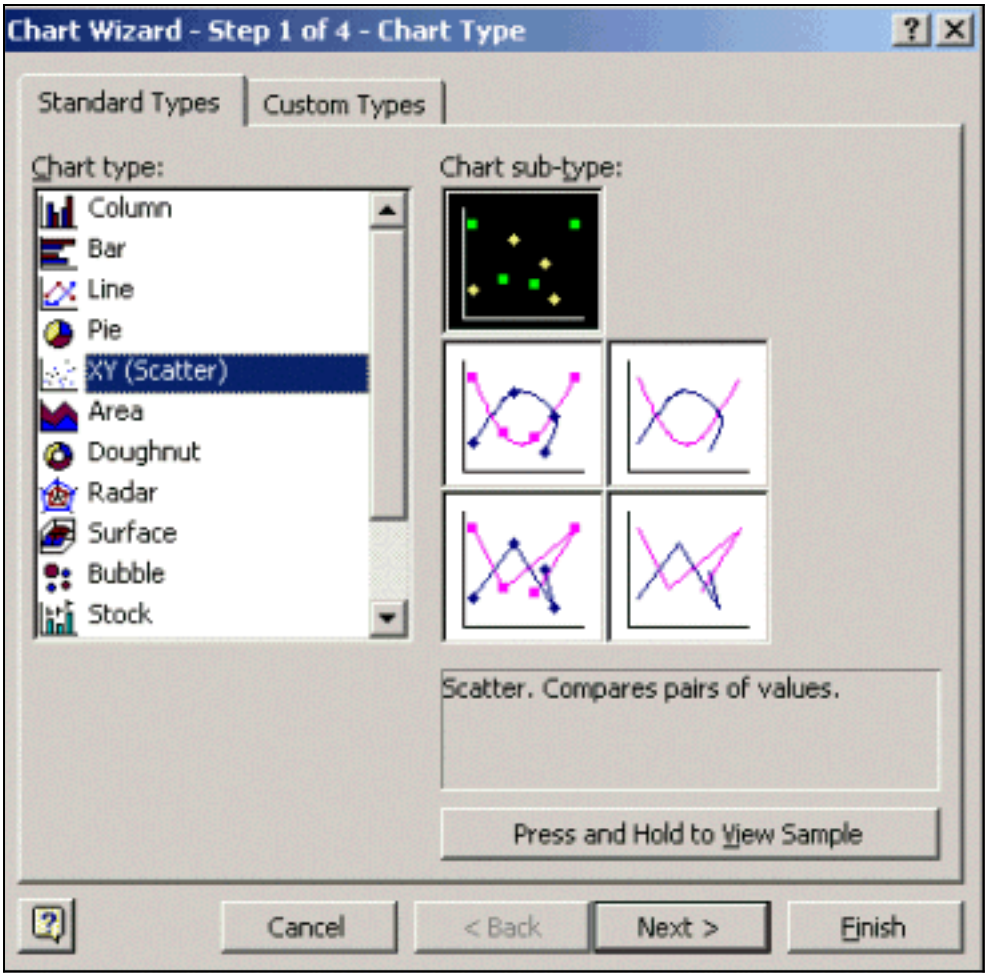


	A	B	C
1	Wed Oct 11 12:52:23 PDT 2000	cnflsbgb001	23
2	Wed Oct 11 12:57:17 PDT 2000	cnflsbgb001	22
3	Wed Oct 11 13:00:05 PDT 2000	cnflsbgb001	23
4	Wed Oct 11 13:05:05 PDT 2000	cnflsbgb001	24
5	Wed Oct 11 13:10:04 PDT 2000	cnflsbgb001	23
6	Wed Oct 11 13:15:05 PDT 2000	cnflsbgb001	23
7	Wed Oct 11 13:20:04 PDT 2000	cnflsbgb001	24
8	Wed Oct 11 13:25:05 PDT 2000	cnflsbgb001	25
9	Wed Oct 11 13:30:05 PDT 2000	cnflsbgb001	25
10	Wed Oct 11 13:35:05 PDT 2000	cnflsbgb001	23
11	Wed Oct 11 13:40:04 PDT 2000	cnflsbgb001	26
12	Wed Oct 11 13:45:05 PDT 2000	cnflsbgb001	23
13	Wed Oct 11 13:50:05 PDT 2000	cnflsbgb001	22
14	Wed Oct 11 14:00:05 PDT 2000	cnflsbgb001	21
15	Wed Oct 11 14:05:05 PDT 2000	cnflsbgb001	20
16	Wed Oct 11 14:10:05 PDT 2000	cnflsbgb001	20
17	Wed Oct 11 14:15:04 PDT 2000	cnflsbgb001	20
18	Wed Oct 11 14:20:05 PDT 2000	cnflsbgb001	20
19	Wed Oct 11 14:25:04 PDT 2000	cnflsbgb001	19
20	Wed Oct 11 14:30:06 PDT 2000	cnflsbgb001	18
21	Wed Oct 11 14:35:04 PDT 2000	cnflsbgb001	18
22	Wed Oct 11 14:40:05 PDT 2000	cnflsbgb001	17
23	Wed Oct 11 14:45:05 PDT 2000	cnflsbgb001	17
24	Wed Oct 11 14:50:04 PDT 2000	cnflsbgb001	17
25	Wed Oct 11 15:00:04 PDT 2000	cnflsbgb001	29
26	Wed Oct 11 15:05:04 PDT 2000	cnflsbgb001	36
27	Wed Oct 11 15:10:05 PDT 2000	cnflsbgb001	38
28	Wed Oct 11 15:15:05 PDT 2000	cnflsbgb001	41
29	Wed Oct 11 15:20:05 PDT 2000	cnflsbgb001	42
30	Wed Oct 11 15:25:05 PDT 2000	cnflsbgb001	39
31	Wed Oct 11 15:30:05 PDT 2000	cnflsbgb001	36
32	Wed Oct 11 15:35:05 PDT 2000	cnflsbgb001	31
33	Wed Oct 11 15:40:05 PDT 2000	cnflsbgb001	28
34	Wed Oct 11 15:45:05 PDT 2000	cnflsbgb001	27
35	Wed Oct 11 15:50:06 PDT 2000	cnflsbgb001	25

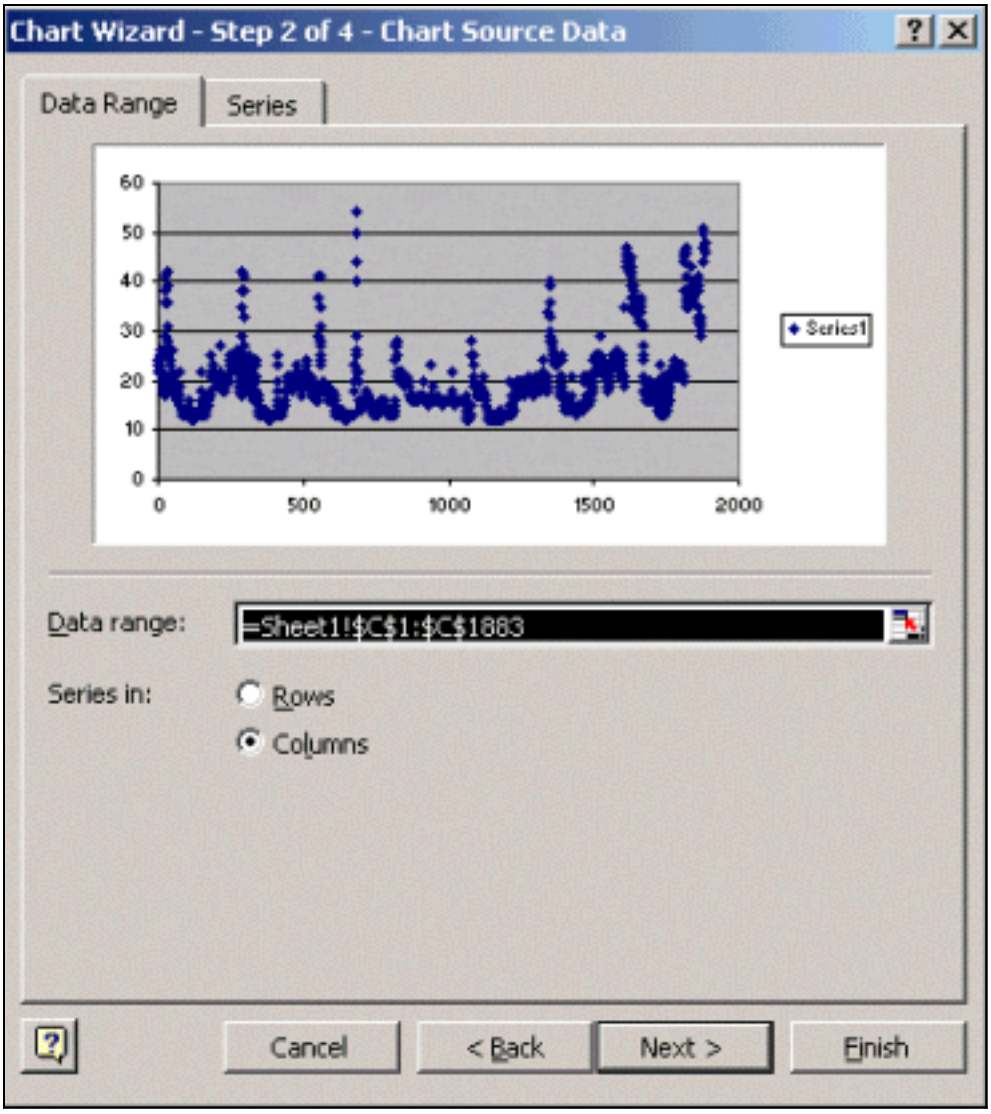
Uma carta do scatter permite-o a visualiza mais facilmente como as várias configurações de limiar trabalhariam na rede.

Para criar um gráfico de dispersão, realce a coluna C no arquivo importado e, em seguida, clique no ícone Chart Wizard. Depois, siga as etapas do Wizard de Gráfico para criar um gráfico de dispersão.

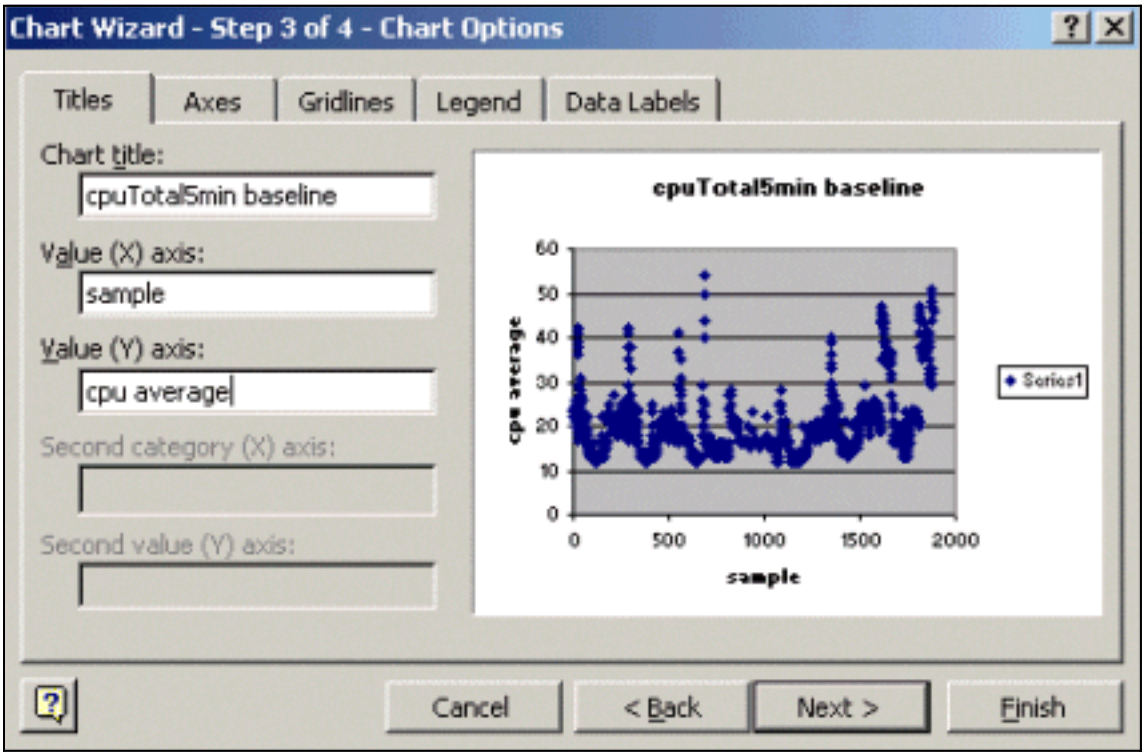
Na etapa do assistente de gráfico 1, como mostrado abaixo, selecione os **tipos padrão** aba, e selecione o tipo **XY da** carta **(do Scatter)**. Em seguida, clique em Avançar.



Na etapa do assistente de gráfico 2, como mostrado abaixo, selecione a aba do **intervalo de dados** e selecione o intervalo de dados e a **opção colunas**. Clique em Next.



Na etapa do assistente de gráfico 3, como mostrado abaixo, incorpore os valores do título da carta e da linha central X e Y, e clique-os então **em seguida**.



Na etapa do assistente de gráfico 4, selecione se você quer a carta do scatter em uma página nova ou como um objeto na página existente.

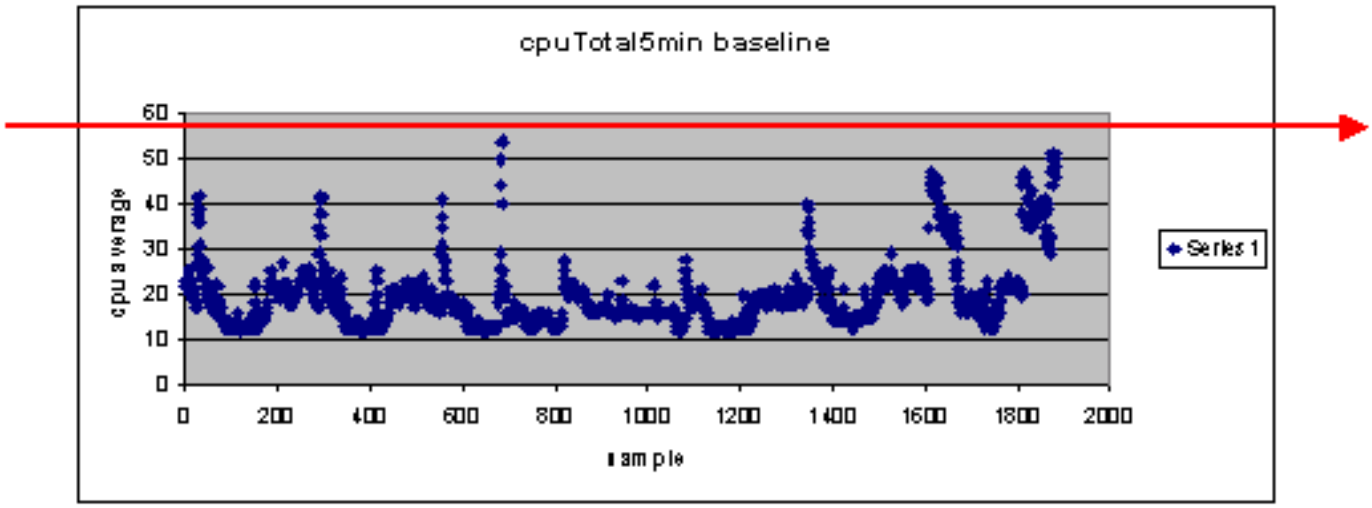
Clique o **revestimento** para colocar a carta em seu lugar desejado.

What If? Análise

Não é possível usar o gráfico de dispersão na análise. Contudo, antes de continuar, você precisa de fazer as seguintes perguntas:

- O que o fornecedor (no exemplo, o fornecedor é a Cisco) recomenda como um limiar desta variável de MIB?Geralmente, Cisco recomenda que um roteador central não excede uma utilização CPU média de 60 por cento. Sessenta por cento estiveram escolhidos porque um roteador precisa algumas despesas gerais caso que experimentam o problema ou a rede tem algumas falhas. Cisco calcula que um roteador central precisa aproximadamente 40 percentuais de CPU em cima caso que um protocolo de roteamento tem que voltar a calcular ou reconvergir. Essas porcentagens variam com base nos protocolos que você usa e na topologia e estabilidade da rede.
- O que acontece se eu usar 60 por cento como configuração de limiar?Se você desenha uma linha através da carta do scatter horizontalmente em 60, você verá que nenhuns dos pontos de dados excedem 60 percentuais de utilização de CPU. Um ponto inicial do grupo 60 em suas estações do sistema de gerenciamento de rede (NMS) não se terá ajustado assim fora de um alarme de limiar durante o período de polling. Uma porcentagem de 60 é aceitável para este roteador. Contudo, observação na carta do scatter que alguns dos pontos de dados são próximos a 60. Seria agradável saber quando um roteador está aproximando o ponto inicial de 60 por cento assim que você pode saber adiantadamente que o CPU está aproximando 60 por cento e para ter um plano para que o que faça quando alcança esse ponto.
- Que se eu ajustei o ponto inicial aos por cento dos 50 pés?Calcula-se que este roteador alcançou o porcentagem de utilização dos 50 pés quatro vezes durante este ciclo de polling e geraria um alarme de limiar cada vez. Este processo torna-se mais importante quando você olha *grupos de Roteadores* para ver o que as configurações de limiar diferentes fariam. Por exemplo, “que se eu ajustei o ponto inicial em por cento dos 50 pés para a rede central inteira?” Perceba que é muito difícil escolher somente um número.

Limiar de CPU “que se” análise



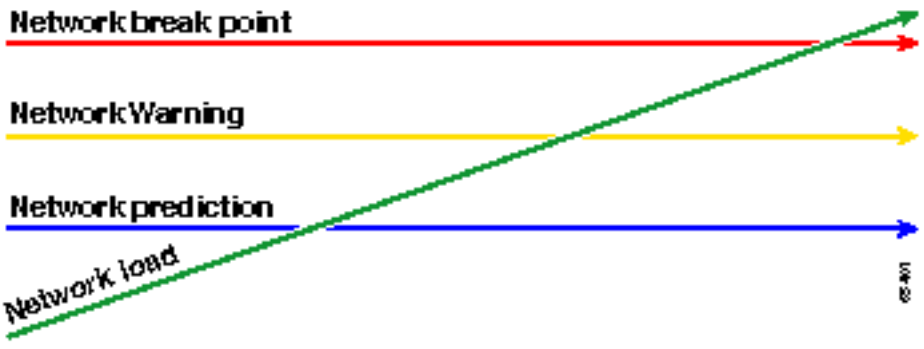
Uma estratégia que você pode se usar para fazer este mais fácil está a pronta, grupo, vai metodologia de limiar. Essa metodologia utiliza três números limiares sucessivos.

- Pronto — o ponto inicial que você se ajusta como um predictor de que dispositivos precisarão provavelmente a atenção no futuro
- Defina—o limiar que é usado como um indicador de antecipação, que o alerta quando iniciar o planejamento de um reparo, reconfiguração ou atualização
- Vá — o ponto inicial que você e/ou o vendedor acreditam são uma condição de defeito e exige alguma ação repará-la; neste exemplo é 60 por cento

A tabela a seguir mostra a estratégia de Pronto, Configurar, Continuar.

Limite	Ação	Resultado
45 por cento	Investigue mais	Lista de opções para planos de ação
por cento dos 50 pés	Formule o plano de ação	Lista de etapas no plano de ação
60%	Plano de ação do implementar	O roteador não excede mais os limiares. De volta ao modo pronto

A metodologia Ready, Set, Go muda o gráfico de linha de base original discutido anteriormente. O diagrama a seguir mostra o gráfico alterado da linha de base. Se você pode identificar os outros pontos de interseção na carta, você tem agora mais tempo para planejar e reagir do que você fez antes.



Observe que neste processo, a atenção está centrada sobre as exceções na rede e não estada

relacionada com os outros dispositivos. Supõe-se que enquanto os dispositivos estão abaixo dos pontos iniciais, são muito bem.

Se você tem estas etapas pensadas para fora desde o início, você será bem preparado para manter a rede saudável. Executar este tipo de planeamento é igualmente extremamente útil para o planejamento de orçamento. Se você conhece o que seus cinco superiores **vão o** Roteadores, seus roteadores de conjunto intermediários, e seus **roteadores prontos** inferiores são, você pode facilmente planejar em quanto orçamento você precisará para as elevações baseadas em que tipo do Roteadores são e quais suas opções do plano de ação são. A mesma estratégia pode ser usada para os links do Wide Area Network (WAN) ou o todo o outro MIB OID.

Passo 5: Problemas imediatos identificados reparo

Esta é uma das etapas mais fáceis do processo de linha de base. Depois de identificados os dispositivos que excedem o limiar de ida, crie um plano de ação para recolocar esses dispositivos sob o limiar.

Você pode abrir um caso com centro de assistência técnica (TAC) de Cisco ou contactar seu coordenador de sistemas para opções disponíveis. Você não deve supor que aquela obter a coisas o ponto inicial inferior traseiro custará lhe a dinheiro. Alguns problemas de CPU podem ser resolvidos alterando a configuração para garantir que todos os processos sejam executados da maneira mais eficiente. Por exemplo, algum Access Control Lists (ACLs) pode fazer um CPU de roteador executar muito alta devido ao trajeto os pacotes para tomar através do roteador. Em alguns casos, você pode executar o Netflow Switching para mudar o trajeto do packet switching e para reduzir o impacto do ACL no CPU. Independentemente dos problemas, é necessário retornar todos os roteadores abaixo desse limiar nessa etapa para que você consiga implementar esses limiares mais tarde sem o risco de inundar as estações NMS com muitos alarmes de limiar.

Passo 6: Testar monitoramento do limiar

Esta etapa envolve o teste de thresholds no laboratório usando as ferramentas que você utilizará na rede de produção. Há duas abordagens comuns para monitorar thresholds. Você deve decidir qual método é melhor para sua rede.

- Vote e compare o método usando uma plataforma de SNMP ou a outra ferramenta de monitoramento SNMPEste método usa mais largura de banda de rede para o tráfego de polling e pega ciclos de processamento em sua plataforma de SNMP.
- Use as configurações de alarmes e eventos de Monitorização remota (RMON) nos roteadores, de modo que eles enviem um alerta somente quando for ultrapassado um limiarEste método reduz o uso de largura de banda da rede, mas também aumenta a utilização de memória e de CPU nos roteadores.

Executando um ponto inicial usando o SNMP

Para estabelecer o método SNMP usando o HP OpenView NNM, **opções** seletas **> levantamento de dados & pontos iniciais** como você fez quando você estabelecer o polling inicial. Dessa vez, selecione no menu de coleções Store, Check Thresholds rather than Store, No Thresholds no menu de coleções. Depois que você estabelece o ponto inicial, você pode aumentar a utilização CPU no roteador enviando lhe sibilos múltiplos e/ou o SNMP múltiplo anda. Pode ser necessário reduzir o valor de limiar se não for possível forçar a CPU a um valor alto o suficiente para ultrapassar o limiar. Em todo caso, você deve assegurar-se de que o threshold mechanism esteja

trabalhando.

Uma das limitações da utilização desse método é que você não pode implementar simultaneamente múltiplos limiares. São necessárias três plataformas SNMP para configurar três limiares simultâneos diferentes. As ferramentas tais como acordos para sanidade da rede e trinagy trend permitem limiares múltipla para o mesmo exemplo OID.

Se seu sistema pode somente segurar um ponto inicial de cada vez, você pode considerar o pronto, grupo, vai estratégia na forma de série. Ou seja, quando o limite de prontidão for atingido continuamente, inicie a sua investigação e aumente o limite para o nível definido desse dispositivo. Quando o nível definido é alcançado continuamente, comece a formular seu plano de ação e aumente o limite do nível de atividade para aquele dispositivo. Em seguida, quando o limiar de partida for alcançado continuamente, implemente seu plano de ação. Isso deve funcionar tão bem quanto os três métodos de limiar simultâneos. Apenas toma um pouco de mais tempo que muda as configurações de limiar da plataforma de SNMP.

Executando um ponto inicial usando o alarme de RMON e o evento

Usando o alarme RMON e as configurações de eventos, você pode fazer com que o roteador se monitore para vários limiares. Quando o roteador detecta uma condição acima do limiar, ele envia uma armadilha de SNMP à plataforma SNMP. É necessário ter um receptor de desvio de SNMP configurado em sua configuração do roteador para a armadilha ser encaminhada. Há uma correlação entre um alarme e um evento. O alarme verifica o OID para ver se há o ponto inicial dado. Se o ponto inicial é alcançado, o processo do alarme ateia fogo ao processo do evento que pode qualquer um enviar um mensagem de armadilha de SNMP, cria uma entrada de registro RMON, ou ambos. Para mais detalhe neste comando, veja o alarme de RMON e os comandos de configuração de evento.

Os comandos de configuração de roteador a seguir fazem com que o roteador monitore o cpmCPUTotal5min a cada 300 segundos. Ateará fogo ao evento 1 se o CPU excede 60 por cento e ateará fogo ao evento 2 quando o CPU cai de volta a 40 por cento. Em ambos os casos, um mensagem de armadilha de SNMP será enviado à estação NMS com a corda privada da comunidade.

Para utilizar método Ready, Set, Go, utilize todas as seguintes instruções de configuração:

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

O seguinte exemplo mostra a saída do comando show rmon alarm que foi configurada pelas seguintes declarações.

```
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
```

O exemplo a seguir mostra a saída do 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
```

Você pode experimentar os dois métodos para ver qual é o método que melhor se adapta ao seu ambiente. Você pode até descobrir que uma combinação de métodos funciona adequadamente. Em todo caso, testar deve ser feito em um ambiente de laboratório para assegurar-se de que tudo trabalhe corretamente. Após o teste no laboratório, uma distribuição limitada em um grupo pequeno de Roteadores permitirá que você teste o processo de enviar alertas a seu centro de operações.

Neste caso, você terá que abaixar os pontos iniciais para testar o processo: Tentar aumentar artificialmente o CPU em um roteador de produção não é recomendada. Você também deve garantir que, quando os alertas forem enviados às estações NMS no Centro de Operações, haverá uma política de escalação para garantir que você será informado quando os dispositivos excederem os limiares. Essas configurações foram testadas em laboratório com um Cisco IOS Versão 12.1(7). Se você encontra quaisquer edições, você deve verificar com os coordenadores do planejamento ou de sistemas de Cisco para ver se você tem um erro em sua Versão do IOS.

Passo 7: Monitoramento de limiar do implementar que usa o SNMP ou o RMON

Após ter testado totalmente o monitoramento de limiar no laboratório e em uma versão limitada, você estará pronto para implementar limiares em toda a rede principal. Agora você pode seguir esse processo de linha de base sistematicamente para obter outras variáveis MIB importantes na rede, como os buffers, a memória livre, os erros de verificação de redundância cíclica (CRC), a perda de células AMT e outras.

Se você usa o alarme de RMON e as configurações de evento, você pode agora parar de votar de sua estação NMS. Isso reduzirá a carga no servidor NMS e diminuirá a quantidade de dados de chamadas seletivas na rede. Sistematicamente atravessando este processo para indicadores de saúde da rede importante, você poderia facilmente vir ao ponto que o equipamento de rede se está monitorando que usam o alarme de RMON e o evento.

MIBs adicionais

Depois que você aprendeu este processo, você pode querer investigar o outro MIBs à linha de base e ao monitor. As subseções a seguir apresentam uma lista resumida de alguns OIDs e descrições úteis.

MIBs do roteador

As Características de memória são muito úteis em determinar a saúde de um roteador. Um roteador saudável deve quase sempre ter o espaço de buffer disponível com que para trabalhar. Se o roteador começa a ser executado fora do espaço de buffer, o CPU terá que trabalhar mais duramente para criar bufferes novos e para tentá-los encontrar bufferes para entrante e pacotes de saída. Uma discussão aprofundada dos bufferes é além do alcance deste documento. Contudo, em regra geral, um roteador saudável deve ter muito poucos, eventualmente, faltas do buffer e não deve ter nenhumas falhas de buffer, ou uma condição de memória livre zero.

Objeto	Descrição	OID
ciscoMemoryPool Free	O número de bytes do pool de memória atualmente não utilizados no dispositivo gerenciado.	1.3.6.1.4.1.9.9. 48.1.1.1.6
ciscoMemoryPool LargestFree	O número o maior de bytes contíguos do conjunto de memória que é Currently Unused	1.3.6.1.4.1.9.9. 48.1.1.1.7
bufferElMiss	O número de elementos de buffer está ausente	1.3.6.1.4.1.9.2. 1.12
bufferFail	O número de falhas de alocação de buffer	1.3.6.1.4.1.9.2. 1.46
bufferNoMem	O número de buffers gera falhas devido à ausência de memória livre	1.3.6.1.4.1.9.2. 1.47

MIBs de Switch Catalyst

Objeto	Descrição	OID
cpmCPUTotal5min	Percentual cpu busy total no último período de cinco minutos. Esse objeto deprecia o objeto avgBusy5 de OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5
cpmCPUTotal5sec	Percentual cpu busy total no último período de cinco segundos. Este objeto substitui o objeto busyPer do OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.3
sysTraffic	A porcentagem de utilização da largura de banda do intervalo de eleição anterior	1.3.6.1.4.1.9.5.1.1.8
sysTrafficPeak	Valor do medidor de tráfego de pico desde a última vez que os contadores da porta foram limpos ou o sistema foi iniciado.	1.3.6.1.4.1.9.5.1.1.19
sysTrafficPeaktime	O tempo (em centésimos de segundo) desde que ocorreu o valor do medidor do tráfego de pico	1.3.6.1.4.1.9.5.1.1.20
portTopNUtilization	Utilização da porta no sistema	1.3.6.1.4.1.9.5.1.20.2.1.4
portTopNBufferOverFlow	O número de excessos de buffer da porta no sistema	1.3.6.1.4.1.9.5.1.20.2.1.10

MIBs de enlace serial

Objeto	Descrição	OID
locIfInputQueueDrops	O número de pacotes descartados porque a fila de entrada estava cheia	1.3.6.1.4.1.9.2.2.1.1.26
locIfOutputQueueDrops	O número de pacotes descartados porque a fila de saída estava cheia	1.3.6.1.4.1.9.2.2.1.1.27
locIfInCRC	O número de pacotes de entrada com erros de checksum de redundância cíclica.	1.3.6.1.4.1.9.2.2.1.1.12

Comandos de configuração de alarme e evento RMON

Alarmes

Os alarmes RMON podem ser configurados com a sintaxe a seguir:

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

Elemento	Descrição
número	O número do alarme, que é idêntico ao alarmIndex na alarmTable no RMON MIB.
variável	O objeto MIB a ser monitorado, que se converte no alarmVariable usado na alarmTable do RMON MIB.
intervalo	A hora, em segundos, que o alarme monitora a variável MIB, que é idêntica a alarmInterval usado em alarmTable de RMON MIB.
delta	Testa a mudança entre variáveis MIB, que afeta o alarmSampleType no alarmTable do MIB RMON.
absoluto	Testa cada variável do MIB diretamente, o que afeta alarmSampleType na alarmTable do RMON MIB.
elevação de valor limiar	O valor em que o alarme é provocado.
número do evento	(Opcional) o número de evento a provocar quando a aumentação ou o limiar de queda excederem seu limite. Este valor é idêntico ao alarmRisingEventIndex ou ao alarmFallingEventIndex na alarmTable do MIB de RMON.
valor de falling-threshold	O valor no qual um alarme é redefinido.
série de proprietário	(Opcional) Especifica um proprietário para o alarme, que é idêntico ao alarmOwner na alarmTable do RMON MIB.

Events

Os eventos RMON podem ser configurados com a seguinte sintaxe:

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

Elemento	Descrição
número	Número de evento atribuído, que é idêntico ao eventIndex no eventTable no MIB RMON.
log	(Opcional) Gera uma entrada de registro RMON quando o evento é disparado e configura a IETF (Internet Engineering Task Force) no MIB de RMON para fazer registrar ou registrar e desviar.
comunidade trap	(Opcional) série de comunidade SNMP usada para esta armadilha. Configura o ajuste do eventType no MIB RMON para esta fileira como SNMP-armadilha ou log-e-armadilha. Este valor é idêntico ao eventCommunityValue no eventTable no MIB RMON.
description string	(Opcional) Especifica uma descrição do evento, que é idêntica à descrição na Tabela de Evento do RMON MIB.
série de proprietário	(Opcional) Proprietário desse evento, que é idêntico ao eventOwner na eventTable do MIB de RMON.

Implementação de evento e alarme de RMON

Para informações detalhadas sobre da implementação de Alarme e de Evento de RMON, leia por favor a seção de implementação de alarme e de evento de RMON do White Paper dos *melhores prática dos sistemas de gerenciamento de rede*.

Informações Relacionadas

- Suporte técnico e documentação - Cisco Systems