Whitepaper over beste praktijken in het basisproces

Inhoud

Inleiding

In dit document worden basisconcepten en -procedures beschreven voor zeer beschikbare netwerken. Het omvat kritieke succesfactoren voor netwerk baselining en dorsvorming helpen succes evalueren. Het biedt ook belangrijke details voor basis- en drempelwaardeprocessen en -implementatie die voldoen aan de richtlijnen voor beste praktijken die zijn vastgesteld door het HA-team (High Availability Services) van Cisco.

Dit document neemt u stap voor stap door het proces van baselining. Sommige huidige Network Management System (NMS) producten kunnen dit proces helpen automatiseren, maar het basisproces blijft hetzelfde of u nu geautomatiseerde of handmatige tools gebruikt. Als u deze NMS-producten gebruikt, moet u de standaardinstellingen voor de drempelwaarden voor uw unieke netwerkomgeving aanpassen. Het is belangrijk om een proces te hebben om deze drempels op een intelligente manier te kiezen, zodat ze zinvol en correct zijn.

Uitgangswaarde

Wat is een Baseline?

Een basislijn is een proces om het netwerk met regelmatige intervallen te bestuderen om ervoor te zorgen

dat het netwerk zoals ontworpen werkt. Het is meer dan een enkel verslag waarin de gezondheid van het netwerk op een bepaald moment wordt beschreven. Door het basislijnproces te volgen, kunt u de volgende informatie verkrijgen:

- Verkrijg waardevolle informatie over de status van de hardware en software
- Bepaal het huidige gebruik van netwerkresources
- Nauwkeurige beslissingen nemen over netwerkalarmdrempels
- Huidige netwerkproblemen identificeren
- Problemen in de toekomst voorspellen

Een andere manier om naar de basislijn te kijken, wordt geïllustreerd in het volgende diagram.

De rode lijn, het netwerk breekpunt, is het punt waarop het netwerk zal breken, dat wordt bepaald door de kennis van hoe de hardware en de software presteren. De groene lijn, de netwerkbelasting, is de natuurlijke progressie van de belasting op het netwerk als nieuwe toepassingen worden toegevoegd, en andere dergelijke factoren.

Het doel van een basislijn is te bepalen:

- Waar uw netwerk zich op de groene lijn bevindt
- Hoe snel de netwerkbelasting toeneemt
- Hopelijk voorspelt u op welk tijdstip de twee elkaar zullen kruisen

Door regelmatig een basislijn uit te voeren, kunt u de huidige staat te weten komen *en* extrapoleren wanneer de mislukkingen zich zullen voordoen en zich op hen vooraf voorbereiden. Dit helpt u ook om beter gefundeerde beslissingen te nemen over wanneer, waar en hoe u begrotingsgeld kunt besteden aan netwerkupgrades.

Waarom een Baseline?

Een basislijnproces helpt u om kritieke problemen met de beperking van bronnen in het netwerk te identificeren en op de juiste manier te plannen. Deze problemen kunnen worden beschreven als besturingsplane bronnen of dataplane bronnen. De besturingsplane is uniek voor het specifieke platform en de modules binnen het apparaat en kan worden beïnvloed door een aantal problemen, waaronder:

- Gegevensgebruik
- Functies ingeschakeld
- Netwerkontwerp

De besturingsplane omvat parameters zoals:

- CPU-gebruik

- Geheugengebruik
- Buffergebruik

De middelen van het gegevensplatform worden slechts beïnvloed door het type en de hoeveelheid verkeer en omvatten verbindingsgebruik en backplane gebruik. Door het gebruik van bronnen in kritieke gebieden te baseren, kunt u ernstige prestatieproblemen voorkomen of, erger nog, een netwerkmeltdown.

Met de introductie van latency-gevoelige toepassingen zoals spraak en video, is baselining nu belangrijker dan ooit. De traditionele toepassingen van Transmission Control Protocol/Internet Protocol (TCP/IP) zijn vergevingsgezind en staan voor een bepaalde hoeveelheid vertraging toe. Spraak en video zijn gebaseerd op User Datagram Protocol (UDP) en bieden geen mogelijkheden voor hertransmissies of netwerkcongestie.

Dankzij de nieuwe mix van toepassingen, helpt baselining u om zowel de besturingsplane als de dataplane te begrijpen en proactief te plannen voor veranderingen en upgrades om blijvend succes te verzekeren.

Datanetwerken bestaan al vele jaren. Tot voor kort is het redelijk vergevingsgezind om de netwerken in bedrijf te houden, met enige ruimte voor fouten. Door de toenemende acceptatie van latentiegevoelige toepassingen zoals Voice over IP (VoIP) wordt het steeds moeilijker om het netwerk te gebruiken en is meer precisie vereist. Om nauwkeuriger te zijn en een netwerkbeheerder een stevige basis te geven waarop om het netwerk te beheren, is het belangrijk om één of ander idee van hoe het netwerk loopt te hebben. Om dit te doen, moet je een proces doorlopen dat een basislijn wordt genoemd.

Basisdoelstelling

Het doel van een basislijn is:

1. De huidige status van netwerkapparaten bepalen
2. Vergelijk die status met standaard prestatierichtlijnen
3. Drempelwaarden instellen om u te waarschuwen wanneer de status deze richtlijnen overschrijdt

Vanwege de grote hoeveelheid gegevens en de hoeveelheid tijd die nodig is om de gegevens te analyseren, moet u eerst het bereik van een basislijn beperken om het proces te vergemakkelijken. De meest logische, en soms de meest voordelige, plek om te beginnen is met de kern van het netwerk. Dit deel van het netwerk is gewoonlijk het kleinste en vereist de meeste stabiliteit.

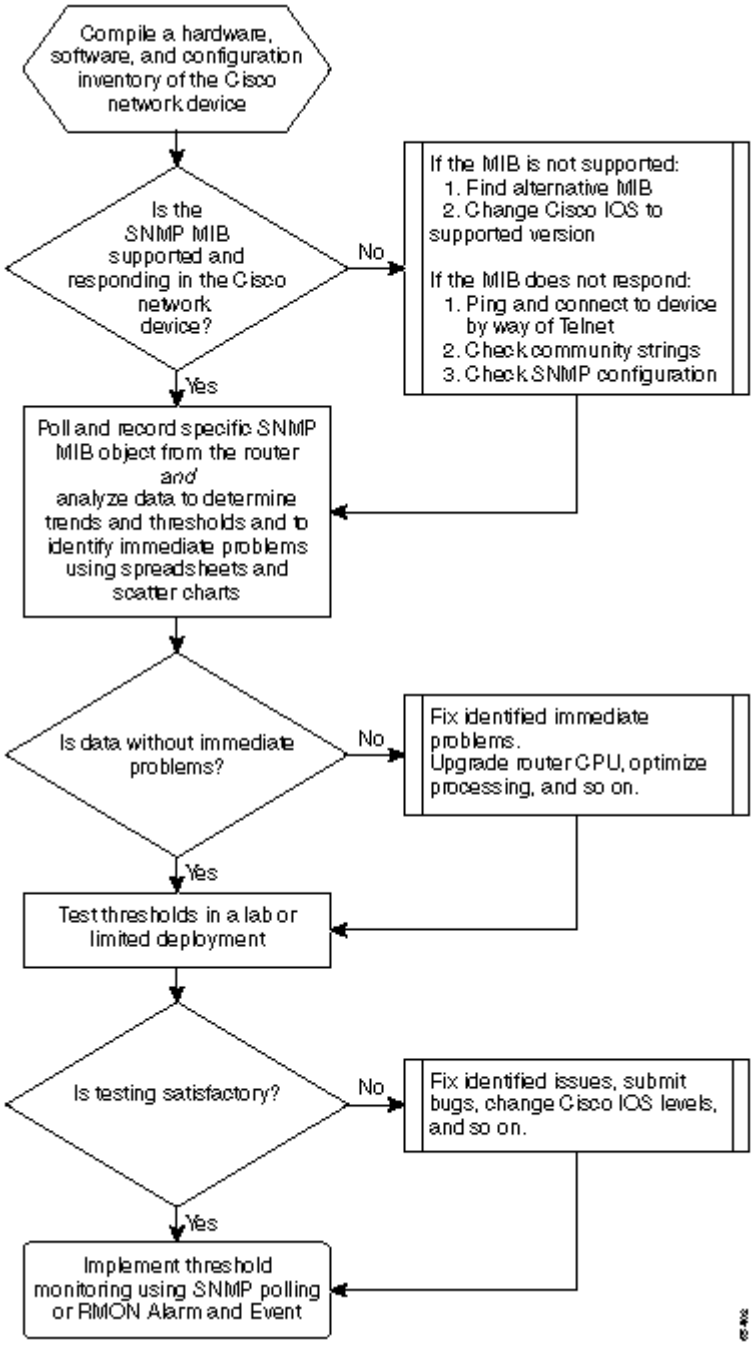
Voor de eenvoud wordt in dit document uitgelegd hoe u een zeer belangrijke Simple Network Management Protocol Management Information Base (SNMP MIB) kunt baseren: cpmCPUTotal5min. cpmCPUTotal5min is het 5-minuten-rotatiesnelheidsgemiddelde van de centrale verwerkingseenheid (CPU) van een Cisco-router en is een prestatie-indicator voor het besturingsplane. De basislijn wordt uitgevoerd op een Cisco 7000 Series router.

Zodra u het proces hebt geleerd, kunt u het op om het even welke gegevens toepassen beschikbaar in het enorme gegevensbestand van SNMP dat in de meeste apparaten van Cisco, zoals beschikbaar is:

- Gebruik van digitaal netwerk voor geïntegreerde services (ISDN)
- Celverlies in Asynchronous Transfer Mode (ATM)
- Gratis systeemgeheugen

Core Baseline-stroomschema

Het volgende stroomschema toont de basisstappen van het basislijnproces van de kern. Hoewel er producten en tools beschikbaar zijn om enkele van deze stappen voor u uit te voeren, hebben ze vaak hiaten in flexibiliteit of gebruiksgemak. Zelfs als u van plan bent om de hulpmiddelen van het netwerkbeheersysteem (NMS) te gebruiken om baselining uit te voeren, is dit nog een goede oefening in het bestuderen van het proces en het begrijpen van hoe uw netwerk werkelijk werkt. Dit proces kan ook een deel van het mysterie wegnemen uit hoe sommige NMS-tools werken omdat de meeste tools in wezen dezelfde dingen doen.



Uitgangsprocedure

Stap 1: Een inventaris van hardware, software en configuratie samenstellen

Het is van groot belang dat u een inventaris opmaakt van de hardware, software en configuratie, en wel om verschillende redenen. Eerst en vooral zijn Cisco SNMP MIB's in bepaalde gevallen specifiek voor de Cisco IOS-release die u uitvoert. Sommige MIB-objecten worden vervangen door nieuwe of worden soms volledig geëlimineerd. De hardware-inventaris is het belangrijkste nadat de gegevens zijn verzameld, aangezien de

drempels die u na de eerste basislijn moet instellen vaak zijn gebaseerd op het type CPU, de hoeveelheid geheugen, enzovoort, op de Cisco-apparaten. De configuratie inventaris is ook belangrijk om ervoor te zorgen dat u de huidige configuraties kent: U kunt apparatenconfiguraties na uw basislijn willen veranderen om buffers te stemmen, etc.

De meest efficiënte manier om dit deel van de basislijn voor een Cisco-netwerk uit te voeren, is met CiscoWorks 2000 Resource Manager Essentials (Essentials). Als deze software correct in het netwerk is geïnstalleerd, moet Essentials de huidige inventarissen van alle apparaten in zijn database hebben. Je hoeft alleen maar naar de inventarissen te kijken om te zien of er problemen zijn.

De volgende tabel is een voorbeeld van een rapport voor de software-inventaris van Cisco Router Class dat is geëxporteerd van Essentials en vervolgens wordt bewerkt in Microsoft Excel. Vanuit deze inventaris, merk op dat u SNMP MIB-gegevens en Object Identifiers (OIDâ€™s) moet gebruiken die te vinden zijn in de 12.0x en 12.1x Cisco IOS-releases.

Device Name (Apparaatnaam)	Routertype	Versie	Softwareversie
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	0 x 00	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	0 x 00	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)

Als Essentials niet in het netwerk is geïnstalleerd, kunt u de UNIX opdrachtregel tool **snmpwalk** gebruiken van een UNIX werkstation om de IOS versie te vinden. Dit wordt in het volgende voorbeeld getoond. Als u niet zeker weet hoe deze opdracht werkt, typt u **man snmpwalk** bij de UNIX prompt voor meer informatie. De IOS-versie is belangrijk wanneer u begint met het kiezen van welke MIB OIDâ€™s naar de basislijn, omdat de MIB-objecten IOS-afhankelijk zijn. Merk ook op dat door het routertype te kennen, u later bepalingen kunt maken over wat de drempels voor cpu, buffers zouden moeten zijn, etc.

```
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
```

Stap 2: Controleer dat SNMP MIB wordt ondersteund in de router

Nu u een inventaris van het apparaat hebt wilt u voor uw basislijn opiniepeilen, kunt u beginnen de specifieke OIDs te kiezen u wilt opiniepeilen. Het bespaart veel frustratie als je voor aanvang verifieert dat de gegevens die je wilt, er daadwerkelijk staan. Het object cpmCPUTotal5min MIB bevindt zich in Cisco-PROCES-MIB.

Om de OID te vinden die u wilt enquêteren, hebt u een conversietabel nodig die beschikbaar is op de Cisco CCO-website. Als u deze website wilt openen vanuit een webbrowser, gaat u naar de Cisco MIBs-pagina en klikt u op de koppeling OIDâ€™s.

Om toegang te krijgen tot deze website via een FTP-server, typt u **ftp://ftp.cisco.com/pub/mibs/oid/**. Van deze site, kunt u de specifieke MIB die is gedecodeerd en gesorteerd door OID-nummers downloaden.

Het volgende voorbeeld wordt afgeleid uit de Cisco-PROCES-MIB.oid-tabel. Dit voorbeeld laat zien dat de OID voor de **cpmCPUTotal5min** MIB 0,1.3.6.1.4.1.9.9.109.1.1.1.1.5 is.

Opmerking: vergeet niet om een "." toe te voegen aan het begin van de OID of u krijgt een fout wanneer u probeert deze te pollen. U moet ook een ".1" toevoegen aan het einde van de OID om het te concretiseren. Dit vertelt het apparaat de instantie van de OID die u zoekt. In sommige gevallen, hebben OIDs meer dan één instantie van een bepaald type van gegevens, zoals wanneer een router meerdere CPUs heeft.

<#root>

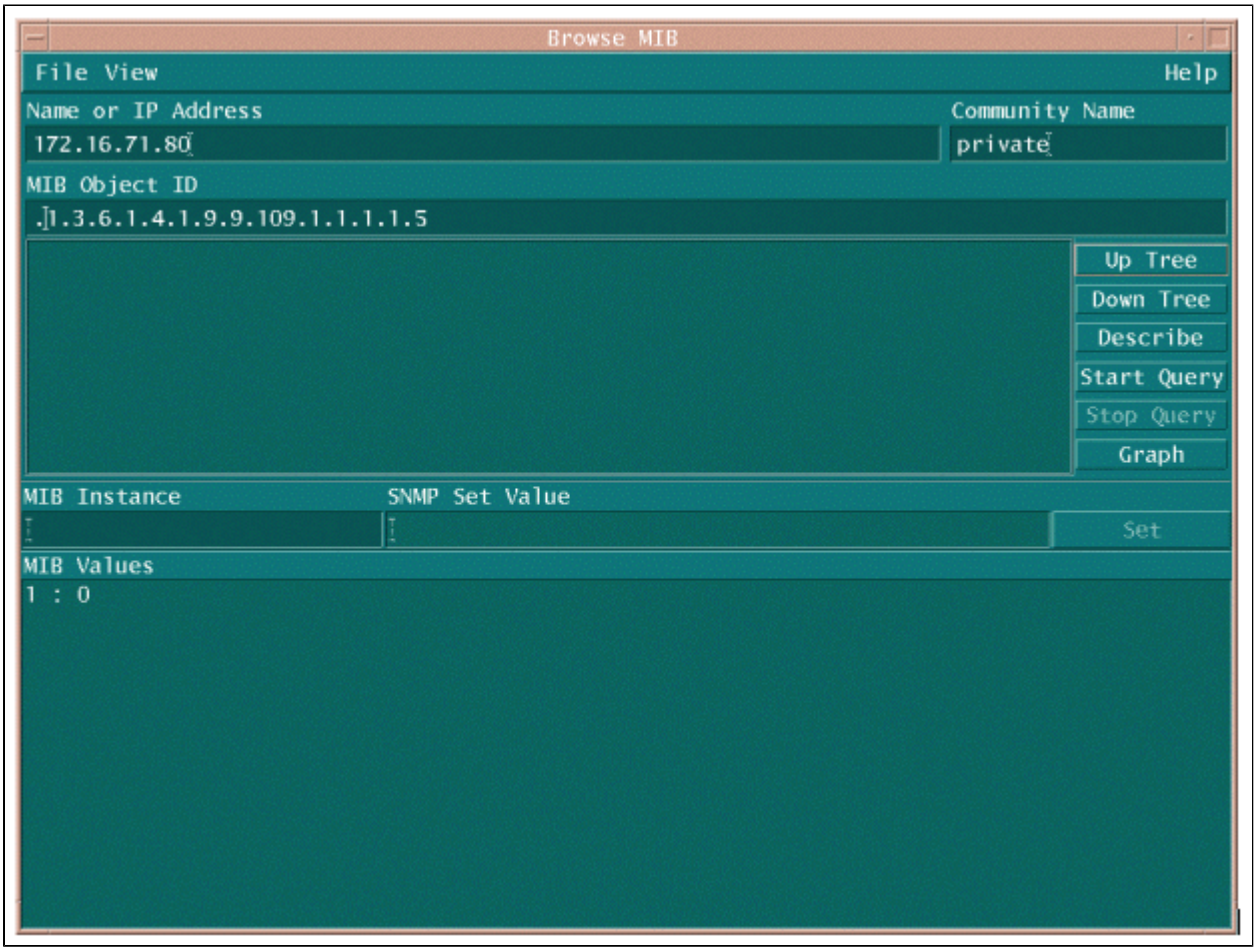
```
ftp://ftp.cisco.com/pub/mibs/oid/CISCO-PROCESS-MIB.oid
### THIS FILE WAS GENERATED BY MIB2SCHEMA
"org" "1.3"
"dod" "1.3.6"
"internet" "1.3.6.1"
"directory" "1.3.6.1.1"
"mgmt" "1.3.6.1.2"
"experimental" "1.3.6.1.3"
"private" "1.3.6.1.4"
"enterprises" "1.3.6.1.4.1"
"cisco" "1.3.6.1.4.1.9"
"ciscoMgmt" "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"
```

Er zijn twee gemeenschappelijke manieren om MIB OID te pollen om ervoor te zorgen dat het beschikbaar en functionerend is. Het is een goed idee om dit te doen voordat je begint met het verzamelen van bulkgegevens, zodat je geen tijd verspilt aan het opiniepeilen van iets dat er niet is en eindigen met een lege database. Een manier om dit te doen is door een MIB-walker van uw NMS-platform te gebruiken zoals HP

OpenView Network Node Manager (NNM) of CiscoWorks Windows, en de OID in te voeren die u wilt controleren.

Het volgende is een voorbeeld van HP OpenView SNMP MIB walker.



Een andere makkelijke manier om de MIB OID te pollen is om de UNIX commando **snellwalk** te gebruiken zoals in het volgende voorbeeld.

```
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.cpmCPUTo
```

In beide voorbeelden gaf de MIB een waarde van 0 terug, wat betekende dat de CPU voor die opiniepeilcyclus een gemiddelde benuttingsgraad van 0% had. Als u moeite hebt om het apparaat te laten reageren met de juiste gegevens, probeer dan het apparaat te pingelen en het apparaat te bereiken via Telnet. Als u nog steeds een probleem hebt, controleer dan de SNMP-configuratie en de SNMP-communitystrings. Mogelijk moet u een alternatieve MIB of een andere versie van IOS vinden om dit te kunnen doen werken.

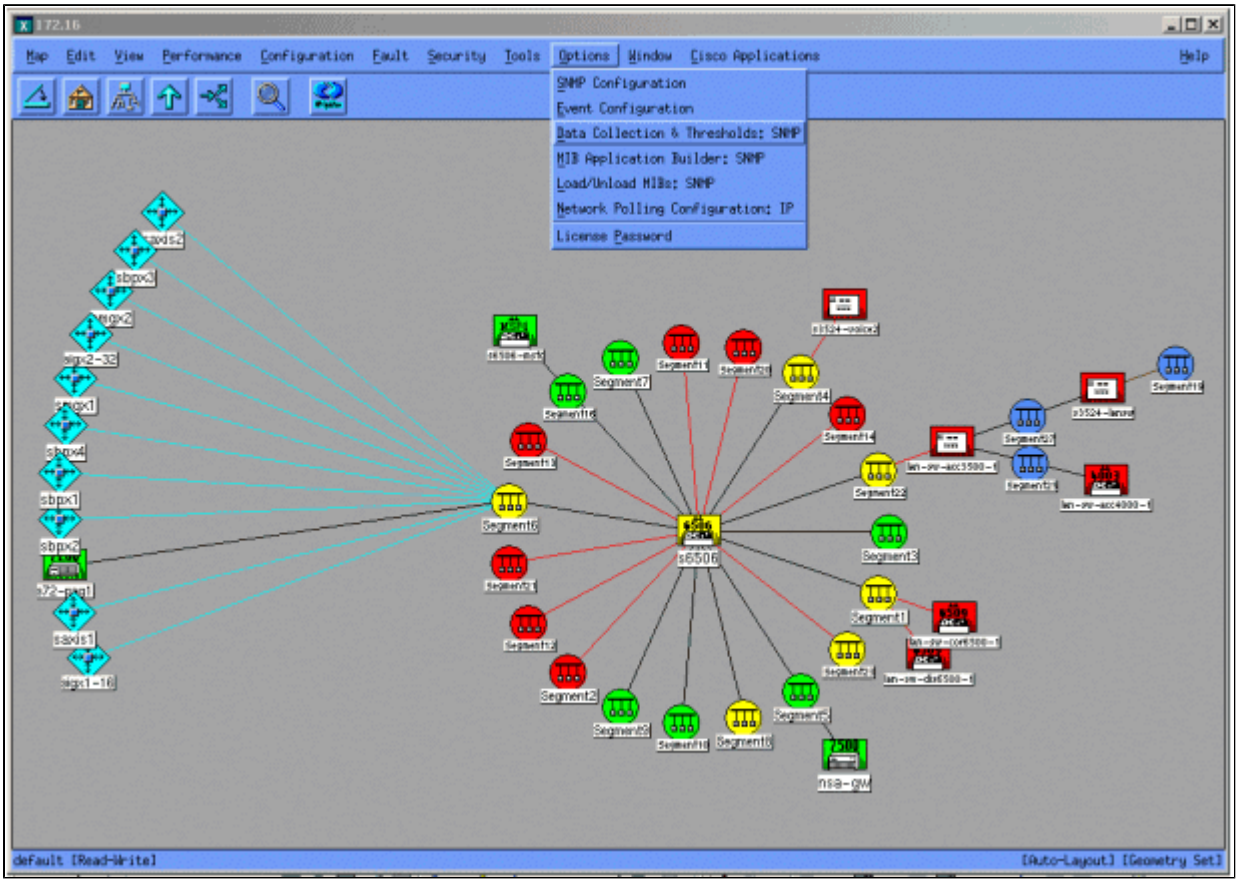
Stap 3: Poll and Record Specific SNMP MIB-object van de router

Er zijn verschillende manieren om MIB-objecten te pollen en de uitvoer op te nemen. Er zijn kant-en-klare producten, shareware-producten, scripts en verkooptools beschikbaar. Alle front-end tools gebruiken de SNMP **get** proces om de informatie te verkrijgen. De belangrijkste verschillen betreffen de flexibiliteit van

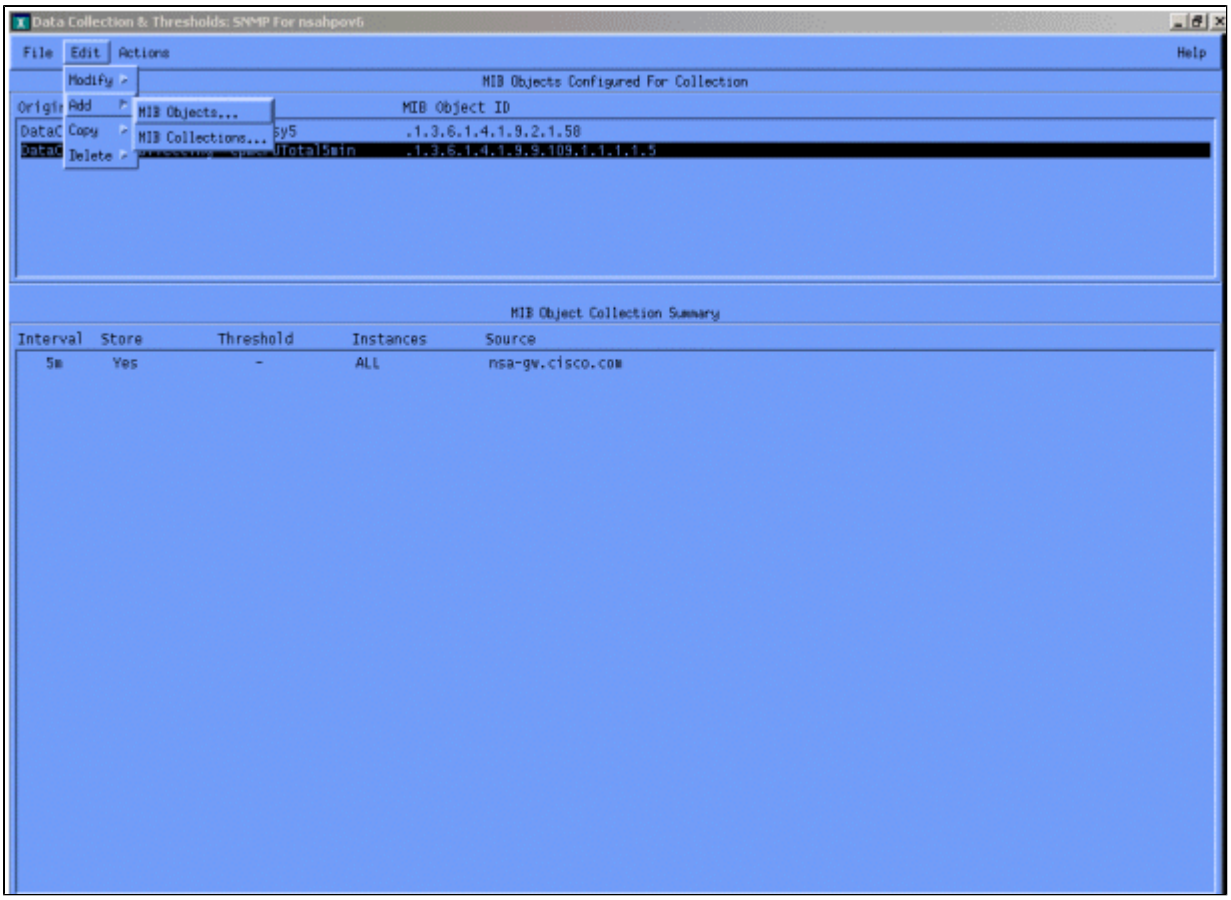
de configuratie en de manier waarop de gegevens in een database worden opgeslagen. Nogmaals, bekijk de processor MIB om te zien hoe deze verschillende methodes werken.

Nu u weet wordt OID gesteund in de router, moet u beslissen hoe vaak om het te krijgen en hoe te het te registreren. Cisco raadt aan de CPU MIB te enquêteren met intervallen van vijf minuten. Een lager interval zou de belasting op het netwerk of apparaat verhogen, en aangezien de MIB-waarde toch een vijf-minuten-gemiddelde is, zou het niet nuttig zijn om het vaker te enquêteren dan de gemiddelde waarde. Ook wordt over het algemeen aanbevolen dat de basislijn polling ten minste een periode van twee weken heeft, zodat u ten minste twee wekelijkse conjunctuurcycli op het netwerk kunt analyseren.

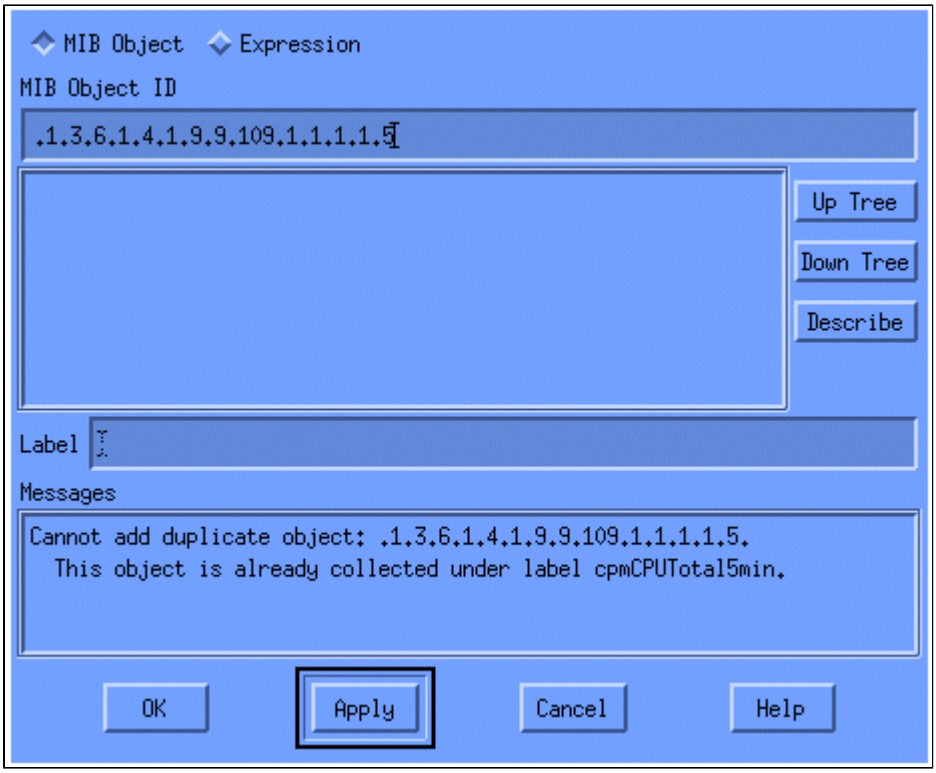
De volgende schermen tonen hoe u MIB-objecten kunt toevoegen met HP OpenView Network Node Manager versie 6.1. Selecteer vanuit het hoofdscherm **Opties > Gegevensverzameling en drempels**.



Selecteer vervolgens **Bewerken > Toevoegen > MIB-objecten**.

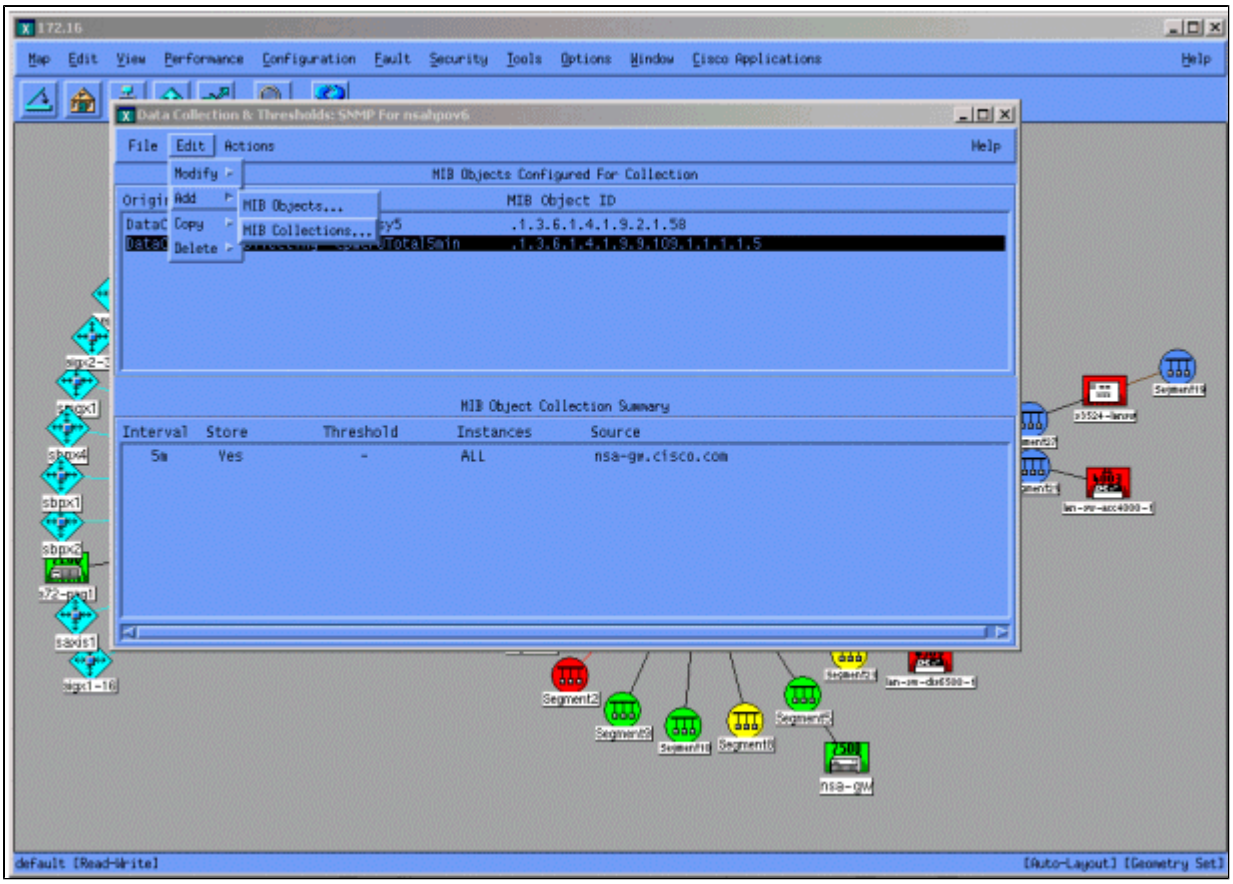


Voeg in het menu de OID-tekenreeks toe en klik op **Toepassen**. U hebt nu het MIB-object in het HP OpenView-platform ingevoerd, zodat het kan worden ondervraagd.



Vervolgens moet u HP OpenView laten weten welke router u voor deze OID moet kiezen.

Selecteer in het menu Gegevensverzameling de optie **Bewerken > Toevoegen > MIB-collecties**.

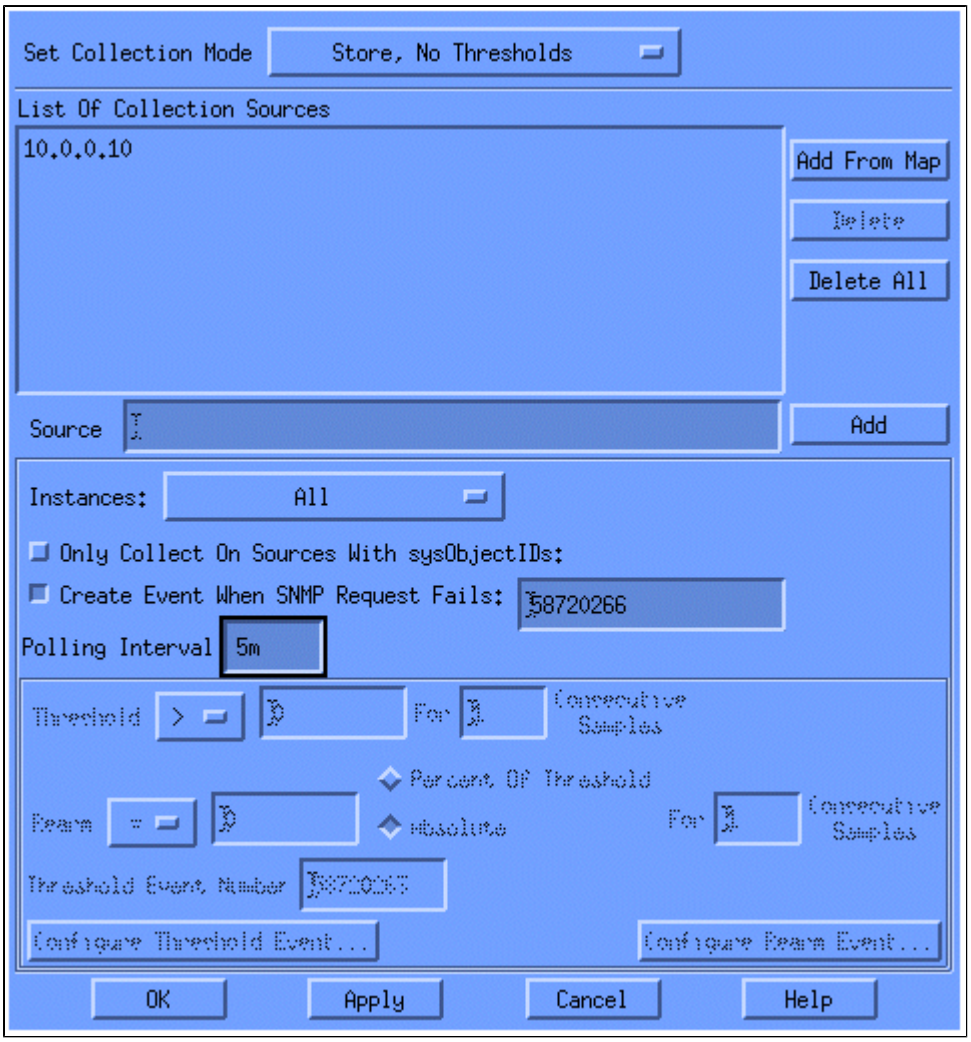


Voer in het veld Bron de naam (DNS) of het IP-adres van het domeinnaamgevingssysteem van de te enquêteren router in.

Selecteer **Opslaan, Geen drempelwaarden** uit de lijst Instelmodus.

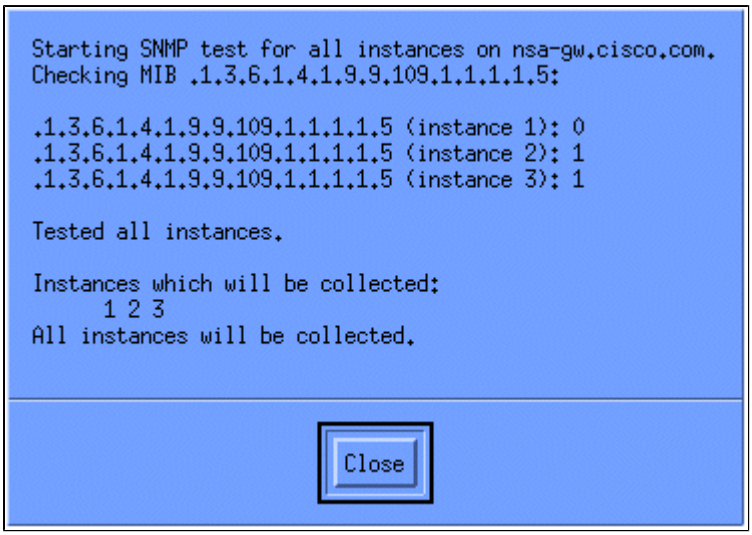
Stel het pollinginterval in op **5 m**, met tussenpozen van vijf minuten.

Klik op **Apply** (Toepassen).



U moet **Bestand > Opslaan** selecteren om de wijzigingen door te voeren.

Om te verifiëren dat de inzameling behoorlijk is opgezet, benadruk de inzamelingssummiere lijn voor de router en selecteer **Acties > Test SNMP**. Dit controleert om te zien of de community string correct is en zal opiniepeilen voor alle exemplaren van de OID.



Klik op **Sluiten** en laat de collectie een week draaien. Aan het einde van de weekperiode worden de gegevens voor analyse geëxtraheerd.

De gegevens worden eenvoudiger geanalyseerd als u ze naar een ASCII-bestand dumpt en in een spreadsheet, zoals Microsoft Excel, importeert. Om dit met HP OpenView NNM te doen, kunt u de opdrachtregel tool **snmpColDump** gebruiken. Elke geconfigureerde collectie schrijft naar een bestand in de directory /var/opt/OV/share/databases/snmpCollect/.

Extraheer de gegevens naar een ASCII-bestand met de naam **testfile** met de volgende opdracht:

<#root>

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

```
testfile
```

Opmerking: cpmCPUTotal5min.1 is het databasebestand dat HP OpenView NNM heeft gemaakt toen de OID-enquête begon.

Het gegenereerde testbestand lijkt op het volgende voorbeeld.

```
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/â€¦â€¦â€¦
```

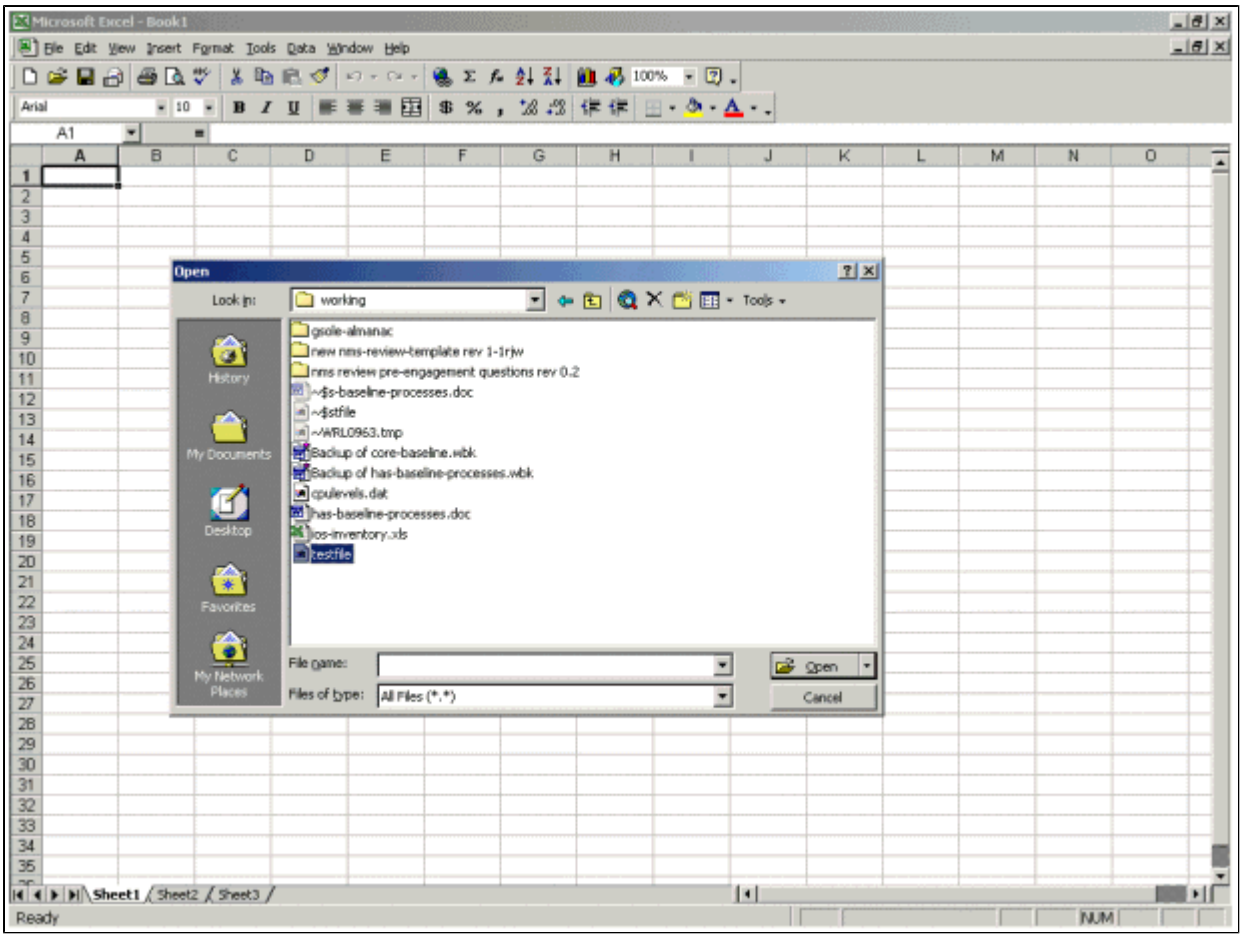
Zodra de output van het testbestand op uw UNIX-station staat, kunt u het naar uw PC overbrengen met behulp van File Transfer Protocol (FTP).

U kunt de gegevens ook verzamelen met behulp van uw eigen scripts. Om dit te doen, voer een **snmpget** voor de CPU OID elke vijf minuten uit en dump de resultaten in een .csv-bestand.

Stap 4: Gegevens analyseren om drempelwaarden te bepalen

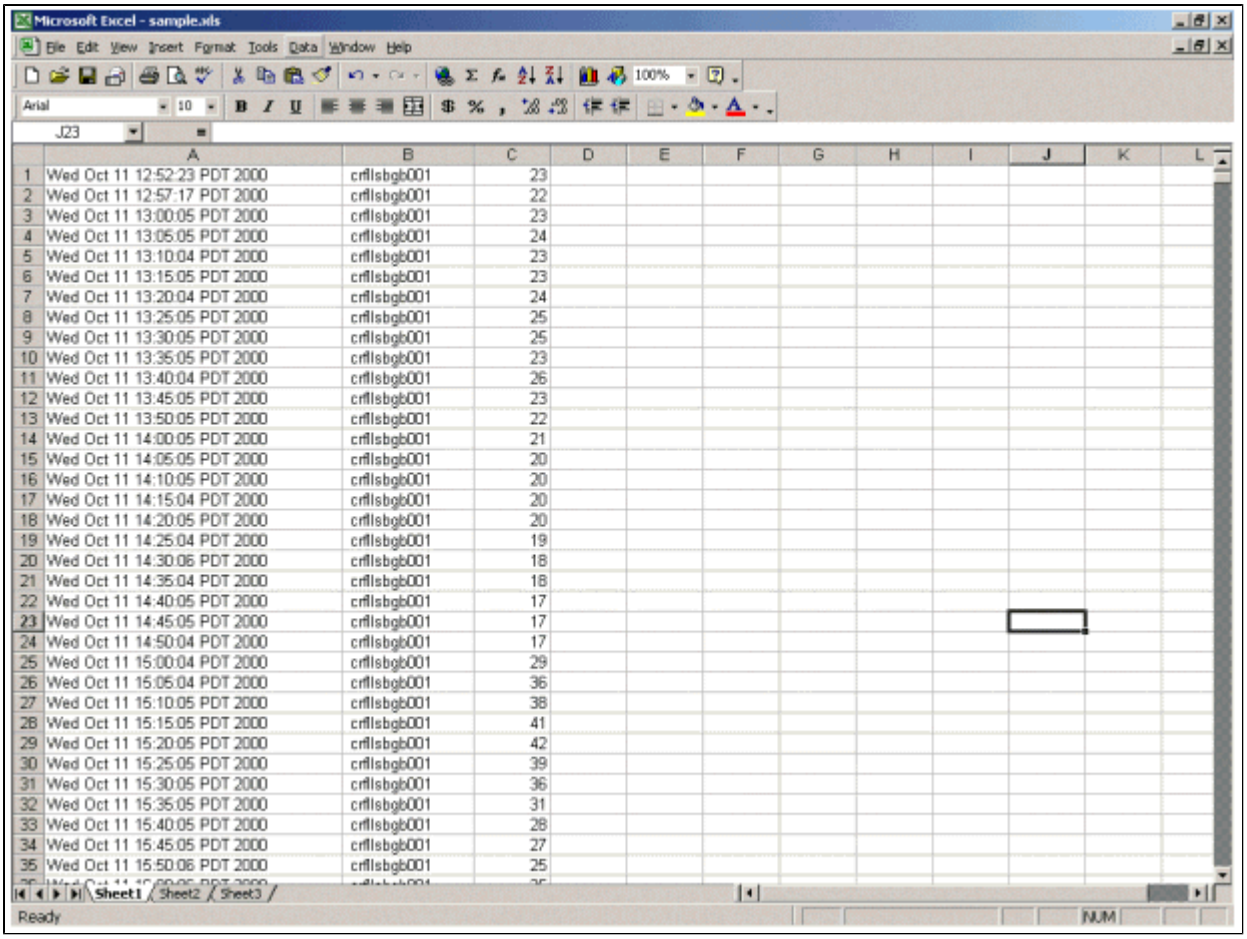
Nu je wat gegevens hebt, kan je beginnen ze te analyseren. Deze fase van de basislijn bepaalt de drempelinstellingen die u kunt gebruiken en die een nauwkeurige maatstaf zijn voor prestaties of fouten en niet te veel alarmen uitschakelen wanneer u de drempelbewaking inschakelt. Een van de eenvoudigste manieren om dit te doen is om de gegevens te importeren in een spreadsheet zoals Microsoft Excel en een spreidingsdiagram te plotten. Deze methode maakt het zeer gemakkelijk om te zien hoe vaak een bepaald apparaat een uitzonderingsalarm zou hebben gecreëerd als u het voor een bepaalde drempel zou controleren. Het is niet aan te raden om drempelwaarden in te schakelen zonder een basislijn uit te voeren, aangezien dit kan leiden tot waarschuwingsstormen van apparaten die de door u gekozen drempelwaarde hebben overschreden.

Als u het testbestand in een Excel-spreadsheet wilt importeren, opent u Excel en selecteert u **Bestand > Openen** en selecteert u uw gegevensbestand.



De Excel-toepassing vraagt u vervolgens om het bestand te importeren.

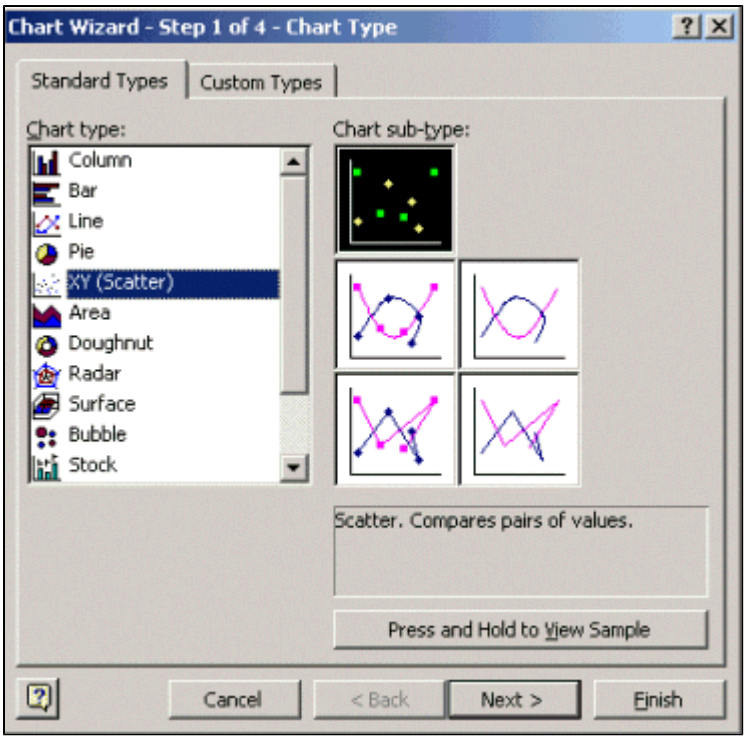
Als u klaar bent, ziet het geïmporteerde bestand er ongeveer hetzelfde uit als het volgende scherm.



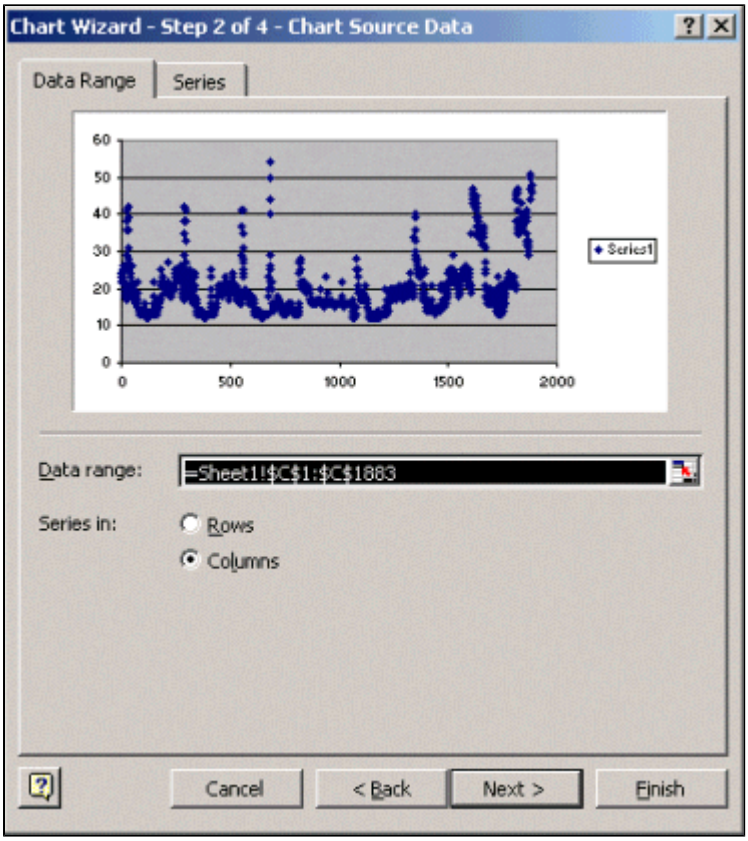
Met een spreidingsdiagram kunt u gemakkelijker visualiseren hoe verschillende drempelinstellingen zouden werken op het netwerk.

Als u het spreidingsdiagram wilt maken, markeert u kolom C in het geïmporteerde bestand en klikt u vervolgens op het pictogram **van** de **wizard Grafiek**. Dan volg de stappen door de Wizard Grafiek voor het maken van een spreidingsdiagram.

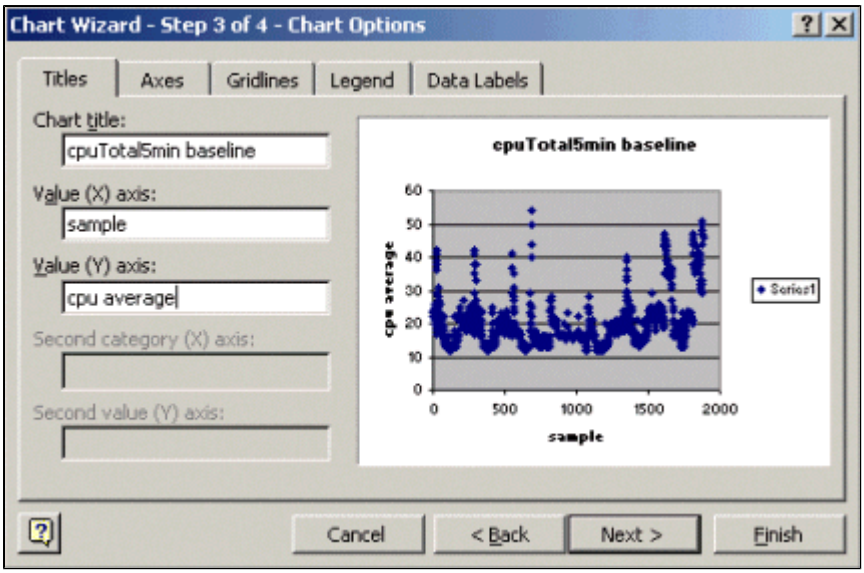
Selecteer in stap 1 van de wizard Grafiek de tab **Standaardtypen** en selecteer het type **XY (Scatter)**-tabel. Klik vervolgens op **Volgende**.



Selecteer in stap 2 van de wizard Grafiek de optie **Gegevensbereik** en selecteer het gegevensbereik en de optie **Kolommen**. Klik op **Next** (Volgende).



Voer in stap 3 van de wizard Grafiek de grafiektitel en de waarden van de X- en Y-as in en klik vervolgens op **Volgende**.



Selecteer in stap 4 van de wizard Grafiek of u het spreidingsdiagram op een nieuwe pagina of als een object op de bestaande pagina wilt weergeven.

Klik op **Voltooien** om de tabel op de gewenste locatie te plaatsen.

"Wat als?" Analyse

U kunt nu de spreidingsgrafiek voor analyse gebruiken. Voordat u echter verdergaat, moet u de volgende vragen stellen:

- Wat adviseert de verkoper (in dit voorbeeld is de verkoper Cisco) als drempel voor deze MIB-variabele?

  In het algemeen, adviseert Cisco dat een kernrouter niet 60 percenten gemiddeld gebruik van cpu overschrijdt. Zestig percent werd gekozen omdat een router wat overheadkosten voor het geval nodig heeft het problemen ervaart of het netwerk sommige mislukkingen heeft. Cisco schat dat een kernrouter ongeveer 40 procent CPU-overhead nodig heeft voor het geval dat een routeringsprotocol moet worden herberekend of opnieuw moet worden geconvergeerd. Deze percentages variëren gebaseerd op de protocollen die u gebruikt en de topologie en stabiliteit van uw netwerk.

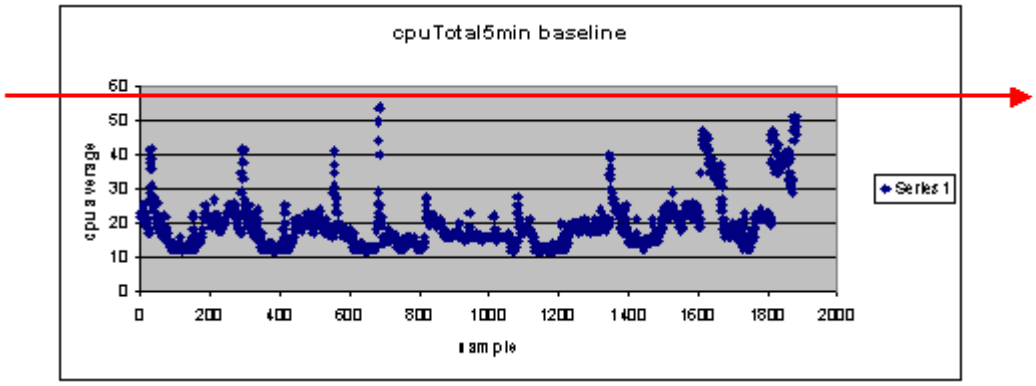
- Wat als ik 60 procent gebruik als drempelwaarde?

  Als u op 60 horizontaal een lijn over het spreidingsdiagram tekent, ziet u dat geen van de gegevenspunten meer dan 60 procent CPU-gebruik bedraagt. Dus een drempelwaarde van 60 die is ingesteld op uw netwerkbeheersysteem (NMS) stations zal geen drempelalarmmelding hebben geactiveerd tijdens de verkiezingsperiode. Een percentage van 60 is aanvaardbaar voor deze router. Merk echter in het spreidingsdiagram op dat sommige gegevenspunten dicht bij 60 liggen. Het zou fijn zijn om te weten wanneer een router de drempel van 60 percenten nadert zodat kunt u voor tijd weten dat cpu 60 percenten nadert en een plan hebt voor wat te doen wanneer het dat punt bereikt.

- Wat als ik de drempel op 50 procent stel?

  Geschat wordt dat deze router 50 percent gebruik vier keer tijdens deze opiniepeilingscyclus bereikte en een drempelalarm elke keer zou geproduceerd hebben. Dit proces wordt belangrijker wanneer u *groepen routers* bekijkt om te zien wat de verschillende drempelinstellingen zouden doen. Bijvoorbeeld: "Wat als ik de drempel op 50 procent stel voor het gehele kernnetwerk?" Je ziet dat het heel moeilijk is om slechts één getal te kiezen.

CPU drempelwaarde "wat als"-analyse



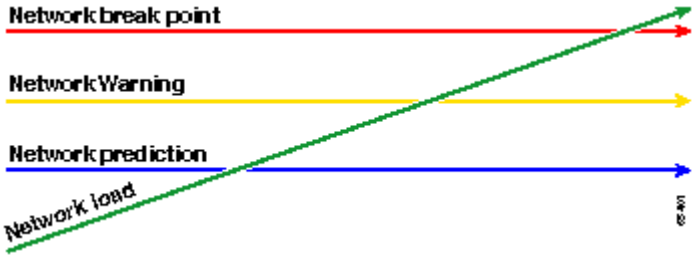
Een strategie die u kunt gebruiken om dit te vergemakkelijken is de Ready, Set, Go drempelmethodologie. Deze methode gebruikt drie opeenvolgende drempelwaarden.

- De kant-en-klare drempelwaarde die u instelt als een voorspeller van welke apparaten in de toekomst waarschijnlijk aandacht nodig zullen hebben
- De reeks-drempel die als vroege indicator wordt gebruikt, die u alarmeert beginnen plannend voor een reparatie, een aanpassing, of een verbetering
- Ga-de drempel die u en/of de verkoper geloven is een foutvoorwaarde en vereist één of andere actie om het te herstellen; in dit voorbeeld is het 60 percent

De volgende tabel toont de strategie van de strategie Klaar, Stel, Ga.

Drempel	Actie	Resultaat
45 procent	Verder onderzoeken	Lijst van opties voor actieplannen
50%	Actieplan opstellen	Lijst van stappen in het actieplan
60%	Actieplan uitvoeren	De router overschrijdt geen drempels meer. Terug naar de modus Klaar

De methodologie Ready, Set, Go verandert de oorspronkelijke basislijnkaart die eerder is besproken. In het volgende diagram wordt het gewijzigde basislijnschema weergegeven. Als je de andere snijpunten in de grafiek kunt identificeren, heb je nu meer tijd om te plannen en te reageren dan voorheen.



Bericht dat in dit proces, de aandacht op de uitzonderingen in het netwerk wordt geconcentreerd en niet met andere apparaten betrokken is. Er wordt van uitgegaan dat zolang apparaten onder de drempelwaarden liggen, ze in orde zijn.

Als je deze stappen vanaf het begin hebt doordacht, ben je goed voorbereid op het gezond houden van het netwerk. Het uitvoeren van dit soort planning is ook zeer nuttig voor begrotingsplanning. Als u weet wat uw top vijf **go** routers, uw midden **set** routers, en uw bodem **klaar** routers zijn, kunt u gemakkelijk plannen op hoeveel budget u nodig hebt voor upgrades gebaseerd op wat voor soort routers zij zijn en wat uw actieplan opties zijn. Dezelfde strategie kan worden gebruikt voor WAN-koppelingen (Wide Area Network) of andere MIB-OIDâ€™s.

Stap 5: Oplossen van geïdentificeerde onmiddellijke problemen

Dit is een van de makkelijkste onderdelen van het basisproces. Zodra u hebt geïdentificeerd welke apparaten de **go** drempel overschrijden, zou u een actieplan moeten maken om die apparaten terug onder drempel te krijgen.

U kunt een case openen met het Cisco Technical Assistance Center (TAC) of contact opnemen met uw Systems Engineer voor beschikbare opties. Je moet er niet van uitgaan dat het terugkrijgen van dingen onder de drempel je geld zal kosten. Sommige CPU-problemen kunnen worden opgelost door de configuratie te wijzigen, zodat alle processen op de meest efficiënte manier worden uitgevoerd. Sommige toegangscontrolelijsten (ACLâ€™s) kunnen bijvoorbeeld een router-CPU zeer hoog laten draaien vanwege het pad dat de pakketten door de router nemen. In bepaalde gevallen kunt u NetFlow-switching implementeren om het pakketswitchingpad te wijzigen en de impact van de ACL op de CPU te verminderen. Wat de problemen ook zijn, het is noodzakelijk om alle routers terug onder drempel in deze stap te krijgen zodat u de drempels later kunt implementeren zonder het risico van het overspoelen van de NMS-stations met te veel drempelalarmen.

Stap 6: Bewaking van testdrempels

Deze stap omvat het testen van de drempels in het laboratorium met behulp van de tools die u in het productienetwerk zult gebruiken. Er zijn twee gemeenschappelijke benaderingen voor de bewaking van drempelwaarden. U moet beslissen welke methode het beste is voor uw netwerk.

- Poll en vergelijk methode met een SNMP-platform of een ander SNMP-controleprogramma

  Deze methode gebruikt meer netwerkbandbreedte voor opiniepeilingsverkeer en neemt verwerkingscycli op uw SNMP-platform in beslag.

- Gebruik configuraties voor externe bewaking (RMON) van alarmsignalen en gebeurtenissen in de routers, zodat er alleen een waarschuwing wordt verzonden wanneer een drempelwaarde wordt overschreden

  Deze methode vermindert het gebruik van de netwerkbandbreedte maar verhoogt ook het geheugen en het CPU-gebruik op de routers.

Een drempelwaarde implementeren met SNMP

Als u de SNMP-methode wilt instellen met HP OpenView NM, selecteert u **Opties > Gegevensverzameling en drempelwaarden** zoals u hebt gedaan bij het instellen van de eerste peiling. Dit keer selecteert u echter **Store, Drempelwaarden controleren in** plaats van Store, Geen Drempelwaarden in het menu Collecties. Nadat u de drempel hebt ingesteld, kunt u het CPU-gebruik op de router verhogen door deze meerdere pings en/of meerdere SNMP-wandelingen te verzenden. Het kan zijn dat u de drempelwaarde moet verlagen als u de CPU niet hoog genoeg kunt dwingen om de drempelwaarde te overschrijden. In ieder geval moet u ervoor zorgen dat het drempelmechanisme werkt.

Een van de beperkingen van het gebruik van deze methode is dat je niet meerdere drempels tegelijk kunt implementeren. U hebt drie SNMP-platforms nodig om drie verschillende gelijktijdige drempels in te

stellen. Tools zoals Concord Network Health en Trinagy TREND staan meerdere drempels toe voor dezelfde OID-instantie.

Als uw systeem slechts één drempelwaarde tegelijk kan verwerken, kunt u de Ready, Set, Go-strategie seriële overwegen. Dat wil zeggen, wanneer de **gereed** drempelwaarde voortdurend wordt bereikt, start uw onderzoek en verhoog de drempelwaarde naar het ingestelde niveau voor dat apparaat. Wanneer het **vastgestelde** niveau voortdurend wordt bereikt, begin dan met het formuleren van uw actieplan en verhoog de drempel naar het **go** niveau voor dat apparaat. Als de go-drempel dan voortdurend wordt bereikt, voer dan uw actieplan uit. Dit zou net zo goed moeten werken als de drie gelijktijdige drempelmethode. Het duurt alleen een beetje meer tijd om de SNMP-platform drempelinstellingen te veranderen.

Een drempelwaarde implementeren met RMON - alarm en gebeurtenis

Gebruikend RMON alarmconfiguraties en gebeurtenisconfiguraties, kunt u de routermonitor zelf voor veelvoudige drempels hebben. Wanneer de router een over-drempelvoorwaarde ontdekt, verzendt het een val van SNMP naar het platform van SNMP. U moet in uw routerconfiguratie een SNMP-trap-ontvanger hebben ingesteld om de trap door te sturen. Er is een correlatie tussen een alarm en een gebeurtenis. Het alarm controleert OID de bepaalde drempel. Als de drempel wordt bereikt, het alarmproces vuurt het gebeurtenisproces dat of een SNMP- valbericht kan verzenden, een RMON- logboekingang, of allebei creëren. Zie RMON-alarmopdrachten en configuratieopdrachten voor gebeurtenissen voor meer informatie over deze opdracht.

De volgende opdrachten voor routerconfiguratie hebben de routermonitor cpmCPUTotal5min om de 300 seconden. Het zal gebeurtenis 1 ontslaan als de CPU meer dan 60 procent bedraagt en zal gebeurtenis 2 ontslaan als de CPU terugvalt naar 40 procent. In beide gevallen wordt er een SNMP-trap-bericht naar het NMS-station verzonden met de community private string.

Om de Ready, Set, Go methode te gebruiken, gebruikt u alle volgende configuratie-instructies.

```
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
```

Het volgende voorbeeld toont de output van het bevel van het **show rmon alarm** dat door de bovengenoemde verklaringen werd gevormd.

<#root>

```
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
```

Het volgende voorbeeld toont de output van het bevel van de **show rmon gebeurtenis**.

<#root>

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
```

U kunt beide methoden proberen om te zien welke methode het beste bij uw omgeving past. U kunt zelfs

vinden dat een combinatie van methodes goed werkt. In ieder geval moeten testen in een laboratoriumomgeving worden uitgevoerd om er zeker van te zijn dat alles correct werkt. Na het testen in het laboratorium, zal een beperkte plaatsing op een kleine groep routers u toestaan om het proces te testen om alarm naar uw Verrichtingen Centrum te verzenden.

In dit geval zult u de drempels moeten verlagen om het proces te testen: het is niet aan te raden om te proberen de CPU op een productierouter kunstmatig te verhogen. U dient er ook voor te zorgen dat wanneer de waarschuwingen binnenkomen in de NMS-stations bij het Operations Center, er een escalatiebeleid is om ervoor te zorgen dat u op de hoogte wordt gesteld wanneer apparaten drempelwaarden overschrijden. Deze configuraties zijn getest in een laboratorium met Cisco IOS versie 12.1(7). Als u problemen ondervindt, dient u contact op te nemen met Cisco Engineering of Systems Engineers om te zien of u een bug hebt in uw IOS-versie.

Stap 7: Voer drempelwaardebewaking uit met SNMP of RMON

Zodra u grondig de controle van de drempel in het laboratorium hebt getest, en in een beperkte plaatsing, bent u bereid om drempels over het kernnetwerk uit te voeren. U kunt nu systematisch door dit basislijnproces voor andere belangrijke MIB variabelen op uw netwerk gaan, zoals buffers, vrij geheugen, cyclische overtolligheidscontrole (CRC) fouten, AMT celverlies, etc.

Als u RMON alarm- en gebeurtenisconfiguraties gebruikt, kunt u nu stoppen met stemmen vanaf uw NMS-station. Dit zal de lading op uw NMS server verminderen en zal de hoeveelheid opiniepeilingsgegevens over het netwerk verminderen. Door systematisch door dit proces voor belangrijke netwerkgezondheidsindicatoren te gaan, zou u gemakkelijk tot het punt kunnen komen dat de netwerkapparatuur zichzelf controleert met behulp van RMON Alarm en Gebeurtenis.

Aanvullende MIBâ€™s

Nadat u dit proces hebt geleerd, kunt u andere MIBs aan basislijn willen onderzoeken en controleren. De volgende subsecties presenteren een korte lijst van enkele OID's en beschrijvingen die u nuttig kunt vinden.

RouterMIBâ€™s

De kenmerken van het geheugen zijn zeer nuttig in het bepalen van de gezondheid van een router. Een gezonde router zou bijna altijd beschikbare bufferruimte moeten hebben om mee te werken. Als de router geen bufferruimte meer heeft, zal de CPU harder moeten werken om nieuwe buffers te maken en om te proberen buffers te vinden voor inkomende en uitgaande pakketten. Een diepgaande discussie over buffers valt buiten de reikwijdte van dit document. Als algemene regel echter, een gezonde router zou zeer weinig, als om het even welk, buffermissen moeten hebben en geen buffermislukkingen, of een nul vrije geheugenvoorwaarde moeten hebben.

Voorwerp	Beschrijving	OID
Cisco Memory PoolFree	Het aantal bytes uit de geheugenpool die momenteel niet worden gebruikt op het beheerde apparaat	1.3.6.1.4.1.9.9.48.1.1.1.6
Cisco Memory PoolGrootste gratis	Het grootste aantal aangrenzende bytes uit de geheugenpool die momenteel niet	1.3.6.1.4.1.9.9.48.1.1.1.7

	worden gebruikt	
bufferElMiss	Het aantal ontbrekende bufferelementen	1.3.6.1.4.1.9.2.1.12
bufferFail	Het aantal fouten bij de toewijzing van buffers	1.3.6.1.4.1.9.2.1.46
buffermengsel	Het aantal buffers leidt tot storingen als gevolg van geen vrij geheugen	1.3.6.1.4.1.9.2.1.47

Catalyst Switch MIBâ€™s

Voorwerp	Beschrijving	OID
cpm PUT Totaal5min	Totale CPU-drukpercentage in de laatste vijf minuten. Dit object degradeert het object avgBusy5 van het bestand OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5
cpm PUT Totaal5sec	Totale CPU-drukpercentage in de laatste vijf seconden. Dit object veroudert het taak-per object van de OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.3
Systeemverkeer	Het percentage van bandbreedtegebruik voor het vorige pollinginterval	1.3.6.1.4.1.9.5.1.1.8
sysTrafficPeak	De piekwaarde van de verkeersmeter sinds de laatste klaring van de havenloketten of het opstarten van het systeem	1.3.6.1.4.1.9.5.1.1.19
sysTrafficPeaktime	De tijd (in honderdste van een seconde) sinds de piekwaarde van de verkeersmeter	1.3.6.1.4.1.9.5.1.1.20

poortTopNUtilization	Gebruik van de poort in het systeem	1.3.6.1.4.1.9.5.1.20.2.1.4
portTopNBufferOverFlow	Het aantal bufferoverlopen van de haven in het systeem	1.3.6.1.4.1.9.5.1.20.2.1.10

Seriële link MIBâ€™s

Voorwerp	Beschrijving	OID
locifInputQueueDrops	Het aantal pakketten daalde omdat de invoerwachtrij vol was	1.3.6.1.4.1.9.2.2.1.1.26
locifOutput QueueDrops	Het aantal pakketten daalde omdat de uitvoerwachtrij vol was	1.3.6.1.4.1.9.2.2.1.1.27
locIfInCRC	Het aantal invoerpakketten met cyclische redundantie controlesomfouten	1.3.6.1.4.1.9.2.2.1.1.12

RMON - configuratieopdrachten voor alarm en gebeurtenis

Alarmen

RMON - alarmen kunnen met de volgende syntaxis worden geconfigureerd:

<#root>

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

element	Beschrijving
aantal	Het alarmnummer, dat identiek is aan de alarmIndex in de alarmTable in RMON MIB.
veranderlijk	Het te controleren MIB-object, dat zich vertaalt in de alarmvariabele in de alarmtabel van RMON MIB.
tussenruimte	De tijd, in seconden, het alarm controleert de MIB variabele, die aan het alarmInterval

	identiek is dat in de alarmTable van RMON MIB wordt gebruikt.
delta	Test de verandering tussen MIB variabelen, die alarmSampleType in de alarmTable van RMON MIB beïnvloedt.
absoluut	Test elke MIB variabele direct, die alarmSampleType in de alarmTable van RMON MIB beïnvloedt.
drempelwaarde voor stijging	De waarde waarbij het alarm wordt geactiveerd.
nummer van het evenement	(Optioneel) Het gebeurtenisnummer dat moet worden geactiveerd wanneer de drempelwaarde wordt overschreden. Deze waarde is identiek aan het alarmRisingEventIndex of het alarmFallingEventIndex in de alarmTable van RMON MIB.
dalende drempelwaarde	De waarde waarbij het alarm wordt teruggesteld.
eigenaarsstring	(Optioneel) Specificeert een eigenaar voor het alarm, dat identiek is aan het alarmOwner in de alarmTable van RMON MIB.

Gebeurtenissen

RMON - gebeurtenissen kunnen met de volgende syntaxis worden geconfigureerd:

<#root>

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

element	Beschrijving
aantal	Toegewezen gebeurtenisnummer, dat identiek is aan de eventIndex in de eventTable in RMON MIB.
logboek	(Optioneel) genereert een RMON-logingang wanneer de gebeurtenis wordt geactiveerd en stelt de eventType in RMON MIB in op log of log-and-trap.
valstrik	(Optioneel) SNMP-community-string gebruikt voor deze trap. Configureert de instelling van eventType in RMON MIB voor deze rij als snmp-trap of log-and-trap. Deze waarde is identiek aan de eventCommunityValue in de eventTable in de RMON MIB.

beschrijvingsstring	(Optioneel) Specificeert een beschrijving van de gebeurtenis, die identiek is aan de beschrijving van de gebeurtenis in de eventTable van de RMON MIB.
eigenaarsstring	(Optioneel) Eigenaar van dit evenement, dat identiek is aan de eventOwner in de eventTable van de RMON MIB.

RMON - implementatie van alarm en gebeurtenis

Voor gedetailleerde informatie over RMON - alarm en gebeurtenisimplementatie, te lezen gelieve de sectie RMON van het Alarmsysteem en van de Gebeurtenis van de Implementatie van het Witboek van de *Beste praktijken van de Systemen van het Netwerkbeheer*.

Gerelateerde informatie

- **Technische ondersteuning en documentatie - Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.