Whitepaper: Best Practices für Baseline-Prozesse

Inhalt

Einleitung

In diesem Dokument werden grundlegende Konzepte und Verfahren für hochverfügbare Netzwerke beschrieben. Er enthält wichtige Erfolgsfaktoren für Netzwerk-Baselining und Grenzwertbildung, die bei der Erfolgsbewertung helfen. Darüber hinaus enthält er detaillierte Informationen zu Baseline- und Schwellenwertprozessen sowie zur Implementierung, die den Best Practice-Richtlinien folgen, die vom Cisco High Availability Services (HAS)-Team festgelegt wurden.

Dieses Dokument führt Sie Schritt für Schritt durch den Baselining-Prozess. Einige aktuelle Produkte des Netzwerkmanagementsystems (NMS) können bei der Automatisierung dieses Prozesses behilflich sein. Der Baselining-Prozess bleibt jedoch unabhängig davon, ob Sie automatisierte oder manuelle Tools verwenden, gleich. Wenn Sie diese NMS-Produkte verwenden, müssen Sie die Standardschwellenwerteinstellungen für Ihre individuelle Netzwerkumgebung anpassen. Es ist wichtig, diese Schwellenwerte auf intelligente Weise auszuwählen, damit sie sinnvoll und korrekt sind.

Grundlinie

Was ist eine Baseline?

Eine Baseline ist ein Prozess, bei dem das Netzwerk in regelmäßigen Abständen überprüft wird, um sicherzustellen, dass es ordnungsgemäß funktioniert. Es ist mehr als nur ein einziger Bericht, der den Zustand des Netzwerks zu einem bestimmten Zeitpunkt beschreibt. Wenn Sie den grundlegenden Prozess

befolgen, können Sie die folgenden Informationen abrufen:

- Sammeln Sie wertvolle Informationen über den Zustand von Hardware und Software.
- Bestimmen der aktuellen Nutzung von Netzwerkressourcen
- Treffen genauer Entscheidungen über Alarmschwellenwerte im Netzwerk
- Identifizieren aktueller Netzwerkprobleme
- Vorhersage zukünftiger Probleme

Eine weitere Betrachtungsweise der Baseline ist im folgenden Diagramm dargestellt.

Die rote Linie, der Netzwerk-Unterbrechungspunkt, ist der Punkt, an dem das Netzwerk unterbrochen wird. Dieser Punkt wird durch das Wissen über die Leistung von Hardware und Software bestimmt. Die grüne Linie, die Netzwerklast, beschreibt den natürlichen Verlauf der Netzwerklast beim Hinzufügen neuer Anwendungen und andere Faktoren.

Der Zweck einer Baseline besteht darin, Folgendes zu bestimmen:

- Das Netzwerk befindet sich an einem grünen Punkt
- Wie schnell die Netzwerklast zunimmt
- Hoffentlich vorhersagen, zu welchem Zeitpunkt die beiden schneiden

Wenn Sie regelmäßig eine Baseline erstellen, können Sie den aktuellen Status ermitteln *und* extrapolieren, wann Ausfälle auftreten, und sich im Voraus darauf vorbereiten. Dies hilft Ihnen auch, fundiertere Entscheidungen darüber zu treffen, wann, wo und wie Sie Budgetmittel für Netzwerk-Upgrades ausgeben sollten.

Warum eine Baseline?

Ein grundlegender Prozess hilft Ihnen, kritische Probleme mit der Ressourcenbeschränkung im Netzwerk zu identifizieren und richtig zu planen. Diese Probleme können als Ressourcen der Kontroll- oder Datenebene bezeichnet werden. Die Ressourcen der Kontrollebene sind spezifisch für die Plattform und die Module im Gerät und können von einer Reihe von Problemen betroffen sein:

- Datennutzung
- Funktionen aktiviert
- Netzwerkdesign

Zu den Ressourcen auf der Kontrollebene gehören u. a. folgende Parameter:

- CPU-Auslastung
- Speichernutzung

- Puffer-Auslastung

Die Ressourcen der Datenebene werden nur durch den Typ und die Menge des Datenverkehrs beeinträchtigt. Hierzu zählen die Verbindungsauslastung und die Backplane-Auslastung. Durch die Festlegung einer Baselining-Strategie für die Ressourcennutzung in kritischen Bereichen können Sie ernsthafte Leistungsprobleme oder sogar einen Netzwerkzusammenbruch vermeiden.

Mit der Einführung latenzanfälliger Anwendungen wie Sprache und Video ist Baselining wichtiger denn je. Herkömmliche TCP/IP-Anwendungen (Transmission Control Protocol/Internet Protocol) sind weniger zeitaufwendig und erlauben eine gewisse Verzögerung. Sprache und Video basieren auf User Datagram Protocol (UDP) und ermöglichen keine Neuübertragungen oder Netzwerküberlastungen.

Dank der neuen Anwendungskombination hilft Ihnen Baselining dabei, Probleme bei der Ressourcennutzung auf Kontroll- und Datenebene zu verstehen und proaktiv Änderungen und Upgrades zu planen, um einen kontinuierlichen Erfolg zu gewährleisten.

Datennetzwerke gibt es schon seit vielen Jahren. Bis vor Kurzem war die Aufrechterhaltung des Netzwerkbetriebs ein eher nachsichtiger Prozess mit einer gewissen Fehlertoleranz. Mit der zunehmenden Akzeptanz latenzempfindlicher Anwendungen wie Voice over IP (VoIP) wird der Netzwerkbetrieb immer schwieriger und erfordert mehr Präzision. Um präziser zu sein und einem Netzwerkadministrator eine solide Grundlage für die Verwaltung des Netzwerks zu geben, ist es wichtig, sich einen Überblick über die Funktionsweise des Netzwerks zu verschaffen. Dazu müssen Sie einen Prozess durchlaufen, der als Baseline bezeichnet wird.

Basisziel

Das Ziel eines Referenzrahmens ist es,

1. Ermitteln des aktuellen Status von Netzwerkgeräten
2. Vergleichen Sie diesen Status mit den Standard-Performance-Richtlinien.
3. Grenzwerte festlegen, die Sie benachrichtigen, wenn der Status diese Richtlinien überschreitet

Aufgrund der großen Datenmengen und der Zeit, die für die Analyse der Daten benötigt wird, müssen Sie zunächst den Umfang einer Baseline begrenzen, um den Prozess leichter zu erlernen. Der logischste und zuweilen vorteilhafteste Ausgangspunkt ist der Kern des Netzwerks. Dieser Teil des Netzwerks ist normalerweise der kleinste und erfordert die meiste Stabilität.

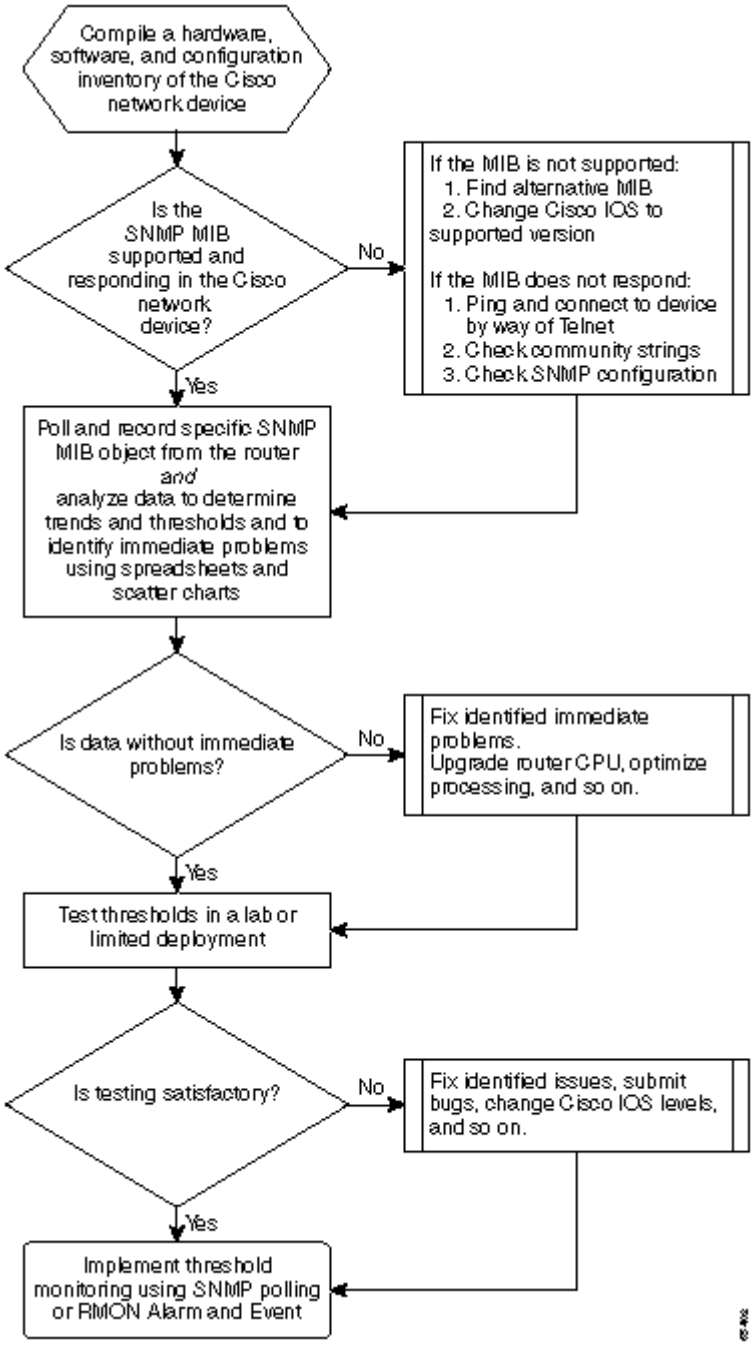
Der Einfachheit halber wird in diesem Dokument erläutert, wie eine sehr wichtige Simple Network Management Protocol Management Information Base (SNMP MIB) als Ausgangsbasis verwendet werden kann: cpmCPUTotal5min. cpmCPUTotal5min ist der fünf Minuten dauernde Durchschnitt der zentralen Verarbeitungseinheit (CPU) eines Cisco Routers und stellt einen Leistungsindikator auf der Kontrollebene dar. Die Baseline wird auf einem Cisco Router der Serie 7000 ausgeführt.

Nachdem Sie den Prozess gelernt haben, können Sie ihn auf alle Daten anwenden, die in der riesigen SNMP-Datenbank verfügbar sind, die in den meisten Cisco Geräten verfügbar ist, z. B.:

- Nutzung des Integrated Services Digital Network (ISDN)
- Verlust von Zellen im asynchronen Übertragungsmodus (ATM)
- Freier Systemspeicher

Grundlegender Flussdiagramm

Das folgende Flussdiagramm zeigt die grundlegenden Schritte des Core-Baseline-Prozesses. Zwar stehen Ihnen Produkte und Tools zur Verfügung, mit denen Sie einige dieser Schritte durchführen können, sie weisen jedoch in der Regel Lücken in der Flexibilität oder Benutzerfreundlichkeit auf. Auch wenn Sie planen, mithilfe von NMS-Tools (Network Management System) Baselining durchzuführen, ist dies immer noch eine gute Übung, um den Prozess zu studieren und zu verstehen, wie Ihr Netzwerk wirklich funktioniert. Dieser Prozess kann auch einige der Rätsel aus, wie einige NMS-Tools arbeiten, da die meisten Tools im Wesentlichen die gleichen Dinge tun.



Baseline-Verfahren

Schritt 1: Zusammenstellen eines Hardware-, Software- und Konfigurationsbestands

Es ist äußerst wichtig, dass Sie aus mehreren Gründen eine Bestandsaufnahme der Hardware, Software und Konfiguration erstellen. Erstens sind Cisco SNMP MIBs in einigen Fällen spezifisch für die von Ihnen ausgeführte Cisco IOS-Version. Einige MIB-Objekte werden durch neue ersetzt oder zeitweise vollständig eliminiert. Der Hardwarebestand ist nach der Datenerfassung am wichtigsten, da die Schwellenwerte, die Sie nach der anfänglichen Baseline festlegen müssen, häufig auf der CPU-Art, der Speichergröße usw. auf den Cisco Geräten basieren. Der Konfigurationsbestand ist auch wichtig, um sicherzustellen, dass Sie die aktuellen Konfigurationen kennen: Sie können die Gerätekonfigurationen nach der Baseline ändern, um Puffer anzupassen usw.

Die effizienteste Möglichkeit, diesen Teil der Basislinie für ein Cisco Netzwerk zu übernehmen, ist CiscoWorks2000 Resource Manager Essentials (Essentials). Wenn diese Software korrekt im Netzwerk installiert ist, sollte Essentials über die aktuellen Bestände aller Geräte in seiner Datenbank verfügen. Sie müssen sich nur die Bestände ansehen, um festzustellen, ob es irgendwelche Probleme gibt.

Die folgende Tabelle zeigt ein Beispiel für einen Softwareinventarbericht der Cisco Router Class, der aus Essentials exportiert und dann in Microsoft Excel bearbeitet wurde. Beachten Sie, dass aus diesem Bestand SNMP MIB-Daten und OIDs (Object Identifiers) verwendet werden müssen, die in den Cisco IOS-Versionen 12.0x und 12.1x enthalten sind.

Device Name (Gerätename)	Routertyp	Version	Software-Version
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	0 x 101	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 (5 T)

Wenn Essentials nicht im Netzwerk installiert ist, können Sie mithilfe des UNIX-Befehlszeilentools **snmpwalk** von einer UNIX-Workstation aus nach der IOS-Version suchen. Dies wird im folgenden Beispiel veranschaulicht. Wenn Sie nicht sicher sind, wie dieser Befehl funktioniert, geben Sie **man snmpwalk** an der UNIX-Eingabeaufforderung ein, um weitere Informationen zu erhalten. Die IOS-Version spielt eine wichtige Rolle, wenn Sie die MIB-OIDs für die Baseline auswählen, da die MIB-Objekte vom IOS abhängig sind. Beachten Sie auch, dass Sie, indem Sie den Routertyp kennen, später bestimmen können, welche Grenzwerte für CPU, Puffer usw. gelten sollen.

```
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
```

Schritt 2: Überprüfen der Unterstützung von SNMP MIB auf dem Router

Nachdem Sie ein Inventar des Geräts erstellt haben, das Sie für Ihre Baseline abfragen möchten, können Sie mit der Auswahl der spezifischen OIDs beginnen, die Sie abfragen möchten. Es spart eine Menge Frustration, wenn Sie im Voraus überprüfen, dass die gewünschten Daten tatsächlich vorhanden sind. Das Objekt cpmCPUTotal5min MIB befindet sich in der CISCO-PROCESS-MIB.

Um die OID zu finden, die Sie abfragen möchten, benötigen Sie eine Umwandlungstabelle, die auf der CCO-Website von Cisco zur Verfügung steht. Um über einen Webbrowser auf diese Website zuzugreifen, rufen Sie die Cisco MIB-Seite auf, und klicken Sie auf den Link zu den OIDs.

Um über einen FTP-Server auf diese Website zuzugreifen, geben Sie **ftp://ftp.cisco.com/pub/mibs/oid/ ein**. Von dieser Website können Sie die spezifische MIB herunterladen, die entschlüsselt und nach OID-Nummern sortiert wurde.

Das folgende Beispiel ist aus der Tabelle CISCO-PROCESS-MIB.oid extrahiert. Dieses Beispiel zeigt, dass die OID für die **cpmCPUTotal5min** MIB .1.3.6.1.4.1.9.9.109.1.1.1.1.5 ist.

Hinweis: Vergessen Sie nicht, ein "." zu Beginn der OID hinzuzufügen, oder Sie erhalten einen Fehler, wenn Sie versuchen, es abzufragen. Sie müssen außerdem eine ".1" zum Ende der OID hinzufügen, um sie zu instanziieren. Dies teilt dem Gerät die gesuchte OID-Instanz mit. In einigen Fällen enthalten OIDs mehr als eine Instanz eines bestimmten Datentyps, z. B. wenn ein Router mehrere CPUs hat.

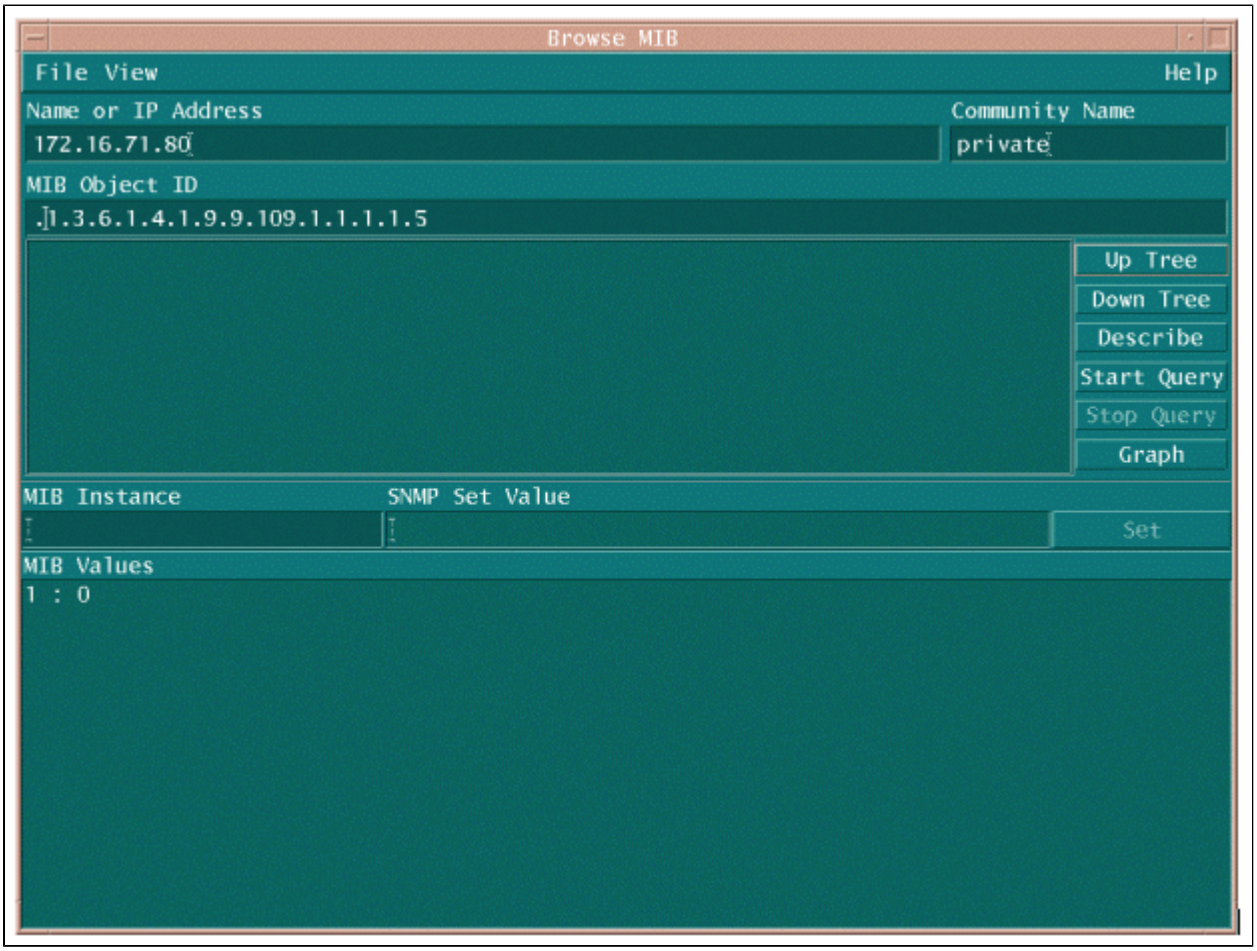
<#root>

```
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"
```

Es gibt zwei gebräuchliche Möglichkeiten, die MIB-OID abzufragen, um sicherzustellen, dass sie verfügbar ist und funktioniert. Es ist eine gute Idee, dies zu tun, bevor Sie die Sammeldatensammlung beginnen, sodass Sie keine Zeit verschwenden, etwas abzufragen, das nicht da ist, und am Ende mit einer leeren Datenbank. Eine Möglichkeit besteht darin, einen MIB-Walker von Ihrer NMS-Plattform aus zu verwenden, z. B. HP OpenView Network Node Manager (NNM) oder CiscoWorks Windows, und die zu überprüfende OID einzugeben.

Nachfolgend finden Sie ein Beispiel für HP OpenView SNMP MIB Walker.



Eine weitere einfache Möglichkeit zum Abrufen der MIB-OID ist die Verwendung des UNIX-Befehls **snmpwalk**, wie im folgenden Beispiel gezeigt.

```
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
```

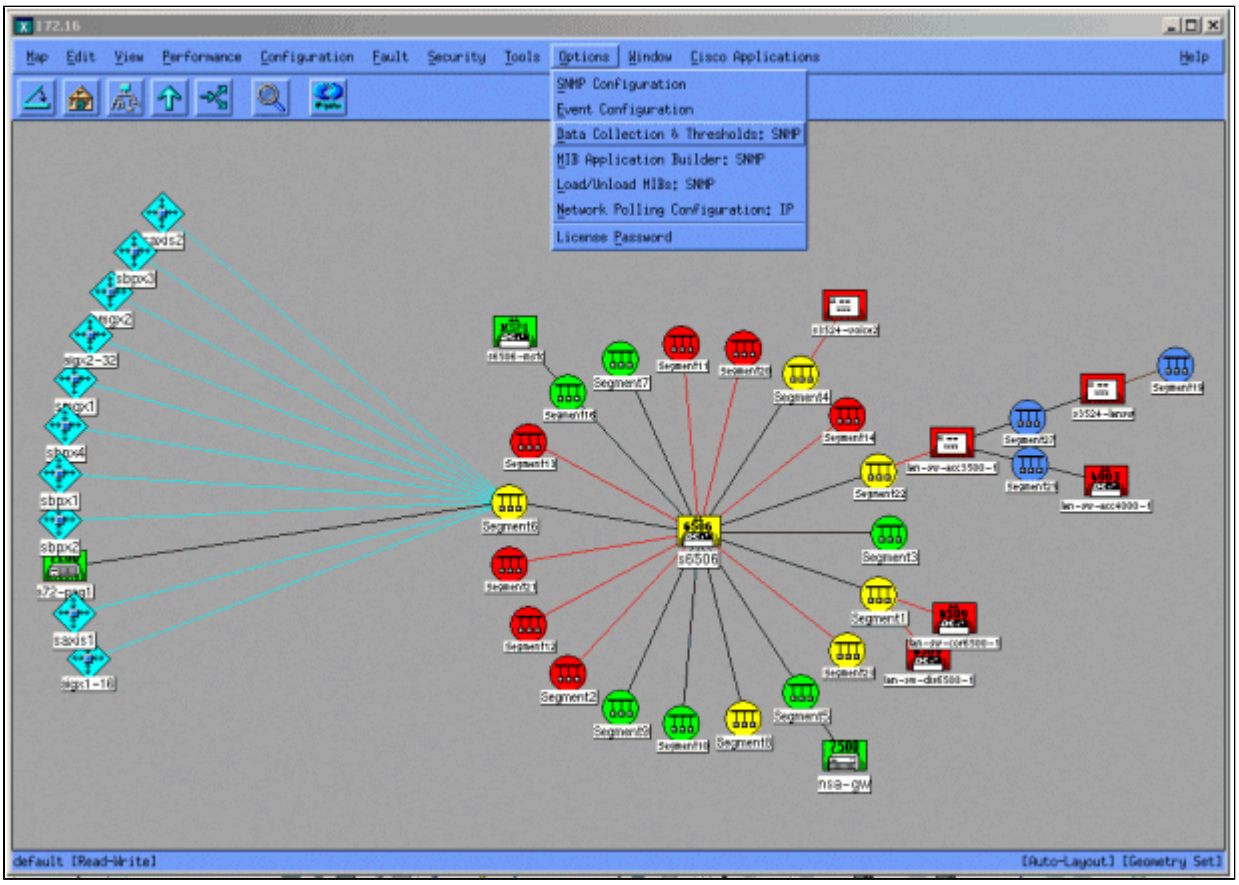
In beiden Beispielen gab die MIB den Wert 0 zurück, d. h., die CPU nutzte für diesen Abfragezyklus durchschnittlich 0 %. Wenn Sie Schwierigkeiten haben, das Gerät mit den richtigen Daten zu beantworten, senden Sie einen Ping-Befehl an das Gerät, und greifen Sie über Telnet auf das Gerät zu. Wenn weiterhin ein Problem besteht, überprüfen Sie die SNMP-Konfiguration und die SNMP Community Strings. Möglicherweise benötigen Sie eine alternative MIB oder eine andere Version von IOS, damit dies funktioniert.

Schritt 3: Abfragen und Aufzeichnen eines bestimmten SNMP MIB-Objekts vom Router

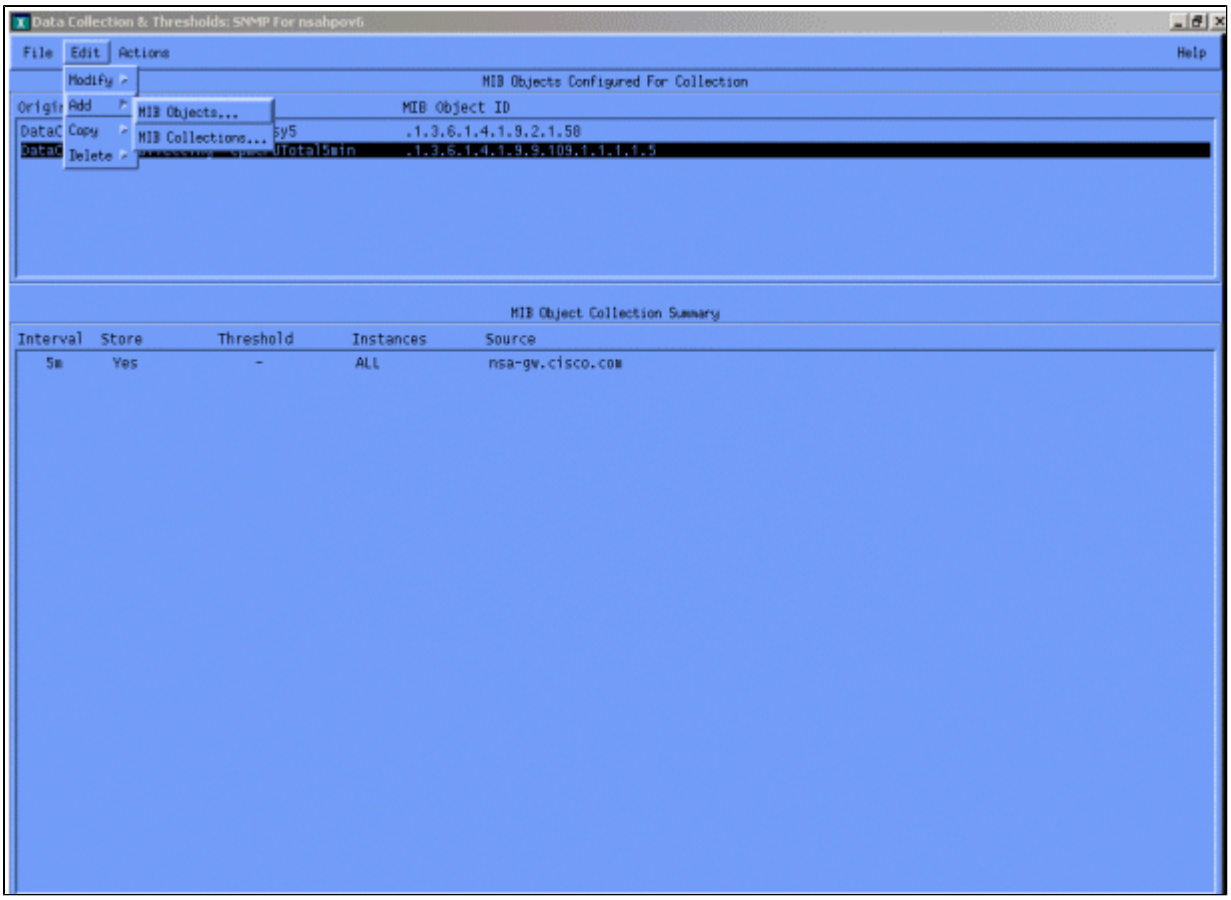
Es gibt mehrere Möglichkeiten, MIB-Objekte abzufragen und die Ausgabe aufzuzeichnen. Produkte von der Stange, Shareware-Produkte, Skripte und Anbieter-Tools sind erhältlich. Alle Front-End-Tools verwenden den SNMP-Abrufprozess, um die Informationen abzurufen. Die wichtigsten Unterschiede bestehen in der Flexibilität der Konfiguration und in der Art und Weise, wie die Daten in einer Datenbank erfasst werden. Sehen Sie sich erneut die Prozessor-MIB an, um zu sehen, wie diese verschiedenen Methoden funktionieren.

Nachdem Sie nun wissen, dass die OID vom Router unterstützt wird, müssen Sie entscheiden, wie oft Sie sie abfragen und aufzeichnen. Cisco empfiehlt, das Polling der CPU-MIB in Intervallen von fünf Minuten durchzuführen. Ein niedrigeres Intervall würde die Netzwerkauslastung oder die Geräteauslastung erhöhen. Da der MIB-Wert ohnehin ein Fünf-Minuten-Durchschnitt ist, wäre es nicht sinnvoll, ihn öfter abzufragen als den Durchschnittswert. Es wird außerdem generell empfohlen, dass die Baseline-Abfrage mindestens zwei Wochen dauert, damit Sie mindestens zwei Wochen im Netzwerk analysieren können.

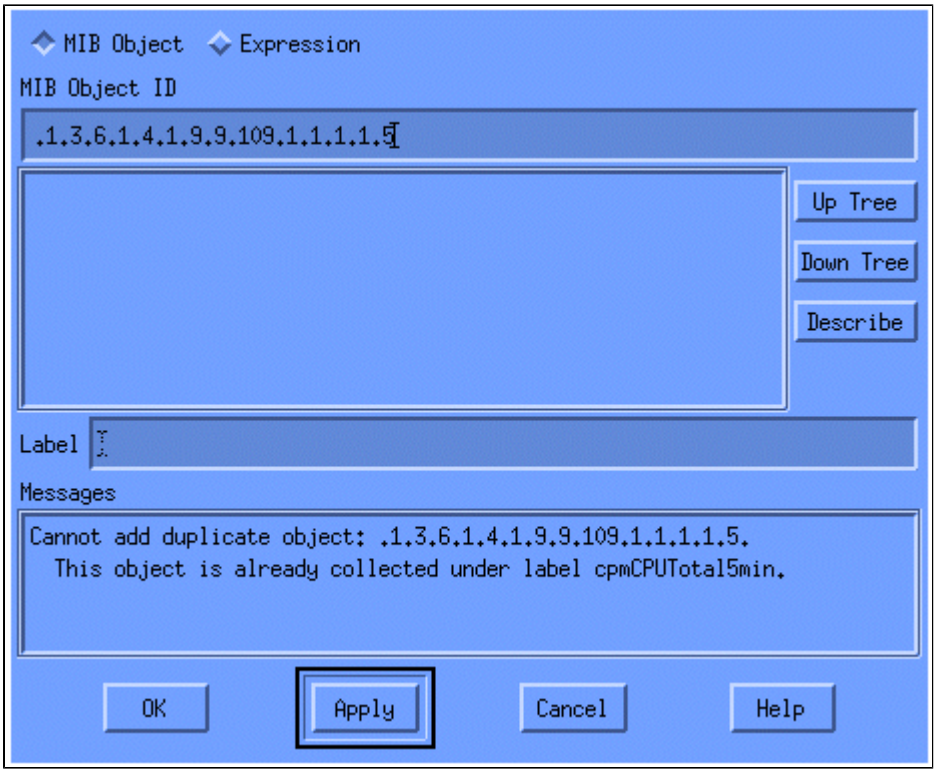
Die folgenden Bildschirme zeigen, wie Sie MIB-Objekte mit HP OpenView Network Node Manager Version 6.1 hinzufügen. Wählen Sie im Hauptbildschirm **Options > Data Collection & Thresholds aus**.



Wählen Sie anschließend **Bearbeiten > Hinzufügen > MIB-Objekte aus**.

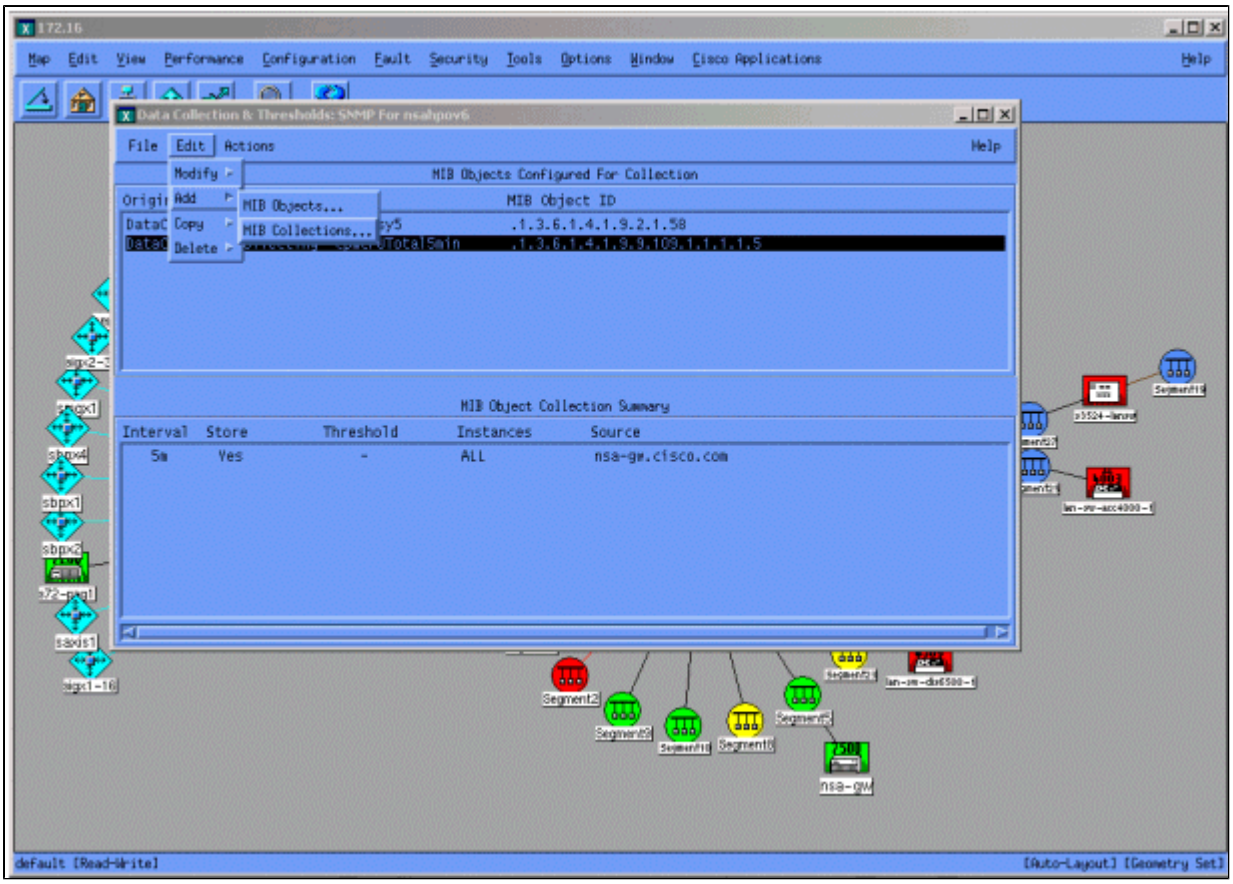


Fügen Sie im Menü die OID-Zeichenfolge hinzu, und klicken Sie auf **Apply**. Sie haben nun das MIB-Objekt in die HP OpenView-Plattform eingegeben, sodass es abgefragt werden kann.



Geben Sie als Nächstes HP OpenView bekannt, welcher Router für diese OID abgefragt werden soll.

Wählen Sie im Menü Datenerfassung die Optionen **Bearbeiten > Hinzufügen > MIB-Auflistungen aus**.

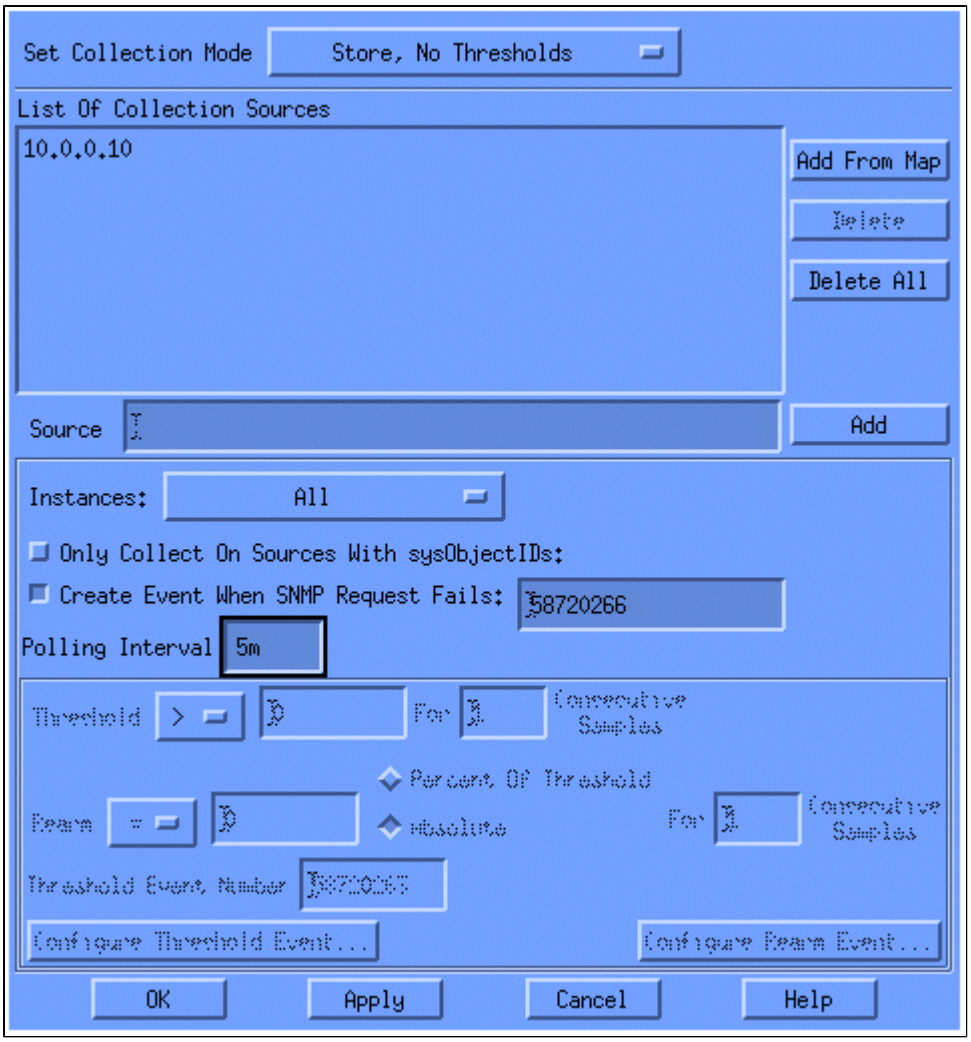


Geben Sie im Feld "Source" (Quelle) den DNS-Namen oder die IP-Adresse des abzufragenden Routers ein.

Wählen Sie **Speichern, Keine Schwellenwerte** aus der Liste Erfassungsmodus festlegen aus.

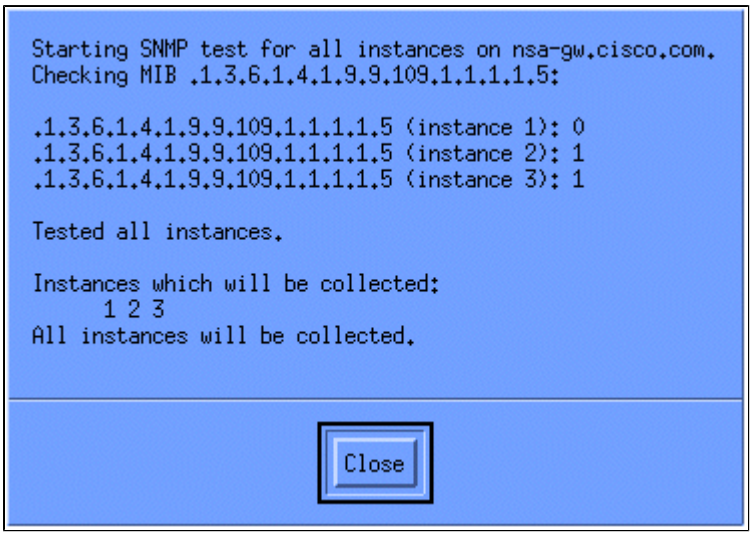
Legen Sie das Abfrageintervall für fünf Minuten auf **5 m fest**.

Klicken Sie auf **Apply** (Anwenden).



Sie müssen **Datei > Speichern** auswählen, damit die Änderungen übernommen werden.

Um sicherzustellen, dass die Sammlung ordnungsgemäß eingerichtet ist, markieren Sie die Übersichtszeile für den Router, und wählen Sie **Aktionen > SNMP testen aus**. Dadurch wird überprüft, ob der Community-String korrekt ist, und es wird eine Abfrage für alle Instanzen der OID durchgeführt.



Klicken Sie auf **Schließen**, und lassen Sie die Auflistung eine Woche lang laufen. Extrahieren Sie am Ende des Wochenzeitraums die Daten zur Analyse.

Die Daten lassen sich einfacher analysieren, wenn Sie sie in eine ASCII-Datei kopieren und in ein Tabellenkalkulationstool wie Microsoft Excel importieren. Um dies mit HP OpenView NNM zu tun, können Sie das Befehlszeilentool **snmpColDump** verwenden. Jede konfigurierte Sammlung schreibt in eine Datei im Verzeichnis /var/opt/OV/share/database/snmpCollect/.

Extrahieren Sie die Daten in eine ASCII-Datei namens **testfile** mit dem folgenden Befehl:

<#root>

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

testfile

Hinweis: cpmCPUTotal5min.1 ist die Datenbankdatei, die HP OpenView NNM erstellt hat, als das OID-Polling begann.

Die generierte Testdatei sieht ähnlich aus wie im folgenden Beispiel.

```
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€¦
```

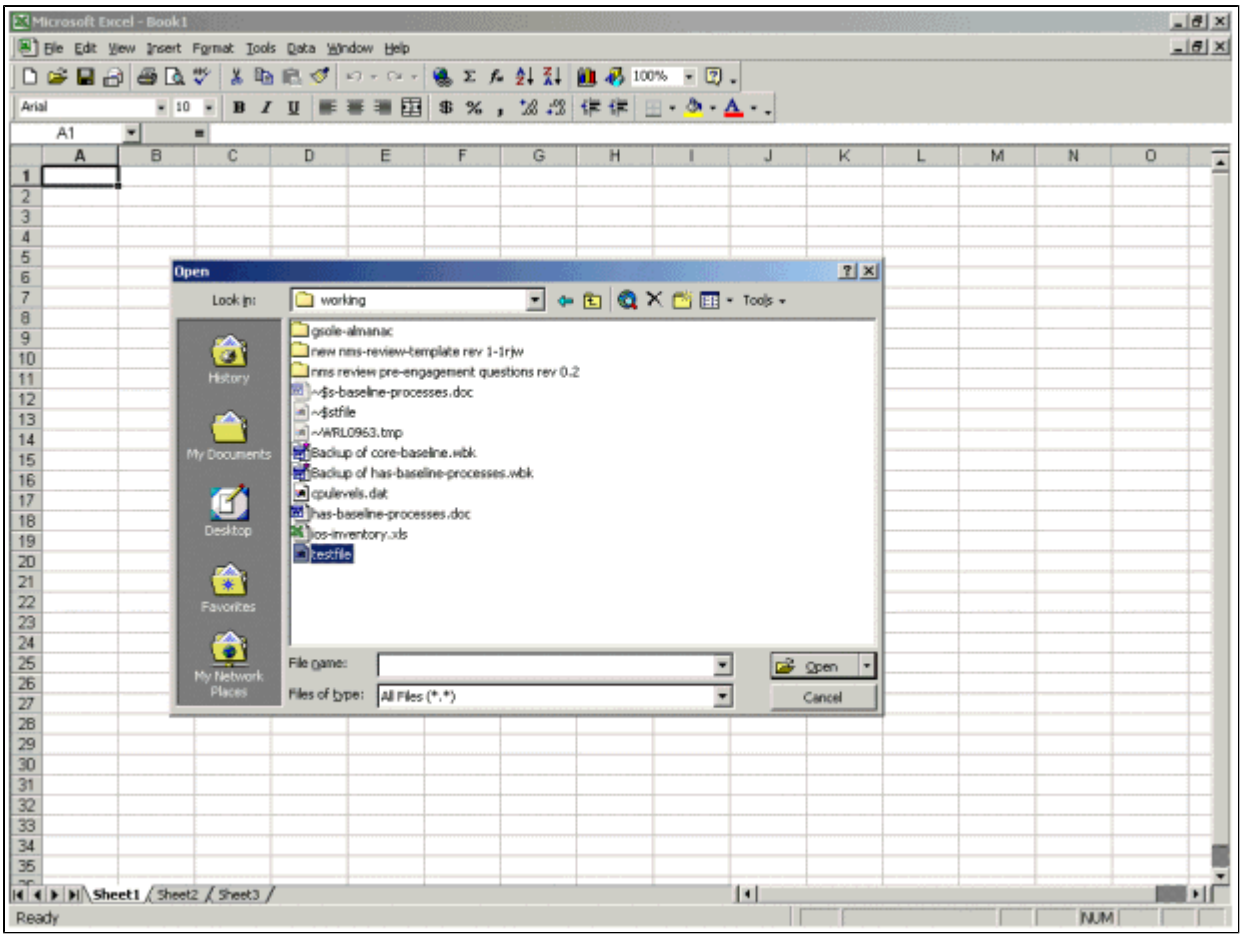
Sobald sich die Testdateiausgabe auf Ihrer UNIX-Station befindet, können Sie sie mithilfe von File Transfer Protocol (FTP) auf Ihren PC übertragen.

Sie können die Daten auch mit eigenen Skripten sammeln. Führen Sie dazu alle fünf Minuten ein **snmpget** für die CPU-OID aus, und legen Sie die Ergebnisse in eine CSV-Datei ab.

Schritt 4: Analysieren von Daten zur Bestimmung von Grenzwerten

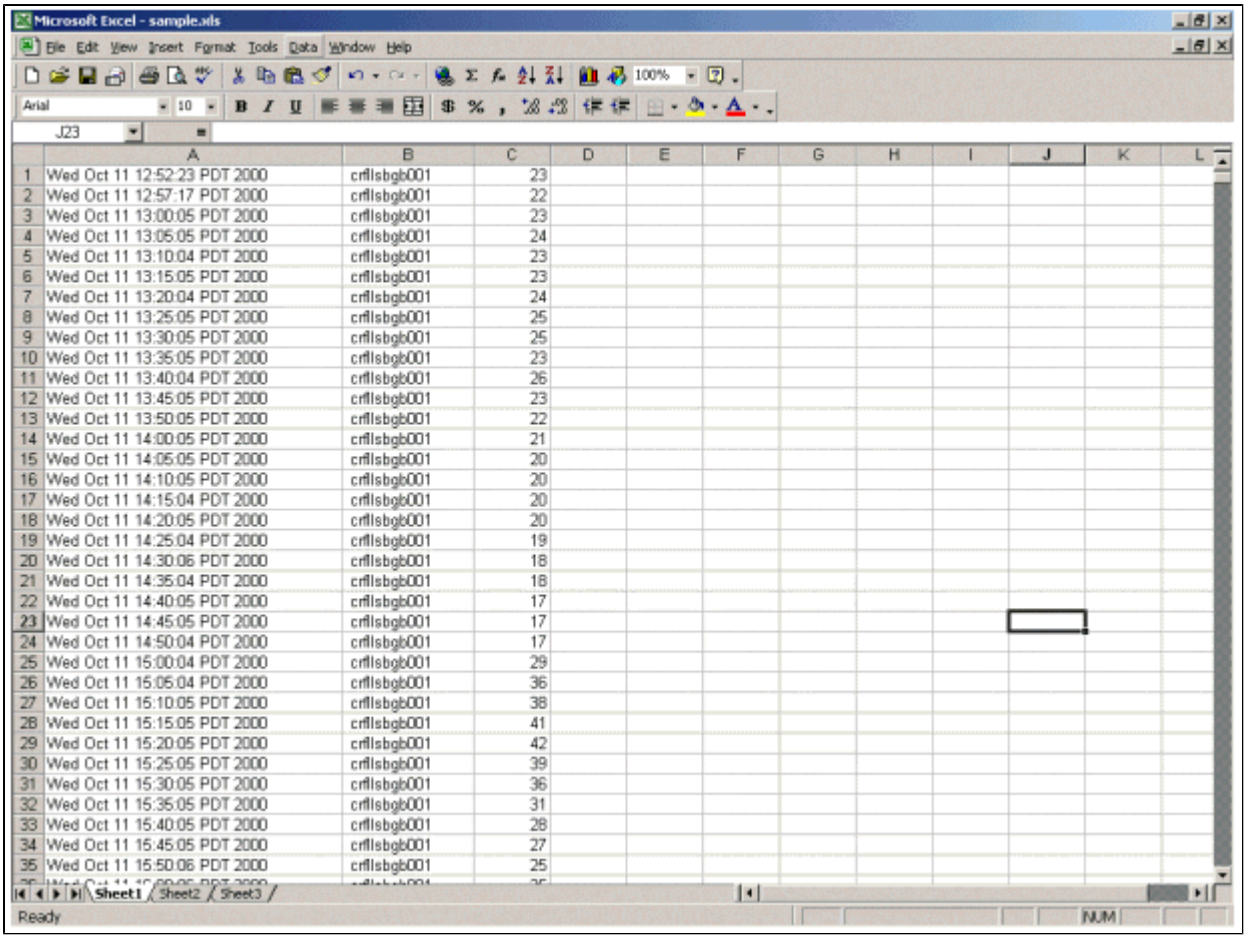
Jetzt, da Sie einige Daten haben, können Sie damit beginnen, sie zu analysieren. Diese Phase der Baseline legt die Schwellenwerteinstellungen fest, die Sie verwenden können, um die Leistung oder den Fehler genau zu messen. Wenn Sie die Schwellenwertüberwachung aktivieren, werden nicht zu viele Alarme ausgelöst. Eine der einfachsten Möglichkeiten, dies zu tun, ist das Importieren der Daten in ein Tabellenkalkulationsprogramm wie Microsoft Excel und das Zeichnen eines Scatter-Diagramms. Diese Methode macht sehr einfach erkennbar, wie oft ein bestimmtes Gerät eine Ausnahmewarnung erstellt hätte, wenn Sie es auf einen bestimmten Schwellenwert überwachen. Es ist nicht ratsam, Schwellenwerte zu aktivieren, ohne eine Baseline zu erstellen, da dies zu Warnstürmen bei Geräten führen kann, die den von Ihnen gewählten Schwellenwert überschritten haben.

Um die Testdatei in eine Excel-Tabelle zu importieren, öffnen Sie Excel, wählen Sie **Datei > Öffnen aus,** und wählen Sie Ihre Datendatei aus.



Die Excel-Anwendung fordert Sie dann zum Importieren der Datei auf.

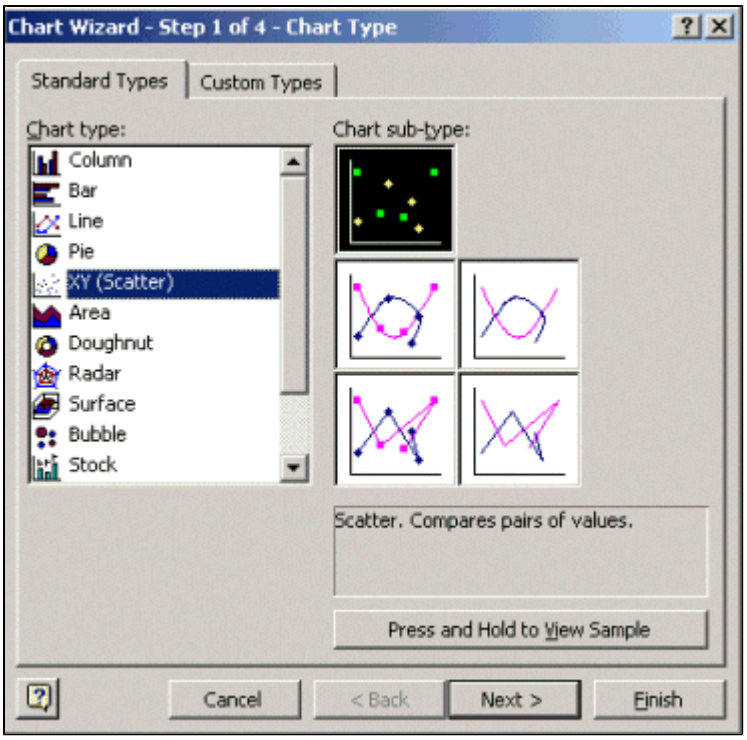
Wenn Sie fertig sind, sollte die importierte Datei ähnlich wie der folgende Bildschirm aussehen.



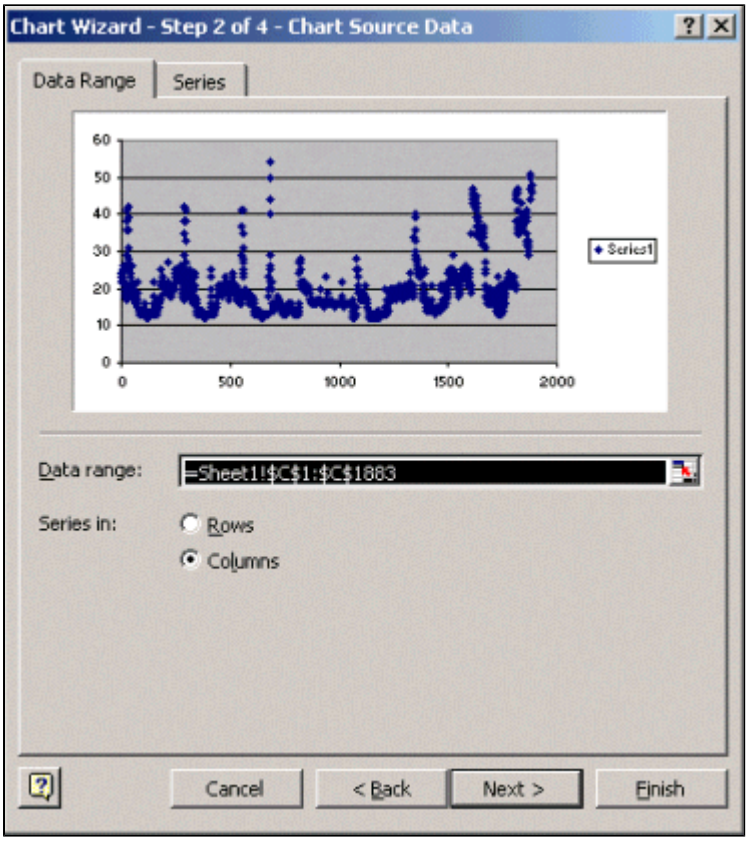
Mithilfe eines Streudiagramms können Sie leichter visualisieren, wie verschiedene Schwellenwerteinstellungen im Netzwerk funktionieren würden.

Um das Scatter-Diagramm zu erstellen, markieren Sie die Spalte C in der importierten Datei, und klicken Sie dann auf das Symbol **Diagramm-Assistent**. Folgen Sie dann den Schritten durch den Diagramm-Assistenten, um ein Scatter-Diagramm zu erstellen.

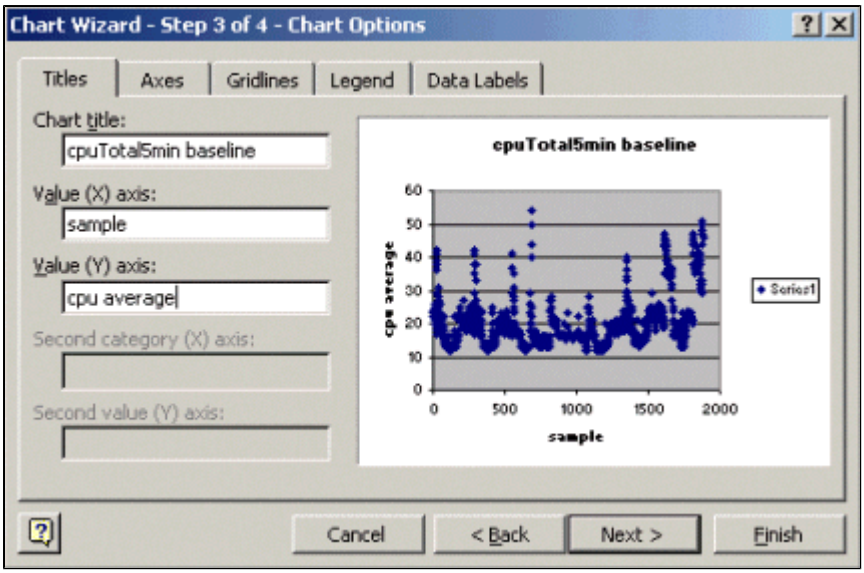
Wählen Sie im Diagramm-Assistenten in Schritt 1, wie unten dargestellt, die Registerkarte **Standardtypen** und dann den **XY-**Diagrammtyp (**Streuung**) aus. Klicken Sie dann auf **Weiter**.



Wählen Sie im Diagramm-Assistenten in Schritt 2, wie unten dargestellt, die Registerkarte **Datenbereich aus,** und wählen Sie den Datenbereich und die Option **Spalten** aus. Klicken Sie auf **Next** (Weiter).



Geben Sie in Diagramm-Assistent Schritt 3, wie unten gezeigt, den Diagrammtitel und die X- und Y-Achsenwerte ein, und klicken Sie dann auf **Weiter**.



Wählen Sie im Diagramm-Assistenten in Schritt 4 aus, ob das Streudiagramm auf einer neuen Seite oder als Objekt auf der vorhandenen Seite angezeigt werden soll.

Klicken Sie auf **Fertig stellen**, um das Diagramm an der gewünschten Position zu platzieren.

"Was wäre wenn?" Analyse

Sie können jetzt das Scatter-Diagramm für die Analyse verwenden. Bevor Sie jedoch fortfahren können, müssen Sie folgende Fragen stellen:

- Was empfiehlt der Anbieter (in diesem Beispiel ist der Anbieter Cisco) als Schwellenwert für diese MIB-Variable?

  Im Allgemeinen empfiehlt Cisco, dass die durchschnittliche CPU-Auslastung eines Core-Routers 60 % nicht überschreitet. 60 % wurden ausgewählt, weil ein Router einen gewissen Overhead benötigt, falls Probleme auftreten oder das Netzwerk ausfällt. Cisco schätzt, dass ein Core-Router ca. 40 Prozent CPU-Overhead benötigt, falls ein Routing-Protokoll neu berechnet oder neu konvergiert werden muss. Diese Prozentsätze variieren je nach den von Ihnen verwendeten Protokollen sowie der Topologie und Stabilität Ihres Netzwerks.

- Was wäre, wenn ich 60 Prozent als Schwellenwerteinstellung verwende?

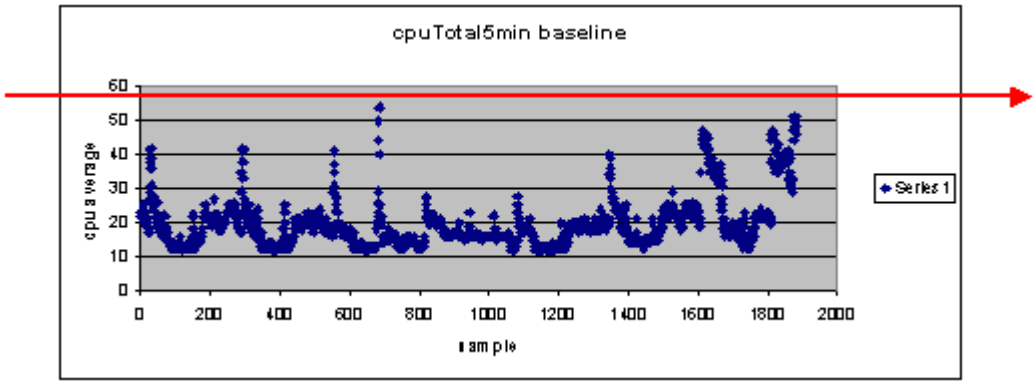
  Wenn Sie eine Linie über das Scatter-Diagramm horizontal bei 60 zeichnen, werden Sie sehen, dass keiner der Datenpunkte 60 Prozent CPU-Auslastung überschreitet. Ein Schwellenwert von 60 in den Stationen Ihres Netzwerkmanagementsystems (NMS) wurde also nicht für einen Schwellenwert-Alarm während des Abfragezeitraums festgelegt. Für diesen Router ist ein Prozentsatz von 60 zulässig. Beachten Sie jedoch, dass einige Datenpunkte in der Nähe von 60 liegen. Es wäre schön zu wissen, wenn sich ein Router dem Schwellenwert von 60 % nähert, damit Sie frühzeitig wissen können, dass die CPU sich 60 % nähert, und einen Plan haben, was zu tun ist, wenn er diesen Punkt erreicht.

- Was wäre, wenn ich den Schwellenwert auf 50 Prozent festlege?

  Schätzungen zufolge erreichte dieser Router in diesem Abfragezyklus die Auslastung von 50 % viermal und hätte jedes Mal einen Schwellenwert-Alarm ausgelöst. Dieser Prozess wird umso wichtiger, wenn Sie sich *Routergruppen* ansehen, um festzustellen, wie die verschiedenen Schwellenwerteinstellungen aussehen würden. Beispiel: "Was wäre, wenn ich den Schwellenwert für das gesamte Kernnetzwerk auf 50 Prozent festlege?" Sehen Sie, es ist sehr schwierig, nur eine

Nummer zu wählen.

Analyse des CPU-Schwellenwerts "Was wäre wenn"



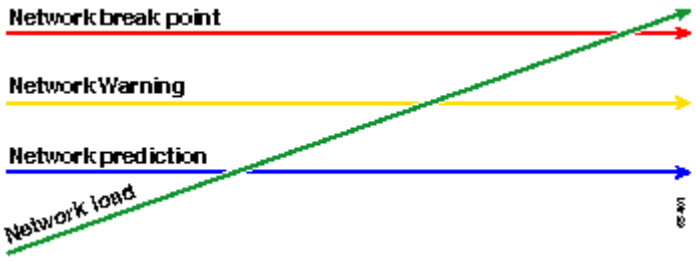
Eine Strategie, die Ihnen dies erleichtern soll, ist die Ready, Set, Go-Schwellenwertmethode. Bei dieser Methode werden drei Schwellenwerte nacheinander verwendet.

- Bereit - der Schwellenwert, den Sie als Vorhersage dafür festlegen, welche Geräte in Zukunft wahrscheinlich Ihre Aufmerksamkeit benötigen
- Festlegen: Dieser Schwellenwert dient als Frühwarnsystem, das Sie darüber informiert, mit der Planung einer Reparatur, Neukonfiguration oder eines Upgrades zu beginnen.
- Los: Der Schwellenwert, von dem Sie und/oder der Anbieter glauben, dass er ein Fehler ist, für den eine Maßnahme zur Reparatur erforderlich ist. In diesem Beispiel liegt er bei 60 Prozent.

Die nachfolgende Tabelle zeigt die Strategie der Ready, Set, Go-Strategie.

Grenzwert	Aktion	Ergebnis
45 Prozent	Weitere Untersuchungen	Liste der Optionen für Aktionspläne
50 %	Aktionsplan formulieren	Liste der im Aktionsplan vorgesehenen Maßnahmen
60 %	Aktionsplan implementieren	Der Router überschreitet die Schwellenwerte nicht mehr. Zurück zum Bereitschaftsmodus

Die Ready, Set, Go-Methodik ändert das zuvor besprochene ursprüngliche Baseline-Diagramm. Das folgende Diagramm zeigt das geänderte Baseline-Diagramm. Wenn Sie die anderen Schnittpunkte im Diagramm identifizieren können, haben Sie jetzt mehr Zeit für Planung und Reaktion als zuvor.



Beachten Sie, dass bei diesem Prozess die Aufmerksamkeit auf die Ausnahmen im Netzwerk und nicht auf andere Geräte gerichtet ist. Es wird davon ausgegangen, dass Geräte in Ordnung sind, solange sie unterhalb der Schwellenwerte liegen.

Wenn Sie diese Schritte von Anfang an durchdacht haben, sind Sie gut darauf vorbereitet, den Zustand des Netzwerks aufrechtzuerhalten. Die Durchführung einer solchen Planung ist auch für die Budgetplanung äußerst hilfreich. Wenn Sie wissen, welche Router am häufigsten **eingesetzt** werden, welche Router am mittleren **Ende** und welche am unteren Ende **einsatzbereit** sind, können Sie leicht planen, wie viel Budget Sie für Upgrades benötigen, je nachdem, um welche Art von Routern es sich handelt und welche Aktionsplanoptionen Sie benötigen. Dieselbe Strategie kann für WAN-Verbindungen (Wide Area Network) oder andere MIB-OIDs verwendet werden.

Schritt 5: Beheben identifizierter unmittelbarer Probleme

Dies ist einer der einfacheren Teile des Ausgangsprozesses. Sobald Sie festgestellt haben, welche Geräte die **Go-**Schwelle überschreiten, sollten Sie einen Aktionsplan erstellen, um diese Geräte wieder unter die Schwelle zu bringen.

Sie können ein Ticket beim Cisco Technical Assistance Center (TAC) erstellen oder sich bezüglich der verfügbaren Optionen an Ihren Systemtechniker wenden. Du solltest nicht davon ausgehen, dass es dich Geld kosten wird, wenn du die Dinge wieder unter die Schwelle bringst. Einige CPU-Probleme können durch eine Änderung der Konfiguration behoben werden, um sicherzustellen, dass alle Prozesse auf die effizienteste Weise ausgeführt werden. Beispielsweise können einige Zugriffskontrolllisten (ACLs) eine sehr hohe Router-CPU verursachen, da die Pakete den Router durchlaufen. In einigen Fällen können Sie NetFlow-Switching implementieren, um den Paketvermittlungspfad zu ändern und die Auswirkungen der ACL auf die CPU zu reduzieren. Unabhängig von den Problemen ist es in diesem Schritt erforderlich, alle Router wieder unter den Schwellenwert zu bringen, damit Sie die Schwellenwerte später implementieren können, ohne dass das Risiko besteht, dass die NMS-Stationen mit zu vielen Schwellenwertalarmen überflutet werden.

Schritt 6: Überwachen des Testschwellenwerts

In diesem Schritt werden die Grenzwerte in der Übung mit den Tools getestet, die Sie im Produktionsnetzwerk verwenden werden. Für die Überwachung der Schwellenwerte gibt es zwei gemeinsame Ansätze. Sie müssen entscheiden, welche Methode für Ihr Netzwerk am besten geeignet ist.

- Abfrage- und Vergleichsmethode unter Verwendung einer SNMP-Plattform oder eines anderen SNMP-Überwachungstools

  Diese Methode nutzt mehr Netzwerkbandbreite für das Polling des Datenverkehrs und nimmt Verarbeitungszyklen auf der SNMP-Plattform in Anspruch.

- Verwenden Sie Remote Monitoring (RMON)-Alarm- und Ereigniskonfigurationen in den Routern, damit diese nur dann eine Warnung senden, wenn ein bestimmter Grenzwert überschritten wird.

  Diese Methode verringert die Bandbreitennutzung im Netzwerk, erhöht aber auch die Arbeitsspeicher- und CPU-Auslastung auf den Routern.

Implementieren eines Schwellenwerts mithilfe von SNMP

Um die SNMP-Methode mit HP OpenView NNM einzurichten, wählen Sie **Options > Data Collection & Thresholds (Optionen > Datensammlung und Schwellenwerte)** aus, wie Sie dies beim Einrichten der ersten Abfrage getan haben. Wählen Sie dieses Mal im Menü "**Sammlungen"** jedoch die Option "Speichern", "**Schwellenwerte überprüfen**" statt "Speichern" und "Keine Schwellenwerte". Nachdem Sie

den Schwellenwert festgelegt haben, können Sie die CPU-Auslastung auf dem Router erhöhen, indem Sie ihm mehrere Pings und/oder mehrere SNMP-Schritte senden. Sie müssen möglicherweise den Schwellenwert senken, wenn Sie die CPU nicht so hoch drücken können, dass der Schwellenwert überschritten wird. In jedem Fall sollten Sie sicherstellen, dass der Schwellenwertmechanismus funktioniert.

Eine der Einschränkungen bei der Verwendung dieser Methode besteht darin, dass Sie nicht mehrere Schwellenwerte gleichzeitig implementieren können. Sie benötigen drei SNMP-Plattformen, um drei verschiedene Schwellenwerte gleichzeitig festzulegen. Tools wie Concord Network Health und Trinagy TREND ermöglichen mehrere Schwellenwerte für dieselbe OID-Instanz.

Wenn Ihr System immer nur einen Schwellenwert bewältigen kann, können Sie die Strategie "Bereit, Festlegen, Los" als serielle Methode in Betracht ziehen. Das heißt, wenn die **Bereitschaftsschwelle** kontinuierlich erreicht wird, beginnen Sie Ihre Untersuchung und heben Sie die Schwelle auf die für das Gerät festgelegte Stufe. Wenn der **festgelegte** Pegel kontinuierlich erreicht wird, beginnen Sie, Ihren Aktionsplan zu formulieren, und erhöhen Sie den Schwellenwert auf den **Go**-Pegel für das Gerät. Dann, wenn die Go-Schwelle ständig erreicht wird, setzen Sie Ihren Aktionsplan um. Dies sollte genauso gut funktionieren wie die Drei-gleichzeitig-Schwellenwertmethode. Es dauert nur etwas länger, die SNMP-Plattform-Schwellenwerteinstellungen zu ändern.

Implementieren eines Schwellenwerts mithilfe von RMON-Alarm- und -Ereignisfunktionen

Mithilfe von RMON-Alarm- und Ereigniskonfigurationen kann der Router sich selbst auf mehrere Schwellenwerte überwachen lassen. Wenn der Router eine Bedingung erkennt, die einen Schwellenwert überschreitet, sendet er ein SNMP-Trap an die SNMP-Plattform. In der Routerkonfiguration muss ein SNMP-Trap-Empfänger eingerichtet sein, damit das Trap weitergeleitet werden kann. Es besteht eine Korrelation zwischen einem Alarm und einem Ereignis. Der Alarm überprüft die OID für den angegebenen Grenzwert. Wenn der Schwellenwert erreicht ist, löst der Alarmprozess den Ereignisprozess aus, der entweder eine SNMP-Trap-Nachricht senden, einen RMON-Protokolleintrag erstellen oder beides gleichzeitig ausführen kann. Weitere Informationen zu diesem Befehl finden Sie unter RMON Alarm and Event Configuration Commands.

Die folgenden Router-Konfigurationsbefehle zeigen den Router-Monitor cpmCPUTotal5min alle 300 Sekunden an. Es löst Ereignis 1 aus, wenn die CPU über 60 Prozent liegt, und Ereignis 2, wenn die CPU auf 40 Prozent zurückfällt. In beiden Fällen wird eine SNMP-Trap-Nachricht mit dem Community Private String an die NMS-Station gesendet.

Um die Ready, Set, Go-Methode zu verwenden, verwenden Sie alle der folgenden Konfigurationsanweisungen.

```
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
```

Das folgende Beispiel zeigt die Ausgabe des Befehls **show rmon alarm**, der mit den obigen Anweisungen konfiguriert wurde.

```
<#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
```

Im folgenden Beispiel wird die Ausgabe des Befehls **show rmon event** veranschaulicht.

```
<#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
```

Sie können beide Methoden ausprobieren, um zu sehen, welche Methode am besten zu Ihrer Umgebung passt. Sie können sogar feststellen, dass eine Kombination von Methoden gut funktioniert. In jedem Fall sollten die Tests in einer Laborumgebung durchgeführt werden, um sicherzustellen, dass alles ordnungsgemäß funktioniert. Nach den Tests im Labor ermöglicht Ihnen eine eingeschränkte Bereitstellung auf einer kleinen Gruppe von Routern, den Prozess des Sendens von Warnmeldungen an Ihr Operations Center zu testen.

In diesem Fall müssen Sie die Schwellenwerte senken, um den Prozess zu testen: Es wird nicht empfohlen, die CPU auf einem Produktions-Router künstlich anzuheben. Sie sollten außerdem sicherstellen, dass bei Eingang der Warnmeldungen in die NMS-Stationen im Operations Center eine Eskalationsrichtlinie vorhanden ist, um sicherzustellen, dass Sie informiert werden, wenn die Geräte die Schwellenwerte überschreiten. Diese Konfigurationen wurden in einer Übung mit Cisco IOS Version 12.1(7) getestet. Wenn Probleme auftreten, sollten Sie sich an Cisco Engineering- oder Systemtechniker wenden, um herauszufinden, ob in Ihrer IOS-Version ein Fehler vorliegt.

Schritt 7: Implementierung der Grenzwertüberwachung mithilfe von SNMP oder RMON

Nachdem Sie die Grenzwertüberwachung im Labor eingehend getestet und in einer begrenzten Bereitstellung durchgeführt haben, können Sie Grenzwerte im gesamten Kernnetzwerk implementieren. Für andere wichtige MIB-Variablen im Netzwerk, wie Puffer, freier Speicher, CRC-Fehler (zyklische Redundanzprüfung), AMT-Zellverlust usw., können Sie diesen Baseline-Prozess jetzt systematisch durchlaufen.

Wenn Sie RMON-Alarm- und Ereigniskonfigurationen verwenden, können Sie das Polling von Ihrer NMS-Station aus beenden. Dadurch wird der NMS-Server entlastet, und es werden weniger Polling-Daten im Netzwerk benötigt. Wenn Sie diesen Prozess für wichtige Indikatoren für den Netzwerkzustand systematisch durchlaufen, können Sie leicht den Punkt erreichen, an dem die Netzwerkgeräte sich selbst mithilfe von RMON Alarm and Event überwachen.

Zusätzliche MIBs

Nachdem Sie diesen Prozess gelernt haben, möchten Sie möglicherweise andere MIBs untersuchen, um sie als Baseline zu verwenden und zu überwachen. In den folgenden Unterabschnitten finden Sie eine kurze Liste einiger OIDs und Beschreibungen, die Sie möglicherweise nützlich finden.

Router MIBs

Die Speichereigenschaften sind sehr hilfreich, um den Zustand eines Routers zu bestimmen. Ein intakter Router sollte fast immer über verfügbaren Pufferspeicher verfügen, mit dem er arbeiten kann. Wenn dem Router der Pufferspeicher ausgeht, muss die CPU mehr arbeiten, um neue Puffer zu erstellen und Puffer für eingehende und ausgehende Pakete zu finden. Eine ausführliche Erläuterung der Puffer würde den Rahmen dieses Dokuments sprengen. Generell sollte ein intakter Router jedoch nur sehr wenige Pufferausfälle

aufweisen und keine Pufferausfälle oder einen Zustand ohne freien Speicher aufweisen.

Objekt	Beschreibung	OID
ciscoSpeicherPoolFrei	Die Anzahl der Bytes aus dem Speicherpool, die auf dem verwalteten Gerät derzeit nicht verwendet werden.	1.3.6.1.4.1.9.9.48.1.1.1.6
ciscoSpeicherPoolGrößterFrei	Die größte Anzahl zusammenhängender Bytes aus dem Speicherpool, die derzeit nicht verwendet werden.	1.3.6.1.4.1.9.9.48.1.1.1.7
PufferElVerpasst	Die Anzahl von Pufferelementfehlern	1.3.6.1.4.1.9.2.1.12
BufferFail	Die Anzahl der Fehler bei der Pufferzuweisung	1.3.6.1.4.1.9.2.1.46
PufferNeinMem	Die Anzahl der Puffererstellungsfehler, die aufgrund eines fehlenden freien Speichers auftreten	1.3.6.1.4.1.9.2.1.47

Catalyst Switch-MIBs

Objekt	Beschreibung	OID
cpmCPUTotal5min	Der prozentuale Gesamtanteil der CPU-Auslastung in den letzten fünf Minuten. Dieses Objekt veraltet das Objekt avgBusy5 aus der ALTEN CISCO-SYSTEM-MIB.	1.3.6.1.4.1.9.9.109.1.1.1.5
cpmCPUTotal5sec	Der prozentuale Gesamtanteil der CPU-Auslastung in den letzten fünf Sekunden. Dieses Objekt überholt das Objekt "busyPer" aus der OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.3
sysDatenverkehr	Der Prozentsatz der Bandbreitennutzung für das vorherige Abfrageintervall	1.3.6.1.4.1.9.5.1.1.8

sysVerkehrsspitze	Der Spitzenwert des Datenverkehrsmessers seit dem letzten Löschen der Port-Zähler oder Start des Systems	1.3.6.1.4.1.9.5.1.1.19
sysVerkehrsspitzenzeit	Die Zeit (in Hundertstelsekunden) seit dem Auftreten des maximalen Datenverkehrsmesswerts	1.3.6.1.4.1.9.5.1.1.20
portTopNBenutzung	Auslastung des Ports im System	1.3.6.1.4.1.9.5.1.20.2.1.4
PortTopNBufferOverFlow	Die Anzahl der Pufferüberläufe des Ports im System	1.3.6.1.4.1.9.5.1.20.2.1.10

Serielle Link-MIBs

Objekt	Beschreibung	OID
locIfInputQueueDrops	Die Anzahl der wegen einer vollen Eingabewarteschlange blockierten Pakete	1.3.6.1.4.1.9.2.2.1.1.26
locIfOutputQueueDrops	Die Anzahl der wegen einer vollen Ausgabewarteschlange verworfenen Pakete	1.3.6.1.4.1.9.2.2.1.1.27
LokalWennInCRC	Die Anzahl der Eingangspakete mit zyklischen Redundanz-Prüfsummenfehlern.	1.3.6.1.4.1.9.2.2.1.1.12

RMON Alarm- und Ereigniskonfigurationsbefehle

Alarme

RMON-Alarme können mit der folgenden Syntax konfiguriert werden:

<#root>

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

Element	Beschreibung
Zahl	Die Alarmnummer, die mit dem alarmIndex in der alarmTable in der RMON-MIB

	identisch ist.
variabel	Das zu überwachende MIB-Objekt, das in die alarmVariable übersetzt wird, die in der alarmTable der RMON-MIB verwendet wird.
Intervall	Die Zeit (in Sekunden), die der Alarm die MIB-Variable überwacht, die mit dem in der alarmTable der RMON-MIB verwendeten alarmInterval identisch ist.
Delta	Prüft die Änderung zwischen MIB-Variablen, die sich auf alarmSampleType in der alarmTable der RMON-MIB auswirkt.
absolut	Testet jede MIB-Variable direkt, was den alarmSampleType in der alarmTable der RMON MIB beeinflusst.
ansteigender Schwellenwert	Der Wert, bei dem der Alarm ausgelöst wird.
Ereignisnummer	(Optional) Die Ereignisnummer, die ausgelöst wird, wenn der steigende oder fallende Schwellenwert den Grenzwert überschreitet. Dieser Wert ist identisch mit alarmRisingEventIndex oder alarmFallingEventIndex in der alarmTable der RMON MIB.
fallender Schwellenwert	Der Wert, bei dem der Alarm zurückgesetzt wird.
Besitzerstring	(Optional) Gibt einen Besitzer für den Alarm an, der identisch mit alarmOwner in der alarmTable der RMON MIB ist.

Events

RMON-Ereignisse können mit der folgenden Syntax konfiguriert werden:

<#root>

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

Element	Beschreibung
Zahl	Zugewiesene Ereignisnummer, die mit dem eventIndex in der eventTable in der RMON-MIB identisch ist.
Logbuch	(Optional) Generiert einen RMON-Protokolleintrag, wenn das Ereignis ausgelöst wird, und legt eventType in der RMON MIB auf log oder log-and-trap fest.
Trap	(Optional) Für dieses Trap verwendeter SNMP

Community	Community String. Konfiguriert die Einstellung von eventType in der RMON-MIB für diese Zeile entweder als snmp-trap oder als log-and-trap. Dieser Wert ist identisch mit eventCommunityValue in eventTable in der RMON-MIB.
Zeichenkette	(Optional) Gibt eine Beschreibung des Ereignisses an, die mit der Ereignisbeschreibung in der eventTable der RMON-MIB identisch ist.
Besitzerstring	(Optional) Besitzer dieses Ereignisses, das mit eventOwner in der eventTable der RMON MIB identisch ist.

RMON-Alarm- und Ereignisimplementierung

Detaillierte Informationen zu RMON-Warnmeldungen und -Ereignisimplementierungen finden Sie im Abschnitt RMON-Warnmeldungen und -Ereignisimplementierung des Whitepapers *Best Practices für Netzwerkmanagementsysteme*.

Zugehörige Informationen

- **Technischer Support und Dokumentation - Cisco Systems**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.