
A|C|M|P
efficient networks

Dieses Whitepaper erklärt SNMP, wie man SNMP mit ACMP nutzen kann und welche Erweiterungsmöglichkeiten ACMP für das Arbeiten mit SNMP bietet. Zunächst gibt es eine Einführung in SNMP. Anschließend wird erläutert, wie ACMP standardmäßig SNMP-Daten inventarisiert. Im Anschluss daran folgt eine Beschreibung, wie ACMP für weitere SNMP-Daten modifiziert werden kann. Für einen schnelleren Einstieg in SNMP werden zum Schluss einige SNMP-Felder vorgestellt.

1. SNMP

Die Abkürzung SNMP steht für *Simple Network Management Protocol* und wurde von der IETF entwickelt. Die Hauptaufgabe von SNMP besteht darin, Netzwerkelemente wie z.B. Router, Switches und Drucker von einer zentralen Station aus überwachen und steuern zu können. Dazu gehören Aufgaben wie die Überwachung, die Fernsteuerung bzw. die Fernkonfiguration sowie die Fehlererkennung bzw. die Fehlerbenachrichtigung. SNMP regelt dabei den Ablauf der Kommunikation der Netzwerkelemente untereinander.

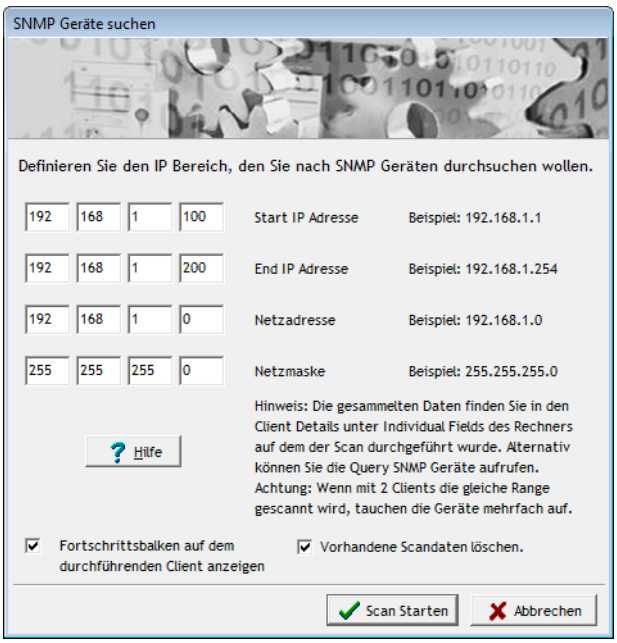
Die Daten, die ein Netzwerkelement liefert, können sich bei SNMP unterscheiden, da SNMP selbst nicht angibt, welche Daten eine Komponente liefern muss. Damit SNMP diese Daten trotzdem nutzen kann, gibt es die *Management Information Base* (MIB). Die MIB beinhaltet die Daten einer Netzwerkkomponente, welche in einer Baumstruktur dargestellt werden können. Dabei besitzt jedes Element dieser Baumstruktur einen eindeutigen Namen sowie eine eindeutige Nummer. Kombiniert man die Namen bzw. die Nummern der Elemente, kann man durch die Baumstruktur exakt zu den benötigten Werten navigieren und diese abfragen bzw. zu setzen. Diese Kombination wird *Object Identifier* genannt. Ein Object Identifier für die MIB2 könnte z.B. *internet.management.mib-2.ip.ipDefaultTTL* oder alternativ *1.2.1.4.2* lauten. Welche Werte genau genutzt werden, definieren viele Hersteller in eigenen MIBs.

Weiterhin bietet SNMP die Möglichkeit, so genannte *Communities* einzusetzen. Standard-Communities sind *public* und *private*. Während es der Community *private* erlaubt ist, Werte zu lesen und zu schreiben, darf die Community *public* nur Werte lesen. Meist können eigene Communities in den SNMP-Komponenten definiert werden. Da die Community jedoch im Klartext übertragen wird, bietet diese keinen besonders hohen Schutz vor nicht-autorisierten Zugriffen. Die neueste Version von SNMP (v3) bietet daher bessere Mechanismen an.

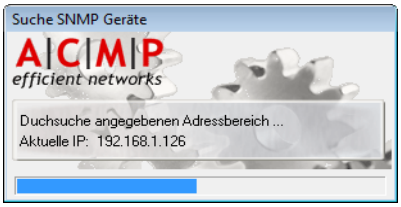
2. Netzwerkelemente mit SNMP und ACMP inventarisieren

Mit ACMP haben Sie die Möglichkeit, SNMP-fähige Netzwerkelemente automatisch inventarisieren zu lassen. Dazu besitzt ACMP das Client Command *SNMP Geräte suchen*. Dieses Client Command wird von einem Client ausgeführt, wobei die Ergebnisse in den Individuellen Feldern des Clients gespeichert werden. Dies spricht dafür, das Client Command vom ACMP Server aus auszuführen.

Um das Client Command *SNMP Geräte suchen* auszuführen, führen Sie zunächst eine einfache Abfrage im *Browse and Management* aus. Markieren Sie anschließend den Client, von dem aus die Suche nach SNMP-fähigen Netzwerkelementen gestartet werden soll. Öffnen Sie die *Client Commands*-Sparte, welche sich zwischen der Plugin-Übersicht und der soeben ausgeführten Abfrage befindet. Klicken Sie auf *SNMP Geräte suchen* und tragen Sie nötigen Angaben in den Dialog ein:



Nachdem Sie die Daten angegeben und auf *Scan Starten* geklickt haben, wird die Suche innerhalb weniger Minuten auf dem zuvor markierten Client gestartet. Falls Sie die entsprechende Option nicht demarkiert haben, wird der Suchfortschritt angezeigt:



Werden SNMP-fähige Netzwerkelemente gefunden, werden die vier SNMP-Felder *Name*, *Location*, *Description* und *Services* ausgelesen. Dies geschieht über die folgenden *Object Identifier* der *MIB*:

- system.sysName.0
- system.sysLocation.0
- system.sysDescr.0
- system.sysServices.0

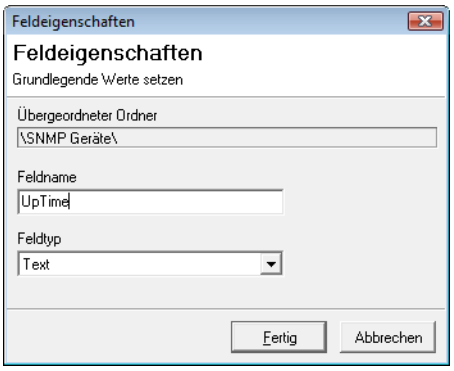
Die Ergebnisse des Suchvorgangs finden Sie in den *Client-Details* unter *Individuelle Felder - SNMP*. Die Client-Details können Sie einsehen, indem Sie in den Ergebnissen einer Abfrage einen Doppelklick auf den entsprechenden Client ausführen. Alternativ können Sie auch die Abfrage *SNMP-Geräte* aus der Kategorie *Pro Queries* ausführen:

Die Abfrage *SNMP-Geräte* hat hier den Vorteil, dass sämtliche SNMP-fähige Netzwerkelemente kompakt dargestellt werden, falls diese auf Grund der Netzwerkarchitektur nicht alle von einem zentralen Rechner erfasst werden können und die Daten somit auf mehr als einem Rechner gespeichert sind.

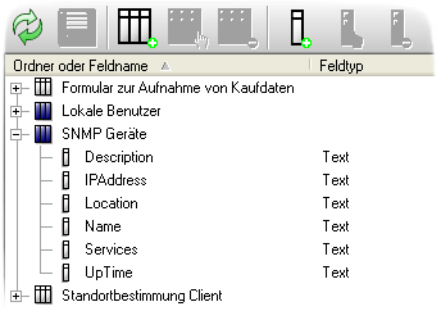
3. Weitere SNMP-Daten inventarisieren

Neben den SNMP-Daten *Name*, *Location*, *Description* und *Services* ist es natürlich möglich, weitere SNMP-Daten zu inventarisieren. Dazu müssen die *Individuellen Felder* sowie das Client Command *SNMP-Geräte suchen* angepasst werden. Im Folgenden wird dies am Beispiel des SNMP-Datum *Up Time* beschrieben.

Wechseln Sie im *Client Management Center* auf *Individuelle Felder*. Wählen Sie dort *SNMP Geräte* und klicken Sie auf *Feld erstellen*.

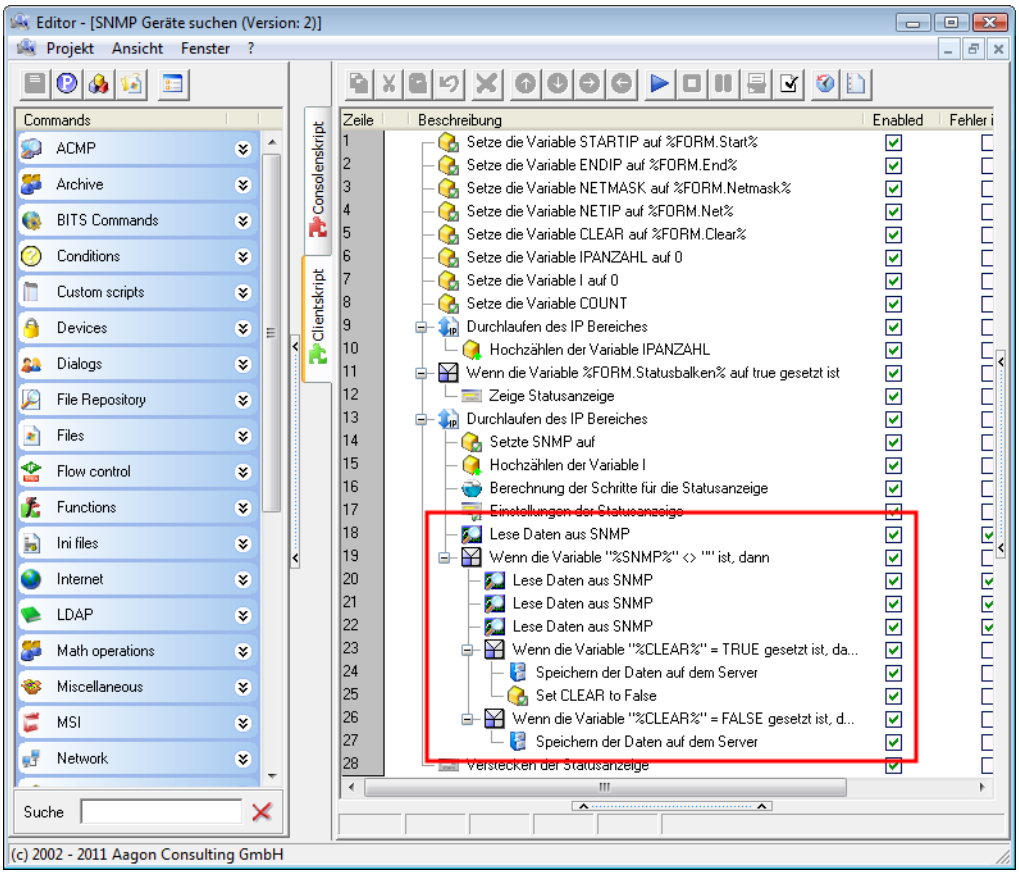


Tragen Sie als *Feldname UpTime* ein. Der *Feldtyp* kann auf *Text* belassen werden. Klicken Sie auf *Fertig*.

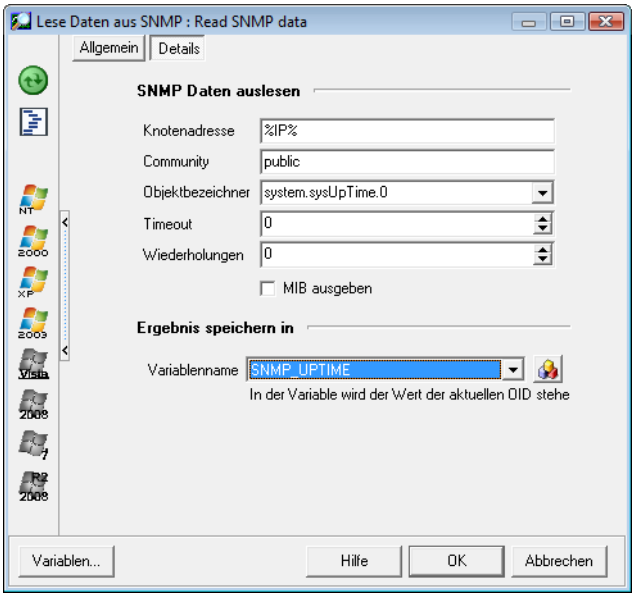


Die Kategorie *SNMP Geräte* verfügt nun zusätzlich über den Eintrag *UpTime*. Speichern Sie die Änderung und wechseln Sie zum *Client Command Center*, wo das Client Command *SNMP Geräte suchen* angepasst werden kann.

Im Client Command Center wechseln Sie zur Phase *Erstellen*. Unter der Kategorie *Erweiterte Inventarisierung* finden Sie das Client Command *SNMP Geräte suchen*. Markieren Sie das Client Command und klicken Sie auf das Icon *Neue Version* in der Schnellwahlleiste. Öffnen Sie anschließend das Client Command im *Client Command Editor*, indem Sie einen Doppelklick auf das Client Command ausführen. Wechseln Sie im Client Command Editor zum *Clientskript*.

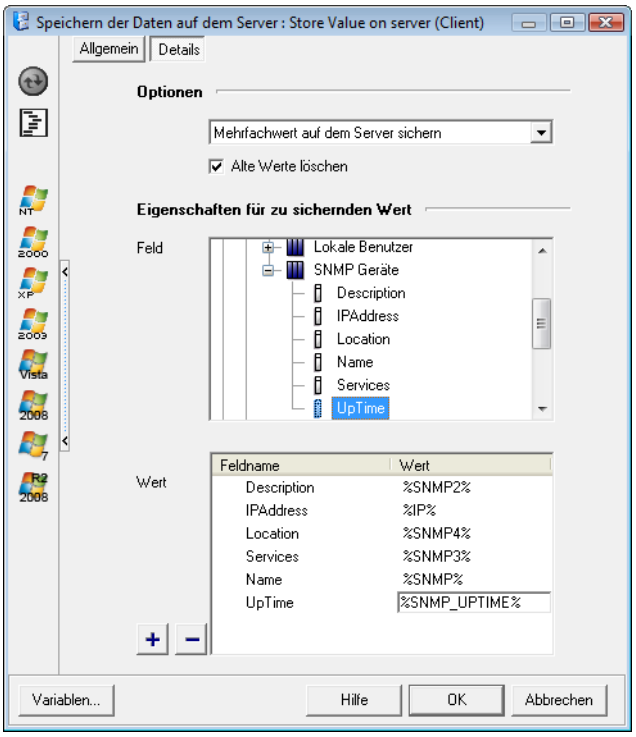


Im unteren Bereich des Clientskript finden Sie den Teil des Skripts, in welchem die SNMP-Daten ausgelesen und gespeichert werden. Markieren Sie hier einen der drei aufeinanderfolgenden *Lese Daten aus SNMP*-Kommandos und duplizieren Sie es per Copy&Paste. Alternativ können Sie dieses Kommando aus der Kategorie *Network* per Drag&Drop einfügen. Nun sollte das Skript vier aufeinanderfolgende *Lese Daten aus SNMP*-Kommandos aufweisen.



Tragen Sie als *Knotenadresse* die Variable *%IP%* ein. Als *Objektbezeichner* wählen Sie *system.sysUpTime.0* aus der DropDown-Liste, wobei hier jeder beliebige Wert auch manuell eingetragen werden kann. Rufen Sie über den unteren Button neben dem *Variablenname* die Variablenverwaltung auf und erstellen Sie die Variable *SNMP_UPTIME*. Wählen Sie die neu erstellte Variable als *Variablenname* aus und klicken Sie auf *OK*.

Nachdem das SNMP-Datum *UpTime* über das modifizierte *Lese Daten aus SNMP*-Kommando ausgelesen werden kann, muss das Datum nur noch gespeichert werden. Dazu finden Sie zwei Instanzen des Kommandos *Speichern der Daten auf dem Server*. Öffnen Sie die erste Instanz des Kommandos. Wählen Sie unter *Feld* den Wert *UpTime* unterhalb der Kategorie *Client - Individual Fields - SNMP Geräte*. Fügen Sie den Wert per Doppelklick der Auflistung *Wert* hinzu.



Als *Wert* für *UpTime* geben Sie die Variable *%SNMP_UPTIME%* an, welche Sie zuvor bei der Erstellung des *Lese Daten aus SNMP*-Kommandos angelegt haben. Über die Tastenkombination *STRG+Leertaste* erhalten Sie eine Auflistung aller zu Verfügung stehenden Variablen, aus der Sie die entsprechende Variable wählen können. Klicken Sie auf *OK*.

Fügen Sie das UpTime-Feld ebenfalls in der zweiten Instanz des *Speichern der Daten auf dem Server*-Kommandos hinzu.

Speichern Sie das Client Command und schließen Sie den Client Command Editor. Führen Sie einen Rechtsklick auf das Client Command durch und wählen Sie *Freigeben*. Das Client Command ist nun in der Lage, weitere SNMP-Felder - hier das Feld *UpTime* - auszulesen und zu speichern.

4. SNMP-Daten abfragen

Um die gesammelten SNMP-Daten abfragen zu können, gibt es die vordefinierte Abfrage *SNMP* in den Abfragen der *Pro Queries*. Alternativ können Sie sich die abgefragten Daten in den Client-Details des Clients anzeigen lassen, von dem die Daten abgefragt wurden.

4.1 Eine SQL-Abfrage um Individuelle Felder erweitern

Die *SNMP*-Abfrage zeigt lediglich die SNMP-Werte an, die standardmäßig inventarisiert werden. Daher muss die Abfrage abgeändert werden, was momentan noch etwas komplex ist. Diese Komplexität wird sich in der nächsten Version von ACMP deutlich verringern.

Die Abfrage *SNMP* ist eine erweiterte Abfrage und stützt sich auf eine SQL-Abfrage. Klicken Sie daher in der geöffneten Abfrage auf den Tab *SQL*. Die Abfrage könnte wie Folgt aussehen:

```
SELECT DISTINCT
  CLT_13323378AE9E4C07B0452.FCD913F73978C48BF8B9E66176 AS IPAddress,
  CLT_13323378AE9E4C07B0452.FEB00CC94C69843DF9A7151B9F AS Name,
  CLT_13323378AE9E4C07B0452.FF59326237F0F4E71B73359E88 AS Location,
  CLT_13323378AE9E4C07B0452.F0E100A9D0C5D4FC791DD59745 AS Description,
  CLT_13323378AE9E4C07B0452.F333E72005D5F4985A80FAD27A AS Services
FROM
  CLT_13323378AE9E4C07B0452
```

Diese kryptisch wirkende Abfrage wird erweitert, indem weitere Zeilen zwischen eingefügt werden. Dazu klicken Sie auf den Button *Bearbeiten*. Öffnen Sie zusätzlich das *SQL Server Management Studio*, welches von Microsoft in der Version *2005 Express* und *2008 Express* frei zum Download gestellt wird. Verbinden Sie sich mit dem SQL-Server und öffnen Sie die Datenbank *ACMP*. Öffnen Sie die Tabelle *dbo.SYS_IndiFields*. In dieser Tabelle sind alle Individuellen Felder gespeichert. Suchen Sie den Datensatz, welcher als *Caption* den Namen des individuellen Feldes hat, welches zur Abfrage hinzugefügt werden soll. In diesem Beispiel ist dies *UpTime*.

Notieren Sie sich nun die *FieldID*, die *FolderID* sowie die *DisplayFieldID*. Wechseln Sie nun zur Tabelle *dbo.SYS_IndiFields_Folders*. Falls hier ein Datensatz existiert, welcher als *FolderID* den gleichen Wert besitzt, wie die zuvor notierte *FolderID*, ist das Feld (*UpTime*) ein Multi-Feld.

Falls das Feld (*UpTime*) kein Multi-Feld ist, nehmen Sie die zuvor notierte *FieldID*, entfernen die Bindestriche und stellen ein *F* voran. Anschließend nehmen Sie die ersten 26 Zeichen als ID (z.B. `FC94C6AD69843D4985A80237F0`) für die SQL-Abfrage. Ergänzen Sie diese ID in der Abfrage mit dem *AS* Kommando um einen sprechenden Namen und setzen Sie den Tabellennamen vor die ID:

```
SELECT DISTINCT
  CLT_13323378AE9E4C07B0452.FCD913F73978C48BF8B9E66176 AS IPAddress,
  CLT_13323378AE9E4C07B0452.FEB00CC94C69843DF9A7151B9F AS Name,
  CLT_13323378AE9E4C07B0452.FF59326237F0F4E71B73359E88 AS Location,
  CLT_13323378AE9E4C07B0452.F0E100A9D0C5D4FC791DD59745 AS Description,
  CLT_13323378AE9E4C07B0452.F333E72005D5F4985A80FAD27A AS Services,
  CLT_13323378AE9E4C07B0452.FC94C6AD69843D4985A80237F0 AS UpTime
FROM
  CLT_13323378AE9E4C07B0452
```

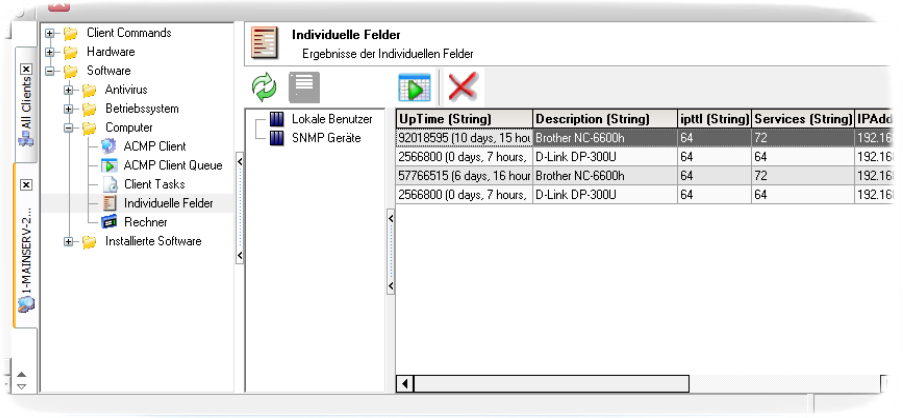
Falls das Feld (*UpTime*) ein Multi-Feld ist, nehmen Sie die zuvor notierte *DisplayID*, entfernen die Bindestriche und stellen ein *F* voran. Ebenso nehmen Sie die zuvor notierte *FolderID*, entfernen die Bindestriche und stellen ein *CLT_* voran. Nehmen Sie von der modifizierten *FolderID* die ersten 25 Zeichen, gefolgt von einem Punkt (.) und den ersten 26 Zeichen der modifizierten *DisplayID*. Ergänzen Sie diese Zeichenkette (z.B. `CLT_C07B045213323378AE9E4.FE100A9DF0F4E71B0F4E71B7D4`) mit dem *AS* Kommando um einen sprechenden Namen. Falls die ermittelte und modifizierte *FolderID* noch nicht im *FROM*-Ausdruck vorkommt, muss diese dort eingetragen werden:

```
SELECT DISTINCT
  CLT_13323378AE9E4C07B0452.FCD913F73978C48BF8B9E66176 AS IPAddress,
  CLT_13323378AE9E4C07B0452.FEB00CC94C69843DF9A7151B9F AS Name,
  CLT_13323378AE9E4C07B0452.FF59326237F0F4E71B73359E88 AS Location,
  CLT_13323378AE9E4C07B0452.F0E100A9D0C5D4FC791DD59745 AS Description,
  CLT_13323378AE9E4C07B0452.F333E72005D5F4985A80FAD27A AS Services,
  CLT_C07B045213323378AE9E4.FE100A9DF0F4E71B0F4E71B7D4 AS UpTime
FROM
  CLT_13323378AE9E4C07B0452, CLT_C07B045213323378AE9E4
```

Nachdem Sie die Abfrage gespeichert haben, können Sie sie ausführen. Es empfiehlt sich jedoch, die komplette SQL-Abfrage testweise über das *SQL Server Management Studio* auszuführen, um mögliche Fehler besser finden zu können.

4.2 Daten in den Client-Details

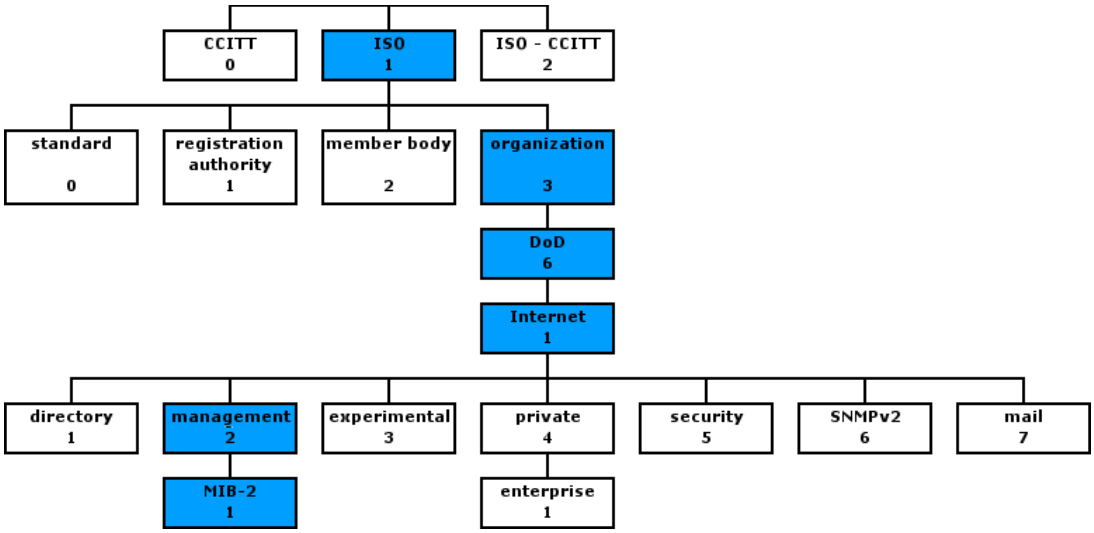
Alternativ können Sie die SNMP-Daten in den Details des Clients einsehen, von dem aus die SNMP-Abfrage gestellt wurde. Führen Sie dazu eine Abfrage aus, in der der entsprechende Client gelistet ist und rufen Sie über einen Doppelklick auf den Client die Details auf.



In den Details markieren Sie die Kategorie *Individuelle Felder* unterhalb des Pfades *Software\Computer*. In der rechtsseitigen Ansicht finden Sie alle Gruppen, welche in den *Individuellen Feldern* angelegt sind. Klicken Sie hier auf *SNMP Geräte*. Es werden Ihnen die alle Felder der Gruppe mit ihren jeweiligen Werten angezeigt.

5. SNMP Object Identifier

Mit Hilfe eines *Object Identifiers* kann ein bestimmtes Datum eines SNMP-fähigen Netzwerkelements angesprochen werden. Im Folgenden sollen die wichtigsten OIDs der MIB-2 vorgestellt werden. Es werden jedoch nicht alle vorgestellt. Weitere Informationen zu OIDs können unter www.oid-info.com oder mit dem *SNMP Object Navigator* von Cisco eingesehen werden. Hersteller von Netzwerkelementen können zusätzlich eigene OIDs festlegen, welche standardmäßig in der entsprechenden Produkt-Dokumentation gelistet werden. Die folgende Grafik zeigt einen teilweisen Aufbau der OIDs:



Das Kommando *Lese Daten aus SNMP* benötigt die OID unterhalb der MIB-2 (1.3.6.1.2.1) oder den kompletten OID-Pfad. Zum Beispiel muss zum Auslesen der Gerätebeschreibung lediglich *system.sysDescr.0* angegeben werden. Beachten Sie, dass zusätzlich eine *.0* angehängt wird, um den entsprechenden Datensatz zu kennzeichnen. Bei einem Ergebnis mit mehreren Werten können so die einzelnen Werte abgefragt werden. Allerdings ist es möglich, die *.0* auszulassen und so alle Werte eines Ergebnisses abzufragen.

system (1)

sysDescr (1)
Beschreibung des Gerätes. Enthält meistens den Namen, die Versionsnummer sowie Angaben zur internen Software.

sysObjectID (2)
Die vom Hersteller verbindlich festgelegte Identifikationsnummer des Netzwerkmanagement-Untersystems dieses Gerätes. Dieser Wert ist in den SMI-Enterprises-Subtrees (1.3.6.1.4.1) festgelegt und bietet ein eindeutiges Hilfsmittel um herauszufinden, um welche Art von Gerät es sich handelt.

sysUpTime (3)
Die Zeit (in hundertstel Sekunden), die das System seit dem letzten Reset aktiv ist.

sysContact (4)
Kontaktinformationen zur Person, welche das entsprechende Gerät betreut.

sysName (5)
Der administrativ zugewiesene Name des Gerätes.

sysLocation (6)
Die physikalische Adresse des Gerätes (z.B. Raumnummer).

sysServices (7)
Dieser Wert gibt an, welche Dienste ein Gerät anbietet. Der Wert wird dabei über Teilwerte summiert. Für jede Schicht des OSI-Modells wird ein Teilwert nach dem Muster $2^{SchichtX+SchichtY+...SchichtZ-1}$ berechnet, z.B. 2^{3+4-1} falls das Gerät Dienste der Schichten 3 und 4 anbietet. Die Schichten sind wie Folgt definiert:

1) Pysical (z.B. Repeater)
2) Datalink/Subnetwork (z.B. Bridges)
3) Internet (z.B. IP-Gateways)
4) End to end (z.B. IP-hosts)
5-6) Schicht 5 und 6 werden in der Regel nicht direkt unterstützt, sind jedoch möglich, falls sie vom Gerät unterstütz werden.
7) Application (z.B. Mail-Relays)

Bei Systemen welche OSI-Layer 5 und 6 unterstützen, werden diese auch gezählt.

interfaces (2)

ifNumber (1)
Die Anzahl der Netzwerkanschlüsse (ungeachtet des aktuellen Status) des Gerätes.

ip (4)

ipDefaultTTL (2)
Dieser Wert wird in das *Time-to-live*-Feld des IP-Headers eingefügt, wenn bei ankommenden Paketen kein *TTL*-Wert angegeben ist.

icmp (5)

icmpInMsgs (1)
Die Gesamtanzahl von ICMP-Nachrichten, welche das Gerät empfangen hat; inklusive aller *icmpInErrors*-Nachrichten.

icmpInErrors (2)
Die Anzahl von ICMP-Nachrichten, welche von der Einheit empfangen wurden, jedoch einen ICMP-spezifischen Fehler enthalten (bspw. falsche ICMP-Kontrollsumme, falsche Länge etc.).

icmpInRedirects (7)
Die Anzahl von empfangenen Redirect-ICMP-Nachrichten *[umgeleiteten ICMP-Nachrichten]*.

icmpInEchos (8)
Die Anzahl von empfangenen ICMP-Echo-Anfragen

icmpInEchoReps (9)
Die Anzahl von empfangenen ICMP-Echo-Antwortnachrichten

icmpOutMsgs (14)
Die Gesamtanzahl von ICMP-Nachrichten, welche das Gerät versucht hat zu senden. Bitte beachten Sie, dass dieser Zähler auch alle Nachrichten enthält, die von icmpOutErrors gezählt wurden.

icmpOutErrors (15)
Die Anzahl von ICMP-Nachrichten, welche das Gerät wegen fehlenden Puffers innerhalb von ICMP entdeckt hat. Dieser Wert enthält keine Fehler, welche außerhalb des ICMP-Layers entdeckt wurden, wie z.B. die Unfähigkeit der IP das resultierende Datagramm weiterzuleiten. In einigen Installationen gibt es keine Fehlertypen, welche diesen Fehlerwert beeinflussen.

icmpOutRedirects (20)
Die Anzahl von gesendeten Redirects-ICMP-Nachrichten. Bitte beachten Sie, dass die Zahl bei einem Host immer Null ist, denn ein Host sendet keine Redirects-ICMP-Nachrichten.

icmpOutEchos (21)
Die Anzahl der gesendeten ICMP-Echo- (Anfragen-) Nachrichten.

icmpOutEchoReps (22)
Die Anzahl von gesendeten ICMP-Echo-Antwort-Nachrichten.

tcp (6)

tcpMaxConn (4)
Die maximale Anzahl von gleichzeitigen TCP-Verbindungen, welche von dem Gerät unterstützt werden. In Geräten, in denen die maximale Anzahl von Verbindungen dynamisch ist, enthält diese Variable den Wert -1.

tcpActiveOpens (5)
Die Häufigkeit, in der TCP-Verbindungen direkt vom SYN-SENT-Status zum Closed-Status wechselten.

tcpPassiveOpens (6)
Die Häufigkeit, in der TCP-Verbindungen direkt vom SYN-RCVD-Status zum Closed-Status wechselten.

tcpInSegs (10)
Die gesamte Anzahl aller fehlerhaften empfangenen TCP-Segmente. Dieser Zähler enthält auch Segmente, welche bei bereits bestehenden Verbindungen empfangen wurden.

tcpOutSegs (11)
Alle gesendeten Segmente, inklusive derer von bestehenden Verbindungen, aber ohne die Segmente, welche bereits gesendete Oktets beinhalten.

tcpInErrs (14)
Die gesamte Anzahl von fehlerhaften Segmenten, die empfangen wurden. Bspw. wegen falscher TCP-Checksummen.

tcpOutRsts (15)
Die Anzahl der gesendeten TCP-Segmente mit dem Wert *RST*.

udp (7)

udpInDatagrams
Die gesamte Anzahl von UDP-Paketen, welche zum UDP-Benutzer versendet wurden.

udpOutDatagrams
Die gesamte Anzahl an UDP-Paketen, welche von diesem Gerät versendet wurden.

snmp (11)

snmpInPkts
Die gesamte Anzahl von Nachrichten, welche vom Transport-Service an das SNMP-Gerät gesendet wurden.

snmpInTraps
Die gesamte Anzahl von SNMP-Trap-PDU*3 Nachrichten, welche von dem SNMP-Interface akzeptiert und weitergeleitet wurden.

snmpOutPkts
Die gesamte Anzahl von SNMP-Nachrichten, welche von SNMP-Protokoll-Gerät zum Transport-Dienst weitergeleitet wurden.

snmpOutTraps
Die gesamte Anzahl von SNMP-Trap-PDU-Nachrichten, welche von dem SNMP-Interface gesendet wurden.