



Technisch-Naturwissenschaftliche
Fakultät

SNMP - Simple Network Monitoring Protokoll

SICHERHEIT IN APPLIKATIONSPROTOKOLLEN

Eingereicht von:
Christian Eisner, Thomas Mayr

Linz, November 2011

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
1 Einleitung	3
2 Begriffe.....	3
2.1 SNMP Agent.....	3
2.2 SNMP Client (Managementkonsole).....	3
2.3 OID (Object Identifier).....	4
2.4 MIB (Management Information Base)	4
2.5 Community	5
3 SNMPv1	5
3.1 Definierte Funktionen.....	5
3.1.1 Get.....	5
3.1.2 GetNext	5
3.1.3 Set.....	5
3.1.4 Responce	5
3.1.5 Trap	6
4 SNMPv2.....	6
4.1 zusätzliche Funktionalitäten	6
4.1.1 User-Based Authentication (SNMPv2p)	6
4.1.2 Community-Based Authentication (SNMPv2c)	6
4.1.3 GetBulk (in allen SNMPv2 Versionen)	6
5 SNMPv3.....	7
5.1 Sicherheitsanforderungen	7
5.2 Rahmenwerk.....	7
5.3 User Security Model.....	8
5.4 View Access Control Model.....	9
Literaturverzeichnis.....	10

1 Einleitung

SNMP (Simple Network Management Protokoll) dient zur Überwachung und zur Konfiguration von Netzwerkgeräten. Notwendig dafür sind SNMP fähige Geräte und eine passende Software auf einem möglichst zentralen Computer. Die meisten Geräte wie Router, Switches und Netzwerksensoren unterstützen heutzutage mindestens SNMPv2c. Dieses muss aktiviert werden und kann danach über das SNMP Protokoll angesprochen werden.

SNMP ist hilfreich bei der Verwaltung vieler Netzwerkkomponenten, da nur eine Netzwerkverbindung zu diesem Gerät notwendig ist, um es administrieren zu können. Es ist auch möglich automatisierte Nachrichten sogenannte Traps bei der Veränderung zu senden. Vom Sicherheitsaspekt her ist SNMPv1 und SNMPv2 leider eher schlecht bestückt.

SNMP ist absichtlich einfach gehalten, damit es auch von sehr leistungsschwachen Geräten wie Sensoren (Feuchtigkeitssensor oder Rauchsensor) verwendet werden kann. Diese Geräte sind für Rechenzentren wichtig, jedoch ist es schwer dieses einzeln über eine Konsole anzusprechen. Einfach ist es mittels eines zentralen Managements alle gleichzeitig konfigurieren zu können.

2 Begriffe

2.1 SNMP Agent

Als SNMP Agent wird das Netzwerkgerät bezeichnet, das mit SNMP von der zentralen Managementkonsole angesprochen wird. Der Agent wird mit SNMP überwacht und konfiguriert. Er stellt die in der entsprechenden MIB definierten OID Daten bereit. In den meisten Fällen muss der Agent vor der Verwendung manuell aktiviert werden, um keine unbekanntes Sicherheitslücken im System zu offen zu halten.

2.2 SNMP Client (Managementkonsole)

Der SNMP Client ist vergleichbar mit einer Managementkonsole. Von ihm gehen die SNMP Anfragen aus. Der Client ist in den meisten Fällen auch die Schnittstelle zwischen Mensch und Maschine. Er verwaltet die SNMP Agenten und ermöglicht es dem Benutzer die konfigurierten und zugewiesenen Agenten zu verwalten, also die Daten auszulesen und Konfigurationswerte zu setzen. Die MIBs werden beim Client benötigt, damit bekannt ist, welche Datenwerte beim Gerät verfügbar sind, welchen Datentyp sie besitzen und ob sie gelesen oder geschrieben werden können. Die Managementkonsole verwendet oft ein Softwareinterface um die Darstellung der Daten für den Benutzer zu vereinfachen. z.B. Nagios

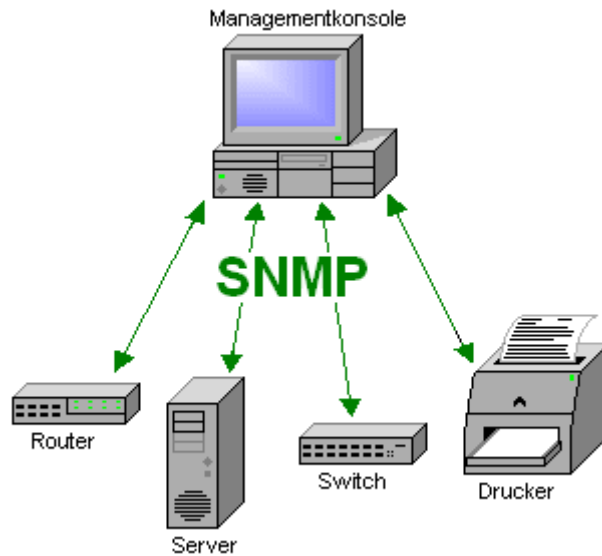


Abb.1: SNMP Agent - Managementkonsole

2.3 OID (Object Identifier)

Die OID ist ein Zahlenwert, der eindeutig den Wert eines bestimmten Datenfelds eines SNMP fähigen Gerätes beschreibt. Die OIDs sind baumförmig organisiert und werden von der Wurzel bis zu einer bestimmten Tiefe von der IANA verwaltet. Die OIDs beschreiben nur die Zahlen durch den Baum. (Z.B. 1-3-6-1-4-...) Die Auflösung zu Namen erfolgt erst mittels der MIB.

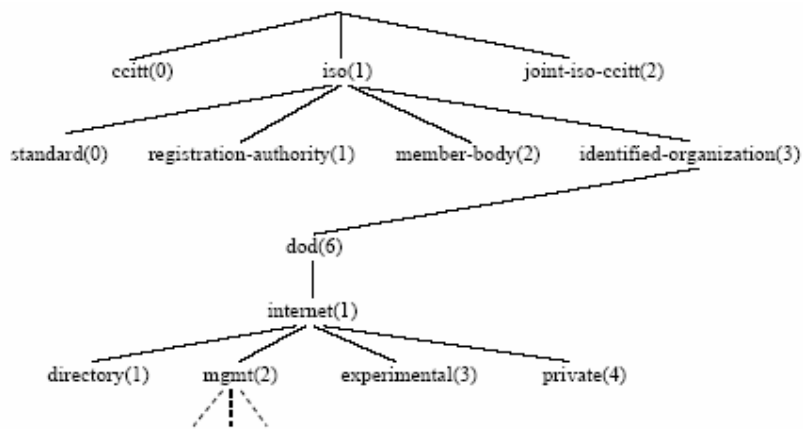


Abb.2: OID Baum

2.4 MIB (Management Information Base)

Die MIB ist die Beschreibung einer OID. Sie enthält den Namen, den Datentyp und die Zugriffsmöglichkeiten auf eine bestimmte OID. Auch kann sie eine Beschreibung beinhalten. Mit der Hilfe der MIBs wird der OID Baum auch für den Menschen lesbar. Des Weiteren wird die MIB vom Managementsystem benötigt. Erst nachdem die MIB geladen wurde weiß das System welche Daten von einem bestimmten Gerät abgefragt oder gesetzt werden können.

```

cpqCmcValueVoltage OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Actual value of power supply (voltage monitoring and fans) in V"
::= { cpqCmcValues 3 }

```

Abb.3: Ausschnitt aus MIB eines Spannungssensors

2.5 Community

Die Community existiert seit der Version SNMPv1, ist jedoch nicht in den ursprünglichen RFCs angeführt. Sie ist ein einfacher String, der auf den Geräten mit bestimmten Zugriffsberechtigungen verbunden ist. Der Community-String wird bei jeder Anfrage mitgesendet, um die Berechtigungsebene des Managementsystems dem zu verwaltenden Gerät mitzuteilen. Der Agent kann die Community bestimmten Rechten zuteilen und so entscheiden, ob eine Anfrage beantwortet werden kann oder nicht.

3 SNMPv1

SNMPv1 wurde 1988 in 3 RFCs (RFC 1155, RFC 1156, RFC 1157) definiert. Es beinhaltet keine Sicherheitsfeatures. Aus diesem Grund wurde Secure SNMP entwickelt, jedoch nie eingesetzt.

3.1 Definierte Funktionen

Im Standard von SNMPv1 sind folgende Funktionen definiert:

3.1.1 Get

Mit dem GET Befehl kann ein bestimmter Datenwert (OID) vom SNMP Agenten abgefragt werden.

3.1.2 GetNext

Der GETNEXT Befehl ruft den Datenwert ab, der auf eine bestimmte OID folgt. Damit kann durch ein Array durchiteriert werden. Arrays werden z.B. bei Datendurchsatzraten oder Ports verwendet.

3.1.3 Set

Mit Hilfe des SET Befehls kann ein Datenwert gesetzt werden. Voraussetzung dafür ist, dass er in der MIB als "writeable" definiert ist. Beispiele für Datenwerte die geschrieben werden können ist z.B. der Name des Agenten.

3.1.4 Responce

Die Responce-Nachricht ist die Antwort eines Agenten auf eine Anfrage.

3.1.5 Trap

Normalerweise werden bei SNMP die Daten nur auf Anfrage gesendet. Der Trap ist hierbei eine Ausnahme. Es ist möglich sogenannte Traps zu definieren. Dann sendet der Agent von sich aus bei Veränderung des Datenwertes eine Nachricht an die eingestellten Managementstationen. Ein Anwendungsbeispiel hierfür ist der Ausfall eines Links oder das Überschreiten eines bestimmten Wertes bei einem Sensor.

4 SNMPv2

SNMPv2 wurde direkt aus Secure SNMP entwickelt. Es wurde 1993 von der IETF veröffentlicht. Es gibt 3 unterschiedliche Versionen, von denen jedoch nur SNMPv2c Einsatz gefunden hat. Die anderen beiden sind SNMPv2p (Party-Based SNMP) und SNMPv2u (User-Based SNMP). Zusätzlich zu den "Sicherheitsfeatures" wurde die Möglichkeit mehrere Datenwerte auf einmal auslesen zu können (GETBULK) implementiert. SNMPv2 wurde wie auch SNMPv1 in mehreren RFCs definiert.

4.1 zusätzliche Funktionalitäten

Mit SNMPv2 wurden einigen neue Funktionalitäten zum Standard SNMPv1 hinzugefügt. Mit diesen sollte auch die Sicherheit erhöht werden, jedoch können die Sicherheitsfunktionen leicht umgangen werden.

4.1.1 User-Based Authentication (SNMPv2p)

Bei SNMPv2p wird mittels eines mitübertragenen Benutzernamens entschieden, ob die Anfrage akzeptiert wird oder nicht. Diese Methode stellt viel Aufwand für den Administrator dar, da die Benutzer auf jedem Gerät einzeln eingetragen werden müssen. Außerdem könnte durch senden eines "falschen" Benutzers dessen Rechte erhalten werden. SNMPv2p wird nicht eingesetzt bzw. ist auf den Geräten nicht implementiert.

4.1.2 Community-Based Authentication (SNMPv2c)

Bei SNMPv2c wird ein Communitystring als "Authentifikation" verwendet. Hierbei wird der Name der Community in jeder Anfrage mitgesendet. Die Community ist auf den Geräten gespeichert und bestimmt welche Berechtigungen eine Anfrage dieser Gruppe hat. Das Anfragen mit einer falschen Community ist jedoch wieder möglich. Somit kann diese Methode auch nicht als sehr sicher angesehen werden.

4.1.3 GetBulk (in allen SNMPv2 Versionen)

Mit dem GETBULK Befehl können mehrere Datenwerte einer OID auf einmal ausgelesen werden. Hilfreich ist das z.B. beim Auslesen von Tabellen oder Arrays. Es muss somit nicht mehr die gesamte Tabelle mit GETNEXT durchgelaufen werden.

5 SNMPv3

Sicherheit war zu Beginn von SNMP kein Thema. Es wurden dann zwar gemäß RFC 1901 die *Community Names* eingeführt, die eine Art von Passwörtern darstellen, doch diese wurden in Klartext zwischen SNMP-Manager und SNMP-Agent übertragen. Weitere Sicherheitsmaßnahmen, wie sie später aufgeführt werden, fehlen. Um die Sicherheit bei SNMP auf den aktuellen Stand der Technik zu bringen, wurde dann SNMPv3 entwickelt und im Dezember 2002 in mehreren RFCs veröffentlicht.

5.1 Sicherheitsanforderungen

In RFC 3411 werden unter anderem die Sicherheitsanforderungen an die neue SNMP Architektur gestellt. Die folgenden vier Punkte werden in SNMPv3 berücksichtigt:

- **Datenintegrität:** Es muss sichergestellt sein, dass eine Änderung der Nachricht während der Übertragung erkannt wird
- **Authentifizierung:** Es muss sichergestellt sein, dass der rechtmäßige Absender und der rechtmäßige Empfänger miteinander kommunizieren.
- **Vertraulichkeit:** Es muss sichergestellt sein, dass kein unberechtigter Dritter die enthaltenen Nachrichten lesen kann.
- **Aktualität der Daten:** Es muss sichergestellt sein, dass korrekte Nachrichten zeitgemäß übertragen werden.

Zwei Bedrohungen werden ebenfalls angeführt, jedoch wurden diese aufgrund geringerer Bedeutung ausgeschlossen. Es handelt sich um eine *Denial-of-Service* Attacke und eine *Verkehrsanalyse*.

5.2 Rahmenwerk

Bei SNMPv3 wurde ein neues Rahmenwerk vorgestellt, das ein neues SNMP Nachrichten Format, Sicherheit, Zugriffskontrolle und Remote Konfiguration von SNMP Parametern einführt. Die Managementstation sowie die Agenten werden in den RFCs als SNMP Entitäten bezeichnet. In Abb. 4 wird die Struktur einer SNMP Entität dargestellt. Jede SNMP Entität enthält eine SNMP Engine, die durch eine eindeutige Nummer (*snmpEngineID*) identifiziert werden kann. Je nach Art, Managementstation oder Agent, werden die verschiedenen Applikationen verwendet.

Die SNMP Engine verfügt über vier Subsysteme. Das erste Subsystem, der Dispatcher, ist für den Empfang und Versand von SNMP Nachrichten mit dem jeweiligen Transportprotokoll, wie UDP oder IPX, verantwortlich. Das Message Processing Subsystem interagiert mit dem Dispatcher und verarbeitet die Nachrichten gemäß der verwendeten SNMP Version. Beide Subsysteme sind im RFC 3412 detailliert beschrieben. Die unterstützten Protokolle der Transportschicht werden in RFC 3417 näher erläutert.

Das Security Subsystem behandelt die Authentifizierung und Verschlüsselung zwischen den Entitäten. Derzeit ist nur das User Security Model definiert, das in Punkt 5.3 näher erläutert wird.

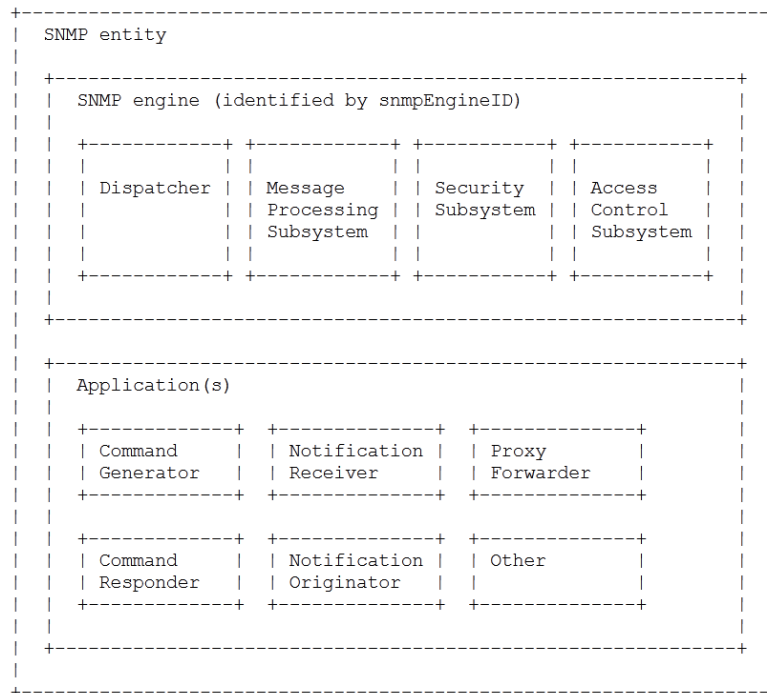


Abb. 4: SNMP Entität gemäß RFC 3411

Das letzte Subsystem, das Access Control Subsystem, regelt den Zugriff auf die einzelnen Objekte eines SNMP Agenten, in Punkt 5.4 erläutert wird.

Das Framework definiert neben den Subsystemen verschiedene Applikationen, die je nach Art der Entität verwendet werden. Ein SNMP Agent verwendet die Applikationen *Command Responder*, *Notification Originator* sowie den *Proxy Forwarder*. Eine Management-station verwendet die Applikationen *Command Generator*, *Notification Receiver* und *Notification Originator*. Gemäß den Namen wird der jeweilige Empfang, Versand und Weiterleitung von SNMP Nachrichten geregelt. Detaillierte Informationen können dem RFC 3413 entnommen werden.

5.3 User Security Model

Das User Security Model (USM) wird in RFC 3414 definiert und deckt mehrere Bedrohungen, die in einem SNMP verwaltetem Netzwerk vorkommen können. Es ist für die Authentifikation und Verschlüsselung verantwortlich. Es sind drei Security-Level möglich:

- Ohne Authentifikation und ohne Verschlüsselung (noAuthNoPriv)
- Mit Authentifikation und ohne Verschlüsselung (authNoPriv)
- Mit Authentifikation und mit Verschlüsselung (authPriv)

Zur Authentifikation und Integrität wird ein Hashed Message Authentication Code (HMAC, RFC 2104) herangezogen. Derzeit kann zwischen einem HMAC-MD5-96 und einem HMAC-SHA1-96 gewählt werden. Eine kryptografischen Hashfunktion, wie MD5 oder SHA1, dient zur Feststellung der Integrität zweier Nachrichten. Bei der Berechnung eines HMACs werden die Nachricht und ein geheimer Schlüssel verwendet, um den Hash zu berechnen. Sollte der Empfänger bei der Kontrolle

einen anderen HMAC erhalten, dann kann dieser nicht feststellen, ob der Absender den falschen Schlüssel gewählt hat oder ob die Nachricht während des Transports verändert wurde.

Um die Vertraulichkeit zu gewährleisten, kann zur Ver- und Entschlüsselung zwischen den Algorithmen *Data Encryption Standard* im Cipher Block Chaining Mode (CBC-DES, 56 bit) und dem *Advanced Encryption Standard* (AES, 128 bit) gewählt werden, der erst 1,5 Jahre später im RFC 3826 ergänzt wurde.

Um einen Schutz gegen Verzögerungen und gegen Replay-Attacken zu bieten, wurden zwei Werte in den USM Security Parametern eingeführt. Der erste Wert, *snmpEngineBoots*, enthält die Anzahl der Neustarts der SNMP Engine. *snmpEngineTime*, der zweite Wert, enthält die Anzahl der Sekunden seit der letzten Erhöhung von *snmpEngineBoots*. Das Zeitfenster laut RFC 3414 beträgt 150 Sekunden, danach wird die Nachricht nicht mehr verarbeitet.

5.4 View Access Control Model

Das derzeit einzige Zugriffskontrollsystem bei SNMPv3 lautet View Access Control Model (VACM) und wird in RFC 3415 definiert. Nachfolgend werden anhand des Entscheidungsprozesses (Abb. 5) die einzelnen Begriffe, Tabellen und Abläufe erläutert:

1. Als erstes wird geprüft, ob die Kontext-Tabelle (*vacmContextTable*) den Kontext enthält. Als Kontext wird eine Sammlung von Management-Informationen bezeichnet, die einer SNMP Entität zugänglich gemacht wird. Fehlt der Kontext in der Kontext-Tabelle, dann wird der Zugriff verweigert.
2. Als nächstes wird in der internen Tabelle (*vacmSecurityToGroupTable*) nach einem Gruppennamen gesucht, der sich aus dem *Security Model* (z.B. USM) und dem Security Namen (z.B. der Benutzername bei USM) zusammensetzt. Fehlt der Eintrag in der Tabelle, dann wird der Zugriff verweigert.
3. Im dritten Schritt werden die Zugriffsrechte für die Gruppe in der Tabelle *vacmAccessTable* abgefragt. Dazu werden der Gruppename, der Kontext, das Security Model/Level und den *ViewType* benötigt. Der *ViewType* enthält die gewünschte Sicht, wie Lesen, Schreiben oder Melden.
4. Die vierte Tabelle *vacmViewTreeFamilyTable* enthält „MIB Views“. Eine MIB View stellt eine setzt sich aus einer MIB und einer Bitmaske zusammen. Beispiele werden in [5] vorgestellt.

Sollten alle Tabellen passende Einträge enthalten, dann wird der Zugriff gewährt.

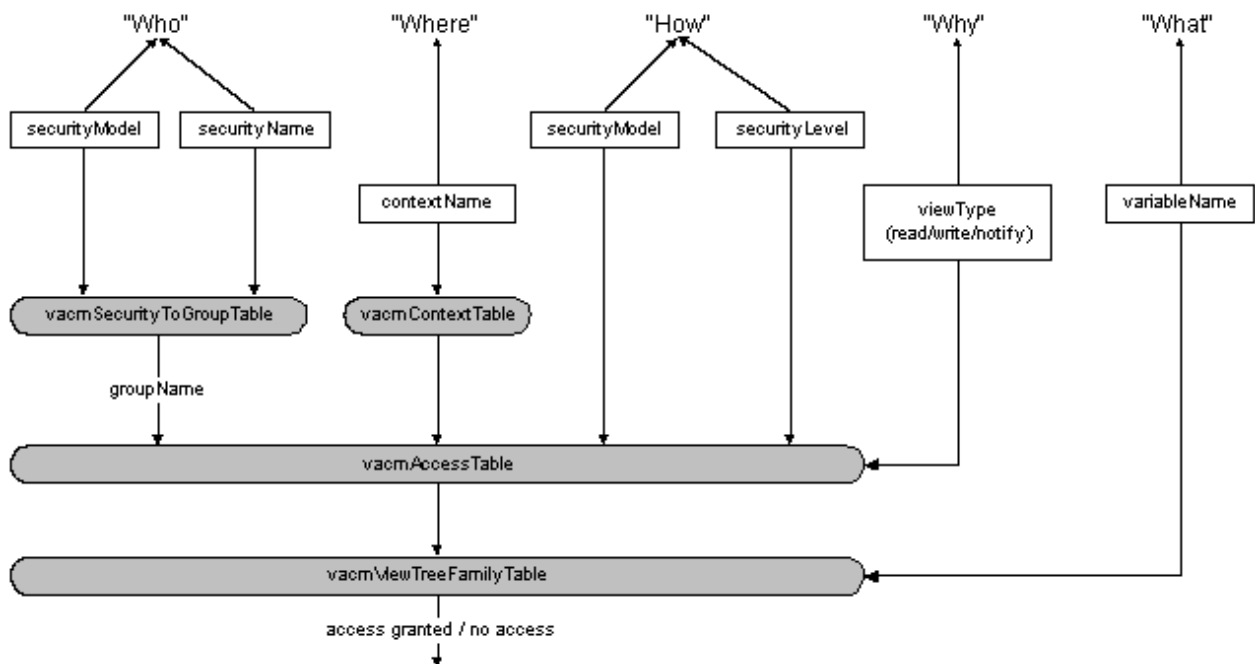


Abb. 5: Entscheidungsprozess des View-based Access Control Models (VACM) [1999, Paila]

Literaturverzeichnis

- [1] DI Hörmanseder Rudolf; Netzwerkmanagement SNMP = Simple Network Protocol (Vorlesung 2010, N_Netzwerk-Management SNMP.pdf)
- [2] Wikipedia, Simple Network Management Protokoll (http://de.wikipedia.org/wiki/Simple_Network_Management_Protocol)
- [3] 1999 Paila, The Security of Network Management (<http://www.tml.tkk.fi/Opinnot/Tik-110.501/1999/papers/management/netsec.html>)
- [4] Davis, SNMPv3 - User Security Model (<http://insanum.com/docs/usm.html>)
- [5] Davis, SNMPv3 - SNMPv3 - View Access Control Model (<http://insanum.com/docs/vacm.html>)