



Landesakademie für
Fortbildung u.
Personalentwicklung an
Schulen - Standort Esslingen

Simple Network Management Protocol (SNMP), SNMP-Sicherheit und SNMP-Monitoring



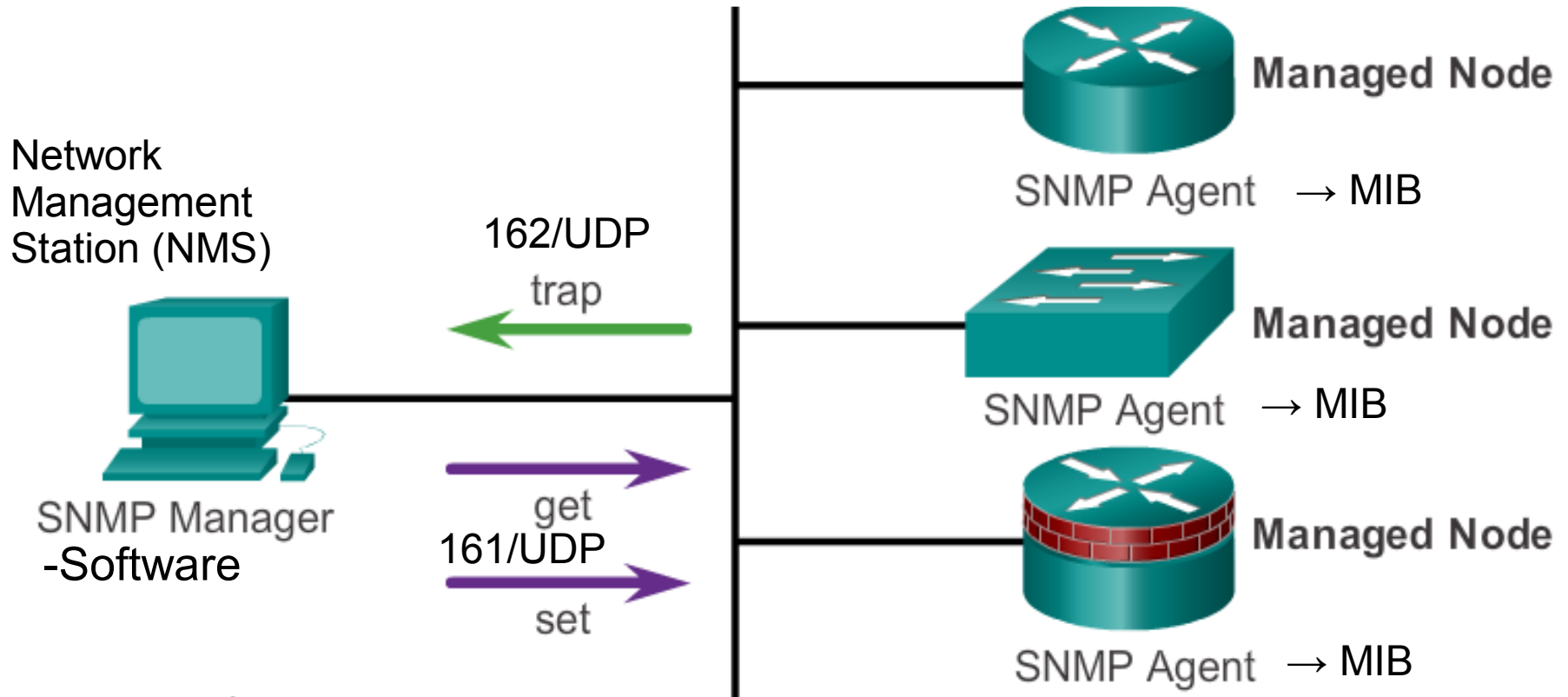
Andreas Grupp
grupp@lehrerfortbildung-bw.de



„Simple Network Management Protocol (SNMP) & SNMP-Sicherheit“ von Andreas Grupp ist lizenziert unter einer Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 3.0 Unported Lizenz.

SNMP-Grundlagen

Kommunikation erfolgt zwischen SNMP-Manager und SNMP-Agent



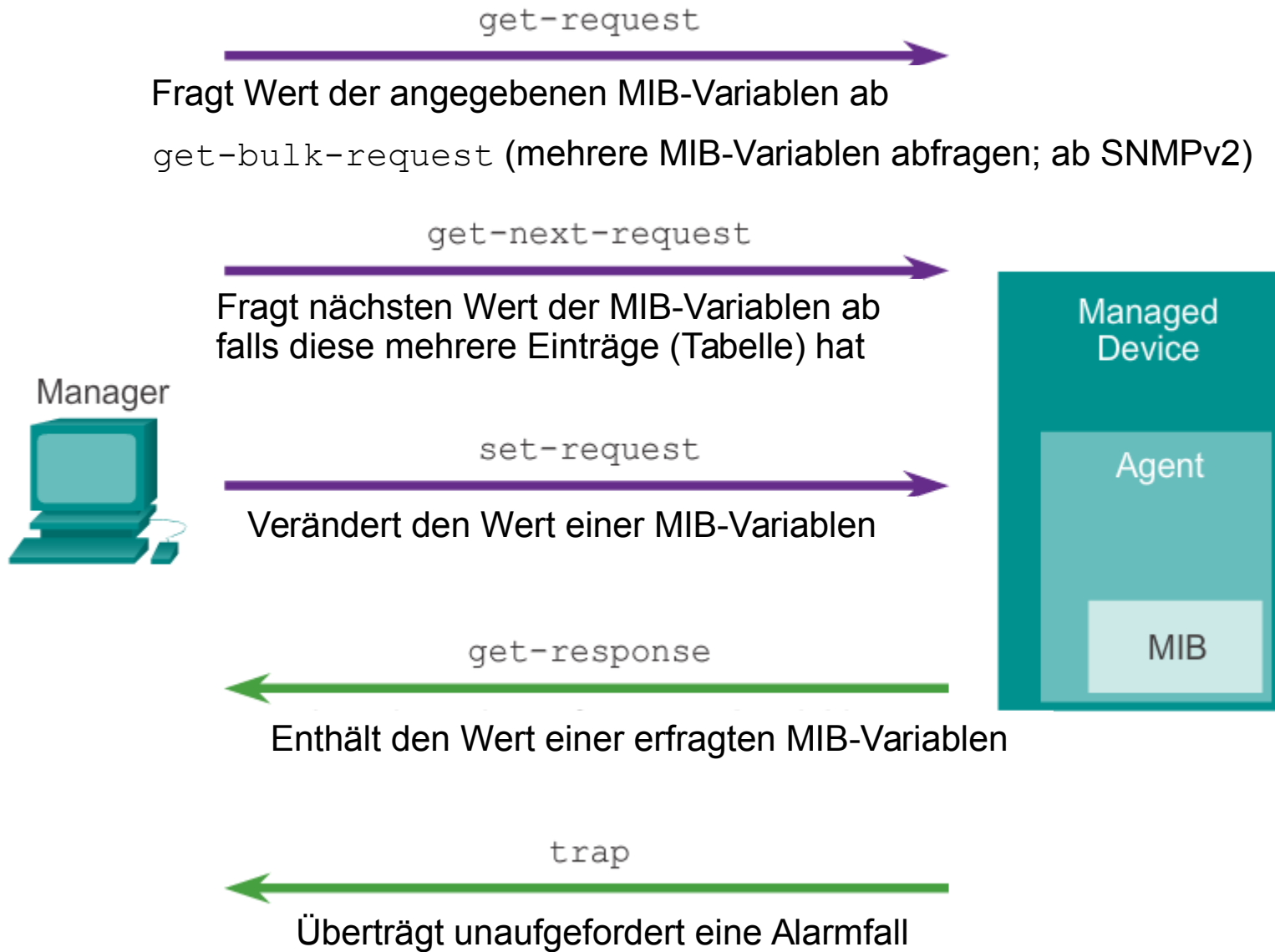
Einträge der Geräte-MIBs mit SNMP-“get“ abfragbar. Objekte die auch Schreibzugriff erlauben können mit SNMP-“set“ verändert werden.

Jedes der SNMP-fähigen Netzgeräte speichert Zustandsinformationen lokal in seiner eigenen **Management Information Base (MIB)**, einer internen Datenstruktur / Datenbank.

Besondere Ereignisse kann Netzwerk-Gerät via SNMP-“trap“ selbständig an NMS melden!



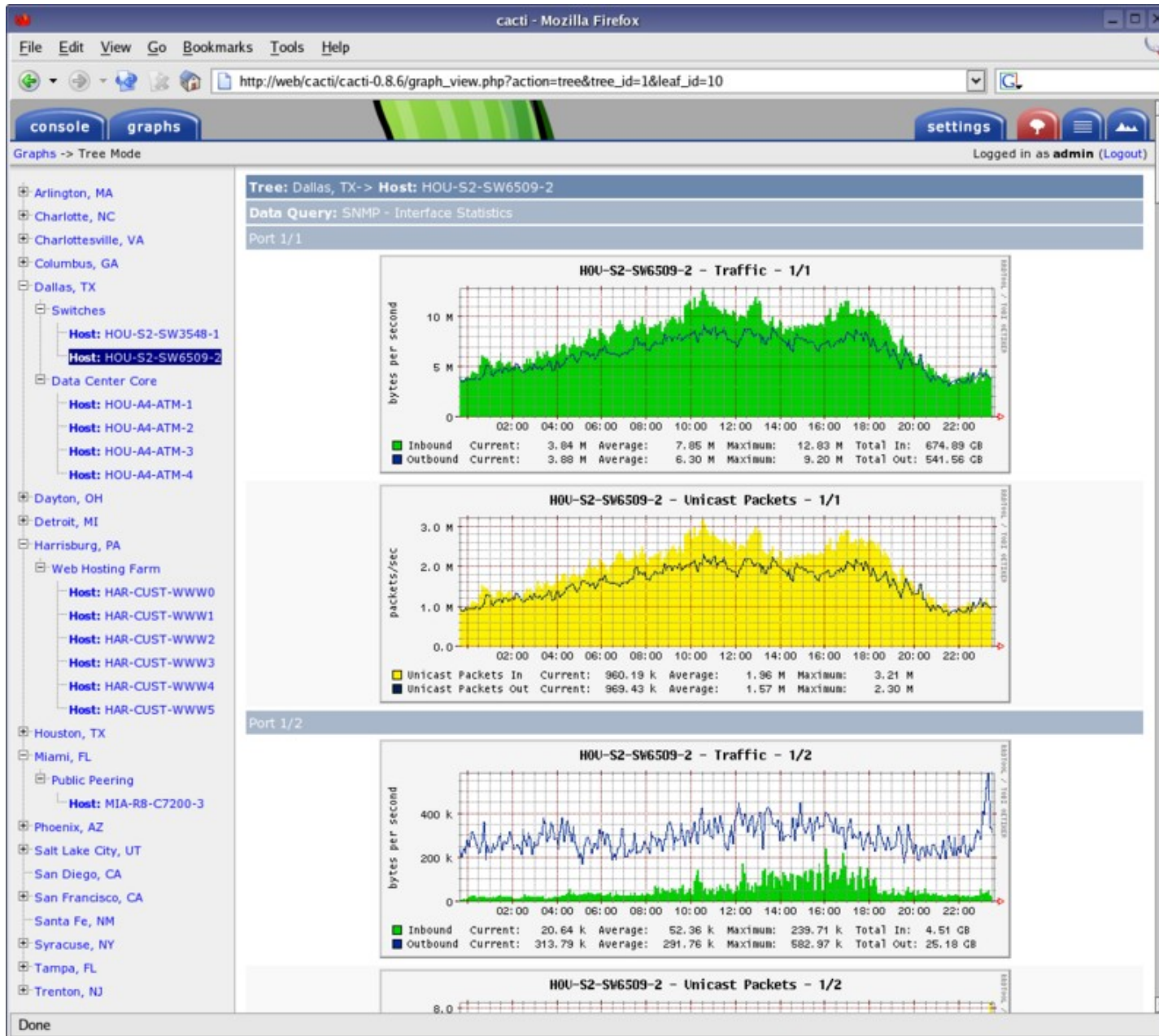
SNMP-Operationen



trap-Liste C2960: auth-framework, bridge, call-home, cluster, config, config-copy, config-ctid, copy-config, cpu, dot1x, energywise, entity, envmon, errdisable, flash, fru-ctrl, ipsla, mac-notification, port-security, power-ethernet, snmp, storm-control, stpx, syslog, transceiver, tty, vlan-membership, vlancreate, vlandelete, vstack, vtp



Periodische get-Requests ...



... erlauben es der NMS die Daten auch grafisch als Übersicht darzustellen.

Nebenstehend Ansicht der PHP-Anwendung Cacti.

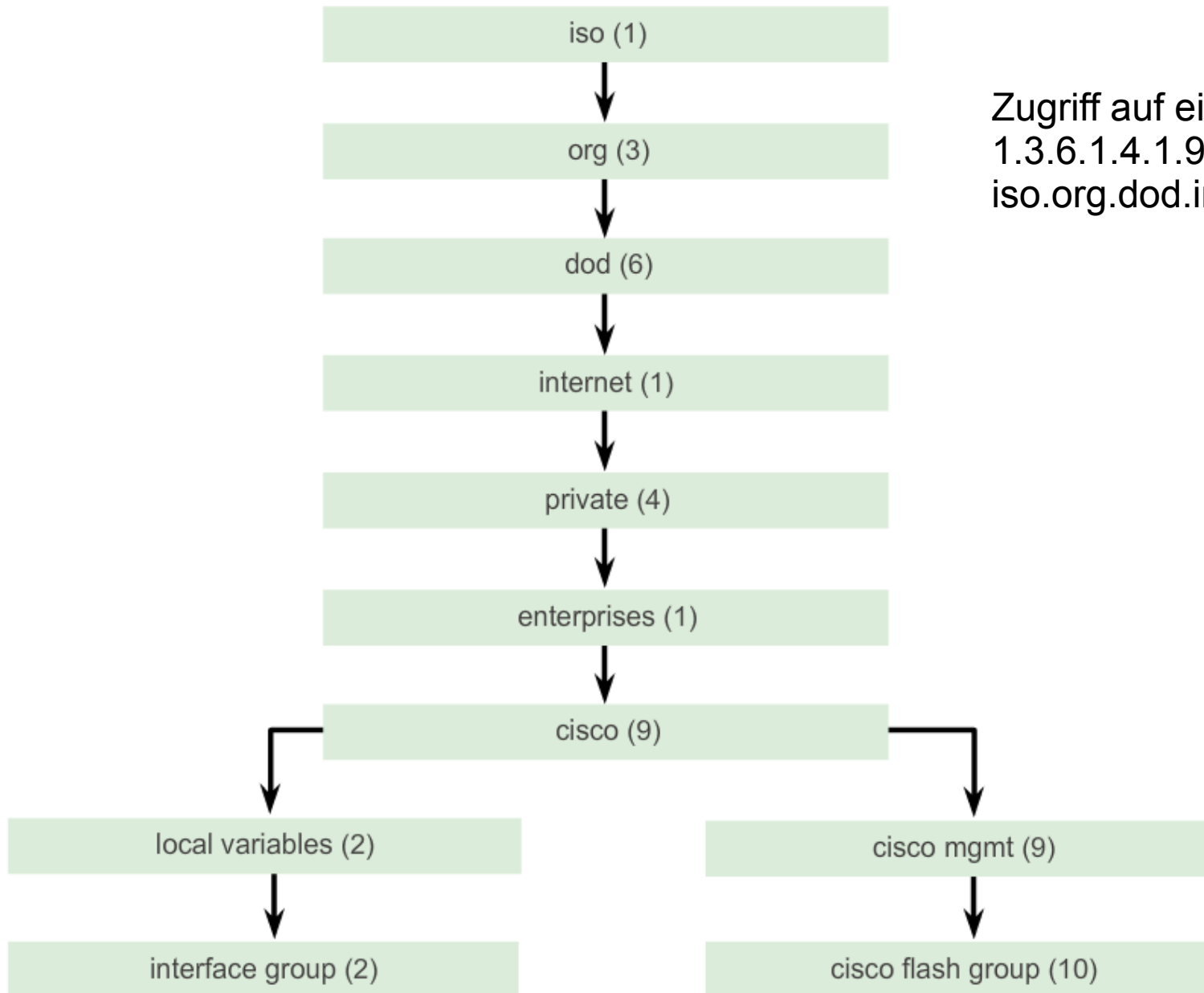
Für dringende Ereignisse ist periodisches Polling zu selten / langsam. Erhöhung der Frequenz ist ein Bandbreitenproblem.

Deshalb → Traps vom Gerät an NMS ohne Get-Request.



Quelle: <http://www.cacti.net/>

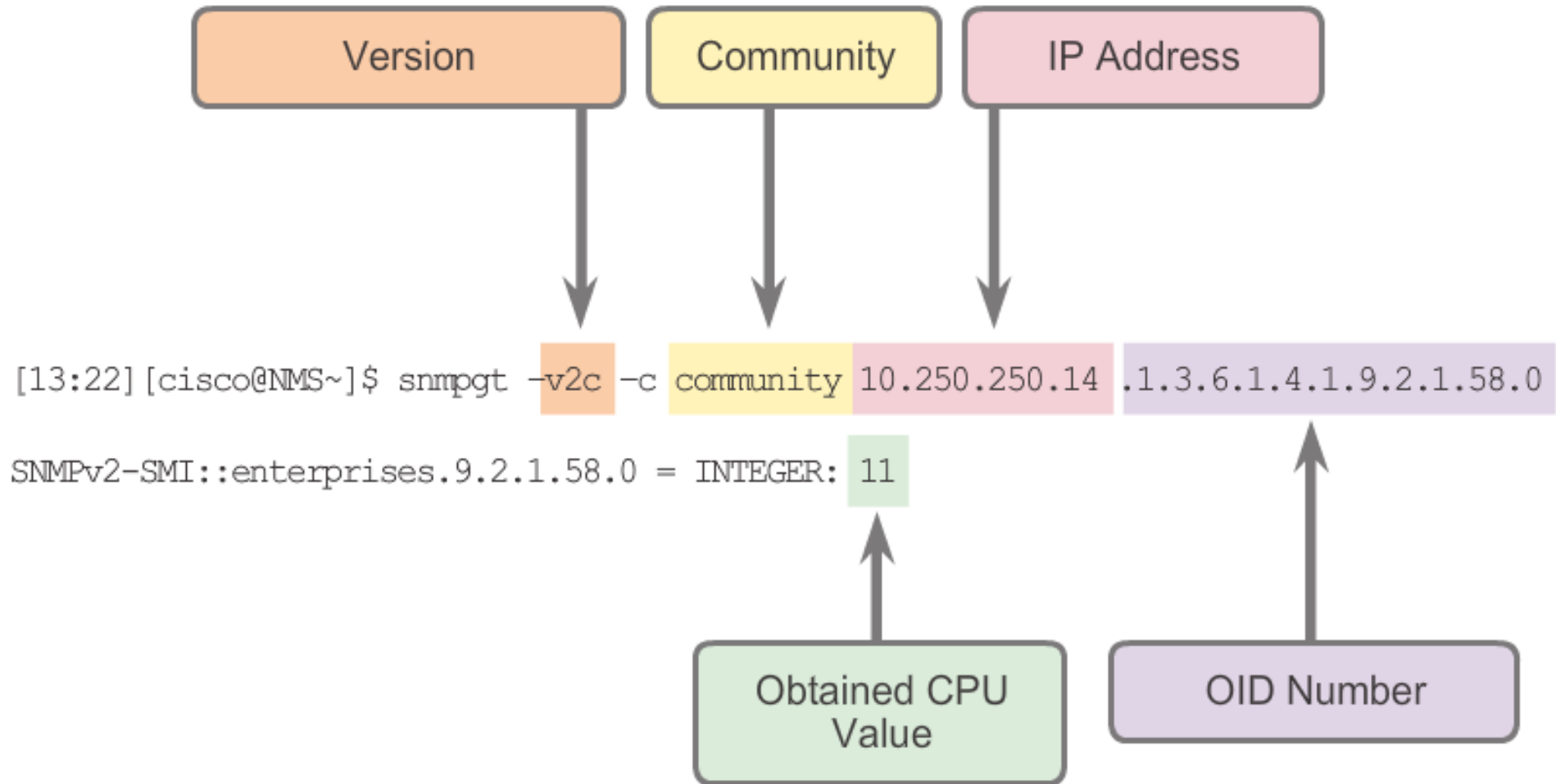
Organisation der MIB Objekte als Baumstruktur



Zugriff auf einzelne Objekte:
1.3.6.1.4.1.9. ... oder
iso.org.dod.internet. ...



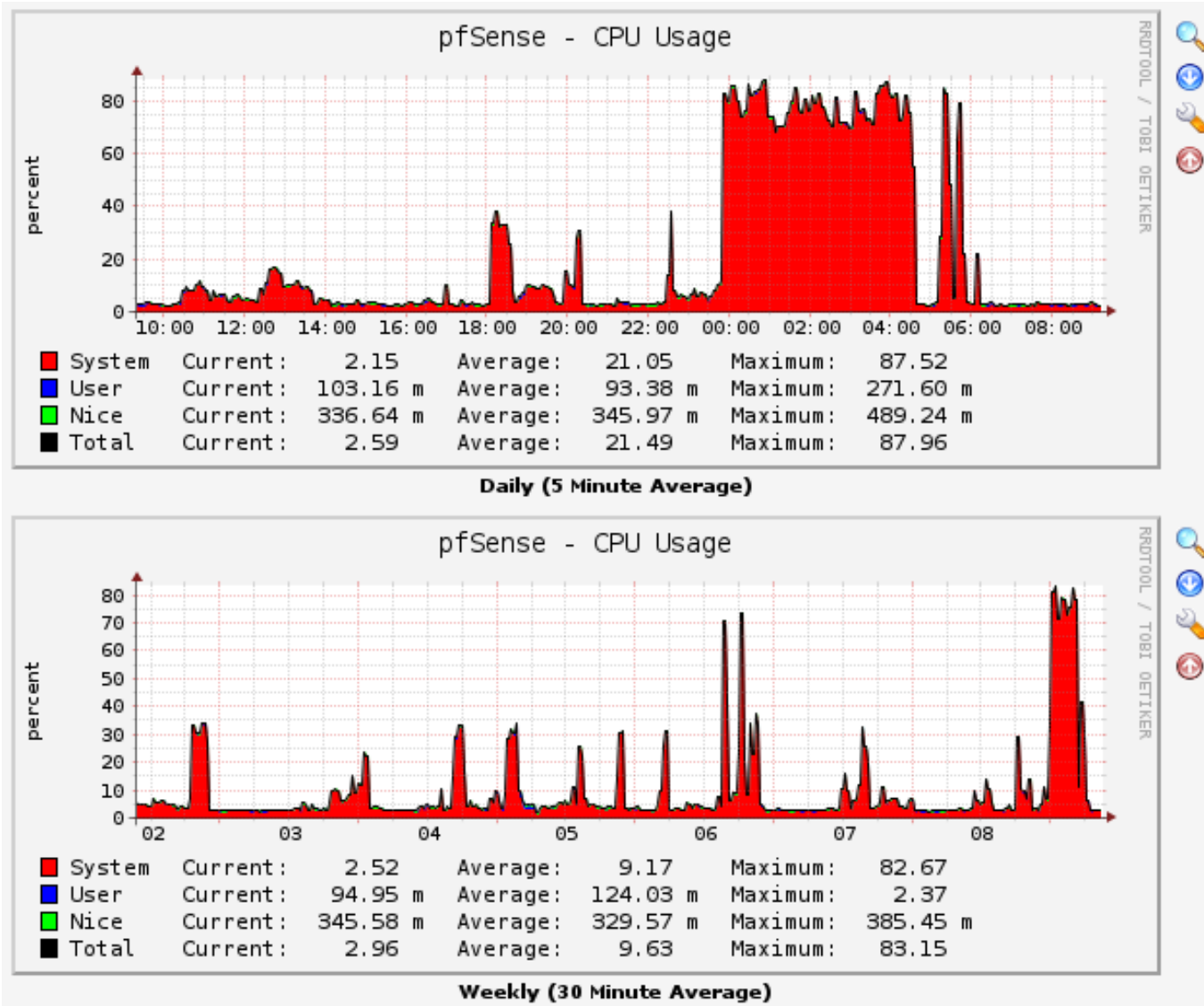
Shell- bzw. Skriptzugriff auf OID mit „snmpget“



Download für verschiedene Plattformen (auch Windows) → Link zu Sourceforge folgen:
<http://www.net-snmp.org/download.html> oder über Paketverwaltung Ihres Betriebssystems



Darstellung am Beispiel der CPU-Auslastung



Monitoring vieler weitere Werte, z.B. Netz- bzw. Interfaceauslastung, Festplattenbelegung, ... erlauben raschen Überblick über einzelne Geräte, Netze, gesamte Infrastruktur

Neben Cacti, das nur vergleichsweise einfaches Monitoring erlaubt, sind aktive, „große“ Netzwerk-Management-Werkzeuge z.B. Nagios, Icinga, Zabbix, ...

SNMP-Object-Navigator ist z.B. bei Cisco verfügbar:
<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do>



SNMP Objekt Navigator von Cisco

<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do>



Products

Tools & Resources

SNMP Object Navigator

[HOME](#)

[SUPPORT](#)

[TOOLS & RESOURCES](#)

SNMP Object Navigator

TRANSLATE/BROWSE

SEARCH

DOWNLOAD MIBS

MIB SUPPORT - SW

Translate

[Browse The Object Tree](#)

Translate OID into object name or object name into OID to receive object details

Enter OID or object name:

Translate

examples -
OID: 1.3.6.1.4.1.9.9.27
Object Name: ifIndex

Object Information

Specific Object Information

Object	avgBusy5
OID	1.3.6.1.4.1.9.2.1.58
Type	INTEGER
Permission	read-only
Status	mandatory
MIB	OLD-CISCO-CPU-MIB ; - View Supporting Images
Description	"5 minute exponentially-decayed moving average of the CPU busy percentage."



Beispiel einer SNMPv2-Konfiguration

```
R1# configure terminal
! Read-only Community-String setzen
R1(config)# snmp-server community lesen ro NMSACL
! Read-Write Community-String setzen
R1(config)# snmp-server community schreiben rw NMS-MANAG-ACL
! Kontaktinfos
R1(config)# snmp-server location Landesakad. ES, S.07
R1(config)# snmp-server contact Andreas Grupp - LAK Esslingen
! Network-Management-Server definieren
R1(config)# snmp-server host 10.1.198.223 version 2c lesen
R1(config)# snmp-server enable traps [notification types]
```

Ohne dieses Kommando keinerlei „Traps“ - nur Polling durch NMS.
Ohne Trap-Notification-Types werden alle aktiviert (siehe Folie 11)!

```
R1(config)# ip access-list standard NMSACL
R1(config-std-nacl)# permit 10.1.198.223
R1(config-std-nacl)# ip access-list standard NMS-MANAG-ACL
R1(config-std-nacl)# ...
```

Konfiguration einer ACL die es nur noch den Workstations der Administration erlaubt in dieser Form per SNMP „schreibend“ zuzugreifen!



Überprüfung der Konfiguration von SNMPv2

```
S2#show snmp
Chassis: FCQ1646Y6YY
Contact: Andreas Grupp
Location: Unter dem Schreibtisch (Testzwecke)
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Input queue packet drops (Maximum queue size 1000)
24 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  24 Trap PDUs
SNMP global trap: enabled

SNMP logging: enabled
  Logging to 172.16.0.232.162, 0/10, 7 sent, 0 dropped.
SNMP agent enabled
```



Überprüfung der Konfiguration von SNMPv2

```
S2#show snmp community
```

```
Community name: SeCrEt-lesen  
Community Index: SeCrEt-lesen  
Community SecurityName: SeCrEt-lesen  
storage-type: nonvolatile          active
```

```
Community name: SeCrEt-lesen@1  
Community Index: SeCrEt-lesen@1  
Community SecurityName: SeCrEt-lesen  
storage-type: read-only          active
```

```
S2#debug snmp ?
```

```
cef          SNMP CEFMIB Errors  
energywise  SNMP ENERGYWISE MIB Errors  
headers     SNMP packet headers  
packets     SNMP packets  
requests    SNMP requests  
sessions    SNMP sessions  
timers      SNMP timer activity
```



- Bis incl. Version 2c → Klartext Community-Strings.
 - komplexe Strings verwenden
 - regelmäßig ändern
 - insbesondere bei Personalwechsel der Admins
- Über ACLs regeln woher überhaupt auf die SNMP-Engine zugegriffen werden kann / wohin überhaupt SNMP-Messages gehen können
- Nach Möglichkeit aber authentifiziertes und verschlüsseltes SNMP v3 verwenden

SNMP-fähige Geräte z.B. mit Metasploit scannen

```
=[ metasploit v4.11.4-2015090201 ]
+ -- ---[ 1476 exploits - 852 auxiliary - 239 post ]
+ -- ---[ 432 payloads - 37 encoders - 8 nops ]
+ -- ---[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/snmp/snmp_login
msf auxiliary(snmp_login) > set RHOSTS 10.1.0.0/16
RHOSTS => 10.1.0.0/16
msf auxiliary(snmp_login) > set THREADS 10
THREADS => 10
msf auxiliary(snmp_login) > set PASS_FILE /usr/share/metasploit-framework/data/...
PASS_FILE => /usr/share/metasploit-framework/data/wordlists/snmp_default_pass.txt
msf auxiliary(snmp_login) > run
```

Bei (zu) vielen Herstellern ist SNMP nicht nur als Fähigkeit an Bord, sondern per Default schon aktiviert und sträflich mit herstellerspezifischen „well-known“ Community-Strings versehen

```
...
[+] 10.1.2.3:161 - LOGIN SUCCESSFUL: s!a@m#n$p%c (Access level: read-write); Proof
(sysDescr.0): Samsung ML-4550 Series; OS 1.01.30.104 10-01-2008;Engine 1.00.39;NIC
V3.03.09 (ML-4550) 09-30-2008; 4921B1AQC00323T
...
```

Und damit beginnt nun der große „Spaß“!



Grafische SNMP-Werkzeuge – z.B. gut für SET-Cmd.

Skripting über Net-SNMP-Werkzeuge unschlagbar.

Für das Setzen einzelner Werte, oder das Blättern in den möglichen Werten, GUI-Tools evtl. leichter.

Options

General | Default Values | Agents | MIB Files

IP Address	Port	Version	Read Community	Write Community
10.0.0.241	161	2	*****	*****
127.0.0.1	161	1		

The screenshot shows the iReasoning MIB Browser interface. On the left, a MIB tree is expanded to show the 'system' folder and its sub-objects, including 'ifAdminStatus'. The main window displays a 'Result Table' with columns for Name/OID, Value, Type, and IP:Port. The table contains multiple rows for 'ifOutErrors' with a value of 0 and type 'Counter32'. An 'SNMP SET' dialog box is open in the foreground, showing the OID '.1.3.6.1.2.1.2.2.1.7.10013', Data Type 'Integer', and Value '2'. The dialog has 'Ok' and 'Cancel' buttons.

Beispielsoftware:
iReasoning MIB Browser
(kann in der Free-Edition
leider kein SNMPv3)



- Frei unter <http://www.net-snmp.org/> oder direkt über Paketverwaltung Ihres Betriebssystems
- Stellt einige Shell-Befehle zur Verfügung (DOS-Fenster, bash, ...)
- Ist damit skriptbar (Batchdatei, Shellskript, ...)

- **Beispiele:**

```
snmpwalk -v 2c -c public 172.16.0.200
```

```
snmpset -v 2c -c private 172.16.0.200
```

```
IF-MIB::ifAdminStatus.10017 i 2
```

SNMP-Sicherheits-Modi und Levels / Versionen

Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2C	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication.
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: <ul style="list-style-type: none">• DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.• 3DES 168-bit encryption• AES 128-bit, 192-bit, or 256-bit encryption

Quelle: cisco.com → Catalyst 2960 and 2960-S Switches Software Configuration Guide, Release 15.0(1)SE

Authentifizierung bei SNMPv1 und v2c: Nur über „Community Strings“ im Klartext (!!!).
Ein String für reinen Lesezugriff (RO), ein weiterer String für Lese-/Schreibzugriff (RW)



Einfache SNMPv3-Konfig. (am Bsp. eines C2960)

Die üblichen Standard-Informationen analog zu SNMPv2

```
SNMP-Sw(config)#snmp-server location Landesakad. ES, S.07
SNMP-Sw(config)#snmp-server contact Andreas
                               Grupp - LAK Esslingen
```

ACL zur Einschränkung von wo aus zugegriffen werden darf

```
SNMP-Sw(config)#ip access-list standard SNMPACL
SNMP-Sw(config-std-nacl)#permit 192.168.100.0 0.0.0.255
```

Definition eines Views „ISO“ – quasi View-Based Access Model (VACM)

```
SNMP-Sw(config)#snmp-server view ISO iso included
```

Definition einer Benutzergruppe „ADMINS“ & Kopplung an View „ISO“

```
SNMP-Sw(config)#snmp-server group ADMINS
                               v3 priv read ISO access SNMPACL
```

Definition des Users „grupp“ in Gruppe „ADMINS“ & und Festlegung des SNMPv3 Sicherheits-Levels „authPriv“

```
SNMP-Sw(config)#snmp-server user grupp ADMINS v3 auth sha
                               GanzGeHeim priv aes 128 SuperGeHeim
```



Schritte zur Konfiguration von SNMPv3 sind somit ...

- 1) Passende ACL definieren die SNMP-Managern den Zugriff erlaubt
- 2) Einen SNMP-View definieren der regelt auf welche Teile der MIB zugegriffen werden darf
- 3) SNMP-User-Gruppe anlegen, und festlegen
 - welcher „View“ und welche ACL assoziiert sind
 - ob Lese- oder Schreibzugriff
- 4) User anlegen, einer Gruppe zuordnen und den Security-Level (noauthNopriv, authNopriv, authPriv) festlegen – ggf. mit Passwörtern



Beispiel: SNMPv3-Abfrage via Kommandozeile

Die Monitoring-Tools verwenden im Hintergrund oft (immer?) die Net-SNMP-Tools → die können „nur“ AES-128!

Bridging-Course sagt deshalb: Nur AES-128 verwenden!

User-Namen, Hashing-Verfahren f. User-Authen. und -Passwort, sowie Verschlüsselungsverfahren für Datenteil und Verschl.-Passwort

```
snmpget -v3 -u grupp -l AuthPriv -a SHA -A GanzGeHeim  
-x AES -X SuperGeHeim 172.16.0.213 1.3.6.1.2.1.1.6.0
```

Ergebnis dieser Abfrage ist dann z.B.:

```
SNMPv2-MIB::sysLocation.0 = STRING: Landesakad. ES, S.07
```

```
snmpwalk -v3 -u grupp -l AuthPriv -a SHA -A GanzGeHeim  
-x AES -X SuperGeHeim 172.16.0.213 1.3.6.1.2.1.1
```



Mitgeschnittene SNMPv3-PDU – authPriv-Mode

```
▶ Frame 1: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits)
▶ Ethernet II, Src: Micro-St_19:b0:c1 (d4:3d:7e:19:b0:c1), Dst: CiscoInc
▶ Internet Protocol Version 4, Src: 172.16.0.131 (172.16.0.131), Dst: 172
▶ User Datagram Protocol, Src Port: 33260 (33260), Dst Port: 161 (161)
▼ Simple Network Management Protocol
  msgVersion: snmpv3 (3)
  ▶ msgGlobalData
  ▶ msgAuthoritativeEngineID: 800000090300001a6dfc4181
  msgAuthoritativeEngineBoots: 5
  msgAuthoritativeEngineTime: 8725
  msgUserName: grupp
  msgAuthenticationParameters: 9bb5e0540f968535fe3a2c75
  msgPrivacyParameters: ceaa3682639fe0ae
  ▼ msgData: encryptedPDU (1)
    encryptedPDU: 8495df2d88229f8513e7b19979217f73a621a8e98e62b20d...
```

User-Namen
(od. Security Name)

Verschlüsselter
Datenteil



Kontrolle der SNMP-Einstellungen

```
SNMP-Sw#show snmp group
```

```
groupname: ADMINS                security model:v3 priv  
contextname: <no context specified> storage-type: nonvolatile  
readview : ISO                    writeview: <no writeview specified>  
notifyview: <no notifyview specified>  
row status: active              access-list: SNMPACL
```

```
SNMP-Sw#show snmp user
```

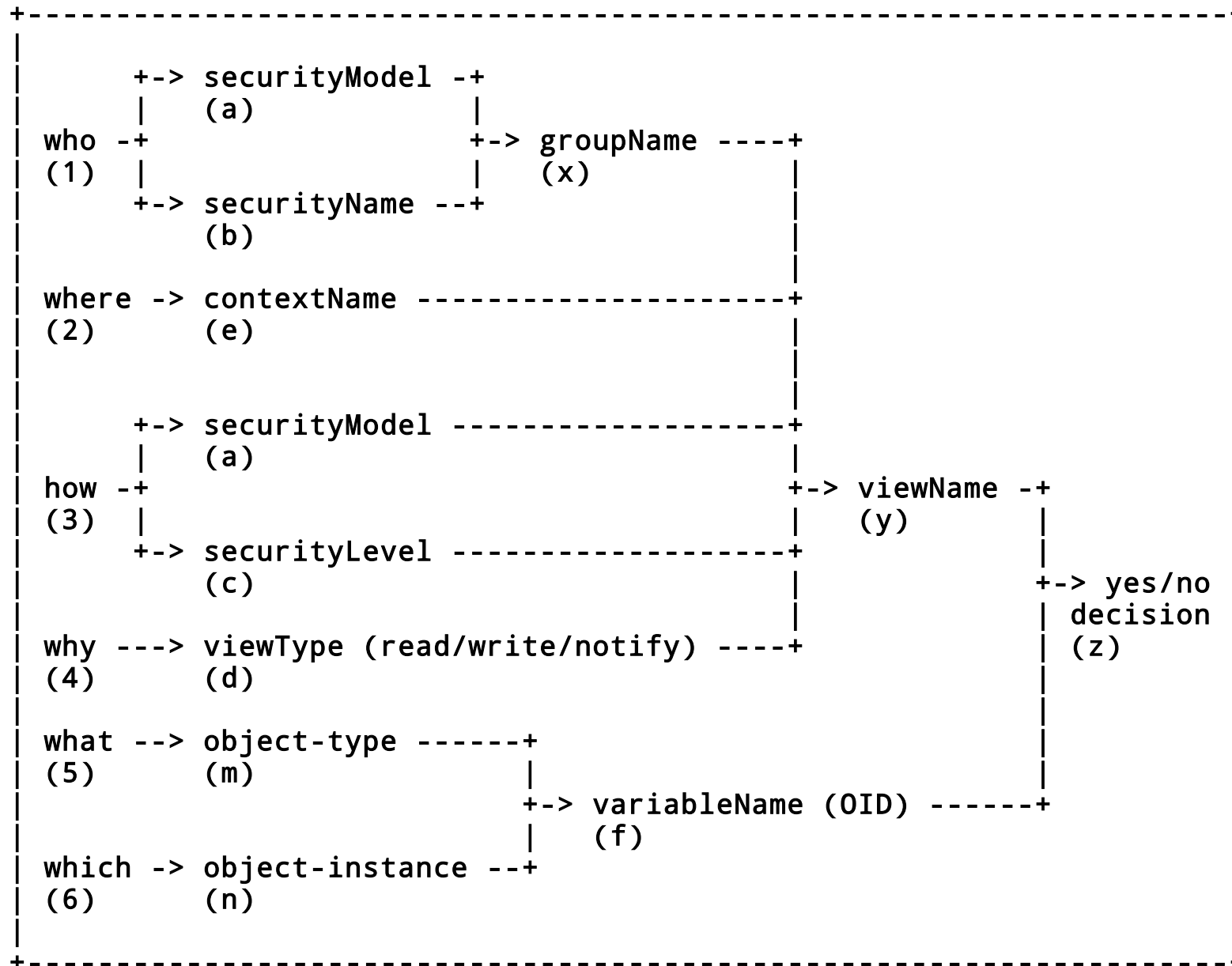
```
User name: grupp  
Engine ID: 800000090300001A6DFC4181  
storage-type: nonvolatile          active  
Authentication Protocol: SHA  
Privacy Protocol: AES128  
Group-name: ADMINS
```



- Es werden „nur“ Sicherheits-Features nachgerüstet → restliches Protokoll bleibt wie gehabt
- Statt „Manager“ u. „Agents“ → SMTP-Entities
- Usernamen wird oft als „Security Name“ bezeichnet – z.B. in Monitoring-Systemen
- Passwörter müssen lt. Standard mind. 8 Zeichen Länge haben → fehlt im Bridging-Course aktuell
- Zugriffsberechtigung → komplexe Modelle:
 - USM - "User-based Security Model"
 - VACM - "View-based Access Control Model"



"View-based Access Control Model" nach RFC 3415



- Net-SNMP – essentiell für
 - Kontrollen via CLI, Demos (z.B. Port an/aus), ...
 - In vielen grafischen od. webbasierten Werkzeugen das eigentliche Arbeitstier im Hintergrund
- iReasoning MIB Browser – kann in der freien Version kein SNMPv3
- Cacti – webbasierendes Tool
- Nagios, Icinga, Zabbix – web-basierende Werkzeuge. Auch Monitoring von Servern, Diensten ... über maßgeschneiderte Clients



Monitoring mit Zabbix

ZABBIX

The Enterprise-class Monitoring Solution for Everyone

日本語 | Русский

Customer Login ▶

Product

Solutions

Services

Training

Partners

Download

Community

About Us

MONITORING SOLUTION
THAT CONTINUES TO SURPRISE

ZABBIX 3.2

Learn More

Next Webinars

6 Apr - Italian - Panoramica di sistema
7 Apr - German - Zabbix advanced - Erweiterte Remote Ko...
11 Apr - German - Wie Netzwerkmonitoring Kosten senkt

Upcoming Trainings

3 - 7 April 2017, Brazil
10 - 14 April 2017, Argentina
10 - 12 April 2017, Italy



Contact Sales

USA: 1-877-4-ZABBIX
Europe: +371-6778-4742
Japan: 03-4405-7338

The Ultimate Enterprise-class Monitoring Platform

Zabbix is the ultimate enterprise-level software designed for real-time monitoring of millions of metrics collected from tens of thousands of servers, virtual machines and network devices.
Zabbix is Open Source and comes at no cost.



- Mit den meisten Systemen zu komplex und nicht realisierbar
- Mein Favorit → Zabbix
 - Echtes Open-Source – alle Features frei verfügbare
 - Fertige, funktionsfähige VMs downloadbar
 - SNMP- und Agentbasierendes Monitoring

Macros in Zabbix – vererben sich auf alle Objekte

2.) **ZABBIX** Monitoring Inventory Reports Configuration **Administration** 1.)

General Proxies Authentication User groups Users Media types Scripts Queue Zabbix Appliance

Macros 3.) Macros

Macro	Value	
<input data-bbox="421 762 825 810" type="text" value="{SNMP_AUTHPW}"/>	= <input data-bbox="868 762 1364 810" type="text" value="sehrgeheim2"/>	Remove
<input data-bbox="421 834 825 882" type="text" value="{SNMP_COMMUNITY}"/>	= <input data-bbox="868 834 1364 882" type="text" value="public"/>	Remove
<input data-bbox="421 906 825 954" type="text" value="{SNMP_PRIVPW}"/>	= <input data-bbox="868 906 1364 954" type="text" value="sehrgeheim1"/>	Remove
<input data-bbox="421 978 825 1026" type="text" value="{SNMP_USER}"/>	= <input data-bbox="868 978 1364 1026" type="text" value="username"/>	Remove

[Add](#)

4.) zwei der Macros sind schon vordefiniert, die anderen beiden passen zu meinen Templates für SNMPv3 (siehe später) und sollten bei Bedarf ergänzt werden!



Vorkonfigurierte Geräte-Templates

1.)

ZABBIX Monitoring Inventory Reports Configuration Administration

Host groups Templates Hosts Maintenance Actions Event correlation Discovery IT services Zabbix Appliance

Templates 2.) Group Templates Create template Import

Filter ▲

Name

Apply Reset

<input type="checkbox"/>	Name ▲	Applications	Items	Triggers	Graphs	Screens	Discovery	Web	Linked templates	Linked to
<input type="checkbox"/>	Template App FTP Service	Applications 1	Items 1	Triggers 1	Graphs	Screens	Discovery	Web		

Bei der Durchsicht findet man die SNMPv1 bzw. SNMPv2-Templates sofort. SNMPv3-Templates fehlen in der aktuellen Version.

Gerade bei den SNMP-Templates kann man in dieser Übersicht dann aber auch die Abhängigkeiten erkennen. So ist z.B. „SNMP Device“ aus den beiden Templates „SNMP Generic“ und „SNMP Interfaces“ zusammengesetzt.

Damit hat „SNMP Device“ auch die „Items“- und die „Discovery“-Regeln geerbt.



Leider fehlen SNMPv3-Templates – hier Selfmade

<input type="checkbox"/>	Template SNMP Processors	Applications 1	Items	Triggers	Graphs	Screens	Discovery 1	Web	
<input type="checkbox"/>	Template SNMPv3 Device	Applications 2	Items 6	Triggers	Graphs	Screens	Discovery 1	Web	Template SNMPv3 Generic, Template Interfaces
<input type="checkbox"/>	Template SNMPv3 Disks	Applications 1	Items	Triggers	Graphs	Screens	Discovery 1	Web	
<input type="checkbox"/>	Template SNMPv3 Generic	Applications 1	Items 5	Triggers	Graphs	Screens	Discovery	Web	
<input type="checkbox"/>	Template SNMPv3 Interfaces	Applications 1	Items 1	Triggers	Graphs	Screens	Discovery 1	Web	
<input type="checkbox"/>	Template SNMPv3 OS Linux	Applications 4	Items 6	Triggers	Graphs	Screens	Discovery 3	Web	Template SNMPv3 Disks, Template SI Generic, Template SNMPv3 Interfaces SNMPv3 Processors
<input type="checkbox"/>	Template SNMPv3 OS Windows	Applications 4	Items 6	Triggers	Graphs	Screens	Discovery 3	Web	Template SNMPv3 Disks, Template SI Generic, Template SNMPv3 Interfaces SNMPv3 Processors
<input type="checkbox"/>	Template SNMPv3 Processors	Applications 1	Items	Triggers	Graphs	Screens	Discovery 1	Web	

„Items“ sind die SNMP-Datenquellen / SNMP-OIDs die vordefiniert im Template enthalten sind.

„Discovery“-Regeln sind sehr mächtige, vordefinierte Werkzeuge. Sie erlauben es z.B. auf Basis der bei einem konkreten Gerät erkannten Interface-Anzahl, für jedes Interface vollautomatisch weitere „Items“ in das konkrete Gerät einzufügen!

In Templates → „Items“ die Datenquellen entsprechen

ZABBIX Monitoring Inventory Reports Configuration Administration

Host groups Templates **Hosts** Maintenance Actions Event correlation Discovery IT services

Items

All templates / Template SNMPv3 OS Linux Applications 4 **Items 6** Triggers Graphs Screens Discovery rules 3 Web scenarios

Filter ▲

Host group Type Type of information State

Host Update interval (in sec) History (in days)

Application Trends (in days) Triggers

Name

Key Template

Subfilter affects only filtered data

APPLICATIONS
[General 5](#) [Interfaces 1](#)

TYPE OF INFORMATION
[Character 4](#) [Numeric \(unsigned\) 2](#)

<input type="checkbox"/> Wizard	Name ▲	Triggers	Key	Interval	History	Trends	Type	Applications	Status
<input type="checkbox"/>	... Template SNMPv3 Generic: Device contact details		sysContact	1m	7d		SNMPv3 agent	General	Enabled
<input type="checkbox"/>	... Template SNMPv3 Generic: Device description		sysDescr	1m	7d		SNMPv3 agent	General	Enabled
<input type="checkbox"/>	... Template SNMPv3 Generic: Device location		sysLocation	1m	7d		SNMPv3 agent	General	Enabled
<input type="checkbox"/>	... Template SNMPv3 Generic: Device name		sysName	1m	7d		SNMPv3 agent	General	Enabled
<input type="checkbox"/>	Template SNMPv3 Generic: Device uptime		sysUpTime	1m	7d	365d	SNMPv3 agent	General	Enabled
<input type="checkbox"/>	Template SNMPv3 Interfaces: Number of network interfaces		ifNumber	1m	7d	365d	SNMPv3 agent	Interfaces	Enabled

Displaying 6 of 6 found



Konfiguration eines Items – mit Bezug zu Macros

ZABBIX

Monitoring Inventory Reports Configuration Administration

Host groups Templates Hosts Maintenance Actions Event correlation Discovery IT services

Items

All templates / Template SNMPv3 OS Linux Applications 4 Items 6 Triggers Graphs Screens Discovery rules 3 Web scenarios

Parent items [Template SNMPv3 Generic](#)

Name

Type

Key

SNMP OID

Context name

Security name

Security level

Authentication protocol

Authentication passphrase

Privacy protocol

Privacy passphrase

Port

Type of information

Update interval (in sec)



Neues SNMP-Device anlegen ...

ZABBIX

Monitoring Inventory Reports Configuration Administration

Host groups Templates Hosts Maintenance Actions Event correlation Discovery IT services

Hosts

All hosts / Catalyst 2960 Enabled ZBX SNMP JMX IPMI Applications 2 Items 230 Triggers 28 Graphs 28 Discovery rules 1 Web scenarios

Host Templates IPMI Macros Host inventory Encryption

Host name 172.16.0.213

Visible name Catalyst 2960

Groups In groups

Switches

Other groups

Discovered hosts
Hypervisors
Linux servers
Templates
Virtual machines
Zabbix servers

New group

Agent interfaces IP address DNS name Connect to Port Default

[Add](#)

Das „Zabbix“-Agent-Interface wird bei einem reinem SNMP-Gerät nicht benötigt und wurde hier gelöscht! Dafür wurde ein „SNMP-Interface“ hinzugefügt.

SNMP interfaces

172.16.0.213 IP DNS 161 [Remove](#)

Use bulk requests

[Add](#)



Vor dem Speichern passendes Template hinterlegen

ZABBIX Monitoring Inventory Reports Configuration Administration

Host groups Templates **Hosts** Maintenance Actions Event correlation Discovery IT services

Hosts

All hosts / Catalyst 2960 Enabled ZBX **SNMP** JMX IPMI Applications 2 Items 230 Triggers 28 Graphs 28 Discovery rules 1 Web scen

Host **Templates** IPMI Macros Host inventory Encryption

Linked templates	Name	Action
	Template SNMPv3 Device	Unlink Unlink and clear

Link new templates

type here to search

[Add](#)

Rückgriff auf passendes Template – hier ein selbstdefiniertes SNMPv3 Template



Sofern abweichende Werte → Macros ggf. anpassen

Andernfalls werden geerbte Werte aus den generellen Einstellungen verwendet.

The screenshot shows the Zabbix web interface. At the top, there is a navigation bar with the ZABBIX logo and menu items: Monitoring, Inventory, Reports, Configuration, and Administration. Below this is a sub-navigation bar with Host groups, Templates, Hosts, Maintenance, Actions, Event correlation, Discovery, and IT services. The main content area is titled 'Hosts' and shows a breadcrumb trail: All hosts / Catalyst 2960 / Enabled / ZBX / SNMP / JMX / IPMI. Below the breadcrumb, there are statistics for Applications 2, Items 230, Triggers 28, Graphs 28, and Discovery rules 1. A sub-menu is open for 'Macros', showing 'Host macros' and 'Inherited and host macros'. The 'Host macros' section contains a table with three entries:

Macro	Value	
{SNMP_AUTHPW}	GanzGeHeim	Remove
{SNMP_PRIVPW}	SuperGeHeim	Remove
{SNMP_USER}	grupp	Remove

Below the table is an 'Add' link and a row of buttons: Update, Clone, Full clone, Delete, and Cancel.

Beachten Sie die Fülle an autom. eingefügten Items, Graphen, Trigger! (auf Basis der Template-Discovery-Regel!)

Wenn alles stimmt, wird der Host als „grün“ angezeigt – Dauert ein wenig ...

Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encry
C2960-Demo	Applications 2	Items 230	Triggers 28	Graphs 28	Discovery 1	Web	192.168.100.100:161	Template SNMPv3 Device (Template SNMPv3 Generic, Template SNMPv3 Interfaces)	Enabled	ZBX SNMP JMX IPMI	NONE

**Fragen
???**

