Vorlesung 1

Was sind die idealen Umweltbedingungen für einen Rechenzentrum Standort? Welche Umwelt Risiken gibt es?

Bei Neubau:

nicht neben

- Flüssen (Hochwassergefahr)
- Flughäfen, Bahnhöfen (elektromagnetische Störungen)
- Unwetterzonen
- feuergefährdete Betriebsstätten wie Tankstellen sowie Öl-, Gas- und Chemikalienlager
- Terrorgefährdeten Zonen
- Smog belasteten Gebieten (Filter!)

wichtig

- Stromversorgung (alternative Energie?, Redundanz)
  Internetanbindung (redundanz)
- kühles Klima (im Norden)
- Abwärme Nutzen

In bestehenden Gebäuden

keine Wasserrohre (Heizung, Ab und Zuwasser)
Luftfeuchtigkeit nicht zu hoch (Wasser leitet Wärme besser, Gefahr der elektrostatischen Ladung) und nicht zu niedrig

In welchen Anwendungsfällen macht ein BUS- System Sinn? (!!!)

Stern Topologie

Nachteile:

- bei Ausfall der Schaltzentrale ist keine Kommunikation mehr möglich (Single point of failure)
- sehr hohe Verkabelungskosten (+Kosten für Switches)

Vorteile:

- sehr einfache und kostengünstige Netzsteuerung und Kontrolle
- gleicher Datenbestand für alle Knoten
- sehr leicht erweiterbar
- keine Störung des Netzwerks bei Ausfall eines beteiligten Rechners

Bus-Topologie

Nachteile:

- ein Kabelbruch bedeutet den Ausfall des gesamten Netzwerks
- ein Kabelfehler ist schwer zu orten
- Netzwerkknoten teilen Bandbreite des Übertragungsmediums → Engpass
- nicht "abhörsicher" (ohne Verschlüsselung)

Vorteile:

- keine Störung des Netzwerks bei Ausfall eines beteiligten Rechners
- geringe Verkabelungskosten und in dieser Reihe kein Hub/Switch nötig
    - eignet sich gut bei langen Distanzen
- leicht erweiterbar

Bei der Auswahl der Topologie ist vor allem folgendes zu beachten:

- Welche Bandbreite wird benötigt?
- Welche Verkabelung ist möglich, wird angestrebt?
- Macht Wlan sinn?
- Was soll das System kosten?
- Welche Frequenz?
- ...

Das OSI 7 Schichten Modell? (!!!)

All - People - Seem - To - Need - Data - Packets

1. **Physical Layer:**
   Aufgaben: Maßnahmen und Verfahren zur Übertragung von Bitfolgen. Umwandlung der Bits in ein zum Medium passendes Signal und physikalische Übertragung.
   Hardware: Serielle Schnittstellen, Ethernet (physischen Teile), Token Ring (physischen Teile),..
   Hardware: Repeater, Hubs, Leitungen, Stecker
   Data: Bits

2. **Data Link Layer**
   Aufgaben: Segmentierung der Pakete in Frames und Hinzufügen von Prüfsummen.
   Protokolle: Ethernet (CSMA/CD,...), Token Ring (Protokol), MAC, ...
   Hardware: Bridge, Layer-2-Switch (Multiport-Bridge)
   PDU: Frames

3. **Network Layer**
   Aufgaben: Routing der Datenpakete zum nächsten Knoten.
   Protokolle: IP
   Hardware: Router, Layer-3-Switch (BRouter: Schaut in und arbeitet mit IP Paketen, Der Vortragende verabscheut angeblich den Ausdruck Layer-3-Switch)
   PDU: Packets

4. **Transport Layer**
   Aufgaben: Zuordnung der Datenpakete zu einer Anwendung.
   Protokolle: TCP, UDP
   PDU: Segments

5. **Session Layer**
   Aufgaben: Steuerung der Verbindungen und des Datenaustauschs.
   Protokolle: Telnet, FTP, HTTP, SMTP
   PDU: Data

6. **Presentation Layer**
   Aufgaben: Umwandlung der systemabhängigen Daten in ein unabhängiges Format.
   Protokolle: SSL
   PDU: Data

7. **Application Layer**
   Aufgaben: Funktionen für Anwendungen, sowie die Dateneingabe und -ausgabe.
   Protokolle:
   PDU: Data

Anmerkung: Protokolle der Layers 5-7 werden öfters unterschiedlich zugeordnet.

Was ist der Unterschied zwischen UDP und TCP, wann macht welche Technik Sinn?

TCP (Transmission Control Protocol):

- Ist ein verbindungsorientiertes Protokoll.
  - Zwischen den beiden Gesprächspartnern wird eine Verbindung aufgebaut, über welche die Kommunikation abgewickelt wird.
  - TCP Handshake

- Es ist garantiert, dass die Pakete in der Reihenfolge ankommen, in der sie gesendet wurden.
- Header: 20 bytes → größer als UDP
- langsamer als UDP
- Verwendung:
  - Wenn Verlässlichkeit wichtig ist
  - Geschwindigkeit weniger wichtig

UDP (Universal Datagram Protocol):

- Ist ein verbindungsloses Protokoll.
  - Entspricht dem “in die Menge Schreien”.
  - keine Verbindung, Beziehung (keine Sockets) zwischen Gesprächspartnern
- Header: 8 bytes
- schneller als TCP
- keine Garantie das Pakete ankommen, oder dass die Reihenfolge stimmt
- Verwendung:
  - Wenn Geschwindigkeit wichtig ist
  - Verlässlichkeit weniger
  - Beispiele: Streaming, online Games, Wenn ein Server viele kleine Anfragen von vielen Clients bekommt (Overhead von Verbindungsaufbau zu groß)

Funktionsweise von Evercookies?

Evercookies sind Cookies die nur sehr schwer zu löschen sind.

Zusätzlich zu einem konventionellen Cookie wird dieses auch an anderen stellen repliziert:
Session Storage, Local Storage, Global Storage und Database Storage (neue HTML5 Techniken).
In den RGB Werten von Bilddateien werden identifizierende Informationen gespeichert. Der Browser cached diese Daten welche dann mittels HTML5 Canvas-Tag wieder ausgelesen und so das Cookie rekonstruiert.
Zusätzlich wird das Cookie auch in der Browser History gespeichert.

HTTP für Management? (!!!)

Welche Anforderungen hat ein GUI für einen Manager:

1. **Funktionalität** - *"Es soll die Wahrheit anzeigen"*
2. **Zuverlässigkeit -** *"Funktionierts?"*
3. **Zeitnähe** - *"Wie oft wird die Anzeige auf dem Webbrowser aktualisiert"*

Geographische Grenzen des Smart Home?

Die Verlegung eines Hausinternen BUS Systems sollte aus Sicherheitsgründen den gesicherten Bereich des Hauses (die Hausmauern) nicht verlassen, da derartige Systeme meist über keine Security (Verschlüsselung,...) verfügen. Ein Angreifer könnte sich sonst z.B: über die Türklingel mit dem Hausnetz verbinden und Schindluder treiben.
Weiters sollte kein Wireless Netzwerk zur Steuerung eines Smart Homes verwendet werden, da hier trotzt Verschlüsselung keine Sicherheit garantiert werden kann (Reichweite geht über Hausmauern hinaus…)

Vorlesung 2

Welche 6 Stufen gibt es in der Policy Hierachie?

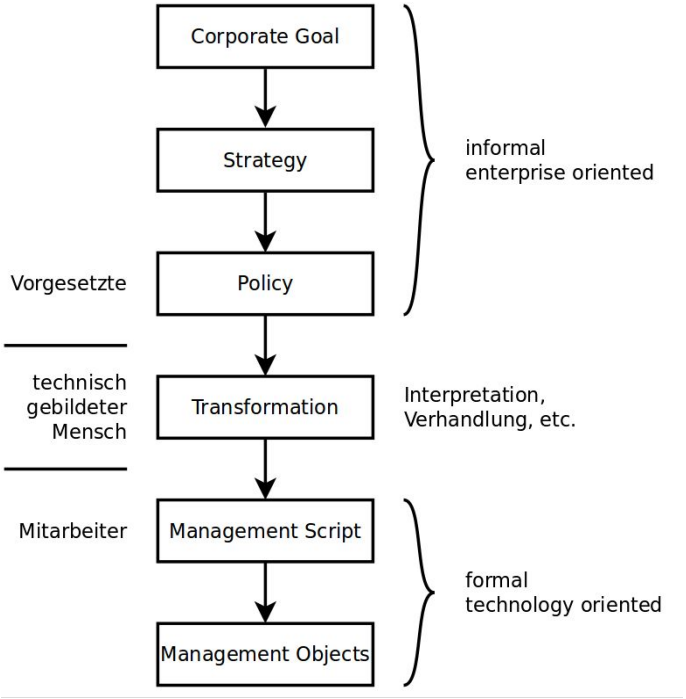
1. Corporate Goal (bei vielen „Gewinn", Gemeinnutzen bei NGOs, Forschung und Lehre bei Unis,...)
2. Strategie
3. Policy (wie hat man zu verfahren, aus der Strategie abgeleitet)
4. Management + Decision (Policy zu ungenau um direkt auszuführen)
5. Scripts
6. Ressourcen (Hardware)

Skizze ist zu zeichnen!

Welche Art von Corporate Goal kommt für Sie in Frage.
Welche schließen sie aus?

Könnte als offene Frage gestellt werden.

Eine Beispielantwort: “Ich würde aus moralischen Gründen und pol. Überzeugung Nichts von einer rechtsradikalen Institution betreuen.”



Corporate Goal: Gewinnorientierte Unternehmen / öffentliche Verwaltung / non-profit Organisationen / ...

Strategy: viele kleine Kunden / wenige große Kunden, Expansion, ...

Policy: nur Kunden mit mehr als 10k Einnahmen, Delay von Datennetz muss unter 50ms sein, etc.

Transformation: ist notwendig um informale Beschreibungen in formale Anleitung überzuführen - ggf. Verhandlungen, usw. notwendig.
Hier ist die technisch gebildete Person notwendig
Bei der Transformation muss ständig nach “oben” Rückfrage gehalten werden, was wie gemeint ist.

Management Script:
ist wie ein Kochbuch, sehr detailliert.
z.b. Laserdrucker ist nur während Arbeitszeit eingeschaltet

Management Object (Ressource / Hardware):
ist das Ding, worauf ich direkt einfluss nehme.
z.b. einen Laserdrucker kann ich ein und ausschalten

Welche 2 Sprachen kommen in dieser zum Einsatz?

1. *informell*: Corporate Goal, Strategie
2. *formal*: Scripts, Ressourcen

Die Management Ebene muss beide Sprachen beherrschen und in jeweils die andere übersetzten können.

Was ist die ideale Größe für ein Team? Warum?

5 +/- 2 Personen.
Beruht auf der Tatsache, dass ein Mensch nicht mehr als diese Anzahl von gegenständen im Auge behalten kann.

Auf welche Weise kann das Management überzeugt werden den Kauf neuer Technik Komponenten zu finanzieren?

Dies kommt auf die jeweilige Organisation an:

In der Forschung: Reine Zielerreichung funktioniert nicht… Um kreativ zu sein muss man verschwenderisch sein. Außer in AUT → Not macht erfinderisch <3

In der Wirtschaft: Kann der Gewinn dadurch maximiert werden, das Risiko gesenkt werden.

In einem Spital: Ausfallsicherheit, Personalentlastung,

In jedem Fall helfen aber **Statistiken**, welche für die Investition sprechen.

Wie einen Finanzierungsantrag formulieren? (Viertel bis Halbe Seite) **Risiko, Gewinn, Effizienz, Budget**

Vorlesung 3

Ist eine Userbefragung als Monitoring Mittel sinnvoll?

ja
Es kommt darauf an was aufgrund der eingebrachten Messergebnisse bewertet werden soll (Ist dies zum Beispiel die Kundenzufriedenheit → gut geeignet)
Diskrepanz zwischen technischen Messwerten und Benutzerbefragung? Welchen Werten vertraut man eher?
Benutzer sagen oft “es passt eigentlich eh…”

Ist Monitoring sinnvoll?

Entscheidender Faktor ist hierbei die Größe des Netzwerks.

Im Allgemeinen aber JA. Durch Monitoring kann
- die erwartete Lebensdauer
- Ausfallwahrscheinlichkeit
- genauer Ort eines Ausfalls
- jede kleine Änderung erkannt werden
- …

bestimmt werden.

Vorteile

- Risiken können minimiert werden
- bessere Planung (wann tauschen wir etwas?)
- Altdaten sammeln zur Fehleranalyse bzw. Erstellen von Statistiken
- Überwachung essentieller Funktionen und Schwellwerte
- etc.

Wo kann die Konfiguration eines Netzwerks gespeichert sein? Welche Konsequenzen entstehen daraus?

- In der Ressource direkt
- In einer Datenbank (muss immer aktuell gehalten werden um den IST-Zustand abzubilden) z.B. Kabellagepläne, Anfang, Ende, Namensgebung wichtig

Dokumentation der Netzwerktopologie?

(Es kann auch etwas dokumentiert werden wo keine Konfiguration existiert, zB. Layer 1)
Wie dokumentieren und welche Schichten (Zusammenhang). Wie stützen sich die Schichten aufeinander?

IST-Zustand: Wie ist der Zustand der Ressourcen
SOLL-Zustand: Was soll noch geändert werden?

Dokumentation der Zusammenhänge zwischen den Netzwerkteilnehmern:

- Wann darf welcher Part des Netzwerks ausfallen ohne Fehler zu verursachen?
- Wann kann ein Part ausfallen?
- Wie hängt Part A mit Part B zusammen

3 Grundprinzipien von Shared Media? (!!!)

1. Eindeutige Namensgebung → MAC – Adresse
2. Zugriffsverfahren (es darf nur einer reden)
3. Sendebeschränkung (man muss das Medium wieder freigeben)

Topologiearten (Stern, Ring,….)?

Quelle: http://www.elektronik-kompendium.de/sites/net/0503281.htm
<u>Stern</u>:

In der Stern-Topologie befindet sich eine **zentrale Station**, die eine Verbindung zu allen anderen Stationen unterhält. Jede Station ist über eine eigene Leitung mit der zentralen Station verbunden. Es handelt sich im Regelfall um einen Hub oder einen Switch. Der Hub oder Switch übernimmt die Verteilfunktion für die Datenpakete. Dazu werden die Datenpakete entgegen genommen und an das Ziel weitergeleitet.

Baum

Die Baum-Topologie ist eine erweiterte Stern-Topologie. Größere Netze haben diese Struktur. Vor allem dann, wenn mehrere Topologien miteinander kombiniert werden. Meist bildet ein übergeordnetes Netzwerk-Element, entweder ein Koppel-Element oder eine anderen Topologie, die Wurzel. Von dort bildet sich ein Stamm mit vielen Verästelungen und Verzweigungen.

Ring

Die Ring-Topologie ist eine **geschlossene Kabelstrecke** in der die Netzwerk-Stationen im Kreis angeordnet sind. Das bedeutet, dass an jeder Station ein Kabel ankommt und ein Kabel abgeht.
Im Ring befindet sich keine aktive Netzwerk-Komponente. Die Steuerung und der Zugriff auf das Übertragungsmedium regelt ein Protokoll, an das sich alle Stationen halten.
Wird die Kabelverbindung an einer Stelle unterbrochen fällt das Netzwerk aus, es sei denn die eingesetzte Übertragungstechnik kennt den Bus-Betrieb, auf den alle Stationen umschalten können.

BUS

Die Bus-Topologie, manchmal auch **Ketten-Topologie** genannt, besteht aus mehreren Stationen, die hintereinander geschaltet sind. Die Stationen sind über eine gemeinsame Leitung miteinander verbunden. Alle Stationen, die an dem Bus angeschlossen sind, haben Zugriff auf das Übertragungsmedium und die Daten, die darüber übertragen werden. Um Störungen auf der Leitung zu verhindern und die physikalischen Bedingungen zu verbessern, werden die beiden Kabelenden mit einem Abschlusswiderstand versehen.

Masche

Die Maschen-Topologie bzw. vermaschte Topologie ist ein dezentrales Netzwerk, das **keinen verbindlichen Strukturen unterliegen** muss. Allerdings sind alle Netzwerk-Stationen irgendwie miteinander verbunden. Häufig dient dieses Modell als perfektes Netzwerk in dem jede Netzwerk-Station mit

allen anderen Stationen mit der vollen Bandbreite verbunden ist. Diese Maschen-Topologie wird zumindest virtuell mit jeder anderen Topologie realisierbar, wenn genug Bandbreite zur Verfügung steht und aktive Netzwerk-Komponenten das Routing der Datenpakete übernehmen.
Beim Ausfall einer Verbindung gibt es im Regelfall einige alternative Strecken, um den Datenverkehr unterbrechungsfrei fortzuführen.
Die Struktur des dezentralen Netzwerkes entspricht einem Chaos an verschiedenen Systemen und Übertragungsstrecken. Das Internet stellt ein solches Netzwerk dar.

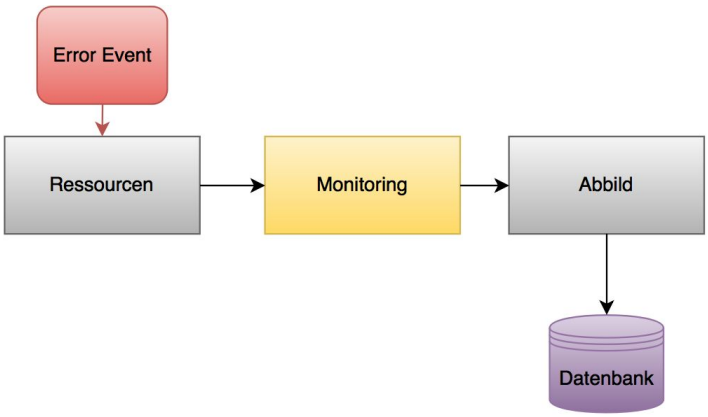
Ursache, Symptom, Wirkung?

Beispiel Mailserver: Es wird nur Netzwerkfehler angezeigt

NMAL (siehe unten) - Representation : User Ressourcen → Representation
Es gibt eine Wirkung, wir vermuten dazu ein Symptom und schließen daraus auf eine oder mehrere Ursachen
Diese Bewertung im Sinn der NMAL muss nicht mit Realität übereinstimmen.
Kommt es zu einem Fehler hierbei können die negativen Auswirkungen noch verstärkt werden.

Unschärfe bei Monitoring

Wie kann die in der VO beschriebene Skizze von der Realität abweichen?



Vorlesung 4

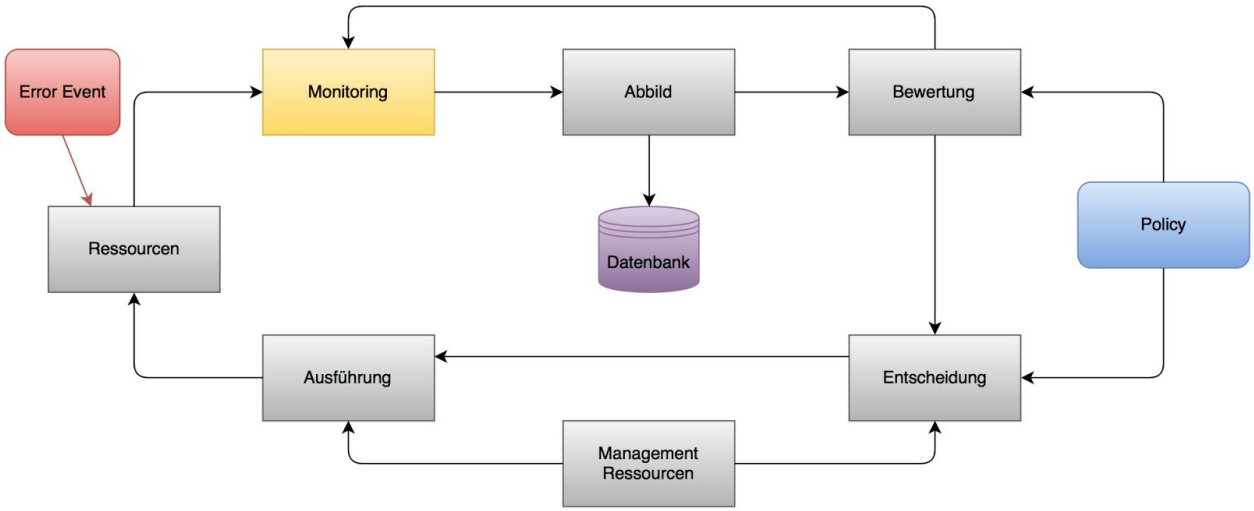
Beispiele für Managementressourcen

Nutzer (User) Ressourcen: Bringen dem Unternehmen direkt etwas.
Managementressourcen sind Ressourcen die nicht direkt zur Produktion beitragen.

Beispiele: Alles was fürs Monitoring aufgebaut wird (Monitoring System), Sekretärin,...

Network management activity loop (NMAL)

(grafik) → bild Zeichnen!!! und erklären können
Was kann man daraus ableiten?



Die Netzwerkressourcen werden von einem Monitoring System dauerhaft untersucht und mittels einer passenden Abbildung abstrahiert und in die Datenbank gespeichert. Hierbei ist zu beachten, dass der IST und SOLL Zustand der Netzwerkdokumentation aktuell gehalten wird.
Anhand der Abbildung wird eine Bewertung erstellt, welche, falls diese nicht eindeutig bzw. ungenau ist zum Monitoring Part rückgeführt wird, um die Genauigkeit durch eine höhere Anzahl an Messwerten zu verbessern und im anderen Falle zu einer Entscheidung führt. Die Bewertungs- und Entscheidungskriterien werden von einer bestehenden Policy abgeleitet.
Nachdem die Entscheidung gefallen ist, wird diese unter der Aufsicht der Management Ressourcen auf den Ressourcen ausgeführt.
Falls nun ein Fehlerfall auftritt, bemerkt das Monitoring System diesen und leitet sofort Gegenmaßnahmen ein. Durch die Gefahr von Schwingungen in unserem Regelkreis sollte eine menschliche Komponente als Dämpfungsglied bedacht werden.

Wie kommt es zu einem Fehlalarm? Konsequenzen?

- Defekte Sensorik
- Falsche interpretation von erhaltenen Daten

Konsequenzen:
- “Sinnfreie” Alarmierung von Notsystemen und Personal
- Sensorik und Methodik wie der Fehler ausgelöst wird überprüfen. Achtung, nicht zu unscharf einstellen, da sonst wirklich Fehlerfälle nicht erkannt werden könnten.

Welche Konsequenzen sollte ein ausgelöster Fehlalarm für die auslösende Person haben?

Am besten gar keine. Wird die Person dafür bestraft, wird sie das nächste Mal in einem ähnlichen Fall wahrscheinlich nicht Alarm schlagen und somit eventuell einen echten Fehler nicht weitermelden.

Signalisieren mittels Farbzuständen und Bewegung, Piktogramm

Wie baut man ein GUI für jemanden der lange hinschauen muss.
Wichtigkeit mittels Farben signalisieren.
Bsp: Es ist etwas ausgefallen : einfache Ressource (rot), redundante Ressource (gelb)
„Messwert liegt nicht vor“ sollte nicht gleich rot sein (oft helles blau, beige)

Farbenblindheit beachten! Farbe ausschreiben und andere Methoden in Betracht ziehen, wie z.B. Blinken einer Meldung und andere visuelle Möglichkeiten

Schwingneigung einer Schleife

Auch die Network Management Acitvity Loop ist eine Schleife und hat somit ähnlich dem Konzept in der Elektrotechnik eine latente Schwingneigung.

Bei einer vollständigen Automatisierung kann dies zu Problemen führen:
Temperatur zu hoch → Klimaanlage an, Temperatur wird zu niedrig → Klimaanlage ab, Temperatur zu hoch,… Kreislauf. Der Mensch kann dies erkennen aber autonomes System meist nicht.

Um dies zu vermeiden muss ein Schwingungsdämpfer eingebaut werden. Zum Beispiel eine Person mit ihrer Erfahrung und ihrem Gedächtnis (in der Bewertung und Entscheidung)

Informationsspeicher zur Gegenkopplung

- **Mitkopplung**: verstärkt Gegenausschlag
- **Gegenkopplung**: dämpft Gegenausschlag
  Problem bei zu starker Gegenkopplung: es kommt zu zu hohen Gegenmaßnahmen, die zu einer potentiellen Schwingneigung führen

Woraus leite ich meinen Handlungsbedarf ab?

Vergleiche Darstellung (Abbildung) mit Policy. Daraus ergibt sich die Bewertung aus welcher der Handlungsbedarf abgeleitet werden kann.
In einem Unternehmen letztendlich aus der Policy.

Vorlesung 5

Was ist Teil von SNMP (Simple Network Management Protocol)? Kreuzen Sie 4 Stück an

Grundelemente:

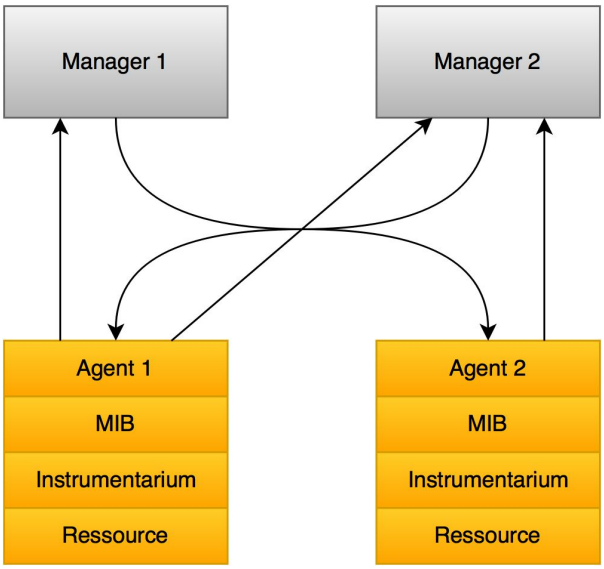
- Manager
- Agent:
    - Management Information Base – MIB (Datenmodell)
    - Instrumentarium: Führt die Abbildung von Ressource auf MIB durch.
    - Ressource
- SNM Protokoll - Beschreibt wie Daten transportiert werden?
- MIB

Wieso keine Security in SNMP?

SNMP war ursprünglich nur als Übergangslösung vorgesehen, bis das entsprechende OSI Management Model fertig implementiert war. Das SNM Protokoll wurde dementsprechend auf eine Lebensdauer von 2 Jahren hin entwickelt. Deswegen wurde Security einfach nicht als Priorität gesehen. Es gibt lediglich einen community String, welcher bekannt sein muss.

Man kann Security jedoch zu SNMP hinzufügen indem man die Verbindung an sich sichert (VLAN).

Topologie bei SNMP?



Ein Manager kann mehrere Agents verwalten. Ein Agent kann auch von mehreren Managern verwaltet werden.
Es ist keine horizontale Kommunikation zwischen den Komponenten vorgesehen.

Welche Probleme ergeben sich aus diesen Topologien?

Manager können sich nicht koordinieren und Daten austauschen und Agents genauso wenig. Das heißt, dass jegliche Kommunikation immer über einen Manager führen muss und die Agents nicht autonom kommunizieren können (Problem wenn ein Manager ausfällt -> Agent nutzlos).

Welche Aufgabe hat das Instrumentarium?

Wie kann diese gebaut werden von der Struktur her?

- Event basiert?
- Periodisch (Zyklisch)?

Welche vor und nachteile bei den verschiedenen Varianten

Dient dazu die in der MIB vorhandenen Werte aus der r wäre sonst "Argonaut*in" die State-of-the-art-Beigentlichen Resource auszulesen.

Welcher Teil eines Agents sollte nach einem Ressource Wechsel konstant bleiben?

Die MIB sollte in jedem Fall konstant bleiben. (z.B. Drucker durch anderen Drucker austauschbar wenn die MIB gleich bleibt)
Das Instrumentarium kann sich ändern. Die MIB kann man sich als Interface vorstellen, welche die Abbildung zur Ressource bildet. Das Instrumentarium ist dann der Treiber, welcher direkt auf die Ressource mappt.

Welchen Effekt hat es wenn sie nicht gleich bleibt?
Der Manager kann eventuell auf die gleiche Frage keine Antwort mehr bekommen, da dieser Teil der MIB vom Agent nicht mehr implementiert wird. Es muss eine neue MIB geladen werden.

Definition eines Pseudo- Zufallsgenerator

Pseudozufallsgeneratoren erzeugen zufällig aussehende Folge von Zahlen. Diese unterscheiden sich von echten Zufallszahlen dadurch, dass sie vom Zustand der internen Variablen des Pseudozufallsgenerator abhängen und mit deren Kenntnis durchaus vorhersagbar beziehungsweise reproduzierbar sind.

Der Pseudozufallsgenerator benutzt deswegen einen Seed, welcher ihm übergeben wird und nicht erraten werden kann (oder sollte).
Oft werden die Werte dann durch die Kombination von zufällig auftretenden Ereignissen (wie die Mausbewegungen,...) erstellt.

Wann holt sich das Instrumentarium die Echtwerte aus der Ressource?

(ident zu vorheriger Frage)

1. *Periodisch (Zyklisch)*:
   Hierbei ist besonders die Wahl des Zeitintervalles kritisch.
   Auch sollte mitgeliefert werden um wie viel der Wert veraltet ist, also wann die Messung vorgenommen wurde.

2. *Beim Auftreten eines Ereignisses (Event)*: In diesem Fall muss dies aber von der Hardware unterstützt werden (bei einem Temperaturfühler zum Beispiel ändern sich die Werte bei weitem zu häufig)

Vorlesung 6

Vor- und Nachteile von Traps?

Wann sollte man sie einsetzen, wann nicht?

Vorteil

- Selbstständing & Unmittelbar: Fehler kann gleich gemeldet werden und wird nicht erst beim Polling vom Manager bemerkt.

Nachteile

- Muss die Adresse vom Manager wissen
- Wenn Manager IP-ändert müssen alle Agents nachkonfiguriert werden
- Läuft über UPD. Ist also nicht sicher, dass Manager von Fehler erfährt

Grundsätzliche Funktion?

- Asynchron (Manager = Server)
- von Agent zum Manager

Spezialsituation? Adresse muss hinterlegt werden
TODO add further
Vorteile:

- Asynchron
- Passiert sofort
- kein Polling nötig

Nachteile:

- Client braucht für Trap die Adresse des Managers.
- Wenn die Nachricht nicht ankommt, dann erfährt man nie vom Zwischenfall.

5 Telegrammarten – Protocol Data Units (PDUs, SNMP v1)

1. *GET REQUEST*: zum Anfordern eines Management-Datensatzes, Manager möchte Wert Wissen
2. *GET RESPONSE*: Antwort auf eines der vorherigen Pakete.
3. *SET REQUEST*: um einen oder mehrere Datensätze eines Netzelementes zu verändern. Manchmal verlangt ein Netzelement die gleichzeitige Änderung mehrerer Datensätze, um die Konsistenz zu überprüfen. Beispielsweise erfordert die Konfiguration einer IP-Adresse die gleichzeitige Angabe der Netzwerkmaske.
4. *GETNEXT REQUEST*: um den nachfolgenden Datensatz abzurufen (um Tabellen zu durchlaufen)

5. *TRAP*: unaufgeforderte Nachricht von einem Agenten an den Manager, dass ein Ereignis eingetreten ist.

ACHTUNG: Es gibt kein SET RESPONSE!

Wann wird der erste TRAP eines Agenten gesendet?

Bei dessen Start, wenn er im Netzwerk verfügbar wird.
Kaltstart: von 0 (ausgeschaltet) Starten → Hardware (z.B. Schnittstelle) wird neu initialisiert
Warmstart: Aufgrund eines Software Reboot

Holschuld vs Bringschuld (Polling vs Interrupt)

Generell ist das Thema Hol- vs Bringschuld nicht eindeutig beantwortbar und muss in jedem Fall einzeln Beantwortet werden. Für jeden Anwendungsfall bietet das eine oder andere passende Vorteile.
z.B. Wie soll ein Sensor für eine Tür behandelt werden? Polling: schwierig das richtige Intervall zu finden. Interrupt: Wann soll der Interrupt ausgeführt werden? Beim Öffnen, Schließen oder bei beiden?

Interrupt Nachteil:
Wenn die Nachricht nicht ankommt, dann erfährt man nie vom Zwischenfall. Könnte Agent bzw. die Ressource bei zu vielen Interrupts überlasten.

Polling Nachteil:
Intervall muss so klein wie nötig, aber so groß wie möglich bestimmt werden (Polling mit hoher Frequenz benötigt viel CPU Leistung!). Gefahr von bereits veralteter Daten durch unpassende Zyklen.

Wann macht eine Kombination von beiden Techniken Sinn?

Wie Kommunikationsmodell zwischen mehreren Partnern aufbauen?
Vorteile, Nachteile von jeweiligen. Wann machen wann nicht?

Welche Probleme können bei mehreren Anfragen in einem Request auftreten?

SNMP Layer 4 Protokoll: Datenmenge kann unendlich groß sein.

- Timeout wenn Bearbeitung zu lange dauert
- Zu viele Anfragen in einem Telegramm (Nachricht)
  → Bytes können aus dem Buffer hinausfallen
- Unterschiedliche Bearbeitungszeit
- Paketverlust
- Agents: Ressourcenknappheit (Kostenersparnis). Agent kann schnell Überfordert werden (Input Queue). Wenn die Queue voll, Input wird ignoriert

Vorlesung 7

Welche Gruppe wird von allen Agents implementiert?

System Gruppe
Werte siehe nächste Frage

Interface Gruppe, System Gruppe?

Was ist drinnen, was les ich da und wofür kann ich es nutzen?
http://casecomms.com/snmp-mib-ii/

System (die wichtigsten):

- *sysDescr* - System Description (String, menschenlesbar)
- *sysUpTime* - System Uptime
- *sysObjectID* - OID (dient zum Erkennen um was für ein Gerät es sich bei dem Agent handelt)
- *sysServices* - Beschreibt welche Services der Agent anbietet. Summe aus 2er Potenzen (2^1: Router, 2^2: Switch. Kann er beides: die Summe daraus)
- *sysContact* - IP (Verantwortlicher)
- *sysName*
- *sysLocation* - String der den Ort des Gerätes beschreibt

Interface (die wichtigsten):

- ifNumber - Anzahl der Interfaces
- ifTable - Liste von Interface Einträgen
    - ifIndex
    - ifDescr
    - ifType
    - ifSpeed
    - ifPhysAddress
    - ifOperStatus - Ist eine Verbindung vorhanden (read only)
    - ifAdminStatus - “softwareseitiger” Status des Interfaces, kann über diesen (de)aktiviert werden
    - ifLastChange
    - ...

Was sagt die sysuptime /hrsysuptime wirklich aus?

SysUPTIme (in System Gruppe) ist im Fall des PCs: Wann wurde der **(SNMP)Agent gestartet** (ungleich dem Systemstart).
Der zurückgegebene Wert ist ein Counter (32 Bit), welcher bei bei Überlauf wieder bei 0 beginnt (Sägezahnmuster).

hrsysuptime enthält im Gegensatz dazu den Wert wann das **Gerät an sich gestartet** wurde.

Wie funktioniert ein Counter?

Sägezahn!

mit welchem intervall müssen sie mindestens pollen, sodass die werte noch aussagekräftig sind?

Beispiel:
32 Bit Counter
1 GBit/Sec Interface (voll Auslastung)

Wie lange dauert es bis dieser counter überläuft?
(2^32)/(1024*1.000.000) * 8 = ~34 Sekunden (8→ counter zählt Oktetten)

Gründe für einen Reboot?

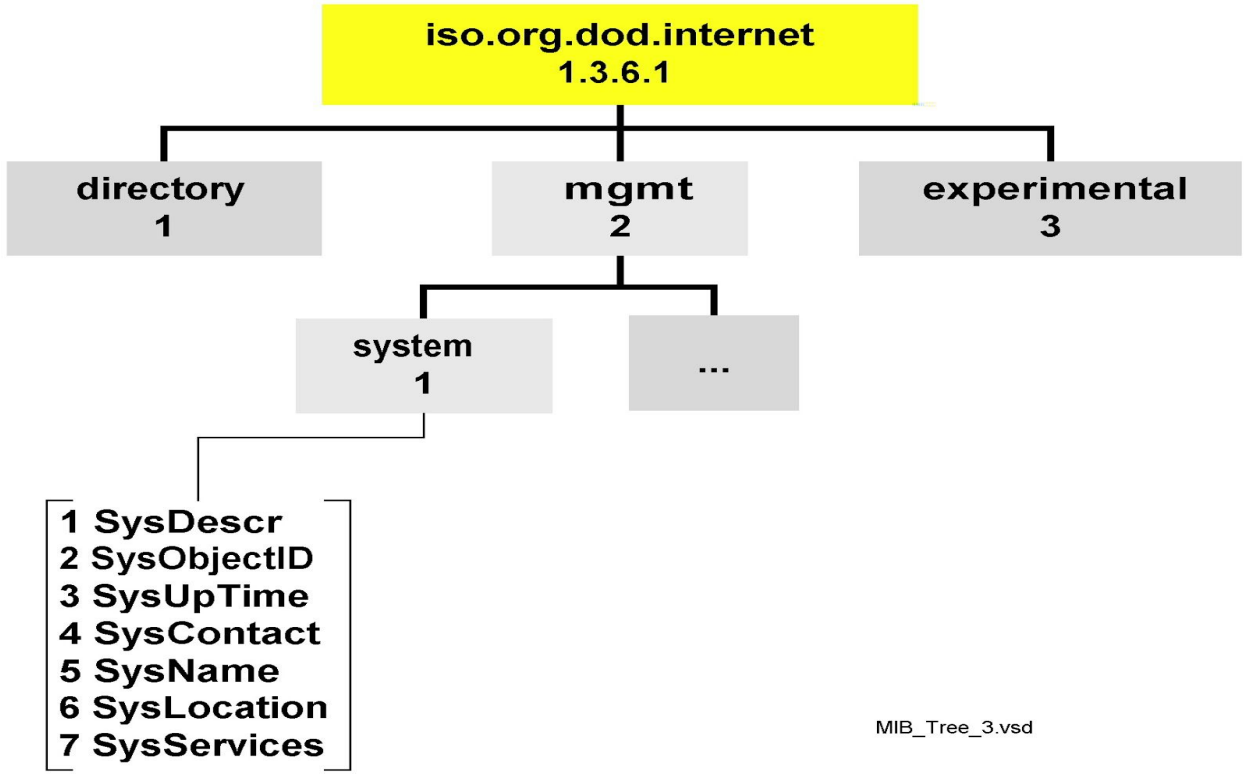
Stromausfall, Management Reboot, Software Fehler, Security Breach

Wie kann der Manager herausfinden um was für einen Typ von Agent es sich handelt?

Die Art eines Agents kann via eines Abfragens von sysObjectID erfolgen. Dieser Aufruf retourniert eine OID. Diese OID repräsentiert den Agenten und muss in einer eigenen Datenstruktur (gleich aufgebaut wie MIB) geladen werden.

Aufbau einer OID?

Der OID (Object Identifier) ergibt sich aus den Nummern der Knoten die gewählt werden muss um zum jeweiligen Blatt in der MIB zu gelangen.



Aufbau der Mib

Baumstruktur, Information (2 dimensionale Tabellen oder einfache Werte) an den Blättern,…
Welche 2 Großen Bereiche gibt es?
Wo sind die eigentlichen Informationen und wo sind versteckte Informationen?

Vorlesung 8

keine Fragen gegeben. Behandelt wurde: (dies wurde in der Vorbesprechung zur Prüfung aber gekonnt verschwiegen :D)

Proxy

Schnittstelle zwischen 2 Welten. Hat auch eine Transformationsaufgabe (Sprache der einen Welt in die der anderen)
Beispiel: Zwischen Bus System und Ethernet

Midlevel Manager

Ist nicht Teil des SNMP. Es kommen propriätere Lösungen zum Einsatz.

Der **Mid-Level Manager** wird als Dual Role Manager umgesetzt. Er ist sowohl Agent als auch Manager.

- Für den Manager der Anfragen an ihn stellt ist er ein Agent,
- Für den Agent, von dem er Anfragen anfordert ist er ein Manager

Der Midlevel Manager delegiert die Arbeit an die Agents (und überprüft deren korrekte Ausführung). Auf diese Weise kann einiges an Traffic gespart werden: Der Manager muss nicht mehr bei allen Agents pollen, sondern der Midlevel Manager kann ihm diese Daten bereits aufbereitet zur Verfügung stellen.

Beispiel TU: Mid Level manager überwacht die Switches eines Gebäudetrakt. Er senden im Normalfall nur die Nachricht „ist ok“.

IP Addressen

Schnell erwähnt, damit sie zur Prüfung gegeben werden können

Ausrechnen oder
Sind diese Werte korrekt?

Beispiel aus der VO:

```
ip: 192.168.173.12/20
netmask: 255.255.240.0
network address: ip AND nm    = 192.168.160.0
broadcast address: ip OR NOT nm = 192.168.175.255
```

ACHTUNG: es können Beispiele mit unmöglichen Adressen dabei sein, z.B. 192.168.**268**.20

Zum Üben ;) : http://www.ciscolab.de/aufgaben/subnetting.pdf