
Networks made easy!

# Netzwerküberwachung

Den Status eines Netzwerks kennen und verstehen

Networks made easy!

## Leo Künne

Geschäftsführer der CX-Networks GmbH

Seit 2015 in der Branche

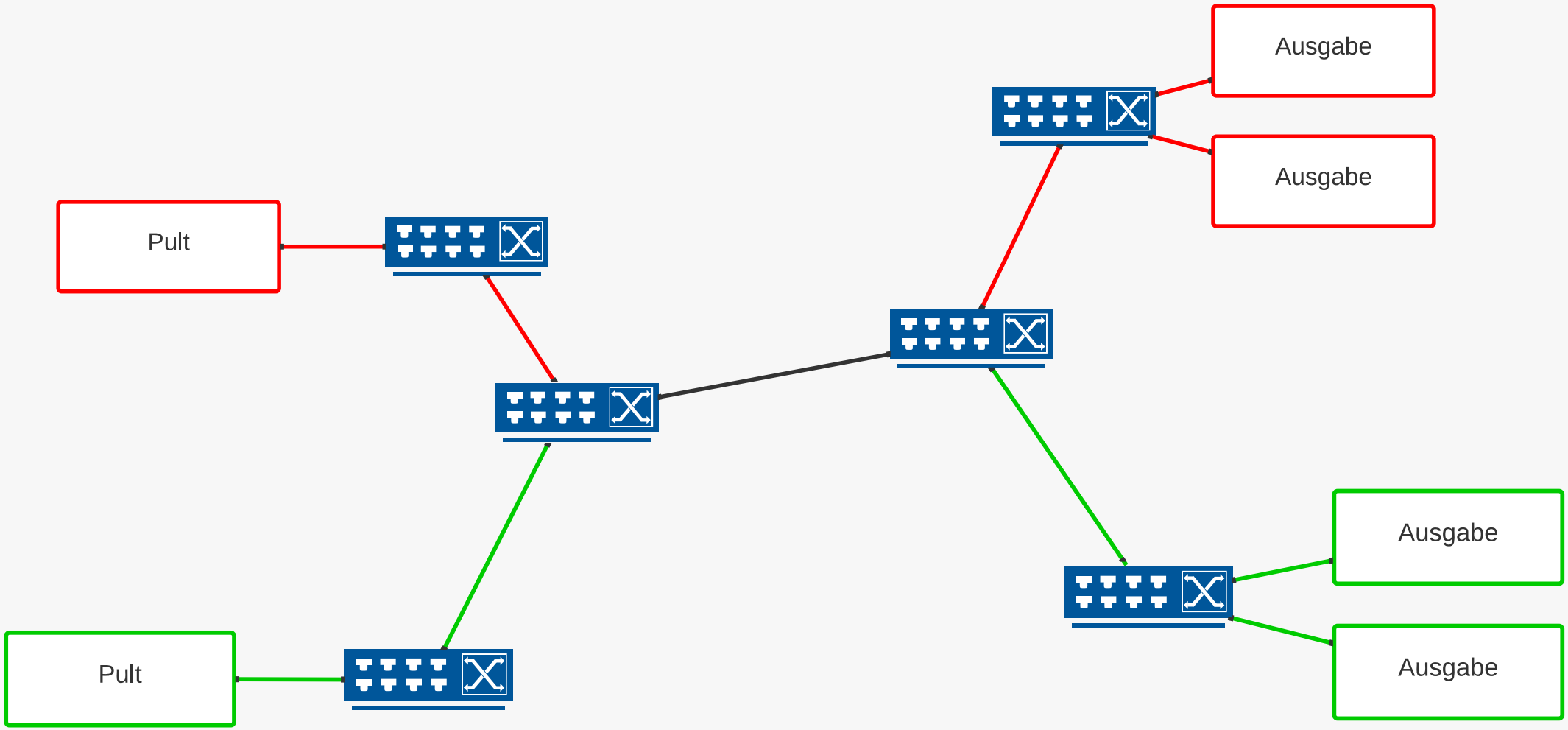
# Was ist Netzwerküberwachung?

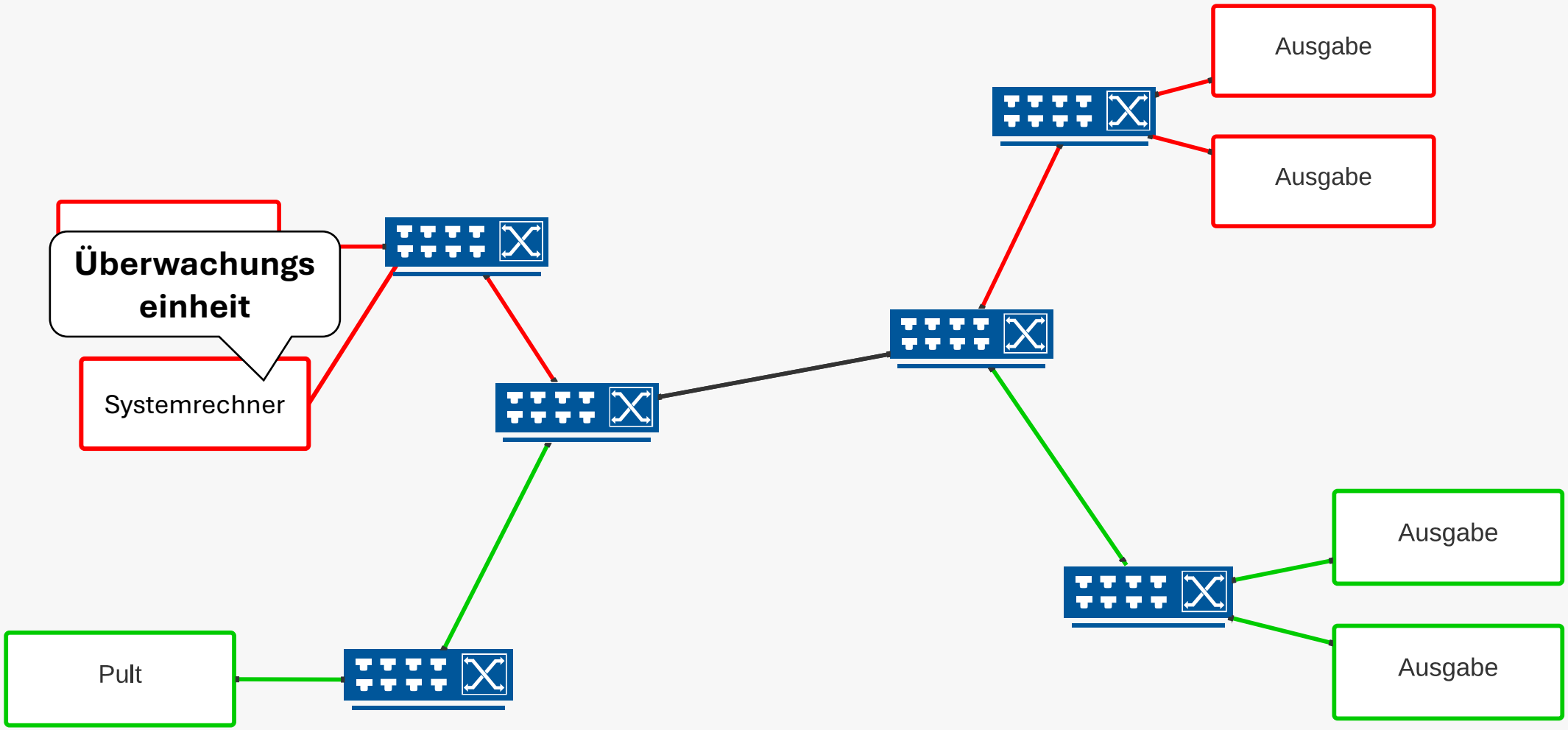
Den Gesundheitszustand eines Netzwerkes kennen

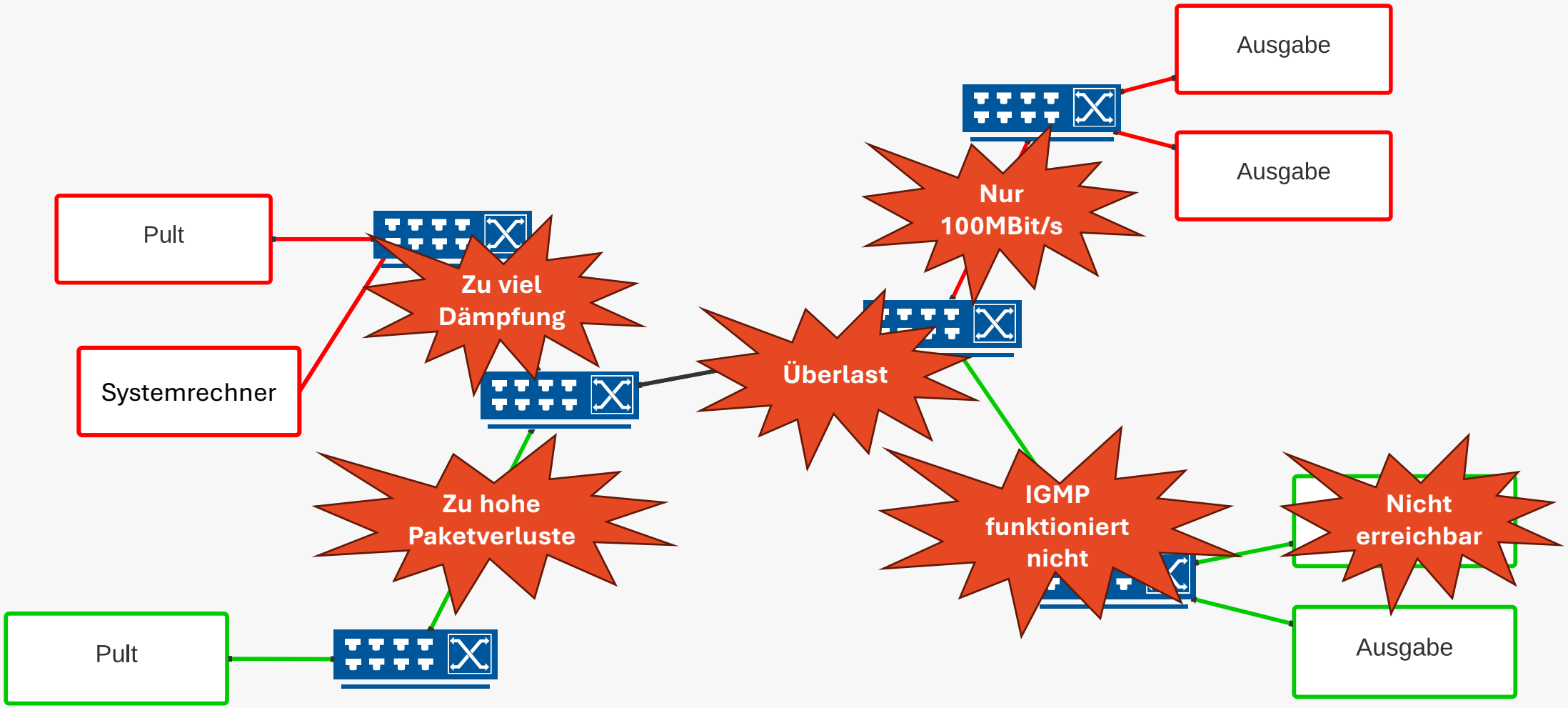
# Beispiele für Überwachung in anderen Gebieten

- Auto
  - Wassertemperatur
  - Öltemperatur
- Task-Manager CPU Auslastung
- Audio
  - Latenz
  - Lautstärkemessung

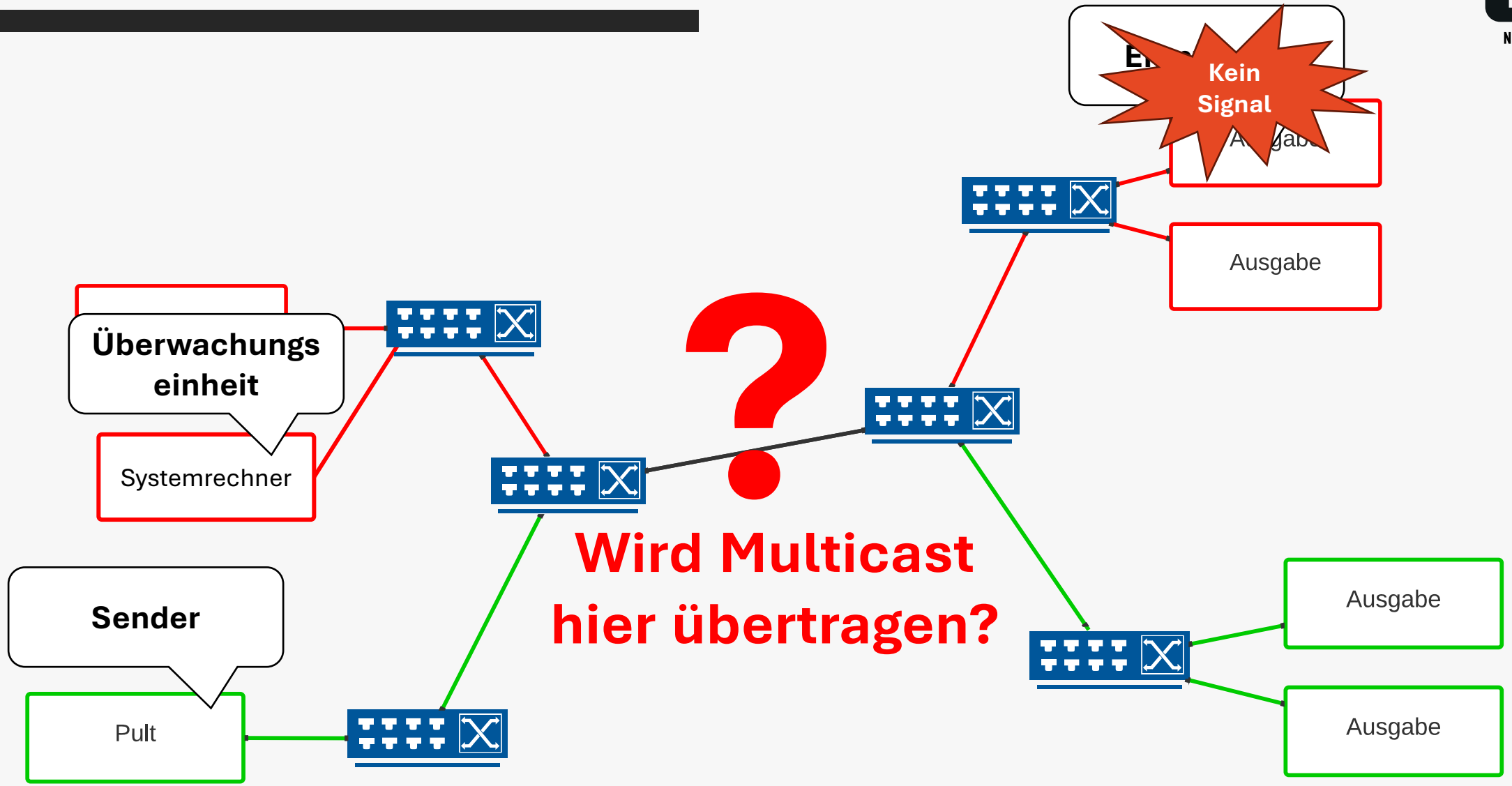
# Veränderungen erkennen


Ausgabe
Ausgabe
Pult
Ausgabe
Ausgabe
Pult

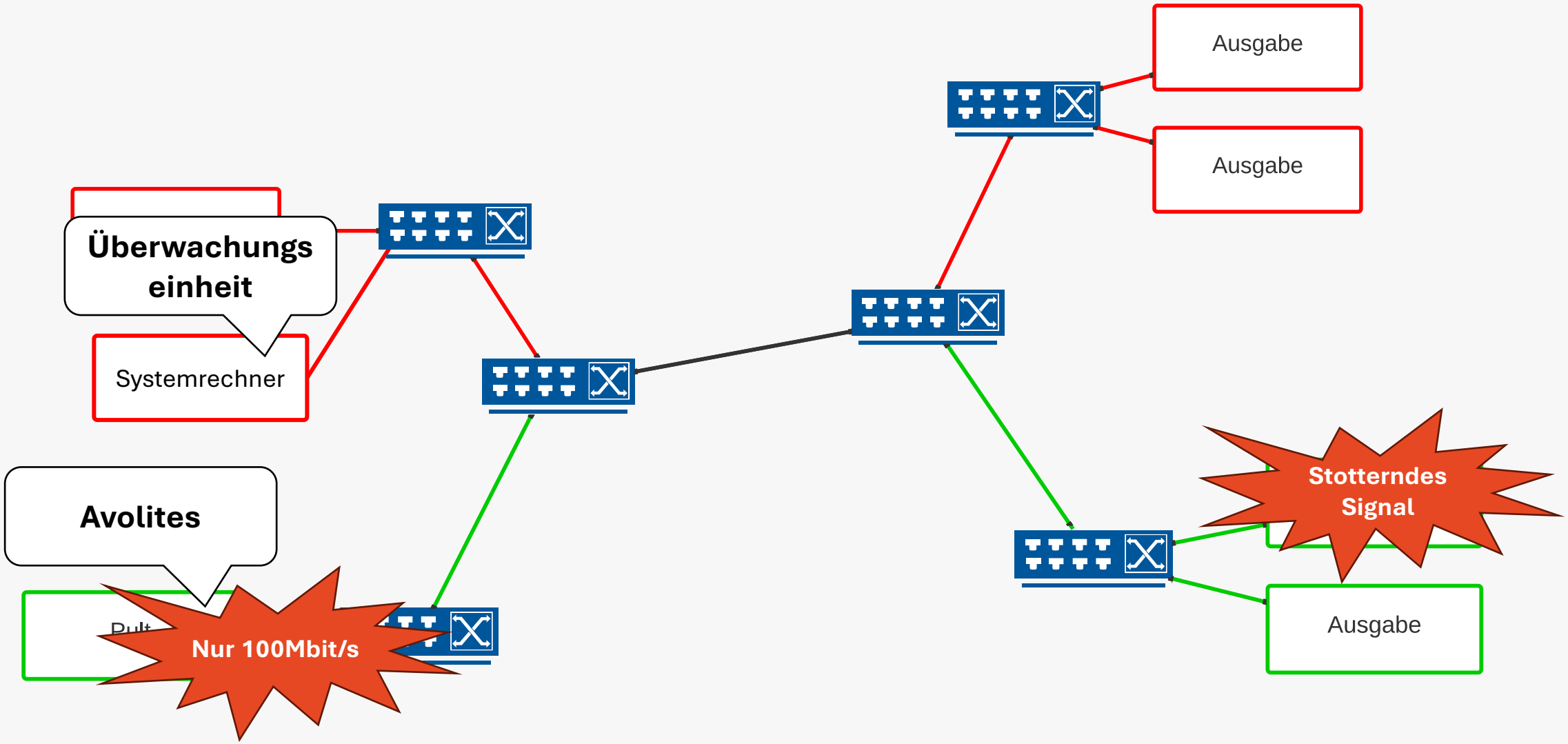

Ausgabe
Ausgabe
Überwachungs einheit
Systemrechner
Ausgabe
Ausgabe
Pult


Ausgabe
Ausgabe
Nur 100MBit/s
Pult
Zu viel Dämpfung
Systemrechner
Überlast
Zu hohe Paketverluste
IGMP funktioniert nicht
Nicht erreichbar
Pult
Ausgabe

# Beispiel: IGMP-Snooping


Kein Signal
Ausgabe
Überwachungs einheit
Systemrechner
Sender
Pult
Wird Multicast hier übertragen?
Ausgabe
Ausgabe

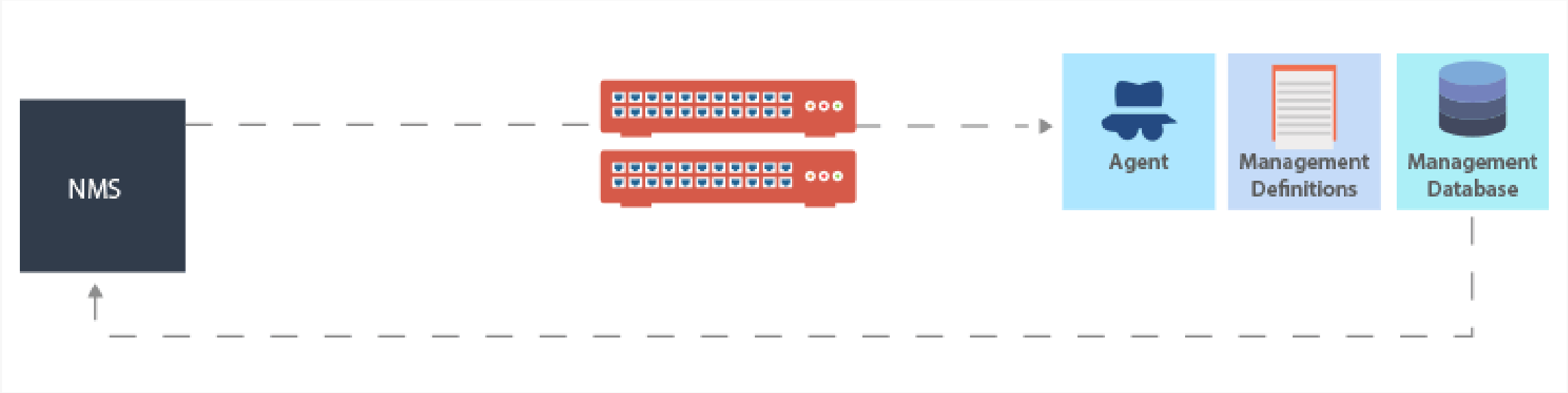
# Beispiel: Avolites


Ausgabe
Ausgabe
Überwachungs einheit
Systemrechner
Avolites
Pult
Nur 100Mbit/s
Stotterndes Signal
Ausgabe

Networks made easy!

# Den Zustand des Systems kennen und verstehen!

Monitoring-Programme helfen uns dabei


NMS
Agent
Management Definitions
Management Database

# SNMP v1

- Erste Version von dem „Simple Network Managment Protocol“
- Autorisierung mittels unverschlüsseltem Community-String
- Funktionen:
  - Abfragen von Konfigurationen
  - Abfragen des Zustandes
  - Setzten von Konfigurationen
  - Benachrichtigung über Zustandsänderungen

# SNMP v2c

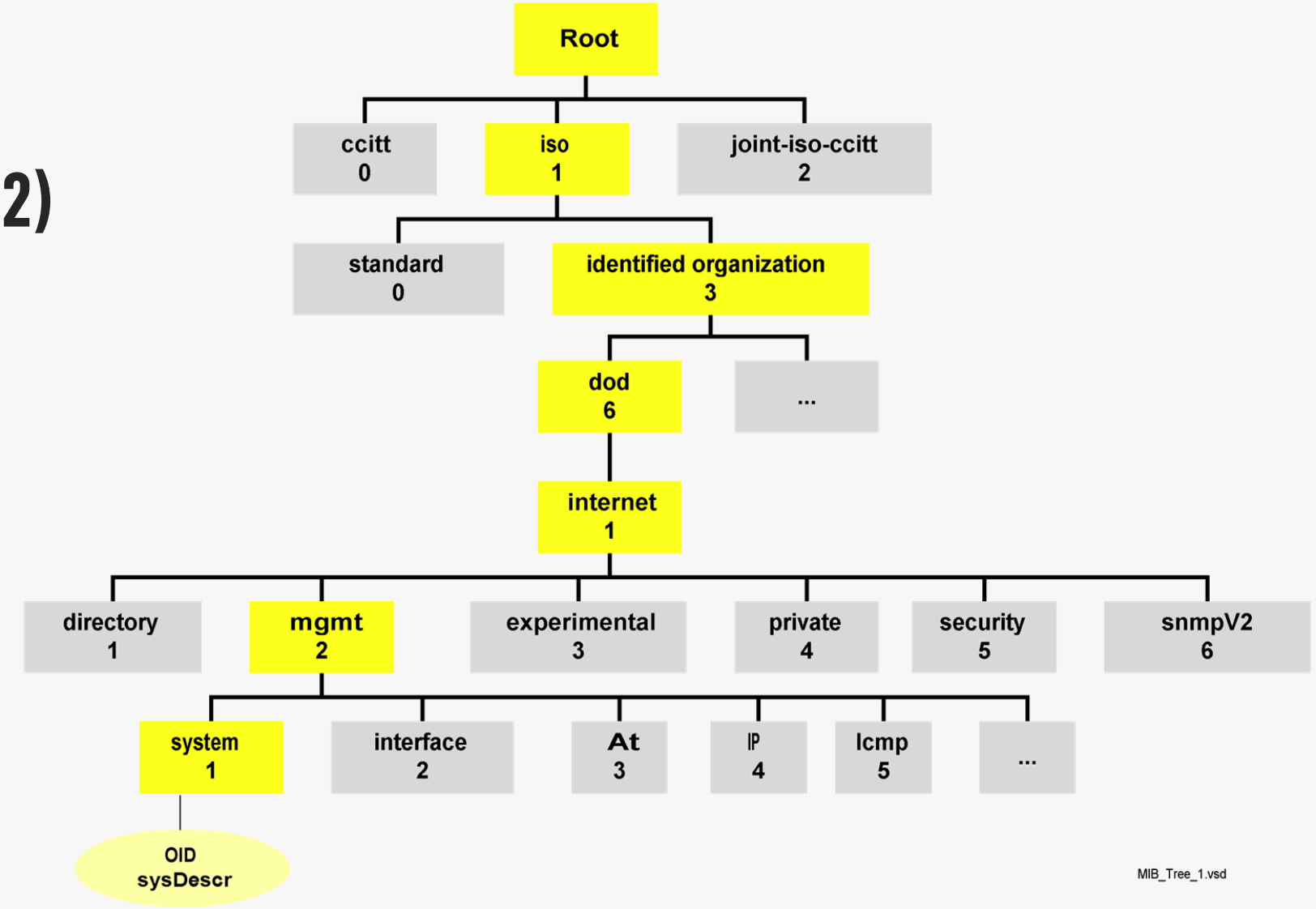
- Nachfolger von „secure SNMP“, SNMPv2p und SNMPv2u
- Autorisierung mittels unverschlüsseltem Community-Strings
- Neuer GetBulk-Befehl

# SNMP v3

- Autorisierung mittels Anmeldedaten
- Verschlüsselung der Anmeldedaten

# OID

## (1.3.6.1.4.1.2681.1.2.102)



# MIB

```
ifIndex OBJECT-TYPE
    SYNTAX      InterfaceIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A unique value, greater than zero, for each interface.  It
            is recommended that values are assigned contiguously
            starting from 1.  The value for each interface sub-layer
            must remain constant at least from one re-initialization of
            the entity's network management system to the next re-
            initialization."
    ::= { ifEntry 1 }

ifDescr OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (0..255))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A textual string containing information about the
            interface.  This string should include the name of the
            manufacturer, the product name and the version of the
            interface hardware/software."
    ::= { ifEntry 2 }
```

https://github.com/cisco/cisco-mibs

# SNMP-Versionen

## SNMP v1

- Autorisierung mittels Community-Strings
- Keine Verschlüsselung

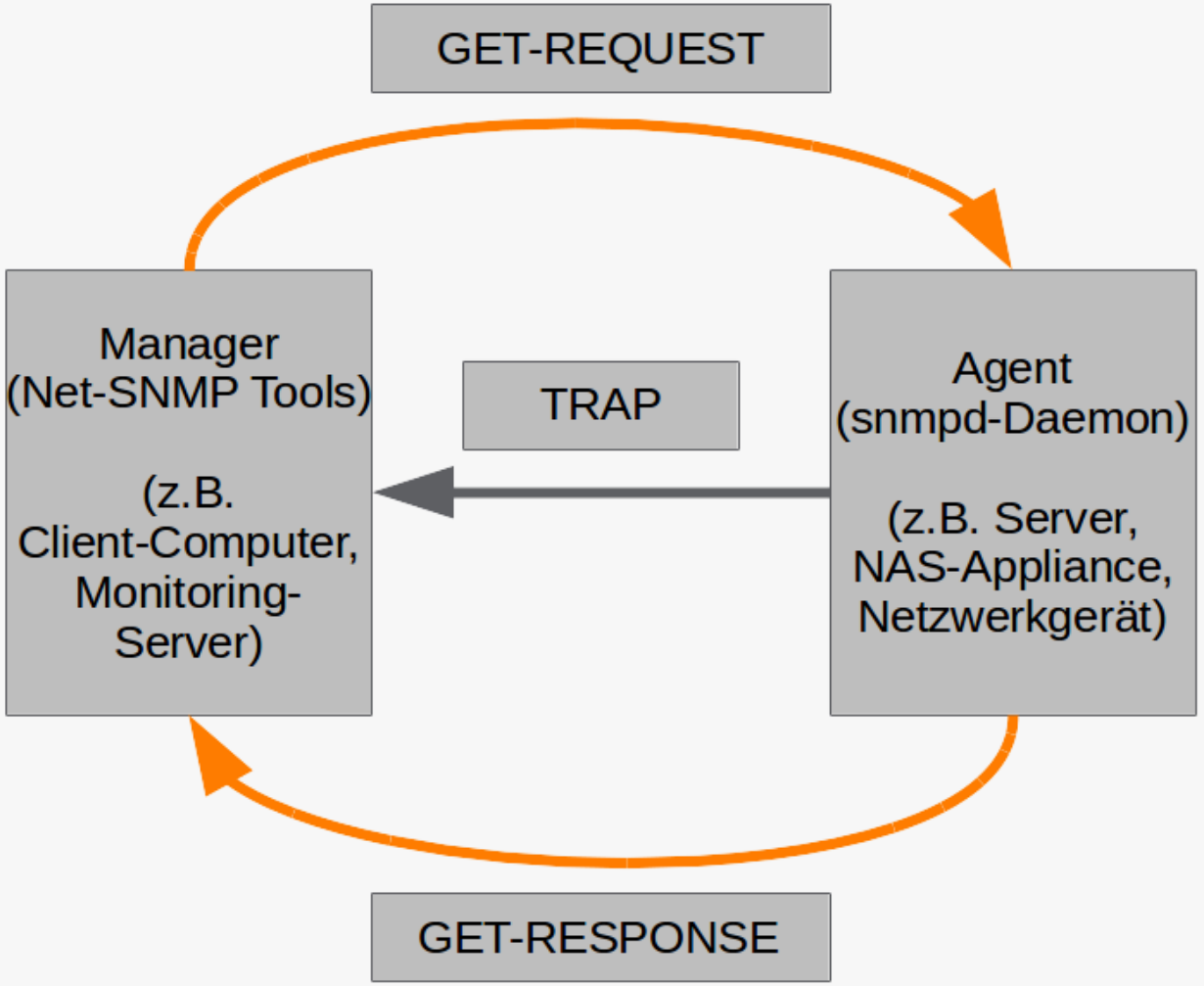
## SNMP v2c

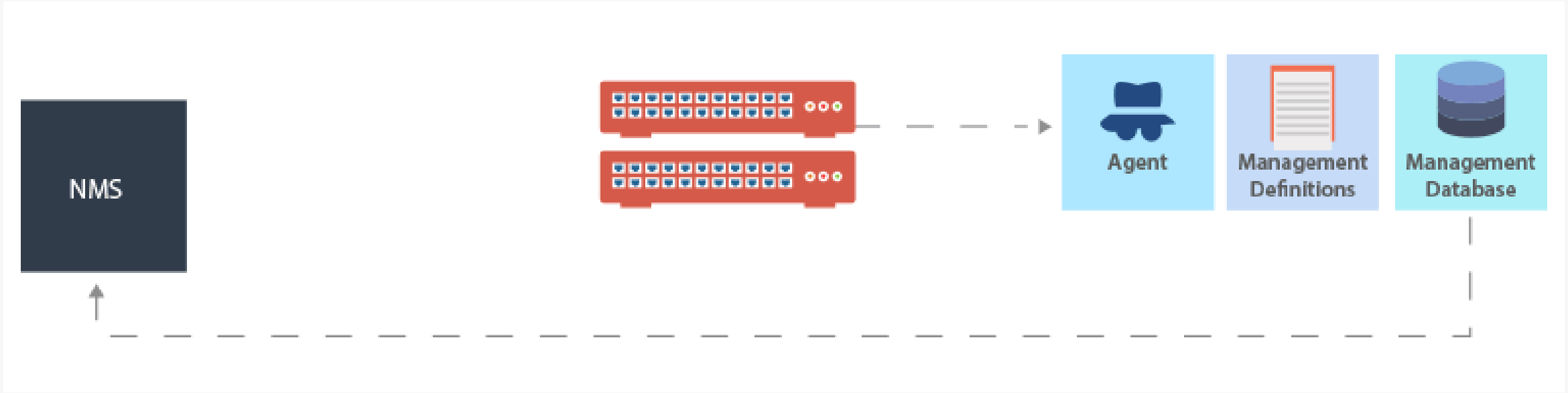
- Überholte Version von v1
- Autorisierung mittels Community-Strings
- Neue GetBulk Funktion für mehr Fehlercodes
- Keine Verschlüsselung

## SNMP v3

- Autorisierung mittels Benutzername und Password
- Authentifizierung mittels View-Based Access Control Model
- Data Integrity Check, Data Origin Authentication and Data Confidentiality check

# SNMP Traps


GET-REQUEST
Manager
(Net-SNMP Tools)
(z.B.
Client-Computer,
Monitoring-
Server)
TRAP
Agent
(snmpd-Daemon)
(z.B. Server,
NAS-Appliance,
Netzwerkgerät)
GET-RESPONSE


NMS
Agent
Management Definitions
Management Database

# Agents und APIs?

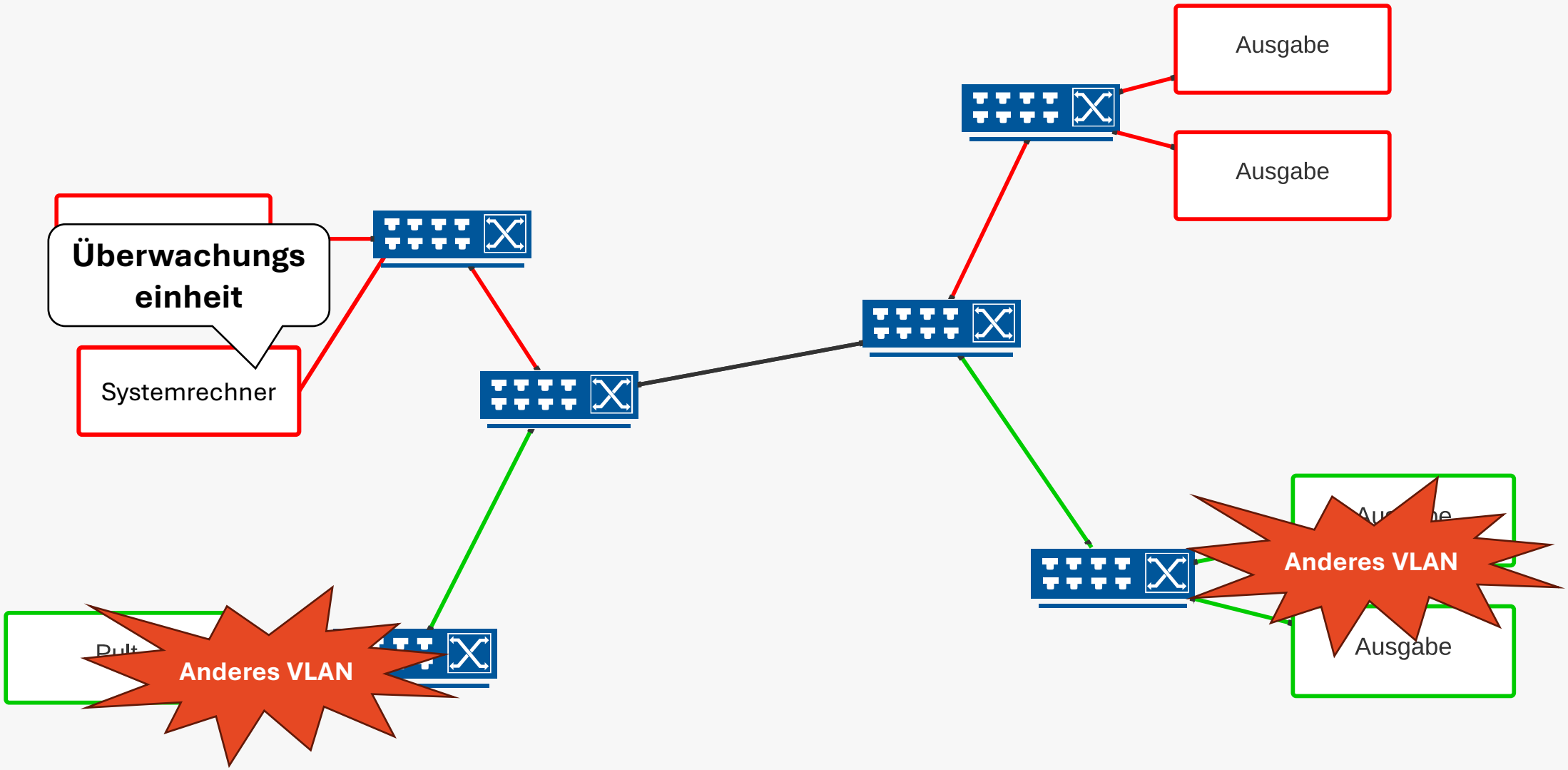
Agents:

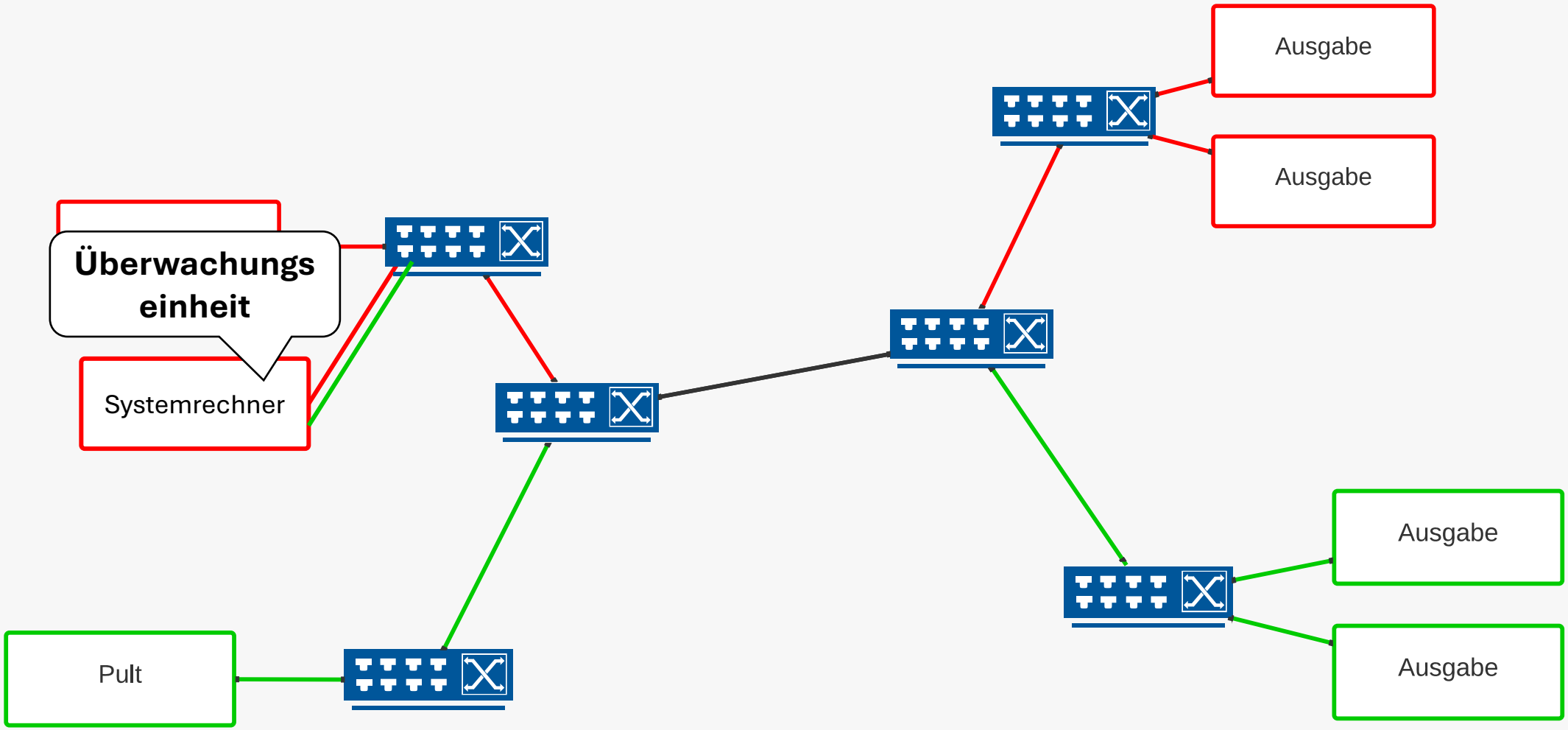
- Werden auf dem zu überwachendem System installiert
- Sammeln Daten auf dem System und senden sie an die Überwachungseinheit

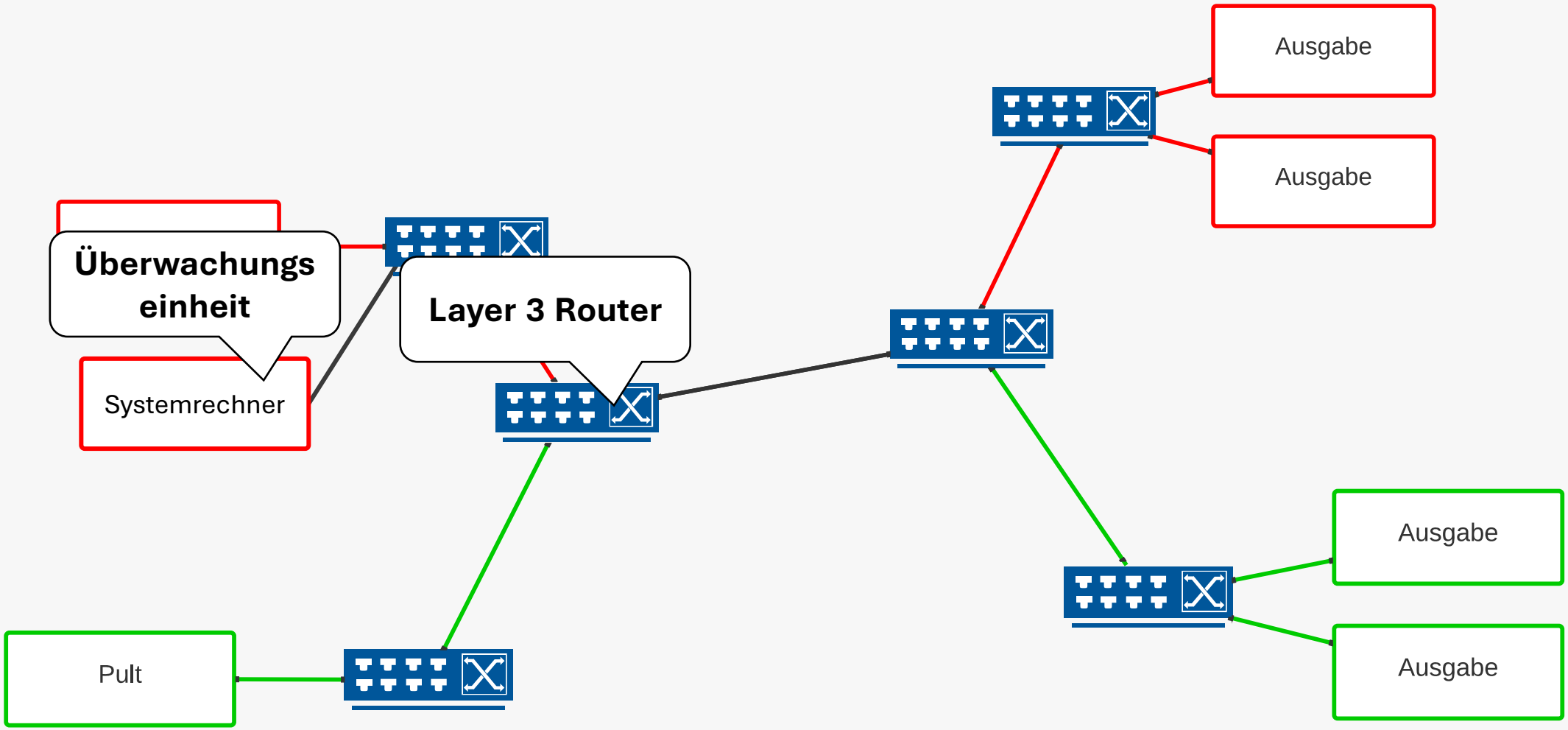
APIs:

- Application Programming Interface (Schnittstelle)
- Werden von Programmen oder Geräten bereitgestellt

# Herausforderung: Mehrere VLANs


Ausgabe
Ausgabe
Überwachungs einheit
Systemrechner
Anderes VLAN
Anderes VLAN
Ausgabe


Ausgabe
Ausgabe
Überwachungs einheit
Systemrechner
Ausgabe
Ausgabe
Pult


Ausgabe
Ausgabe
Überwachungs einheit
Layer 3 Router
Systemrechner
Ausgabe
Ausgabe
Pult

# Herausforderung: Systemrechner?

Bleibt der Systemrechner immer online?

# Was ist Idle und was ist Belastung?

Was ist normal und was nicht?

# Überwachungseinheit



- Wird von tribe29 (München) entwickelt
- Basiert auf Linux und Nagios
- Drei Versionen
  - Raw Edition
    - Kostenlos
    - Eingeschränkte Funktionalität
  - Cloud/Free Edition
    - Kostenlos
    - Volle Funktionalität
    - bis zu 30 Geräte
  - Enterprise Edition
    - Kostenpflichtig
    - Volle Funktionalität

PRTG NETWORK MONITOR

- Wird von Paessler (Nürnberg) entwickelt
- Windows basiert
- Drei Versionen
  - Trail Version
    - Kostenlos
    - Bis zu 100 Sensoren
  - Kommerzielle Versionen
    - Lizensierung nach Sensoren
    - Volle Funktionalität

# Vergleich der wichtigsten Merkmale

| Merkmal | CheckMK | PRTG Network Monitor |
|---|---|---|
| Installation | Kann auf Linux oder als Docker-Container installiert werden. | Windows-basierte Installation. |
| Benutzeroberfläche | Weboberfläche, eher technisch und weniger intuitiv als PRTG. | Sehr intuitive Web- und mobile Oberfläche. |
| Lizenzierung | Open Source (Raw Edition) und kommerziell (Enterprise Edition). | Kommerziell, kostenlose Version mit Limit. |
| Erweiterbarkeit | Kommerziell, kostenlose Version mit Limit. | Eingeschränkter, aber einfacher zu verwenden. |
| Monitoring-Methode | Agentenbasiert und agentenlos. | Hauptsächlich agentenlos. |
| Benachrichtigungssystem | Flexibles Benachrichtigungssystem, gut anpassbar. | Umfangreiche, einfache Konfiguration. |
| Leistung und Skalierbarkeit | Sehr gut für große Netzwerke geeignet. | Ebenfalls gut, aber ab einer gewissen Größe wird es teurer. |
| Integration | Gute Integration mit anderen Tools (z.B. Grafana, Prometheus). | Begrenzte Integration, vor allem mit Windows-Umgebungen. |
| Kosten | Kostenfrei (Open Source) oder kommerzielle Preise. | Kommerziell, Preise steigen mit der Anzahl der Sensoren. |

# Fazit und Empfehlungen

## Wann CheckMK?

- Flexible und erweiterbare Lösung
- Für komplexes Netzwerke
- Steilere Lernkurve

## Wann PRTG?

- einfach zu bedienende Lösung mit schnellem Setup
- für ein kleines bis mittelgroßes Netzwerk
- Benutzerfreundlichkeit
- Nicht kostenlos

# Take Home Messages

**1**

Monitoring macht den Zustand des Netzwerkes sichtbar!

**2**

Alarmierungen helfen bei dem Erkennen von Problemen.

**3**

Habt immer stetig einen Rechner im Netzwerk für die Überwachung!

## Leo Künne

Geschäftsführer der CX-Networks GmbH

Seit 2015 in der Branche