

## *NETZWERKTECHNIK IN AUDIO- UND VIDEONETZWERKEN*

Referent Gunnar Schamber

12.09.2018

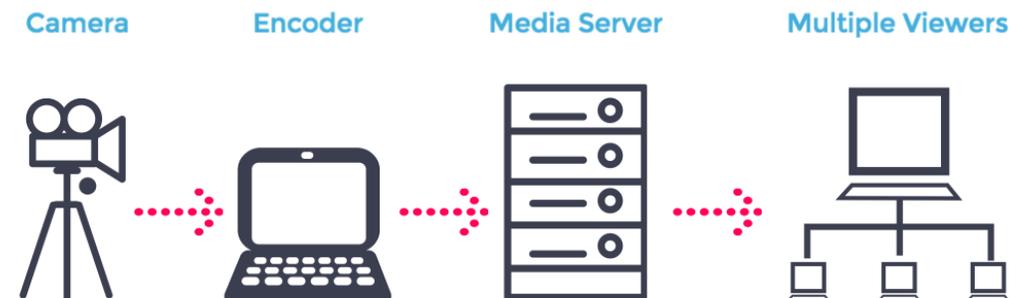
## BESONDERHEITEN VON AUDIO- VIDEONETZWERKEN

Größerer Datentransfer durch Video- und Audio Streams.

Audio- und Bilddaten sind im Gegensatz zu Textdaten und Datenbankdaten um vieles Größer.

Verteilung der Daten durch Multicasts

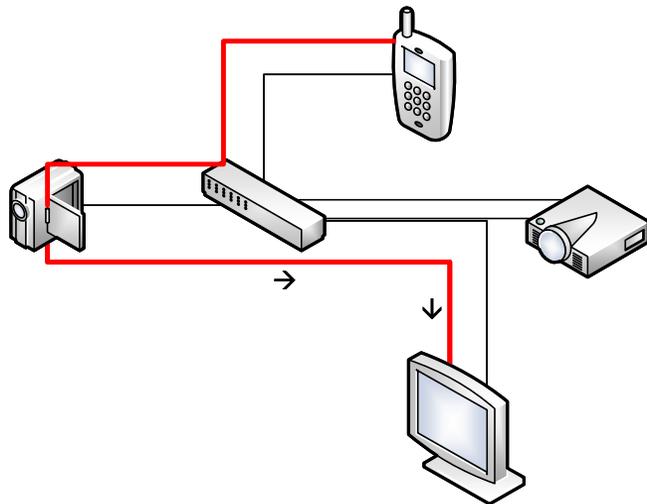
Name	Typ	Größe <sup>^</sup>
 Planung Präsentation.txt	Textdokument	3 KB
 Planung Präsentation.docx	Microsoft Word-Dokument	15 KB
 Text im Bild.PNG	PNG-Datei	53 KB
 Text im Bild.JPG	JPG-Datei	90 KB



## UNICAST

### Unicast

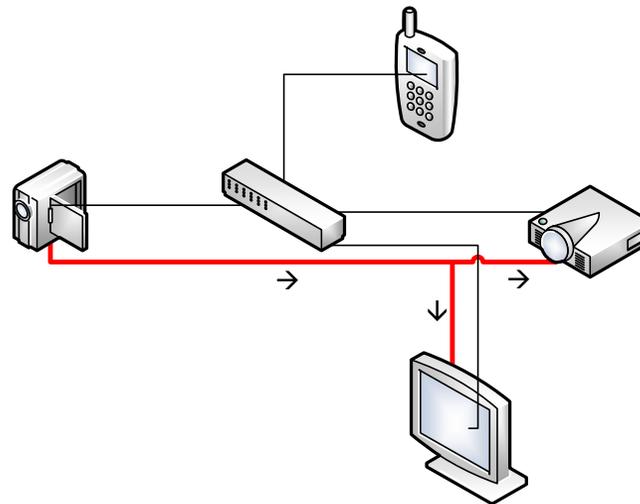
Kommunikation zwischen zwei Geräten



## MULTICAST

### Multicast

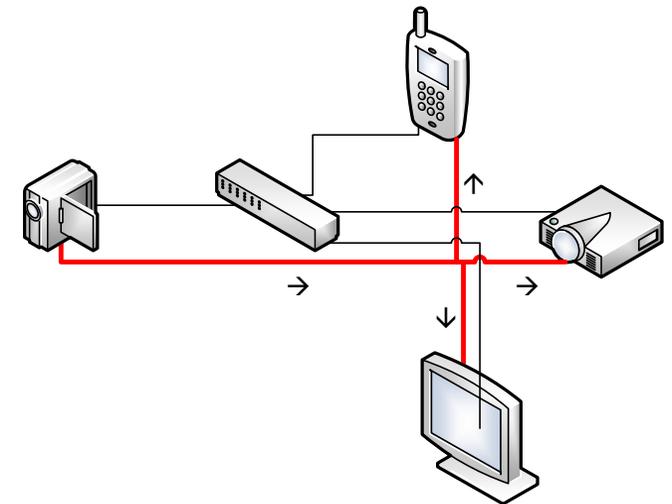
Ein Gerät sendet an alle Geräte, die sich zu diesem Datenstrom angemeldet haben



## BROADCAST

### Broadcast

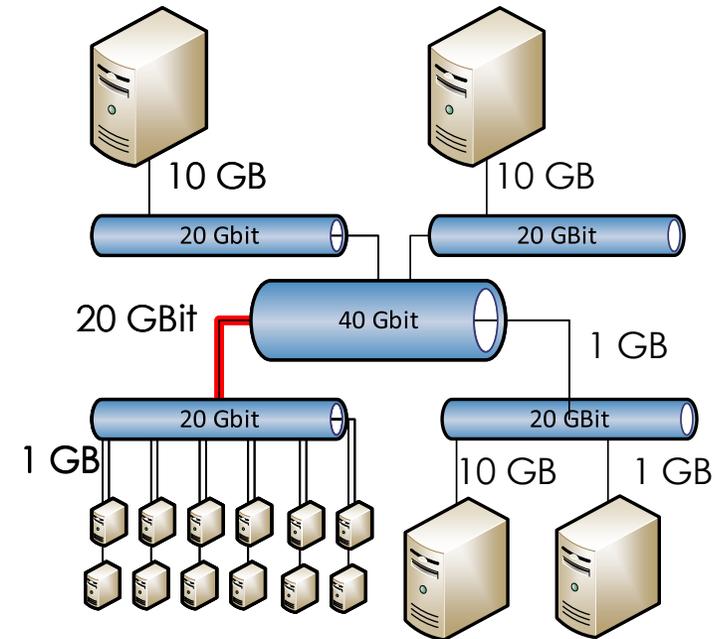
Ein Gerät sendet in das Netzwerk an alle Stationen



## VERMEIDUNG VON ENGPÄSSEN IN DER DATENÜBERTRAGUNG

Bandbreite der Netzwerkanlüsse und Backbones

Priorisierung von verschiedenen Datenpaketarten  
Unterstützung von Quality of Services (QoS) in den Switchs  
Bei Einsatz von Dante und QLAN -> Trennung durch VLAN



## POWER OVER ETHERNET (POE)

PoE = IEEE 802.3af-2003 max. 15,4 Watt pro Gerät

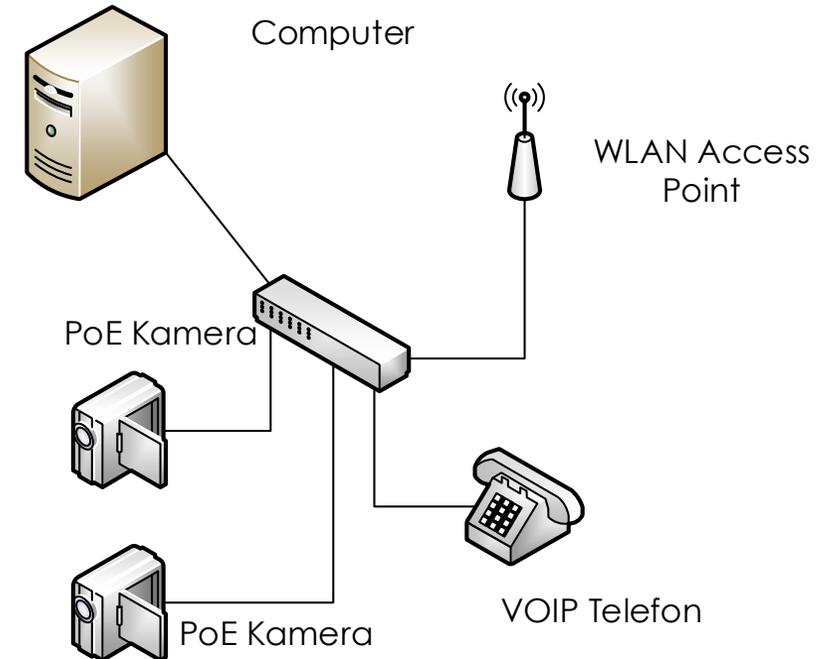
PoE+ = IEEE 802.3at-2009 max. 25,5 Watt pro Gerät

4PPoE oder PoE++ = IEEE 802.3bt

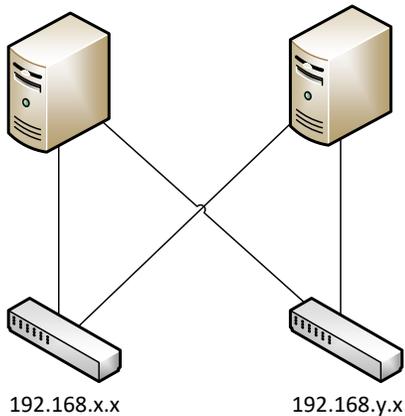
Level 3 max. 55 Watt

Level 4 max. 100 Watt

Beachtung der Gesamtleistung des Switch

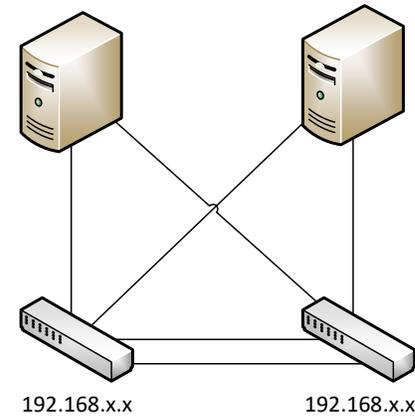


## AUSFALLSICHERHEIT IM NETZWERK



Ausfallsicherheit bei QSC  
und anderen  
Audionetzwerken

Stromausfallsicherung (USV)



Ausfallsicherheit in der IT ohne  
Audionetzwerk.

STP Ausfall ca. 30 Sekunden

RSTP Ausfall ca. 1 Sekunde

MSTP überwacht VLANs mit

## SICHERHEIT IM NETZWERK

- Standard Kennwörter ändern
- Nicht genutzte Anschlüsse sperren oder abschalten
- Zugriff auf die Hardware durch Zugriffskontrolle der Schränke
- Genutzte Anschlüsse auf die MAC Adresse der angeschlossenen Geräte beschränken
- Wenn die verschlüsselte Übertragung der Datensignale nicht möglich → Zugriff auf das Netzwerk nur auf die nötigsten Geräte beschränken.
- Firewall
- Auf vollständige Dokumentation achten



## VIRTUAL LOCAL AREA NETWORK „VLAN“

- Netzwerke in einem Netzwerk
- Performanctesteuerung
- Sicherheit durch Trennung von Netzwerken
- Konfiguration: welcher Port gehört zu welchem VLAN (vom Netzwerkadministrator vergeben)
- Angeschlossene Geräte können meist keine eigene VLAN Kennung rausgeben

## ROUTER

- Verbinden von verschiedenen Netzwerken
- Verbindung von verschiedenen Standorten
- Blockiert Broadcast
- Durch Firewalls werden ungewollte Kommunikationen unterbunden
- Ermöglicht auch Einwahl in Netzwerke per VPN
- Manche Layer3 Switchs haben auch Routing implementiert.
- QLAN kann geroutet werden
- Wie sieht es in Zukunft mit IPv6 aus?

## RICHTIGE PLANUNG DER HARDWARE

- Verarbeitung von Multicast?
- Unterstützung des passenden (Q)uality (o)f (S)ervices?
- Genügend Bandbreite im Backbone?
- Ausreichende Stromversorgung und Kühlung?
- Ausfallsicherheit ist RSTP implementiert?
- Sicherheit ausreichend für Kunde?
- Hardware einsparen durch VLAN Nutzung!

*VIELEN DANK!*

*[HTTPS://WWW.HEIMEDIA.DE/486/PRAESENTATIONEN.HTM](https://www.heimedia.de/486/praesentationen.htm)*

***HeiMedia*** - *Michael Heidler und Tim Heidler GbR*

<http://www.HeiMedia.de>

Mail: [info@heimedia.de](mailto:info@heimedia.de)

Referent Gunnar Schamber

12.09.2018