

AV-Netzwerktechnik

Netzwerkanalyse mit Wireshark

Benny Platte



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences



[hs-mittweida.de](https://www.hs-mittweida.de)

Echtzeit-Audio/Video-Netzwerke

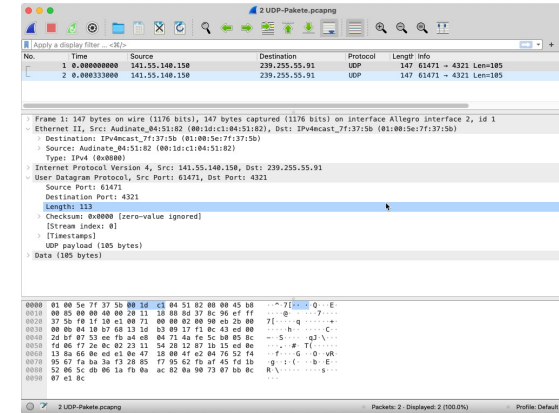
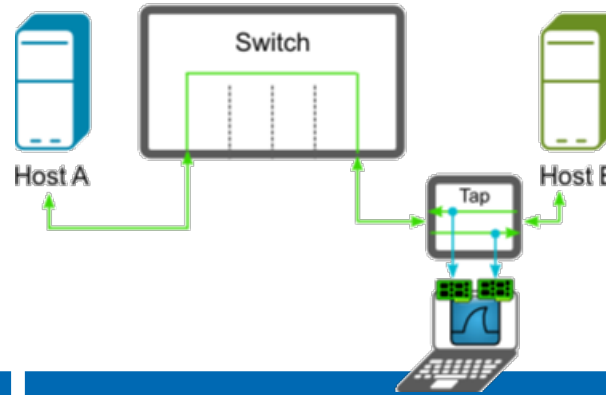
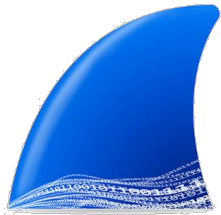
digitale
Übertragung

Töne
und deren
Digitalisierung

Grundlagen
Netzwerk-
technik



Themen



Vorb

Wireshark Literatur und Software

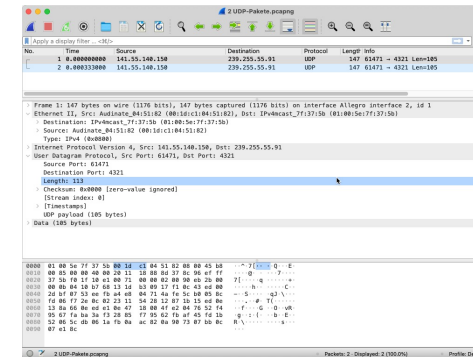
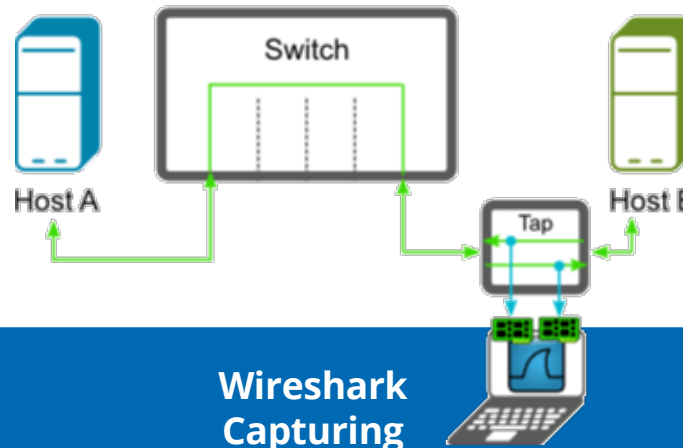
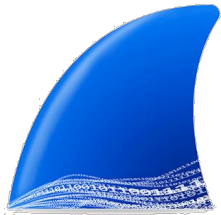
Wireshark Capturing

Wireshark Pakete im Detail

- Hubbing
- Man in the middle
- Tapping
- Port Mirroring

- Bedienung Software
- Paketzusammensetzung
- Herleitung

Sie können...



Wireshark Literatur und Software

Wireshark Capturing



- Beschreiben, wie Sie Pakete aufzeichnen würden
- Technologische Voraussetzungen benennen
- Vor- und Nachteile von Hubbing, Tapping und Port Mirroring erklären
- für einen gegebenen Fall Vorschläge unterbreiten, welches Verfahren Sie anwenden würden

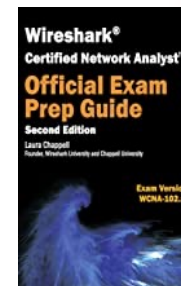
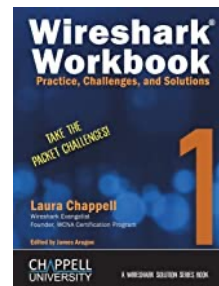
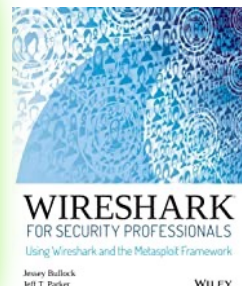
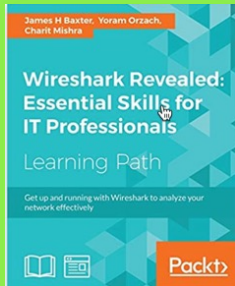
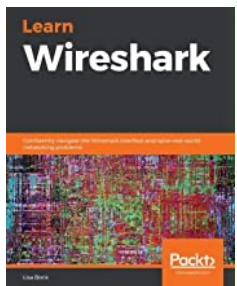
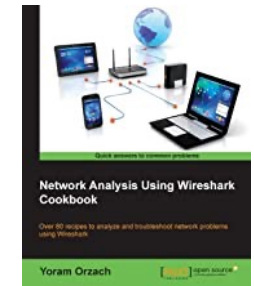
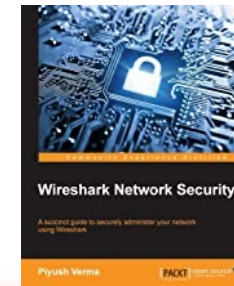
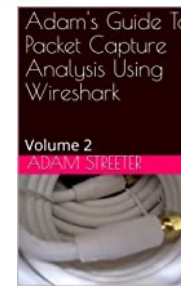
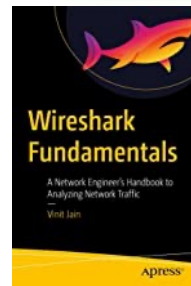
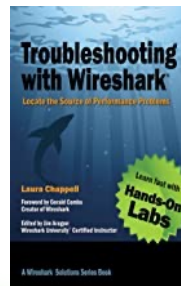
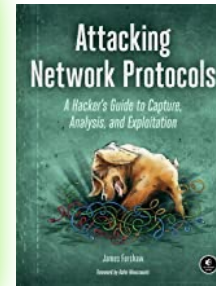
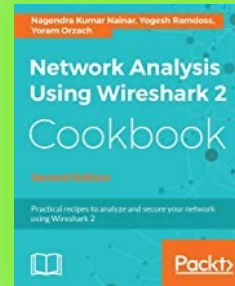
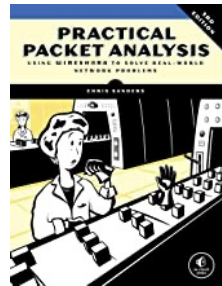
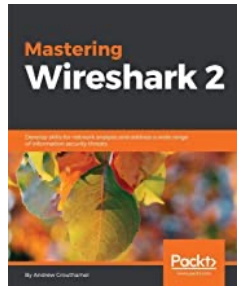
Wireshark Pakete im Detail

- Mit Hilfe von Wireshark ein als Hexwert aufgezeichnetes Paket dekodieren und die enthaltenen Adressen benennen
- Dekodieren, ob es sich um ein IPv4 oder IPv6-Paket handelt
- Angeben, ob es sich um ein fragmentiertes Paket handelt

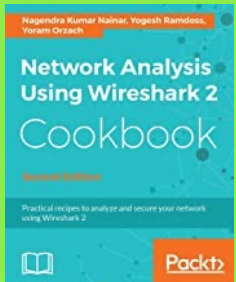
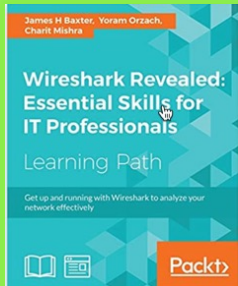


Bücherdaten befinden sich in OPAL unter

Vorb



Bücherdaten in OPAL



OPAL

Suche Benny Platte

Startseite Lehren & Lernen Kursangebote AV-Netzwerke

AV-Netzwerke

AV-Netzwerke

- AV-Netzwerke
 - 00: Einführung
 - Peer-to-Peer-Hilfeforum
 - Vorschläge für Prüfungsfragen
 - Skripte/Vorbereitungen
 - nützliche Literatur
 - 01: Töne und Digitalisierung
 - Vorbereitung: Musikstück/Lit
 - 03 Grundlagen Netzwerktechnik
 - Vorbereitung, Material

nützliche Literatur

Altrichter, T. (2014). *Ethernet-basierte lokale Audionetzwerke im Vergleich: Erklärung und Diskussion verschiedener Technologien und Anwendungsmöglichkeiten*. AV Akademikerverlag.

Chappel, L. (2018). *Wireshark® 101: Einführung in die Protokollanalyse - Deutsche Ausgabe* (22018. Aufl.). mitp.

Hauser, B. J., Lehrer, Lehrbeauftragter, Industrieelektronik, Informationstechnik, & Dipl Ing. (2018). *Fachwissen Netzwerktechnik Modelle - Geräte - Protokolle* (3. Auflage). Haan-Gruiten Verlag Europa-Lehrmittel, Nourney, Vollmer GmbH & CoKG.

Hein, M., Ladner, R., & Scholz, U. (2021). *Wireshark - Standard-Tool zur Analyse von Netzwerken: Praxiswissen: Netzwerkprotokolle aufzeichnen, darstellen und analysieren*. Independently published.

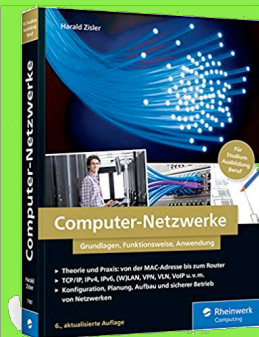
Hildebrand, A. (o. J.). *AES67 Practical Guide*. Ravenna.

Lock, D. B. (2019). *Digitale Audiosignale in Netzwerken*. Hochschule der Medien Stuttgart.

Riselvato, J. (2020). *The FFmpeg Quick Reference of 100+ Scripts for Video, Audio and Streaming*. Independently published.

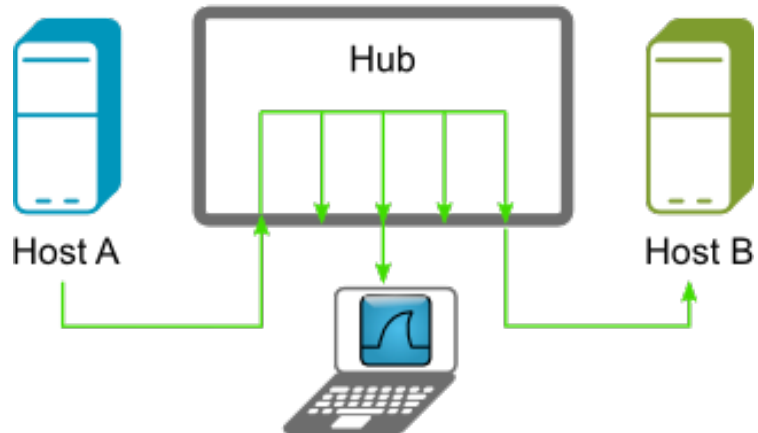
Schreiner, R. (2019). *Computernetzwerke: Von den Grundlagen zur Funktion und Anwendung. Inkl. E-Book* (7., aktualisierte Edition). Carl Hanser Verlag GmbH & Co. KG.

Zisler, H. (2020). *Computer-Netzwerke: Grundlagen, Funktionsweisen, Anwendung. Für Studium, Ausbildung und Beruf. Inkl. OpenWRT* (6. Aufl.). Rheinwerk Computing.

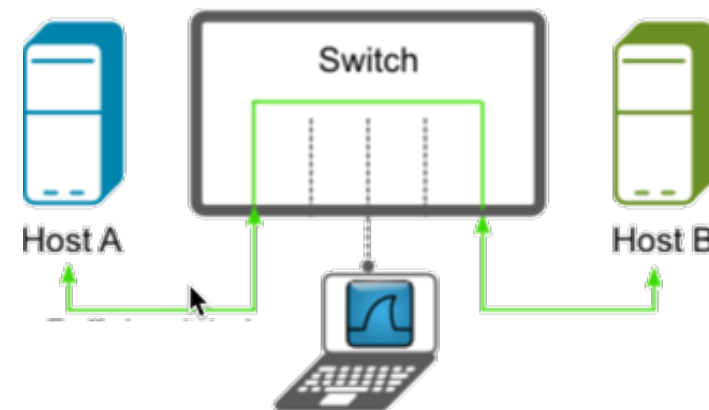
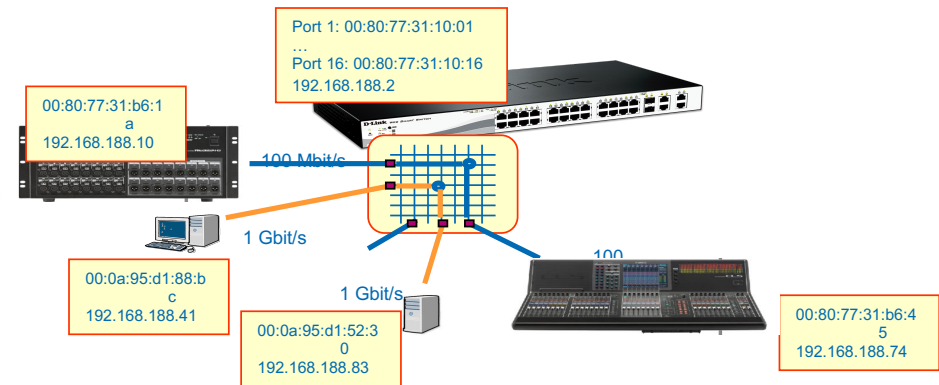


Wireshark Setup

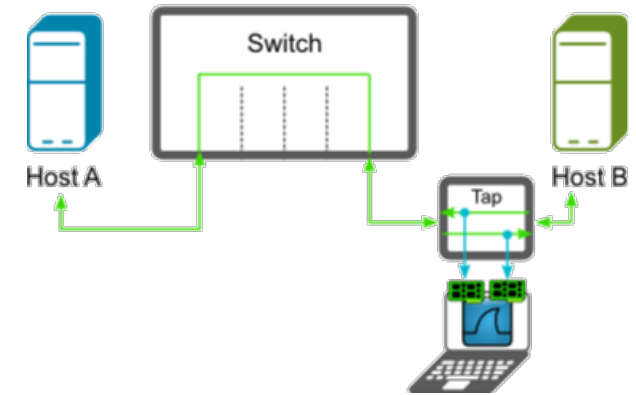
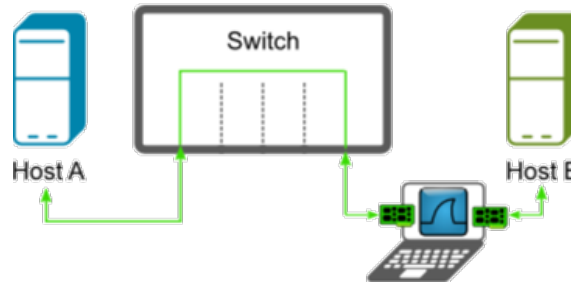
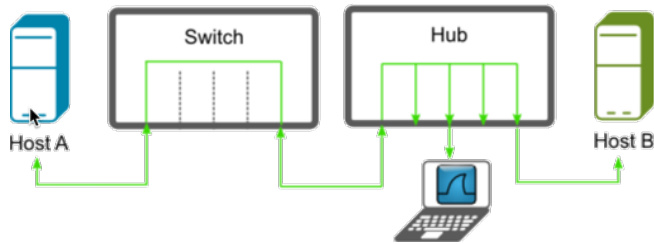
Shared Network (früher, WLAN)
„jeder hört alles“



Switched Network

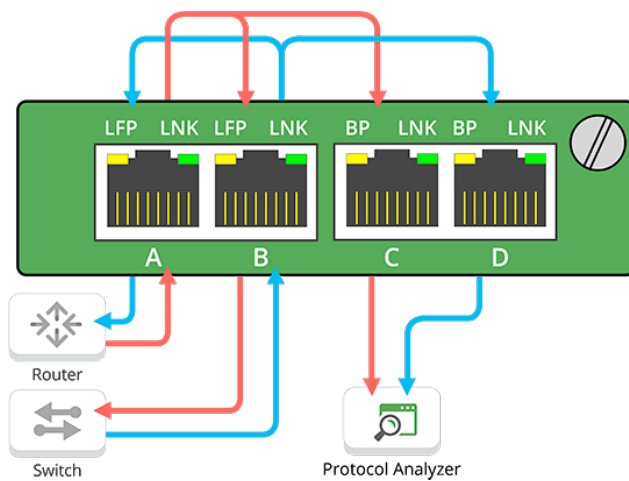


Wireshark Aufzeichnung an switched network

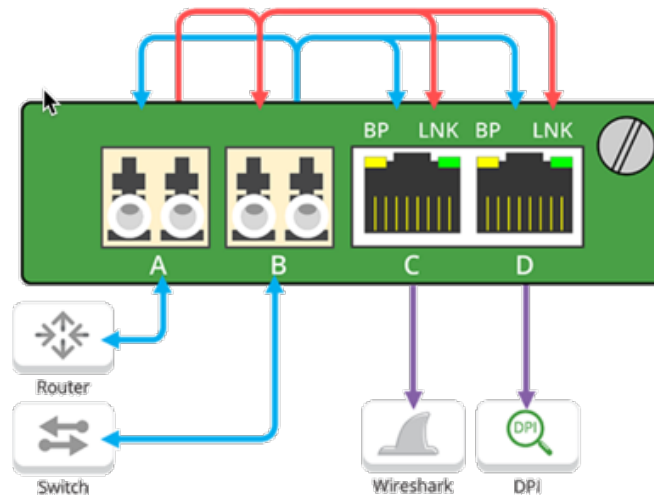


Wireshark Aufzeichnung „tapped“

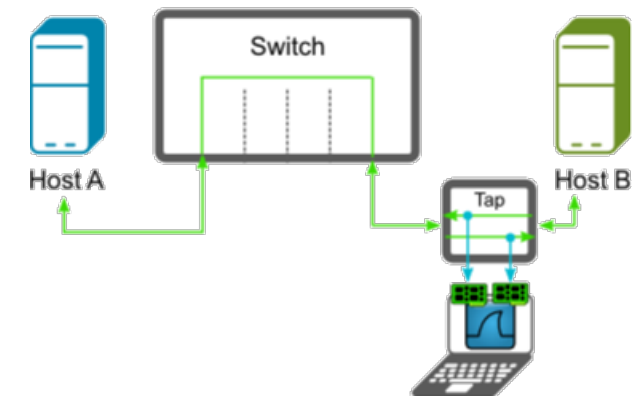
„Breakout-Tap“



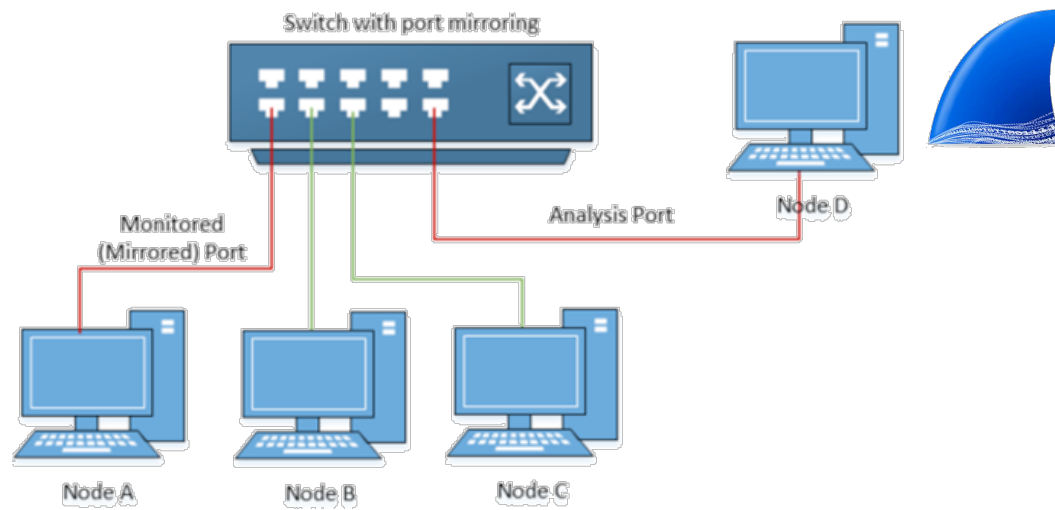
„Media Conversion TAP“



„Tapping“



Managed Switch: Port Mirroring



Managed Switch: Port Mirroring

LINKSYS

Linksys Smart Gigabit Switches



8-Port Business Smart Gigabit Switch (LGS308)

18-Port Business Smart Gigabit Switch (LGS318)

26-Port Business Smart Switch (LGS326)

Key Features

- 8, 18, or 26 Gigabit Ethernet ports
- Easy configuration and management
- Proven performance and reliability
- Energy efficient
- Network security
- IP telephony support
- IPv6 support
- Limited lifetime warranty

Designed for business-class management, security, speed, and quality of service, Linksys Smart Gigabit Switches provide a network your business can grow on.

Quality of Service (QoS)

Numerous QoS features ensure that traffic is prioritized properly to deliver the best possible user experience for real-time applications like voice and video along with bandwidth-intensive graphic/video file uploads and downloads. ICMP-snooping limits IP multicast traffic to the ports that requested it, enabling the rest of the network to operate at peak efficiency.

Network Security

Unauthorized access to the network and mission-critical data is a constant concern. Linksys smart switches help secure networks through port authentication and MAC-based port security, requiring clients to authenticate themselves before any data is passed. Advanced DHCP snooping and IP-MAC binding functions ensure network integrity and help prevent network attacks.

Network Expansion

Linksys smart switches include features for quickly expanding and growing your network. Multiple high-bandwidth trunks between switches enhance availability and redundancy. Spanning Tree Protocol (STP) and Storm Control features help control planned or inadvertent cable loops, so you can confidently build a mesh of switches and quickly expand your network to support your growing workforce.

NETGEAR
BUSINESSData Sheet
Gigabit Ethernet Plus SwitchesControl and Configure Beyond
Plug-and-Play Connectivity

CISCO SG350-10p

Also shown: Internet Service from Cisco RV340



Guide Version:

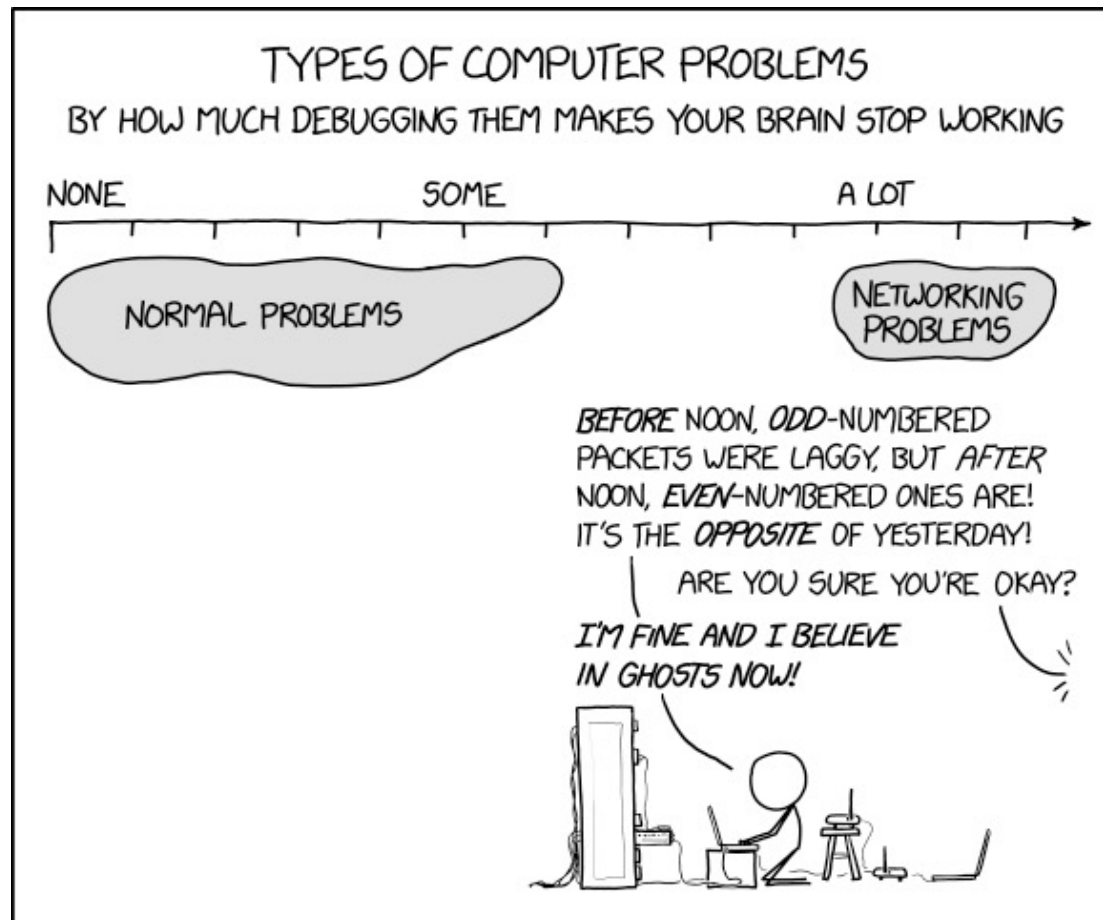
0.993, November 2020

SG350 Firmware Version:

2.4.0.94



Wireshark Paketanalyse



Wireshark Paketanalyse

The screenshot shows the Wireshark interface with a packet capture of two UDP packets. The packet list pane shows two packets, both of length 147 bytes, captured on interface Allegro interface 2. The packet details pane shows the structure of the first packet: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (UDP). The UDP payload is 105 bytes. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	141.55.140.150	239.255.55.91	UDP	147	61471 → 4321 Len=105
2	0.000333000	141.55.140.150	239.255.55.91	UDP	147	61471 → 4321 Len=105

Packet Details (Frame 1):

- Frame 1: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface Allegro interface 2, id 1
- Ethernet II, Src: Audinate_04:51:82 (00:1d:c1:04:51:82), Dst: IPv4mcast_7f:37:5b (01:00:5e:7f:37:5b)
 - Destination: IPv4mcast_7f:37:5b (01:00:5e:7f:37:5b)
 - Source: Audinate_04:51:82 (00:1d:c1:04:51:82)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 141.55.140.150, Dst: 239.255.55.91
- User Datagram Protocol, Src Port: 61471, Dst Port: 4321
 - Source Port: 61471
 - Destination Port: 4321
 - Length: 113
 - Checksum: 0x0000 [zero-value ignored]
 - [Stream index: 0]
 - [Timestamps]
 - UDP payload (105 bytes)
- Data (105 bytes)

Packet Bytes:

```

0000  01 00 5e 7f 37 5b 00 1d c1 04 51 82 08 00 45 b8  ...^7[...Q...E
0010  00 85 00 00 40 00 20 11 18 88 8d 37 8c 96 ef ff  ...@...7...
0020  37 5b f0 1f 10 e1 00 71 00 00 02 00 90 eb 2b 00  7[...q...+...
0030  00 0b 04 10 b7 68 13 1d b3 09 17 f1 0c 43 ed 00  ...h...C...
0040  2d bf 07 53 ee fb a4 e8 04 71 4a fe 5c b0 05 8c  ...S...qJ.\...
0050  fd 06 f7 2e 0c 02 23 11 54 28 12 87 1b 15 ed 0e  ...#...T(...
0060  13 8a 66 0e ed e1 0e 47 18 00 4f e2 04 76 52 f4  ...f...G...0...vR...
0070  95 67 fa ba 3a f3 28 85 f7 95 62 fb af 45 fd 1b  ...g...(:...b...E...
0080  52 06 5c db 06 1a fb 0a ac 82 0a 90 73 07 bb 0c  R.\...s...
0090  07 e1 8c
  
```

Wireshark Paketanalyse

```
0000  01 00 5e 7f 37 5b 00 1d c1 04 51 82 08 00 45 b8
0010  00 85 00 00 40 00 20 11 18 88 8d 37 8c 96 ef ff
0020  37 5b f0 1f 10 e1 00 71 00 00 02 00 90 eb 2b 00
0030  00 0b 04 10 b7 68 13 1d b3 09 17 f1 0c 43 ed 00
0040  2d bf 07 53 ee fb a4 e8 04 71 4a fe 5c b0 05 8c
0050  fd 06 f7 2e 0c 02 23 11 54 28 12 87 1b 15 ed 0e
0060  13 8a 66 0e ed e1 0e 47 18 00 4f e2 04 76 52 f4
0070  95 67 fa ba 3a f3 28 85 f7 95 62 fb af 45 fd 1b
0080  52 06 5c db 06 1a fb 0a ac 82 0a 90 73 07 bb 0c
0090  07 e1 8c
```

