TINA / ProfiNet-WATCHDOG / TINA-II

Benutzerhandbuch
V1.14

Deutsch

Handbuch passend zur Firmware V1.11 und neuer!

© Copyright by PI 2017-2025

Inhalt

1 Allgemeines

1.1 Zum Handbuch

Dieses Handbuch beschreibt die Geräte ***TINA*** / ***TINA-II*** (Abkürzung für „**T**ragbarer **I**ntelligenter **N**etzwerk-**A**nalyser“) und ProfiNet-WATCHDOG, im nachfolgenden als Gerät, Analysegerät oder Analyzer bezeichnet.

Diese Dokumentation kann über die Webseite des Produkts unter Downloads ➔ Dokumentation heruntergeladen werden.

Das Handbuch richtet sich an folgende Benutzergruppen:

- Planer
- Betreiber
- Inbetriebnehmer
- Service- und Wartungspersonal

Vor der Verwendung des Geräts ist unbedingt das Handbuch zu lesen.

Bei Fragen und / oder Problemen wenden Sie sich bitte an den technischen Support Ihres Vertriebspartners.

2 Systemvoraussetzungen

2.1 Software

Für den Einsatz / Gebrauch des Analysegeräts benötigen Sie folgende Tools / Software:

- Internet-Browser (z. B. Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome)

Der Einsatz des Geräts ist dabei unabhängig von Betriebssystem und Browser des jeweiligen Computers, Tablets oder Handys.

Wichtig:
Um die Webseite korrekt anzuzeigen, stellen Sie bitte sicher, dass in Ihrem Browser JavaScript nicht deaktiviert ist.

Falls an Ihrem ProfiNet-Watchdog obwohl beide LAN-Schnittstellen angeschlossen sind und das Gerät mit 24V DC versorgt ist und keine Data-LEDs beider LAN-Buchsen leuchten und Sie keine Daten in der Aufzeichnung bekommen obwohl die Kommunikation über das Gerät läuft, dann bitte diese Einstellung im Gerätemanager Ihrer Netzwerk-Karte prüfen: „Energy-Efficient Ethernet“

Dieser Eintrag bitte auf „disabled“ setzen und übernehmen. Dann müssen im selben Zug die LEDs aufleuchten und Sie sehen in der Aufzeichnung sofort Daten.

2.2 Hardware

Für die Inbetriebnahme und Verwendung des Geräts benötigen Sie, neben dem Analysegerät, folgende Hardware:

- Gerät mit WLAN-Schnittstelle (für den Zugriff per WLAN)
- 24VDC-Versorgung über abziehbaren Stecker oder USB-Versorgung aus dem PC / Power-Pack
- 2 x Ethernet-Kabel (LAN)

3 Inbetriebnahme

Das Gerät besitzt eine WLAN-Schnittstelle und zwei LAN-Schnittstellen. Die WLAN-Schnittstelle dient dazu, dass Sie sich mit Ihrem Laptop, Tablet oder Handy mit dem Gerät verbinden können. Die LAN-Schnittstellen werden zur Analyse des Netzwerkverkehrs verwendet.

Hinweis:
Bei den TINA- und TINA-II-Geräten ist der Zugriff auf den Webserver auch über die LAN-A-Schnittstelle des Geräts möglich.

Falls Sie die WLAN-Schnittstelle nicht verwenden dürfen oder können, haben Sie die Möglichkeit mit dem separat erhältlichen „Ethernet über USB“-Adapter Ihr Gerät um eine weitere LAN-Schnittstelle zu erweitern, mit welcher Sie dann auf das Gerät zugreifen können. Bei Interesse wenden Sie sich bitte an Ihren Vertriebspartner.

Wichtig:
Dieses Kapitel beschreibt den Auslieferungszustand des Geräts. Über die Konfiguration können Sie z. B. auch eine Bridge zwischen LAN und WLAN konfigurieren.

3.1 Webserverzugriff

Der Zugriff auf das ***TINA***- und ***TINA-II***-Gerät kann im Auslieferungszustand über zwei Wege erfolgen: entweder über die WLAN- oder über die LAN-A-Schnittstelle.

Der Zugriff auf den ProfiNet-WATCHDOG kann nur über die WLAN-Schnittstelle erfolgen.

Falls Sie über den „Ethernet über USB“-Adapter verfügen, dann können Sie auch über den Adapter auf den Webserver des Geräts zugreifen. Dies gilt für alle Gerätetypen.

3.1.1 Zugriff per WLAN

Für den Zugriff per WLAN, stellen Sie bitte sicher, dass Ihre WLAN-Schnittstelle aktiviert ist und lassen Sie sich dann die verfügbaren WLAN-Netzwerke anzeigen.

In der Liste der verfügbaren WLAN-Netze sollte nun ein Netzwerk mit der SSID „TINA WiFi“ bzw. „ProfiNet-WATCHDOG WiFi“ (je nach Gerätetyp) zu sehen sein. Dieses Netzwerk ist unverschlüsselt, weshalb Sie kein Passwort benötigen, um sich damit zu verbinden.

Die Geräte sind so konfiguriert, dass auf der WLAN-Schnittstelle ein DHCP-Server aktiv ist. Ist die WLAN-Schnittstelle Ihres Computers, Tablets oder Handys auf DHCP-Client eingestellt (Standardeinstellung), so können Sie direkt auf das Gerät zugreifen. Haben Sie eine feste IP-Adresse eingestellt, so müssen Sie entweder auf DHCP umstellen oder Ihre IP-Adresse umstellen, sodass Sie sich im Subnetz 192.168.1.0/24 befinden (Adressen von 192.168.1.1 bis 192.168.1.254). Die Adresse 192.168.1.1 darf nicht verwendet werden, da es die IP-Adresse des Analyzers ist.

3.1.2 Zugriff per LAN

Möchten Sie per LAN (mit einem Netzwerkkabel) zugreifen, so müssen Sie zunächst Ihren Computer mit einem LAN-Kabel mit der LAN-A-Schnittstelle des Geräts verbinden. Natürlich können auch beide Geräte an einen Switch oder Hub angeschlossen werden.

Auf der LAN-Schnittstelle läuft standardmäßig kein DHCP-Server. Daher müssen Sie die Einstellungen der Netzwerkkarte Ihres Computers öffnen und in den IP-Einstellungen eine feste IP-Adresse aus dem Subnetz 192.168.2.0/24 (Adressen von 192.168.2.1 bis 192.168.2.254) zuweisen. Die IP-Adresse 192.168.2.1 ist bereits durch den Analyzer belegt und darf somit nicht verwendet werden.

Wichtig:
Der Zugriff über die LAN-A-Schnittstelle ist nur bei den TINA- und TINA-II-Geräten möglich.

3.1.3 Zugriff per USB-LAN

Falls Sie den separat erhältlichen „Ethernet über USB“-Adapter erworben haben, können Sie auch mit diesem auf das Gerät zugreifen. Schließen Sie hierzu zunächst den Adapter an die USB-Buchse Ihres Geräts an. Als nächstes müssen Sie nur noch Ihren Computer oder Switch über ein Netzwerkkabel mit dem Adapter verbinden.

Im Werkszustand ist auf der USB-LAN-Schnittstelle ein DHCP-Server aktiviert, wodurch automatisch IP-Adressen an die Netzwerkteilnehmer verteilt werden. Falls Ihr Computer bereits auf DHCP eingestellt ist (Standardeinstellung) müssen Sie nichts weiteres unternehmen. Andernfalls müssen Sie in den Einstellungen Ihrer Netzwerkkarte auf DHCP umstellen oder aber Ihrem PC eine Adresse aus dem Subnetz 192.168.0.0/24 (Adressen von 192.168.0.1 bis 192.168.0.254) zuweisen. Die IP-Adresse 192.168.0.1 darf nicht verwendet werden, da diese vom USB-Adapter verwendet wird.

3.1.4 Weboberfläche

Sobald Sie mit dem Gerät physikalisch verbunden sind, müssen Sie einen Webbrowser öffnen und in der Adresszeile 192.168.1.1 (beim Zugriff über WLAN), 192.168.2.1 (beim Zugriff über LAN-A) oder 192.168.0.1 (beim Zugriff über USB-LAN) eingeben.

Bei der ersten Verwendung des Geräts erscheint nun ein Dialog mit mehreren Hinweisen sowie einem Eingabefeld für die Seriennummer. Dort müssen Sie nun die Seriennummer Ihres Geräts (diese steht auf der Unterseite oder rechten Seite des Geräts) eintragen und anschließend auf den Button „Gerät freischalten“ klicken:

Ist Ihre Eingabe korrekt, dann ist das Gerät nun freigeschalten und Sie können es ganz normal verwenden und bedienen. Sie werden im Anschluss auf die Konfigurationsseite des Geräts weitergeleitet *(siehe Kapitel Webserver → Konfiguration)*. Die Funktionsfreigabe des Geräts muss selbstverständlich nur ein einziges mal durchgeführt werden.

Wichtig:
Die Funktionsfreigabe dient zum Schutz Ihrer Netzwerkdaten, da standardmäßig das WLAN-Netz des Geräts offen ist und sich somit jede Person, die in Reichweite ist, damit verbinden kann.

3.2 Bridge-Schnittstellen

Der Analyzer ist in der Lage den Netzwerkverkehr zu analysieren. Hierfür besitzt das Gerät zwei LAN-Schnittstellen, die als eine Art Bridge funktionieren, d. h. alle Frames die auf Schnittstelle A empfangen werden, werden auf Schnittstelle B versendet und umgekehrt. Sind Einstellungen gesetzt, wodurch das Gerät die Aufgabe hat Frames zu ändern, so unterscheiden sich die Frames, die auf Schnittstelle A eingegangen sind von denen die auf Schnittstelle B versendet werden. Dies gilt auch in die Richtung von Schnittstelle B zu Schnittstelle A.

Haben Sie z. B. Probleme bei der Kommunikation zwischen zwei Teilnehmern, so verbinden Sie einfach den ersten Teilnehmer mit einem LAN-Kabel mit der ersten Schnittstelle und den zweiten Teilnehmer mit einem weiteren LAN-Kabel mit der zweiten Schnittstelle. Dadurch wird die komplette Kommunikation durch den Analyzer geführt.

Über den Webserver können Sie dann die Kommunikation zwischen den zwei (oder auch mehreren) Teilnehmern analysieren und den Grund für die fehlerhafte Kommunikation einfach finden.

Hinweis:
Beide LAN-Schnittstellen unterstützen das automatische Drehen der Sende- und Empfangsleitung (Auto-MDIX). Sie können daher 1:1 belegte sowie gekreuzte Netzwerkkabel verwenden.

Wichtig:
Der ProfiNet-WATCHDOG kann den Netzwerkverkehr zwischen den LAN-Schnittstellen nicht verändern oder aktiv Daten senden. Dadurch wird das RealTime-Verhalten nicht beeinflusst!

3.3 Anwenderinteraktion

Das Gerät besitzt einige Status-LEDs an der Frontseite des Geräts. Die LEDs haben folgende Bedeutung:

- **ON:** leuchtet, wenn das Gerät mit Spannung versorgt ist
- **Wi:** leuchtet bei aktivem WLAN und blinkt bei Datentransfer
- **S1:** aktuell nicht in Verwendung
- **S2:** aktuell nicht in Verwendung
- **S3:** aktuell nicht in Verwendung
- **S4:** aktuell nicht in Verwendung
- **LAN A:** leuchtet bei aktivem Linkstatus von Schnittstelle A und blinkt bei Datentransfer
- **LAN B:** leuchtet bei aktivem Linkstatus von Schnittstelle B und blinkt bei Datentransfer

Des Weiteren besitzt das Gerät an der rechten Seite (beim Tischgehäuse) bzw. an der Unterseite (beim Klemmengehäuse) zwei Taster. Diese haben die folgende Funktion:

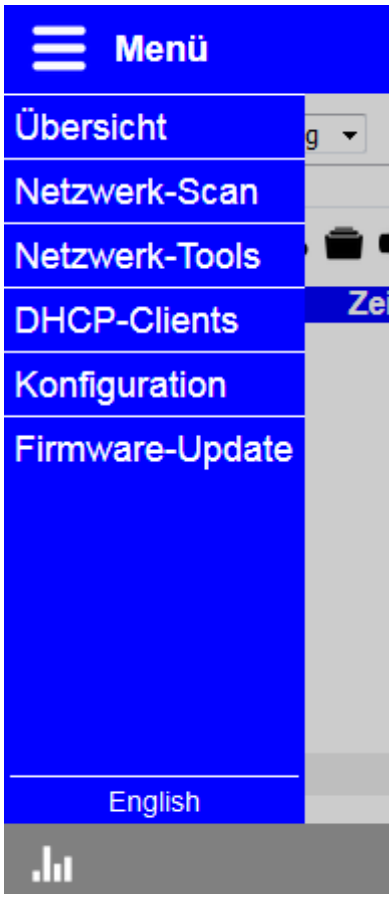
- **FS:** Taster zum Auslösen von Werkseinstellungen
- **T:** aktuell nicht in Verwendung

3.3.1 Werkseinstellungen

Wenn Sie Ihr Gerät auf Werkseinstellungen zurücksetzen möchten, dann müssen Sie den Taster „FS“ für mindestens 3 Sekunden gedrückt halten. Verwenden Sie zum Drücken der Taste am Besten eine Büroklammer.
Nachdem Sie die Taste 3 Sekunden lang gedrückt gehalten und dann wieder losgelassen haben, wird Ihr Gerät auf Werkseinstellungen zurückgesetzt. Das Gerät macht anschließend einen Neustart und sollte nach ca. 30 Sekunden mit den Standardeinstellungen, wie in diesem Kapitel beschrieben, erreichbar sein.

4 Webserver

Die komplette Bedienung des Geräts (Anzeige und Parametrierung) erfolgt über den integrierten Webserver, welcher, je nach Konfiguration, über die WLAN- und / oder LAN-A-Schnittstelle des Geräts sowie die optionale USB-LAN-Schnittstelle (per Adapter) erreichbar ist.



Die Oberflächen aller Webseiten bestehen aus einer Kopfzeile, einer Fußzeile und einem großen Inhaltsbereich. Dadurch ist auf den Seiten viel Platz für den eigentlichen Inhalt, was vor allem bei Geräten mit geringer Auflösung bzw. Bildschirmgröße, wie z. B. Smartphones, von Vorteil ist.

Um die Navigationsleiste einzublenden, müssen Sie lediglich auf das Icon oder den Schriftzug „Menü“ oben links klicken. Über die gleiche Vorgehensweise kann das Menü auch wieder ausgeblendet werden. Die Seiten des Menüs werden in den folgenden Punkten noch genauer erklärt.

Falls Sie in der Konfiguration ein Passwort festgelegt haben und aktuell am Gerät angemeldet sind, so erscheint als letzter Menüpunkt noch zusätzlich der Eintrag „Abmelden“, mit welchem Sie sich wieder abmelden können.

Die Sprache der Oberflächen kann im Menü unten links zwischen Deutsch und Englisch umgeschaltet werden.

4.1 Zugriffsschutz

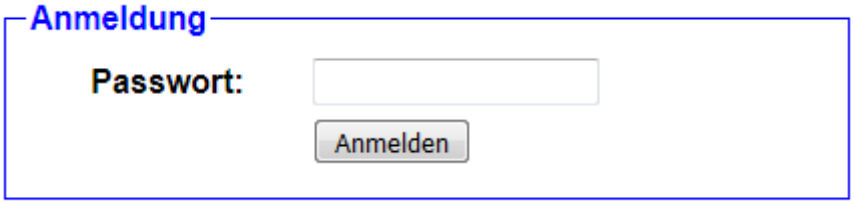
Da der Analyzer den Netzwerkverkehr, der durch das Gerät geleitet wird, analysieren sowie verändern kann und somit Zugriff auf sensible Daten hat sowie die Funktion des Netzwerks beeinflussen kann, ist es möglich und auch empfehlenswert das Gerät mit einem Passwort zu schützen. Hierdurch kann verhindert werden, dass unautorisierte Personen Ihr Netzwerk abhören und stören können.

Die folgende Tabelle zeigt, welche Passwörter es gibt und für welche Seiten diese notwendig sind:

Seite	**Passwort**	**Beschreibung**
Übersicht	Anzeige	Analyse, Überwachung und Steuerung des Netzwerkverkehrs
Netzwerk-Scan	Tool	aktive Analyse und Steuerung des Netzwerks sowie Ausführen von Testfunktionen
Netzwerk-Tool		
DHCP-Clients		
Konfiguration	Konfig	einsehen und bearbeiten der Konfiguration (auch Passwörter) sowie aktualisieren der Firmware
Firmware-Update		

Die Vergabe von Passwörtern ist über die Seite „Konfiguration“ möglich. Ist ein leeres Passwort definiert, wie es im Werkszustand der Fall ist, so ist keine Anmeldung (und Abmeldung) erforderlich. Der Zugriff kann dann also direkt erfolgen.

Möchten Sie auf eine Seite zugreifen, die mit einem Passwort geschützt ist, dann erscheint folgendes Anmeldefenster:

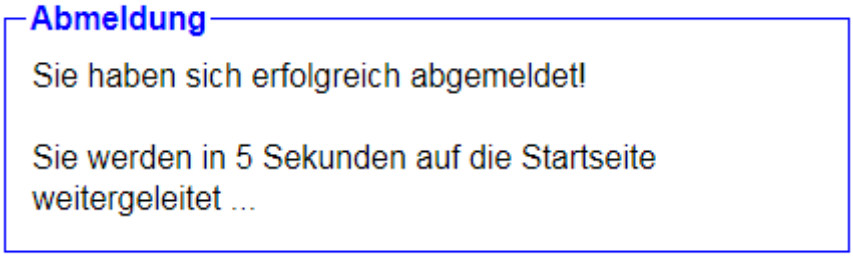


Sobald Sie das Passwort eingegeben und auf „Anmelden“ geklickt haben, werden Sie auf die Seite die Sie ursprünglich aufrufen wollten, umgeleitet.

Haben Sie sich z. B. für die Seite „Übersicht“ mit dem Anzeige-Passwort angemeldet und klicken nun auf den Menüpunkt „Konfiguration“, den Sie ebenfalls mit einem Passwort geschützt haben, so sehen Sie nun erneut die Anmeldemaske und müssen dort das Konfig-Passwort eingeben. Ihre Anmeldung mit dem Anzeige-Passwort bleibt dabei erhalten.

Aus Sicherheitsgründen empfehlen wir Ihnen nach Abschluss der Arbeiten am Gerät sich abzumelden. Hierfür gibt es im Menü den Menüpunkt „Abmelden“:

Nachdem Sie auf den Link geklickt haben, wird folgende Meldung angezeigt und Sie werden in 5 Sekunden auf die Startseite weitergeleitet:



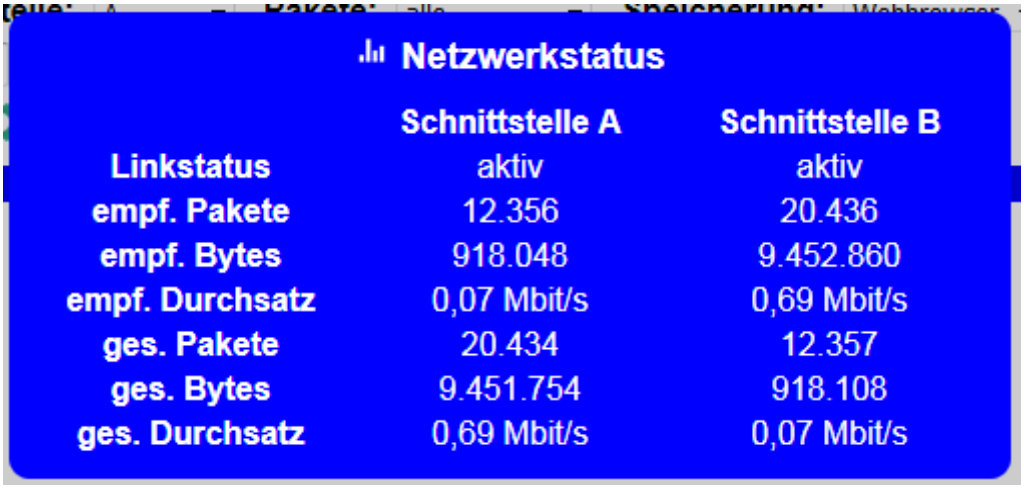
Hinweis:
Nach einem Firmware-Update oder Neustart müssen bzw. können Sie sich nicht abmelden, da durch den Geräteneustart alle Benutzer automatisch abgemeldet werden.

Wichtig:
Im Auslieferungszustand sind keine Passwörter definiert. Es kann daher jeder die Daten Ihres Netzwerks analysieren, verändern, Tools ausführen und die Konfiguration einsehen und ändern.

4.2 Statusanzeige

In der Fußzeile wird Ihnen (auf allen Seiten zur Analyse und Steuerung des Netzwerks) unter links ein Balkendiagramm-Symbol zur Anzeige des Netzwerksstatus angezeigt.

Wenn Sie auf das Icon geklickt haben, wird Ihnen der folgende Dialog angezeigt, welcher sich alle 5 Sekunden automatisch aktualisiert:

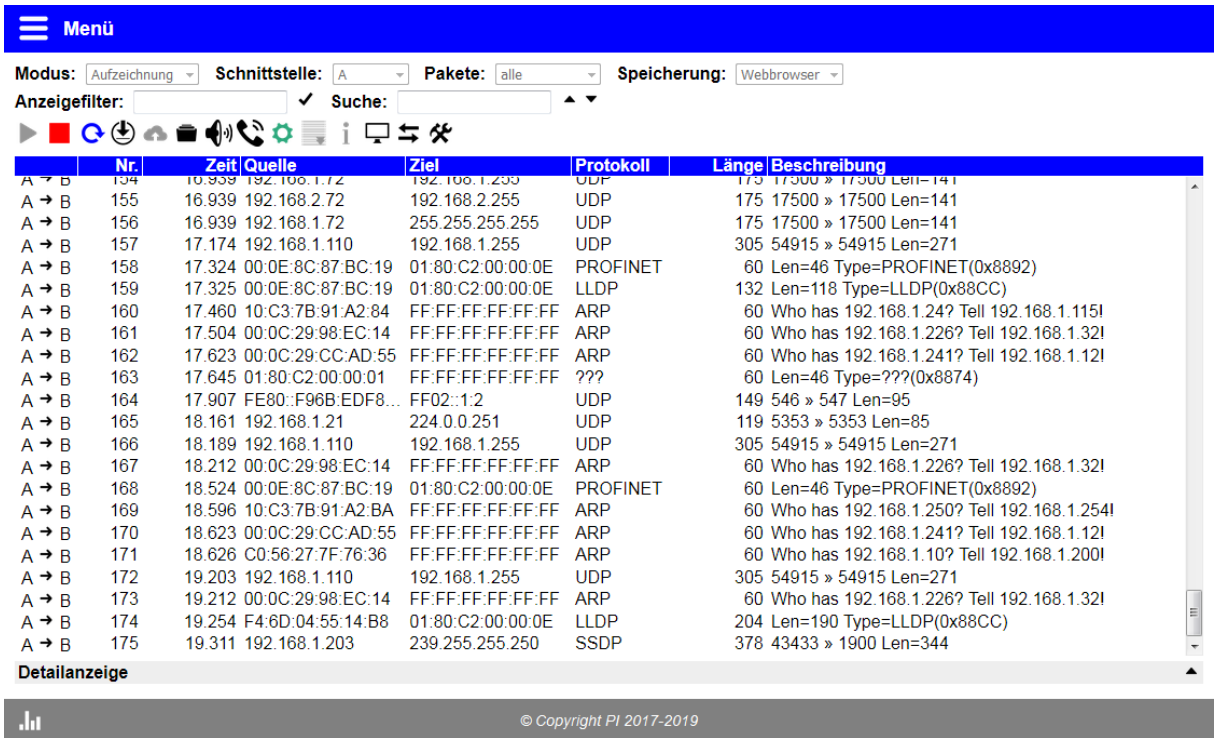


Folgende Informationen werden tabellarisch und somit auch getrennt nach Schnittstelle A und Schnittstelle B dargestellt:

- **Linkstatus:** Gibt an, ob ein Linkstatus vorhanden ist.
- **empf. Pakete:** Anzahl der empfangenen Pakete.
- **empf. Bytes:** Summe der empfangenen Bytes.
- **empf. Durchsatz:** Datendurchsatz der empfangen Bytes.
- **ges. Pakete:** Anzahl der gesendeten Pakete.
- **ges. Bytes:** Summe des gesendeten Bytes.
- **ges. Durchsatz:** Datendurchsatz der gesendeten Bytes.

Sollte im Gerät ein Fehler aufgetreten sein (z. B. Fehler beim E-Mail-Versand) oder die Verbindung zum Gerät unterbrochen sein, so wird Ihnen auf der rechten Seite der Fußzeile ein rotes Warnsymbol angezeigt. Durch einen Klick auf das Icon wird/werden Ihnen dann der/die Fehler angezeigt.

4.3 Seite Übersicht



Die Seite „Übersicht“ stellt das Herzstück des Analyzers dar und ermöglicht es den Netzwerkverkehr zu analysieren, zu überwachen und zu steuern.

Die Grundfunktion der Seite besteht darin, den Netzwerkverkehr der Bridge-Schnittstellen aufzuzeichnen und die Daten direkt im Webbrowser zu analysieren.

Bevor Sie eine Aufzeichnung starten können, müssen Sie ein paar Einstellungen festlegen.

Hierzu müssen Sie zunächst den „Modus“ wählen. Als Modus steht Ihnen „Aufzeichnung“ und „Überwachung“ zur Verfügung. Im Modus „Aufzeichnung“ können nach Bedarf ein- und / oder ausgehende Frames, die durch die Bridge verarbeitet und weitergeleitet werden, aufgezeichnet werden, wohingegen im Modus „Überwachung“ nur die Frames aufgezeichnet werden, die für die Netzwerk-Überwachung einen Einbruch, also das Vorkommen einer nicht eingelernten Adresse, darstellt.

Als nächstes müssen Sie noch die Schnittstelle und die Paketart auswählen, von welcher Frames aufgezeichnet werden sollen. Mit der Auswahl „A und B“ werden beiden Schnittstellen berücksichtigt. Das

gleiche gilt für die Paketart „alle“, welche ein- und ausgehende Frames beachtet. Mit Hilfe dieser beiden Einstellungen können Sie die Aufzeichnung völlig frei und nach Bedarf konfigurieren. Bei einer Aufzeichnungs-Überwachung gelten alle Frames als eingehend. Hier empfiehlt es sich daher die Schnittstelle „A und B“ zu verwenden, um somit Einbrüche beider Schnittstellen mitzubekommen.

Zuletzt muss noch der Speicherort ausgewählt werden. Mit der Schnittstelle „Speicherung“ können Sie wählen, ob die Anzeige bzw. Speicherung im Webbrowser, auf einem FTP-Server oder auf einem USB-Stick erfolgen soll. Die Speicherung auf den FTP-Server erfordert eine bereits erfolgreich durchgeführte Konfiguration des FTP-Servers *(siehe Kapitel Webserver → Konfiguration → FTP-Einstellungen)*. Möchten Sie auf einen USB-Stick aufzeichnen, muss dieser vor dem Starten der Aufzeichnung eingesteckt werden. Nach der Beendigung der Aufzeichnung, kann der USB-Stick wieder entfernt werden.

Hinweis:
Der USB-Stick muss mit einem FAT-Dateisystem formatiert sein, um diesen verwenden zu können.

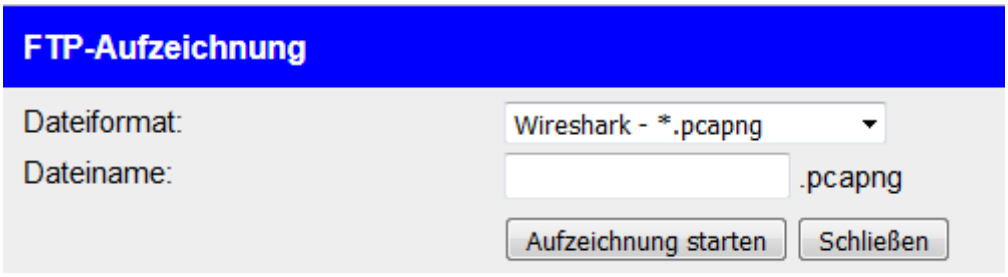
Wichtig:
Stecken Sie den USB-Stick nicht während einer laufenden Aufzeichnung aus. Dies kann sonst zur Beschädigung der Datei und des Dateisystems führen.

Um nun die Aufzeichnung zu starten, müssen Sie lediglich auf das Symbol ▶ klicken.

Über das Symbol ■ können Sie die Aufzeichnung wieder stoppen. Möchten Sie mit der Aufzeichnung von vorne beginnen bzw. die Anzeige zurücksetzen, so können Sie die Aufzeichnung mit Hilfe des Symbols ⟳ neu starten (nur bei Speicherung im Webbrowser verfügbar).

Über das Icon ▤ können Sie das automatische Scrollen an das Tabellenende aktivieren. Dieses Scrollen wird, sofern es aktiviert ist, ausgeführt, wenn ein neues Frame in die Tabelle eingetragen wird. Mit dem Icon ▤ können Sie das Scrollen wieder deaktivieren.

Falls Sie auf einen FTP-Server oder USB-Stick aufzeichnen möchten, so werden Sie beim Starten der Aufzeichnung dazu aufgefordert, ein Dateiformat (aktuell stehen die Wireshark-Dateiformate .pcapng und .pcap zur Verfügung) auszuwählen sowie einen Dateinamen (ohne Dateiendung) anzugeben:

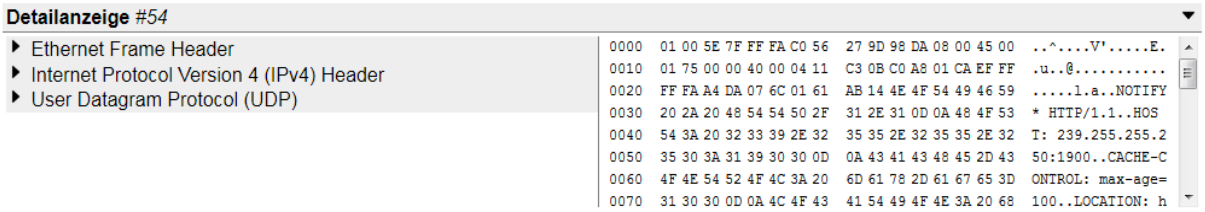


Läuft eine Aufzeichnung auf den FTP-Server oder USB-Stick, so sehen Sie in der Frame-Tabelle keine Frames, da diese direkt an den FTP-Server gesendet bzw. auf den USB-Stick geschrieben werden. Ob die Aufzeichnung auf den FTP-Server oder USB-Stick funktioniert bzw. ggf. welcher Fehler aufgetreten ist, können Sie der Statusanzeige oben rechts (gleiche Höhe wie die Toolbar mit den Icons) entnehmen:

4.3.1 Detailanzeige

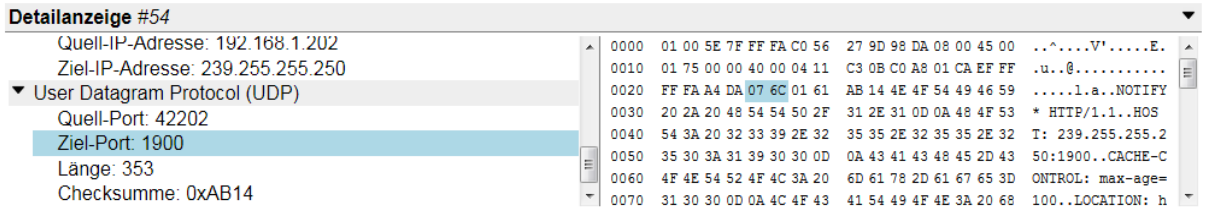
Die Aufzeichnungs-Tabelle zeigt nur die Transferrichtung, eine fortlaufende Nummer, die Zeit, die Quelle und das Ziel des jeweiligen Frames an. Bei ausreichendem Platz werden auch noch das Protokoll, die Länge und eine Beschreibung des Frames angezeigt.

Für eine detaillierte Anzeige bzw. Analyse ist dies jedoch nicht ausreichend. Daher gibt es die Detailanzeige. Um die Detailanzeige eines Frames aufzurufen, müssen Sie lediglich auf ein Frame in der Tabelle klicken. Darauf erscheint folgende Ansicht:



Die linke Seite zeigt die analysierte Daten des Frames in Textform. Auf der rechten Seite sehen Sie die Rohdaten des Frames. Bei geringer Bildschirmbreite werden die analysierten Daten und Rohdaten untereinander angezeigt.

Sowohl die Einträge in der Textansicht als auch die Bytes in der Rohdatenansicht können angeklickt werden. Der gewählte Eintrag sowie dessen Rohdaten bzw. dessen Eintrag in der Textansicht werden daraufhin markiert:



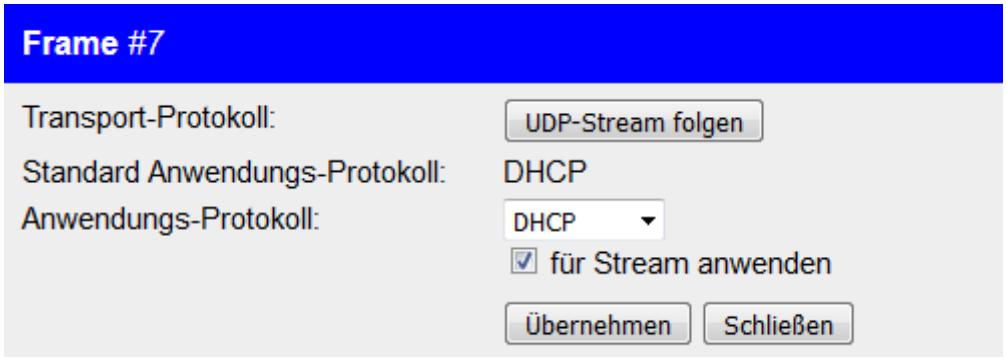
Hinweis:
Einträge in der Textansicht, welche über Unterpunkte verfügen, werden, sobald diese angeklickt werden, automatisch aufgeklappt.

4.3.2 Frameinformationen und -einstellungen

Jedes Frame verfügt noch über Informationen, aber auch Einstellungen, die nicht innerhalb der Tabelle oder in der Detailanzeige angezeigt werden.

Um die Anzeige mit Informationen und Einstellungen eines einzelnen Frames zu öffnen, müssen Sie das Frame zunächst in der Tabelle anklicken. Der Eintrag wird daraufhin hellblau hinterlegt und ggf. öffnet

sich auch die Detailanzeige. Nun müssen Sie auf das ℹ-Icon, welches Sie in der Toolbar, oberhalb der Tabelle mit den Frames finden, klicken. Sie sollten nun folgenden Dialog sehen:



Die einzelnen Zeilen, haben dabei folgende Bedeutung:

Transport-Protokoll:	Handelt es sich bei dem Frame um ein TCP- oder UDP-Frame, so können Sie mit dem entsprechenden Button einen Anzeigefilter setzen, wodurch nur noch Frames angezeigt werden, die dem TCP- oder UDP-Stream des gewählten Frames angehören. Zudem wird bei TCP-Frames noch ein Button angezeigt, um den Analyse-Dialog des TCP-Streams öffnen zu können.
Standard Anwendungs-Protokoll:	Hier wird das Anwendungsprotokoll (falls vorhanden) angezeigt, als welches das Frame standardmäßig analysiert wird.
Anwendungs-Protokoll:	Hier können Sie auswählen, als welches Anwendungsprotokoll das Frame analysiert werden soll. Ist der Hacken im Kontrollkästchen „für Stream anwenden“ gesetzt, so gilt die Einstellung auch für alle anderen Frames, die dem gleichen TCP- oder UDP-Stream angehören.

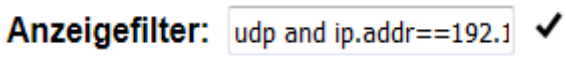
Sollten Sie das Anwendungs-Protokoll des Frames geändert haben, so müssen Sie auf den Button „Übernehmen“ klicken, um das Frame bzw. den Stream neu analysieren zu lassen.

4.3.3 Anzeigefilter

Um die aufgezeichneten Daten im Browser zu filtern, um somit nur Frames mit bestimmten IP-Adressen, Ports oder Protokollen anzuzeigen, haben Sie die Möglichkeit einen Anzeigefilter einzugeben. Der Anzeigefilter ist eine Zeichenkette, die aus einer oder mehreren Bedingungen besteht.

Wichtig:
Der Anzeigefilter beeinflusst nur die Anzeige im Webbrowser. Das Gerät zeichnet immer alle Daten auf.

Um den Anzeigefilter zu übernehmen, betätigen Sie, sofern sich der Fokus auf dem Textfeld befindet, einfach die Eingabetaste oder klicken Sie auf Symbol ✓ hinter dem Textfeld.



Hinweis:
Die Eingaben und Befehle für den Anzeigefilter sind weitestgehend mit denen von dem Programm Wireshark kompatibel.

Für die Felder (siehe Tabelle auf der nächsten Seite) sind zwischen folgenden Datentypen zu unterscheiden:

Name	Beschreibung
-	Felder ohne Datentyp können nur auf Existenz geprüft werden
Wahrheitswert	y für wahr; n für unwahr
Nummer	Zahlenwerte (hexadezimal mit 0x, oktal mit 0, binär mit 0b oder dezimal)

Name	Beschreibung
Zeichenkette	eine Zeichenkette; auch DNS-Name oder NBNS-Name
MAC-Adresse	eine MAC-Adresse; Adressblocks am Ende können beliebig weggelassen werden
IPv4-Adresse	eine IPv4-Adresse; Adressblocks am Ende können beliebig weggelassen werden
IPv6-Adresse	eine IPv6-Adresse; Verkürzung mit :: erlaubt; Adressblocks am Ende können beliebig weggelassen werden

Folgende Felder können beim Anzeigefilter geprüft werden:

Name	Datentyp	Beschreibung
eth	-	Ethernet-Header
eth.dst	MAC-Adresse	Ziel-MAC-Adresse
eth.src	MAC-Adresse	Quelle-MAC-Adresse
eth.vlan.tpid	Nummer	VLAN Protokoll-ID
eth.vlan.prio	Nummer	VLAN Priorität
eth.vlan.cfi	Wahrheitswert	VLAN DEI-/CFI-Bit
eth.vlan.id	Nummer	VLAN ID
eth.type	Nummer	Ethernet-Type
eth.len	Nummer	Frame-Länge
llc	-	LLC-Header
llc.dsap	Nummer	Ziel SAP
llc.ssap	Nummer	Quell SAP
llc.control	Nummer	Steuerwert
llc.snap	-	SNAP-Erweiterungs-Header
llc.snap.oui	Nummer	Herstellerkennung

Name	Datentyp	Beschreibung
llc.snap.vlan.tpid	Nummer	VLAN Protokoll-ID
llc.snap.vlan.prio	Nummer	VLAN Priorität
llc.snap.vlan.cfi	Wahrheitswert	VLAN DEI-/CFI-Bit
llc.snap.vlan.id	Nummer	VLAN ID
llc.snap.proto	Nummer	Protokoll (Ethernet-Type)
ip	-	IPv4-Header
ip.version	Nummer	Version
ip.hdr_len	Nummer	Header-Länge
ip.tos	Nummer	Type Of Service (QoS-Parameter)
ip.len	Nummer	Gesamtlänge
ip.id	Nummer	Identifikations-Nummer
ip.flags	Nummer	Flags
ip.frag_offset	Nummer	Fragmentierungs-Offset
ip.ttl	Nummer	Time To Live (Lebenszeit)
ip.proto	Nummer	IP-Protokoll
ip.checksum	Nummer	Header-Checksumme
ip.src	IPv4-Adresse	Quell-IPv4-Adresse
ip.dst	IPv4-Adresse	Ziel-IPv4-Adresse
ip.opt	-	IPv4-Option
ip.opt.type	Nummer	Optionstyp
ip.opt.len	Nummer	Optionslänge
ip.opt.data	-	Optionsdaten
ipv6	-	IPv6-Header
ipv6.version	Nummer	Version
ipv6.class	Nummer	Klassifizierung (QoS-Parameter)

Name	Datentyp	Beschreibung
ipv6.flow	Nummer	Flussbezeichnung
ipv6.plen	Nummer	Nutzdaten-Länge
ipv6.nxt	Nummer	IP-Protokoll bzw. nächster Header
ipv6.hlim	Nummer	Maximale Anzahl an Hops
ipv6.src	IPv6-Adresse	Quell-IPv6-Adresse
ipv6.dst	IPv6-Adresse	Ziel-IPv6-Adresse
arp	-	ARP-Protokoll
arp.hw.type	Nummer	Typ der Hardware-Adressen
arp.proto.type	Nummer	Typ der Protokoll Adressen
arp.hw.size	Nummer	Größe der Hardware-Adressen
arp.proto.size	Nummer	Größe der Protokoll-Adressen
arp.opcode	Nummer	Operations-Code
arp.src.hw	MAC-Adresse	Quell-Hardware-Adresse
arp.src.proto	IPv4-Adresse	Quell-Protokoll-Adresse
arp.dst.hw	MAC-Adresse	Ziel-Hardware-Adresse
arp.dst.proto	IPv4-Adresse	Ziel-Protokoll-Adresse
rarp	-	RARP-Protokoll
rarp.hw.type	Nummer	Typ der Hardware-Adressen
rarp.proto.type	Nummer	Typ der Protokoll Adressen
rarp.hw.size	Nummer	Größe der Hardware-Adressen
rarp.proto.size	Nummer	Größe der Protokoll-Adressen
rarp.opcode	Nummer	Operations-Code
rarp.src.hw	MAC-Adresse	Quell-Hardware-Adresse
rarp.src.proto	IPv4-Adresse	Quell-Protokoll-Adresse
rarp.dst.hw	MAC-Adresse	Ziel-Hardware-Adresse

Name	Datentyp	Beschreibung
rarp.dst.proto	IPv4-Adresse	Ziel-Protokoll-Adresse
lldp	-	LLDP-Protokoll
lldp.tlv	-	Typ-Länge-Wert (TLV)
lldp.tlv.type	Nummer	TLV-Typ
lldp.tlv.len	Nummer	TLV-Länge
lldp.tlv.data	-	TLV-Wert
mrp	-	MRP-Protokoll
mrp.version	Nummer	Version
mrp.block	-	Block
mrp.type	Nummer	Blocktyp
mrp.length	Nummer	Blocklänge
mrp.sequence_id	Nummer	Sequenz-Nummer
mrp.domain_uuid	Nummer	Domain-UUID
mrp.prio	Nummer	Priorität
mrp.sa	MAC-Adresse	Sender-MAC-Adresse
mrp.port_role	Nummer	Port-Status
mrp.ring_state	Nummer	Ring-Status
mrp.transition	Nummer	Übergang
mrp.timestamp	Nummer	Zeitstempel
mrp.interval	Nummer	Intervall
mrp.blocked	Nummer	Blockierung
mrp.oui	Nummer	OID
mrp.data	-	Nutzdaten
mrp.padding	-	Padding
hopopts	-	Hop-By-Hop-Header (IPv6)

Name	Datentyp	Beschreibung
hopopts.nxt	Nummer	IP-Protokoll bzw. nächster Header
hopopts.len	Nummer	Header-Länge
hopopts.opts	-	Optionen
routing	-	Routing-Header (IPv6)
routing.nxt	Nummer	IP-Protokoll bzw. nächster Header
routing.len	Nummer	Header-Länge
routing.type	Nummer	Routing-Typ
routing.segleft	Nummer	Anzahl der übrigen Segmente
routing.data	-	Typabhängige Daten
fragment	-	Fragmentierungs-Header (IPv6)
fragment.nxt	Nummer	IP-Protokoll bzw. nächster Header
fragment.reserved	-	-
fragment.offset	Nummer	Fragmentierungs-Offset
fragment.filler	-	-
fragment.more	Wahrheitswert	Gibt an, ob weitere Fragmente folgen
fragment.id	Nummer	Identifikation
dstopts	-	Ziel-Options-Header (IPv6)
dstopts.nxt	Nummer	IP-Protokoll bzw. nächster Header
dstopts.len	Nummer	Header-Länge
dstopts.opts	-	Optionen
icmp	-	ICMPv4-Protokoll
icmp.type	Nummer	Typen-Kennung
icmp.code	Nummer	Code (je nach Typ)
icmp.checksum	Nummer	Checksumme

Name	Datentyp	Beschreibung
icmp.data	-	Nutzdaten
icmpv6	-	ICMPv6-Protokoll
icmpv6.type	Nummer	Typen-Kennung
icmpv6.code	Nummer	Code (je nach Typ)
icmpv6.checksum	Nummer	Checksumme
icmpv6.data	-	Nutzdaten
igmp	-	IGMP-Protokoll
igmp.type	Nummer	Typen-Kennung
igmp.code	Nummer	Code (je nach Typ)
igmp.max_resp	Nummer	maximale Antwortzeit
igmp.reserved	-	-
igmp.resp_code	Nummer	Antwortcode
igmp.checksum	Nummer	Checksumme
igmp.id	Nummer	Identifikation
igmp.maddr	IPv4-Adresse	Gruppen-Adresse
igmp.key	Nummer	Schlüssel
igmp.filler	-	-
igmp.s	Wahrheitswert	Unterdrückungs-Flag (Router)
igmp.qrv	Nummer	QRV-Wert
igmp.qqic	Nummer	QQIC-Wert
igmp.num_src	Nummer	Anzahl an Quellen
igmp.src	IPv4-Adresse	Quell-Adresse
tcp	-	TCP-Header
tcp.srcport	Nummer	Quell-Port
tcp.dstport	Nummer	Ziel-Port

Name	Datentyp	Beschreibung
tcp.seq	Nummer	Sequenz-Nummr
tcp.ack	Nummer	Acknowledge-Nummer
tcp.hdr_len	Nummer	Header-Länge
tcp.reserved	-	-
tcp.flags	Nummer	Flags
tcp.window_size	Nummer	Fenster-Größe
tcp.checksum	Nummer	Checksumme
tcp.urgent_pointer	Nummer	Urgent-Pointer
tcp.opt	-	TCP-Option
tcp.opt.type	Nummer	Optionstyp
tcp.opt.len	Nummer	Optionslänge
tcp.opt.data	-	Optionsdaten
udp	-	UDP-Header
udp.srcport	Nummer	Quell-Port
udp.dstport	Nummer	Ziel-Port
udp.len	Nummer	Gesamtlänge
udp.checksum	Nummer	Checksumme
dhcp	-	DHCP-Protokoll
dhcp.type	Nummer	Typ des Protokolls
dhcp.hw.type	Nummer	Typ der physikalischen Adresse
dhcp.hw.len	Nummer	Länge der physikalischen Adresse
dhcp.hops	Nummer	Anzahl der Relay-Agents
dhcp.id	Nummer	Identifikation
dhcp.seconds	Nummer	Sekunden seit dem Start des Clients
dhcp.flags	Nummer	Flags

Name	Datentyp	Beschreibung
dhcp.ip.client	IPv4-Adresse	Client-IP-Adresse
dhcp.ip.your	IPv4-Adresse	eigene IP-Adresse
dhcp.ip.server	IPv4-Adresse	Server-IP-Adresse
dhcp.ip.relay	IPv4-Adresse	Relay-Agent-IP-Adresse
dhcp.hw.addr	MAC-Adresse	Client-MAC-Adresse
dhcp.hw.addr_pad	.	Padding nach der MAC-Adresse
dhcp.hostname	Zeichenkette	Name des Servers
dhcp.file	Zeichenkette	Dateiname der Boot-Datei
dhcp.magic	Nummer	Magische Zahl
dhcp.opt	-	DHCP-Option
dhcp.opt.type	Nummer	Optionstyp
dhcp.opt.len	Nummer	Optionslänge
dhcp.opt.data	-	Optionsdaten
dns	-	DNS-Protokoll
dns.id	Nummer	Identifikation
dns.type	Nummer	Typenkennung
dns.opcode	Nummer	Operationscode
dns.flags	Nummer	Flags
dns.rcode	Nummer	Antwortcode
dns.count.queries	Nummer	Anzahl der Anfragen
dns.count.answers	Nummer	Anzahl der Antworten
dns.count.auth_rr	Nummer	Anzahl der Namensserver-Einträge
dns.count.add_rr	Nummer	Anzahl der zusätzlichen Einträge
dns.qry	-	Anfrage
dns.qry.name	Zeichenkette	DNS-Name
dns.qry.type	Nummer	Typenkennung

Name	Datentyp	Beschreibung
dns.qry.class	Nummer	Klasse
dns.ans	-	Antwort
dns.ans.name	Zeichenkette	DNS-Name
dns.ans.type	Nummer	Typenkennung
dns.ans.class	Nummer	Klasse
dns.ans.ttl	Nummer	Lebenszeit (TTL)
dns.ans.dlen	Nummer	Datenlänge
dns.ans.data	-	Daten
dns.ans.ip	IPv4-Adresse	IPv4-Adresse
dns.ans.ipv6	IPv6-Adresse	IPv6-Adresse
dns.ans.hostname	Zeichenkette	Hostname
dns.auth	-	Namensserver-Eintrag
dns.auth.name	Zeichenkette	DNS-Name
dns.auth.type	Nummer	Typenkennung
dns.auth.class	Nummer	Klasse
dns.auth.ttl	Nummer	Lebenszeit (TTL)
dns.auth.dlen	Nummer	Datenlänge
dns.auth.data	-	Daten
dns.auth.ip	IPv4-Adresse	IPv4-Adresse
dns.auth.ipv6	IPv6-Adresse	IPv6-Adresse
dns.auth.hostname	Zeichenkette	Hostname
dns.add	-	Zusätzlicher Eintrag
dns.add.name	Zeichenkette	DNS-Name
dns.add.type	Nummer	Typenkennung
dns.add.class	Nummer	Klasse
dns.add.ttl	Nummer	Lebenszeit (TTL)

Name	Datentyp	Beschreibung
dns.add.dlen	Nummer	Datenlänge
dns.add.data	-	Daten
dns.add.ip	IPv4-Adresse	IPv4-Adresse
dns.add.ipv6	IPv6-Adresse	IPv6-Adresse
dns.add.hostname	Zeichenkette	Hostname
nbns	-	NBNS-Protokoll
nbns.id	Nummer	Identifikation
nbns.type	Nummer	Typenkennung
nbns.opcode	Nummer	Operationscode
nbns.flags	Nummer	Flags
nbns.rcode	Nummer	Antwortcode
nbns.count.queries	Nummer	Anzahl der Anfragen
nbns.count. answers	Nummer	Anzahl der Antworten
nbns.count.auth_rr	Nummer	Anzahl der Namensserver-Einträge
nbns.count.add_rr	Nummer	Anzahl der zusätzlichen Einträge
nbns.qry	-	Anfrage
nbns.qry.name	Zeichenkette	NBNS-Name
nbns.qry.type	Nummer	Typenkennung
nbns.qry.class	Nummer	Klasse
nbns.ans	-	Antwort
nbns.ans.name	Zeichenkette	NBNS-Name
nbns.ans.type	Nummer	Typenkennung
nbns.ans.class	Nummer	Klasse
nbns.ans.ttl	Nummer	Lebenszeit (TTL)
nbns.ans.dlen	Nummer	Datenlänge

Name	Datentyp	Beschreibung
nbns.ans.data	-	Daten
nbns.ans.flags	Nummer	Flags
nbns.ans.ip	IPv4-Adresse	IPv4-Adresse
nbns.auth	-	Namenserver-Eintrag
nbns.auth.name	Zeichenkette	NBNS-Name
nbns.auth.type	Nummer	Typenkennung
nbns.auth.class	Nummer	Klasse
nbns.auth.ttl	Nummer	Lebenszeit (TTL)
nbns.auth.dlen	Nummer	Datenlänge
nbns.auth.data	-	Daten
nbns.auth.flags	Nummer	Flags
nbns.auth.ip	IPv4-Adresse	IPv4-Adresse
nbns.add	-	Zusätzlicher Eintrag
nbns.add.name	Zeichenkette	NBNS-Name
nbns.add.type	Nummer	Typenkennung
nbns.add.class	Nummer	Klasse
nbns.add.ttl	Nummer	Lebenszeit (TTL)
nbns.add.dlen	Nummer	Datenlänge
nbns.add.data	-	Daten
nbns.add.flags	Nummer	Flags
nbns.add.ip	IPv4-Adresse	IPv4-Adresse
ntp	-	NTP-Protokoll
ntp.li	Nummer	Sprung-Warnung
ntp.vn	Nummer	Version
ntp.mode	Nummer	Modus
ntp.stratum	Nummer	Schicht

Name	Datentyp	Beschreibung
ntp.poll	Nummer	Polling-Interval
ntp.precision	Nummer	Genaugikeit
ntp.delay	Nummer	Verzögerung
ntp.dispersion	Nummer	Abweichung
ntp.refid	Nummer	Referenz-ID
ntp.reftime	Nummer	Referenz-Zeitstempel
ntp.org	Nummer	ursprünglicher Zeitstempel
ntp.rec	Nummer	Empfangs-Zeitstempel
ntp.xmt	Nummer	Übertragungs-Zeitstempel
tftp	-	TFTP-Protokoll
tftp.opcode	Nummer	Operationscode
tftp.file	Zeichenkette	Dateiname
tftp.mode	Zeichenkette	Modus
tftp.datablock	Nummer	Block-Nummer (bei Daten)
tftp.data	-	Daten
tftp.ackblock	Nummer	Block-Nummer (bei Bestätigung)
tftp.error.code	Nummer	Fehlercode
tftp.error.msg	Zeichenkette	Fehlermeldung
snmp	-	SNMP-Protokoll
snmp.tlv	-	Typ-Länge-Wert (TLV)
snmp.tlv.type	Nummer	TLV-Typ
snmp.tlv.length	Nummer	TLV-Länge
snmp.tlv.data	-	TLV-Wert
snmp.value.int	Nummer	TLV-Wert als Nummer
snmp.value.string	Zeichenkette	TlLV-Wert als Zeichenkette

Name	Datentyp	Beschreibung
snmp.value.counter	Nummer	TLV-Wert als Zähler
snmp.value.tticks	Nummer	TLV-Wert als Zeitstempel
ftp	-	FTP-Protokoll
ftp.line	Zeichenkette	Zeile
ftp.req.command	Zeichenkette	Anfrage-Kommando
ftp.req.parameter	Zeichenkette	Anfrage-Parameter
ftp.rsp.code	Zeichenkette	Antwort-Code
ftp.rsp.arg	Zeichenkette	Antwort-Argumente
http	-	HTTP-Protokoll
http.req	Zeichenkette	Anfrage
http.req.method	Zeichenkette	Methode
http.req.uri	Zeichenkette	Pfad
http.req.version	Zeichenkette	Version
http.resp	Zeichenkette	Antwort
http.resp.version	Zeichenkette	Version
http.resp.code	Zeichenkette	Antwort-Code
http.resp.desc	Zeichenkette	Antwort-Text
http.field	Zeichenkette	HTTP-Eigenschaft
http.field.name	Zeichenkette	Feldname
http.field.value	Zeichenkette	Feldwert
smtp	-	SMTP-Protokoll
smtp.line	Zeichenkette	Zeile
smtp.req.command	Zeichenkette	Anfrage-Kommando
smtp.req.parameter	Zeichenkette	Anfrage-Parameter

Name	Datentyp	Beschreibung
smtp.rsp.code	Zeichenkette	Antwort-Code
smtp.rsp.parameter	Zeichenkette	Antwort-Parameter
pop	-	POP-Protokoll
pop.line	Zeichenkette	Zeile
pop.req.command	Zeichenkette	Anfrage-Kommando
pop.req.parameter	Zeichenkette	Anfrage-Parameter
pop.rsp.indicator	Zeichenkette	Antwort-Indikator
pop.rsp.desc	Zeichenkette	Antwort-Beschreibung
imap	-	IMAP-Protokoll
imap.line	Zeichenkette	Zeile
imap.tag	Zeichenkette	Tag
imap.data	Zeichenkette	Daten
sip	-	SIP-Protokoll
sip.req	Zeichenkette	Anfrage
sip.req.method	Zeichenkette	Methode
sip.req.uri	Zeichenkette	URI
sip.req.version	Zeichenkette	Version
sip.resp	Zeichenkette	Antwort
sip.resp.version	Zeichenkette	Version
sip.resp.code	Zeichenkette	Antwort-Code
sip.resp.desc	Zeichenkette	Antwort-Text
sip.field	Zeichenkette	SIP-Eigenschaft
sip.field.name	Zeichenkette	Feldname
sip.field.value	Zeichenkette	Feldwert
sdp	-	SDP-Protokoll

Name	Datentyp	Beschreibung
sdp.version	Zeichenkette	Version
sdp.owner	Zeichenkette	Session-Besitzer
sdp.owner. username	Zeichenkette	Benutzername
sdp.owner.id	Zeichenkette	Session-ID
sdp.owner.version	Zeichenkette	Version
sdp.owner.ntype	Zeichenkette	Netzwerktyp
sdp.owner.atype	Zeichenkette	Adresstyp
sdp.owner.address	Zeichenkette	Adresse
sdp.session_name	Zeichenkette	Session-Name
sdp.session_info	Zeichenkette	Session-Info
sdp.uri	Zeichenkette	URI
sdp.email	Zeichenkette	E-Mail-Adresse
sdp.phone	Zeichenkette	Telefonnummer
sdp.s_con_info	Zeichenkette	Verbindungsdaten der Session
sdp.s_con_info. ntype	Zeichenkette	Netzwerktyp
sdp.s_con_info. atype	Zeichenkette	Adresstyp
sdp.s_con_info. address	Zeichenkette	Adresse
sdp.s_bandwidth	Zeichenkette	Bandbreite der Session
sdp.time	Zeichenkette	Zeit
sdp.time.start	Zeichenkette	Startzeit
sdp.time.stop	Zeichenkette	Endzeit
sdp.repeat_time	Zeichenkette	Wiederholungszeit
sdp.timezone	Zeichenkette	Zeitzone

Name	Datentyp	Beschreibung
sdp.s_enc_key	Zeichenkette	Verschlüsselungs-Schlüssel der Session
sdp.session_attr	Zeichenkette	Session-Attribut
sdp.media	Zeichenkette	Medien-Beschreibung
sdp.media.media	Zeichenkette	Medientyp
sdp.media.port	Zeichenkette	Port
sdp.media.proto	Zeichenkette	Protokoll
sdp.media.format	Zeichenkette	Format
sdp.media.title	Zeichenkette	Medien-Titel
sdp.m_con_info	Zeichenkette	Verbindungsdaten des Mediums
sdp.m_con_info.ntype	Zeichenkette	Netzwerktyp
sdp.m_con_info.atype	Zeichenkette	Adresstyp
sdp.m_con_info.address	Zeichenkette	Adresse
sdp.m_bandwidth	Zeichenkette	Bandbreite des Mediums
sdp.m_enc_key	Zeichenkette	Verschlüsselungs-Schlüssel des Mediums
sdp.media_attr	Zeichenkette	Medien-Attribut
rtp	-	RTP-Protokoll
rtp.version	Nummer	Version
rtp.p	Wahrheitswert	Gibt an, ob Padding vorhanden ist
rtp.x	Wahrheitswert	Gibt an, ob ein Erweiterungs-Header vorhanden ist
rtp.cc	Nummer	CSRC-Anzahl
rtp.marker	Wahrheitswert	Marker-Flag
rtp.p_type	Nummer	Typ der Nutzdaten

Name	Datentyp	Beschreibung
rtp.seq	Nummer	Sequenz-Nummer
rtp.timestamp	Nummer	Zeitstempel
rtp.ssrc	Nummer	SSRC
rtp.csrc	Nummer	CSRC
rtp.ext	-	RTP-Erweiterungs-Header
rtp.ext.profile	Nummer	Profil-/Typwert
rtp.ext.len	Nummer	Länge
rtp.ext.data	-	Daten
rtp.payload	-	Nutzdaten
rtp.padding	-	Padding
rtcp	-	RTCP-Protokoll
rtcp.version	Nummer	Version
rtcp.p	Wahrheitswert	Gibt an, ob Padding vorhanden ist
rtcp.rc	Nummer	Report-Anzahl
rtcp.sc	Nummer	CSRC-Anzahl
rtcp.subtype	Nummer	Subtyp
rtcp.pt	Nummer	Pakettyp
rtcp.length	Nummer	Länge
rtcp.data	-	Daten
rtcp.padding	-	Padding
tpkt	-	TPKT-Protokoll
tpkt.version	Nummer	Version
tpkt.reserved	-	-
tpkt.length	Nummer	Länge
q931	-	Q.931-Protokoll

Name	Datentyp	Beschreibung
q931.disc	Nummer	Protokoll-Diskriminator
q931.call_ref_len	Nummer	Länge der Verbindungskennung
q931.call_ref	Nummer	Verbindungskennung
q931. message_type	Nummer	Nachrichtentyp
q931.ie	-	Informationselement
q931.ie.id	Nummer	Identifikation
q931.ie.len	Nummer	Länge
q931.ie.data	-	Daten
pn_rt	-	PROFINET-Realtime-Protokoll
pn_rt.frame_id	Nummer	Frame-ID
pn_rt.cycle_ counter	Nummer	Zykluszähler
pn_rt.ds	Nummer	Datenstatus
pn_rt.transfer_ status	Nummer	Übertragungsstatus
pn_dcp	-	PROFINET-DCP-Protokoll
pn_dcp.service_id	Nummer	Service-ID
pn_dcp.service_ type	Nummer	Service-Typ
pn_dcp.xid	Nummer	Identifikation
pn_dcp.response_ delay	Nummer	Antwort-Verzögerung
pn_dcp.data_ length	Nummer	Datenlänge
pn_dcp.block	-	Block
pn_dcp.block.opt	Nummer	Block-Option

Name	Datentyp	Beschreibung
pn_dcp.block. subopt	Nummer	Block-Suboption
pn_dcp.block. length	Nummer	Blocklänge
pn_dcp.block. status	Nummer	Status
pn_dcp.block.data	-	Blockdaten
pn_dcp.padding	-	Padding
pn_ptcp	-	PROFINET-PTCP-Protokoll
pn_ptcp.header	-	Header
pn_ptcp.pad1	-	Padding
pn_ptcp.res1	-	Reserviert
pn_ptcp.res2	-	Reserviert
pn_ptcp.delay10ns	Nummer	10ns Verzögerung
pn_ptcp.sequence _id	Nummer	Sequenz-Nummer
pn_ptcp.delay1ns_ byte	Nummer	1ns Verzögerung (Byte)
pn_ptcp.pad2	-	Padding
pn_ptcp.delay1ns	Nummer	1ns Verzögerung
pn_ptcp.tlvheader	-	Block
pn_ptcp.tl_type	Nummer	Blocktyp
pn_ptcp.tl_length	Nummer	Blocklänge
pn_ptcp.tl_data	-	Blockdaten
pn_mrrt	-	PROFINET-MRRT-Protokoll
pn_mrrt.version	Nummer	Version
pn_mrrt.block	-	Block

Name	Datentyp	Beschreibung
pn_mrrt.type	Nummer	Blocktyp
pn_mrrt.length	Nummer	Blocklänge
pn_mrrt.sequence_id	Nummer	Sequenz-Nummer
pn_mrrt.domain_uuid	Nummer	Domain-UUID
pn_mrrt.sa	MAC-Adresse	Sender-MAC-Adresse
pn_mrrt.data	-	Daten
pn_mrrt.padding	-	Padding
dcerpc	-	DCE/RPC-Protokoll
dcerpc.ver	Nummer	Version
dcerpc.ver_minor	Nummer	Unterversion
dcerpc.pkt_type	Nummer	Pakettyp
dcerpc.cn_flags	Nummer	Flags (nur CN)
dcerpc.dg_flags1	Nummer	Flags Teil 1 (nur DG)
dcerpc.dg_flags2	Nummer	Flags Teil 2 (nur DG)
dcerpc.drep	-	Datendarstellung
dcerpc.drep.byteorder	Nummer	Bytereihenfolge
dcerpc.drep.character	Nummer	Zeichensatz
dcerpc.drep.fp	Nummer	Gleitkommaformat
dcerpc.dg_serial_hi	Nummer	Seriennummer (höherwertig)
dcerpc.dg_obj_id	-	Objekt-ID (nur DG)
dcerpc.dg_if_id	-	Schnitstellen-ID
dcerpc.dg_act_id	-	Aktivitäts-ID

Name	Datentyp	Beschreibung
dcerpc.dg_server_boot	Nummer	Server-Boot-Zeitstempel
dcerpc.dg_if_ver	Nummer	Schnittstellen-Version
dcerpc.dg_seqnum	Nummer	Sequenz-Nummer
dcerpc.dg_opnum	Nummer	Operationsnummer (nur DG)
dcerpc.dg_if_hint	Nummer	Schnittstellenhinweis
dcerpc.dg_act_hint	Nummer	Aktivitätshinweis
dcerpc.frag_len	Nummer	Fragmentierungslänge
dcerpc.dg_frag_num	Nummer	Fragmentierungsnummer
dcerpc.dg_auth_proto	Nummer	Authentifizierungs-Protokoll
dcerpc.cn_auth_len	Nummer	Authentifizierungs-Länge
dcerpc.dg_serial_lo	Nummer	Seriennummer (niederwertig)
dcerpc.cn_call_id	Nummer	Kommunikations-ID
dcerpc.cn_alloc_hint	Nummer	Allokierungshinweis
dcerpc.cn_ctx_id	Nummer	Kontext-ID
dcerpc.cn_cancel_cnt	Nummer	Abbruchanzahl
dcerpc.cn_status	Nummer	Status (nur CN)
dcerpc.cn_opnum	Nummer	Operationsnummer (nur CN)
dcerpc.cn_obj_id	-	Objekt-ID (nur CN)
dcerpc.cn_reject_res	Nummer	Ablehnungsgrund
dcerpc.cn_max_xmit	Nummer	maximale Übertragung

Name	Datentyp	Beschreibung
dcerpc.cn_max_recv	Nummer	maximaler Empfang
dcerpc.cn_assoc_group	Nummer	Gruppe
dcerpc.dg_status	Nummer	Status (nur DG)
dcerpc.dg_cancel_vers	Nummer	Abbruchsversion
dcerpc.dg_cancel_id	Nummer	Abbruch-ID
dcerpc.dg_cancel_acc	Wahrheitswert	Abbruch-Unterstützung
dcerpc.fack_vers	Nummer	Version
dcerpc.fack_win	Nummer	Fenstergröße
dcerpc.fack_tsdu	Nummer	maximale TSDU
dcerpc.fack_frag	Nummer	maximale Fragmentgröße
dcerpc.fack_serial	Nummer	Seriennummer
dcerpc.fack_selack_len	Nummer	Selektive Bestätigungslänge
dcerpc.fack_selack	-	Selektive Bestätigungen
pn_io	-	PROFINET-IO-Protokoll
pn_io.alarm_dst_ep	Nummer	Ziel-Endpunkt
pn_io.alarm_src_ep	Nummer	Quell-Endpunkt
pn_io.pdu_version	Nummer	PDU-Version
pn_io.pdu_type	Nummer	PDU-Typ
pn_io.tack	Nummer	TACK
pn_io.window_size	Nummer	Fenstergröße

Name	Datentyp	Beschreibung
pn_io.send_seq_num	Nummer	Sende Sequenz-Nummer
pn_io.ack_seq_num	Nummer	Bestätigungs Sequenz-Nummer
pn_io.args_max	Nummer	maximale Argumente
pn_io.args_len	Nummer	Argumentenlänge
pn_io.var_part_len	Nummer	Datenlänge
pn_io.var_part	-	Daten
pn_io.user_data	-	Benutzerdaten
pn_io.status	-	Status
pn_io.status.code	Nummer	Fehlercode
pn_io.status.decode	Nummer	Fehlerdekodierung
pn_io.status.code1	Nummer	Fehlercode 1
pn_io.status.code2	Nummer	Fehlercode 2
pn_io.array	-	Array
pn_io.array.max_count	Nummer	maximale Anzahl
pn_io.array.offset	Nummer	Offset
pn_io.array.act_count	Nummer	aktuelle Anzahl
pn_io.block	-	Block
pn_io.block.type	Nummer	Blocktyp
pn_io.block.length	Nummer	Blocklänge
pn_io.block.version_h	Nummer	Version
pn_io.block.version_l	Nummer	Unterversion

Name	Datentyp	Beschreibung
pn_io.block.data	-	Daten
wol	-	Wake-On-LAN-Protokoll
wol.sync	MAC-Adresse	Synchronisations-Stream
wol.mac_block	-	MAC-Adressen-Block
wol.mac	MAC-Adresse	MAC-Adresse
wol.passwd_ip	IP-Adresse	Passwort als IP-Adresse
wol.passwd_mac	MAC-Adresse	Passwort als MAC-Adresse
llmnr	-	LLMNR-Protokoll
llmnr.id	Nummer	Identifikation
llmnr.type	Nummer	Typenkennung
llmnr.opcode	Nummer	Operationscode
llmnr.flags	Nummer	Flags
llmnr.rcode	Nummer	Antwortcode
llmnr.count.queries	Nummer	Anzahl der Anfragen
llmnr.count. answers	Nummer	Anzahl der Antworten
llmnr.count.auth_rr	Nummer	Anzahl der Namensserver-Einträge
llmnr.count.add_rr	Nummer	Anzahl der zusätzlichen Einträge
llmnr.qry	-	Anfrage
llmnr.qry.name	Zeichenkette	LLMNR-Name
llmnr.qry.type	Nummer	Typenkennung
llmnr.qry.class	Nummer	Klasse
llmnr.ans	-	Antwort
llmnr.ans.name	Zeichenkette	LLMNR-Name
llmnr.ans.type	Nummer	Typenkennung
llmnr.ans.class	Nummer	Klasse

Name	Datentyp	Beschreibung
llmnr.ans.ttl	Nummer	Lebenszeit (TTL)
llmnr.ans.dlen	Nummer	Datenlänge
llmnr.ans.data	-	Daten
llmnr.ans.ip	IPv4-Adresse	IPv4-Adresse
llmnr.ans.ipv6	IPv6-Adresse	IPv4-Adresse
llmnr.ans. hostname	Zeichenkette	Hostname
llmnr.auth	-	Namenserver-Eintrag
llmnr.auth.name	Zeichenkette	LLMNR-Name
llmnr.auth.type	Nummer	Typenkennung
llmnr.auth.class	Nummer	Klasse
llmnr.auth.ttl	Nummer	Lebenszeit (TTL)
llmnr.auth.dlen	Nummer	Datenlänge
llmnr.auth.data	-	Daten
llmnr.auth.ip	IPv4-Adresse	IPv4-Adresse
llmnr.auth.ipv6	IPv6-Adresse	IPv6-Adresse
llmnr.auth. hostname	Zeichenkette	Hostname
llmnr.add	-	Zusätzlicher Eintrag
llmnr.add.name	Zeichenkette	LLMNR-Name
llmnr.add.type	Nummer	Typenkennung
llmnr.add.class	Nummer	Klasse
llmnr.add.ttl	Nummer	Lebenszeit (TTL)
llmnr.add.dlen	Nummer	Datenlänge
llmnr.add.data	-	Daten
llmnr.add.ip	IPv4-Adresse	IPv4-Adresse
llmnr.add.ipv6	IPv6-Adresse	IPv6-Adresse

Name	Datentyp	Beschreibung
llmnr.add. hostname	Zeichenkette	Hostname
ssdp	-	SSDP-Protokoll
ssdp.req	Zeichenkette	Anfrage
ssdp.req.method	Zeichenkette	Methode
ssdp.req.uri	Zeichenkette	Pfad
ssdp.req.version	Zeichenkette	Version
ssdp.resp	Zeichenkette	Antwort
ssdp.resp.version	Zeichenkette	Version
ssdp.resp.code	Zeichenkette	Antwort-Code
ssdp.resp.desc	Zeichenkette	Antwort-Text
ssdp.field	Zeichenkette	SSDP-Eigenschaft
ssdp.field.name	Zeichenkette	Feldname
ssdp.field.value	Zeichenkette	Feldwert
cotp	-	COTP-Protokoll
cotp.li	Nummer	Länge
cotp.type	Nummer	Typ
cotp.destref	Nummer	Ziel-Referenz
cotp.srcref	Nummer	Quell-Referenz
cotp.class	Nummer	Klassifizierung
cotp.opts	Nummer	Optionen
cotp.reason	Nummer	Verbindungsabbruch-Grund
cotp.eot	Wahrheitswert	Letzte TPDU
cotp.tpdu_number	Nummer	TPDU-Nummer
cotp.sequence_ number	Nummer	Sequenz-Nummer

Name	Datentyp	Beschreibung
cotp.cause	Nummer	Fehler-Ursache
cotp.parameter	-	Parameter
cotp.parameter.code	Nummer	Parameter-Code
cotp.parameter.length	Nummer	Parameter-Länge
cotp.parameter.value	-	Parameter-Wert
cotp.tpdu_size	Nummer	TPDU-Größe
cotp.src_tsap	Nummer	Quell-TSAP
cotp.dst_tsap	Nummer	Ziel-TSAP
cotp.checksum	Nummer	Checksumme

Des Weiteren gibt es Gruppenfelder, die für eines von mehreren der oberen Feldern gelten (logisches ODER):

Name	Felder
eth.addr	eth.dst; eth.src
ip.addr	ip.src; ip.dst
ipv6.addr	ipv6.src; ipv6.dst
arp.hw.addr	arp.src.hw; arp.dst.hw
arp.proto.addr	arp.src.proto; arp.dst.proto
rarp.hw.addr	rarp.src.hw; rarp.dst.hw
rarp.proto.addr	rarp.src.proto; rarp.dst.proto
tcp.port	tcp.srcport; tcp.dstport
udp.port	udp.srcport; udp.dstport

Name	Felder
dns.resp	dns.ans; dns.auth; dns.add
dns.resp.name	dns.ans.name; dns.auth.name; dns.add.name
dns.resp.type	dns.ans.type; dns.auth.type; dns.add.type
dns.resp.class	dns.ans.class; dns.auth.class; dns.add.class
dns.resp.ttl	dns.ans.ttl; dns.auth.ttl; dns.add.ttl
dns.resp.dlen	dns.ans.dlen; dns.auth.dlen; dns.add.dlen
dns.resp.data	dns.ans.data; dns.auth.data; dns.add.data
dns.resp.ip	dns.ans.ip; dns.auth.ip; dns.add.ip
dns.resp.ipv6	dns.ans.ipv6; dns.auth.ipv6; dns.add.ipv6
dns.resp.hostname	dns.ans.hostname; dns.auth.hostnane; dns.add. hostname
nbns.resp	nbns.ans; nbns.auth; nbns.add
nbns.resp.name	nbns.ans.name; nbns.auth.name; nbns.add.name
nbns.resp.type	nbns.ans.type; nbns.auth.type; nbns.add.type
nbns.resp.class	nbns.ans.class; nbns.auth.class; nbns.add.class
nbns.resp.ttl	nbns.ans.ttl; nbns.auth.ttl; nbns.add.ttl
nbns.resp.dlen	nbns.ans.dlen; nbns.auth.dlen; nbns.add.dlen
nbns.resp.data	nbns.ans.data; nbns.auth.data; nbns.add.data
nbns.resp.flags	nbns.ans.flags; nbns.auth.flags; nbns.add.flags
nbns.resp.ip	nbns.ans.ip; nbns.auth.ip; nbns.add.ip
tftp.block	tftp.datablock; tftp.ackblock
http.version	http.req.version; http.resp.version
smtp.parameter	smtp.req.parameter; smtp.rsp.parameter
sip.version	sip.req.version; sip.resp.version

Name	Felder
sdp.con_info	sdp.s_con_info; sdp.m_con_info
sdp.con_info.ntype	sdp.s_con_info.ntype; sdp.m_con_info.ntype
sdp.con_info.atype	sdp.s_con_info.atype; sdp.m_con_info.atype
sdp.con_info.address	sdp.s_con_info.address; sdp.m_con_info.address
sdp.bandwidth	sdp.s_bandwidth; sdp.m_bandwidth
sdp.enc_key	sdp.s_enc_key; sdp.m_enc_key
dcerpc.obj_id	dcerpc.dg_obj_id; dcerpc.cn_obj_id
dcerpc.opnum	dcerpc.dg_opnum; dcerpc.cn_opnum
wol.passwd	wol.passwd_ip; wol.passwd_mac
llmnr.resp	llmnr.ans; llmnr.auth; llmnr.add
llmnr.resp.name	llmnr.ans.name; llmnr.auth.name; llmnr.add.name
llmnr.resp.type	llmnr.ans.type; llmnr.auth.type; llmnr.add.type
llmnr.resp.class	llmnr.ans.class; llmnr.auth.class; llmnr.add.class
llmnr.resp.ttl	llmnr.ans.ttl; llmnr.auth.ttl; llmnr.add.ttl
llmnr.resp.dlen	llmnr.ans.dlen; llmnr.auth.dlen; llmnr.add.dlen
llmnr.resp.data	llmnr.ans.data; llmnr.auth.data; llmnr.add.data
llmnr.resp.ip	llmnr.ans.ip; llmnr.auth.ip; llmnr.add.ip
llmnr.resp.ipv6	llmnr.ans.ipv6; llmnr.auth.ipv6; llmnr.add.ipv6
llmnr.resp.hostname	llmnr.ans.hostname; llmnr.auth.hostname; llmnr.add.hostname
ssdp.version	ssdp.req.version; ssdp.resp.version

Neben den Feldern, welche auf Daten innerhalb des Frames zeigen, gibt es auch ein paar Felder, die auf Informationen über das Frame selbst zugreifen:

Name	**Datentyp**	**Beschreibung**
frame.number	Nummer	Index des Frames
frame.intf	Zeichenkette	Schnittstelle von der das Frame aufgezeichnet wurde
frame.rx	Wahrheitswert	Gibt an, ob das Frame ein eingehendes Frame war
frame.time	Nummer	Zeitstempel des Frames (in s)
tcp.stream	Nummer	Index des TCP-Streams
tcp.analysis. window_update	-	TCP-Frame, welches ein „Window Update“ darstellt
tcp.analysis.zero_ window	-	TCP-Frame, welches ein „Zero Window“ darstellt
tcp.analysis.zero_ window_probe	-	TCP-Frame, welches ein „Zero Window Probe“ darstellt
tcp.analysis.zero_ window_probe_ack	-	TCP-Frame, welches ein „Zero Window Probe ACK“ darstellt
tcp.analysis.keep_ alive	-	TCP-Frame, welches ein „Keep Alive“ darstellt
tcp.analysis.keep_ alive_ack	-	TCP-Frame, welches ein „Keep Alive ACK“ darstellt
tcp.analysis. retransmission	-	TCP-Frame, welches eine „Retran-smission“ darstellt
tcp.analysis.rto_ frame	Nummer	Index des Frames, zu welcher die Retransmission gehört
tcp.analysis. duplicate_ack	-	TCP-Frame, welches ein „Duplicate ACK“ darstellt
tcp.analysis. duplicate_ack_num	Nummer	Fortlaufende Zahl für das Duplicate ACK von diesem Strang

Name	Datentyp	Beschreibung
tcp.analysis. duplicate_ack_ frame	Nummer	Index des Frames, zu welchem das Duplicate ACK gehört
udp.stream	Nummer	Index des UDP-Streams
rtp.stream	Nummer	Index des RTP-Streams
voip.stream	Nummer	Index der VoIP-Verbindung
pn_io.stream	Nummer	Index der PN-IO-Verbindung

Um ein Feld mit einem anderen Feld oder einem Festwert zu vergleichen, können Sie einen der folgenden Vergleichs-Operatoren verwenden:

C-Syntax	Textform	Beschreibung
		prüft, ob das Feld vorhanden ist *(kein Vergleichs-Operator und Vergleichs-Wert)*
==	eq	prüft, ob eine Übereinstimmung besteht
!=	ne	prüft, ob eine Übereinstimmung nicht besteht
>=	ge	prüft, ob der Feldwert größer als der oder gleich dem Wert ist
>	gt	prüft, ob der Feldwert größer als der Wert ist
<=	le	prüft, ob der Feldwert kleiner als der oder gleich dem Wert ist
<	lt	prüft, ob der Feldwert kleiner als der Wert ist
&		prüft, ob die bitweise UND-Verknüpfung ungleich 0 ergibt
	contains	prüft, ob das Feld den Wert enthält

Beispiel: *udp.srcport>=1024*

Hinweis:
Für die Datentypen „Wahrheitswert“, „MAC-Adresse“, „IPv4-Adresse“ und „IPv6-Adresse“ sowie für den Vergleich von zwei Feldern oder Feldgruppen sind nur die Operatoren ==/eq und !=/ne sowie die Prüfung auf die Existenz des Felds möglich. Der Operator contains kann zudem nur auf den Datentyp „Zeichenkette“ angewendet werden.

Um mehrere Bedingungen miteinander verknüpfen zu können, können Sie die folgenden Kombinations-Operatoren verwenden:

C-Syntax	Textform	Beschreibung
&&	and	logisches UND, beide Bedingungen müssen zutreffen
||	or	logisches ODER, eine Bedingung muss zutreffen
^^	xor	logisches Exklusiv-ODER, nur eine Bedingung darf zutreffen

Beispiel: *ip or ipv6*

Für die Gruppierung von Bedingungen können die runden Klammern verwendet werden. (z. B. *ip.addr==192.168.1.10 and (udp or tcp)*)

Um eine Bedingung zu negieren, muss vor dem Feldnamen oder der öffnenden Klammer (bei einer Gruppe) ein Ausrufezeichen notiert werden. (z. B. *!udp*)

Hinweis:
Möchten Sie den Filter entfernen, so müssen Sie die Eingabe im Textfeld für den Anzeigefilter einfach löschen und die leere Eingabe bestätigen.

4.3.4 Suche

Neben der Filterung der Anzeige, haben Sie auch die Möglichkeit in der Frame-Tabelle nach Rohdaten zu suchen. Dies ist vor allem dann nützlich, wenn das Protokoll nicht weiter analysiert werden kann. Die Suche ist abhängig vom Filter, d. h. werden z. B. nur UDP-Datagramme angezeigt (da als Anzeigefilter *udp* verwendet wurde), wird auch nur in diesen Frames gesucht.

Für die Suche, steht Ihnen ein Textfeld zur Verfügung, in welchem Sie entweder eine Zeichenkette (muss in doppelten Anführungszeichen notiert werden, z. B. *"Hallo"*) oder eine oder mehrere Hexadezimal-Werte (muss mit 0x beginnen, z. B. *0x1A2B3C*) eingeben können.

Um die Suche letztendlich durchzuführen, können Sie entweder mit dem Symbol ▼ vorwärts suchen oder mit dem Symbol ▲ rückwärts suchen. Befindet sich der Fokus im Textfeld der Suche, so können Sie auch die Eingabetaste betätigen, um vorwärts zu suchen. Die Suche beginnt, sobald diese am Ende angekommen ist, automatisch wieder am Anfang.

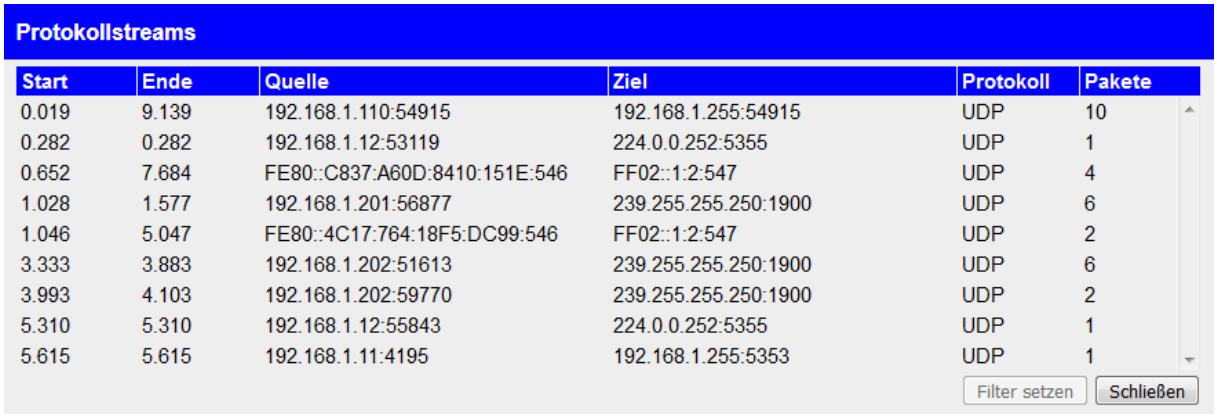
Wurde die Zeichenkette oder der Hexadezimal-Wert gefunden, so wird die Detailanzeige des Frames, in welchem die Eingabe gefunden wurde, geöffnet und die gefundene Stelle in den Rohdaten (und ggf. in den analysierten Daten) hervorgehoben.

4.3.5 Protokollstreams

Oft ist es nicht möglich, dass alle Daten innerhalb eines Frames versendet werden oder es benötigt einfach nur mehrere Durchläufe, bis z. B. eine IP-Adresse per DHCP vergeben ist. Daher kann es nützlich sein, alle Frames die dem gleichen Stream (OSI-Layer 4) angehören auf einmal anzeigen zu können.

Auf der Website wird während der Aufzeichnung eine Liste mit Streams (aktuell werden hier die Transportprotokolle TCP und UDP unterstützt) erzeugt. Die Zuordnung eines Frames zu einem Stream funktioniert hierbei über die IP-Adressen und Ports.

Möchten Sie sich die Liste mit allen Streams anzeigen lassen, so müssen Sie lediglich auf das Symbol in der Toolbar klicken. Sie sollten nun einen Dialog sehen:



In diesem Dialog sehen Sie nun eine Liste mit allen TCP- und UDP-Streams. Die einzelnen Zeilen der Tabelle sind anklickbar. Durch einen Klick wird die Zeile hellblau markiert und der Button „Filter setzen“ sowie ggf. der Button „Analyse anzeigen“ (aktuell nur bei TCP-Streams) freigeschalten. Klicken Sie auf den Button „Filter setzen“, so wird ein Anzeigefilter gesetzt, wodurch nur noch Frames angezeigt werden, die dem gewählten Stream angehören. Über den Button „Analyse anzeigen“ (falls verfügbar) öffnet sich ein neuer Dialog, in welchem dann weitere Informationen über den selektierten Stream angezeigt werden, die während der Aufzeichnung analysiert wurden.

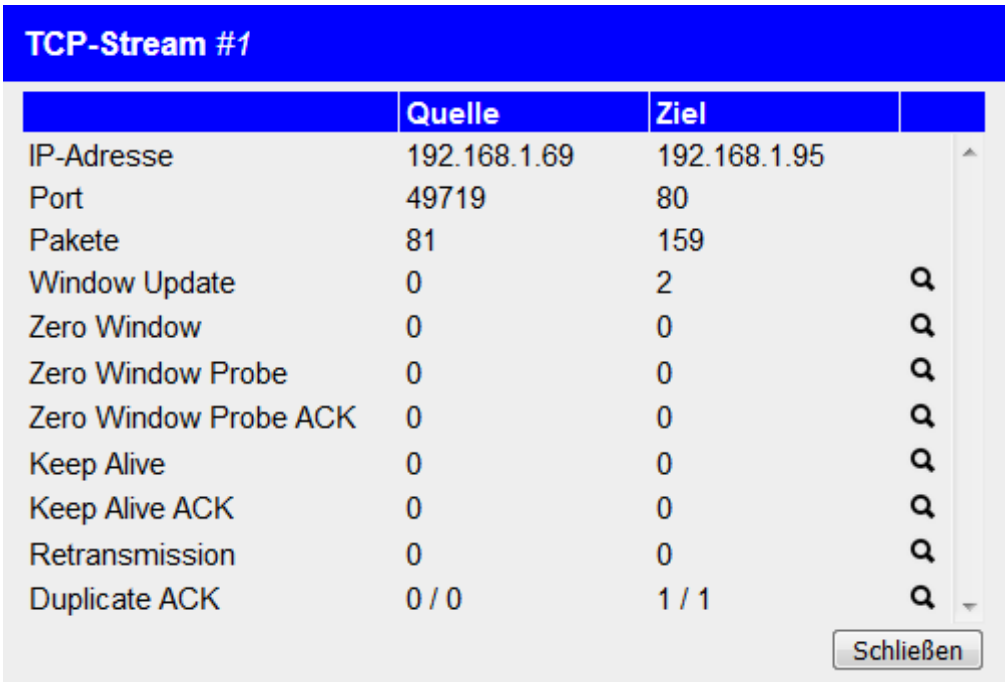
Der Anzeigefilter und der Analyse-Dialog kann auch direkt über ein einzelnes Frame gesetzt bzw. geöffnet werden. Öffnen Sie hierzu zunächst den Dialog für „Frameinformationen und -einstellungen“. Dort haben Sie dann die Möglichkeit über den Button „TCP-Stream folgen“ bzw. „UDP-Stream folgen“ den Anzeigefilter für den Stream, zu welchem das Frame gehört, zu setzen. Des Weiteren können Sie bei TCP-Frames über den Button „TCP-Stream-Analyse anzeigen“ den Analyse-Dialog für den TCP-Stream öffnen.

4.3.6 TCP-Analyse

Einige Informationen von TCP-Streams können nicht aus den einzelnen Frames abgelesen werden, sondern müssen über mehre Frames hinaus analysiert werden. Dadurch lassen sich dann Staus, Wiederholungen und einiges mehr erkennen.

Weil die Analyse dieser Stream-Informationen relativ komplex ist und gute Kenntnisse im TCP-Protokoll benötigt wären, müssen Sie dies natürlich nicht händisch machen. Vielmehr bietet Ihnen die Webseite des Analyzers die Möglichkeit diese Informationen bequem anzuzeigen.

Möchten Sie die Analyse eines TCP-Streams anzeigen, so können Sie den Dialog über den Button „TCP-Stream-Analyse anzeigen“ im Dialog „Frameinformationen und -einstellungen“ oder aber über den Button „Analyse anzeigen“ im Dialog „Protokollstreams“ öffnen. Sie sollten nun diesen Dialog sehen:



Der Dialog zeigt eine Tabelle mit verschiedenen Informationen getrennt nach Quelle und Ziel, also den beiden Verbindungspartnern, an. In den oberen Zeilen werden zunächst die IP-Adresse, der Port und die Paketanzahl von beiden Teilnehmern angezeigt. In den nächsten Zeilen werden dann die TCP relevanten Analyse-Daten angezeigt:

Window Update: Ein Paket, welches den Partner über eine geänderte Fenstergröße informiert.

Zero Window:	Ein Paket, welches den Partner darüber informiert, dass keine weiteren Daten gesendet werden dürfen. Dies kann ein Hinweis auf einen Datenstau sein.
Zero Window Probe:	Ein Paket, welches an den Partner gesendet wird, um festzustellen, ob immer noch keine Daten gesendet werden dürfen.
Zero Window Probe ACK:	Ein Paket, welches den Partner darüber informiert, dass weiterhin keine weiteren Daten gesendet werden dürfen.
Keep Alive:	Ein Paket, welches an den Partner gesendet wird um die Verbindung zu erhalten. Dies ist notwendig, falls die Verbindung bestehen bleiben soll, aber nicht dauerhaft Daten gesendet werden.
Keep Alive ACK:	Ein Paket, welches das Erhalten der Verbindung bestätigt.
Retransmission:	Ein Paket, welches erneut gesendet wird. Es handelt sich also um eine Wiederholung.
Duplicate ACK:	Ein Paket, welches ein erhaltenes Paket erneut bestätigt. Die erste Zahl gibt die Anzahl der Paket-Zuordnungen an und die zweite die tatsächliche Anzahl der Duplicate ACK Pakete.

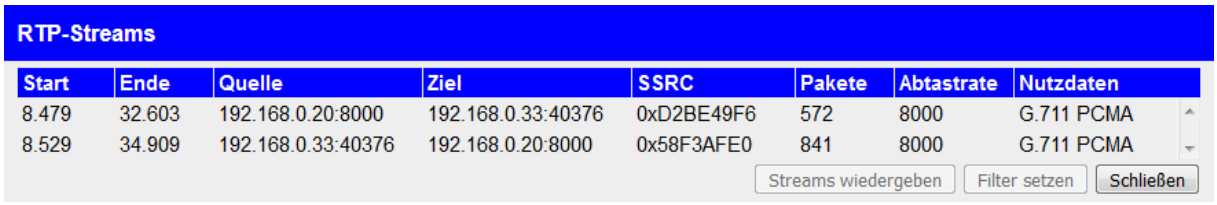
Für die unterschiedlichen „Pakettypen“ können auch direkt Filter gesetzt werden. Hierzu können Sie das Icon 🔍 in der letzten Spalte der Tabelle verwenden. Wenn Sie also auf das Symbol in der Zeile „Retransmission“ klicken, dann wird ein Filter gesetzt, wodurch nur noch Frames des aktuellen analysierten Streams, die erneut gesendet wurden, angezeigt werden.

4.3.7 RTP-Streams

RTP-Streams sind Datenströme für die Übertragung von Audio- und Videodaten in Echtzeit. Die Zuordnung von RTP-Streams läuft dabei nicht nur über die IP-Adressen und Ports, sondern auch über die im Frame enthaltene SSRC.

Die Analyse von einzelnen RTP-Frames ist eher umständlich. Deshalb können Sie sich auf der Webseite eine Liste mit allen RTP-Streams anzeigen lassen. Des Weiteren haben Sie, abhängig des Nutzdatentyps, die Möglichkeit sich die Nutzdaten der RTP-Streams wiedergeben zu lassen *(siehe unten)*.

Um sich die Liste mit RTP-Streams anzeigen zu lassen, müssen Sie in der Toolbar auf das Icon klicken. Sie sollten nun einen Dialog sehen, der dem folgenden ähnlich sieht:



Der Dialog umfasst eine Tabelle, wobei jeder RTP-Stream durch eine eigene Zeile dargestellt wird. Für jeden Stream werden dabei unter anderem die Start- und Endzeit, sowie die Quelle, das Ziel und die SSRC angezeigt. Des Weiteren wird noch die Anzahl an Paketen, die Abtastrate (nur bei unterstützten Audioformaten) und der Nutzdatentyp angezeigt.

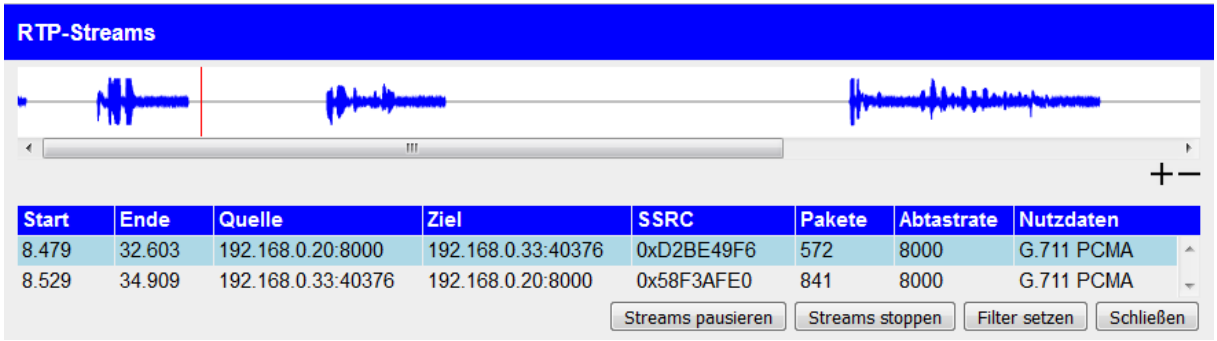
Die Zeilen in der Tabelle können auch angeklickt werden. Durch das Wählen eines Streams wird dieser mit einer hellblauen Farbe markiert und die Buttons „Streams wiedergeben“ und „Filter setzen“ werden aktiviert. Ein Klick auf den Button „Filter setzen“ führt dazu, dass ein Anzeigefilter gesetzt wird, wodurch nur noch der gewählte Stream in der Frametabelle angezeigt wird.

Falls Sie mehrere Streams selektieren möchten, so müssen Sie die Strg/Ctrl-Taste gedrückt halten, während Sie auf eine der Zeilen klicken. Mit der gleichen Methode können Sie die Auswahl eines Streams auch wieder aufheben. Das Auswählen eines Streams ohne dabei die Strg/Ctrl-Taste gedrückt zu halten, entfernt die Auswahl aller anderen Streams automatisch.

Die Wiedergabe von einem (oder auch mehreren) Stream(s) kann mit Hilfe des Buttons „Streams wiedergeben“ gestartet werden. Diese Funktion beschränkt sich aktuell jedoch auf die Wiedergabe von Audiostreams. Als Nutzdaten für die Audiostreams werden die Codecs

„G.711 PCMA“ und „G.711 PCMU“ unterstützt. Andere Codecs können aktuell nicht wiedergegeben werden.

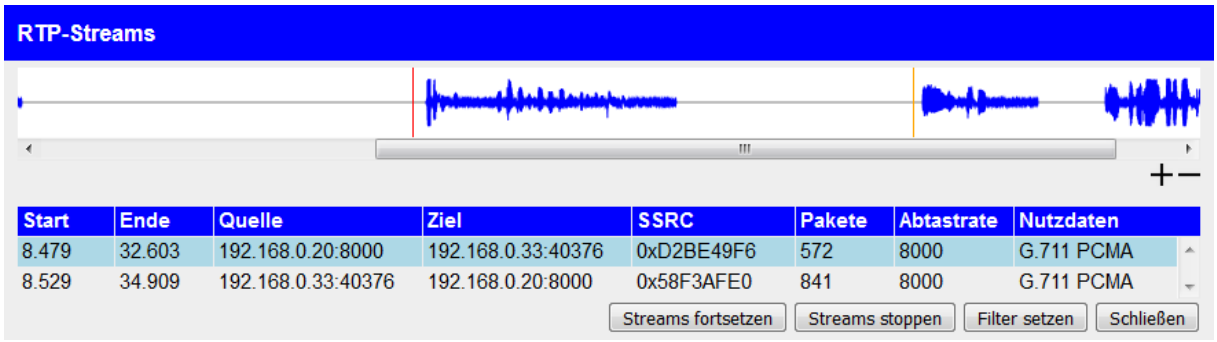
Sofern Sie bereits mindestens einen Audiostream mit unterstütztem Codec gewählt haben, so sollten Sie oberhalb der Tabelle ein Waveform-Diagramm sehen, wie man es auch aus Audio-Bearbeitungsprogrammen kennt:



Der rote Strich innerhalb des Diagramms zeigt die aktuelle Position der Wiedergabe an. Dieser wird jedoch nur angezeigt, falls die Wiedergabe aktuell läuft oder pausiert ist. Mit Hilfe der Icons + und ─ haben Sie die Möglichkeit das Waveform-Diagramm bzw. die Audiospuren zu Vergrößern oder zu Verkleinern.

Haben Sie die Wiedergabe bereits gestartet *(wie im Bild oben zu sehen)*, so sehen Sie nun an Stelle des Buttons „Streams wiedergeben“ die Buttons „Streams pausieren“ und „Streams stoppen“, wodurch Sie die Wiedergabe pausieren oder komplett stoppen können. Ist die Wiedergabe pausiert, so sehen Sie an Stelle des Buttons „Streams pausieren“ den Button „Streams fortsetzen“, mit welchem die Wiedergabe an der vorherigen Stelle wieder fortgesetzt werden kann.

Sie können die Wiedergabe-Position auch manuell setzen. Hierfür müssen Sie mit der Maus einfach in das Waveform-Diagramm fahren. Dieser „Hand-Cursor“ wird durch eine orange Linie gekennzeichnet. Haben Sie Ihre gewünschte Position gefunden, so müssen Sie lediglich die linke Maustaste einmalig drücken. Der (rote) Wiedergabe-Cursor wird nun automatisch an diese Position gesetzt.



Hinweis:
Für die Audio-Wiedergabe wird die „Web Audio API“ Ihres Browser verwendet. Einige Browser (u. a. der Microsoft Internet Explorer und der Android Browser) unterstützen diese Funktion leider nicht.

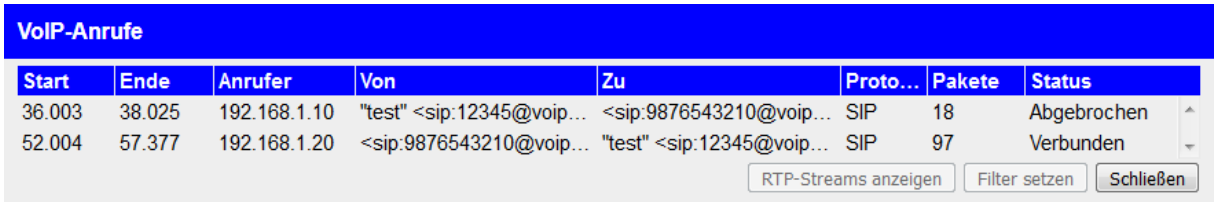
4.3.8 VoIP-Verbindungen

Um eine VoIP-Verbindung aufzubauen und Gesprächsdaten übertragen zu können, nutzt die VoIP-Technologie mehrere Protokolle. Des Weiteren müssen erst ein paar Frames empfangen und versendet werden, bevor eine Verbindung bzw. ein Anruf zu Stande kommt.

Da die Analyse mit reinen Protokolldissektoren eher weniger komfortabel ist, werden die VoIP-Protokolle automatisch detaillierter analysiert, wodurch mehrere Frames zu einer gemeinsamen Verbindung und somit zu einem Anruf zugeordnet werden. Als Signalisierungsprotokoll wird aktuell nur SIP (Session Initiation Protocol) in Verbindung mit SDP (Session Description Protocol) unterstützt. Für die Gesprächsdaten-übertragung werden die Protokolle RTP und RTCP unterstützt.

Des Weiteren haben Sie auch die Möglichkeit die Gesprächsdaten (Audio), welcher per RTP übertragen werden zu analysieren und wiederzugeben.

Möchten Sie sich die VoIP-Anrufe der Aufzeichnung anzeigen lassen, so müssen Sie lediglich auf das -Symbol in der Toolbar (oberhalb der Frametabelle) klicken. Es öffnet sich nun folgender Dialog:



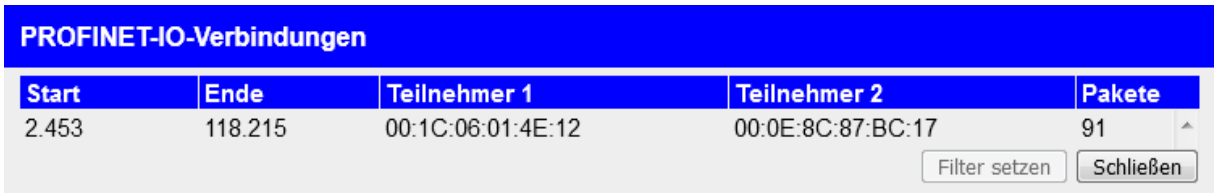
Im Dialog ist eine Tabelle zu sehen, wobei jede Zeile einen VoIP-Anruf repräsentiert. Die Zeile umfasst dabei Informationen wie z. B. die Start- und Endzeit, die zwei Teilnehmer des Anrufs sowie den Status der Verbindung. Die Zeilen der Tabellen sind anklickbar. Sobald Sie auf einen Eintrag geklickt haben, wird die Zeile hellblau markiert und die Buttons „RTP-Streams anzeigen“ und „Filter setzen“ freigeschalten. Ein Klick auf den Button „RTP-Streams anzeigen“ zeigt die Liste mit RTP-Streams an. In der Liste werden jetzt jedoch nur die Streams angezeigt, welcher der VoIP-Verbindung angehören. Der Dialog für die RTP-Streams wurde bereits im vorherigen Thema erklärt. Falls Sie auf den Button „Filter setzen“ klicken, dann wird ein Anzeigefilter gesetzt, wodurch nur noch Frames, die dieser VoIP-Verbindung angehören, angezeigt werden.

4.3.9 PROFINET-IO-Verbindungen

Falls Sie mit Ihrem Gerät PROFINET-IO-Kommunikation (kurz PN-IO) analysieren möchten, kann es sinnvoll sein, bei der Analyse nur den PROFINET-Traffic zwischen zwei Teilnehmern zu sehen.

Um eine Alternative zur manuellen Eingabe von MAC-Adressen und weiteren Filtern anzubieten, können Sie sich eine Liste mit allen PN-IO-Kommunikationen einfach anzeigen lassen. Hierbei werden sowohl die PN-IO-Protokolle, die direkt per Ethernet oder auch per TCP oder UDP empfangen und versendet werden, als auch die für die Verwaltung genutzten PN-IO-Context-Manager-Protokolle berücksichtigt.

Möchten Sie sich die Liste mit PN-IO-Verbindungen anzeigen lassen, so müssen Sie lediglich auf das Symbol ⚙ klicken, welches Sie in der Toolbar (oberhalb der Frame-Tabelle) finden können. Sie sollten nun folgenden Dialog sehen:



Im Dialog sehen Sie eine Tabelle mit allen Verbindungen. Dabei wird die Zeit des ersten und letzten Frames, die MAC-Adressen der beiden Kommunikations-Teilnehmer sowie die Anzahl der Frames angezeigt. Jede Tabellenzeile kann angeklickt werden. Dabei wird die Zeile hellblau hinterlegt und der Button „Filter setzen“ freigeschalten. Mit Hilfe des Buttons „Filter setzen“ können Sie einen Anzeigefilter setzen, wodurch dann nur noch Frames, die der PROFINET-IO-Verbindung angehören angezeigt werden.

4.3.10 Anwendungsprotokolle

Die Auswahl eines Anwendungsprotokolls (OSI-Layer 5 bis 7) bei der Frameanalyse ist, anders als bei den OSI-Layern 2 bis 4, nicht eindeutig, d. h. das Anwendungsprotokoll wird auf Basis des Transportprotokolls und der verwendeten Ports (Quell- und Zielport) getroffen. Es gibt zwar standardisierte Ports, jedoch können diese meist nach belieben geändert werden (z. B. für Portweiterleitungen).

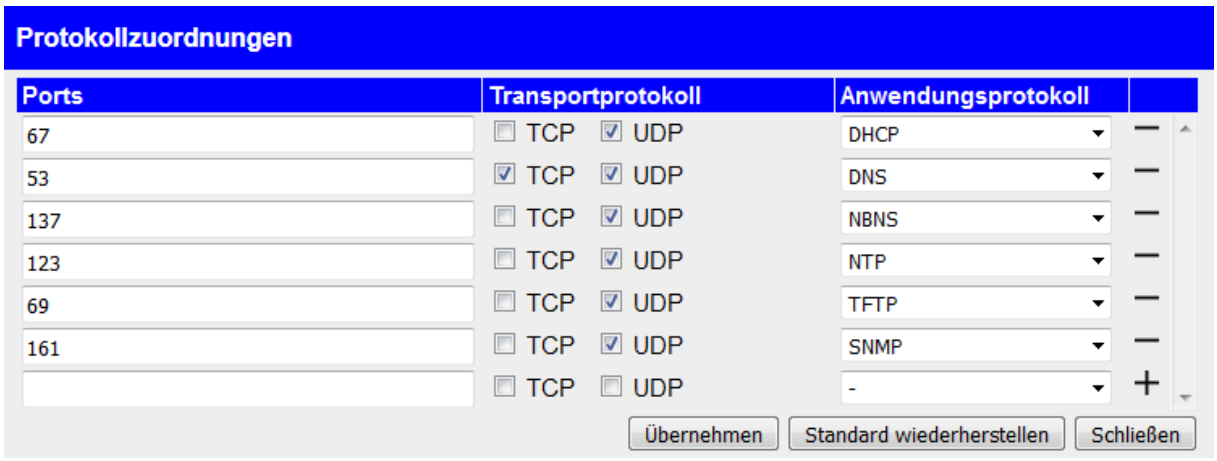
Auf der Aufzeichnungsseite des Geräts haben Sie deshalb die Möglichkeit die Zuordnungen von Ports in Kombination mit dem Transportprotokoll zu einem Anwendungsprotokoll selbst völlig frei festzulegen.

Die folgende Tabelle zeigt die standardmäßigen Protokollzuordnungen, welche bei der Geräteauslieferung gesetzt sind:

Ports	**Transportprotokoll**	**Anwendungsprotokoll**
67	UDP	DHCP
53	TCP; UDP	DNS
137	UDP	NBNS
123	UDP	NTP
69	UDP	TFTP
161	UDP	SNMP
21	TCP	FTP
80	TCP	HTTP
25	TCP	SMTP
110	TCP	POP
143	TCP	IAMP
5060	TCP; UDP	SIP
102	TCP	TPKT
1720	TCP	Q931

Ports	Transportprotokoll	Anwendungsprotokoll
34962, 34963	TCP; UDP	PN-RT
135	TCP	DCE/RPC
34964	TCP; UDP	PN-IO *(CM per DCE/RPC)*
0, 7, 9	UDP	WOL
5355	TCP; UDP	LLMNR
1900	UDP	SSDP

Möchten Sie sich die aktuellen Protokollzuordnungen anschauen oder diese editieren, so können Sie auf das 🛠-Icon, welches sich in der Toolbar oberhalb der Tabelle befindet, klicken. Darauf erscheint folgender Dialog:



Jede Zeile der Tabelle stellt eine Zuordnung dar. Möchten Sie mit einer Zuordnung mehrere Ports verknüpfen, so haben Sie die Möglichkeit mehrere Ports durch Komma getrennt anzugeben (z. B. *123,124*). Über die Auswahlkästchen in der Spalte „Transportprotokoll“ können Sie wählen, bei welchen Transportprotokollen die Zuordnung gilt. In der letzten Spalten wählen Sie dann letztendlich das Anwendungsprotokoll aus.

Um eine bestehende Zuordnung zu löschen, müssen Sie lediglich auf das ─-Symbol am Ende der Zeile klicken.

Möchten Sie dagegen eine neue Zuordnung hinterlegen, so müssen Sie die letzte Zeile ausfüllen und auf das Symbol + klicken.

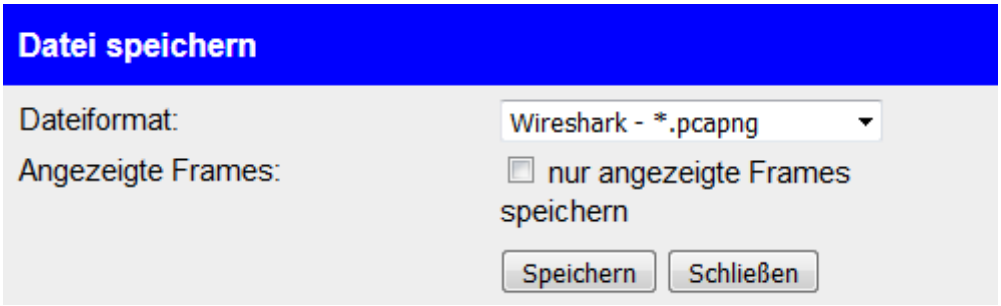
Sobald Sie die Zuordnungen konfiguriert haben, können Sie über den Button „Übernehmen“ die Zuordnung speichern. Dadurch werden alle Frames der aktuellen Aufzeichnung, die über ein Anwendungsprotokoll verfügen neu analysiert. Zudem werden die Zuordnungen in der Konfiguration gespeichert, wodurch diese nach einem Seitenwechsel oder einem Geräteneustart weiterhin verfügbar sind. Falls Sie auf den Button „Schließen“ oder auf die dahinterliegende Seite (außerhalb des Dialogs) klicken, dann gehen die Änderungen, welche Sie ggf. bereits im Dialog durchgeführt haben, wieder verloren.

Falls Sie die Standardzuordnungen wiederherstellen möchten (siehe Tabelle oben), dann können Sie auf den Button „Standard wiederherstellen“ klicken. Im Anschluss müssen Sie auf „Übernehmen“ klicken, um die Standardzuordnungen dann auch wirklich zu speichern.

4.3.11 Aufzeichnung speichern

Möchten Sie die Aufzeichnung (also die Frame-Tabelle in Ihrem Browser) speichern, so haben Sie die Möglichkeit die Daten direkt im Wireshark-Dateiformat auf Ihrem Computer abzuspeichern. Klicken Sie dazu einfach auf das ⊕ Symbol in der Toolbar.

Daraufhin erscheint folgendes Pop-up:



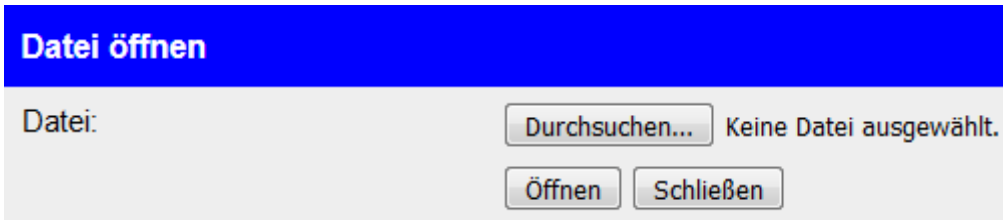
Sie können dort zum einen wählen, in welchem Dateiformat (.pcapng oder .pcap) die Aufzeichnung gespeichert werden soll, und, ob nur angezeigte Frames (abhängig des Anzeigefilters) in der Datei gespeichert werden sollen.

Mit einem Klick auf „Speichern“ erhalten Sie, je nach Einstellung im Browser, ein Download-Fenster angezeigt oder die Datei wird direkt im Downloads-Ordner gespeichert.

4.3.12 Aufzeichnung öffnen

Sie haben über die Aufzeichnungs-Seite auch die Möglichkeit, eine bereits bestehende Aufzeichnungs-Datei wieder zu öffnen. Dabei spielt es keine Rolle, ob diese von einem Ihrer Analysegeräte oder vom Programm Wireshark erzeugt wurde. Das Öffnen einer Aufzeichnungs-Datei ist mit Hilfe des Icons ☁ möglich.

Nachdem Sie auf das Symbol geklickt haben, erhalten Sie folgende Anzeige:



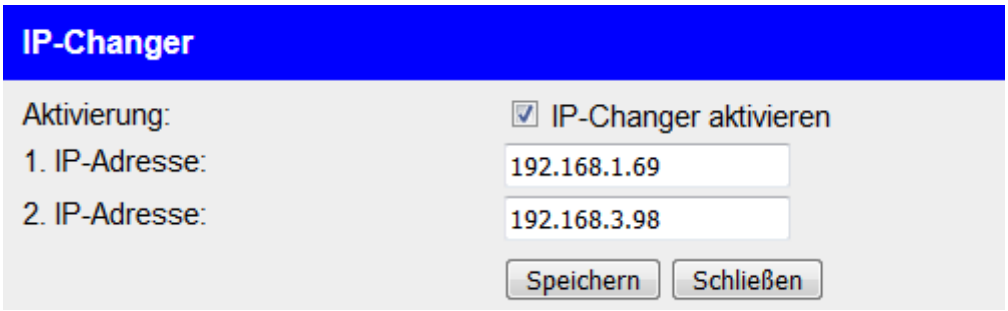
Sobald Sie eine Datei ausgewählt haben, können Sie mit einem Klick auf den Button „Öffnen“ die Datei öffnen. Nun wird der Dateiinhalt eingelesen und die darin enthaltenen Frames in der bekannten Oberfläche angezeigt.

4.3.13 IP-Changer

Der Analyzer ist in der Lage IPv4-Adressen zu tauschen, um somit zwei Teilnehmer die sich in einem unterschiedlichen Subnetz befinden, in das gleiche Subnetz zu bringen, sodass diese miteinander kommunizieren können.

Der IP-Changer muss dazu aktiviert und die zwei IPv4-Adressen, die miteinander kommunizieren sollen, müssen eingestellt werden. Des Weiteren müssen sich die beiden Geräte mit den eingestellten IPv4-Adressen auf unterschiedlichen Schnittstellen befinden, sodass der Netzwerkverkehr durch das Analysegerät geleitet wird und von diesem verändert werden kann.

Um den IP-Changer einzustellen, müssen Sie auf das Symbol ⇆ in der Toolbar klicken. Es sollte sich nun folgender Dialog öffnen:



In folgendem Beispiel *(siehe Bild auf der vorherigen Seite)* wird davon ausgegangen, dass das Gerät mit der IP-Adresse 192.168.1.69 an Schnittstelle A und das Gerät mit der IP 192.168.3.98 hingegen an der Schnittstelle B angeschlossen ist.

Sobald Sie den IP-Changer konfiguriert und aktiviert haben, kann das Gerät mit der IP-Adresse 192.168.1.69 nun auf das andere Gerät mit Hilfe der „virtuellen“ IP-Adresse 192.168.1.98 zugreifen, welches eigentlich die IP-Adresse 192.168.3.98 hat. Das gleiche Verfahren gilt auch anders herum.

Hinweis:
Der IP-Changer tauscht immer nur die ersten drei Bytes der IP-Adresse. Das vierte und letzte Byte der IP-Adresse bleibt erhalten.

Wichtig:
Das Gerät prüft nicht ob die virtuelle IP-Adressen frei sind. Sind die Adressen belegt und Sie aktivieren den IP-Changer trotzdem, dann kommt es zu einem IP-Konflikt.

Wenn Sie nun eine Aufzeichnung im Webbrowser durchführen (hier eignet sich nun das Aufzeichnen der Schnittstelle „A und B“), können Sie sehen, wie die IP-Adressen verändert werden. Die IP-Adressen-Felder von Frames deren IP-Adresse durch den IP-Changer geändert werden bzw. bereits wurden werden in roter Textfarbe dargestellt:

A → B	3	0.494	192.168.1.69	192.168.1.98	TCP	66	55666 » 80 [SYN] Win=8192
B ← A	4	0.494	192.168.3.69	192.168.3.98	TCP	66	55666 » 80 [SYN] Win=8192
B → A	5	0.494	192.168.3.98	192.168.3.69	TCP	60	80 » 55666 [SYN ACK] Win=512
A ← B	6	0.494	192.168.1.98	192.168.1.69	TCP	60	80 » 55666 [SYN ACK] Win=512
A → B	7	0.495	192.168.1.69	192.168.1.98	TCP	60	55666 » 80 [ACK] Win=64240
B ← A	8	0.495	192.168.3.69	192.168.3.98	TCP	60	55666 » 80 [ACK] Win=64240
A → B	9	0.498	192.168.1.69	192.168.1.98	HTTP	384	55666 » 80 [PSH ACK] Win=64240
B ← A	10	0.498	192.168.3.69	192.168.3.98	HTTP	384	55666 » 80 [PSH ACK] Win=64240

Des Weiteren wird Ihnen, wenn Sie auf eine der Adressen mit der Maus fahren ein Tool-Tip mit weiteren Informationen angezeigt.

Hinweis:
Der IP-Changer beim ProfiNet-WATCHDOG ist ohne Funktion.

4.3.14 Netzwerk-Überwachung

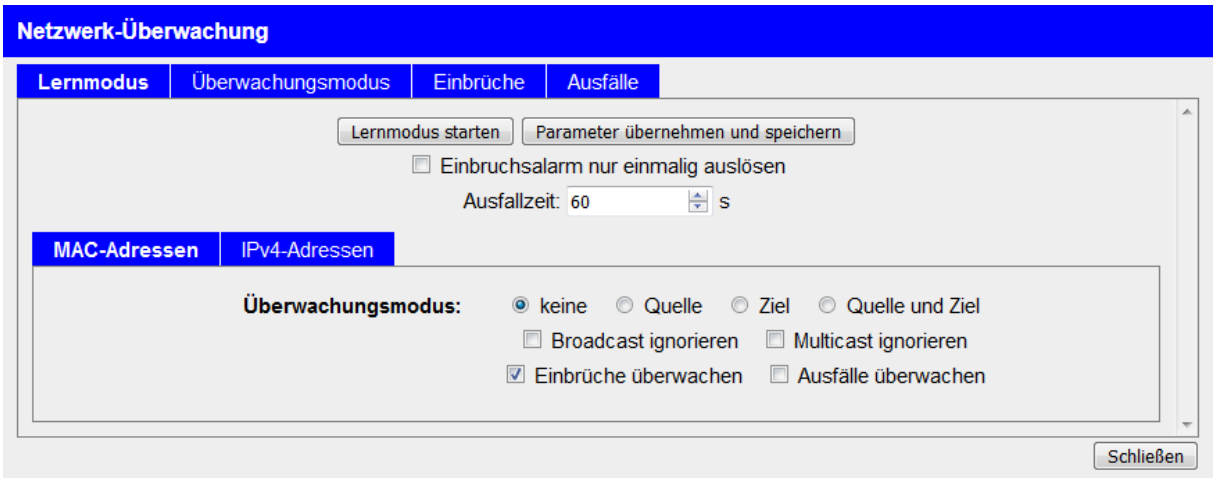
Neben der Bereitstellung verschiedener Anzeigen und Tools zur Analyse des Netzwerks ist es mit den Analysegeräten auch möglich, eine Überwachung des Netzwerks einzurichten und diese dann automatisch durchzuführen.

Als Grundlage für die Netzwerk-Überwachung dienen die eingehenden Frames getrennt nach Schnittstelle A und B. Das Netzwerk kann dabei frei konfigurierbar nach MAC- und / oder IPv4-Adressen auf Einbruch (unbekannte Adresse) und / oder Ausfall (bekannte Adresse für bestimmte Zeit nicht vorhanden) überwacht werden.

Einbrüche, also das Vorkommen von Adressen, die nicht eingelernt sind, können mit Hilfe des Aufzeichnungsmodi „Überwachung“ als vollständiges Frame direkt im Webbrowser angezeigt, an einen FTP-Server geschickt oder auf einen USB-Stick geschrieben werden. Des Weiteren können Sie sich eine Liste mit ausgefallen Adressen auf dem Webserver anzeigen lassen sowie Einbrüche auch direkt als E-Mail versenden lassen.

Die Überwachung von Ausfällen, also die zeitliche Überprüfung, ob eine Adresse für eine im Gerät eingestellte Dauer nicht kommuniziert hat, kann mit Hilfe des Überwachungs-Dialogs direkt im Webbrowser (Anzeige des letzten Kommunikationszeitpunkts) erfolgen. Zudem steht auf dem Webserver ein Log zur Verfügung, welches anzeigt, welche Adressen in welchem Zeitraum ausgefallen sind. Auch hier können Sie sich, falls aktiviert, die Ausfälle als E-Mail schicken lassen.

Um die Netzwerk-Überwachung einzustellen oder den aktuellen Status anzuzeigen, müssen Sie auf das Icon 🖳 klicken, welches Sie in der Toolbar finden. Nun öffnet sich folgender Dialog:



Der Dialog besitzt eine Leiste mit den folgenden Tabs:

- **Lernmodus:** Hier können Sie die Einstellungen für die Überwachung setzen und anschließend (falls gewünscht) das automatische Einlernen von Adressen starten.
- **Überwachungsmodus:** Hier können Sie die Einstellungen der aktiven Überwachung anschauen und bei Bedarf korrigieren sowie die Adressen der aktiven Überwachung verwalten.
- **Einbrüche:** Hier haben Sie die Möglichkeit eine Liste mit Adressen zu verwalten, die einen Einbruchsalarm ausgelöst haben.
- **Ausfälle:** Hier haben Sie die Möglichkeit eine Liste mit Adressen zu verwalten, die über einen bestimmten Zeitraum oder aktuell noch ausgefallen sind.

Bevor Sie mit dem Überwachen des Netzwerks beginnen können, müssen Sie erst mal definieren wie die Überwachung erfolgen soll.

Hierzu müssen Sie den Tab „Lernmodus“ angewählt haben. Dort stehen nun folgende allgemeine Einstellungen zur Verfügung:

- **Einbruchsalarm nur einmalig auslösen:** Gibt an, ob ein Alarm bei einem Einbruch pro Adresse nur einmalig ausgelöst werden soll oder für jedes Frame, welches einen Einbruch darstellt.
- **Ausfallzeit:** Die Zeit in Sekunden, nachdem eine Adresse, falls diese nicht mehr kommuniziert, als ausgefallen gilt.

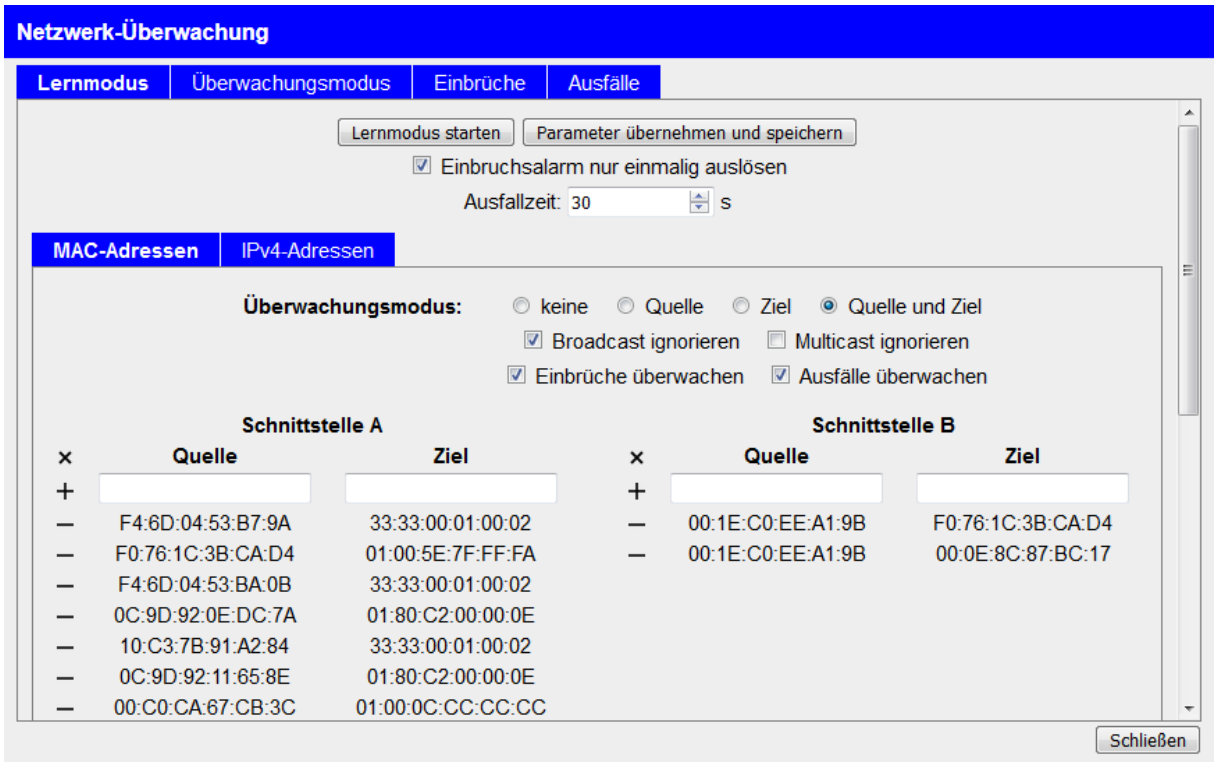
Unterhalb der allgemeinen Einstellungen sehen Sie eine weitere Leiste mit Tabs. Jeder Tab stellt dabei eine andere Adressart dar. Für jede Adressart sind folgende Einstellungen verfügbar:

- **Überwachungsmodus:** Auswahl, welche Adressen der Adressart überwacht werden soll:
  - **keine:** Die Adressen werden nicht überwacht.
  - **Quelle:** Es werden nur die Quell-Adressen überwacht.
  - **Ziel:** Es werden nur die Ziel-Adressen überwacht.
  - **Quelle und Ziel:** Es wird jede Kombination aus Quell- und Ziel-Adresse überwacht.
- **Broadcast ignorieren:** Gibt an, ob Broadcast-Adressen für die Überwachung ignoriert werden sollen (trifft nur für den Modus „Ziel“ und „Quelle und Ziel“ zu).
- **Multicast ignorieren:** Gibt an, ob Multicast-Adressen für die Überwachung ignoriert werden sollen (trifft nur für den Modus „Ziel“ und „Quelle und Ziel“ zu).
- **Einbrüche überwachen:** Gibt an, ob auf Einbrüche, also neue Adressen, überwacht werden soll.
- **Ausfälle überwachen:** Gibt an, ob auf Ausfall, also Adressen die über den angegebenen Zeitraum nicht kommunizieren, überwacht werden soll.

Sobald Sie alle Einstellungen vorgenommen haben, können Sie den Lernmodus (dabei werden alle im Netzwerk vorkommende Adressen automatisch in die Liste aufgenommen) mit Hilfe des Buttons „Lernmodus starten“ beginnen.

Die Liste mit Adressen sollte sich nun, je nach Anzahl der Geräte im Netzwerk, automatisch füllen. Wenn Sie der Meinung sein, dass nun alle Adressen eingelernt sind, können Sie den Lernmodus mit dem Button „Lernmodus stoppen“ beenden.

Bei Bedarf können Sie jetzt auch noch Adressen aus der Liste manuell entfernen, falls diese während des Lernmodus fälschlicherweise aufgenommen wurden, in dem Sie auf das Icon ─ bei dem jeweiligen Adresseintrag klicken.



Natürlich können Sie auch manuell eine fehlende Adresse zu der Liste hinzufügen, falls diese z. B. während des Lernmodus nicht kommuniziert hat. Hierzu müssen Sie die oberste Zeile der Tabelle ausfüllen und dann auf das Icon + klicken.

Des Weiteren haben Sie mit Hilfe des Icons ✕ die Möglichkeit, eine komplette Adressliste zurückzusetzen.

Um den ersten und letzten Kommunikationszeitpunkt einer Adresse (falls vorhanden) zu sehen, müssen Sie nur mit der Maus auf den jeweiligen Eintrag fahren. Die Informationen werden dann als Tool-Tip angezeigt. Dies ist auch bei deaktivierter Ausfallüberwachung verfügbar.

Hinweis:
Sie können den Lernmodus jeder Zeit erneut und beliebig oft ausführen. Eine evtl. bereits laufende Überwachung wird durch den Lernmodus nicht beeinflusst.

Sind Sie mit den Einstellungen noch nicht zufrieden, können Sie die Einstellungen auch noch nach der Durchführung des automatischen Lernmodus anpassen.

Alternativ können Sie auch nachdem Sie die Einstellungen gesetzt haben, alle Adressen manuell eintragen. Die Durchführung des automatischen Lernmodus ist dann nicht notwendig.

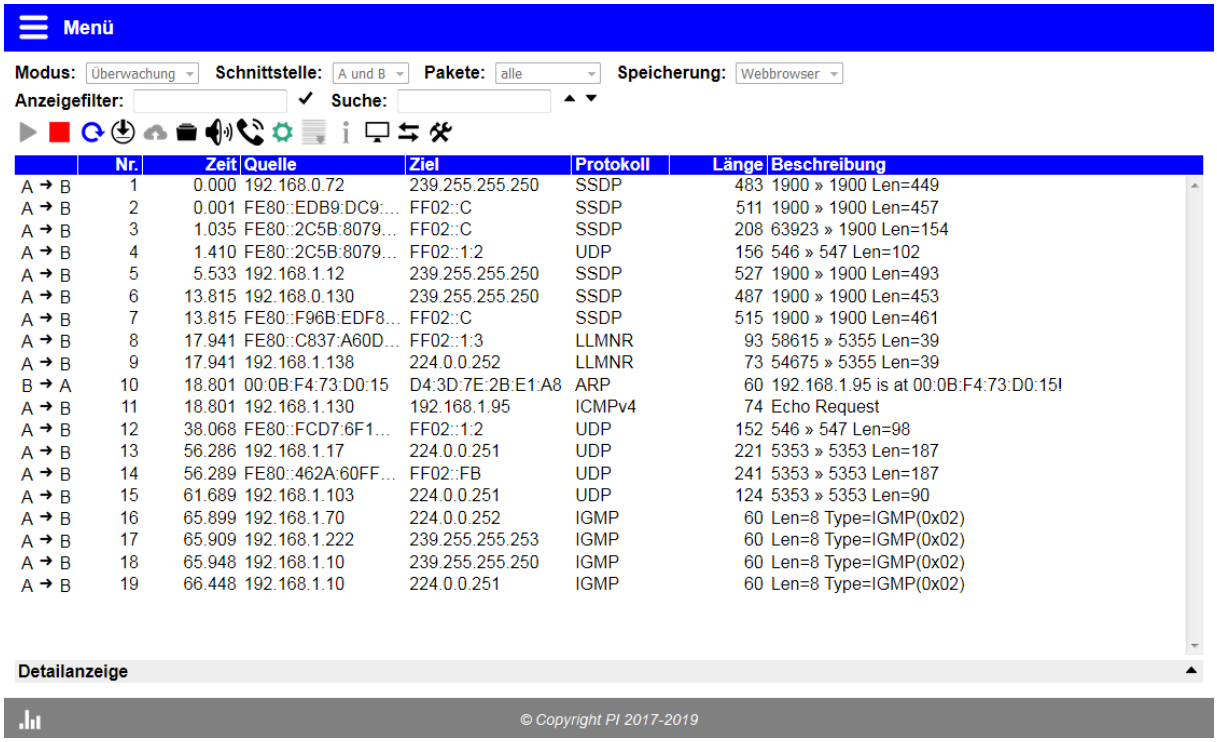
Möchten Sie die Überwachung nun mit den Einstellungen und Adressen des Lernmodus beginnen, so müssen Sie nur noch auf den Button „Parameter übernehmen und speichern“ klicken. Anschließend werden Sie automatisch auf den Tab „Überwachungsmodus“ weitergeleitet.

Auch hier steht Ihnen weiterhin, die Möglichkeit zur Verfügung fehlende Adressen mit dem ┼-Symbol in die Liste aufzunehmen, Adressen mit dem ─-Symbol aus der Liste zu entfernen sowie eine komplette Liste mit dem ✕-Symbol zurückzusetzen.

Das Hinzufügen und Löschen einer Adresse sowie das Zurücksetzen einer Liste wirkt sich dabei direkt auf die laufende Überwachung aus. Soll die Änderung auch nach einem Neustart des Analyzers erhalten bleiben, so müssen Sie noch zusätzlich auf den Button „Parameter speichern“ klicken, sobald Sie mit dem manuellen Hinzufügen und Löschen von Adressen fertig sind. Andernfalls ist die Änderung nach einem Neustart verloren.

Des Weiteren können Sie auch im Überwachungsmodus weiterhin einige Einstellungen anpassen. Sobald Sie eine oder mehrere Einstellung(en) angepasst haben, müssen Sie auf den Button „Parameter speichern“ klicken. Hierdurch werden die aktiven Einstellungen und Adressen für die Überwachung übernommen und im Gerät gespeichert.

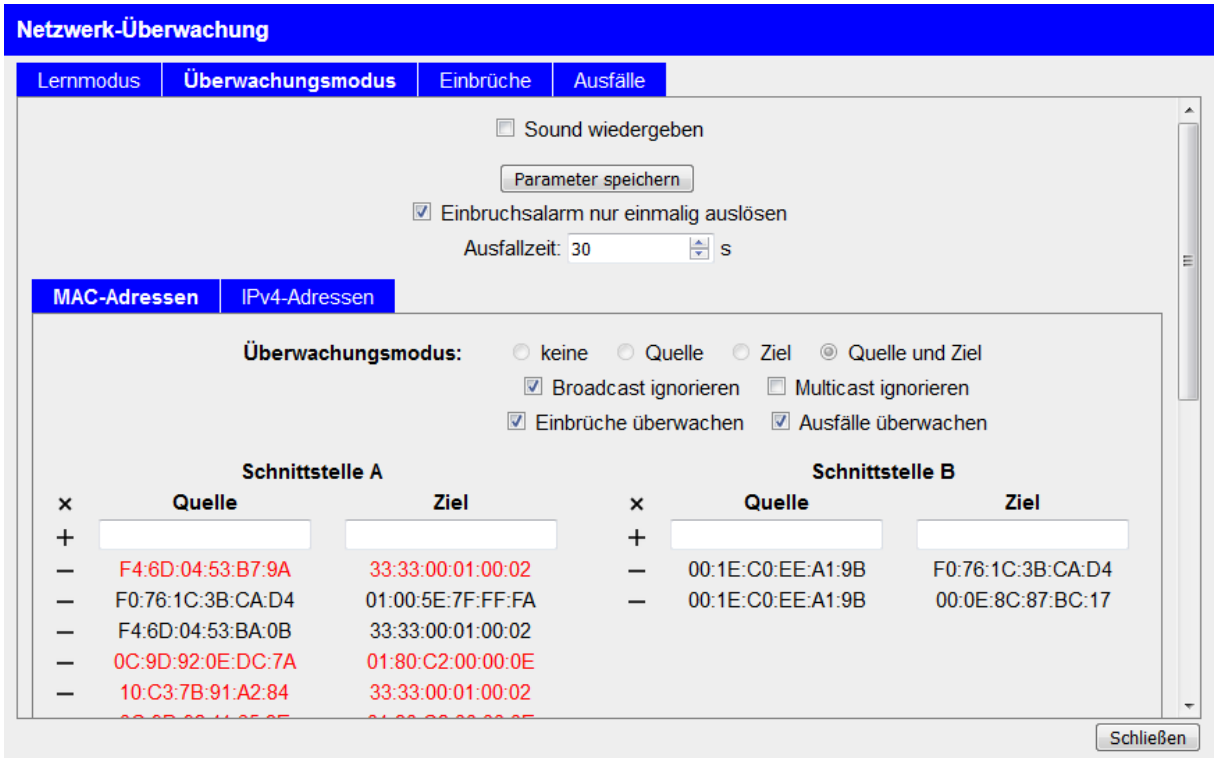
Um nun Frames aufzuzeichnen, die einen Einbruch darstellen, müssen Sie als Modus für die Aufzeichnung „Überwachung“ wählen. Des Weiteren sollten Sie als Schnittstelle „A und B“ auswählen, sodass Einbrüche von beiden Schnittstellen überwacht werden. Anschließend können Sie ganz normal eine Aufzeichnung starten.



	Nr.	Zeit	Quelle	Ziel	Protokoll	Länge	Beschreibung
A → B	1	0.000	192.168.0.72	239.255.255.250	SSDP	483	1900 » 1900 Len=449
A → B	2	0.001	FE80::EDB9:DC9:…	FF02::C	SSDP	511	1900 » 1900 Len=457
A → B	3	1.035	FE80::2C5B:8079…	FF02::C	SSDP	208	63923 » 1900 Len=154
A → B	4	1.410	FE80::2C5B:8079…	FF02::1:2	UDP	156	546 » 547 Len=102
A → B	5	5.533	192.168.1.12	239.255.255.250	SSDP	527	1900 » 1900 Len=493
A → B	6	13.815	192.168.0.130	239.255.255.250	SSDP	487	1900 » 1900 Len=453
A → B	7	13.815	FE80::F96B:EDF8…	FF02::C	SSDP	515	1900 » 1900 Len=461
A → B	8	17.941	FE80::C837:A60D…	FF02::1:3	LLMNR	93	58615 » 5355 Len=39
A → B	9	17.941	192.168.1.138	224.0.0.252	LLMNR	73	54675 » 5355 Len=39
B → A	10	18.801	00:0B:F4:73:D0:15	D4:3D:7E:2B:E1:A8	ARP	60	192.168.1.95 is at 00:0B:F4:73:D0:15
A → B	11	18.801	192.168.1.130	192.168.1.95	ICMPv4	74	Echo Request
A → B	12	38.068	FE80::FCD7:6F1…	FF02::1:2	UDP	152	546 » 547 Len=98
A → B	13	56.286	192.168.1.17	224.0.0.251	UDP	221	5353 » 5353 Len=187
A → B	14	56.289	FE80::462A:60FF…	FF02::FB	UDP	241	5353 » 5353 Len=187
A → B	15	61.689	192.168.1.103	224.0.0.251	UDP	124	5353 » 5353 Len=90
A → B	16	65.899	192.168.1.70	224.0.0.252	IGMP	60	Len=8 Type=IGMP(0x02)
A → B	17	65.909	192.168.1.222	239.255.255.253	IGMP	60	Len=8 Type=IGMP(0x02)
A → B	18	65.948	192.168.1.10	239.255.255.250	IGMP	60	Len=8 Type=IGMP(0x02)
A → B	19	66.448	192.168.1.10	224.0.0.251	IGMP	60	Len=8 Type=IGMP(0x02)

Hinweis:
Bitte achten Sie darauf, dass Sie bei der Auswahl „Pakete“ die Option „alle“ oder „empfangene“ gewählt ist, da für die Überwachung nur eingehende Frames beachtet werden.

Falls Sie die Adressen auch auf Ausfälle überwachen, dann werden im Tab „Überwachungsmodus“ alle Adressen die als ausgefallen gelten, rot markiert. Die Adressen deren Text schwarz gefärbt sind gelten (noch) nicht als ausgefallen.

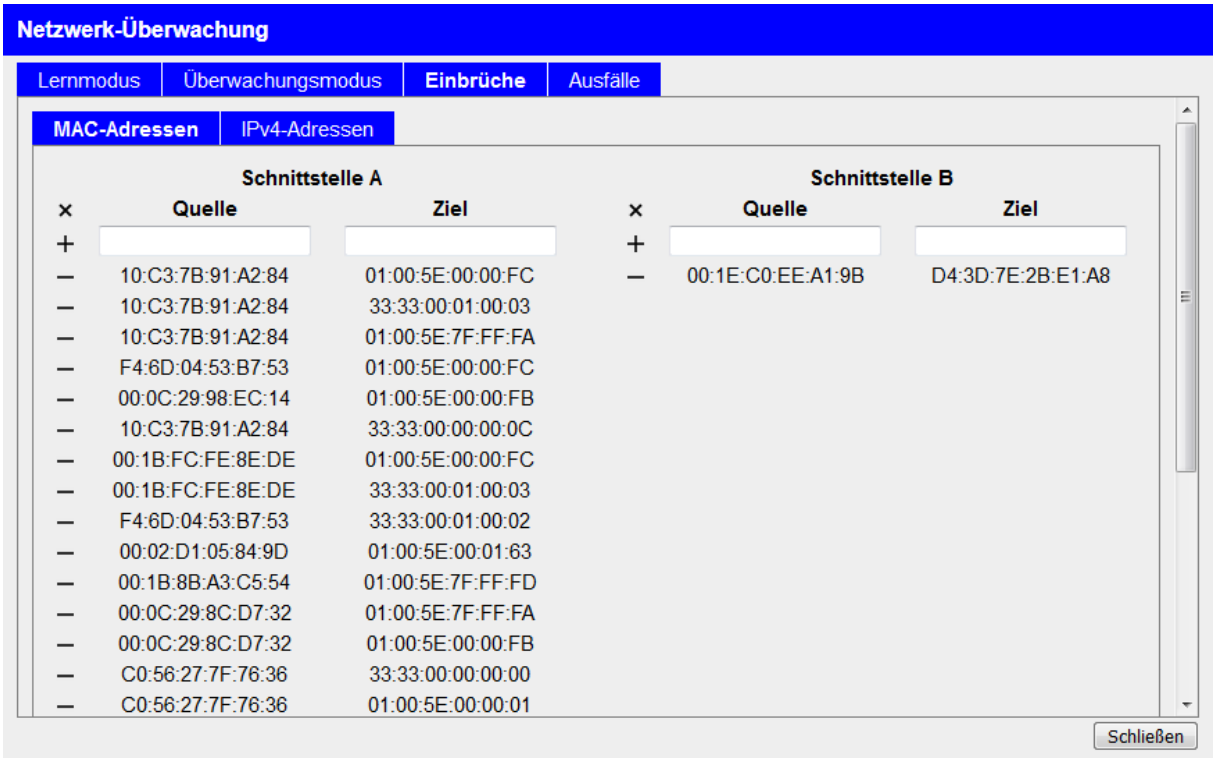


Möchten Sie, die Netzwerk-Überwachung in Ihrem Browser geöffnet lassen und nebenher etwas anderes arbeiten, jedoch über einen Vorfall informiert werden, so können Sie die Einstellung „Sound wiedergeben“ aktivieren. Dadurch wird bei einem Einbruch (nur falls eine Überwachungs-Aufzeichnung im Browser läuft oder die Einstellung „Einbruchsalarm nur einmalig auslösen“ gesetzt ist) oder Ausfall ein Sound wiedergegeben.

Ein tiefer Ton (750 Hz) signalisiert einen Ausfall, wohingegen ein hoher Ton (1250 Hz) einen Einbruch signalisiert.

Hinweis:
Für die Sound-Wiedergabe wird die „Web Audio API“ Ihres Browsers verwendet. Einige Browser (u. a. der Microsoft Internet Explorer und der Android Browser) unterstützen diese Funktion leider nicht.

Falls Sie eine Einbruchsüberwachung aktiviert haben und die Einstellung „Einbruchsalarm nur einmalig auslösen“ gesetzt ist, so haben Sie über den Tab „Einbrüche“ die Möglichkeit zu sehen, welche Adressen bereits einen Einbruchsalarm ausgelöst haben:



Auch hier steht Ihnen der Tool-Tip bei den Adressen zur Verfügung, der den ersten und letzten Kommunikationszeitpunkt (bzw. in diesem Fall den Zeitpunkt des ersten und letzten Einbruchs) anzeigt.

Möchten Sie, dass eine Adresse temporär kein Alarm auslöst, dann können Sie diese über die oberste Zeile und das ┼-Symbol hinzufügen.

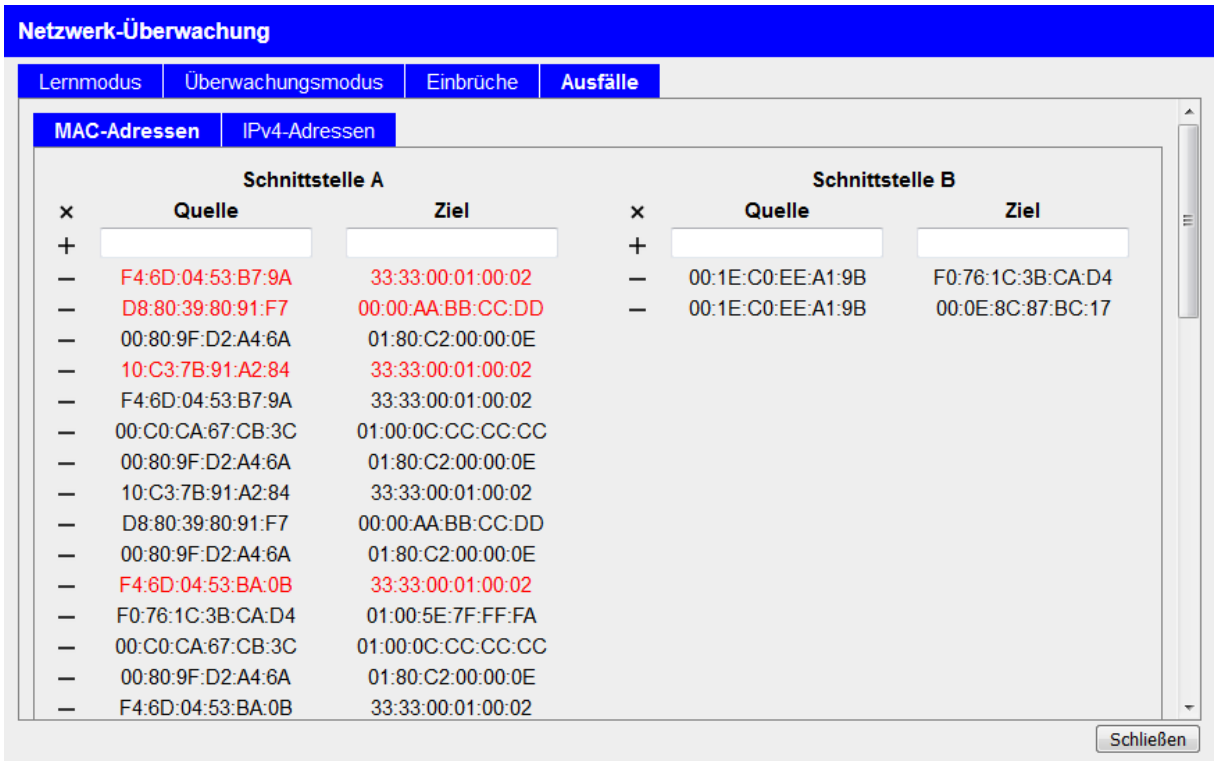
Soll für eine Adresse aus der Liste, erneut ein Alarm ausgelöst werden, so können Sie den jeweiligen Eintrag mit dem ─-Symbol entfernen.

Möchten Sie die Liste mit Einbrüchen komplett zurücksetzen, so können Sie auch hier wieder das ✕-Symbol verwenden.

Hinweis:
Die Überwachung läuft automatisch im Gerät. Die Liste erweitert sich also auch, wenn Sie nicht über die Webseite beobachten.

Wichtig:
Die Liste mit Einbrüchen wird nach einen Neustart zurückgesetzt.

Sofern Sie die Ausfallüberwachung aktiviert haben, können Sie sich im Tab „Ausfälle“ eine Art Log anschauen, welches alle Ausfälle seit Beginn der Überwachung aufführt:



In der Tabelle steht der neuste Ausfall ganz oben. Adressen die seit dem Ausfall nicht wiedergekehrt sind, sind rot markiert, die anderen hingegen schwarz. Um den Zeitpunkt bzw. Zeitraum des Ausfalls zu sehen, müssen Sie lediglich mit der Maus auf den Eintrag fahren. Die Informationen werden dann als Tool-Tip angezeigt.

Das Hinzufügen in das und Löschen von Einträgen aus dem Ausfall-Log mit Hilfe der Icons + und – ist zwar möglich, hat aber keinerlei Auswirkung auf die Ausfallüberwachung an sich.

Das komplette Ausfall-Log kann mit Hilfe des Icons ✕ zurückgesetzt werden.

Hinweis:
Die Überwachung läuft automatisch im Gerät. Die Liste erweitert sich also auch, wenn Sie nicht über die Webseite beobachten.

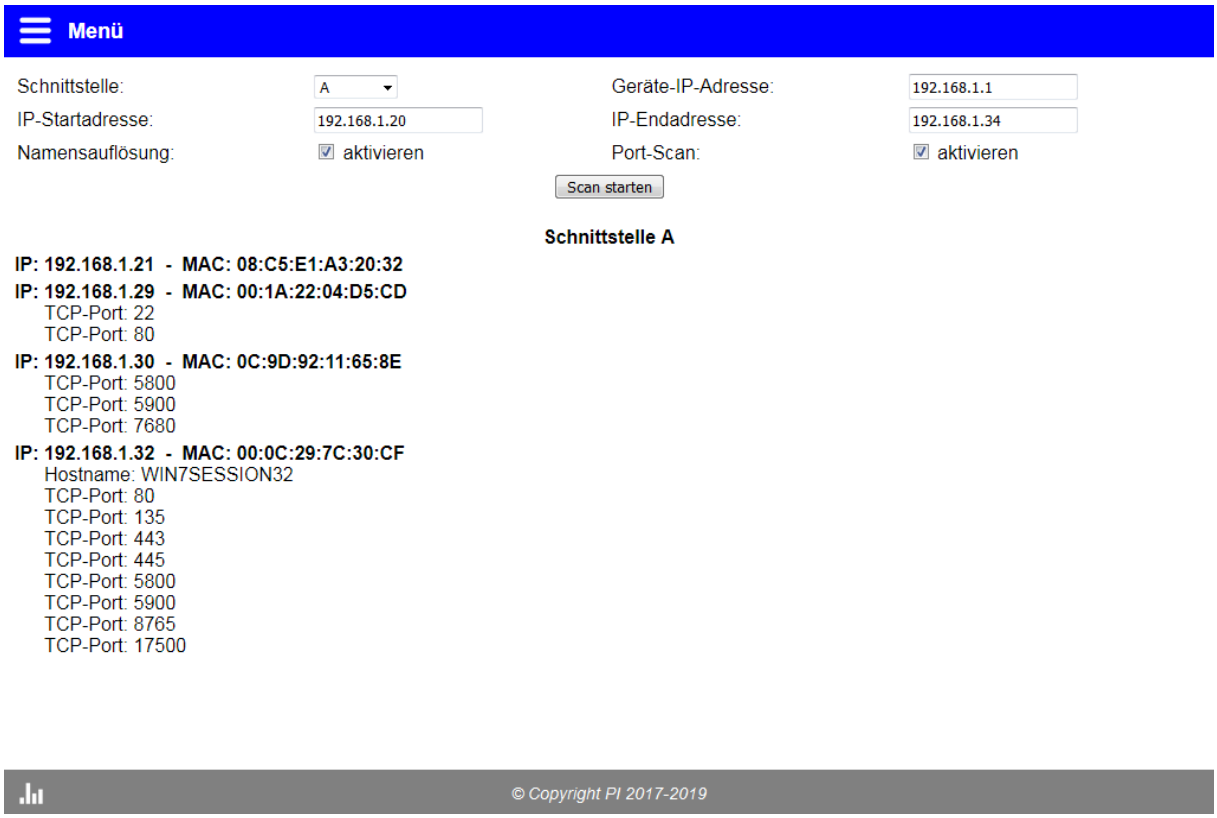
Wichtig:
Die Liste mit Ausfällen wird nach einen Neustart zurückgesetzt.

Wie bereits erwähnt, kann die Netzwerk-Überwachung Einbrüche und Ausfälle auch per E-Mail senden. Hierfür muss auf der Konfigurationsseite ein SMTP-Server konfiguriert sowie die Einstellung „Überwachung aktivieren“ gesetzt sein *(siehe Kapitel Webserver → Konfiguration → SMTP-Einstellungen)*.

Der E-Mail-Versand läuft parallel zur Analyse und Überwachung die Sie im Webbrowser durchführen können. Es ist daher möglich, dass Sie eine Überwachungs-Aufzeichnung im Webbrowser durchführen und gleichzeitig über Einbrüche und Ausfälle per E-Mail informiert werden.

Wichtig:
Bitte beachten Sie, dass je nach Konfiguration für jeden Einbruch und Ausfall eine E-Mail verschickt wird. Dies kann zu einer enormen Anzahl an E-Mails führen. Prüfen Sie Ihre Einstellungen daher sorgfältig, bevor Sie den E-Mail-Versand aktivieren.

4.4 Seite Netzwerk-Scan



Mit Hilfe der Seite „Netzwerk-Scan“ haben Sie die Möglichkeit einen Netzwerk-Scan auszuführen, um somit festzustellen, welche Geräte sich in Ihrem Netzwerk befinden.

Bevor Sie den Scan starten können, müssen Sie diesen konfigurieren. Hierfür stehen Ihnen ein paar Einstellungsmöglichkeiten zur Verfügung:

Schnittstelle:	Die Schnittstelle, auf welcher der Scan ausgeführt werden soll. Es ist auch möglich, den Scan auf Schnittstelle A und B gleichzeitig auszuführen.
Geräte-IP-Adresse:	Die IP-Adresse, welche während dem Scan durch das Gerät verwendet werden soll.
IP-Startadresse:	Die erste IP-Adresse des zu scannenden IP-Bereichs.
IP-Endadresse:	Die letzte IP-Adresse des zu scannenden IP-Bereichs.
Namensauflösung:	Gibt an, ob versucht werden soll, den Namen der gefundenen IP-Adressen zu ermitteln.

Port-Scan: Gibt an, ob die TCP-Ports der gefunden IP-Adressen überprüft werden sollen.

Wichtig:
Bitte stellen Sie sicher, dass es sich bei der gewählten Geräte-IP-Adresse um eine freie IP-Adresse oder die IP-Adresse des Geräts (für den Webserver) handelt. Andernfalls kommt es zu einem IP-Konflikt.

Haben Sie alle Einstellungen vorgenommen, so müssen Sie nur noch auf den Button „Scan starten“ klicken. Die Dauer des Scan-Vorgangs ist abhängig von dem zu scannenden IP-Bereich und den aktivierten Optionen. Der Scan kann jedoch auf jeden Fall mehrere Minuten dauern.

Sobald der Scan läuft, können Sie diesen jeder Zeit mit Hilfe des Buttons „Scan stoppen“ abbrechen. Andernfalls wird der Scan automatisch beendet, sobald das Suchen nach Geräten abgeschlossen ist.

Der Netzwerk-Scan verläuft in 3 grundlegenden Schritten:

1. Zuerst wird versucht zu ermitteln, welche Geräte, des angegebenen Bereichs, sich im Netz befinden. Wurde ein Gerät gefunden, so wird es auf der Webseite angezeigt.
2. Anschließend wird, falls die Namensauflösung aktiviert ist, versucht, den Hostnamen der in Schritt 1 gefundenen Geräten zu ermitteln.
3. Im letzten Schritt werden, falls der Port-Scan aktiviert ist, alle TCP-Ports (Port 1-65535) auf Ihre Erreichbarkeit geprüft. Auch diese Information wird dann auf der Website dargestellt.

Hinweis:
Bitte beachten Sie, dass Geräte, welche sich in einem anderen Subnetz wie die Scan-IP-Adresse des Geräts befinden, im ersten Schritt zwar gefunden werden, die Namensauflösung und der Port-Scan dieser Geräte jedoch fehlschlägt.
Des Weiteren ist zu beachten, dass nur Geräte gefunden werden können, die sich im gleichen physikalischen Netzwerk befinden.

Ist der Netzwerk-Scan abgeschlossen, so können Sie das Ergebnis des Scans mit Hilfe des Buttons „Ergebnis sortieren“ noch nach IP-Adressen und Port-Nummern sortieren lassen. Die unsortierte Reihenfolge stellt die Reihenfolge dar, in welcher die Informationen ermittelt wurden.

Hinweis:
Der Netzwerk-Scan kann bei den ProfiNet-WATCHDOG-Geräten nicht verwendet werden.

4.5 Seite Netzwerk-Tools

Über die Seite „Netzwerk-Tools“ ist es möglich verschiedene Netzwerkbefehle wie Ping, Traceroute, „Wake On LAN“ und Namensauflösungen durchzuführen.

Bevor Sie ein Netzwerk-Tool ausführen können, müssen Sie ein paar Einstellungen festlegen. Die benötigten Einstellungen variieren dabei von Tool zu Tool.

Über die Liste „Tool-Auswahl“ können Sie auswählen, welches Tool verwendet werden soll. Einstellungen, die für dieses Tool keine Bewandtnis haben, werden dadurch automatisch ausgeblendet.

Folgende Einstellungen sind für die lokale Adresse verfügbar:

Schnittstelle:	Die Schnittstelle, auf welchem das Tool ausgeführt werden soll. Es ist auch möglich, dass Tool auf beiden Schnittstellen gleichzeitig auszuführen.
IP-Adresse:	Die IP-Adresse des Geräts für das Tool.
Subnetzmaske:	Die Subnetzmaske des Geräts für das Tool.

Gateway:	Die IP-Adresse des Gateways des Geräts für das Tool.
DNS-Server:	Die IP-Adresse des DNS-Servers des Geräts für das Tool.

Wichtig:
Bitte stellen Sie sicher, dass es sich bei der gewählten IP-Adresse um eine freie IP-Adresse oder die IP-Adresse des Geräts (für den Webserver) handelt. Andernfalls kommt es zu einem IP-Konflikt.

Folgende Einstellungen sind für die Ziel-Adresse verfügbar:

MAC-Adresse:	Die MAC-Adresse des Ziel-Geräts.
IP-Adresse:	Die IP-Adresse des Ziel-Geräts.
Port:	Der Port für das Ziel-Gerät.

Folgende sonstige Einstellungen sind verfügbar:

Hostname:	Der Hostname, welcher aufgelöst werden soll.
SecureOn-Passwort:	Das Passwort, welches bei „Wake On LAN“ verwendet werden kann.

Haben Sie alle Einstellungen vorgenommen, so können Sie das Netzwerk-Tool mit dem Button „Tool starten“ starten. Das Tool beendet sich, sobald es seinen Vorgang abgeschlossen hat, automatisch. Andernfalls können Sie es über den Button „Tool beenden“ auch jeder Zeit manuell stoppen.

Der Fortschritt sowie das Ergebnis des Tools wird im „Ausgabe-Fenster“ unterhalb der Button-Leiste angezeigt.

4.5.1 IP in MAC auflösen

Bei diesem Tool ist nur die Eingabe der lokalen IP-Adresse und Ziel-IP-Adresse notwendig. Mit Hilfe des ARP-Protokolls wird dann versucht die MAC-Adresse des Geräts mit der angegebenen Ziel-IP-Adresse zu ermitteln.

4.5.2 Ping

Das Tool „Ping“ ist ein beliebtes Tool zum Testen der Erreichbarkeit eines Netzwerk-Teilnehmers. Wie auch bei Windows, versendet das Analysegerät 4 Pings *(ICMP Echo-Anforderungen)*. Dieses Tool funktioniert auch über Routerübergange, sofern Sie ein Gateway eintragen.

4.5.3 Traceroute

Möchten Sie die Route zu einem Netzwerk-Teilnehmer verfolgen, so kann es nützlich sein, eine Routenverfolgung durchzuführen. Diese Aufgabe kann das Tool „Traceroute“ (auch bekannt als „tracert“) durchführen. Das Tool arbeitet dabei vergleichbar zu Windows und versendet pro Abschnitt 3 Pings. Die Routenverfolgung läuft maximal über 32 Abschnitte.

4.5.4 NetBIOS-Namen auflösen

Um die IP-Adresse, eines NetBIOS-Namens herauszufinden, können Sie das Tool „NetBIOS-Namen auflösen“ verwenden. Das Tool versendet eine NetBIOS-Anfrage mit dem eingegebenen Hostnamen an die Broadcast-Adresse des lokalen Subnetzes. Die Auflösung von NetBIOS-Namen ist auf das physikalische und logische Netzwerk begrenzt.

4.5.5 NetBIOS-Namen ermitteln

Das Tool „NetBIOS-Namen ermitteln“ ist das Gegenstück zu „NetBIOS-Namen auflösen“. Im Gegensatz zu dem Tool „NetBIOS-Namen auflösen“ ist bei dem Tool „NetBIOS-Namen ermitteln“ die Eingabe der IP-Adresse notwendig. Als Ergebnis erhalten Sie dann den NetBIOS-Namen des Geräts.

4.5.6 LLMNR-Namen auflösen

Das Tool „LLMNR-Namen auflösen“ ist ein Tool, um den Hostnamen von Geräten im lokalen Netzwerk zu ermitteln und somit vergleichbar mit dem Tool „NetBIOS-Namen auflösen“. Einige Netzwerk-Teilnehmer, insbesondere Windows, reagieren sowohl auf NetBIOS- als auch auf LLMNR-Anfragen.

4.5.7 LLMNR-Namen ermitteln

Wie bei dem Tool zum Auflösen von NetBIOS-Namen, gibt es auch bei dem Tool zum Auflösen von LLMNR-Namen ein Gegenstück, welches als Eingabe eine IP-Adresse erwartet und den dazugehörigen Hostnamen des Geräts ermittelt. Dieses Tool finden Sie in der Auswahl über „LLMNR-Namen ermitteln“.

4.5.8 DNS-Namen auflösen

Mit dem Tool „DNS-Namen auflösen“ haben Sie die Möglichkeit, einen DNS-Namen in seine IP-Adresse aufzulösen. Bei den Einstellungen muss beachtet werden, dass noch zusätzlich der DNS-Server angegeben werden muss. Als Ergebnis erhalten Sie neben der IP-Adresse des angegebenen DNS-Namens i. d. R. auch noch Informationen zu den Namensservern, zu welchem der DNS-Name angehört. Im Gegensatz zur Auflösung von NetBIOS- und LLMNR-Namen funktioniert die Auflösung von DNS-Namen auch über Routerübergänge hinaus.

4.5.9 DNS-Namen ermitteln

In einigen Situationen kann es auch nützlich sein, den DNS-Namen einer gegebenen IP-Adresse zu ermitteln. Für diesen Fall gibt es das Tool „DNS-Namen ermitteln“. Hierbei muss lediglich die IP-Adresse des angegeben werden. Als Ergebnis erhalten Sie dann den DNS-Namen des jeweiligen Geräts.

4.5.10 Wake On LAN - MAC

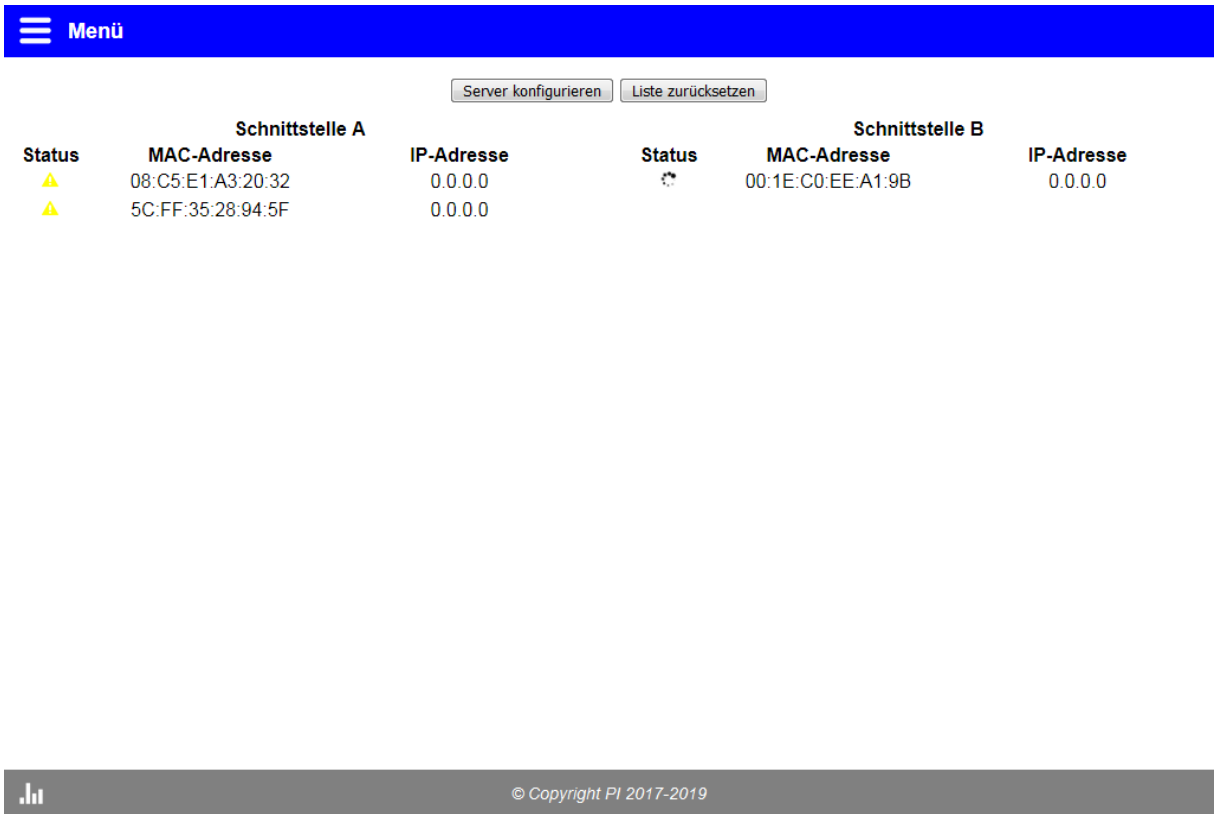
Um ein Gerät über Netzwerk aus der Ferne aufzuwecken bzw. zu starten, wird das „Magic Packet“ des „Wake On LAN“-Protokolls verwendet. Dieses lässt sich mit Hilfe dieses Tools versenden. Als Eingabe ist lediglich die MAC-Adresse des aufzuweckenden Geräts notwendig. Ist das Gerät mit einem SecureOn-Passwort geschützt, so müssen Sie dieses ebenfalls angegeben (in Form einer IP- oder MAC-Adresse). Eine Rückmeldung, ob das Gerät aufgeweckt wurde, ist im Protokoll nicht vorgesehen und kann somit nicht erfolgen.

4.5.11 Wake On LAN - IP

Das Tool „Wake On LAN - IP“ arbeitet ähnlich wie das Tool „Wake On LAN - MAC“, jedoch wird das „Magic Packet“ hier nicht direkt über Ethernet, sondern über das UDP-Protokoll versendet. Deshalb ist noch zusätzlich die Angabe der lokalen IP-Adresse sowie des Ziel-Ports erforderlich. Die Ziel-IP muss nicht angegeben werden, da das Paket an die Broadcast-Adresse versendet wird. Standardports für „Wake On LAN“ sind 0, 7 und 9.

Hinweis:
Die Netzwerk-Tools können bei den ProfiNet-WATCHDOG-Geräten nicht verwendet werden.

4.6 Seite DHCP-Clients



Auf der Seite „DHCP-Clients“ sehen Sie alle DHCP-Clients, die sich in Ihrem Netzwerk befinden. Des Weiteren haben Sie die Möglichkeit einzelnen Geräten eine IP-Adresse zuzuweisen.

In der Tabelle wird dabei für jeden DHCP-Client die MAC- und IP-Adresse angezeigt. Hat der DHCP-Client noch keine IP-Adresse erhalten, so ist diese im Regelfall 0.0.0.0. In der ersten Spalten sehen Sie den Status des jeweiligen DHCP-Clients, der über ein Icon beschrieben wird:

- DHCP-Client such nach Servern
- ⚠ DHCP-Client fragt eine IP-Adresse an / DHCP-Client wurde eine IP-Adresse angeboten
- ⚠ DHCP-Client oder -Server hat die IP-Adresse abgelehnt
- ✓ DHCP-Client wurde eine IP-Adresse zugewiesen

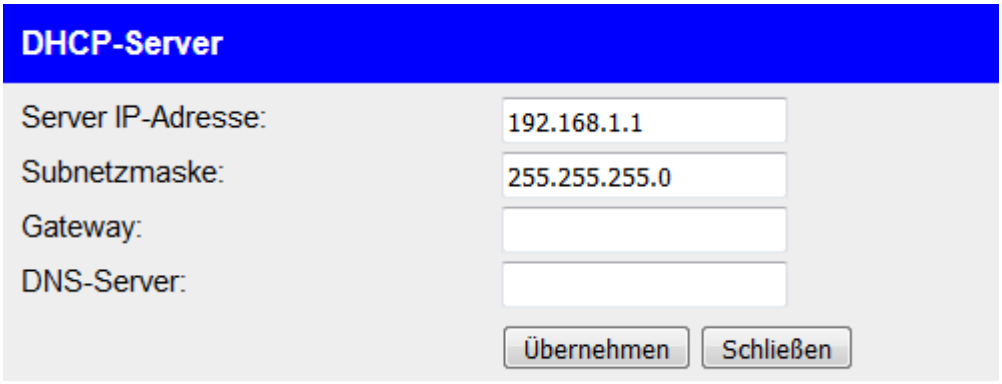
Möchten Sie weitere Informationen zu einem DHCP-Client anzeigen, so müssen Sie lediglich auf einen Eintrag in der Tabelle klicken. Daraufhin erscheint dann folgendes Fenster:

Dort sehen Sie nun z. B. den oben beschriebenen Status in Textform, die Link-Local IP-Adresse (sofern sich das Gerät selber eine IP-Adresse zuweist) und Informationen über das DHCP-Lease (falls das Gerät eine IP-Adresse von einem Server erhalten hat).

Des Weiteren haben Sie hier die Möglichkeit, dem Gerät eine IP-Adresse zuzuweisen. Hierfür müssen Sie lediglich den Hacken in dem Kontrollkästchen setzen und eine IP-Adresse in das Textfeld eintragen. Zum Schluss müssen Sie nur noch auf das Symbol klicken um die Eingabe zu übernehmen (dies ist auch notwendig, falls Sie die Zuweisung wieder zurücknehmen oder ändern möchten).

Wichtig:
Bitte beachten Sie, dass es sich bei der IP-Adresse, welche Sie einem Gerät zuweisen um eine freie IP-Adresse handeln muss, da es andernfalls zu einem IP-Konflikt kommt.
Des Weiteren müssen Sie beachten, dass sich die IP-Adresse, welche Sie einem Gerät zuweisen, im gleichen Subnetz wie die IP-Adresse des Servers befinden muss.

Bevor Sie jedoch eine IP-Zuweisung durchführen können, müssen Sie den DHCP-Server konfigurieren. Klicken Sie hierzu auf der Seite oben auf den Button „Server konfigurieren“. Es sollte nun folgendes Fenster zu sehen sein:



Hier haben Sie nun die Möglichkeit, die IP-Adresse für den DHCP-Server des Geräts festzulegen. Die Angaben zum Gateway und DNS-Server sind optional. Die Einstellungen sind automatisch (falls möglich) mit der IP-Adresse des Geräts vorbelegt. Um die Einstellungen zu übernehmen, müssen Sie auf den Button „Übernehmen“ klicken.

Den DHCP-Server den Sie hier konfigurieren können, hat jedoch nichts mit dem DHCP-Server zu tun, welchen Sie auf der Konfigurationsseite aktivieren können. Der DHCP-Server den Sie auf der Seite „DHCP-Clients“ definieren, verteilt auch nicht automatisch IP-Adressen an Geräte in Ihrem Netzwerk, sondern nur an die Geräte, bei welchen Sie eine manuelle Zuweisung durchführen.

Wichtig:
Bitte stellen Sie sicher, dass es sich bei der gewählten IP-Adresse um eine freie IP-Adresse oder die IP-Adresse des Geräts (für den Webserver) handelt. Andernfalls kommt es zu einem IP-Konflikt.

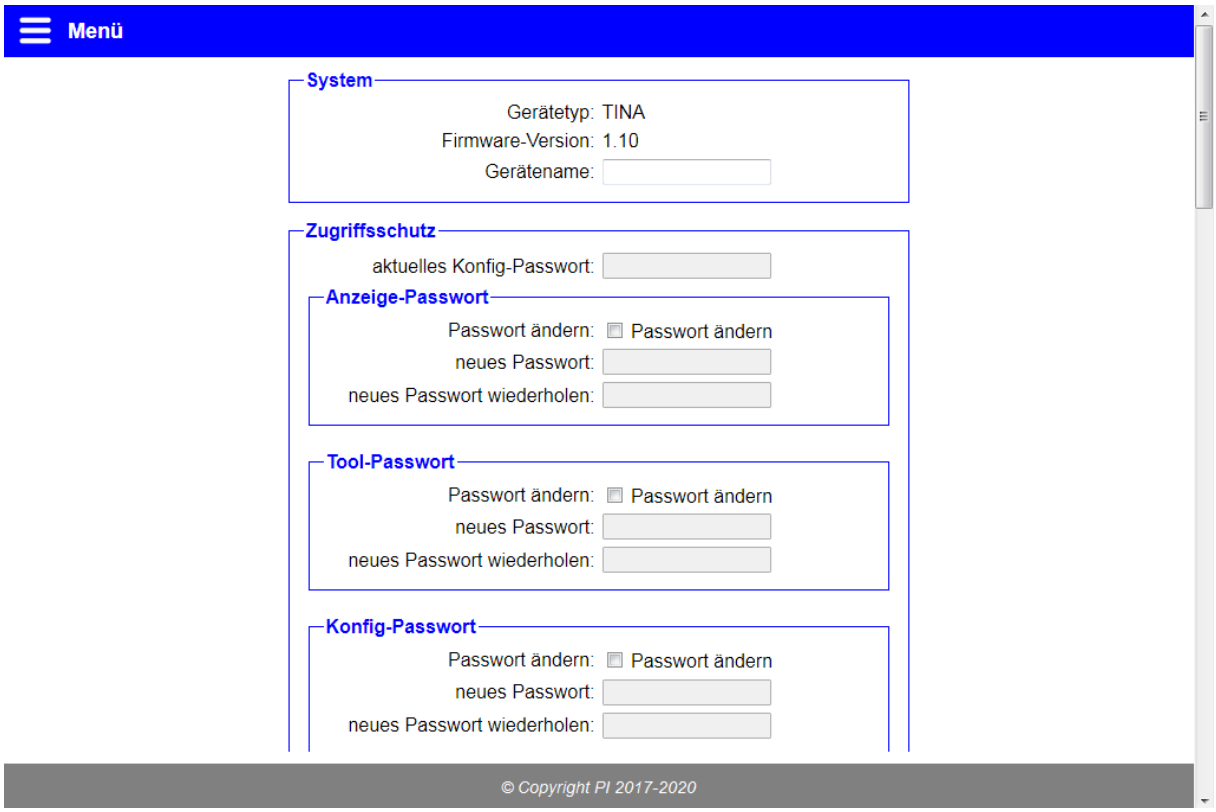
Wurde einem Gerät eine IP-Adresse zugewiesen (unabhängig, ob dies von einem anderen DHCP-Server oder dem DHCP-Server des Geräts durchgeführt wurde), so sehen Sie in der Detailanzeige eines DHCP-Clients nun auch die zugeteilten Parameter sowie die Gültigkeit des DHCP-Leases:

Hinweis:
Falls Sie in der Konfiguration auf einer der Schnittstellen bereits einen DHCP-Server aktiviert haben, so ist die Zuweisung von IP-Adressen für Geräte auf dieser Schnittstelle über die Seite „DHCP-Clients“ nicht mehr möglich.

Möchten Sie die Liste mit DHCP-Clients (und somit auch deren DHCP-Leases) zurücksetzen, so müssen Sie lediglich auf den Button „Liste zurücksetzen“ klicken.

Hinweis:
Die Zuweisung von IP-Adressen mit Hilfe dieser Seite kann bei den ProfiNet-WATCHDOG-Geräten nicht verwendet werden. Zur reinen Überwachung kann die Seite aber weiterhin verwendet werden.

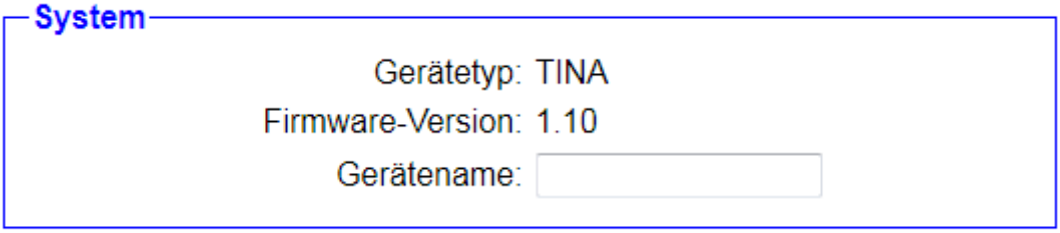
4.7 Seite Konfiguration



Auf der Konfigurationsseite (Menüpunkt „Konfiguration“) haben Sie die Möglichkeit, diverse Einstellungen vorzunehmen, um somit Ihr Gerät nach Belieben anzupassen. Die Konfigurationsmöglichkeiten werden in der folgenden Punkten noch genauer erklärt.

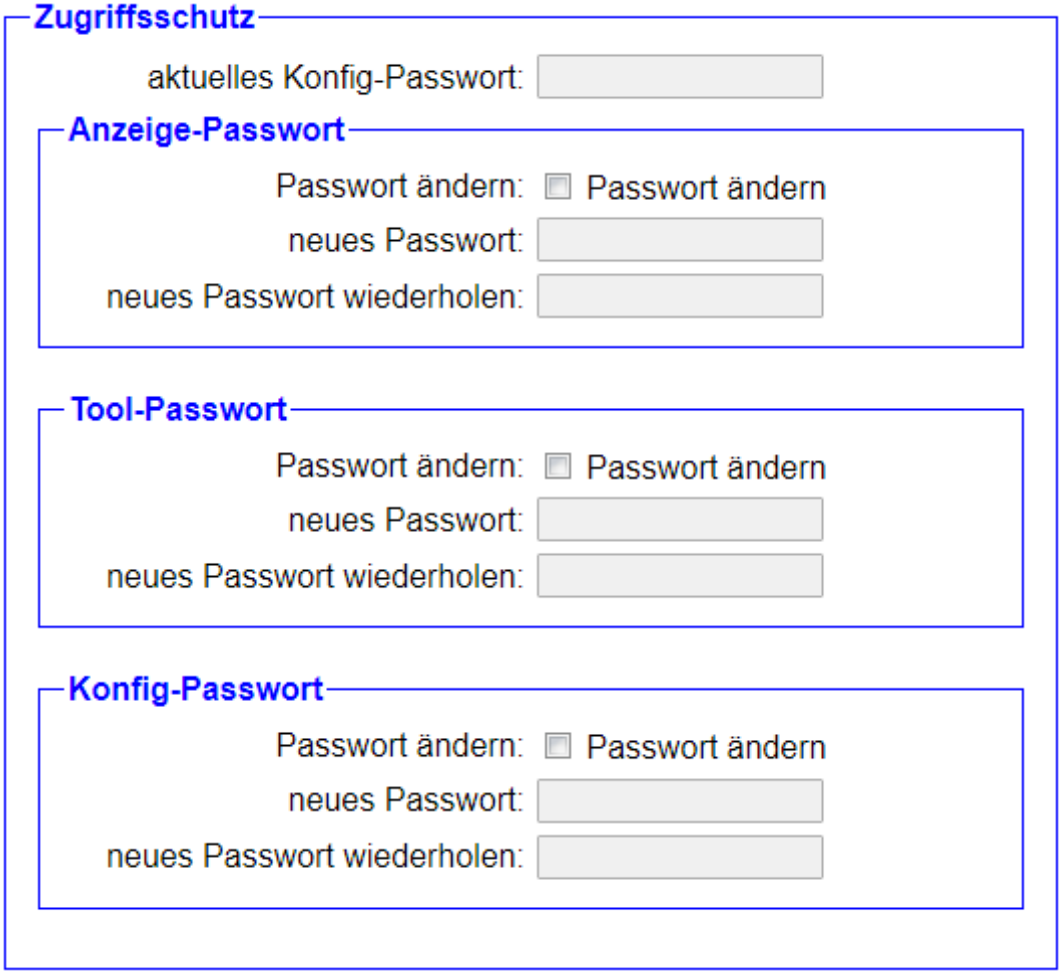
Falls Sie bei einer der Netzwerkschnittstellen DHCP-Client gewählt haben, so können Sie hier sehen, ob das Gerät bereits eine IP-Konfiguration erhalten hat und welche dies ist. Des Weiteren sehen Sie auf dieser Seite auch die MAC-Adressen der einzelnen Schnittstellen.

4.7.1 System



Der Bereich „System“ dient hauptsächlich zur Anzeige von allgemeinen Informationen über das Gerät. So wird Ihnen hier der Typ Ihres Geräts (***TINA***, ProfiNet-WATCHDOG oder ***TINA-II***) sowie die im Gerät laufende Firmware-Version angezeigt. Das Hochladen einer neuen Firmware ist über die Seite „Firmware-Update“ möglich. Über das Feld „Gerätename“ haben Sie zudem die Möglichkeit, dem Gerät einen Namen zu geben, der dann auf der Weboberfläche angezeigt wird.

4.7.2 Zugriffsschutz



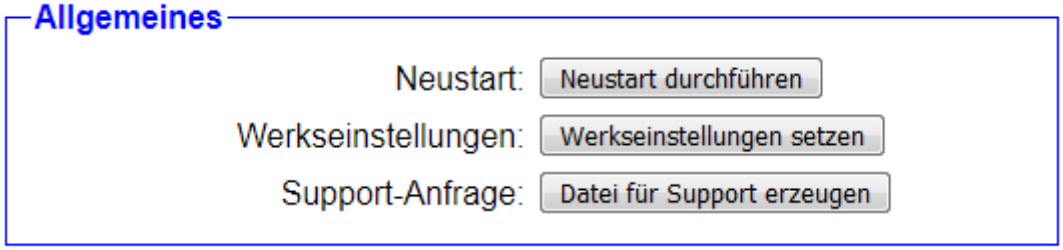
Im Bereich „Zugriffsschutz“ können Sie die Passwörter festlegen, welche für den Zugriff auf die Webseiten Ihres Analyzers notwendig sind. Wird ein leeres Passwort definiert, so kann die jeweilige Seite direkt und ohne Bestätigung eines Passworts aufgerufen werden. Das Gerät bietet Ihnen die Möglichkeit drei unterschiedliche Passwörter festzulegen. Bei Bedarf können Sie ein Passwort auch für mehrere Zugriffsarten vergeben. Folgende Passwörter können vergeben werden:

- **Anzeige-Passwort:** Dieses Passwort wird für den Zugriff auf die Seite „Übersicht“ und somit zur Analyse und Steuerung des Netzwerkverkehrs benötigt.
- **Tool-Passwort:** Dieses Passwort wird benötigt, um auf die Seiten „Netzwerk-Scan“, „Netzwerk-Tools“ und „DHCP-Clients“ zugreifen zu können.
- **Konfig-Passwort:** Mit diesem Passwort haben Sie Zugriff auf die Seiten „Konfiguration“ und „Firmware-Update“. Wer dieses Passwort kennt, kann die anderen Passwörter ändern.

Um eines der oder mehrere Passwörter zu ändern, müssen Sie zunächst überall dort, für welche Zugriffsart Sie das Passwort ändern bzw. setzen möchten, das Kontrollkästchen „Passwort ändern“ angeklickt haben. Anschließend können Sie das neue Passwort eingeben. Zur Sicherheit muss dieses ein zweites mal eingegeben werden, um Tippfehler zu vermeiden. Bevor Sie die Konfiguration nun speichern können, müssen Sie im Feld „aktuelles Konfig-Passwort“ Ihr aktuell vergebenes Konfig-Passwort eingeben. Im Auslieferungszustand ist dies ein leeres Passwort.

Wichtig:
Im Werkszustand ist bei alle Zugriffsarten ein leeres Passwort definiert. Dies sollten Sie unbedingt ändern, um unerlaubte Einsicht in Ihren Netzwerkverkehr sowie unerwünschte Änderungen der Konfiguration an Ihrem Gerät zu vermeiden.

4.7.3 Allgemeines

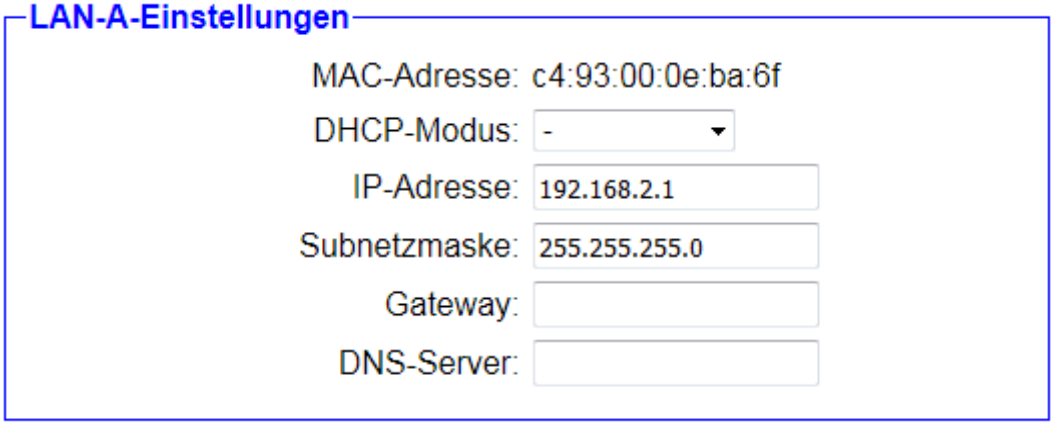


Der Bereich „Allgemeines“ ermöglicht Ihnen das Neustarten Ihres Geräts sowie das Zurücksetzen aller Einstellungen auf den Werkszustand. Hierfür müssen Sie lediglich auf den jeweiligen Button klicken.

Des Weiteren haben Sie mit dem Button „Datei für Support erzeugen“ die Möglichkeit eine .bin-Datei zu erzeugen, die die Konfiguration und den Status des Geräts enthält. Diese Informationen können für den Support hilfreich sein, falls Sie Fragen oder Probleme haben.

Wichtig:
Durch das Auslösen von Werkseinstellungen gehen alle Einstellungen, die Sie am Gerät vorgenommen haben verloren. Auch die Funktionsfreigabe muss erneut erfolgen. Lesen Sie hierzu bitte das Kapitel „Inbetriebnahme“.

4.7.4 LAN-A-Einstellungen



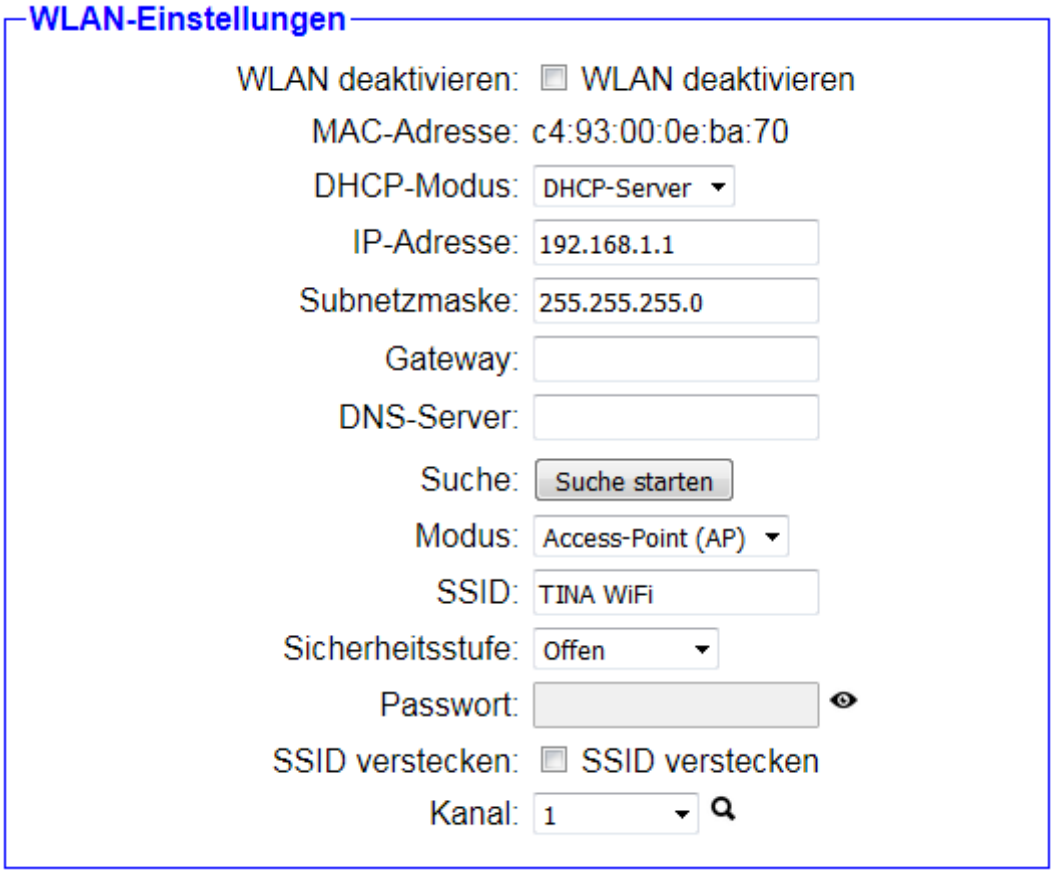
Die Einstellungen in der Gruppe „LAN-A-Einstellungen“ betreffen die Netzwerk-Anbindung des Geräts für die LAN-A-Schnittstelle:

MAC-Adresse:	Die MAC-Adresse der Schnittstelle (diese kann nicht verändert werden).	
DHCP-Modus:	-	Das Gerät ist über die eingestellte Adresse erreichbar.
	Client	Das Gerät bezieht eine IP-Adresse von einem DHCP-Server.
	Server	Das Gerät ist über die eingestellte Adresse erreichbar und stellt anderen Geräten IP-Adressen zur Verfügung.
IP-Adresse:	Die IP-Adresse des Geräts.	
Subnetzmaske:	Die Subnetzmaske des Geräts.	
Gateway:	Die IP-Adresse des Gateways (optional).	
DNS-Server:	Die IP-Adresse des DNS-Servers (optional).	

Hinweis:
Soll der Webservers Ihres Geräts über die LAN-A-Schnittstelle nicht erreichbar sein, so stellen Sie den DHCP-Modus einfach auf den Modus „-“ und entfernen Sie die Eingaben aus den Feldern IP-Adresse und Subnetzmaske.

Wichtig:
ProfiNet-WATCHDOG-Geräte können grundsätzlich nicht über die LAN-A-Schnittstelle erreicht werden, um das RealTime-Verhalten nicht zu beeinflussen.

4.7.5 WLAN-Einstellungen



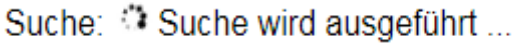
In der Gruppe „WLAN-Einstellungen“ kann die Konfiguration für die WLAN-Schnittstelle festgelegt werden:

WLAN deaktivieren:	Gibt an, ob die WLAN-Schnittstelle deaktiviert werden soll.	
MAC-Adresse:	Die MAC-Adresse der Schnittstelle (diese kann nicht verändert werden).	
DHCP-Modus:	-	Das Gerät ist über die eingestellte Adresse erreichbar.
	Client	Das Gerät bezieht eine IP-Adresse von einem DHCP-Server.

	Server	Das Gerät ist über die eingestellte Adresse erreichbar und stellt anderen Geräten IP-Adressen zur Verfügung.
IP-Adresse:	Die IP-Adresse des Geräts.	
Subnetzmaske:	Die Subnetzmaske des Geräts.	
Gateway:	Die IP-Adresse des Gateways (optional).	
DNS-Server:	Die IP-Adresse des DNS-Servers (optional).	
Modus:	Access-Point	Das Gerät stellt ein eigenes WLAN-Netzwerk zur Verfügung.
	Client	Das Gerät verbindet sich mit einem bestehenden WLAN-Netzwerk.
SSID:	Die SSID (Bezeichnung) des WLAN-Netzwerks.	
Sicherheitsstufe:	Die Sicherheitsstufe/Verschlüsselung des WLAN-Netzwerks.	
Passwort:	Das Passwort, welches zur Anmeldung am WLAN-Netzwerk notwendig ist.	
SSID verstecken:	Gibt an, ob die SSID versteckt werden soll (nur relevant, wenn der Modus Access-Point ist).	
Kanal:	Der Kanal des WLAN-Netzwerks. *(Autokanal = Bester WLAN-Kanal wird gewählt)*	

Sind Sie sich bei den WLAN-Einstellungen Ihres bestehenden WLAN-Netzwerkes nicht sicher, so haben Sie die Möglichkeit, nach bestehenden WLAN-Netzwerken zu suchen. Klicken Sie dazu einfach auf den Button „Suche starten“.

Es erscheint nun folgende Meldung:



Nach ein paar Sekunden wird Ihnen die Liste mit gefundenen WLAN-Netzwerken angezeigt:

BSSID	SSID	Sicherheit	Kanal	Signal
c4:93:00:09:34:bd	TINA WiFi	Offen	1	
00:1e:c0:1a:83:67	EtherSens WiFi	WEP	3	
c0:56:27:9d:98:db	Test-WLAN	WPA2	7	

Um nun die Einstellungen eines WLAN-Netzwerks zu übernehmen, müssen Sie lediglich auf einen Tabelleneintrag klicken. Es werden dann alle notwendigen Felder (Modus, SSID, Sicherheitsstufe und Kanal) vorausgefüllt. Das Passwort müssen Sie, falls vorhanden, natürlich noch selbst eingeben.

Falls Sie den Analyzer als Access-Point (AP) konfigurieren möchten, kann es nützlich sein, herauszufinden, welcher WLAN-Kanal aktuell am wenigsten belastet ist. Hierfür haben Sie die Möglichkeit sich eine Kanalauslastung anzeigen zu lassen. Klicken Sie hierzu einfach auf das 🔍-Symbol hinter der Auswahlliste für den Kanal.

Sobald Sie auf das Symbol geklickt haben, erscheint an Stelle der Lupe eine Ladesymbol. Nach wenigen Sekunden, sollten Ihnen nun die Kanalauslastung angezeigt werden. Dies sieht dann z. B. wie folgt aus:

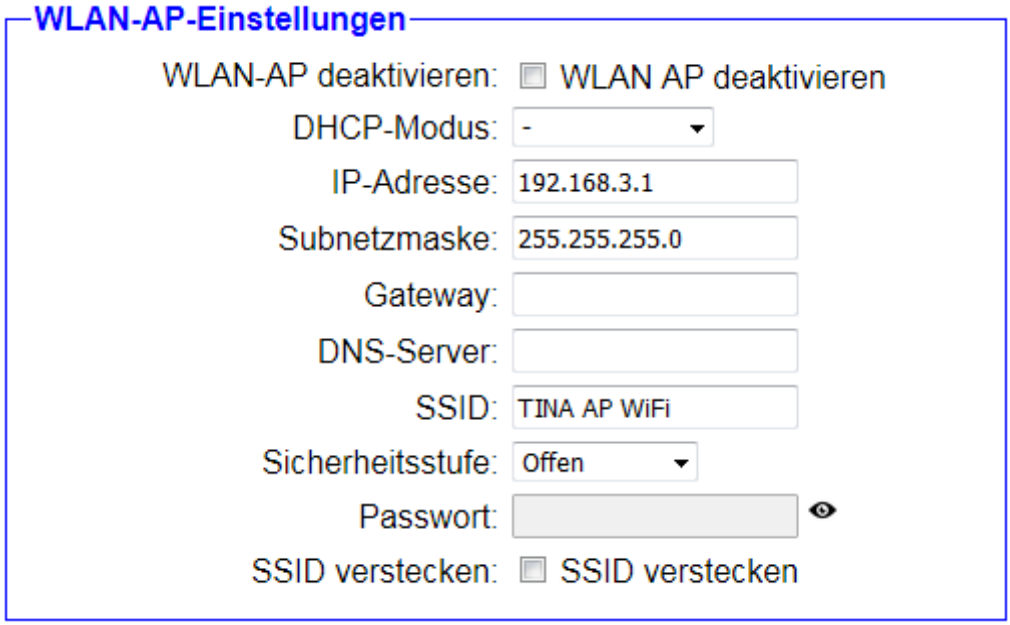
Kanal-Auslastung

Kanal	SSID	Signal
1	TINA WiFi Service	-53 dBm
3	EtherSens WiFi	-82 dBm
3	Test-AP	-56 dBm
7	Test-WLAN	-47 dBm

Hinweis:
Soll der Webserver Ihres Geräts über die WLAN-Schnittstelle nicht erreichbar sein, so stellen Sie den DHCP-Modus einfach auf den Modus „-“ und entfernen Sie die Eingaben aus den Feldern IP-Adresse und Subnetzmaske.

Die WLAN-Schnittstelle kann nur dann deaktiviert werden, wenn als Betriebsmodus „LAN-LAN Bridge“ gewählt ist und eine andere Schnittstelle über eine IP-Adresse verfügt.

Falls Sie den Modus bei den WLAN-Einstellungen auf „Client“ eingestellt haben, so erscheint unterhalb der bereits beschriebenen Felder eine Untergruppe.



Die Einstellungen in dieser Gruppe erlauben es einen zusätzlichen Access-Point zu konfigurieren, d. h. Sie können Ihre WLAN-Schnittstelle zur gleichen Zeit als Client und Access-Point betrieben. Hierzu sind folgende Parameter verfügbar:

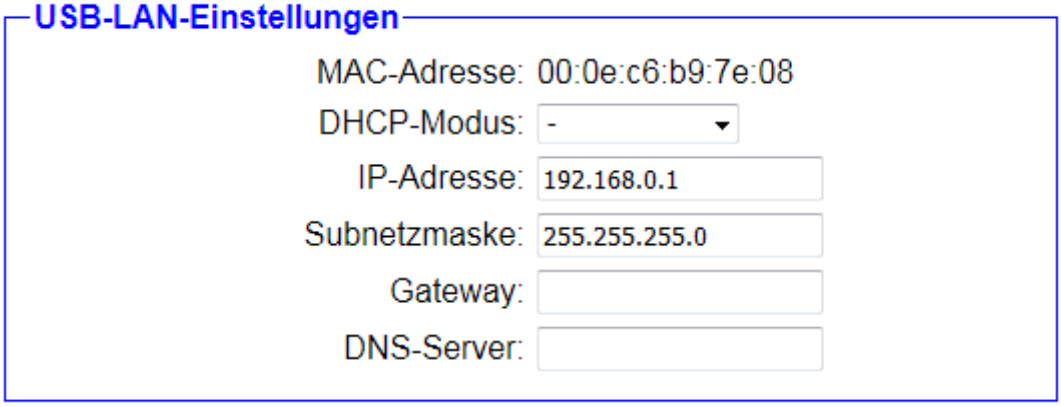
WLAN-AP deaktivieren:	Gibt an, ob die WLAN-AP-Schnittstelle deaktiviert werden soll.	
DHCP-Modus:	-	Das Gerät ist über die eingestellte Adresse erreichbar.
	Client	Das Gerät bezieht eine IP-Adresse von einem DHCP-Server.
	Server	Das Gerät ist über die eingestellte Adresse erreichbar und stellt anderen Geräten IP-Adressen zur Verfügung.
IP-Adresse:	Die IP-Adresse des Geräts.	

Subnetzmaske:	Die Subnetzmaske des Geräts.
Gateway:	Die IP-Adresse des Gateways (optional).
DNS-Server:	Die IP-Adresse des DNS-Servers (optional).
SSID:	Die SSID (Bezeichnung) des WLAN-Netzwerks.
Sicherheitsstufe :	Die Sicherheitsstufe/Verschlüsselung des WLAN-Netzwerks.
Passwort:	Das Passwort, welches zur Anmeldung am WLAN-Netzwerk notwendig ist.
SSID verstecken:	Gibt an, ob die SSID versteckt werden soll.

Hinweis:
Soll der Webserver Ihres Geräts über die WLAN-AP-Schnittstelle nicht erreichbar sein, so stellen Sie den DHCP-Modus einfach auf den Modus „-“ und entfernen Sie die Eingaben aus den Feldern IP-Adresse und Subnetzmaske.
Die WLAN-AP-Schnittstelle kann nur dann deaktiviert werden, wenn als Betriebsmodus nicht „WLAN-WLAN Bridge“ gewählt ist und eine andere Schnittstelle über eine IP-Adresse verfügt.

Wichtig:
Wenn das WLAN-Netzwerk, mit welchem Sie Ihren Analyzer verbunden haben, nicht erreichbar ist, so ist auch die WLAN-AP-Schnittstelle nicht mehr erreichbar.

4.7.6 USB-LAN-Einstellungen

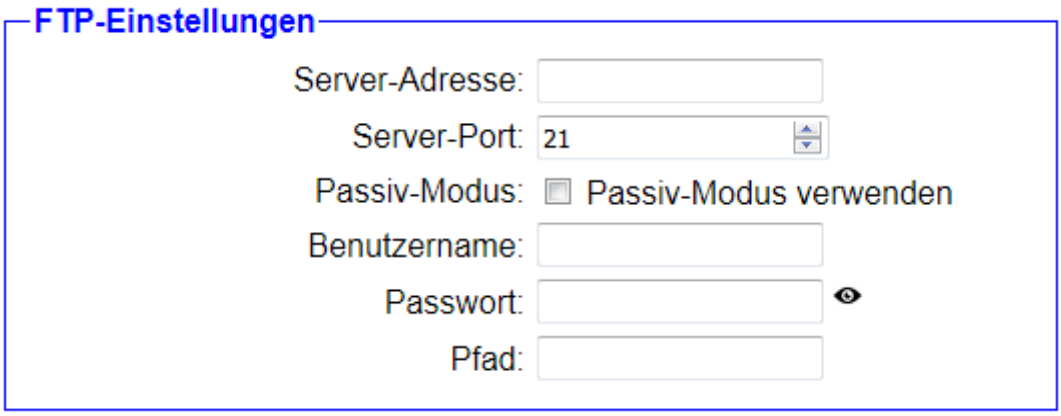


Die Einstellungen in der Gruppe „USB-LAN-Einstellungen“ betreffen die Netzwerk-Anbindung des Geräts für die LAN-Schnittstelle des „Ethernet über USB“-Adapters:

MAC-Adresse:	Die MAC-Adresse der Schnittstelle (diese kann nicht verändert werden).	
DHCP-Modus:	-	Das Gerät ist über die eingestellte Adresse erreichbar.
	Client	Das Gerät bezieht eine IP-Adresse von einem DHCP-Server.
	Server	Das Gerät ist über die eingestellte Adresse erreichbar und stellt anderen Geräten IP-Adressen zur Verfügung.
IP-Adresse:	Die IP-Adresse des Geräts.	
Subnetzmaske:	Die Subnetzmaske des Geräts.	
Gateway:	Die IP-Adresse des Gateways (optional).	
DNS-Server:	Die IP-Adresse des DNS-Servers (optional).	

Hinweis:
Bitte beachten Sie, dass dieser Block nur angezeigt wird, wenn aktuell ein USB-Adapter am Gerät angeschlossen ist.
Soll der Webservers Ihres Geräts über die USB-LAN-Schnittstelle nicht erreichbar sein, so stellen Sie den DHCP-Modus einfach auf den Modus „-“ und entfernen Sie die Eingaben aus den Feldern IP-Adresse und Subnetzmaske.

4.7.7 FTP-Einstellungen

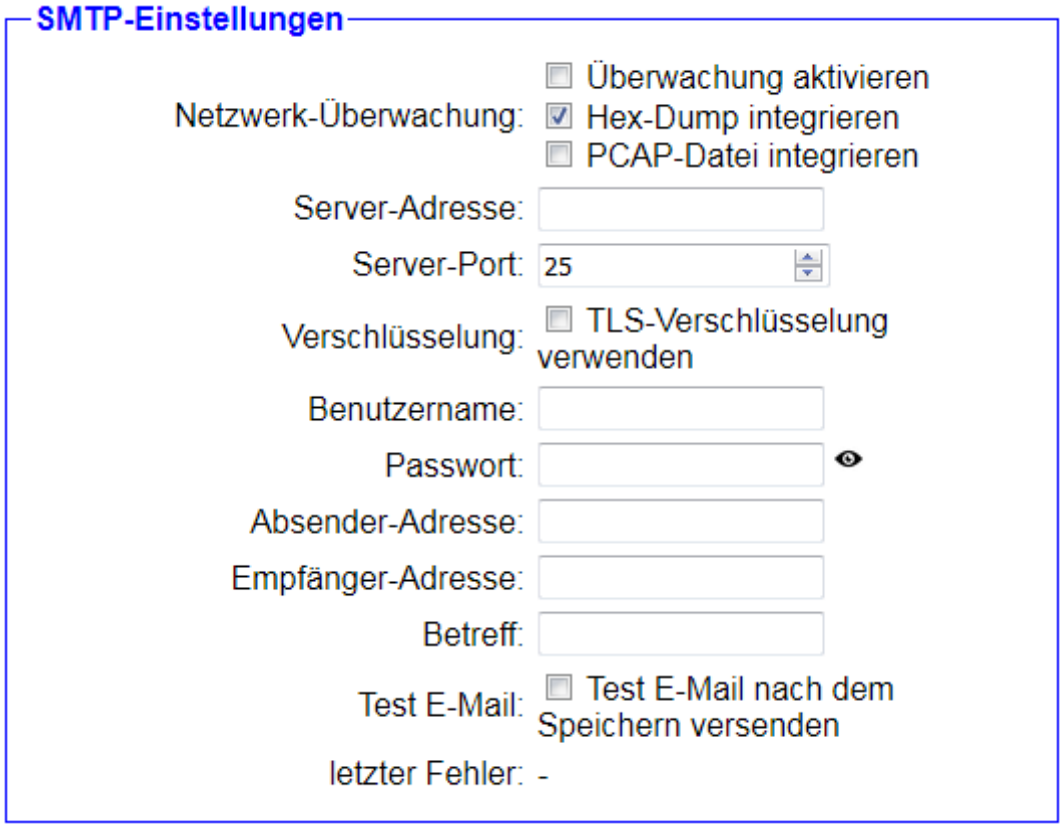


Folgende Einstellungen stehen für den FTP-Server zur Verfügung:

Server-Adresse:	Die IP-Adresse oder der DNS-Name des FTP-Servers.
Server-Port:	Der Port des FTP-Servers *(Standard ist 21)*.
Passiv-Modus:	Gibt an, ob der Passiv-Modus an Stelle des Aktiv-Modus *(immer Port 20 für Datenkommunikation)* verwendet werden soll.
Benutzername:	Der Benutzername, welcher zur Anmeldung am FTP-Server benötigt wird.
Passwort:	Das Passwort, welches zur Anmeldung am FTP-Server benötigt wird *(optional)*.
Pfad:	Der Pfad, in welchen der FTP-Client navigieren soll *(optional)*.

Hinweis:
Bitte beachten Sie, dass im Regelfall für eine Verbindung zu einem FTP-Server, der über das Internet erreichbar ist, der Passiv-Modus benötigt wird.

4.7.8 SMTP-Einstellungen

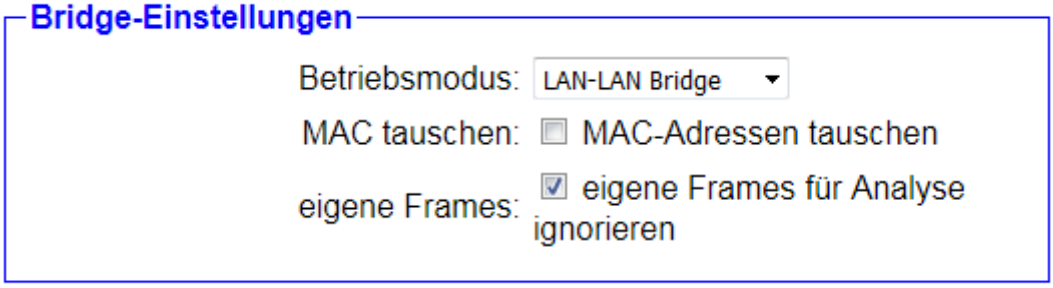


Folgende Einstellungen stehen für den SMTP-Server zur Verfügung:

Netzwerk-Überwachung:	Überwachung aktivieren *(aktivieren des Mail-Versands der Netzwerk-Überwachung)* Hex-Dump integrieren *(hängt bei Einbruchsmeldungen einen Hex-Dump des Frames an den Mail-Inhalt an)* PCAP-Datei integrieren *(hängt bei Einbruchsmeldungen eine .pcap-Datei des Frames an die Mail an)*
Server-Adresse:	Die IP-Adresse oder der DNS-Name des SMTP-Servers.
Server-Port:	Der Port des SMTP-Servers *(Standard ist 25 oder 465 mit TLS)*.
Verschlüsselung:	Gibt an, ob die Verbindung mit TLS verschlüsselt werden soll.
Benutzername:	Der Benutzername, welcher zur Anmeldung am SMTP-Server benötigt wird *(optional)*.

Passwort:	Das Passwort, welches zur Anmeldung am SMTP-Server benötigt wird *(optional)*.
Absender-Adresse:	Die E-Mail-Adresse, von welcher die E-Mails versendet werden sollen.
Empfänger-Adresse:	Die E-Mail-Adresse, an welche die E-Mails gesendet werden sollen.
Betreff:	Der Betreff, welcher in den E-Mails vor dem eigentlichen Betreff der E-Mail angehängt wird *(optional)*.
Test E-Mail:	Gibt an, ob nach dem Speichern der Einstellungen eine Test-E-Mail versendet werden soll.
letzter Fehler:	Zeigt den Fehler des letzten E-Mail-Versand an *(leer, falls kein Fehler aufgetreten ist)*.

4.7.9 Bridge-Einstellungen



Zur Konfiguration der Bridge stehen Ihnen noch die weiteren folgenden Einstellungen unter der Gruppe „Bridge-Einstellungen“ zur Verfügung:

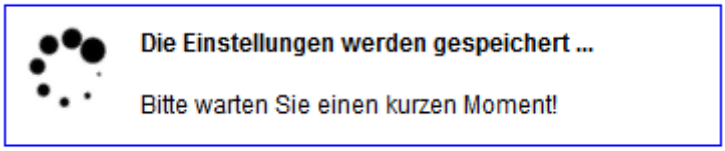
Betriebsmodus:	LAN-LAN-Bridge	Bridge zwischen LAN-A (A) und LAN-B (B)
	LAN-WLAN-Bridge	Bridge zwischen WLAN (A) und LAN-B (B)
	WLAN-WLAN-Bridge	Bridge zwischen WLAN-Client (A) und WLAN-AP (B)
MAC tauschen:	Gibt an, ob die MAC-Adressen auf der Schnittstelle A (LAN-A oder WLAN) durch die MAC-Adresse des Geräts ersetzt werden sollen.	

eigene Frames:	Gibt an, ob die „eigenen“ Frames *(Frames von und für das Gerät)* für die Analyse ignoriert werden sollen *(empfohlen)*.

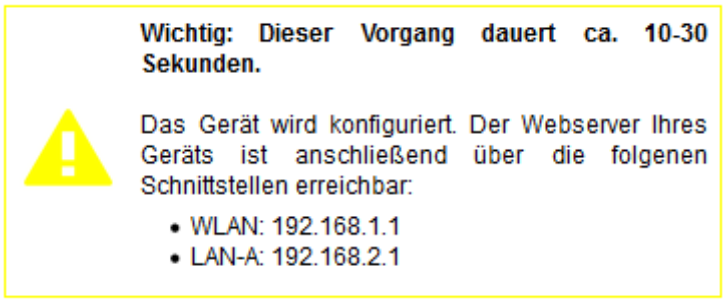
Hinweis:
Die Einstellung „MAC tauschen“ wird abhängig der Einstellungen „Modus“ (bei WLAN) und „Betriebsmodus“ automatisch gesetzt. Es ist jedoch auch möglich, die Einstellung manuell festzulegen.

Wichtig:
Der MAC-Tausch ist, falls der Betriebsmodus „LAN-WLAN Bridge“ ist und die WLAN-Schnittstelle als Client eingestellt ist oder der Betriebsmodus auf „WLAN-WLAN Bridge“ eingestellt ist, zwingend erforderlich. Andernfalls funktioniert die Bridge nicht. Grund dafür ist eine Einschränkung im IEEE 802.11 Protokoll (WLAN).
Durch die Aktivierung des MAC-Tauschs können Layer-2-Protokolle (ausgenommen ARP) auf Schnittstelle A ggf. nicht mehr korrekt zugeordnet werden. Bei den Layer-3-Protkollen wird aktuell nur IPv4 und IPv6 unterstützt.
Ist die Einstellung „eigene Frames für Analyse ignorieren“ nicht aktiviert, so werden in die Aufzeichnung und allen anderen vom Gerät gesammelten Daten auch die Frames, die vom Gerät selbst gesendet und empfangen werden (z. B. auch für den Webserver) berücksichtigt.
Durch das Ändern der Bridge-Einstellungen, wird die Bridge neu gestartet. Falls Sie aktuell eine Aufzeichnung oder das Einlernen von Adressen ausführen, gehen Daten verloren.

Möchten Sie die Konfiguration speichern, so müssen Sie auf den Button „Konfiguration übernehmen“, der sich am unteren Ende der Seite befindet, klicken. Daraufhin erscheint folgende Meldung:



Sollte Ihr Gerät dann innerhalb von 5 Sekunden nicht erneut ansprechbar sein, so erscheint die folgende Meldung:



Diese Meldung weist Sie darauf hin, dass das Gerät zur Zeit unter der aktuellen Adresse nicht mehr erreichbar ist (z. B. weil Sie die IP-Adresse, das WLAN-Netz oder den Betriebsmodus geändert haben) und unter welcher Adresse das Gerät nach der Konfigurationsübernahme erreichbar ist. Die Website wird weiterhin versuchen, die Verbindung zum Gerät herzustellen (ggf. mit der neuen IP-Adresse).

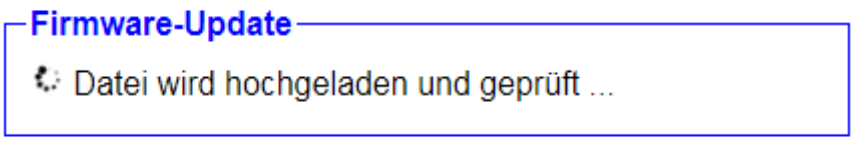
Sollte die erneute automatische Verbindung nach ca. 1 Minute immer noch nicht funktionieren, dann stellen Sie bitte sicher, dass Ihr Computer mit dem Gerät über die richtige Schnittstelle verbunden ist. Kontrollieren Sie ggf. auch die WLAN-Verbindung und die IP-Einstellungen Ihres PCs.

Hinweis:
Sobald das Gerät nach dem Speichern der Konfiguration wieder erreichbar ist, werden Sie auf die Startseite des Geräts weitergeleitet.
Haben Sie im Gerät den DHCP-Client aktiviert, dann erfolgt keine automatische Umleitung auf die Startseite, da die IP-Adresse des Geräts noch unbekannt ist.

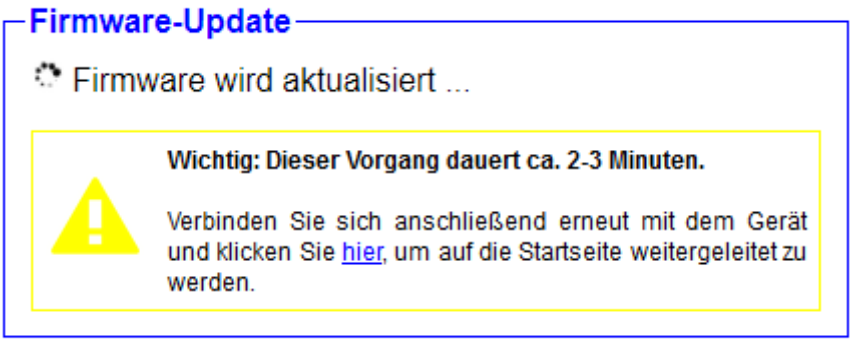
4.8 Seite Firmware-Update

Um die Firmware des Geräts zu aktualisieren, können Sie im Menü auf den Punkt „Firmware-Update“ klicken. Auf der Seite sehen Sie die aktuelle Version, welche in Ihrem Gerät vorhanden ist und haben die Möglichkeit eine Firmware-Datei auszuwählen.

Sobald Sie die Firmware-Datei (dies ist eine Datei mit der Endung .bin) ausgewählt haben, können Sie auf den Button „Firmware aktualisieren“ klicken, um den Update-Vorgang zu starten. Dabei erscheint folgende Meldung:



Wurde die Firmware-Datei akzeptiert, so erscheint nun folgende Meldung:



Das Update dauert ca. 2-3 Minuten. Anschließend sollten Sie sich, falls Ihr Computer, Tablet oder Handy dies nicht automatisch macht, erneut mit dem WLAN-Netzwerk des Geräts verbinden. Dies gilt natürlich nur, wenn der Webserverzugriff auf das Gerät per WLAN erfolgt. Nun sollten Sie automatisch auf die Startseite des Geräts weitergeleitet werden. Sollte die Weiterleitung nicht funktionieren, so haben Sie die Möglichkeit auf den Link im Text zu klicken.

5 Technische Daten

5.1 TINA

Versorgungsspannung:	24V DC +/- 20% (über abziehbaren Stecker)
Leistungsaufnahme:	2 Watt
Anzeige:	Webbrowser Status-LEDs
Bedienung/Konfiguration:	Webbrowser
Schnittstellen:	2 x 10/100BaseTX RJ45-Ethernetbuchse Antennenbuchse RP-SMA(f) (2.4 GHz IEEE 802.11b/g/n)
Betriebstemperatur:	0 - 55°C
Gehäuse:	Kunststoff-Klemmengehäuse für Hutschienenmontage *oder* Kunststoff-Tischgehäuse
Abmessungen:	Klemmengehäuse: 114 x 100 x 22,3 mm Tischgehäuse: 115 x 95 x 30 mm

5.2 ProfiNet-WATCHDOG

Versorgungsspannung:	24V DC +/- 20% (über abziehbaren Stecker) USB (aus PC/Power-Pack)
Leistungsaufnahme:	1,2 Watt
Anzeige:	Webbrowser Status-LEDs
Bedienung/Konfiguration:	Webbrowser
Schnittstellen:	2 x 10/100BaseTX RJ45-Ethernetbuchse Antennenbuchse RP-SMA(f) (2.4 GHz IEEE 802.11b/g/n)
Betriebstemperatur:	0 - 55°C
Gehäuse:	Kunststoff-Klemmengehäuse für Hutschienenmontage *oder* Kunststoff-Tischgehäuse

Abmessungen:	Klemmengehäuse: 114 x 100 x 22,3 mm Tischgehäuse: 115 x 95 x 30 mm

5.3 TINA-II

Versorgungsspannung:	24V DC +/- 20% (über abziehbaren Stecker) USB (aus USB-Netzteil 5V)
Leistungsaufnahme:	9 Watt
Anzeige:	Webbrowser Status-LEDs
Bedienung/Konfiguration:	Webbrowser
Schnittstellen:	2 x 10/100/1000BaseT RJ45-Ethernetbuchse 2 x Antennenbuchse RP-SMA(f) (2x2 MIMO / 2.4 GHz IEEE 802.11b/g/n + 5 GHz IEEE 802.11ac)
Betriebstemperatur:	0 - 55°C
Gehäuse:	Kunststoff-Tischgehäuse
Abmessungen:	115 x 95 x 30 mm