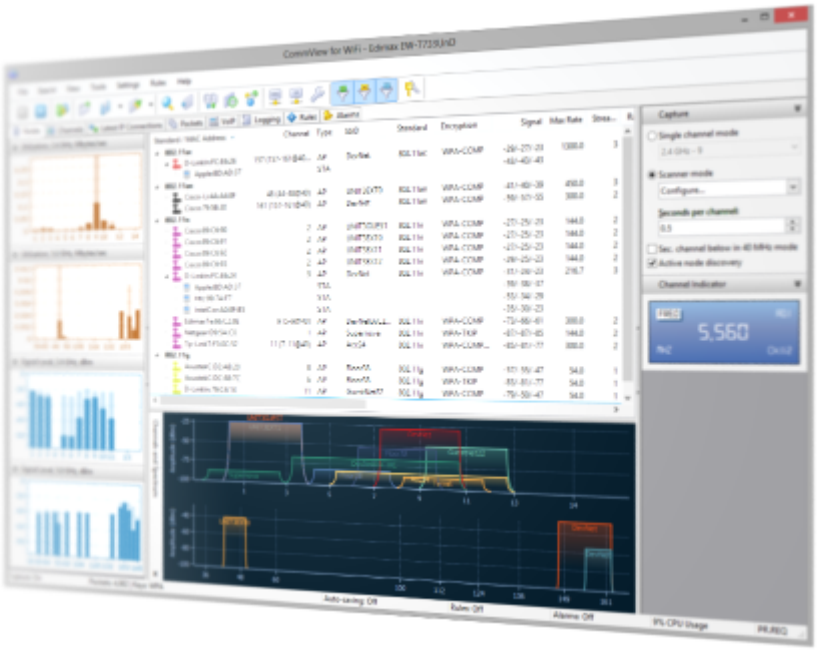
CommView® for WiFi

WLAN Netzwerk Monitor und Analyzer

Hilfe-Dokumentation

Version 7



Copyright © 1999-2024 TamoSoft

Inhalt

Einführung

Über CommView for WiFi

CommView for WiFi ist eine Sonderedition von CommView, die dafür entworfen wurde Netzwerkpakete in kabellosen 802.11 a/b/g/n/ac/ax/be-Netzwerken zu empfangen und zu analysieren. CommView for WiFi sammelt die Informationen des Wireless Adapters und entschlüsselt die zu analysierenden Daten.

CommView for WiFi zeigt Ihnen die Netzwerkverbindungen und wichtigen IP Statistiken, ferner untersucht es individuelle Pakete. Die Pakete können mit den vom Benutzer eingestellten WEP bzw. WPA-PSK Schlüsseln entschlüsselt werden und werden dann auch bis zur untersten Schicht decodiert, einschließlich einer Analyse der am meisten verbreitetsten Protokolle. Auch ist ein Vollzugriff auf Rohdaten möglich. Die empfangenen Pakete können in Logdateien für weitere Analysen abgespeichert werden. Pakete ohne Bedeutung können durch flexible Filter ausgeblendet werden, so dass man nur die wichtigsten sieht. Durch konfigurierbare Alarmmeldungen kann der Anwender über wichtige Events, wie verdächtige Pakete, hohe Bandbreitenausnutzung oder unbekannte Adressen informiert werden.

CommView for WiFi beinhaltet ein VoIP-Modul für detaillierte Analysen, Aufnahme und Wiedergabe von SIP- und H 323-Sprachkommunikationen.

CommView for WiFi ist ein nützliches Tool für WLAN-Administratoren, Sicherheitsexperten, Netzwerkentwickler bzw. für jeden, der seinen WLAN-Traffic im Ganzen überblicken möchte. Diese Applikation erfordert einen kompatiblen drahtlosen Netzwerkadapter. Die unterstützten Adapter finden Sie auf unserer Webseite. CommView for WiFi verfügt über einen erweiterten Protokoll-Decoder, der Tausende der weit verbreiteten Netzwerk-Protokolle parsen kann.

Was ist neu

Version 7.5

- Unterstützung von 802.11be (Wi-Fi 7).
- Unterstützung von Adaptern Intel BE200.

Version 7.4

- Unterstützung für den neuen Tri-Band-USB-Adapter (2,4, 5 und 6 GHz) hinzugefügt: NETGEAR A8000 und Alfa AWUS036AXML.

- CommView for WiFi kann jetzt auf Computern mit ARM64-CPUs laufen.

Version 7.3

- Informationen pro Paket zu MCS-Index, Kanalbreite, Guard Interval und Anzahl der Ströme für jedes Paket
- Neues Erfassungsprotokollformat, NCFX
- Unterstützung von Adaptern Killer Wi-Fi 6 AX1650w, AX1650x und AX1650s

Version 7.2

- Verbesserte Identifizierung von WLAN-Verschlüsselungs- und Autorisierungsmethoden
- Unterstützung von 802.11ax-Adaptern
- Neue Symbole New icons

Version 7.1

- Schnellfilter für die Register “Knoten” und “Kanäle”: Sie können die Pakete nach den Knoten, Kanälen, Pakettyp oder nach Datenrate mit einem Mausklick filtern.
- Unterstützung von Windows 10
- Aktualisierte IP-Adresse-Zuweisungen und Datenbank von MAC-zu-Anbieter

Version 7.0

- Ein wichtiges Upgradeder Bedienfläche: neue Register **Knoten** und **Kanäle**, neue Diagramme und Statistiken
- Integration mit Wi-Spy zur Spektralanalyse

Version 6.5

- Ein komplett überarbeiteter Protokoll-Decoder: mehr unterstützte Protokolle und eine Daten-Zusammenfassung für jedes Paket

Version 6.3

- Unterstützung für USB-Adapter: Ubiquiti SR71-USB (802.11 a/b/g/n), Proxim ORiNOCO 8494 (802.11 a/b/g/n), TP-Link TL-WN821N (802.11 b/g/n), NETGEAR WN111 v2 (802.11 b/g/n)

Version 6.2

- Neue drahtlose Adapter werden unterstützt (Windows Vista oder 7 erforderlich): Intel 3945, 4965, 5100, 5150, 5300, 5350
- UDP-Stream-Rekonstruktion
- Einige Verbesserungen im Protokolldekoder

Version 6.1

- Neue Operationssysteme werden unterstützt: Windows XP 64-bit Edition, Windows Vista 64-bit Edition, Windows Server 2008 32-bit und 64-bit Editionen
- Verringerte RAM-Auslastung durch das VoIP-Analysermodul. Die neue Version kann bei geringerer RAM-Benutzung mehr simultane Anrufe handhaben.
- Einstellbarer Jitter-Puffer für eine realistischere Simulation der realen VoIP-Telefonsoundqualität
- Die Geräuschstärke wird jetzt im Register **Kanäle** angezeigt
- Verbesserter "Suche-Dialog": Suchrichtung und Unicode-Suche (UTF-8, UTF-16) werden jetzt unterstützt
- Mehr flexible Decoder-Baumoptionen: Sie können jetzt die Anzahl der aufzuklappenden Knoten bestimmen.
- Viele andere Verbesserungen und Fehlerbehebungen.

Version 6.0

- VoIP-Modul für eine gründliche erweiterte Analyse, Aufnahme und Wiedergabe von SIP- und H 323-Sprachnachrichten
- Visual TCP-Sitzungen mit graphischer Darstellung von Sitzungsdiagrammen
- Optischer Paketersteller, der die Paketkonstruktion im Paketgenerator erleichtert

Programmbenutzung

Installation der Treiber

CommView for WiFi ist ein Überwachungstool für drahtlose 802.11 a/b/g/n/ac/ax/be-Netzwerke. Zur Benutzung dieses Produktes benötigen Sie einen kompatiblen drahtlosen Adapter. Zwecks Aktivierung der Überwachungsmöglichkeiten Ihres drahtlosen Adapters, benötigen Sie die mit diesem Produkt mitgelieferten speziellen Treiber. Wenn CommView for WiFi nicht läuft, kann Ihr Adapter ganz normal mit anderen drahtlosen Netzwerken und APs kommunizieren. Wenn CommView for WiFi läuft, arbeitet Ihr Adapter ohne Netzwerkverbindung im passiven freizügigen Überwachungsmodus.

Bevor Sie den neuen Treiber für Ihr WLAN-Adapter installieren, überprüfen Sie bitte, ob der Adapter überhaupt zu diesem Produkt kompatibel ist. Eine Liste mit kompatiblen Adapter finden Sie unter:

https://www.tamos.com/download/main/ca

CommView for WiFi unterstützt möglicherweise auch andere Adapter. Wenn Ihr Adapter in der oben genannten Liste nicht aufgelistet ist, können Sie unter unserem FAQ-Kapitel aktuellste Informationen erhalten.

Um eine weitergehende, illustrierte Installationsanweisung zu erhalten, starten Sie bitte das Programm, klicken im Programmmenü auf Hilfe => Hinweise zur Treiberinstallation und scrollen dann bis zum Ende des Fensters.

Übersicht

Das Programminterface besteht aus mehreren Registern, die es Ihnen ermöglichen, sich die Daten anzusehen bzw. verschiedene Aktionen mit den empfangenen Paketen durchzuführen. Die Funktionsfähigkeit dieser Register ist in der folgenden Tabelle beschrieben.

Name des Registers	Beschreibung
Knoten	Das Register dient der Kontrolle der Paketerfassung, zeigt Details für aktive Accesspoints und Stationen sowie Statistiken für die Nutzung der Kanäle und eine grafische Darstellung des drahtlosen Spektrums.
Kanäle	Das Register dient der Darstellung der Statistik pro Kanal sowie von Diagrammen, die die aktivsten Knoten, MB/Sek. und Pakete/Sek. anzeigen.

Aktuelle IP-Verbindungen	Das Register dient der Darstellung detaillierter Informationen über die aktuellen IP-Verbindungen zwischen den WLAN-Knoten. Diese Informationen sind verfügbar, wenn das analysierte Netzwerk keine Verschlüsselung benutzt oder wenn Sie einen korrekten WPA- oder WEP-Schlüssel eingegeben haben.
Pakete	Das Register dient der Auflistung der empfangenen Pakete. Sie können die Pakete prüfen und ihren Inhalt ansehen.
VoIP-Analyse	Das Register dient der detaillierten VoIP-Analyse der empfangenen Pakete. Beachten Sie bitte, dass dieses Register nur für VoIP-Lizenzinhaber oder für Anwender der Testversion mit gewähltem VoIP-Testmodus verfügbar ist.
Logging	Das Register dient dem Abspeichern der empfangenen Pakete in eine Protokolldatei in verschiedenen Formaten und zur Konfigurierung der automatischen Logging.
Regeln	Das Register ermöglicht Ihnen, mit den Paketfiltern zu arbeiten, die zur Regelkonfiguration zum Empfangen/Ignorieren von Paketen auf der Basis verschiedener Kriterien wie der IP-Adresse oder Portnummer dienen.
Alarme	Das Register dient der Erzeugung von Alarmmeldungen, die Sie auf wichtige Ereignisse hinweisen wie verdächtige Pakete, starke Bandbreitennutzung, unbekannte Adressen etc.

Einige der Einstellungen, wie Fonts, Farben und Puffergröße können über den Menüpunkt Einstellungen verändert werden. Weitere Informationen finden sie unter **Einstellungen.**

Hauptmenü

Die Menübefehle der Applikation werden im Folgenden beschrieben.

Datei

- **Erfassung starten** – Startet/stoppt die Paketerfassung.
- **Paketausgabe unterbrechen** – Stoppt/nimmt den Echtzeit Paket-Output im Register **Pakete** wieder auf.
- **Fernüberwachungsmodus** – Blendet eine Leiste für Fernüberwachung ein/aus, durch welche Sie mit den entfernten Datenerfassungsgeräten anschließen können: **Remote Agent for WiFi, RPCAP** oder **Aruba-Fernerfassung**.
- **Knoten speichern unter** – Ermöglicht das Abspeichern der Inhalte des Registers **Knoten**.

- **Kanäle speichern unter** – Ermöglicht das Abspeichern der Inhalte des Registers **Kanäle**.
- **Aktuelle IP Verbindungen speichern unter** – Ermöglicht das Abspeichern des Registers **Aktuelle IP-Verbindungen**.
- **Paketlog speichern unter** – Erlaubt das Abspeichern der Inhalte des Registers **Pakete** in verschiedene Formate.
- **Logbetrachter** – Öffnet ein neues **Logbetrachterfenster**.
- **VoIP-Logbetrachter** – Öffnet ein neues **VoIP-Logbetrachterfenster**.
- **Knoten löschen** – Löscht die Knotentabelle im Register **Knoten**.
- **Kanäle löschen** – Löscht die Kanaltabelle im Register **Kanäle**.
- **Aktuelle IP-Verbindungen löschen** – Löscht den Inhalt des Registers **Aktuelle IP-Verbindungen**.
- **Paketpuffer löschen** – Löscht den Inhalt des Programmpuffers und des Registers **Pakete**.
- **VoIP-Daten leeren** – Entleert den Inhalt des VoIP-Registers.
- **Durchsatzdaten** – Zeigt die Leistungsstatistik des Programms an: die Anzahl der empfangenen und durch den Gerätetreiber ausgeschiedenen Pakete.
- **Beenden** – Beendet das Programm.

Suchen

- **Finde Paket** – Dieser Dialog ermöglicht Ihnen, **Pakete zu finden**, die einen bestimmten Text enthalten.
- **Gehe zu Paket Nummer** – Mit diesem Dialog springen Sie zu einer definierten Paketnummer.

Ansicht

- **Statistiken** – Zeigt ein Fenster mit **Datentransfer- und Protokollverteilungsstatisken**.
- **Port Referenz** – Zeigt ein Fenster mit der **Portreferenzinformation**.
- **Log Verzeichnis** – Öffnet das Verzeichnis in dem standardmäßig die Logs abgespeichert werden.
- **Knotenspalten** – Zeigt/Verbirgt einzelne Spalten im Register **Knoten**.
- **Kanalspalten** – Zeigt/Verbirgt einzelne Spalten im Register **Kanäle**.
- **Aktuelle IP Verbindungsspalten** – Zeigt/Verbirgt einzelne Spalten im Register **Aktuelle IP Verbindungen**.
- **Paketspalten** – Zeigt/Verbirgt einzelne Spalten im Register **Pakete**.
- **Kanäle und Spektrum** – Zeigt/Verbirgt den Ausschnitt **Kanäle und Spektrum** im unteren Bereich des Registers **Knoten**.

Werkzeuge

- **Packetgenerator** – Öffnet den **Packetgenerator**.
- **Rekonstruiere TCP Sitzung** – Ermöglicht Ihnen die **Rekonstruktion einer TCP-Sitzung** ausgehend vom gewählten Paket. Dabei öffnet sich ein Fenster, das die ganze Kommunikation zwischen zwei Hosts darstellt.
- **Rekonstruiere UDP-Stream** – Ermöglicht Ihnen vom ausgewählten Paket ausgehend, **einen UDP-Stream zu rekonstruieren**; es wird ein Fenster eingeblendet, in dem die gesamte Konversation zwischen zwei Hosts angezeigt wird.
- **NIC-Herstelleridentifikation** – Öffnet ein Fenster, mit dem Sie über die MAC-Adresse den **Netzwerkadapterhersteller identifizieren** können.
- **Paketerfassungplaner** – Ermöglicht es **geplante Erfassungsaufgaben** hinzuzufügen oder zu löschen.
- **Knotenzuordnung wiederherstellen** – Öffnet ein Fenster für die **Knotenwiederherstellung**.

Einstellungen

- **Schrift** – Zeigt das Untermenü für die Einstellungen der Interface-Fonts.
- **WEP/WPA Schlüssel...** – Öffnet ein Fenster, zur Verwaltung der **WEP/WPA-Schlüssel**.
- **MAC-Kennname** – Öffnet ein Fenster, in dem Sie MAC-Adressen leicht zu merkende **Kennnamen** zuordnen können.
- **IP-Kennname** – Öffnet ein Fenster, in dem Sie IP-Adressen leicht zu merkende **Kennnamen** zuordnen können.
- **Optionen** – Öffnet das Optionsfenster, in dem Ihnen weitere Einstellmöglichkeiten zur Verfügung stehen.
- **Sprache** – Erlaubt die Auswahl der Interface-Sprache. Versichern Sie sich, daß Sie nach der Sprachauswahl das Programm neu gestartet haben. Das CommView for WiFi-Installationspaket enthält möglicherweise nicht alle für das Interface erhältlichen Sprachen. Klicken Sie auf das Feld **Andere Sprachen** um die weiterführende Sprachdownloadseite unserer Webseite zu erreichen, von der Sie die entsprechende Sprachversion herunterladen können, wenn Sie für die aktuelle Programmversion erhältlich ist.

Regeln

- **Datenpakete erfassen** – Wählen Sie diesen Punkt um das Capturing von Paketen des Typs Daten zu aktivieren/ deaktivieren.
- **Managementpakete erfassen** – Wählen Sie diesen Punkt um das Capturing von Paketen des Typs "Management" zu aktivieren/deaktivieren.

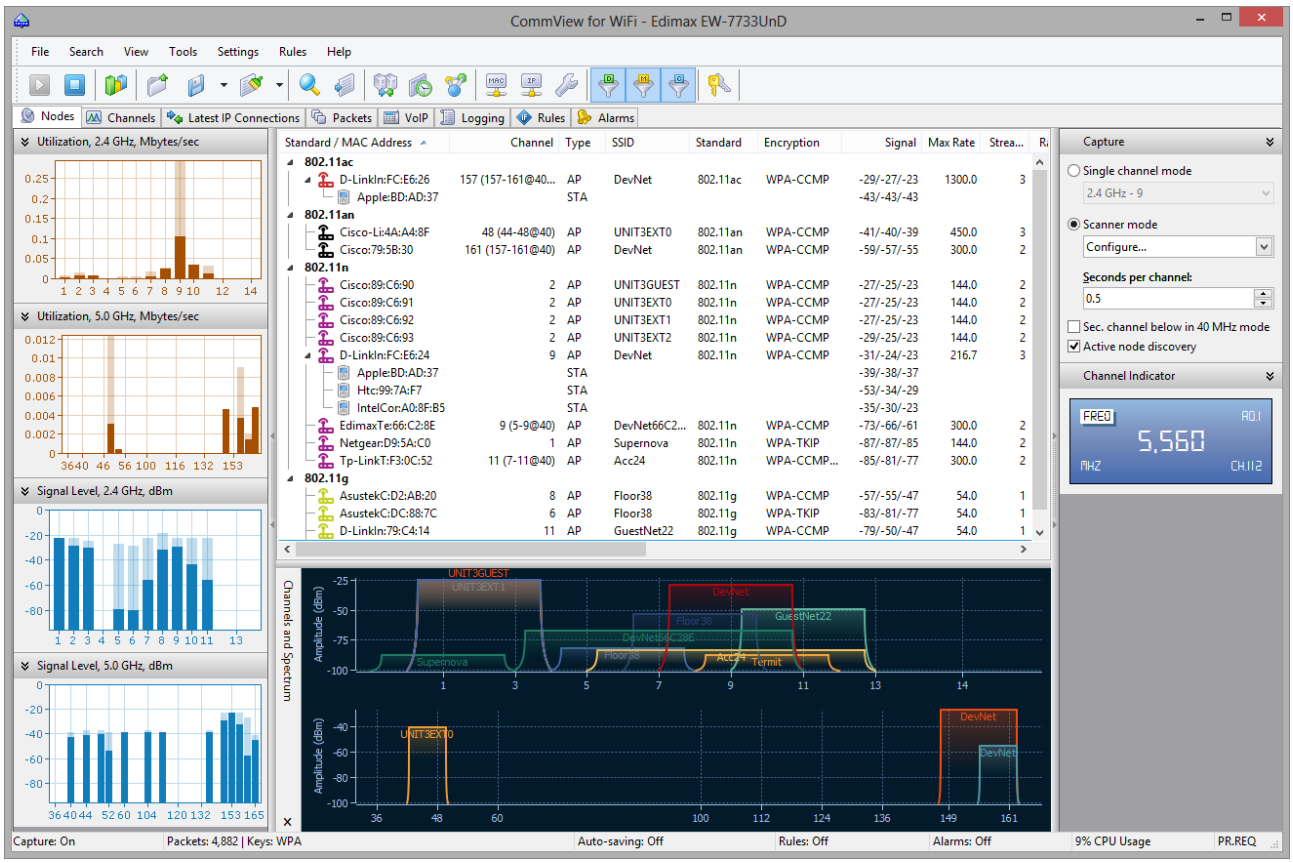
- **Kontrollpakete erfassen** – Wählen Sie diesen Punkt um das Capturing von Paketen des Typs "Kontrolle" zu aktivieren/deaktivieren.
- **Beacons ignorieren** – Wählen Sie diesen Punkt um das Capturing von Paketen des Typs "Beacon" zu aktivieren/deaktivieren.
- **Aktive Regeln speichern als** – Ermöglicht die Speicherung der aktuellen Regeln als Datei.
- **Regeln laden von** – Erlaubt das Laden von vorher abgespeicherten Regelkonfigurationen aus einer Datei.
- **Alles Rücksetzen** – Löscht alle vorhandenen Regeln, sofern vorhanden.

Hilfe

- **Inhalt** – Startet die CommView for WiFi-Hilfe.
- **Suche nach Hilfe über…** – Zeigt den Hilfeindex von CommView for WiFi.
- **Treiberinstallation** – Zeigt eine ausführliche Anleitung zur **Treiberinstallation**.
- **Im Web nach Updates suchen** – Öffnet den Update-Assistent. Bitte folgen Sie der Anleitung auf dem Bildschirm um das neueste Upgrade von CommView for WiFi von der TamoSoft-Website herunterzuladen und zu installieren.
- **Aktivierung** - Ermöglicht Ihnen, Ihre Softwarelizenz freizuschalten oder den gegenwärtigen Aktivierungsstatus einzusehen.
- **Info** – Zeigt Informationen über das Programm.

Knoten

Dies ist das Hauptregister des Programms, das der Kontrolle der Paketerfassung, dem Anzeigen detaillierter Informationen über Accesspoints und dazugehörige Stationen, Kanalauslastungsstatistiken, sowie der grafischen Darstellung des drahtlosen Spektrums dient.



Dieses Fenster besteht aus mehreren in der Größe veränderbaren Ausschnitten, die unten beschrieben sind.

Paketerfassung und Kanal-Anzeige

Der Ausschnitt **Paketerfassung** ermöglicht Ihnen, zwischen zwei Erfassungsmethoden zu wählen: dem **Einkanal-Modus** oder dem **Scanner-Modus**. Wenn Sie den **Einkanal-Modus** wählen, empfängt die Applikation die Pakete auf einem Kanal (oder auf mehreren Kanälen, wenn Sie mehrere unterstützte USB-Adapter benutzen; siehe die Information unten); die Kanäle können Sie in einer Drop-down-Liste auswählen. Wenn Sie den **Scanner-Modus** wählen, wird die Applikation zwischen den Kanälen wechseln; d.h., die Applikation empfängt die Pakete auf dem ersten Kanal, dann auf dem nächsten usw., bis sie am letzten Kanal ankommt. Dann beginnt die Applikation mit einem neuen Scanzyklus. Um die Kanäle fürs Scannen zu wählen, klicken Sie auf den Button **Konfigurieren** und aktivieren Sie die Auswahlkästchen, um die Kanäle zu wählen/abzuwählen. Je nach Land und den regulierenden Domänen, die in Ihrem Adapter eingestellt sind, kann die Liste der unterstützten Adapter variieren. Dies wird detailliert im Kapitel FAQ diskutiert. Benutzen Sie das Feld **Sekunden/ Kanal**, um die Zeit zu konfigurieren, die die Applikation für den Scanprozess jedes Kanals benutzt.

Es gibt auch zwei andere Einstellungen im unteren Bereich des Ausschnitts zur Kontrolle der Paketerfassung. Die Checkbox **Sekundärkanal unter im 40-MHz-Modus** bestimmt die Position des Sekundärkanals, wenn die Kanalbindung im 2,4-GHz-Band benutzt wird. Standardmäßig ist die Frequenz des Sekundärkanals in 802.11-Netzwerken (40 MHz) höher als die Frequenz des

Primärkanals. Aktivieren Sie diese Checkbox, wenn Sie die Pakete in einer Netzwerkumgebung erfassen, in der der Sekundärkanal eine geringere Frequenz hat. Die aktivierte Checkbox hat keine Wirkung, wenn der Sekundärkanal nicht unter dem Primärkanal platziert werden kann. Dies ist z. B. der Fall, wenn Sie auf dem 2,4-GHz-Band die Kanäle 1, 2, 3 oder 4 erfassen. Diese Option ist nur verfügbar, wenn Ihr Adapter die Erfassung auf 40-MHz-Kanälen unterstützt. Wenn die Checkbox **Aktive Entdeckung der Knoten** aktiviert ist, sendet die Applikation periodisch PROBE REQUEST-Pakete. Solche Pakete ermöglichen das Erkennen von Accesspoints, die keine SSID senden. Diese Option ist nur verfügbar, wenn Ihr Adapter die Paketgenerierung unterstützt.

Nachdem Sie die Erfassungsoptionen konfiguriert haben, klicken Sie auf **Paketerfassung starten** in der Werkzeugleiste. Wenn Sie auf einen neuen Kanal oder in den **Scanner-Modus** umschalten möchten, während der **Einkanal-Modus** aktiviert ist, können Sie dies tun, ohne die Erfassung anzuhalten. Der Ausschnitt **Kanal-Anzeige** zeigt den aktuellen Kanal und die Frequenz, während die Applikation Pakete erfasst.

Benutzung mehrerer Adapter für Mehrkanalerfassung

Wenn Sie die Pakete auf mehreren Kanälen simultan erfassen müssen, ist dies möglich, wenn Sie mehrere USB-Adapter benutzen. In diesem Modus wird die Drop-down-Liste für die Kanalauswahl zum Mehrfachauswahl-Bedienelement, das es Ihnen ermöglicht, bei gedrückter **Ctrl**-Taste mehrere Kanäle zu wählen. Der Ausschnitt **Kanal-Anzeige** zeigt dann mehrere Kanal-/Frequenz-Indikatoren an. Beachten Sie, dass nur einige Adapter-Modelle die Anschaltung mehrerer Adapter unterstützen. Weitere Informationen finden Sie im Kapitel Mehrkanalerfassug.

Liste der Knoten

Nachdem die Paketerfassung gestartet ist, fängt das Programm an, die Knotenliste mit den gefundenen drahtlosen Knoten zu befüllen. Der im Programm genutzte Mechanismus zur Paket-Analyse listet alle auf den vorgegebenen Kanälen und Stationen gefundenen Access Points im Ad-hoc-Modus auf sowie alle verbundenen Stationen im Infrastruktur-Modus. Es ist wichtig zu verstehen, dass das Radiomodul in einem drahlosen Adpater Daten nur jeweils auf einem Kanal gleichzeitig erhalten kann. Wenn Sie daher einen bestimmten Kanal zur Überwachung gewählt haben, zeigt die Tabelle nur die APs und Stationen an, die Daten auf diesem gewählten Kanal senden. Sie können allerdings einen anderen Kanal auswählen, ohne die Daten in der Tabelle zu löschen, oder den Scanner-Modus wählen, um die Applikation die Kanäle zyklisch scannen zu lassen, damit Sie alle aktiven Knoten auf verschiedenen Kanälen sehen können.

Die Bedeutung der Tabellenspalten wird im Folgenden beschrieben:

- **SSID/Band/Kanal** – Je nach der ausgewählten Gruppierungsmethode (zugänglich über das Kontextmenü **Aufteilen**), listet die erste Spalte nach SSID, 802.11-Standard oder Kanal

gruppierte drahtlose Knoten auf. Jeder Knoten zeigt die MAC-Adresse oder einen Kennnamen. Die mit den APs verbundenen Stationen werden als untergeordnete Artikel angezeigt, die mit APs auf der obersten Ebene verbunden sind.

- **Kanal** – Der Kanal, auf dem der ausgewählte AP funktioniert. Wenn der AP die Kanalbindung benutzt (40-, 80- oder 160-MHz-Kanäle), wird zuerst der Primärkanal aufgelistet, dann folgen in Klammern Informationen über die zusätzlichen Kanäle.
- **Typ** – Knotentyp. Mögliche Werte sind AP (Accesspoint), STA (Station im Infrastruktur-Modus) und AD HOC (Stationen im Ad-hoc-Modus).
- **SSID** – Service Set Identifier, ein eindeutiger Stringwert, der die verschiedenen WLANs voneinander unterscheidet.
- **Standard** – 802.11-Standard des APs. Mögliche Werte sind 802.11be, 802.11ax, etc.
- **Verschlüsselung** – Zeigt, ob der Knoten WEP- oder WPA-Verschlüsselung benutzt. Diese Spalte zeigt für Accesspoints verfügbare Verschlüsselungsmethoden an, die der AP benutzt.
- **Signal** – Signal-Level im Min.-/Durchschnitts-/Max.-Format. Hier wird der Durchschnittswert seit dem letzten Tabellen-Reset berechnet. Mehr dazu unter Signalstärke.
- **Max. Datenrate** – Maximale Rate der PHY-Daten, die der AP anbieten kann.
- **Ströme** – Die Zahl der spatialen Ströme, die der AP unterstützen kann.
- **Rate (Tx** und **Rx)** – Datentransferrate im Min.-/Durchschnitts-/Max.-Format. Hier wird der Durchschnittswert seit dem letzten Tabellen-Reset berechnet.
- **Bytes (Tx** und **Rx)** – Die vom Knoten verschickte/empfangene Datenmenge in Bytes.
- **Pakete** – Die Zahl der vom Knoten verschickten/empfangenen Pakete.
- **Wiederholung (Tx** und **Rx)** – Die Anzahl der Datenpakete mit Wiederholungsflag.
- **Fragmentiert (Tx** und **Rx)** – Die Anzahl der Datenpakete mit Fragmentiert-Flag.

Einzelne Spalten können durch Rechtsklicken auf die Spaltenüberschriften aus- und eingeblendet werden, oder im Menü **Ansicht => Knotenspalten**. Die Spaltenreihenfolge kann durch Ziehen einer Spaltenüberschrift an eine neue Position geändert werden. Ein Rechtsklick auf die Liste der Knoten öffnet ein Menü mit den folgenden Befehlen:

- **Details…** – Zeigt das Fenster AP and Station Details.
- **Schnellfiltern** – Findet die von/auf den gewählten Knoten gesendeten Pakete, sowie die Pakete in denen MAC-Adresse von den gewählten Knoten der BSSID-Adresse gleichwertig ist, und zeigt diese Pakete in einem neuen Fenster.
- **MAC-Adresse kopieren** – Kopiert die MAC-Adresse des ausgewählten Knotens in die Zwischenablage.
- **Kennname anlegen** – Öffnet ein Fenster, in welchem Sie leicht zu merkende Kennnamen für die ausgewählten MAC-Adressen wählen können.

- **Knoten speichern unter…** – Speichert die Inhalte des Registers **Knoten** als HTML-Report.
- **Knoten löschen** – Löscht die Tabelle.
- **Weitere Statistiken…** – Öffnet ein Fenster mit den **Datentransfer- und Protokollverteilungsstatistiken**.
- **Aufteilen** – Gruppiert die Listen nach dem SSID, Kanal oder Band.

Auslastung und Signal-Level

Diese Ausschnitte links auf dem Register **Knoten** zeigen Pro-Kanal-Auslastungsdiagramme (drei separate Diagramme für 2,4 GHz-, 5 GHz-, und 6 GHz-Kanäle) und Diagramme für Pro-Kanal-Signal-Level (drei separate Diagramme für 2,4 GHz-, 5 GHz-, und 6 GHz-Kanäle) an. Zusätzlich zu den aktuellen Pegeln zeigen diese Diagramme die historischen Höchststände, die in heller Farbe markiert sind.

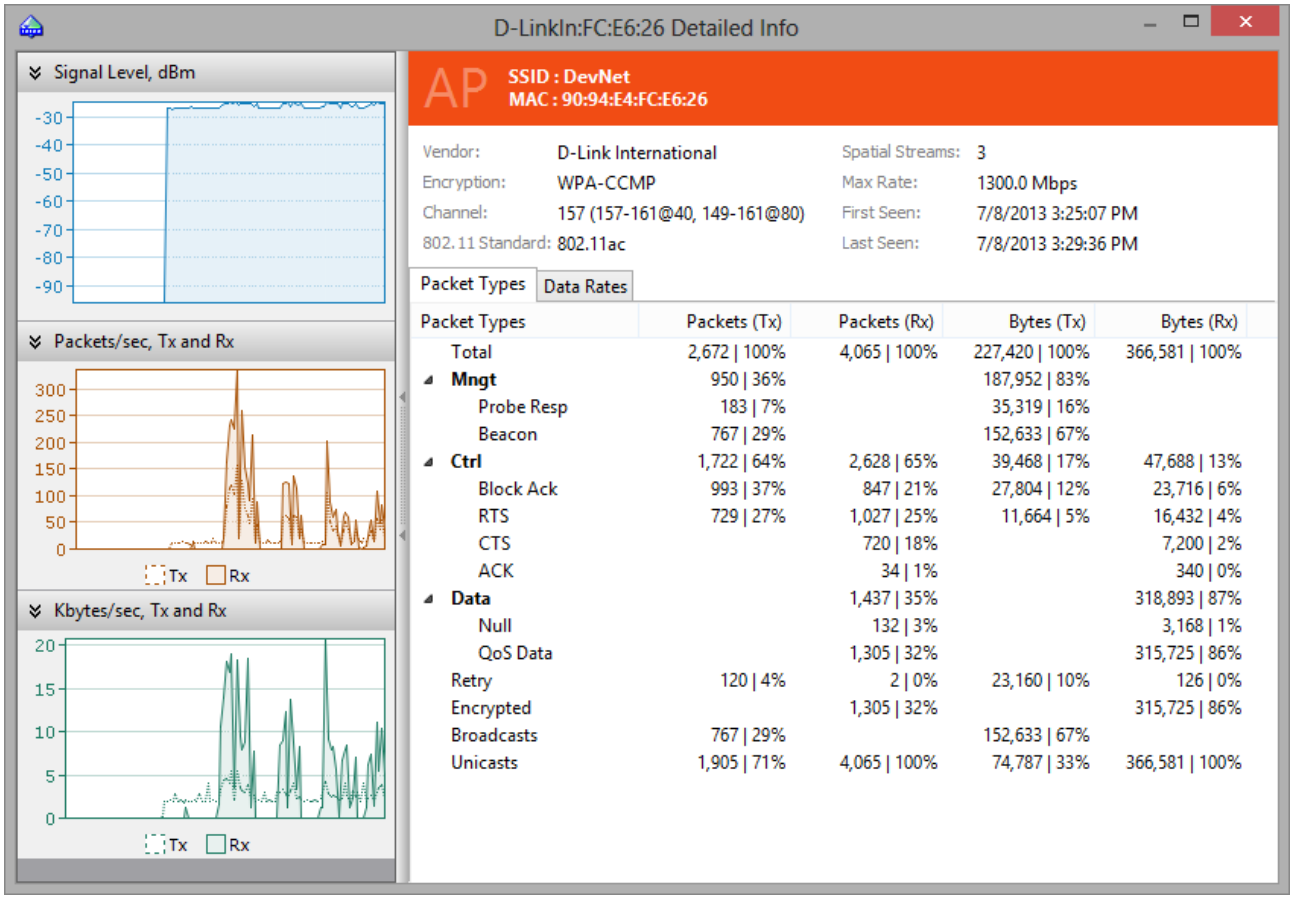
Kanäle und Spektrum

Der im unteren Bereich des Registers **Knoten** befindliche Ausschnitt hat zwei Funktionen:

- Er dient der grafischen Darstellung der aktiven APs, wobei jeder AP mit einer Linie angezeigt wird. Diese Linie entspricht der Spektrumsmaske des APs. Die Maskenbreite hängt von der Kanalbreite ab, die der AP unterstützt; die Maskenhöhe hängt von der aktuellen Signalstärke ab.
- Er dient der Darstellung der Spektrumsdaten, wenn Sie einen USB-basierten Spektralanalysator **WiPry** von **Oscium** oder Wi-Spy von MetaGeek anschließen. Ein Spektralanalysator hört die von den Wi-Fi-Geräten benutzten Frequenzbänder ab und analysiert sie. Weil diese Bänder unlizenziert sind, werden sie oft gemeinsam von RF-Signalen von Nicht-Wi-Fi-Quellen mitgenutzt – wie drahtlosen Videokameras, Mikrowellenöfen oder drahtlosen Telefonen –, wodurch Interferenz verursacht wird. Der Zweck der Spektralanalyse ist es, solche Interferenzquellen zu entdecken, sie zu beseitigen und/oder die WLAN-Kanäle mit minimaler Interferenz zu ermitteln. Mehr dazu unter **Spektralanalyse**.

AP- und Stationsdetails

Bei Rechtsklick auf den AP oder eine Station, die im Register **Knoten** angezeigt werden, öffnet CommView for WiFi ein Fenster, das detaillierte Informationen für den ausgewählten Knoten anzeigt – siehe folgende Abbildung.



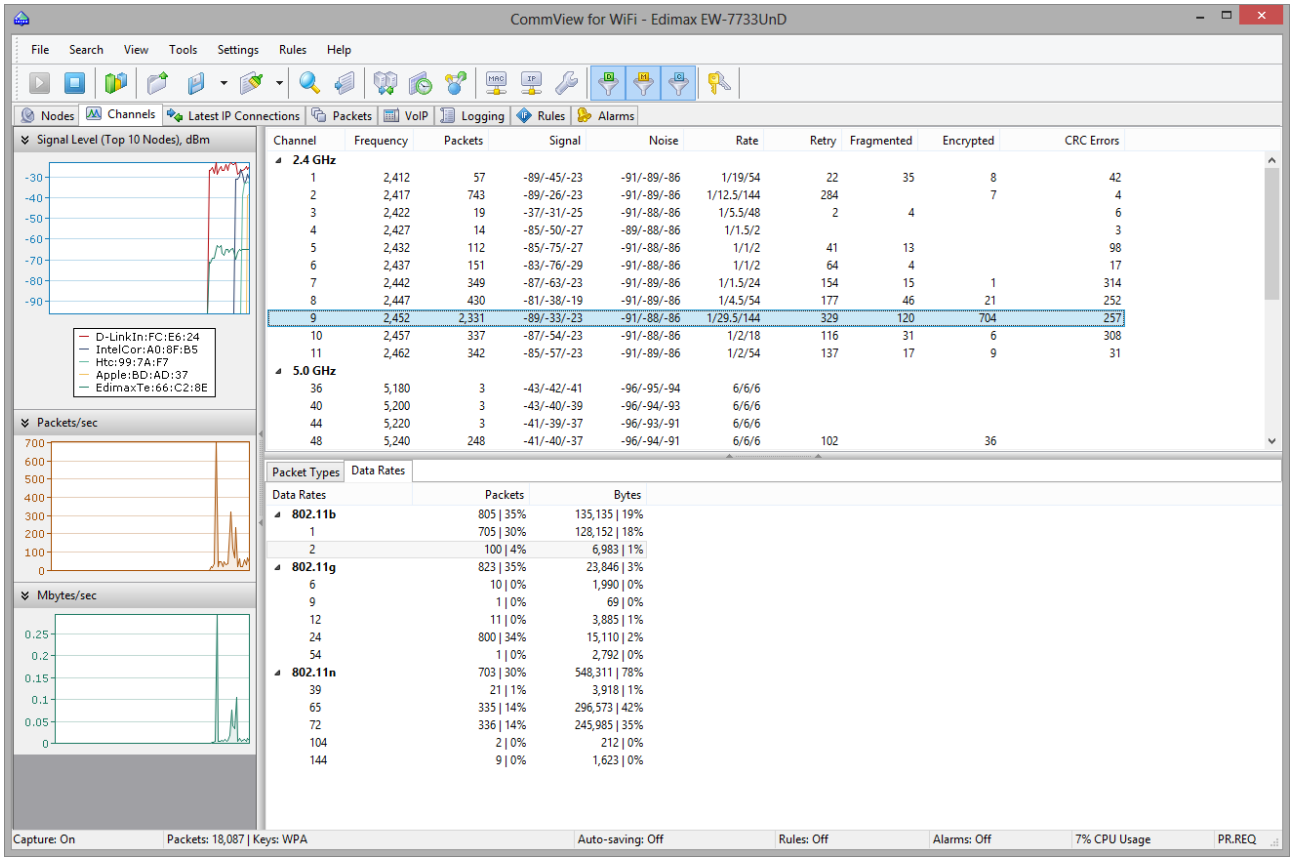
Der obere Ausschnitt zeigt den Typ, die MAC-Adresse und die SSID des ausgewählten Knotens sowie andere wesentliche Details wie den Kanal, die Zeit der ersten und letzten Sichtung usw. Der Ausschnitt benutzt dieselbe Farbe, in der der ausgewählte AP im Ausschnitt **Kanäle und Spektrum** im Hauptfenster der Applikation markiert ist.

Die Tabellen **Pakettypen** und **Datenraten** befinden sich im unteren Ausschnitt. Diese Tabellen zeigen detaillierte Statisken für den ausgewählten Kanal an, die auf Pakettypen, Untertypen basieren, sowie die Statisken für Datenraten.

Im linken Bereich können Sie drei Diagramme sehen: **Signal-Level**, **Pakete/Sek.** und **Mbytes/Sek**. Das Diagramm **Signal-Level** zeigt den Signalpegel für den ausgewählten Knoten. Die Diagramme **Pakete/Sek.** und **Mbytes/Sek.** zeigen die Zahl der Pakete und die Mbytes pro Sekunde, die nach/von dem vorgegebenen Knoten gesendet werden. Beachten Sie, dass diese Diagramme erst aktualisiert werden, wenn die Applikation wirklich die Daten auf dem Kanal empfängt, auf dem der vorgegebene Knoten funktioniert. Wenn Sie z. B. die Daten auf Kanal 5 erfassen und der ausgewählte AP auch auf Kanal 5 arbeitet, werden die Diagramme ständig aktualisiert. Wenn Sie jedoch den **Scanner-Modus** benutzen, werden die Diagramme aktualisiert, wenn die Applikation den Kanal scannt, auf dem der gewählte AP arbeitet.

Kanäle

Dieses Register zeigt für alle überwachten Kanäle die Statistik pro Kanal. Die Zahl der Kanäle in der Tabelle hängt davon ab, wie Sie CommView for WiFi verwenden. Wenn Sie lediglich einen Kanal Ihres WLANs überwachen, werden nur die Daten des ausgewählten Kanals angezeigt, da das im WLAN-Adapter verwendete „Radio“ nur jeweils auf einem Kanal Daten empfangen kann. Wenn Sie nun einen anderen Kanal wählen, wird dieser der Tabelle hinzugefügt. Wenn Sie den **Scanner-Modus** im Register **Knoten** wählen, zeigt die Tabelle die Daten aller gescannten Kanäle an, von denen mindestens ein Paket empfangen wurde.



Da der 802.11-Standard überlappende Kanalfrequenzen im 2,4-GHz-Band benutzt, bemerken Sie vielleicht, dass, selbst wenn Ihr WLAN so konfiguriert wurde, dass es nur einen Kanal benutzt (z. B. Kanal 6), auf den Nachbarkanälen dennoch von Null unterscheidbare Werte erscheinen. Anders als 2,4-GHz-Kanäle, überlappen die 5-GHz-Kanäle nicht.

Die Tabellen **Pakettypen** und **Datenraten** finden Sie in dem unteren Ausschnitt. Diese Tabellen zeigen detaillierte Statistiken für den ausgewählten Kanal an, die auf Pakettypen, Untertypen und Datenraten basieren.

Das Diagramm **Signal-Level** zeigt den Signalpegel für die 10 aktivsten Knoten auf dem ausgewählten Kanal. Die Diagramme **Pakete/Sek.** und **Mbytes/Sek.** zeigen die Zahl der Pakete und

Mbytes pro Sekunde, die auf dem ausgewählten Kanal empfangen wurden. Wenn Sie mit den Daten dieser Diagramme arbeiten, beachten Sie bitte Folgendes:

- Die Diagramme zeigen die Daten nur für den ausgewählten Kanal.
- Die Diagramme werden erst aktualisiert, wenn die Applikation wirklich Daten auf dem ausgewählten Kanal empfängt. Wenn Sie z. B. Daten auf Kanal 2 erfassen und in der Drop-down-Liste Kanal 2 wählen, werden die Diagramme ständig aktualisiert. Wenn Sie Kanal 3 auswählen, werden die Diagramme „eingefroren". Wenn Sie den **Scanner-Modus** benutzen und einen Kanal auswählen, werden die Diagramme jedes Mal aktualisiert, wenn die Applikation den ausgewählten Kanal scannt.

Die Bedeutung der einzelnen Tabellenspalten wird im Folgenden erklärt:

- **Kanal** – Die Kanalnummer.
- **Frequenz** – Die Kanalfrequenz in MHz.
- **Pakete** – Die Gesamtzahl der empfangenen Pakete.
- **Signal** – Signal-Level im Min.-/Durchschnitts-/Max.- Format. Hier wird der Durchschnittswert seit dem letzen Tabellen-Reset berechnet. Mehr dazu unter **Signalstärke**.
- **Geräusch** – Geräuschstärke im Min.-/Durchschnitts-/Max.-Format. Der durchschnittliche Wert wird seit dem letzten Reset in dieser Tabelle errechnet. Die Geräuschinformation ist nicht bei allen Adaptern verfügbar. Diese Spalte ist nicht sichtbar, wenn Ihr Adapter diese Funktion nicht unterstützt.
- **Rate** – Datentransferrate im Format Min./Durchschnitt/Max. Hier wird der Durchschnittswert seit dem letzen Tabellen-Reset berechnet.
- **Wiederholung** – Die Anzahl der Datenpakete mit Wiederholungsflag.
- **Fragmentiert** – Die Anzahl der Datenpakete mit Fragmentiert-Flag.
- **Verschlüsselung** – Die Anzahl der Datenpakete mit Verschlüsselungsflag.
- **CRC-Fehler** – Die Anzahl der Pakete mit CRC-Fehlern. Mehr dazu unter **Hintergründe von CRC- und ICV-Fehlern**.

Einzelne Spalten können durch Rechtsklick auf die Spaltenüberschriften aus- und eingeblendet werden, oder im Menü **Ansicht => Aktuelle IP-Verbindungsspalten**. Die Spaltenreihenfolge kann durch Ziehen einer Spaltenüberschrift an eine neue Position geändert werden. Ein Rechtsklick auf die Kanalliste öffnet ein Menü mit den folgenden Befehlen:

- **Schnellfiltern** – Findet die von dem gewählten Kanal gesendeten Pakete und zeigt sie in einem neuen Fenster. finds the packets sent on the selected channel and displays them in a new window.

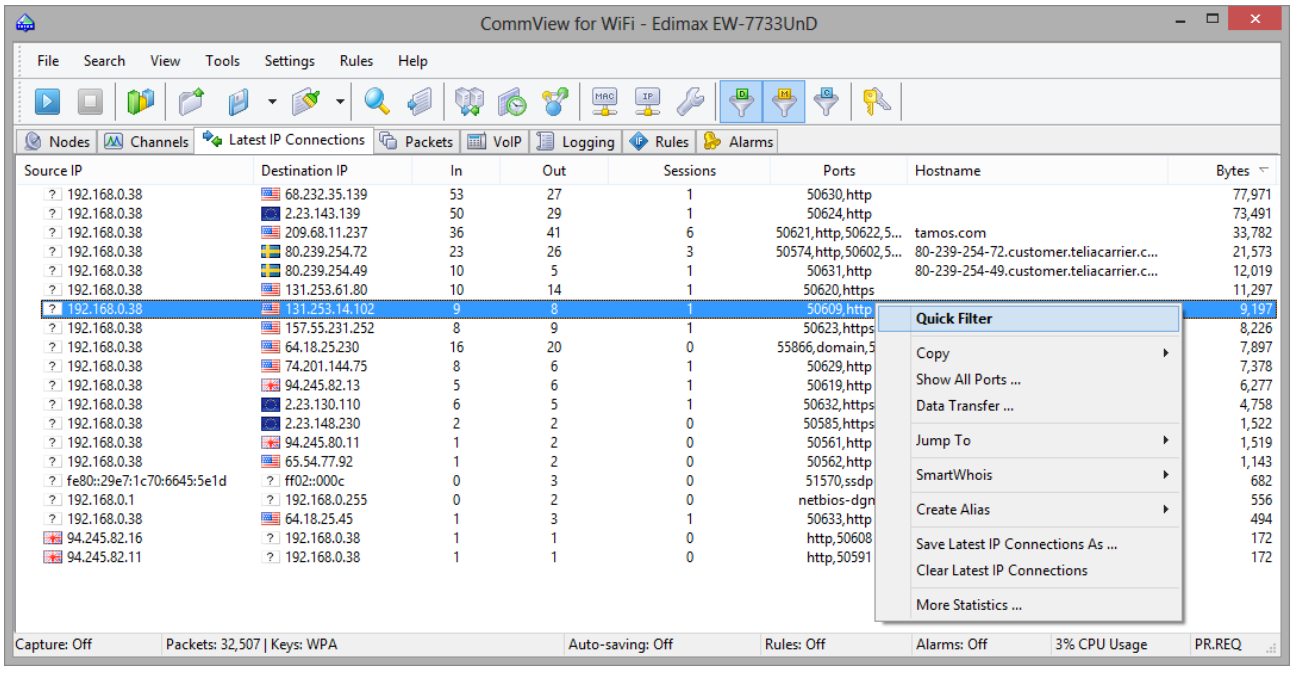
- **Kanäle speichern unter…** – Zum Abspeichern des Inhalts im Register **Kanäle** als HTML-Bericht.
- **Kanäle löschen** – Löscht den Inhalt der Tabelle.
- **Weitere Statistiken** – Zeigt ein Fenster mit den Datentransfer- und Protokollverteilungsstatistiken.

Ein Rechtsklick auf die Tabellen **Pakettyp** und **Dataraten** ruft ein Menü mit dem folgenden Befehl ab:

- **Schnellfiltern** – Findet die Pakete, die dem gewählten Pakettyp oder Datenrate entsprechen und zeigt sie in einem neuen Fenster.

Aktuelle IP-Verbindungen

Dieses Register wird zur Anzeige detaillierter Informationen Ihrer WLAN-Netzwerkverbindungen (nur IP- und IPv6-Protokolle) benutzt. Zum Start der Paketüberwachung wählen Sie im Menü **Datei => Erfassung** starten oder klicken Sie auf den zugehörigen Button in der Werkzeugleiste. Bitte beachten Sie, dass dieser Bereich nicht angefüllt wird, bevor das Programm in der Lage ist WEP-/WPA-verschlüselten Verkehr zu entschlüsseln. Wenn Ihr WLAN WEP-Verschlüsselung nutzt, werden alle versendeten Datenpakete verschlüsselt, so dass es unmöglich ist, Informationen über deren IP-Adresse zu bekommen, solange Sie nicht den korrekten WEP- bzw. WPA-Schlüssel eingegeben haben. Um diese WEP-/WPA-Schlüssel im Menü einzugeben, wählen Sie bitte im Menü **Einstellungen => WEP/WPA Schlüssel**. Zusätzliche Schritte sind bei WPA-Entschlüsselung erforderlich. Mehr dazu unter Hintergründe der WPA-Entschlüsselung.



Die Bedeutung der einzelnen Registerspalten ist im Folgenden erklärt:

- **Quell-IP, Ziel-IP** – Zeigt das IP-Adressenpaar, zwischen denen die Pakete ausgetauscht werden. Das Programm bestimmt automatisch den Standort jeder IP-Adresse, und je nach Ihren Landeseinstellungen, kann der Landesname oder die Landesflagge der IP-Adresse angezeigt werden. Weitere Informationen finden sie unter **Einstellungen**.
- **Eingehend** – Zeigt die Anzahl der eingegangenen Pakete.
- **Ausgehend** – Zeigt die Anzahl der ausgehenden Pakete.
- **Sitzungen** – Zeigt die Anzahl der vorhandenen TCP/IP-Sitzungen. Wenn keine TCP-Verbindungen vorhanden sind ist dieser Wert Null (Verbindungen kamen nicht zustande oder das Protokoll ist UDP/IP bzw. ICMP/IP).
- **Ports** – Zeigt die Ports des Quellcomputers (Sender), die für die TCP/IP-Verbindung genutzt werden bzw. für den Versuch des Verbindungsaufbaus. Diese Liste kann durchaus leer sein, wenn das verwendete Protokoll nicht TCP/IP ist. Ports können entweder als Zahlenwerte dargestellt werden oder als korrespondierender Servicename. Weitere Informationen finden Sie unter **Einstellungen**.
- **Hostname** – Zeigt den Hostnamen des Sendecomputers. Wenn dieser nicht aufgelöst werden kann, wird nichts angezeigt.
- **Bytes** – Zeigt die während der Sitzung übertragene Bytemenge an.
- **Letztes Paket** – Zeigt die Uhrzeit des während der Session zuletzt gesendeten/empfangenen Paketes an.

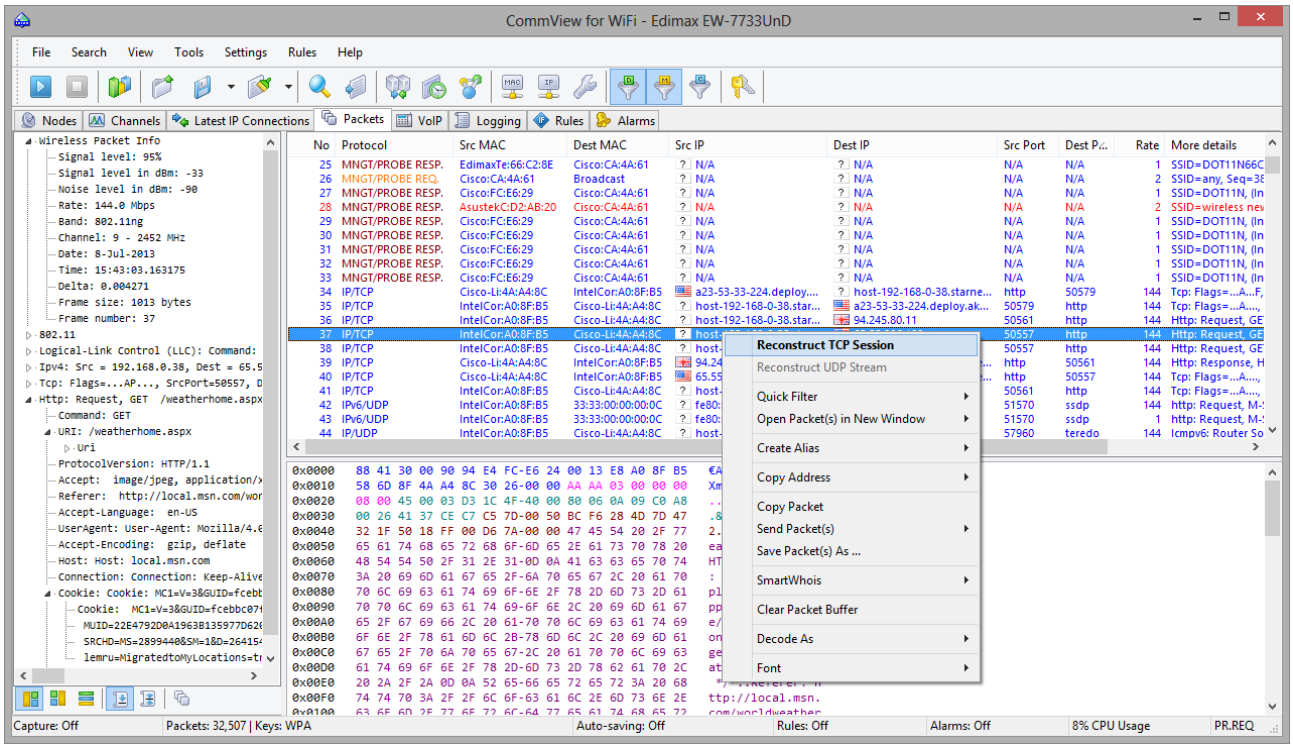
Einzelne Spalten können durch Rechtsklick auf die Spaltenüberschriften aus- und eingeblendet werden, oder im Menü **Ansicht => Aktuelle IP-Verbindungsspalten**. Die Spaltenreihenfolge kann durch Ziehen einer Spaltenüberschrift an eine neue Position geändert werden. Ein Rechtsklick auf das Register Aktuelle IP-Verbindungen öffnet ein Kontextmenü mit den folgenden Befehlen:

- **Schnellfiltern** – Findet die zwischen den ausgewählten IP-Adressen versendeten Pakete und zeigt die Pakete in einem neuen Fenster an. Dies geschieht auch, wenn Sie einen Doppelklick auf das Fenster ausführen.
- **Kopieren** – Kopiert die lokale und die Remote-IP-Adresse bzw. den Hostnamen in die Zwischenablage.
- **Alle Ports anzeigen** – Zeigt eine Liste aller Ports, die für die Kommunikation zwischen dem ausgewählten IP-Adressenpaar verwendet wurden. Dies ist nützlich, wenn viele Ports verwendet wurden und diese nicht in die entsprechende Spalte hineinpassen.
- **Datentrasfer** – Zeigt die Information über das Datentransfervolumen zwischen dem ausgewählten IP-Adressenpaar bzw. über die Uhrzeit des letzten Paketes.

- **Gehe zu** – Hiermit springen Sie schnell zum ersten/letzten Paket der ausgewählten Quell-/Ziel-IP-Adresse. Das Programm zeigt dabei das Register Pakete und setzt den Cursor auf das Paket, welches dem Kriterium entspricht.
- **SmartWhois** – sendet die ausgewählte Ausgangs-/Ziel-IP-Adresse zu SmartWhois, sofern dies auf Ihrem System installiert ist. SmartWhois ist eine selbstständige Anwendung, die von Tamosoft entwickelt wurde. Die Anwendung zeigt dabei automatisch die zu einer IP-Adresse gehörenden Informationen, wie die Domäne, den Netzwerknamen, das Land, den Bundesstaat bzw. den Bezirk und die Stadt. Dieses Programm kann von der Tamosoft-Webseite heruntergeladen werden.
- **Kennname kreieren** – Öffnet ein Fenster, in welchem Sie leicht zu merkende Kennname für die ausgewählten IP-Adressen wählen können.
- **Aktuelle IP Verbindungen speichern unter** – Ermöglicht die Speicherung der Inhalte des Bereichs **Aktuelle IP-Verbindungen** als HTML- Bericht.
- **Aktuelle IP-Verbindungen löschen** – Löscht den Inhalt des Registers.
- **Weitere Statistiken** – Zeigt ein Fenster mit den Datentransfer- und Protokollverteilungsstatiken.

Pakete

Dieses Register dient zur Auflistung aller empfangenen Netzwerkpakete und zeigt detaillierte Informationen über das ausgewählte Paket.



Der **obere Bereich** zeigt eine Liste der empfangenen Pakete. Verwenden Sie diese Liste um ein Paket auszuwählen, dass Sie angezeigt und analysiert haben möchten. Wenn Sie ein Paket durch anklicken auswählen, zeigen die anderen Bereiche Informationen über dieses Paket.

Die Bedeutung der einzelnen Registerspalten ist im Folgenden erklärt:

- **Nr.** – Eine eindeutige Paketnummer.
- **Protokoll** – Zeigt das Paketprotokoll.
- **Src MAC, Dest MAC** – Zeigt die Quell- und Ziel-MAC-Adressen.
- **BSSID** – Zeigt die MAC-Adressen vom AP (wo zutreffend).
- **Src IP, Dest IP** – Zeigt die Quell- und Ziel-IP-Adresse (wo zutreffend).
- **Src Port, Dest Port** – Zeigt die Quell- und Ziel-Ports (wo zutreffend). Die Ports können numerisch oder als entsprechende Servicenamen angezeigt werden. Weitere Informationen finden Sie unter **Einstellungen**.
- **Zeit/Delta** – Zeigt die absolute oder Deltazeit des Pakets. Die Deltazeit ist dabei der Unterschied zwischen den absoluten Zeitangaben der letzten zwei Pakete. Der Wechsel zwischen beiden Zeitarten geschieht durch **Ansicht => Paketspalten => Zeit anzeigen als**.
- **Größe** – Zeigt die Paketgröße in Bytes. Diese Spalte ist standardmässig ausgeblendet.
- **Signal** – Zeigt die Signalstärke im hundertstel oder dBm Format. Mehr dazu unter **Signalstärke**.
- **Rate** – Zeigt die Datentransferrate in Megabits pro Sekunda an.
- **Mehr Details** – Zeigt die Zusammenfassung für jedes Paket.
- **Fehler** – Zeigt Fehlerinformationen. Siehe auch **Hintergründe von CRC- und ICV-Fehlern** für eine detailliertere Beschreibung. Diese Spalte ist standardmäßig ausgeblendet.
- **RA IP** – Wenn Sie Remote Agent(s) benutzen um die Daten zu sammeln, zeigt die Spalte die IP-Adresse vom Remote Agent, der das entsprechende Paket erfasst hat.

Einzelne Spalten können durch Rechtsklicken auf die Spaltenüberschriften aus- und eingeblendet werden, oder im Menü **Ansicht => Paketspalten**. Die Spaltenreihenfolge kann durch Ziehen einer Spaltenüberschrift an eine neue Position geändert werden.

Die kontinuierliche Paketanzeige kann mit **Datei => Paketausgabe unterbrechen** unterbrochen werden. In diesem Modus werden Pakete zwar empfangen, aber nicht im Register **Paket** analysiert. Dies ist nützlich, wenn Sie eher an den allgemeinen Statistiken als an einzelnen Paketen interessiert sind. Um die Echtzeitanzeige der Pakete wieder zu aktivieren klicken Sie auf **Datei => Erfassung starten**.

Der **mittlere Bereich** des Registers zeigt den Grobinhalt des Paketes, sowohl in Hexadezimaldarstellung als auch im Klartext. Im Klartext werden nichtdruckbare Zeichen durch Punkte ersetzt. Wenn im **oberen Bereich** Pakete ausgewählt wurden, zeigt der **mittlere Bereich** die

Gesamtanzahl der ausgewählten Pakete an, ferner deren Gesamtgröße und den zeitlichen Abstand zwischen dem ersten und dem letzten Paket.

Der **untere Bereich** des Registers zeigt die entschlüsselten Paketdaten für das ausgewählte Paket. Dies enthält wichtige Informationen für Netzwerkexperten. Mit einem Rechtsklick auf den Bereich rufen Sie ein kontextsensitves Menü auf, dass es Ihnen ermöglicht die Knoten auf- oder zuzuklappen bzw. den ausgewählten Knoten oder alle zu kopieren.

Das Register **Pakete** beinhaltet ferner eine kleine Werkzeugleiste, wie unten gezeigt:

Sie können die Position des Dekoderfensters verändern, indem Sie auf einen der drei Button dieser Werkzeugleiste klicken (das Dekoderfenster kann unten, links- oder rechtsbündig ausgerichtet werden). Der vierte Button führt ein automatisches Scrollen in der Paketliste zum zuletzt empfangenen Paket durch. Der fünfte Button läßt das auswählte Paket weiterhin sichtbar bleiben (z. B. wenn neue Pakete ankommen). Der sechste Button ermöglicht Ihnen den Inhalt des aktuellen Paket-Buffers in einem neuen Fenster zu öffnen. Diese Funktionalität ist äußerst brauchbar bei schwerer Netzwerkbelastung, gerade wenn die Paketliste rasch scrollt und es schwierig ist, Pakete zu untersuchen, bevor Sie den sichtbaren Bereich wieder verlassen. Klicken auf diesen Button erzeugt einen Schnappschuss des Puffers, sodass Sie den Puffer in einem separaten Fenster untersuchen können. Sie können soviele Schnappschüsse erzeugen wie Sie möchten.

Ein Rechtsklick auf diePaketliste öffnet ein Kontextmenü mit den folgenden Befehlen:

- **TCP-Sitzung rekonstruieren** – Ermöglicht Ihnen die Rekonstruktion einer TCP Session ausgehend vom gewählten Paket; dabei öffnet sich ein Fenster, das die ganze Kommunikation zwischen zwei Hosts darstellt.
- **Rekonstruiere UDP-Stream** – Ermöglicht Ihnen vom ausgewählten Paket ausgehend, einen UDP-Stream zu rekonstruieren; es wird ein Fenster eingeblendet, in dem die gesamte Konversation zwischen zwei Hosts angezeigt wird.
- **Schnellfiltern** – Findet die zwischen zwei ausgewählten MAC- bzw. IP-Adressen oder Ports gesendeten Pakete und zeigt diese in einem neuen Fenster an.
- **Paket(e) in neuem Fenster öffnen** – Ermöglicht Ihnen ein oder mehrere Pakete, für eine komfortable Untersuchung, in einem neuen Fenster zu öffnen.
- **Kennname anlegen** – Öffnet ein Fenster in dem Sie leicht zu merkende Kennnamen den MAC- bzw. IP-Adressen zuordnen können.
- **Kopiere Adresse** – Kopiert die Quell-MAC-Adresse, Ziel-MAC-Adresse, Quell-IP-Adresse, oder die Ziel-IP-Adresse in die Zwischenablage.
- **Kopiere Paket** – Kopiert die Rohdaten des ausgewählten Paketes in die Zwischenablage.

- **Paket(e) speichern unter** – Speichert die Inhalte der ausgewählten Pakete in eine Datei. Dieser Dialog lässt Sie dabei das Format aus einer Dropdown-Liste auswählen.
- **SmartWhois** – Sendet die ausgewählte Quell-/Ziel-IP-Adresse zu SmartWhois, sofern dies auf Ihrem System installiert ist. SmartWhois ist eine selbstständige Anwendung, die von Tamosoft entwickelt wurde. SmartWohis ist in der Lage Informationen über jede IP-Adresse bzw. jeden Hostnamen auf der Welt zu erlangen. Die Anwendung zeigt dabei automatisch die zu einer IP-Adresse gehörenden Informationen, wie die Domäne, den Netzwerknamen, das Land, den Bundesstaat bzw. den Bezirk und die Stadt. Dieses Programm kann von der Tamosoft-Webseite heruntergeladen werden. Diese Option is für nicht-IP-Pakete deaktiviert.
- **Packetpuffer leeren** – Löscht die Inhalte des Programmspeichers. Der Inhalt des Registers Pakete wird auch gelöscht, so dass Sie nicht mehr die bisher erhaltenen Pakete ansehen können.
- **Decodieren als** – Für TCP- und UDP-Packete. Dies ermöglicht es, unterstützte Protokolle, welche nicht standardisierte Ports verwenden zu decodieren. Wenn z.B. Ihr SOCKS-Server auf Port 333 statt 1080 läuft, so können Sie ein Paket der SOCKS-Session wählen und dann über dieses Menü veranlassen, dass CommView for WiFi alle Pakete auf Port 333 als SOCKS-Pakete erkennt. Solche Protokollumbenennungen sind jedoch nicht permanent und nur aktiv bis das Programm beendet wird. Beachten Sie bitte, dass Sie Standardprotokollpaare nicht umdefinieren können. So kann CommView for WiFi Pakete auf Port 80 nicht als TELNET Pakete erkennen.
- **Schrift** – Erlaubt Ihnen die Schriftgröße für Paketanzeige zu verkleinern oder zu vergrößern, dies hat keine Auswirkung auf alle anderen Elemente der Bedienoberfläche.

Ausgewählte Pakete können über Drag&Drop auf den Desktop gezogen werden.

Logging

Dieses Register dient dem Speichern empfangener Pakete in eine Datei auf die Festplatte. CommView for WiFi speichert dabei die Pakete in einem eigenen Format mit der Endung NCF. Sie können diese Dateien jederzeit mit dem **Logbetrachter** anschauen bzw. einfach auf die NCF-Datei doppelklicken, um sie zu laden und zu decodieren. NCF ist ein offenes Format; Mehr dazu unter **CommView-Logdateiformat** für detaillierte NCF-Formatbeschreibungen.

Speichern und Verwalten

Mit diesem Bereich können Sie die empfangenen Pakete manuell abspeichern und abgespeicherte Dateien verbinden bzw. splitten. Alle im Speicher befindlichen Pakete oder ein ausgewählter Bereich können abgespeichert werden. Die Felde **Von** und **Bis** ermöglichen Ihnen die erfordeliche Reihe zu setzen, die sich auf Paketnummern basiert, wie im Register Pakete angezeigt ist. Klicken Sie auf **Speichern unter…** um einen Dateinamen auszuwählen. Um manuell mehrere NCF-Dateien

in eine große Datei zu verbinden, klicken Sie auf **Logs zusammenfügen…** Um zu groß geratene NCF-Dateien zu splitten, klicken Sie auf **Logs splitten…** Das Programm wird Sie dann so führen, dass Sie die Dateien in der gewünschten Größe erhalten.

Autospeicherung

Wählen Sie diese Checkbox, damit das Programm die empfangenen Pakete automatisch bei der Ankunft abspeichert. Mittels des Feldes **Maximale Verzeichnisgröße** legen Sie die Größe der im Logverzeichnis gespeicherten Informationen fest. Wenn diese Größe überschritten wird werden zuerst die ältesten Daten überschrieben. Mit dem Feld **Durchschnittliche Logdateigröße** geben Sie die ungefähre Größe einer Logdatei vor. Wenn die Logdatei diese vorgegebene Größe erreicht, wird automatisch eine neue Logdatei erzeugt. Um das standardmässige Logverzeichnis zu ändern, wählen Sie mittels Log Speichern unter: einen neuen Pfad.

> Wenn Sie ein wichtiges empfangenes Datenpaket lange aufbewahren wollen, sollten Sie es nicht im Standardlogpfad ablegen, denn es könnte durch neuere Daten überschrieben werden. Verschieben Sie die Datei zur Aufbewahrung in ein anderes Verzeichnis.

Bedenken Sie, dass das Programm nicht automatisch jedes Paket nach dessen Empfang abspeichert. Dies bedeutet, wenn Sie die Logdateien in Echtzeit ansehen, die letzten Pakete fehlen können. Um den Puffer in die Logdateien zu schreiben, klicken Sie entweder **Erfassung stoppen** oder deaktivieren Sie die Checkbox **Autospeicherung**.

WWW-Zugriff-Protokollierung

Aktivieren Sie diese Checkbox um das Logging von HTTP-Sitzungen zu starten. Mittels des Feldes **Maximale Dateigröße** begrenzen Sie die Größe der Logdatei. Wenn diese Grenze überschritten wird, werden zuerst die ältesten Logdateien überschrieben. Um den Standardlogdateinamen bzw. -pfad zu ändern, klicken Sie auf die Funktion **Logdateien speichern unter:** und wählen Sie dann einen neuen Namen. Logdateien können im **HTML** - oder **TXT**-Format erzeugt werden. Mittels eines Klicks auf **Konfiguration…** können Sie die Standard-Logging-Optionen ändern. Sie können die Portnummer für den HTTP-Zugang ändern (der Standardwert von 80 funktioniert vielleicht nicht bei Ihnen, da Sie hinter einem Proxy sind) und bestimmte Datentypen ausschließen (in der Regel ist es sinnlos, etwas anderes als HTML-Seiten zu speichern; deswegen empfiehlt es sich, die URLs von Bildern aus der Logdatei auszuschließen).

Logbetrachter

Der Logbetrachter ist ein Werkzeug zum Betrachten und Erforschen von Dateien, die von CommView for WiFi oder anderen Paket-Analyzern gesammelt wurden. Es hat die Funktionaltiät des Registers **Pakete** im Hauptfenster, im Unterschied zum Register **Pakete**, zeigt der Logbetrachter geladene Pakete von auf der Festplatte befindlichen Dateien eher an als die in Echtzeitanzeige erfassten Pakete.

Um den Logbetrachter zu öffnen klicken Sie im Hauptfenster auf **Datei => Logbetrachter** oder doppelklicken Sie auf eine CommView for WiFi Erfassungsdatei, die Sie bereits abgespeichert haben. Sie können beliebig viele Logbetrachterfenster öffnen, und jedes davon kann zur Analyse eines oder mehrerer Dateien heranziehen.

Der Logbetrachter kann auch zur Analyse von Dateien auch anderer Paket-Analyzer und Personal Firewalls benutzt werden. In der aktuellen Version können Dateien aus Network Instruments Observer®-Network General Sniffer® for DOS/Windows-, Microsoft® NetMon-, WildPackets EtherPeek™-, AiroPeek™-, Wireshark/Tcpdump- und Wireshark/pcapng-Formate importiert werden. Diese Formate werden auch oft in Drittherstellerprodukten verwendet. Der Protokollbetrachter besitzt die Fähigkeit Paketdaten durch Dateierzeugung in Network Instruments Observer®-, Network General Sniffer® für DOS/Windows-, Microsoft® NetMon-, WildPackets EtherPeek™-, AiroPeek™-, Wireshark/Tcpdump und Wireshark/pcapng-Formate zu erzeugen, aber auch im eigenen CommView-Format.

Die Verwendung des Logbetrachters ist analog zum Register **Pakete** im Hauptfenster; Mehr dazu im Kapitel Pakete.

Logbetrachtermenü

Datei

- **CommView Logs laden** – Öffnet eine oder mehrere CommView-Erfassungsdateien.
- **Logs importieren** – Importiert Dateien aus anderen Paket-Analyzern.
- **Logs exportieren** – Exportiert die angezeigten Pakete in andere Formate.
- **Fenster leeren** – Löscht den Inhalt der Paketliste.
- **Statistiken generieren** – Lässt CommView-Statistiken über die im Logbetrachter befindlichen Pakete erzeugen. Ferner können auch die im **Statiskfenster** angezeigten Daten gelöscht werden. Diese Funktion zeigt keine Zeitreihenanalyse. Sie zeigt nur Summen, Protokollkarten und LAN-Host-Tabellen.
- **An VoIP-Analyser senden** – sendet alle Paket vom aktuellen Protokollanzeigefenster zu einem neuen **VoIP-Protokollanzeigefenster** für eine VoIP-spezifische Analyse.
- **Fenster schliessen** – Schließt das Fenster.

Suchen

- **Finde Paket** – Dieser Dialog ermöglicht es Pakete zu finden, die einen bestimmten Text enthalten.
- **Gehe zu Paket Nummer** – Mit diesem Dialog springen Sie zu einer definierten Paketnummer.

Regeln

- **Anwenden** – Wendet die aktuellen Regeln auf die im Logbetrachter gezeigten Pakete an. Als Folge werden die nicht mehr passenden Pakete gelöscht. Dies ändert jedoch nicht die gespeicherte Datei.
- **von Datei…** – Analog zu Anweden, allerdings verwenden Sie hier ein bereits gespeichertes Regelset (RLS-Datei) anstatt der aktuellen Regeln.

Regeln

CommView for WiFi erlaubt Ihnen die Definition von zwei Regeltypen:

1. Der erste Typ (**Wireless-Regeln**) ermöglicht es, auf dem Wireless-Pakettyp basierende Pakete zu filtern:**Daten**-,**Management**- und **Kontrollpakete**. Um den Empfang dieses Pakettyps zu aktivieren/deaktivieren, verwenden Sie im Programmmenü **Regeln** bzw. die entsprechenden Werkzeugleisten-Buttons. Ferner können Sie mit dem Menü **Ignoriere Beacons** den Empfang von Beacon-Paketen ein- bzw. abschalten.
2. Der zweite Typ (**Klassische Regeln**) ermöglicht es, Pakete nach vielen Kriterien zu filtern, wie der Portnummer oder der MAC-Adresse. Um diesen Regeltyp zu verwenden, gehen Sie im Hauptfenster in das Register **Regeln**. Wenn eine oder mehrere Regeln festgelegt werden, filtert das Programm die Pakete danach und zeigt dann nur die regelkonformen Pakete an. Wenn eine Regel gewählt ist, wird die entsprechende Seite mit hervorgehobenem Font angezeigt.

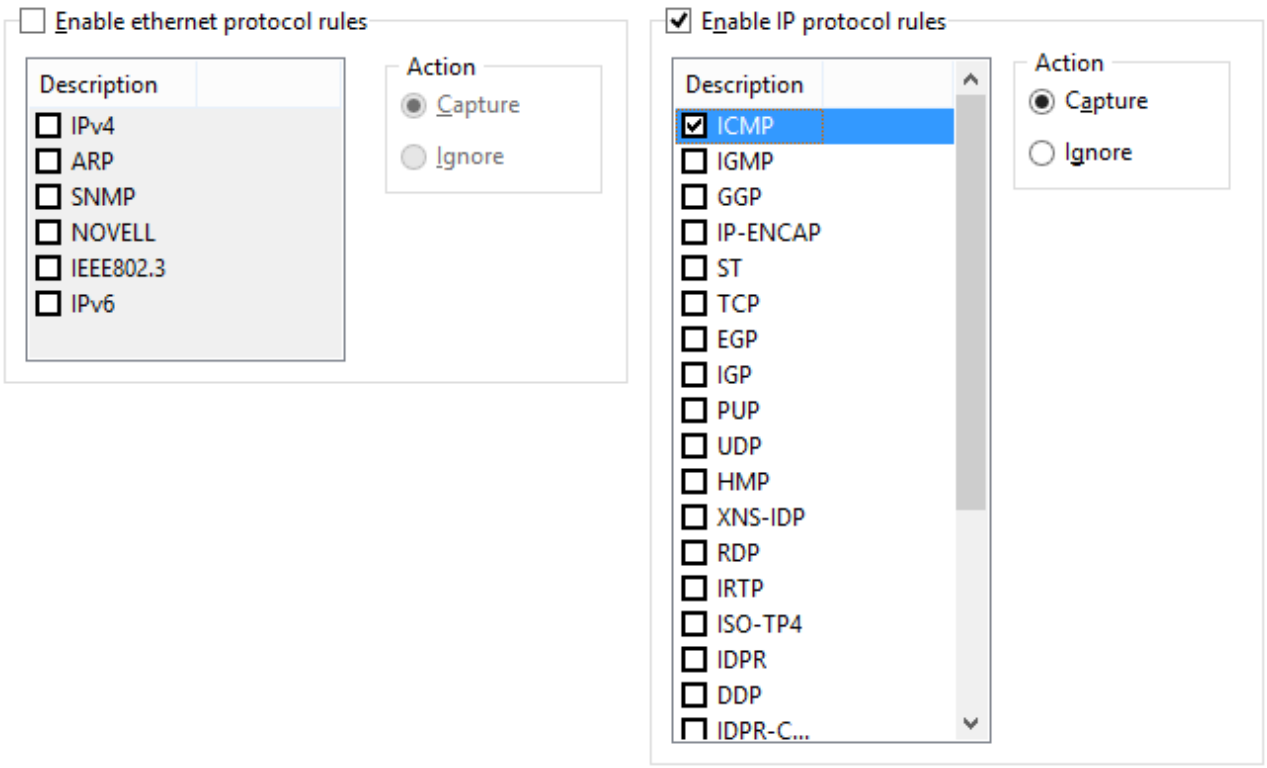
Im Statusbalken des Programms wird die Anzahl der aktiven klassischen Regeln angezeigt. Bitte beachten Sie, dass dies nicht die Anzahl der aktiven WLAN-Regeln zeigt, da der Status der Werkzeugleiste (Ein/Aus) klar zeigt, ob eine solche Regel aktiv ist oder nicht. Wireless-Regeln werden vor allen anderen Dingen aktiv. Jedes erfasste Paket muss zuerst die Wireless-Regeln passieren bevor ein weiterer Prozess stattfindet. So wird z. B. kein Paket durch das Programm angezeigt, wenn keiner der drei Wireless-Werkzeugleisten-Buttons betätigt wurde.

Sie können mittels der Regeln im Programmmenü Ihre Regeleinstellungen in einer Datei speichern und später wieder laden.

Da WLAN-Verkehr oft eine große Zahl von Datenpaketen erzeugt, empfehlen wir die Verwendung von Regeln, um nicht benötigte Pakete auszuschließen. Dadurch werden die benötigten Systemressourcen gesenkt. Wenn Sie eine Regel aktivieren bzw. deaktivieren wollen, wählen Sie den entsprechenden Teil im linken Teil des Fensters (z. B. **IP-Adressen** oder **Ports**) und deaktivieren Sie die Checkbox, die zur Regel gehört (z. B. **Aktiviere IP-Adressenregeln** bzw. **Aktiviere Portregeln**). Die verfügbaren Regeltypen sind unten beschrieben.

Protokolle

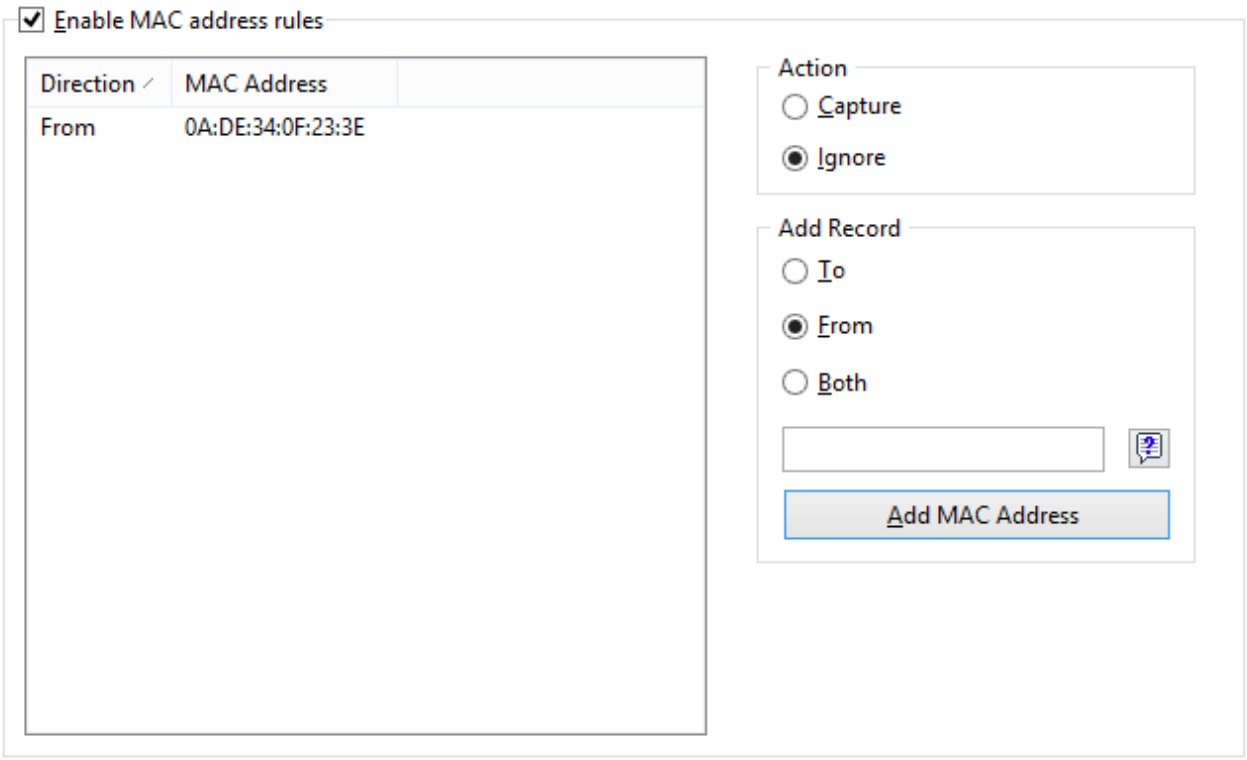
Der Dialog ermöglicht das Ignorieren/Empfangen von Paketen basierend auf den Ethernet (Layer 2)- und IP (Layer 3)-Protokollen.



Dieses Beispiel zeigt, wie man nur ICMP- und UDP-Pakete empfängt. Alle anderen Pakete der IP-Familie werden ignoriert.

MAC-Adressen

Der Dialog ermöglicht das Empfangen/Ignorieren von Paketen basierend auf MAC-Adressen (Hardware). Fügen Sie eine MAC-Adresse in das Eingabefeld **Datensatz hinzufügen** ein, wählen die Richtung (**Nach, Von** oder **Beides**) und klicken auf **MAC-Adresse hinzufügen**. Die neue Regel wird angezeigt. Wählen Sie die durchzuführende Aktion, wenn ein neues Paket verarbeitet wird: Das Paket kann ignoriert oder erfasst werden. Sie können auch auf den Button MAC-Kennname klicken, um eine Liste der Kennnamen zu erhalten. Doppelklicken Sie auf einen Kennnamen, den Sie hinzufügen wollen. Die MAC-Adresse wird der Eingabeliste hinzugefügt.

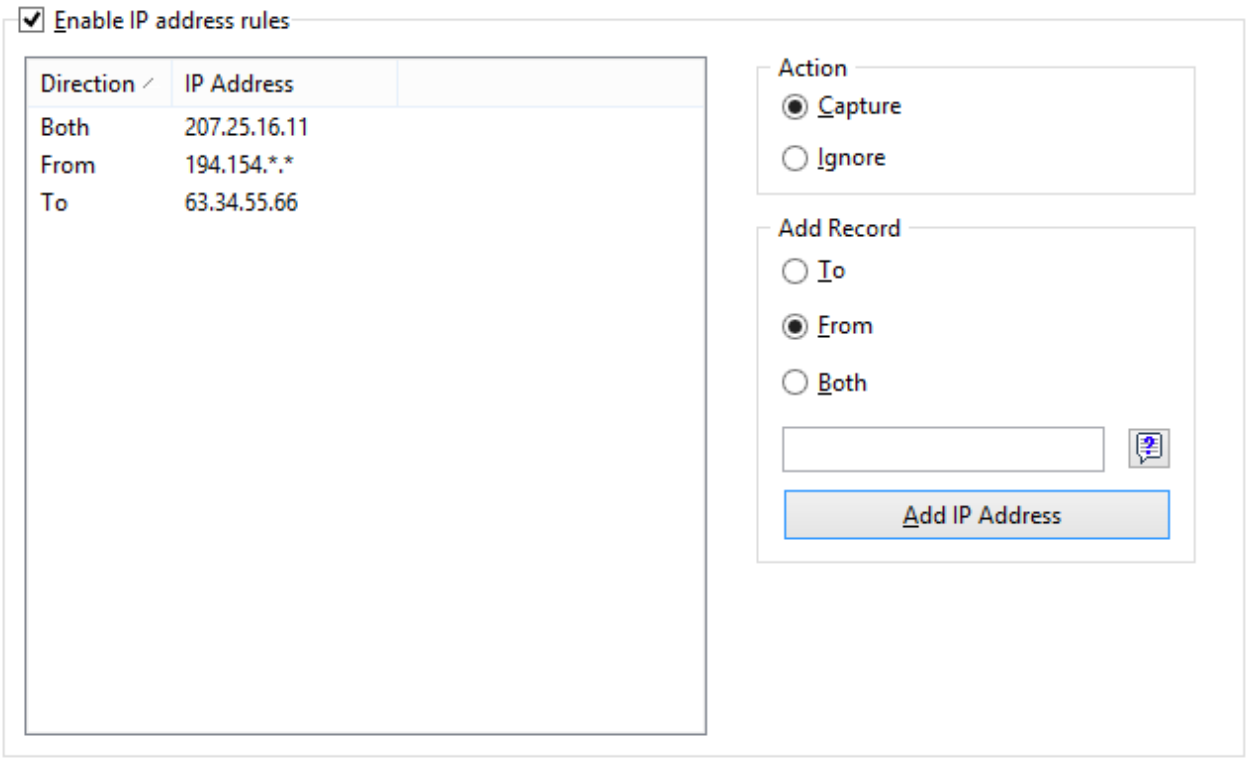


Dieses Beispiel zeigt, wie man das Programm Pakete ignorieren läßt, die von 0A:DE:34:0F:23:03E kommen. Alle Pakete von anderen MAC-Adressen werden empfangen.

IP-Adressen

Mit diesem Dialog können Pakete basierend auf IP-Adressen ignoriert oder empfangen werden. Geben Sie einfach eine IP- oder IPv6-Adresse im Bereich **Datensatz hinzufügen** ein, wählen die Richtung (**Nach**,**Von** oder **Beides**) und klicken dann auf **IP-Adresse hinzufügen**. Sie können dabei für IP-Blöcke sogenannte Wildcards (Platzhalter) verwenden. Die neue Regel wird angezeigt. Wählen Sie die durchzuführende Aktion, wenn ein neues Paket verarbeitet wird: Das Paket kann ignoriert oder erfasst werden. Über den Button IP-Kennname können sie eine Liste von

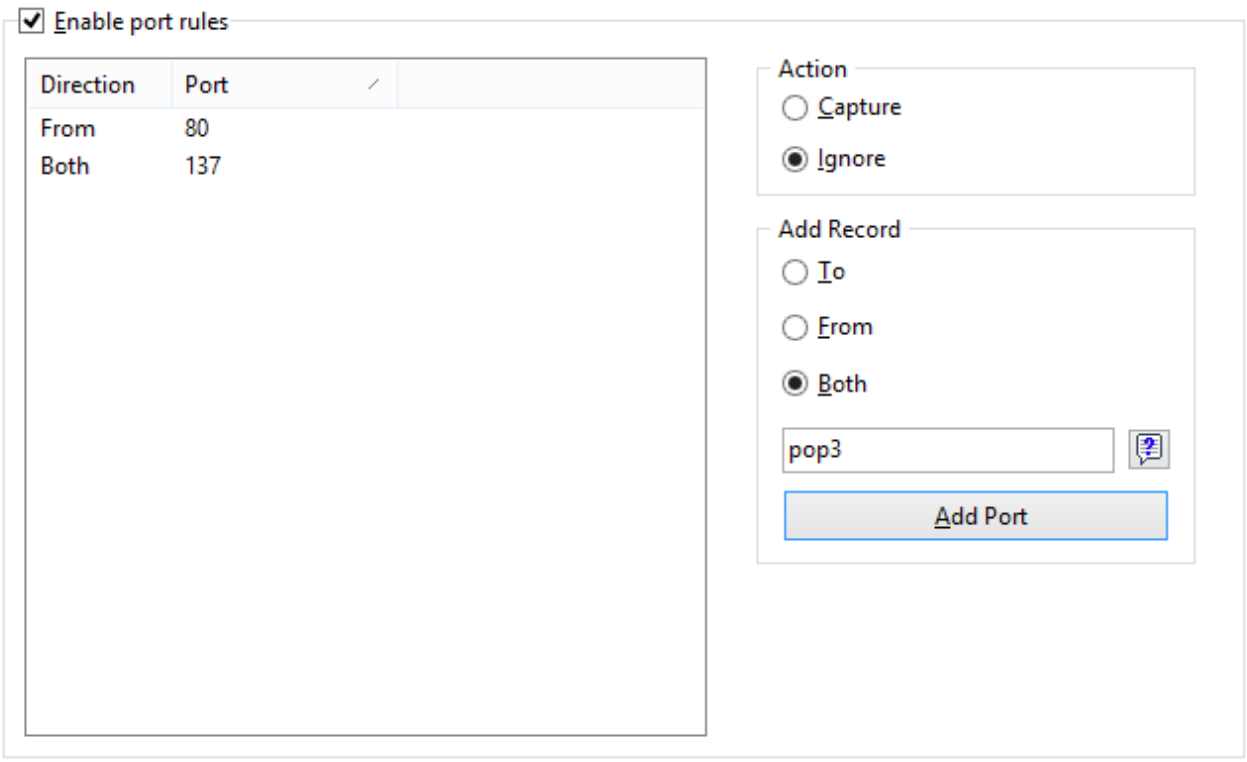
Kennnamen erhalten; Doppelklicken Sie auf den Kennnamen, den Sie hinzufügen wollen und die entsprechende IP-Adresse wird der Eingabeliste hinzugefügt.



In diesem Beispiel zeigen wir wie Sie die Pakete definieren können, die an 63.34.55.66 gehen bzw. von 207.25.16.11 und von allen Adressen im Bereich 194.154.0.0 und 194.154.255.255 kommen. Alle Pakete, die von anderen Adressen kommen, werden ignoriert. Da im IP-Protokoll IP-Adressen verwendet werden, würde eine solche Konfiguration alle Nicht-IP-Pakete automatisch ignorieren. Die Benutzung von IPv6-Adressen erfordert Windows XP oder höher und die IPv6-Stapelung muss installiert sein.

Ports

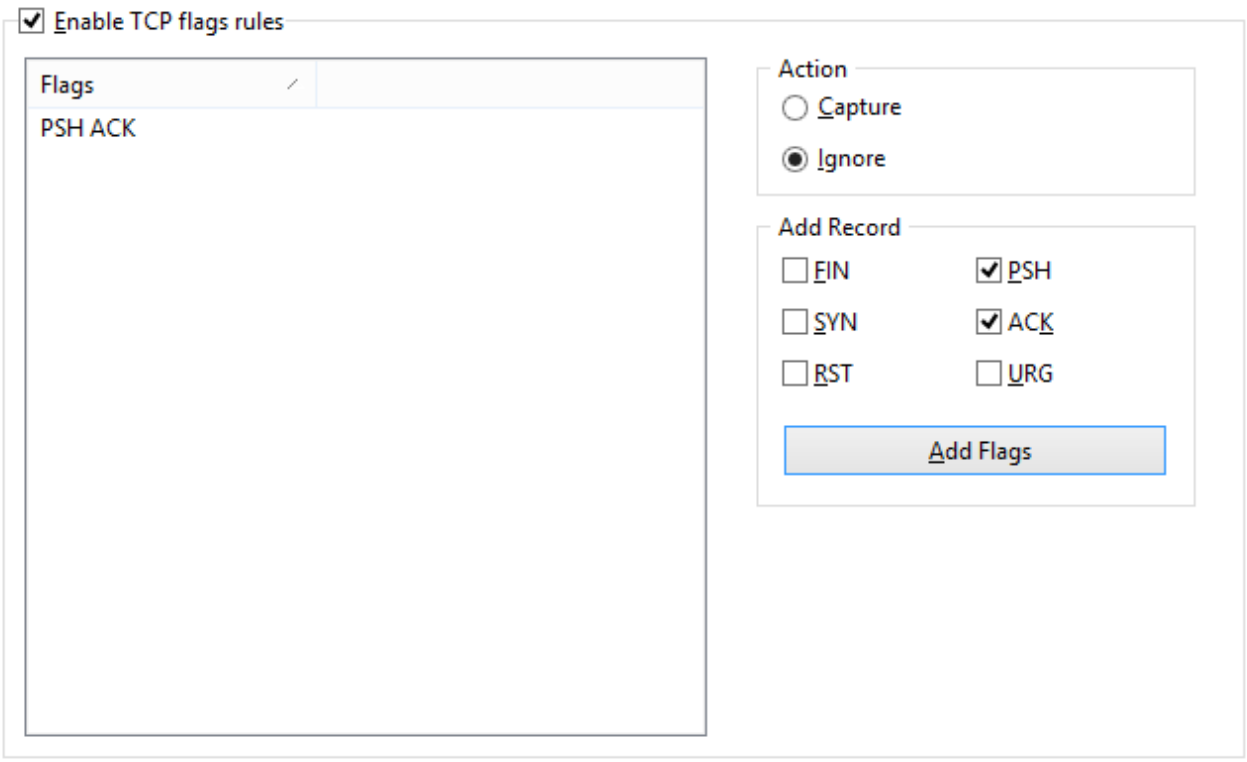
Der Dialog ermöglicht das Ignorieren oder Empfangen von Paketen über Ports. Fügen Sie einfach eine Portnummer im Bereich **Datensatz hinzufügen** ein, wählen dann die Richtung (**Nach**, **Von** oder **Beides**) und klicken **Port hinzufügen** an. Die neue Regel wird angezeigt. Wählen Sie die durchzuführende Aktion, wenn ein neues Paket verarbeitet wird: Das Paket kann ignoriert oder erfasst werden. Betätigen Sie den Button **Port Referenz** um eine Liste aller bekannten Ports zu erhalten. Doppelklicken Sie auf den Port, den Sie hinzufügen wollen und seine Portnummer wird der Eingabeliste hinzugefügt. Ports können als Text eingegeben werden, z. B. *http* oder *pop3*. Das Programm wird dann den Portnamen in einen numerischen Wert umwandeln.



In diesem Beispiel sehen Sie, wie Sie das Programm dazu bringen Pakete von Port 80 kommend bzw. zu Port 137 gehend zu ignorieren. Diese Regel verhindert, dass CommView for WiFi eingehenden HTTP-Verkehr bzw. ein- und ausgehenden NETBIOS NAME Service-Verkehr anzeigt. Alle von oder zu anderen Ports gehende Pakete werden aber angezeigt.

TCP-Flags

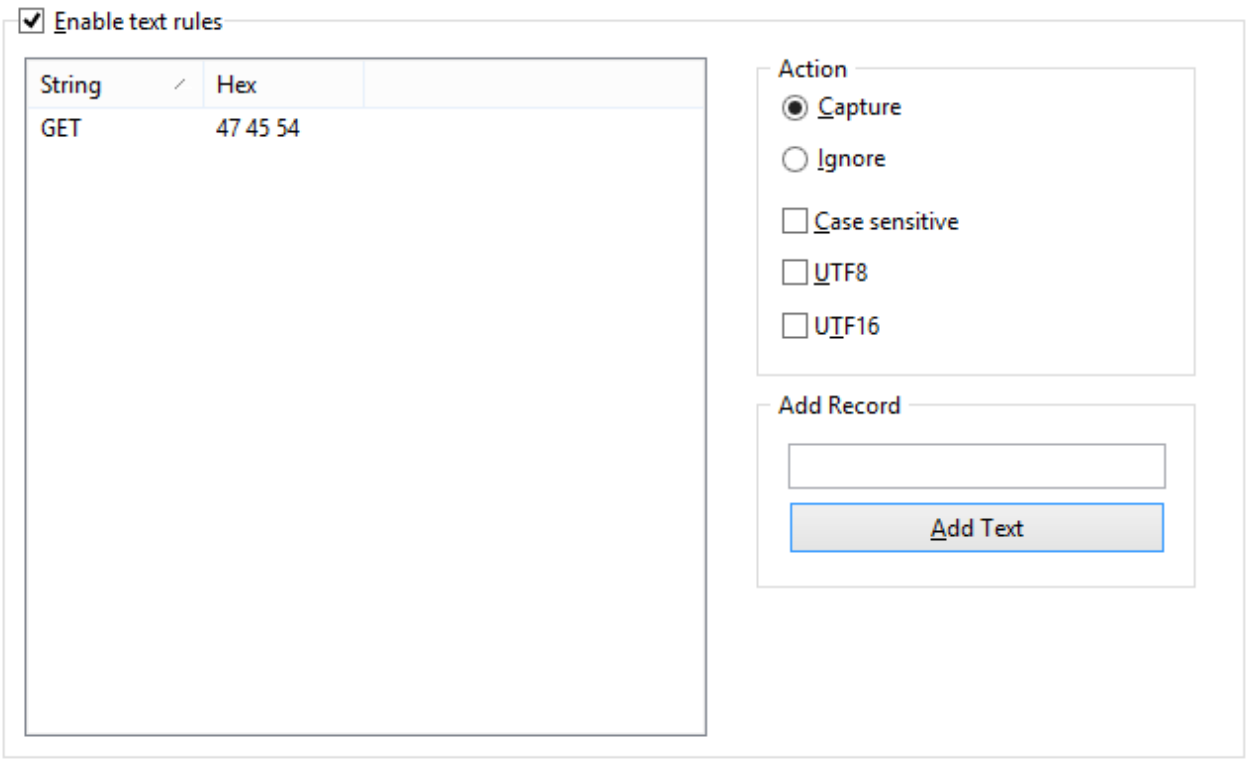
Der Dialog ermöglicht das Ignorieren oder Empfangen von Paketen basierend auf TCP-Flags. Wählen Sie eine oder mehrere Checkboxen im Bereich **Datensatz hinzufügen** und klicken Sie dann auf **Flags hinzufügen**. Die neue Regel wird angezeigt. Wählen Sie die durchzuführende Aktion, wenn ein neues Paket mit einem vorgegebenen TCP-Flag bearbeitet wird: Das Paket mit den kann ignoriert oder erfasst werden.



In diesem Beispiel sehen Sie, wie das Programm TCP-Pakete mit dem PSH ACK-Flag ignoriert. Alle Pakete mit anderen PCP-Flags werden empfangen.

Text

Der Dialog ermöglicht den Empfang von Paketen, die einen bestimmten Text enthalten. Fügen Sie den Text-String im Bereich **Datensatz hinzufügen** ein und klicken Sie dann auf **Text hinzufügen**. Die neue Regel wird angezeigt. Wählen Sie die durchzuführende Aktion, wenn ein neues Paket verarbeitet wird: Das Paket kann ignoriert oder erfasst werden.



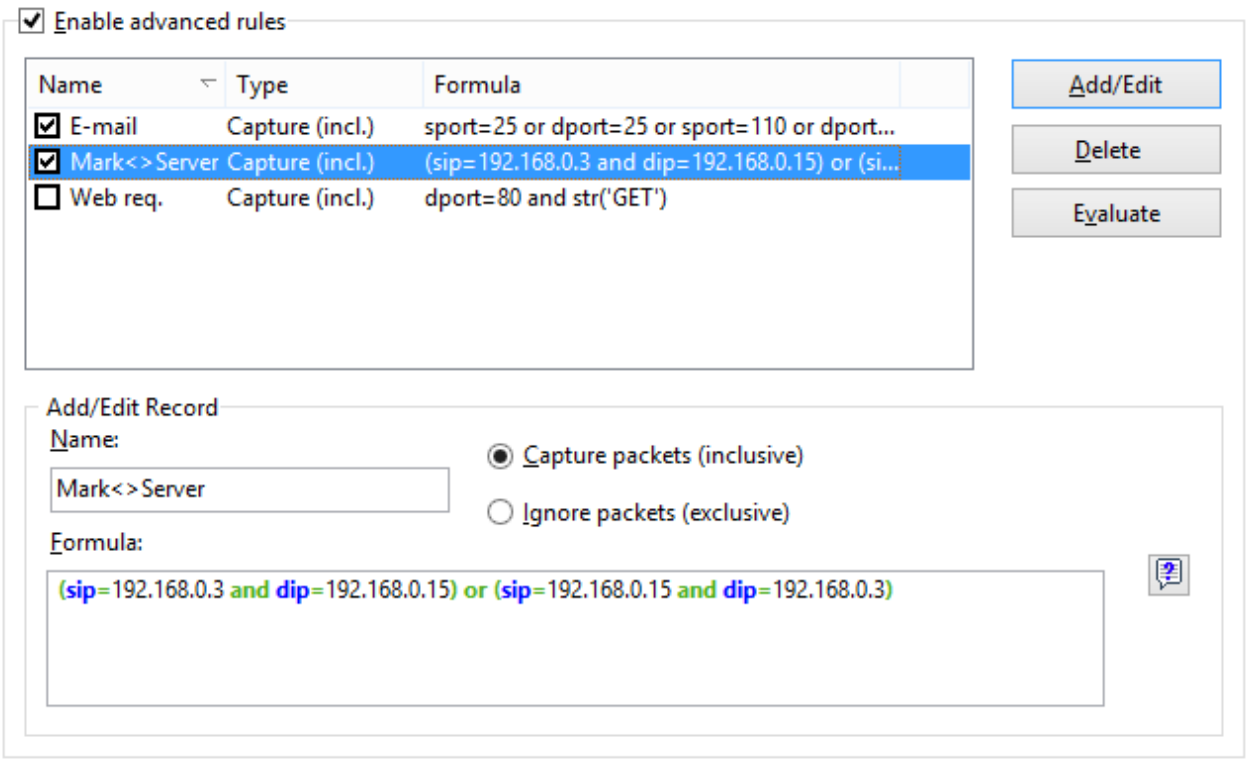
In diesem Beispiel sehen Sie, wie man das Programm dazu bringt, nur Pakete zu empfangen, die "GET" enthalten. Wählen Sie die Checkbox **Gross-/Kleinschreibung** unterscheiden, wenn die Groß- und Kleinschreibung beachtet werden soll. Wählen Sie die Checkbox **UTF8** oder **UTF16**, wenn Sie möchten, dass die Regel mit der jeweiligen Kodierung Ihres Textes übereinstimmt. Alle Pakete, die nicht den genannten Text enthalten, werden nun ignoriert. Wenn Sie eine Regel erstellen möchten, die auf hexadezimalen Bytesequenzen basiert, wenn der Text nicht druckfähig ist (z.B. 0x010203), sehen Sie im Kapitel **Erweiterte Regeln** nach.

Für Fortgeschrittene

Erweiterte Regeln sind die mächtigsten und flexibelsten Regeln, die es Ihnen ermöglichen komplexe Filter basierend auf Bool'scher Logik zu implementieren. Eine detaillierte Hilfe zu der erweiterten Regeln finden Sie im Kapitel **Erweiterte Regeln**.

Erweiterte Regeln

Erweiterte Regeln sind die mächtigsten und flexibelsten Regeln, die es Ihnen ermöglichen komplexe Filter basierend auf Bool'scher Logik zu implementieren. Um diese zu nutzen brauchen Sie grundlegende Kenntnisse in Mathematik und Logik. Die Regelsyntax ist aber leichtverständlich.



Übersicht

Um eine neue Regel hinzuzufügen müssen Sie einen beliebigen Namen im Eingabefeld **Name** eingeben, wählen Sie dann die Aktion **Pakete erfassen/ignorieren**. Geben Sie eine Formel nach der weiter unten erklärten Syntax ein und klicken anschließend auf **Hinzufügen/Editieren**. Die neue Regel wird hinzugefügt und ist augenblicklich aktiv. Es können beliebig viele Regeln hinzugefügt werden. Es sind jedoch nur die Regeln aktiv, die eine aktivierte Checkbox neben ihrem Namen haben. Die Regeln können über die entsprechenden Checkboxen aktiviert/deaktiviert werden. Zum endgültigen Löschen von Regeln verwenden Sie den Button **Löschen**. Wenn mehrere Regeln aktiv sind, können Sie das Ergebnis abschätzen, indem Sie **Auswerten** anklicken. Mehrere aktive Regeln werden über den logischen OR-Operator gekoppelt, wenn Sie also drei aktive Regeln haben, nennen wir sie REGEL1, REGEL2 oder REGEL3, ist das Ergebnis gültig, sobald mindestens eine der drei Regeln zutrifft. Wenn Sie auch negative ("Ignore") Regeln benutzen, werden sie über den logischen AND-Operator dem Ergebniss eingefügt, weil die Kopplung der negativen Regeln über den OR-Operator keinen Sinn hat.

Syntax Beschreibung

Schauen Sie in die 802.11 Standardspezifikationen für detaillierte Informationen zu den 802.11 Paket-Header-Feldern und den von ihnen akzeptierten Werten.

- **dir** – Paketrichtung. Mögliche Werte sind in (inbound), out (outbound), und pass (pass-through). Dieses Schlüsselwort ist nur für die Kompatiobillität mit der nichtdrahtlosen

Standardausgabe von CommView for WiFi. In CommView for WiFi gibt es keine inbound oder outbound Pakete, da Ihr Adapter nicht am Datenaustausch teilnimmt und nur passiv die durchgehenden Pakete überwacht.

- **etherproto** – Ethernet Protokol, das 13. und 14. Byte des Paketes. Erlaubte Werte sind Zahlen (wie *etherproto!=0x0800* für IP) oder allgemeine Kennnamen (wie *etherproto=ARP*, was gleichwertig zu 0x0806 ist).
- **ipproto** – IP Protokoll. Erlaubt sind Zahlen (wie *ipproto=0x06* für TCP) oder allgemeine Kennnamen (wie *ipproto=UDP*, was gleichwertig zu 0x11 ist).
- **smac** – Quell-MAC-Adresse. Erlaubt sind hier MAC-Adressen in Hexnotation (wie *smac=00:00:21:0A:13:00F*) oder benutzerdefinierte Kennnamen.
- **dmac** – Ziel-MAC-Addresse
- **sip** – Quell-IP- oder IPv6-Adresse. Erlaubt sind IP-Adressen in Punktnotation (wie *sip=192.168.0.1*), IP-Adressen mit Wildcards (wie *sip!=*.*.*.255*), ausgenommen für IP6-Adressen, Netzwerkadressen mit Subnet-Masken (wie *sip=192.168.0.4/255.255.255.240* oder *sip=192.168.0.5/28*), IP-Bereiche (wie *sip von 192.168.0.15 bis 192.168.0.18 oder sip in 192.168.0.15 .. 192.168.0.18*) oder benutzerdefinierte Kennnamen. Die Benutzung von IPv6-Adressen erfordert Windows XP oder höher und die IPv6-Stapelung muss installiert sein.
- **dip** – Ziel-IP-Adresse.
- **sport** – Ausgangs-Port für TCP- und UDP-Pakete. Erlaubt sind Zahlen (wie *sport=80* für HTTP), Bereiche (wie *sport von 20 bis 50* oder *sport in 20..50* für alle Portnummer zwischen 20 und 50) oder die vom Betriebssystem definierten Kennnamen (wie *sport=ftp*, was gleichwertig zu 21 ist). Um die Liste aller Betriebssystemkennnamen zu erhalten klicken Sie bitte auf **Ansicht => Portreferenz**.
- **dport** – Ziel-Port für TCP- und UDP-Pakete.
- **flag** – TCP flag. Erlaubt sind Zahlen (wie *0x18* für PSH ACK) oder ein bzw. mehrere der folgenden Zeichen: *F* (FIN), *S* (SYN), *R* (RST), *P* (PSH), *A* (ACK) und *U* (URG) oder das Schlüsselwort has (ist). Dies bedeutet, dass das Flag einen bestimmten Wert enthält. Beispiele: *flag=0x18, flag=SA, flag has F*.
- **size** – Paketgröße. Erlaubt sind Zahlen (wie *size=1514*) oder Bereiche (wie *size from 64 to 84* oder *size in 64..84* für jede Größe zwischen 64 und 84).
- **str** – Paketinhalt. Wählen Sie dieses Argument, wenn das Paket einen bestimmten String enthalten muß. Es gibt drei Argumente: string, position und case sensitivity (Groß-/Kleinschreibung beachten). Das erste Argument ist ein String, wie *'GET'*. Das zweite Argument ist eine Zahl, welche die Stringposition (Offset) im Paket festlegt. Das Offset ist nullbasierend, d. h. wenn Sie das erste Byte des Paketes suchen, muss der Offsetwert *0* sein. Wenn das Offset ohne Bedeutung ist, wählen sie *–1*. Das dritte Argument legt die Bedeutung der Groß-/Kleinschreibung fest. Es ist entweder *false* (case-insensitive) oder *true* (case-sensitive). Das zweite und dritte Argument sind optional. Wenn hier nichts eingetragen wird

ist der Standardwert *–1* und die case-sensitivity Einstellung ist false. Beispiele: str(*'GET',-1,false*), str(*'GET',-1*), str (*'GET'*).

- **hex** – Paketinhalt. Verwenden Sie diese Funktion, wenn das Paket bestimmte Hexadezimalwerte enthalten muß. Diese Funktion hat zwei Argumente: Hexmuster und Position. Das erste Argument ist ein Hexwert, wie *0x4500*. Das zweite Argument ist eine Zahl, welche die Musterposition (Offset) im Paket definiert. Das Offset ist nullbasierend, d. h. wenn Sie das erste Byte des Paketes suchen, muss der Offsetwert *0* sein. Wenn das Offset ohne Bedeutung ist, wählen sie *–1*. Das zweite Argument ist optional, wenn es weggelassen wird, ist die Standardeinstellung *–1*. Beispiele: *hex(0x04500, 14)*, *hex(0x4500, 0x0E), hex (0x010101)*.
- **bit** – Paketinhalt. Mit dieser Funktion ermitteln Sie, ob ein bestimmtes Bit eines definierten Offsets auf 1 gesetzt ist, so dass die Funktion true ausgegeben wird. Sollte das definierte Bit 0 sein oder außerhalb der Paketgrenzen liegen, so ergibt die Funktion false. Diese Funktion hat zwei Argumente: Bit-Index und Byte-Position. Das erste Argument ist der Bit-Index im Byte. Die erlaubten Werte sind hier im Bereich 0-7. Der Index ist nullbasierend, d. h. wenn Sie das 8. Bit suchen ist der Indexwert 7. Das zweite Argument ist die Zahl, die die Byte-Position (Offset) im Paket definiert. Das Offset ist nullbasierend, d. h. wenn Sie auf das 1. Byte im Paket schauen, muss der Offset-Wert 0. Beide Argumente sind zwingend notwendig. Beispiele: *bit(0, 14) , bit(5, 1)*.
- ToDS, FromDS, MoreFrag, Retry, Power, MoreData, WEP, Order, Ftype, FsubType, Duration, FragNum, SeqNum – Zur Verwendung der 802.11-Paket-Header-Felder innerhalb der Erweiterten Regeln. Die Operatorennamen passen zu den in den 802.11-Standards festgelegten Paket-Header-Feldern. Die erlaubten Werte für ToDS, FromDS, MoreFrag, Retry, Power, MoreData, WEP und Order sind 0 oder 1. Für Ftype, FsubType, Duration, FragNum und SeqNum Operatoren sind auch andere numerische Werte gültig.

Die oben genannten Schlüsselwörter können mit den folgenden Operatoren verwendet werden:

- **and** – Bool'sche Verknüpfung.
- **or** – Bool'sche Unterscheidung.
- **not** – Bool'sche Verneinung.
- **=** – gleich.
- **!=** – ungleich.
- **<>** – ungleich.
- **>** – größer als.
- **<** – kleiner als.
- **( )** – Runde Klammer, Operatorenvorrangsregel.

Zahlen entweder in Dezimal- oder Hexadezimalschreibweise. In der Hexnotation muß 0x vor jeder Zahl stehen, z. B. *15* oder *0x0F*.

Beispiele

Folgende Beispiele zeigen die Regelsyntax. Jede Regel besitzt einen Kommentar zur Regelerklärung. Die Kommentare folgen nach zwei Schrägstrichen.

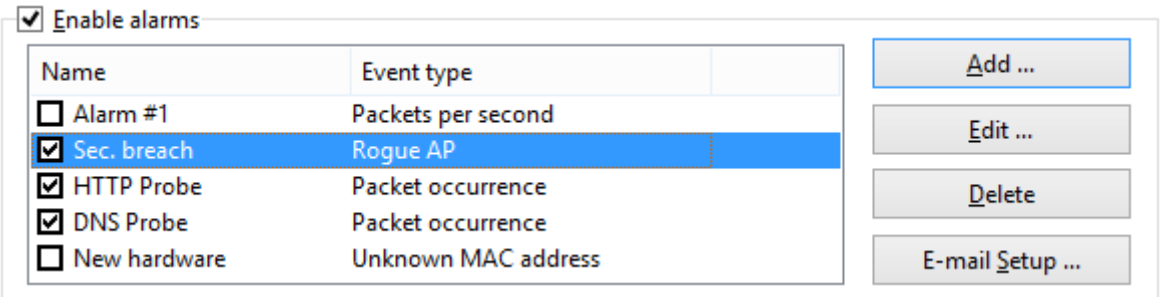
- (smac=**00:00:21:0A:13:00E** or smac=**00:00:21:0A:13:00F**) and etherproto=**arp** // Empfängt die ARP-Pakte, die von den zwei Computern 00:00:21:0A:13:00E und 00:00:21:0A:13:00F gesendet werden.
- ipproto=**udp** and dport=**137** // Empfängt die UDP-/IP-Pakete die an Port 137 gesendet werden.
- dport=**25** and str**('RCPT TO:', -1, true**) // Empfängt die TCP/IP- oder UDP/IP-Pakete, welche "'RCPT TO:" enthalten und die den Ziel-Port 25 haben.
- not (sport>**110)** // Empfängt alle Pakete, außer denen, deren Quell-Port größer als 110 ist.
- (sip=**192.168.0.3** and dip=**192.168.0.15**) or (sip=**192.168.0.15** and dip=**192.168.0.3**) // Empfängt nur die IP-Pakete, die zwischen den Maschinen 192.168.0.3 und 192.168.0.15 ausgetauscht werden. Alle anderen Pakete werden ignoriert.
- ((sip **from 192.168.0.3 to 192.168.0.7**) **and** (dip **=** 192.168.1.0/28)) and **(**flag**=**PA**)** and **(**size in 200..600**)** // Empfängt die TCP-Pakete, deren Größe zwischen 200 und 600 Bytes ist und die aus dem IP-Bereich 192.168.0.3 - 192.168.0.7 kommen, deren IP-Zieladresse im Bereich 192.168.1.0/255.255.255.240 liegt und deren TCP-Flag PSH ACK ist.
- Hex(**0x0203, 89**) **and** (dir<>**in**) // Empfängt die Pakete, die 0x0203 im Offset 89 enthalten und deren Paketrichtung nicht inbound ist.
- not(ftype**=0** and fsubtype=**8)** // Ignoriert Managementpakete des Beacon-Typs.
- ftype=**2** and wep=**1** // Empfängt unverschlüsselte Pakete.
- MoreFrag=**0** and FragNum=**0** // Empfängt unfragmentierte Pakete.

Alarme

Dieser Dialog ermöglicht es Alarme zu erzeugen, die Sie über bestimmte Ereignisse informieren, wie verdächtige Pakete, starke Bandbreitennutzung, unbekannte Adressen usw. Solche Alarme sind sehr nützlich, wenn Sie das Netzwerk auf bestimmte verdächtige Ereignisse überwachen, wie auffällige Bytemuster in den empfangenen Paketen, Portscans oder unerwartete Hardwareverbindungen.

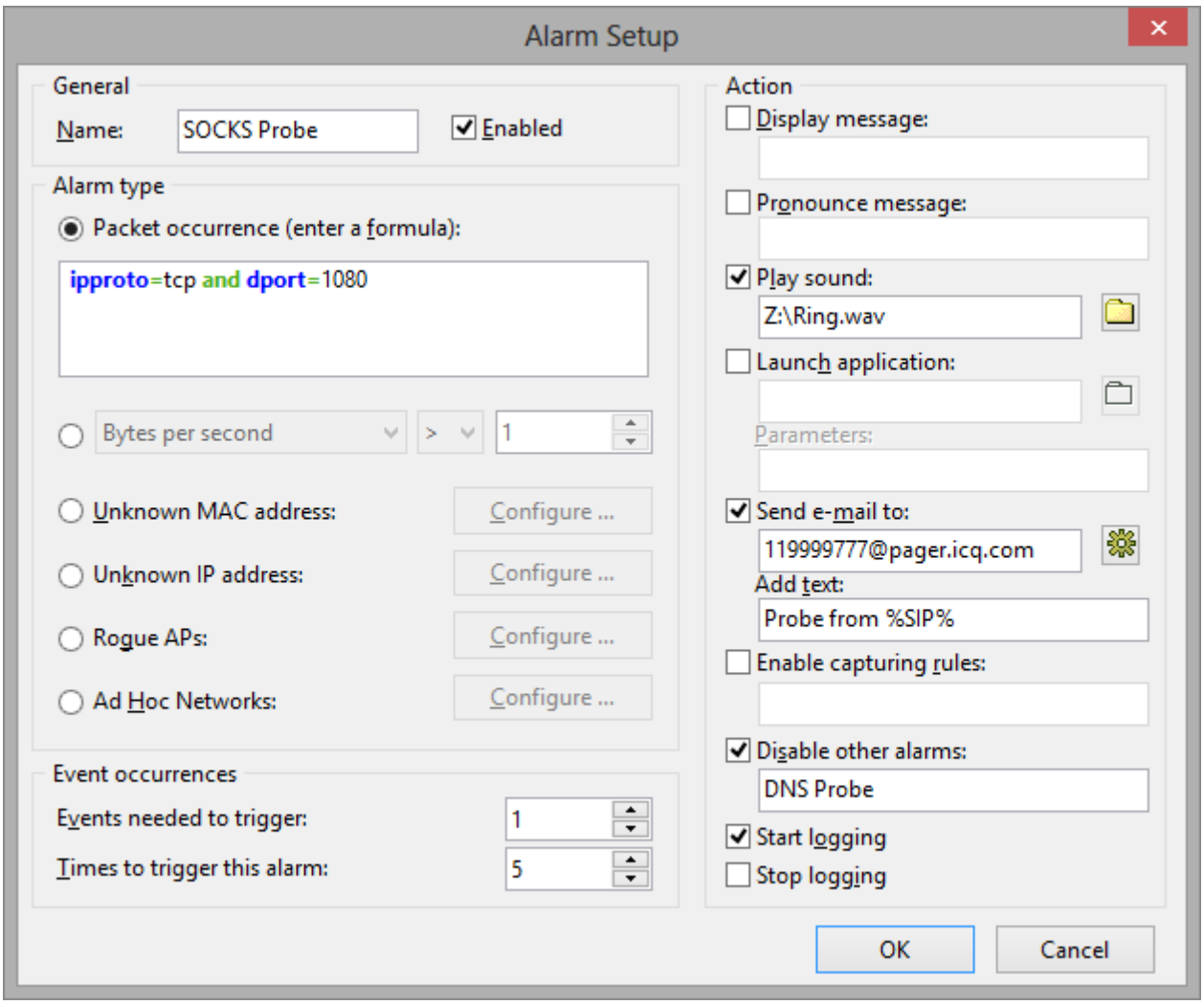
Die Alarme können nur von gefilterten Paketen ausgelöst werden. Wenn Sie z. B. das Programm so konfigurieren, dass es UDP-Pakete ausfiltert und andererseits die Alarmfunktion so einstellen, dass sie durch UDP-Pakete ausgelöst wird, so wird der Alarm nie ausgelöst.

Alarme werden über die folgende Liste verwaltet:



Jede Zeile entspricht einem separaten Alarm und diee Checkbox daneben zeigt, ob der Alarm gegenwärtig aktiv ist. Wenn ein Alarm ausgelöst wird verschwindet die Checkbox. Um einen deaktivierten Alarm wieder zu aktivieren markieren Sie erneut die Checkbox neben dem Alarmnamen. Um alle Alarme zu deaktivieren, leeren Sie die Liste **Alarme aktivieren**. Um einen neuen Alarm zu editieren oder zu löschen verwenden Sie bitte die gleichnamigen Buttons im rechten Teil des Dialogs. Mittels der Schaltfläche **E-Mail-Setup** können Informationen zu Ihrem SMTP-Server eingegeben werden, wenn Sie E-Mail-Benachrichtigung wünschen (siehe unten).

Das Alarmeinstellungsfenster wird unten gezeigt:



Das Feld **Name** sollte für die Beschreibung der Alarmfunktion genutzt werden. Aktivieren Sie die Checkbox **Aktiviert** wenn der Alarm nach dem Hinzufügen/Editieren bei Beendigung des Setup aktiviert werden soll. Diese Checkbox entspricht der in der Alarmliste. Mit dem Auswahlbereich **Alarm Typ** wählen Sie einen von zehn Alarmen aus:

- **Paket-Ereignis** – CommView for WiFi löst den Alarm aus, wenn es ein Paket empfängt, das einer bestimmten Formel entspricht. Die Formelsyntax entspricht der Syntax für die Fortgeschrittenenregeln. Mehr dazu unter **Erweiterte Regeln**.
- **Bytes/Sekunde** – Der Alarm wird ausgelöst, wenn die Byteanzahl/Sekunde einen Grenzwert über- bzw. unterschreitet. Bitte beachten Sie, dass der Wert in Bytes eingegeben werden muss, so dass bei einem gewünschten Alarm ab 1 Mbyte/Sekunde ein Wert von 1000000 eingegeben werden muss.
- **Pakete/Sekunde** – Der Alarm wird ausgelöst, wenn die Anzahl der Pakete/Sekunde einen Grenzwert über- bzw. unterschreitet.
- **Broadcasts/Sekunde** – Der Alarm wird ausgelöst, wenn die Anzahl der Broadcast-Pakete/Sekunde einen Grenzwert über- bzw. unterschreitet.

- **Multicasts/Sekunde** – Der Alarm wird ausgelöst, wenn die Anzahl der Multicast-Pakete/ Sekunde einen Grenzwert über- bzw. unterschreitet.
- **CRC Fehler/Sekunde** – Der Alarm wird ausgelöst, wenn die Anzahl der CRC-Fehler/Sekunde einen Grenzwert über- bzw. unterschreitet.
- **Erneute Versuche/Sekunde** – Der Alarm wird ausgelöst, wenn die Anzahl der Retry-Versuche (erneut Probieren)/Sekunde einen Grenzwert über- bzw. unterschreitet.
- **Unbekannte MAC-Adresse** – Der Alarm wird ausgelöst, wenn CommView for WiFi ein Paket von einer unbekannten Quell- oder zu einer unbekannten Ziel-MAC-Adresse empfängt. Mittels der Schaltfläche **Konfiguration** können Sie eine bekannte MAC-Adresse eingeben. Dieser Alarm ist nützlich, um neue unautorisierte Geräte zu erkennen, die mit Ihrem WLAN verbunden sind.
- **Unbekannte IP-Adresse** – Der Alarm wird ausgelöst, wenn CommView for WiFi ein Paket mit einer unbekannten Quell- oder Ziel-IP-Adresse oder IPv6-Adresse empfängt. Mittels des Buttons **Konfigurieren** können Sie eine bekannte IP-Adresse eingeben. Dieser Alarm ist nützlich, um unautorisierte IP-Verbindungen hinter einer Firmen-Firewall zu entdecken. Die Benutzung von IPv6-Adressen erfordert Windows XP oder höher und die IPv6-Stapelung muss installiert sein.
- **Nicht autorisierter AP** – Der Alarm wird ausgelöst, wenn CommView for WiFi ein Beacon-Paket von einem unbekannten Accesspoint empfängt. Mittels des Konfigurationsbutton Konfiguration können Sie die MAC-Adresse eines bekannten Accesspoints eingeben. Dieser Alarm ist nützlich, um unautorisierte Accesspoints zu entdecken.
- **Ad-Hoc-Netzwerk** – Der Alarm wird ausgelöst, wenn CommView for WiFi ein Beacon-Paket von einer unbekannten Ad-Hoc-Station empfängt. Benutzen Sie den Button **Konfigurieren** um MAC-Adressen bekannter Ad-Hoc-Stationen einzugeben. Dieser Alarmtyp ist nützlich zum Aufspüren unautorisierter Benutzung von Ad-Hoc-Netzwerken.

Das Eingabefeld **Erford. Anzahl Ereignisse für Alarm**: Ermöglicht Ihnen den Schwellenwert für die Ereignisanzahl festzulegen, um einen Alarm auslösen zu lassen. Wenn Sie z. B. einen Wert von 3 wählen, wird ein Alarm erst ausgelöst, wenn das entsprechende Ereignis dreimal auftaucht. Wenn Sie einen bereits existierenden Alarm editieren, wird der Zähler auf Null zurückgesetzt.

Das Eingabefeld **Max. Anzahl Auslösungen des Alarms**: Ermöglicht es Ihnen die Anzahl der Alarme festzulegen, bevor diese deaktiviert werden. Standardmäßig ist hier der Wert gleich 1, so dass nach der Alarm nach dem ersten Paketereignis deaktiviert wird. Wenn Sie diesen Wert erhöhen, wird CommView for WiFi ihn mehrmals auslösen. Wenn Sie einen Alarm editieren, wird der Zähler auf Null zurückgesetzt.

Im Bereich **Aktion** wählen sie die mit dem Alarm auszulösenden Ereignisse. Die folgenden Aktionen sind erhältlich:

%SMAC% – Quell-MAC-Adresse
%DMAC% – Ziel-MAC-Adresse
%SIP% – Quell-IP-Adresse
%DIP% – Ziel-IP-Adresse
%SPORT% – Quell-Port
%DPORT% – Ziel-Port
%ETHERPROTO% – Ethernet-Protokoll
%IPPROTO% – IP-Protokoll
%SIZE% – Paketgröße
%FILE% – Pfad zu einer temporären Datei, die das empfangene Paket enthält.

So wird z. B. in Ihrer Nachricht in der Meldung "SYN Paket von %SIP%, " wird %SIP% im aktuellen Popup-Windowtext ersetzt werden durch die Quell-IP-Adresse des alarmauslösenden Paketes. Wenn Sie die %FILE%-Variable verwenden, wird eine NCF-Datei in einem temporären Verzeichnis erzeugt. Es liegt in Ihrer Verantwortung diese Datei nach der Bearbeitung zu löschen. Sie sollten keine Variablen verwenden, wenn der Alarm ausgelöst wurde von **Bytes/Sekunde-** oder **Pakete/ Sekunde-Werten**, da diese Alarme nicht von individuellen Paketen ausgelöst werden.

- **Nachrichten anzeigen** – Zeigt eine non-modale Meldungsbox mit dem definierten Text. Mit dieser Aktion können Sie Variablen verwenden, die im Alarmfall durch die entsprechenden Parameter des Paketes, das den Alarm hervorrief, ersetzt werden. Diese Variablen sind:
- **Nachricht sprechen** – Lässt Windows, unter Benutzung der Text-to-speech engine, die Nachricht sprechen. Diese Checkbox ist abgeschaltet, wenn Ihre Windows-Version keine Text-to-speech engine besitzt. Standardmäßig kommt Windows nur mit englischen Computerstimmen, sodass Windows nicht in der Lage ist, Nachrichtentext in anderen Sprachen als englisch korreckt auszusprechen. Sie können die in der Sektion **Nachrichten anzeigen** beschriebenen Variablen im Nachrichtentext benutzen.
- **Akustisches Signal** – Spielt die gewählte WAV- Datei ab.
- **Applikation starten** – Startet die ausgewählte EXE- oder COM-Datei. Mit dem optionalen Feld **Parameter:** können in der Befehlszeile Parameter eingegeben werden. Die Variablen, die in der Sektion **Nachrichten anzeigen:** beschrieben wurden können als Befehlszeilenparameter eingegeben werden, sofern Sie möchten, dass die Anwendung Informationen über das alarmauslösende Paket empfängt und bearbeitet.
- **E-Mail senden an** – Sendet eine E-mail an eine definierte Adresse. CommView for WiFi MUSS konfiguriert werden, um Ihren SMPT-Server vor dem Senden der E-Mail nutzen zu können. Mittels des Buttons **E-Mail-Setup** neben der Alarmliste können Sie Ihre SMPT-Server-Einstellungen eingeben und eine Test-E-Mail absenden. Man kann E-Mail-Benachrichtigungen auch an Instant Messenger-Anwendungen, Handy oder Pager senden. Um z. B. eine Nachricht an einen ICQ-User zu senden, geben Sie die E-Mail-Adresse als

ICQ_USER_UIN@pager.icq.com ein, wobei ICQ_USER_UIN die eindeutige ICQ-Identifikationsnummer ist. Dazu müssen die EmailExpress Messages in den ICQ-Optionen aktiviert sein. Mehr dazu in Ihrem Instant Messenger- oder Handy-Handbuch. Das Feld **Text hinzufügen** kann zum Hinzufügen einer beliebigen Nachricht zur E-Mailbenachrichtigung genutzt werden. Sie können die in der Sektion **Nachrichten anzeigen** beschriebenen Variablen im Nachrichtentext benutzen.

- **Paketerfassungsregeln aktivieren** – Aktiviert die Erweiterten Regeln; Sie können dort eine oder mehrere Regeln eingeben. Mehrere Regeln werden komma- bzw. semikolongetrennt eingegeben.
- **Andere Alarme deaktivieren** – Deaktiviert andere Alarme; Sie sollten dabei den/die Alarmnamen angeben. Mehrere Alarme werden komma- bzw. semikolongetrennt eingegeben.
- **Logging starten** – Startet die Autospeicherung (siehe Kapitel Logging). CommView for WiFi beginnt dann Pakete auf der Festplatte abzulegen.
- **Logging stoppen** – Beendet die Autospeicherung.

Klicken Sie auf **OK** um die Einstellungen abzuspeichern und das Alarmdialogfenster zu schliessen.

Alle Ereignisse und Aktionen, die mit den Alarmen zu tun haben, finden Sie im Bereich **Ereignis-Log:** unterhalb der Alarmliste.

WEP-/WPA-Schlüssel

Der Dialog **WEP/WPA-Schlüssel** ermöglicht die Eingabe von WEP-, WPA-, oder WPA2-Schlüsseln zum Entschlüsseln der empfangenen Pakete. Ohne die Schlüssel kann das Programm verschlüsselte Datenpakete in Ihrem WLAN nicht entschlüsseln. Da einige WLAN's Mixed Mode-Verschlüsselung verwenden, bei der sowohl WEP- als auch WPA-basierende Clients sich authentifizieren können, können Sie WEP-Schlüssel und WPA-Passphrases gleichzeitig verwenden.

WEP

Mit diesem Standard können Sie bis zu vier WEP-Schlüssel verwenden, so dass Sie ein bis vier Schlüssel definieren können. Mit der Dropdown-Liste zur Schlüssellänge wählen Sie die Schlüssellänge. Unterstützte Längen sind 64, 128, 152 und 256 Bit, daher sollten Sie einen Hexadezimal-String verwenden, der entsprechend 10, 26, 32, oder 58 Zeichen lang ist.

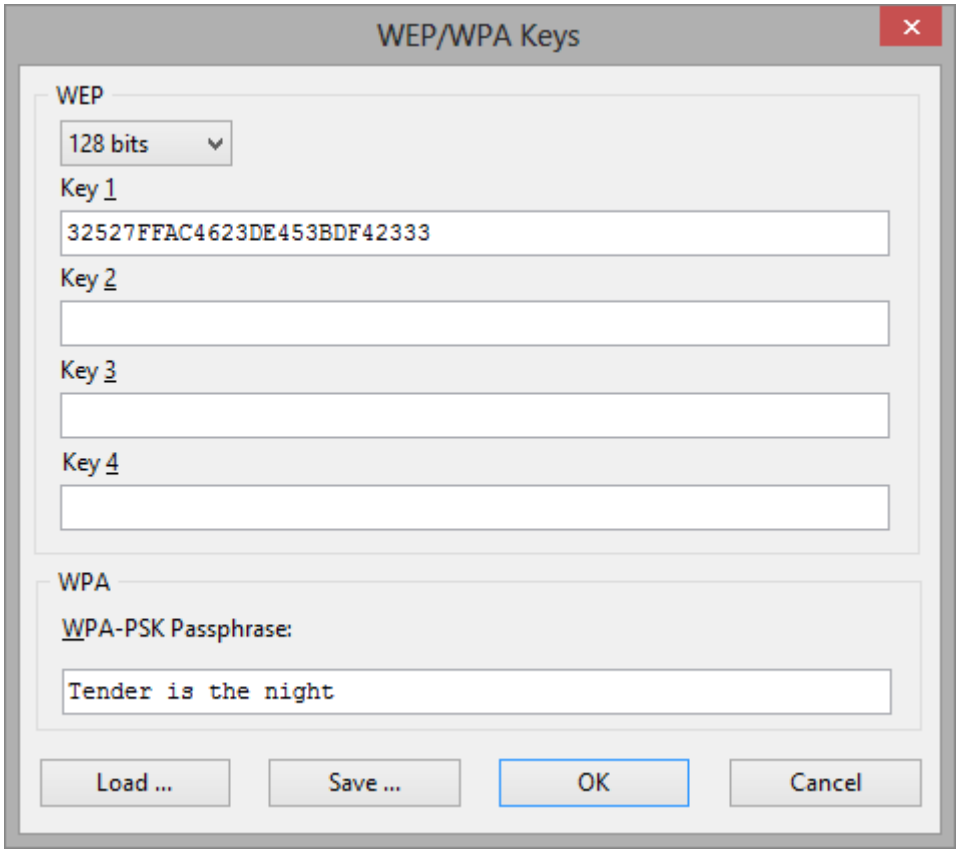
WPA

Der Wi-Fi Protected Access-Standard (WPA) definiert einige Authentifizierungs- und Verschlüsselungsarten. Davon werden aber nicht alle von CommView for WiFi unterstützt, da die

darunterliegenden Sicherheitsmodelle Einschränkungen mit sich bringen. CommView for WiFi unterstützt die Entschlüsselung von WPA oder WPA2 im Pre-Shared Key-Modus (PSK) unter Verwendung des Temporal Key Integrity-Protokolls (TKIP) oder des Advanced Encryption Standard/ Counter CBC-MAC-Protokoll (AES/CCMP) zur Datenverschlüsselung. Sie können hier eine Passphrase oder einen 64 Zeichen langen hexadezimalen Schlüssel eingeben.

Bitte beachten Sie, dass **der mit WPA3 verschlüsselte Paketverkehr nicht entschlüsselt werden kann**. WPA3 verwendet die Passphrase nur zur Authentifizierung. Entschlüsselung ist unmöglich.

Mehr über die Verarbeitung von WPA-verschlüsseltem Verkehr durch CommView for WiFi erfahren Sie im Kapitel **Hintergründe der WPA-Entschlüsselung**. Zur Eingabe einer neuen WPA-Passphrase möchten Sie vielleicht das **Knotenzuordnungswerkzeug** benutzen.

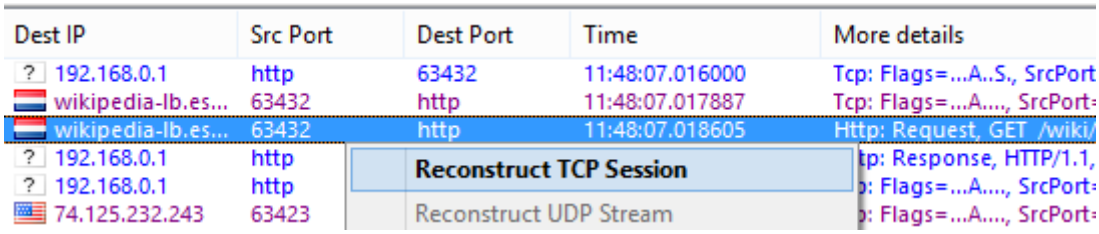


Um das aktuelle Schlüsselset zu speichern, klicken Sie bitte auf **Speichern…**. Zum Laden eines Sets klicken Sie auf **Laden…**.

Das Schlüsselset, das Sie mit diesem Dialog eingeben oder laden können, wird auf die empfangenen Pakete in Echtzeit angewandt, aber auch auf die bisher abgespeicherten NCF-Dateien. Werden empfangene Pakete in eine NCF-Datei gespeichert, werden die erfolgreich entschlüsselten Pakete auch in entschlüsselter Form abgespeichert, während die nicht entschlüsselbaren dann unverändert abgespeichert werden.

TCP-Sitzungen rekonstruieren

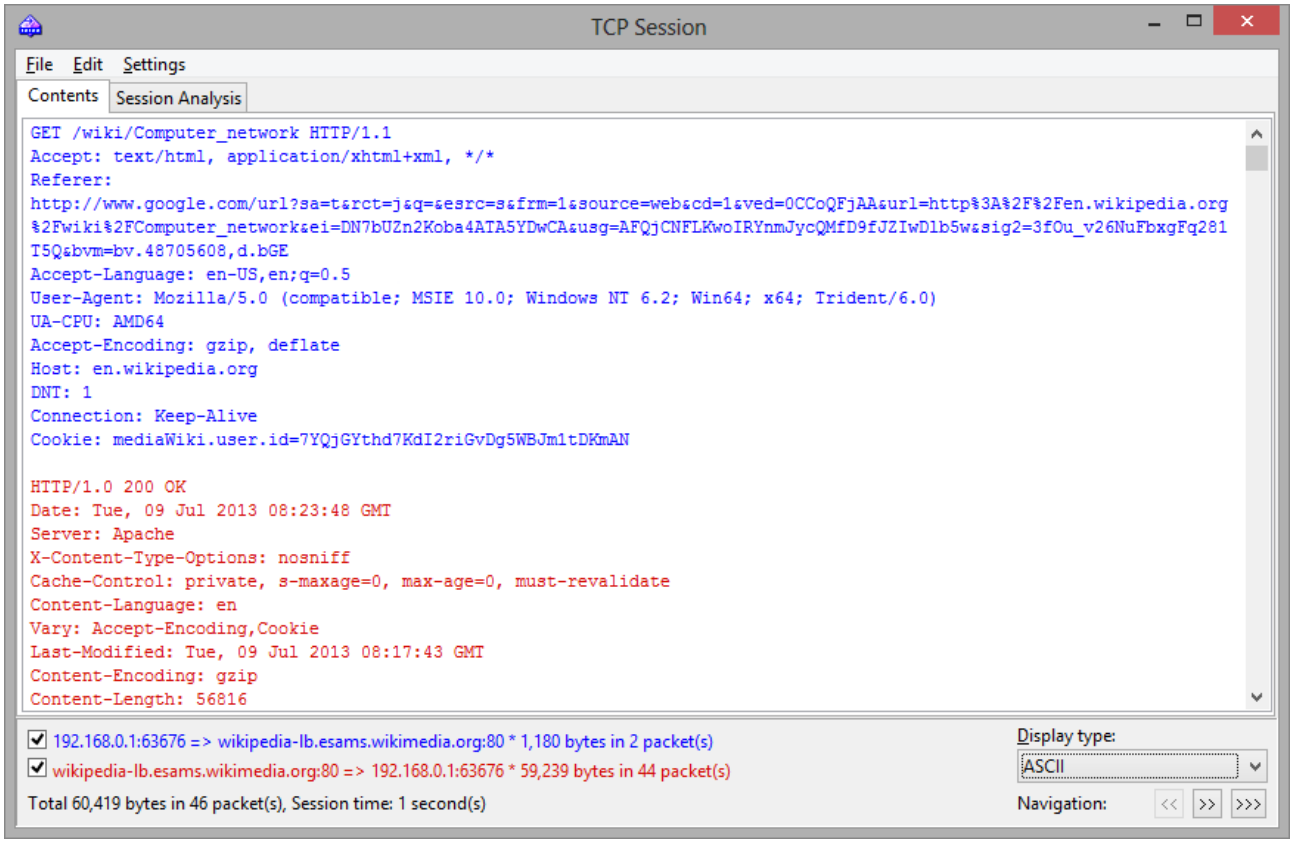
Mit diesem Dialog können Sie sich die TCP-Kommunikation zwischen zwei Host's ansehen. Um eine TCP-Sitzung zu rekonstruieren, wählen Sie als erstes ein TCP-Paket im Register **Pakete**. Abhängig von den Einstellungen (Checkbox: **Suche den Sitzungstart wenn TCP-Sitzungsrekonstruktion startet** in **Einstellungen => Optionen => Dekodierung**), wird die Sitzung von dem ausgewählten Paket ausgehend (kann ein Paket aus der Sitzungsmitte oder vom Sitzungsstart sein) rekonstruiert. Nach dem Sie das Paket gefunden und ausgewählt haben, führen Sie einen Rechtsklick darauf aus und wählen **TCP-Sitzung rekonstruieren** wie unten gezeigt:

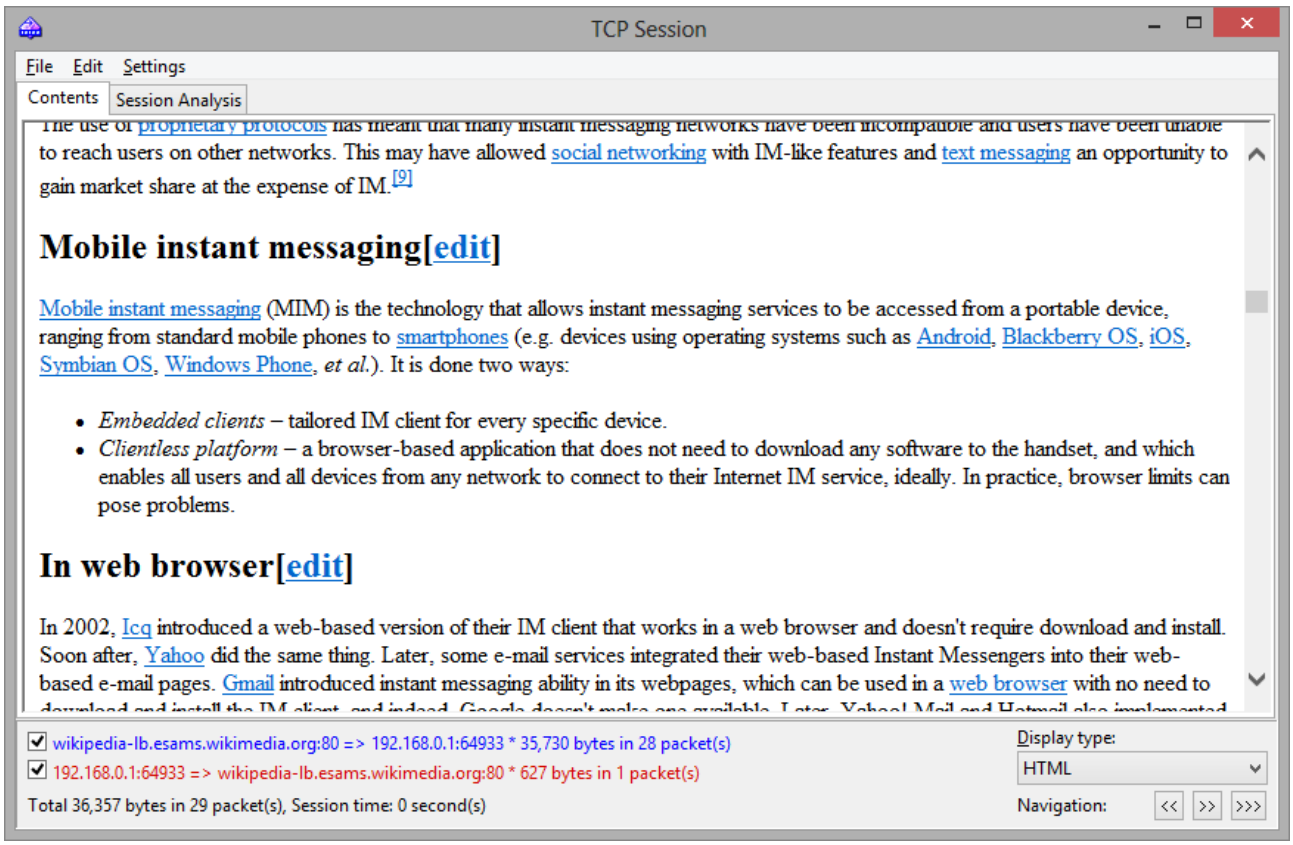


Rekonstruktionssitzungen funktionieren am besten mit textbasierten Protokollen, wie POP3, Telnet oder HTTP. Natürlich können Sie den Download einer großen Zip-Datei rekonstruieren, aber es kann sein, dass CommView for WiFi für die Rekonstruktion von mehreren Megabytes sehr lange braucht, und meist ist dann auch die erhaltene Information sinnlos.

Das Register **Inhalt** zeigt die aktuellen Sitzungsdaten an, während das Register **Sitzungsanalyse**den Fluss der rekonstruierten TCP-Sitzungen graphisch darstellt.

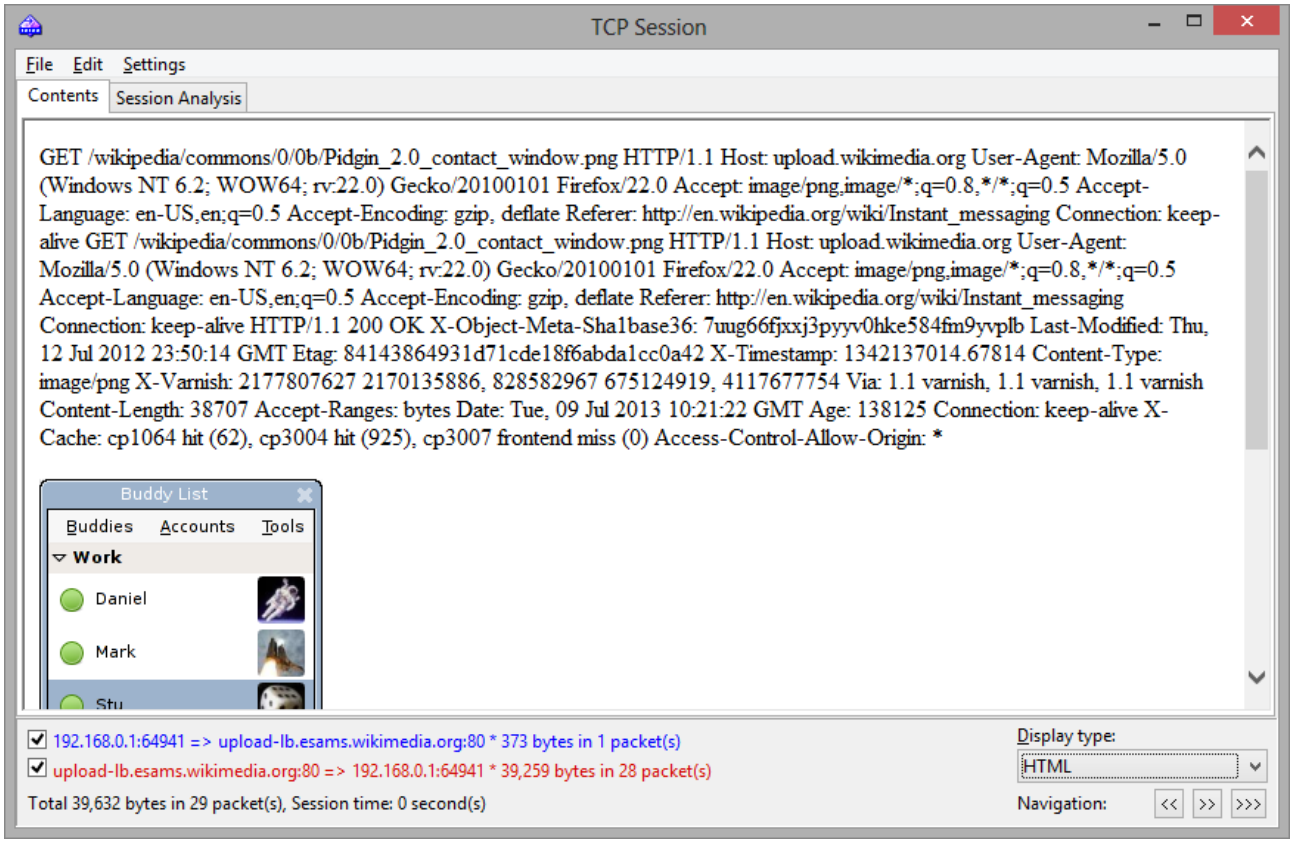
Eine Beispiel-HTTP-Session mit HTML-Daten, die im ASCII- und HTML-Modus angezeigt werden, ist im Folgenden dargestellt:





Normalerweise werden im HTML-Anzeigemodus in den HTML-Seiten keine Bilder angezeigt, da im HTTP-Protokoll Bilder separiert vom Text übertragen werden. Um diese Bilder zu sehen, müssen Sie

zur nächsten TCP-Sitzung navigieren. Im Folgenden finden Sie ein Beispiel für eine HTTP-Sitzung, die Bilder enthält und im HTML-Modus angezeigt wird:



Standardmäßig versucht CommView for WiFi GZIP-ten Webinhalt zu dekomprimieren und Bilder aus dem Binärstrom zu rekonstruieren. Diese Funktion kann im Dialog **Einstellungen** mittels des Bereichs **Decodierung** abgeschaltet werden.

Wenn Sie im unteren Bereich eine der Checkboxen deaktivieren, können Sie Daten, die aus einer bestimmten Richtung kommen ausfiltern. Ein- und ausgehende Daten sind zur besseren Erkennung durch verschiedene Farben markiert. Diese Farben können Sie mittels **Einstellungen => Farben** ändern. Wort-Wrapping kann mittels **Einstellungen => Word Wrap** aktiviert/deaktiviert werden.

Mittels der Dropdown-Liste **Anzeigetyp** können Sie die Daten in folgenden Formaten ansehen: **ASCII**- (Klartext),**HEX**- (hexadezimal), **HTML**- (Webseiten und Bilder), **EBCDIC-Format** (IBM mainframes' data encoding) und **UTF-8** (Unicode-Daten). Bitte beachten Sie, dass die Ansicht der Daten im HTML-Format nicht automatisch dasselbe Ergebniss bringt, wie mit dem Webbrowser (Sie sehen dann keine Inlinegrafik), dennoch erhalten Sie eine ungefähre Vorstellung wie die Seite im Original aussah.

Im Dialog **Optionen** können Sie unter **Decodierung** festlegen, wie der Standardanzeigetyp für die Rekonstruktion von TCP- Sessions aussieht.

Mit den Navigation-Buttons können Sie den Puffer nach der nächsten oder letzten TCP-Sitzung absuchen. Der erste Vorwärts-Button **[>>]** sucht nach der nächsten Sitzung zwischen den beiden

Hosts, die an der ersten Rekonstruktionssitzung beteiligt waren. Der zweite Vorwärts-Button **[>>>]** sucht nach der nächsten Sitzung zwischen zwei beliebigen Hosts. Wenn Sie mehrere TCP-Sitzungen zwischen den zwei Hosts im Puffer haben und alle nacheinander ansehen wollen, empfehlen wir mit der Rekonstruktion der ersten Sitzung anzufangen, da der Rückwärtsbutton **[<<]** nicht weiter zurück als bis zur zuerstrekonstruierten TCP-Sitzung gehen kann.

Die so erhaltenen Daten können als Binärdaten, HTML-, Text- oder Rich-Textdatei durch Klicken auf **Datei => Speichern unter…** gesichert werden. Wenn Sie in ein Textformat speichern, ist die Ergebnisdatei eine Unicode UTF-16-Datei. Wird ins HTML-Format gespeichert, ist die Verschlüsselung der Ergebnisdatei vom aktuell gewählten **Anzeigetyp** abhängig. Wenn HTML aktuell gewählt ist, wird die Ergebnisdatei eine ANSI-Textdatei, für alle anderen Anzeigetypen ist die Ergebnisdatei eine Unicode UTF-16-Datei. Beachten Sie, wenn Sie eine HTTP-Sitzung mit Bildern speichern, werden die Bilder in das temporäre Verzeichnis auf Ihrer Festplatte gespeichjert, falls Sie die Bilder behalten möchten, öffnen Sie die gespeicherte Datei in Ihrem Browser und speichern die Datei in einem Format, dass Bilder beinhaltet, z.B. MHT, bevor Sie CommView for WiFi schließen.

Sie können durch Klicken auf **Bearbeiten => Finden…** nach einer Zeichenkette in der Sitzung suchen.

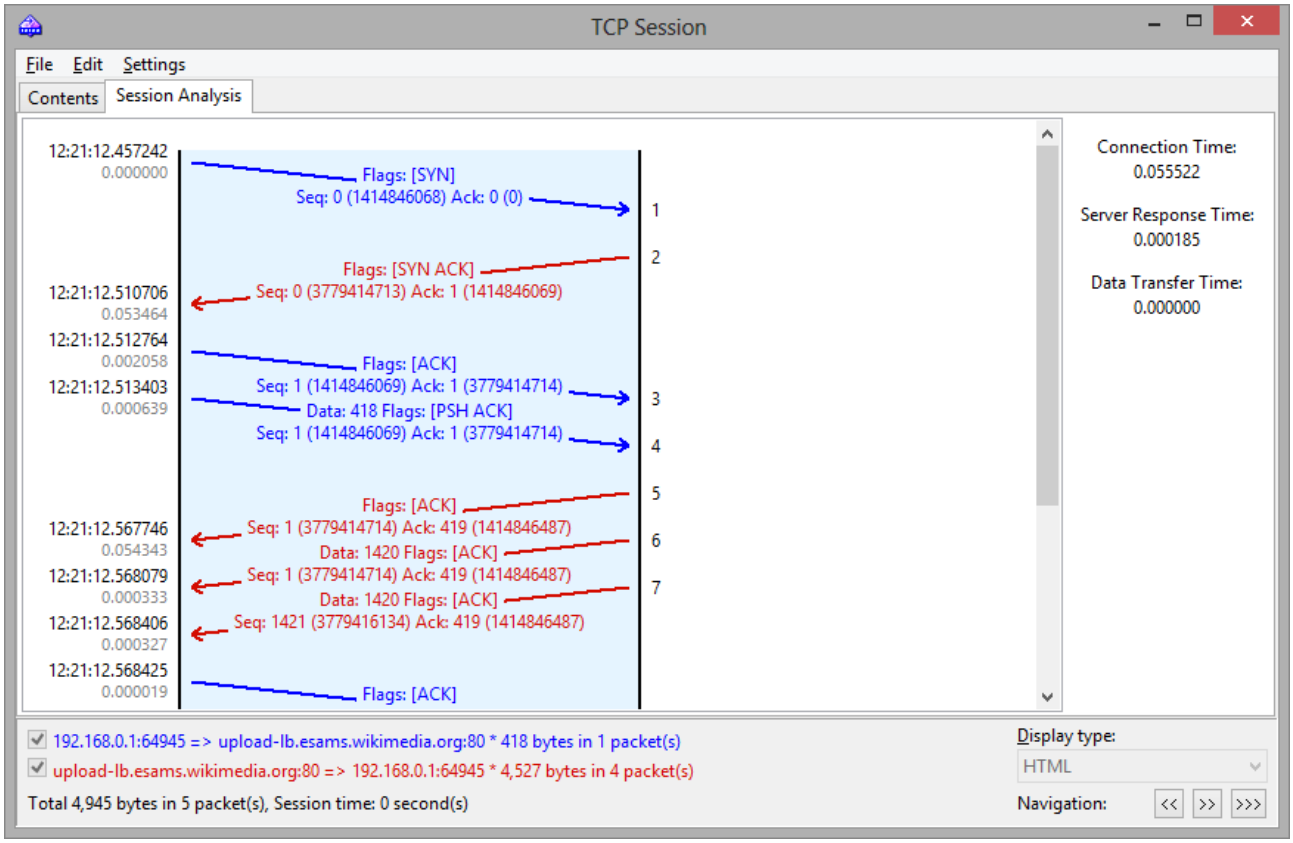
Sitzungsanalyse

Das Register Sitzungsanalyse des TCP-Sitzungsfensters stellt rekonstruierte TCP-Sitzungen grafisch dar. Sie können den Sitzungsdatenfluss, Fehler, Verzögerungen und verlorene erneut übertragene Daten sehen.

Die folgenden Daten werden für jedes Sitzungspaket angezeigt:

- TCP-Flags
- Absolute und relative SEQ- und ACK-Werte
- Paketankunftszeit
- Zeitdifferenz zwischen dem aktuellen und dem vorhergehenden Paket
- Paketnummer in der rekonstruierten Sitzung

Wenn ein Paket Fehler beinhaltet, wird die Eigenschaft des Fehlers erklärt. Es erscheint ein Beschreibungstext am rechten Rand des Diagramms. Wenn Sie die Maus über ein Paket mit Dateninhalt bewegen, wird der Dateninhalt in einem Hinweisfenster angezeigt. Beachten Sie, dass das Feld **Anzeigetyp** bestimmt, wie die Daten im Anzeigefenster decodiert werden. Ein Beispiel für ein Sitzungsanalysefenster wird unten gezeigt:



Der rechte Ausschnitt zeigt einige Basisstatistiken für die vorgegebene Sitzung:

- **Verbindungszeit** – Die benötigte Zeit zur Herstellung der TCP-Verbindung. In anderen Worten, es ist die Dreiweg-TCP-Handshake-Zeit (SYN => SYN ACK => ACK).
- **Server-Antwortzeit** – Die verstrichene Zeit zwischen der Klientenanfangsanfrage und der ersten Datenantwort des Server's.
- **Datenübertragungszeit** – Die Zeit zwischen der ersten und der letzten Datenantwort des Server's (0 bei nur einer Server-Antwort).

Sie können das grafische Schaubild der rekonstruierten TCP-Sitzung als BMP-, GIF- oder PNG-Datei durch Rechtsklick auf das Schaubild und Auswahl des Kontextmenüpunktes **Bild speichern als…** speichern. Sitzungen mit einer großen Paketanzahl werden in mehrere Dateien aufgeteilt.

UDP-Ströme rekonstruieren

Dieses Werkzeug ist dem im vorhergehenden Kapitel beschriebenen Werkzeug **TCP-Sitzungen rekonstruieren** sehr ähnlich; schauen Sie bitte für weitergehende Informationen in diese Kapitel. Allerdings ist UDP, nicht wie TCP, ein verbindungsloses Protokoll, die folgenden Unterschiede bestehen zwischen TCP-Sitzungsrekonstruktion und UDP-Stream-Rekonstruktion:

- Es gibt kein Register Sitzunganalyse, weil es keine Sitzungen, SEQs oder ACKs in UDP gibt.

- Weil es keine SYNs oder FINs in UDP gibt, gelten alle zwischen den IP-Adresspaaren und Ports gesendeten Pakete, als zu demselben Stream gehörend.

Pakete suchen

Um die Pakete aufzufinden, die einen bestimmten Text oder eine bestimmte Adresse enthalten, öffnen Sie den **Finde Paketinhalt** Dialog (**Suchen => Finde Paket**). Geben Sie einen Such-String ein, wählen Sie die Art der eingegebenen Information (**String** oder **Hex**) und klicken Sie auf **Finde nächstes**. Das Programm sucht dann nach Paketen, die dem Suchkriterium entsprechen und zeigt diese dann im Register **Pakete** an.

Sie können den Text als String, hexadezimal Wert, MAC- oder IP-Adresse eingeben. Die Zeichenkettensuche wird in ASCII- und Unicode-Formaten (UTF-8 und UTF-16) ausgeführt. Einen Hex-String sollte benutzt werden wenn Sie nichtdruckbare Zeichen eingeben wollen: Geben Sie die hexadezimalen Werte folgendermaßen ein, z. B. AD0A027804. Die Benutzung von IPv6-Adressen erfordert Windows XP oder höher und die IPv6-Stapelung muss installiert sein.

Aktivieren Sie **Gross-/Kleinschr.** für eine Suche unter Berücksichtigung der Gross- und Kleinschreibung. Aktivieren Sie **Bei Offset**: um einen String zu suchen, der zu einem bestimmten Offset beginnt. Beachten Sie bitte, dass der Offset-Indikator hexadezimal und nullbasierend ist (wenn Sie z. B. nach dem ersten Byte in dem Paket suchen, ist das Offset 0). Sie können ebenso eine Suchrichtung auswählen, **Aufwärts** oder **Abwärts**.

Statistiken und Berichte

Dieser Dialog (**Ansicht => Statistiken**) zeigt wichtige Netzwerkstatistiken für Ihr WLAN-Segment, wie Paketanzahl/Sekunde, Bytes/Sekunde, Ethernet-Protokolle, IP-Protokolle, Sub-Protokolle und die Verteilungsgrafiken zu den Sub-Protokollen. Jede grafische Darstellung kann durch Doppelklicken in die Zwischenablage kopiert werden. Die Kuchengrafiken der Ethernet-Protokolle, IP-Protokolle und der Sub-Protokolle können, mittels der kleinen Buttons im unteren rechten Eck, zur besseren Sichtbarkeit der Bereiche rotiert werden.

Die auf jeder Seite angezeigten Daten können als Bitmap oder kommaseparierte Textdatei über das Kontextmenü bzw. durch Drag&Drop gespeichert werden. Mit der Seite **Bericht** kann CommView for WiFi automatisch individualisierte Berichte im HTML- bzw. kommaseparierten Textformat erstellen.

Netzwerkstatistiken können aus allen über ihr Netzwerkadapter laufenden Daten oder durch die Regeldefinitionen erzeugt werden. Wenn sie wollen, dass die Statistikzähler nur die Daten der Pakete erfassen, die dem aktuellen Regelsatz entsprechen (und keine anderen), sollten Sie die Checkbox **Aktuelle Regeln anwenden** aktivieren.

Allgemein

Dies zeigt die Pakete/Sekunde bzw. Bytes/Secunde oder Bits/Sekunde als Histogramm an, ferner den Bandbreitenverbrauch (Verkehr/Sekunde dividiert durch die Geschwindigkeit des drahtlosen Adapters), ferner den Gesamtpaket- und -bytezähler. Ein Doppelklick auf die Anzeige öffnet ein Dialogfenster, in dem Sie die Adaptergeschwindigkeit manuell konfigurieren können, damit diese für die Bandbreitennutzungsberechnungen verwendet werden kann.

Protokolle

Zeigt die Verteilung der Ethernet-Protokolle, wie ARP, IP, SNAP, SPX, etc. Wählen Sie die Dropdown-Liste **Diagramm von** um eine der zwei möglichen Berechnungsmethoden auszuwählen: Nach der Paketanzahl oder nach der Byteanzahl. Wenn Ihr WLAN WEP- bzw. WPA-Verschlüsselung verwendet, müssen die WEP- bzw. WPA-Schlüssel korrekt konfiguriert sein, damit das Programm den Netzwerkverkehr entschlüsseln kann; ansonsten ist diese Darstellung leer.

IP-Protokoll

Zeigt die Verteilung der IP-Protokolle. TCP, UDP und ICMP. Wählen Sie die Dropdown-Liste **Diagramm von** um eine der zwei möglichen Berechnungsmethoden auszuwählen: Nach der Paketanzahl oder nach der Byteanzahl. Wenn Ihr WLAN WEP- bzw. WPA-Verschlüsselung verwendet, müssen die WEP- bzw. WPA-Schlüssel korrekt konfiguriert sein, damit das Programm den Netzwerkverkehr entschlüsseln kann; ansonsten ist diese Darstellung leer.

IP-Unterprotokolle

Zeigt die Verteilung der wichtigsten IP-Anwendungslevel-Unterprotokolle: HTTP, FTP, POP3, SMTP, Telnet, NNTP, NetBIOS, HTTPS und DNS. Um weitere Protokolle hinzuzufügen verwenden Sie die Schaltfläche **Einstellungen**. Mit diesem Dialog können Sie bis zu 8 selbstdefinierte Protokolle hinzufügen. Geben Sie dazu den Protokollnamen ein, wählen Sie den Protokolltyp (TCP/UDP) und die Portnummer. Wählen Sie die Dropdown-Liste **Diagramm von** um eine der zwei möglichen Berechnungsmethoden auszuwählen: Nach der Paketanzahl oder nach der Byteanzahl. Wenn Ihr WLAN WEP- bzw. WPA-Verschlüsselung verwendet, müssen die WEP- bzw. WPA-Schlüssel korrekt konfiguriert sein, damit das Programm den Netzwerkverkehr entschlüsseln kann; ansonsten ist diese Darstellung leer.

Größe

Zeigt die Verteilung (Grafik) nach Paketgröße.

Hosts nach MAC

Listet die aktiven WLAN-Hosts geordnet nach MAC-Adresse auf und zeigt die Datentransferstatistik. Sie können den MAC-Adressen Kennnamen zuordnen. Wenn Sie zu viel Multicast-Pakete in Ihrem

Netzwerk haben, so dass die Hosts nach MAC-Tabelle überfüllt ist, können Sie die Multicast-Adressen zusammenfassen (GroupedMulticast). Diese Funktion aktivieren Sie mittels Aktivierung der Checkbox **Multicast-Adressen gruppieren**. Beachten Sie, dass nur Pakete, die nach der Aktivierung dieser Funktion ankommen, entsprechend gruppiert werden, vorher empfangene Pakete werden nicht berücksichtigt.

Hosts nach IP

Listet die aktiven WLAN-Hosts nach IP-Adresse auf und zeigt die Datentransferstatistik. Da empfangene IP-Pakete von beliebig vielen IP-Adressen stammen können (innerhalb bzw. außerhalb Ihres WLANs), zeigt diese Tabelle standardmässig keine Statisktik. Zur Anzeige der Statistik müssen Sie erst den zu überwachenden IP-Adressraum durch klicken auf **Bereich hinzufügen/setzen** festlegen. Normalerweise sollte dieser Bereich zu Ihrem WLAN gehören. Durch die Konfiguration eines solchen Bereiches von IP-Adressen erhalten Sie die Nutzungsstatistik. Sie können jeden Bereich definieren, solange der Gesamt-IP-Adressbereich nicht mehr als 1.000 IP-Adressen umfaßt. Um einen Bereich zu löschen rechtsklicken Sie auf die Liste des Bereiches und wählen dann den entsprechenden Menübefehl. Sie können den IP-Adressen Kennnamen zuordnen. Ferner können Sie die Checkbox **Alle** wählen, um alle IP-Adressen aufzulisten; diese Funktion wird jedoch nicht empfohlen für die Nutzungserfassung von RAM und CPU. Wenn Ihr WLAN WEP- bzw. WPA-Verschlüsselung verwendet, müssen die WEP- bzw. WPA-Schlüssel korrekt konfiguriert sein, damit das Programm den Netzwerkverkehr entschlüsseln kann; ansonsten ist diese Darstellung leer.

Matrix nach MAC

Diese Seite zeigt eine grafische Matrix zwischen Hosts und deren MAC-Adressen. Die durch die MAC-Adressen repräsentierten Hosts sind innerhalb des Kreises und die Sessions werden als Verbindungen zwischen diesen angezeigt. Wenn Sie den Mauszeiger über einen Host führen werden alle Verbindungen von diesem Host zu anderen Hosts hervorgehoben. Die Anzahl der aktivsten Hostpaare können Sie mittels des Wertes im Feld **Aktivste Hostpaare** ändern. Wenn Sie die Anzahl der zuletzt untersuchten Paare ändern wollen, verändern Sie bitte den Wert im Feld **Letzte Paare einbeziehen**. Wenn die Matrix zu voll ist, da Ihr Netzwerk zu viele Broadcast- bzw. Multicastpakete hat, aktivieren Sie die Checkboxen **Broadcasts ignorieren** und **Multicasts ignorieren**.

Matrix nach IP

Diese Seite zeigt grafisch den Zusammenhang zwischen Hosts und deren IP-Adressen. Die durch die IP-Adressen repräsentierten Hosts sind innerhalb des Kreises, und die Sitzungen werden als Verbindungen zwischen diesen angezeigt. Wenn Sie den Mauszeiger über einen Host führen werden alle Verbindungen von diesem Host zu anderen Hosts hervorgehoben. Die Anzahl der aktivsten Hostpaare können Sie mittels des Wertes im Feld **Aktivste Hostpaare** ändern. Wenn Sie

die Anzahl der zuletzt untersuchten Paare ändern wollen, verändern Sie den Wert im Feld **Letzte Pakete einbeziehen**. Wenn die Matrix zu voll ist, da Ihr Netzwerk zu viele Broadcast- bzw. Multicastpakete hat, aktivieren Sie die Checkboxen **Broadcasts ignorieren** und **Multicasts ignorieren**. Wenn Ihr WLAN WEP- bzw. WPA-Verschlüsselung verwendet, müssen die WEP- bzw. WPA-Schlüssel korrekt konfiguriert sein, damit das Programm den Netzwerkverkehr entschlüsseln kann; ansonsten ist diese Darstellung leer.

Bericht

Mit diesem Dialog erzeugt CommView for WiFi automatisch Berichte im HTML- (einschl. Bildern von Tabellen und Graphen) oder kommaseparierten Textformat.

Neben den Echtzeitstatistiken kann das Programm auch Statistiken aus bereits gesammelten Daten erstellen. Dazu laden Sie eine Datei in den Logbetrachter und klicken dann **Datei => Statistik generieren**. Vorher im **Statistikfenster** gesammelte Daten können, wenn gewünscht, gelöscht werden. Diese Funktion zeigt keine Zeitreihenanalyse. Sie zeigt nur Summen, Protokollkarten und LAN-Host-Tabellen.

Kennnamen verwenden

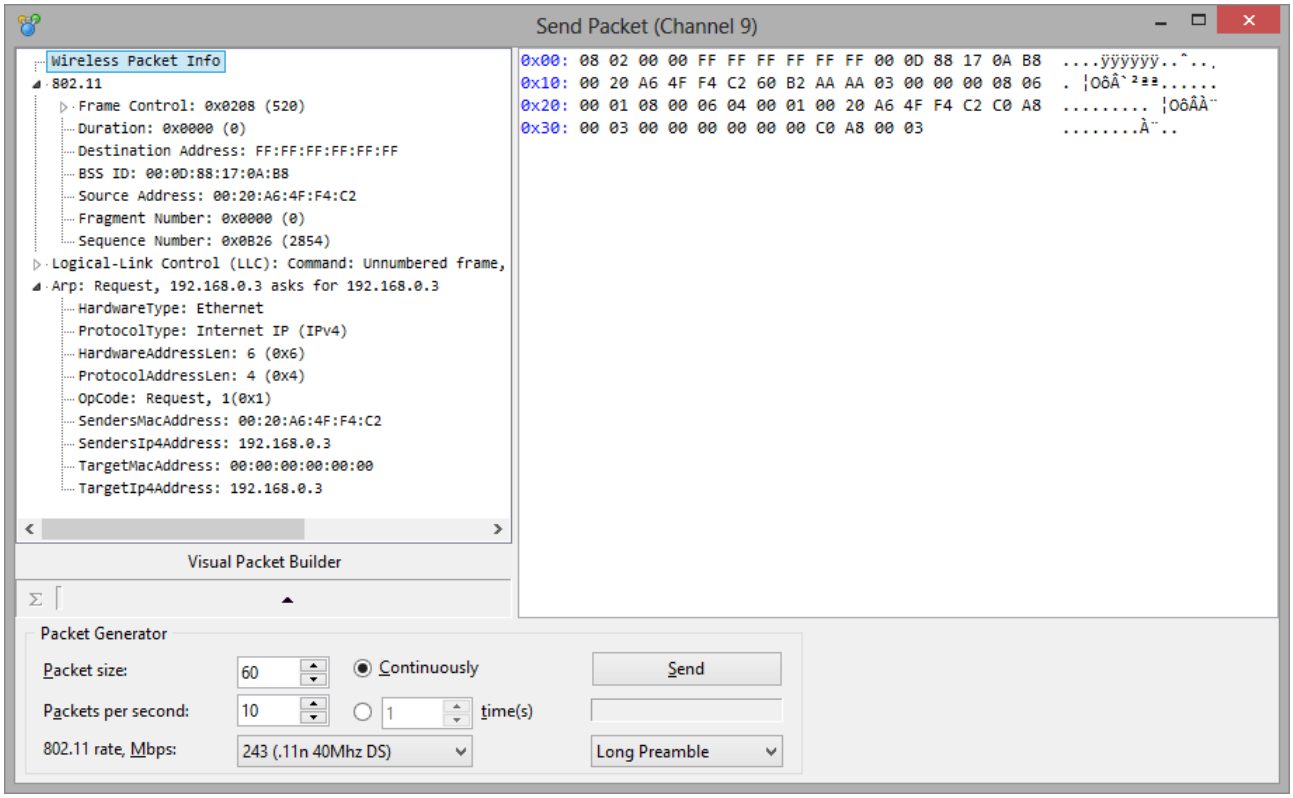
Kennnamen sind leicht zu merkende, für Menschen besser lesbare Namen, die CommView for WiFi anstelle von MAC- bzw. IP-Adressen einsetzt, wenn Pakete in den Registern **Pakete** und **Statistiken** anzeigt werden. Die Pakete können so leichter erkannt und analysiert werden. Es wird z. B. 00:00:19:2D:0D:35 in GATEWAY2 und ns1.earthlink.com wird zu MyDNS gewandelt.

Um einen MAC-Kennnamen zu erzeugen, rechtsklicken Sie auf das Paket und wählen dann im Popup-Menü **Quell-MAC verwenden** oder **Ziel-MAC verwenden**. Es erscheint ein Popup-Fenster, in dem das MAC-Adressenfeld schon ausgefüllt ist und Sie nur noch einen Kennnamen eingeben müssen. Sie können aber auch auf **Einstellungen => MAC Kennname…** klicken und das Feld mit der MAC-Adresse und dem Kennnamen manuell ausfüllen. Um einen Kennnamen zu löschen bzw. die ganze Kennnamenliste zu löschen, rechtsklicken sie auf die Kennnamenliste und wählen dann **Datensatz löschen** bzw. **Alles löschen**. Die Erzeugung von IP-Kennnamen ist analog. Wenn durch einen Rechtsklick auf das Paket ein neuer IP-Kennname gewählt wird, ist das Kennnamenfeld mit dem entsprechenden Hostnamen vorausgefüllt (sofern vorhanden), welcher dann vom Benutzer editiert werden kann.

Paketgenerator

Mit diesem Dialog können Sie Pakete über ihr drahtloses Netzwerkadapter versenden bzw editieren. Um den Paketgenerator zu starten, klicken sie auf **Werkzeuge => Packetgenerator** oder

wählen Sie ein Paket im Register **Pakete**, rechtsklicken Sie darauf und wählen dann den Befehl **Sende Paket(e)**.



Lesen Sie unbedingt die folgenden wichtigen Informationen über die Begrenzungen und Besonderheiten bei der Nutzung des Paketgenerators mit WLAN-Adaptern durch:

- Sie sollten den Paketgenerator nicht verwenden, bis Sie genau wissen, welchen Effekt Sie erreichen wollen. Das Senden von Paketen kann unvorhersehbare Ergebnisse mit sich bringen, wir empfehlen daher dringend, dass Sie dieses Tool nur benutzen, wenn Sie ein erfahrener Netzwerkadministrator sind.
- Möglicherweise wird die Firmware Ihres Adapters bestimmte Pakete nicht versenden oder andere Pakete mehrmals senden. Dies unterliegt der Kontrolle der Firmware und befindet sich außerhalb unserer Eingriffsmöglichkeiten.
- Möglicherweise verhindert Ihre Adapter-Firmware, dass Sie Pakete mit willkürlichen Raten versenden. So kann es sein, dass z. B. bei einer Versendung von Paketen mit einer Rate von 1000/Sekunde, die Firmware die Pakete mit einer geringeren Rate gesendet werden.

Beachten Sie, dass der Paketgenerator sogenannte Application-layer-TCP-Streams nicht versenden kann und soll. Das bedeutet, er kann nicht zunehmende SEQ- oder ACK-Werte automatisch

verarbeiten, die Checksummen oder Paketgrößen anpassen, usw. Wenn Sie einen TCP-Stream versenden wollen, benötigen Sie eine speziell für diesen Zweck entwickelte winsock-basierende Anwendung. Der Paketgenerator ist ein Tool zum Wiederabspielen von gesammelten Daten, zum Testen von Firewalls und Intrusion Detection-Systemen und für andere Aufgaben die manuelle Paketerzeugung benötigen.

Der Paketgenerator ermöglicht es die Paketinhalte zu ändern und das decodierte Paket im linken Fenster beim Editieren anzuzeigen. Sie können damit beliebige Pakete erzeugen und haben volle Kontrolle über die Paketinhalte. Bei IP-, TCP-, UDP- und ICMP-Paketen können Sie die Checksumme automatisch mit der Schaltfläche **Sigma** korrigieren. Um Sie bei der Paketbearbeitung zu unterstützen, ist zusätzlich das Werkzeug **Optischer Paketersteller** vorhanden. Klicken Sie auf den entsprechenden Button, um das Werkzeug aufzurufen.

Sie können auch auf den Pfeilbutton klicken um die Liste der erhältlichen Paketvorlagen zu sehen. Das Programm beinhaltet bereits **TCP**-, **UDP**- und **ICMP-Paketvorlagen**; diese Vorlagen zu benutzen ist oftmals schneller als das Schreiben von HEX-Code im Editor. Diese Vorlagen enthalten typische TCP-, UDP- und ICMP-Pakete, Sie können statt der vorgegebenen, auch eigene Vorlagen verwenden um einzelne Paketfelder selbst zu editieren bzw. Werte einzugeben die Ihren Ansprüchen genügen, wie MAC- und IP-Adressen, Portnummern, SEQ- und ACK-Nummern usw. Sie sollten eher die eigenen Vorlagen als die eingebauten Vorlagen benutzen. Sie können ein Paktet aus dem CommView-Paketbereich durch Drag&Drop in die Vorlagensektion des Paketgenerators ziehen. Wenn Sie mehrere Pakete in die Vorlagensektion einfügen wird nur das Erste als Vorlage verwendet. In der Vorlagenliste wird nun der Eingangsname "Neue Vorlage" vorgegeben. Durch Rechtsklick auf eine neue Vorlage in der Liste können Sie diese mit **Umbennen** neu benennen. Wenn Sie eine Vorlage löschen wollen, rechtsklicken Sie darauf und wählen dann **Löschen** im Kontextmenü. Die Auswahl einer Vorlage in der Liste öffnet sie im Editorfenster, wo sie vor dem Absenden verändert werden kann.

NCF-Dateien können mit den Vorlagen Ihrer Wahl im Anwendungsverzeichnis im Unterordner TEMPLATES abgelegt werden. Wenn CommView for WiFi mindestens eine NCF-Datei im Unterverzeichnis Templates findet, wird die Vorlage in einer Dropdown-Liste zusammen mit den anderen Vorlagen angezeigt. Diese NCF-Dateien sollten nur ein Paket pro Datei enthalten, wenn Sie aber eine Datei mit mehreren Paketen öffen, wird CommView for WiFi nur das erste anzeigen.

Nach dem Editieren des Paketes können Sie mit den folgenden Befehlen die Pakete versenden:

- **Paketgröße** – Ändert die Paketgröße.
- **Pakete/Sekunde** – Beeinflußt die Paketsendegeschwindigkeit.
- **Kontinuierlich** – Hier sendet der Paketgenerator kontinuierlich Pakete, bis Sie **Stop** klicken.
- **Zeiten** – Zur Vorgabe von Versendezeiten durch den Paketgenerator.
- **802.11-Geschwindigkeit** – Modifiziert die 802.11-Frequenz zum Senden von Paketen. Abhängig vom aktuell gewählten Band und Kanal, können nicht alle Geschwindigkeiten

benutzt werden. Zum Beispiel, 802.11a-Pakete können nicht bei bei einer Übertragungsrate von 2 Mb/s gesendet werden.

- **Lange/Kurze Einleitung** – Legt den Einleitungstyp für 802.11b und 802.11g Pakete fest. Nicht auf 802.11a anwendbar.
- **Senden/Stop** – Betätigen Sie den Button wenn Sie Pakete versenden bzw. den Versand stoppen wollen.

Arbeiten mit mehreren Paketen

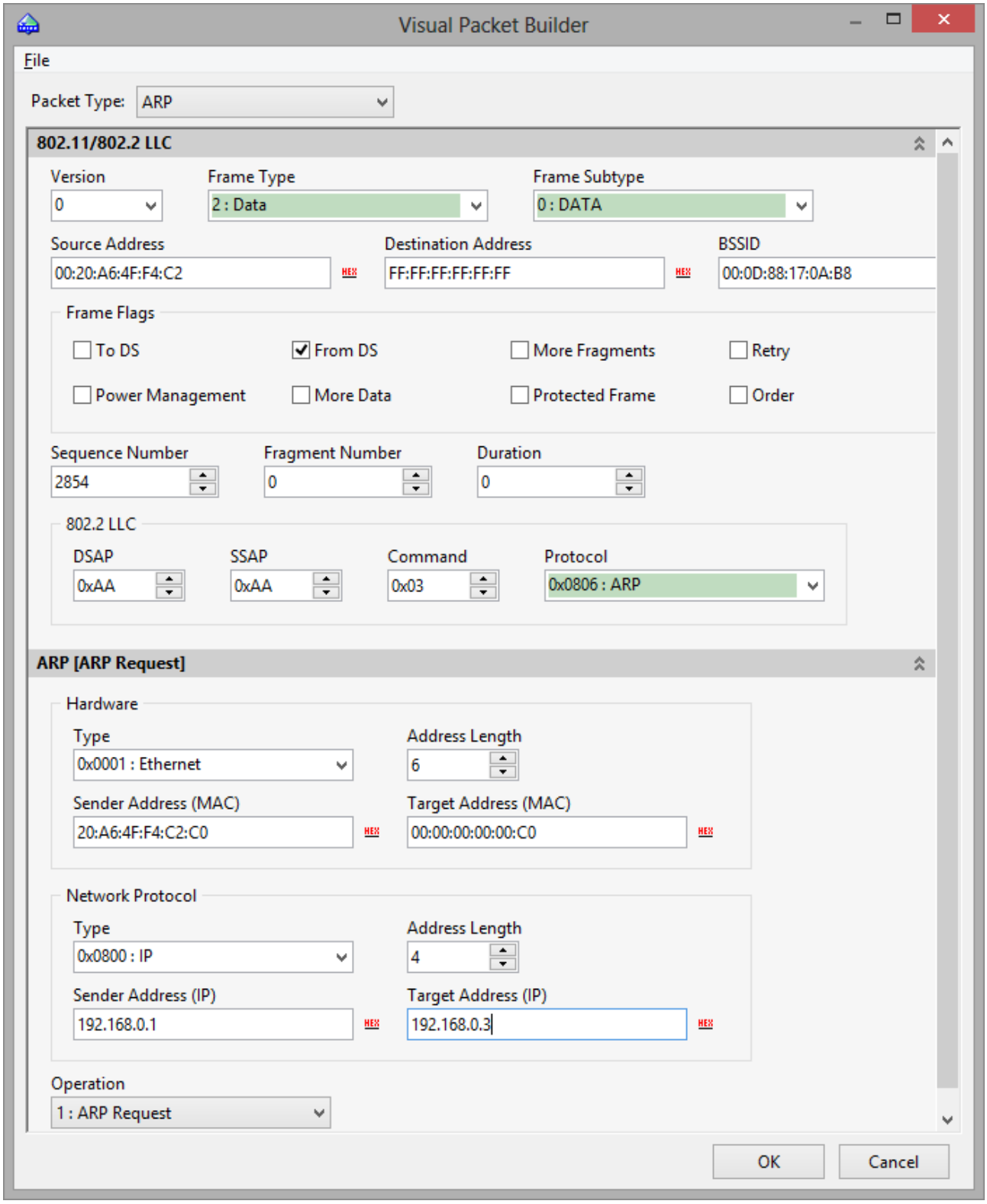
Mit dem Paketgenerator können Sie mehrere Pakete auf einmal senden. Dazu wählen Sie die zu versendenden Pakete in der Liste, aktivieren den Paketgenerator durch das Kontextmenü oder ziehen mittels Drag&Drop die ausgewählten Pakete in das Paketgeneratorfenster. Sie können aber auch die gesammelten Dateien mit Drag&Drop in allen unterstützten Formaten in das Paketgeneratorfenster hineinziehen. Wenn mehrere Pakete versandt werden, werden der Packer-Editor und der Dekoder-Baum sichtbar.

Editierte Pakete speichern

Wenn Sie ein Paket bearbeitet haben und es dann abspeichern möchten, ziehen Sie den Dekoder-Baum auf den Desktop oder auf ein beliebiges Verzeichnis. Es wird eine neue Datei im NCF-Format mit dem Paket erzeugt. Die Datei heißt stets PACKET.NCF. Sie können auch das Paket in das Vorlagenfenster ziehen. Wenn Sie mehrere Pakete bearbeiten wollen, sollten Sie diese nacheinander bearbeiten. Ziehen Sie jedes Mal dabei ein Paket auf den Desktop und benennen die Datei dann um. Danach öffnen Sie einen neuen Logbetrachter und verschieben (Drag&Drop) die bearbeiteten Pakete vom Desktop in den Logbetrachter. Anschliessend wählen Sie die Pakete mit der Taste [Shift] aus und rufen mittels Kontextmenü den Paketgenerator auf.

Optischer Paketersteller

Der Optische Paketersteller ist ein Werkzeug zur leichteren Paketbearbeitung und –erstellung im Paketgenerator. Dieses Werkzeug ermöglicht Ihnen, neue Pakete schnell und korrekt zu erstellen oder bestehende Pakete mit vorgefertigten Vorlagen zu modifizieren. Einmal erstellt oder bearbeitet, kann ein Paket mit dem Paketgenerator im Netzwerk in Umlauf gebracht werden.



Standard TCP- UDP-, ICMP- (auf der 4. und 6. Version des IP-Protokoll basierend) und ARP-Paketgenerierung wird unterstützt. Zur Erstellung eines Paketes, wählen Sie den Typ aus dem Ausklappmenü **Pakettyp**. Die Standardwerte der Paketfelder werden automatisch ausgefüllt, sie können aber nachträglich geändert werden.

ICMP-, TCP-, UDP- und ARP-Pakete beinhalten verschiedene verkapselte Ebenen und das Interface des Optischen Paketerstellers ist entsprechend aufgebaut. Optionen die zu einer entsprechenden Ebene gehören werden in einem separaten Feld angezeigt. Zum Beispiel, ein TCP-Paket beinhaltet 4 Ebenen, **QuellMAC**- und **ZielMAC-Adressfelder** angeordnet im **Ethernet II-Feld** (Datenverbindungsebene) und **Src Port**- und **Dst Port-Werte** werden im **TCP**-Feld (Transportebene) angezeigt. Falls Sie ein Feld ausblenden möchten, klicken Sie auf den in der rechten Ecke des Feldkopfes angeordneten Button **Aus-/Einklappen**.

Beachten Sie, dass einige „Parental“ Ebenenwerte die Pakete auf tiefere Ebenen bewegen; daher kann die Modifizierung höherer Ebenen zur Erneuerung von unteren Ebenen eines Paketes führen. Deshalb führt eine Änderung des **Protkolltyps** im **Ethernet II-Feld** (Datenverbindungsebene) zur Erneuerung des gesamten Paketes. Eine andere Besonderheit die Sie beachten sollten, ist, dass die Werte einiger Felder abhängig vom Inhalt anderer Felder sind, ebenso wie der Dateninhalt tieferer Ebenen. Solche Felder sind: Checksummen und Kopflängen und/oder Daten der unteren Ebenen. Der Optische Paketersteller kalkuliert solche Werte automatisch. Immer wenn Sie ein nichtstandardisiertes Paket erstellen, können Sie verschiedene Werte manuell bestimmen, indem Sie die Checkbox **Standardwerte überschreiben** aktivieren und die gewünschten Werte festlegen.

> Der Optische Ersteller hilft Ihnen die Korrektheit der erstellten Pakete, durch eine rote Hervorhebung der Köpfe und Felder, mit unkorrekten oder nichtstandardisierten Werten zu kontrollieren.

Trotz der Tatsache, dass der Optische Paketersteller nur interne Unterstützung für die TCP-, UPD-, ICMP- und ARP-Protokolle besitzt, können Sie doch Pakete damit bearbeiten, die andere Protokolle benutzen. Für solche Pakete können Sie den Hex-Editor zur Bearbeitung nutzen.

Ist ein Paket einmal erstellt, kann es gespeichert und anschließend wieder in den Optischen Paketersteller geladen werden. Benutzen Sie die jeweiligen Befehle aus dem Menü **Datei** des Optischen Paketerstellers zum Laden/Speichern der erfassten Dateien. Sie können jede mit CommView for WiFi erfasste Datei (NCF) laden; immer wenn die Datei mehr als ein Paket enthält, wird nur das erste Paket geladen.

NIC Vendor (Hersteller) identifizieren

Die ersten 24 Bit der MAC-Adresse einer Netzwerkkarte identifizieren klar den Hersteller. Diese 24-Bit-Nummer wird OUI (Organizationally Unique Identifier) genannt. Der NIC-Hersteller-Identifier ist ein Werkzeug, das Ihnen ermöglicht, den Hersteller über die MAC-Adresse zu ermitteln. Um einen Hersteller zu finden, klicken Sie auf **Werkzeuge => NIC-Herstelleridentifikation**. Geben Sie eine MAC-Adresse ein und klicken Sie auf **Finde**. Sie sehen dann den Namen des Herstellers.

Standardmässig ersetzt CommView for WiFi die ersten drei Oktets der MAC-Adresse durch den Herstellernamen der Netzwerkarte im Register **Pakete**. Dieses Verhalten kann unter **Einstellungen => Allgemein** durch deaktivieren der Checkbox **Herstellernamen in MAC-Adressen anzeigen** im **Optionen**-Dialog des Programms geändert werden. Die Herstellerliste ist in der Datei MACS.TXT im CommView-Anwendungsverzeichnis enthalten und kann manuell verändert werden. Sie können diese Liste manuell bearbeiten um Informationen hinzuzufügen oder zu modifizieren.

Scheduler

Mit diesem Dialog können Sie zeitgesteuerte Aufgaben erzeugen und editieren. Dies ist sinnvoll, wenn CommView for WiFi den Empfang selbstständig zu einem bestimmten Zeitpunkt aktivieren bzw. deaktieren soll, z. B. nachts oder am Wochenende. Eine neue Aufgabe fügen Sie mittels klicken auf **Werkzeuge => Paketerfassungsplaner** hinzu, dann klicken Sie auf den Button **Hinzufügen**.

Im Bereich **Paketerfassung starten** können Sie das Datum und die Uhrzeit festlegen, wann CommView for WiFi den Empfang starten soll. Mit der Dropdown-Liste **Kanal** wählen Sie den zu analysierenden WLAN-Kanal. Im Bereich **Paketerfassung stoppen** kann festgelegt werden, wann CommView for WiFi den Empfang beendet. Die Checkboxen **Paketerfassung starten** und **Paketerfassung stoppen** müssen nicht gleichzeitig aktiviert sein. Wenn nur die erste Checkbox aktiv ist, findet der Empfang bis zum manuellen Abbruch statt. Sie müssen zwar manuell starten wenn nur die zweite Box aktiv ist, CommView for WiFi stoppt dann aber automatisch zum angegeben Zeitpunkt.

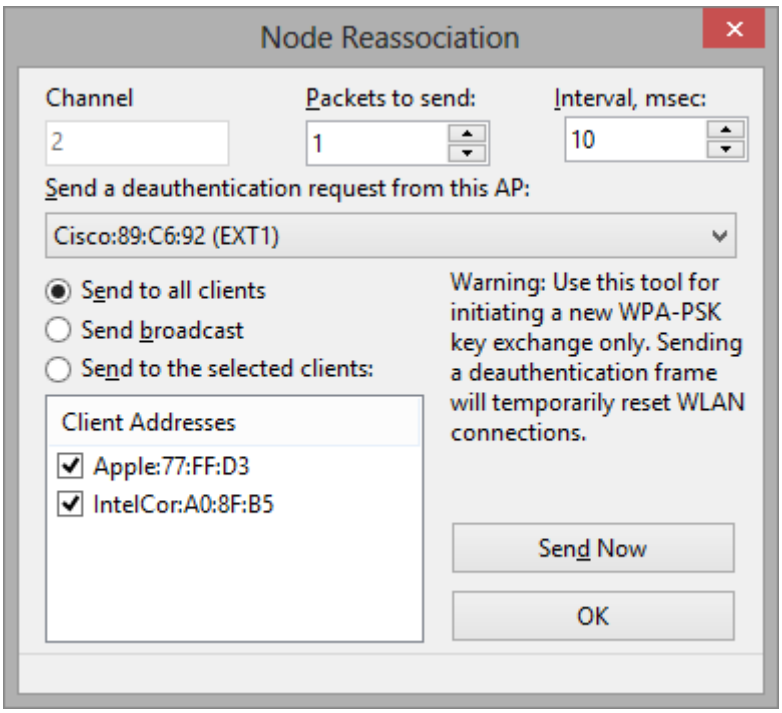
Wenn CommView for WiFi schon Pakete empfängt und gleichzeitig ein anderer Adapter programmiert ist, bricht CommView for WiFi den Empfang ab, wechselt zum neuen Adapter und beginnt den Empfang erneut.

Es ist wichtig zu verstehen, dass zeitgesteuerte Aufgaben nur durchgeführt werden können, wenn CommView for WiFi aktiv ist.

Knotenzuordnung wiederherstellen

Durch die dynamische Natur der WPA-Verschlüsselung hilft allein das Wissen um die WPA-Passphrase auch nicht dabei, den Verkehr sofort nach Eingabe dieser Passphrase entschlüsseln zu können. Um WPA-verschlüsselten Verkehr entschlüsseln zu können muss CommView for WiFi laufen und während der Schlüsselaustauschphase schon Daten sammeln. Der Schlüsselaustausch läuft über das EAPOL-Protokoll. Mehr dazu unter **Hintergründe der WPA-Eneschlüsselung**.

Der Node Reassociation-Dialog kann dazu genutzt werden einen Schlüsselaustausch zu initiieren:



Dieser Dialog sendet eine Deauthentifikation-Anfrage über den Accesspoint an die ausgewählten Stationen. Dies führt zu einer Reassozierung mit dem Accesspoint. Dieser Prozeß dauert meist eine Sekunde und ermöglicht Commview for WiFi EAPOL-Pakete, die für die WPA-PSK-Entschlüsselung benötigt werden, zu empfangen.

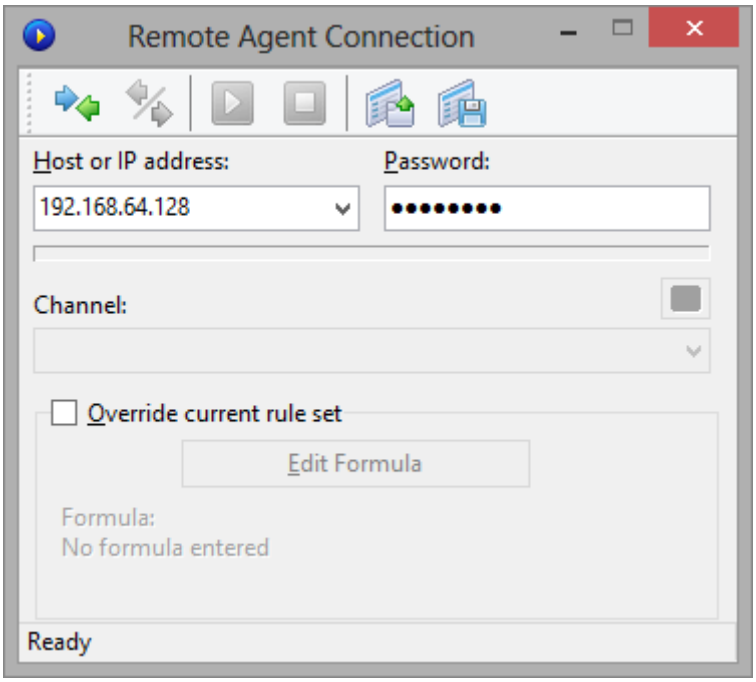
Um die Reassoziation zu initiieren wählen Sie aus der Dropdown-Liste einen Accesspoint, dann die Stationen und klicken anschließend auf **Senden**. Die Optionen **An alle Clients senden** und **An ausgewählte Clients senden** verschickt Unicast-Pakete an ausgewählte oder an alle Clients. Die Option **Broadcast senden** sendet ein Broadcast-Paket an die Adresse FF:FF:FF:FF:FF:FF. Weil diese Option selbst unentdeckte Stationen behandelt, können manche Stationen unbestätigte Anfragen ignorieren. Wenn Sie mehrere Pakete verschicken möchten benutzen Sie die Checkboxen **Pakete an senden** und **Intervall**.

Remote Agent for WiFi einsetzen

CommView Remote Agent for WiFi ist ein Begleitprodukt, das zur Fernüberwachung von Nezwerkverkehr eingesetzt wird. Alles was Sie tun müssen, ist Remote Agent for WiFi auf dem Zielcomputer zu installieren und CommView for WiFi zur Verbindung zum Remote Agent zu benutzen. Sobald Sie sich verbunden und authenifiziert haben, können Sie mit der Überwachung starten als wären Sie vor Ort.

Dieses Kapitel beschreibt wie CommView for WiFi zur Verbindung mit Remote Agent for WiFi benutzt wird und Verkehr fernerfasst wird. Für detaillierte Informationen zur Installation und Konfiguration von Remote Agent, schauen Sie bitte in die Hilfedatei, die mit Remote Agent ausgeliefert wird. Es wird empfohlen, die Remote Agent-Dokumentation sorgfältig zu lesen, bevor Sie das Programm benutzen. CommView for WiFi kann von unserer Webseite heruntergeladen werden.

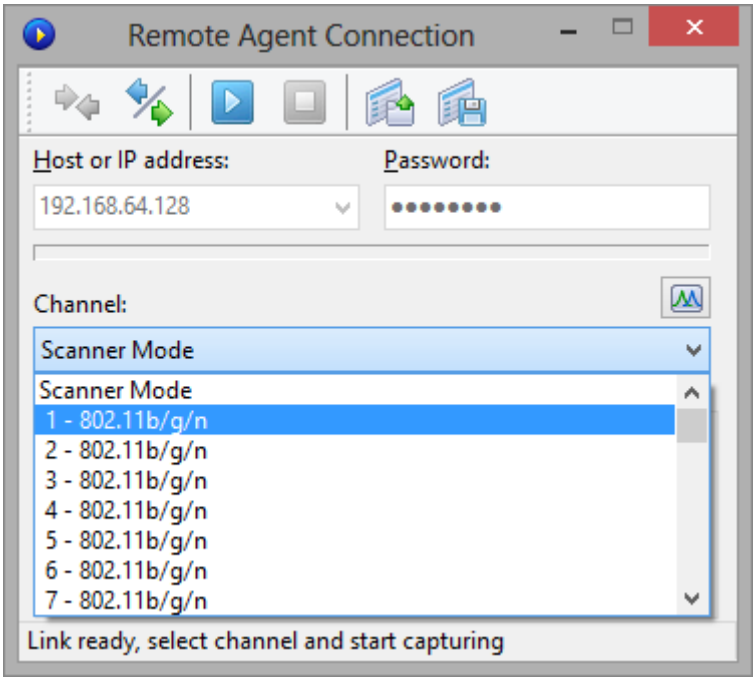
Zur Umschaltung in den Fernüberwachungsmodus, Klicken Sie auf **Datei => Fernüberwachungsmodus**. Eine zusätzliche Werkzeugleiste wird im Hauptfenster von CommView for WiFi in der Nähe der Hauptwerkzeugleiste eingeblendet. Falls Sie sich hinter einer Firewall oder Proxy Server befinden oder einen nichtstandardisierten Remote Agent-Port benutzen, können Sie auf die Schaltfläche **Erweiterte Netzwerkeinstellungen** klicken um die Portnummer zu wechseln und/oder die SOCKS5 Proxy Server-Einstellungen einzugeben. Der Dialog **Erweiterte Netzwerkeinstellungen** ermöglicht auch die Definition ob Remote Agent for WiFi die Filterregeln vor Ort übernimmt oder den gesamten erfassten Verkehr an CommView for WiFi sendet; dies wird detailliert später in diesem Kapitel diskutiert.



Klicken Sie auf den Button **Neue Remote Agent Verbindung** um eine neue Verbindung zu definieren oder klicken Sie auf den Button **Remote Agent Profil laden** um ein bereits vorhandenes Verbindungsprofil zu verwenden. Ein früher gespeichertes Profil kann ebenso aus dem Dialog Neue Remote Agent-Verbindung geladen werden.

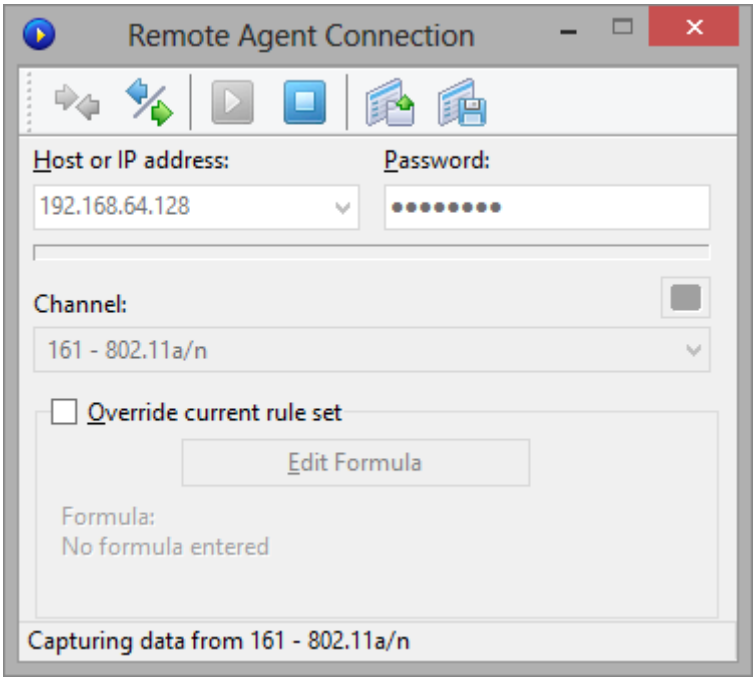
Das Remote Agent-Verbindungsfenster wird eingeblendet. Geben Sie die IP-Adresse des Compuerts in den Eingabebereich für IP-Adressen ein, auf dem Remote Agent for WiFi läuft, geben Sie das Verbindungspasswort ein und klicken auf den Button **Verbinden**. Wenn das Passwort korrekt ist, wird eine Verbindung aufgebaut. Sie sehen dann die Nachricht Verbindung fertig in der Statusleiste und im Bereich Kanalauswahl werden die Kanäle aufgelistet, die durch der drahtlose Adapter des fernüberwachten Computers unterstützt werden. Zusätzlich zu der Kanalliste wird ein spezieller **Scanner-Modus-Punkt** als erster Punkt auf der Liste hinzugefügt.

Wenn Sie den **Scanner-Modus** auswählen, wird sich der drahtlose Fernadapter zyklisch durch die verfügbaren Kanäle bewegen und von jedem Kanal für einige Sekunden Daten erfassen. Die schmale, auf der rechten Seite des Fensters angeordnete Schaltfläche, gerade über dem Bereich Kanalauswahl, ermöglicht Ihnen die Scanner-Einstellungen zu regulieren. Klicken Sie auf diese Schaltfäche, um den im Scanner-Modus zuüberwachenden Kanal auszuwählen und den Interval einzustellen, z.B. die Sekundenanzahl pro Kanal.



Jetzt ist die beste Zeit, die Erfassungsregeln unter Benutzung des Registers **Regeln** im CommView for WiFi Hauptfenster zu konfigurieren. Sie können einen maßgeschneiderten Satz von Erfassungregln auf diese Verbindung übernehmen und die aktuellen, in CommView for WiFi definierten Regeln durch ankreuzen der Checkbox **Überschreibe aktuellen Regelsatz** überschreiben, klicken Sie auf die Schaltfäche **Formel editieren** und geben Sie im Eingabefeld unten die Formel für die Regeln ein. Die Formelsyntax ist die gleiche, wie sie in den Erweiterten Regeln benutzt wird. Sobald Sie zum überwachungsstart bereit sind, wählen Sie einen Kanal aus der Liste und klicken auf den Werkzeugleisten-Button **Erfassung starten**. CommView for WiFi ermöglicht Ihnen, für den späteren schnellen Zugriff, die Remote Agent-Verbindungseinstellungen als Verbindungsprofil zu speichern. Klicken Sie im Dialog **Neue Remote Agent Verbindung** auf den

Werkzeugleisten-Button **Remote Agent-Profil speichern** und geben Sie einen Namen für die Datei ein.



CommView for WiFi wird starten, um den Verkehr des entfernten Adapters zu erfassen, als wäre es Ihr lokaler Netzwerkverkehr; da ist praktisch kein Unterschied zwischen der lokalen oder Fernnutzung von CommView for WiFi. Wenn Sie mit der Fernüberwachung fertig sind, klicken Sie auf den Button **Erfassung stoppen**. Sie können dann den Kanal wechseln oder durch Klicken auf den Werkzeugleisten-Button **Trennen** die Verbindung zu Remote Agent trennen. Zur Rückkehr in den Standardmodus, klicken Sie auf **Datei => Fernüberwachungsmodus** und die zusätzliche Werkzeugleiste wird eingeblendet.

Beachten Sie bitte, dass CommView for WiFi mit mehreren Remote Agents simultan arbeiten kann. Sie können verschiedene Fernverbindungen öffnen, einige haben ihre eigenen Einstellungen und einen unabhängigen Regelsatz und sammeln den Verkehr von fernüberwachten WLAN's in einer CommmView for WiFi-Instanz.

Effektive Nutzung des Remote Agent for WiFi

Der Schlüssel zur effektiven Remote Agent-Nutzung ist die Sicherstellung von genügend verfügbarer Bandbreite zur Übertragung der von Remote Agent gesammelten Daten an CommView for WiFi. Wie vorher erwähnt wurde, sollte Remote Agent auf einem Computer mit einem kompatibelen drahtlosen Adapter (für Überwachungszwecke) und Ethernet-Adapter (für die Verbindung zwischen Remote Agent und CommView for WiFi) installiert sein.

Standardmäßig sendet Remote Agent alle gesammelten Pakete an CommView for WiFi zurück, ungeachtet der Erfassungsregeln, die in CommView for WiFi konfiguriert sind. Dies ist zur

Beschaffung korrekter statistischer Daten und Entschlüsselung nötig, sowie das Vermögen zur korrekten Identifikation von drahtlosen Knotenpunkten. Seit ein vollgeladenes WiFi-Netzwerk Bandbreiten von 1Gbit/s hat, ist es wichtig, dass die Kabelverbindung zwischen Remote Agent und CommView for WiFi zur Verarbeitung dieser Bandbreite in der Lage ist. In einer modernen Büroumgebung, wo Gigabit-Netzwerke alltäglich sind, kann ein einzelner Gigabit-Adapter leicht die Daten von einem Dutzend Remote Agents empfangen.

Es gibt Situationen, bei denen eine schnelle Verbindung Probleme darstellt. Zum Beispiel, wenn Sie ein entferntes WLAN über das Internet überwachen, kann keine hohe Bandbreitenverbindung zur Verfügung stehen. Selbst eine T3-Verbindung (4,5 Mbit/s) ist nicht ausreichend alle Pakete von einem mäßig belasteten WLAN zu übertragen. In solchen Situationen können Sie die Standardeinstellungen ändern und lassen Remote Agent die Pakete vor der Übertragung nach CommView for WiFi filtern. Die Schaltfäche [Erweiterte Netzwerkeinstellungen] auf der zusätzlichen Werkzeugleiste zur Fernüberwachung im CommView for WiFi-Hauptfenster, ermöglicht Ihnen die Option Bandbreite verringern einzuschalten. Ist diese Option eingeschaltet, wird der aktuelle CommView for WiFi-Regelsatz periodisch an Remote Agent gesendet. Dieser Regelsatz wird dann lokal übernommen, sodass nur Pakete, die den Regeln entsprechen an CommView for WiFi zurückgesendet werden. In diesem Modus kann unter Knoten kein Knoten angezeigt werden und das Register Kanäle zeigt keine volle Pro-Kanal-Statistik. Benutzen Sie diesen Modus dwshalb nur bei begrenzter Bandbreite, Sie aber trotzdem den Zugang zu Paketen eines entfernten WLAN benötigen.

Es wird sehr empfohlen, aus den gleichen Bandbreitengründen, KEINE drahtlose Verbindung für den Datenaustausch zwischen Remote Agent und CommView for WiFi zu benutzen. Es ist ebenso eine schlechte Idee, bei der Überwachung drahtloser Adapter, die durch den drahtlosen Adapter gesendeten Pakete aufzufangen und zur Kommunikation mit CommView for WiFi zu benutzen, wenn sie auf den gleichen oder geschlossenen Kanälen wirksam sind. Dies würde einfach einen Schneeballeffekt hervorrufen.

Wenn CommView Remote Agent mehr Daten erfasst, als es an CommView for WiFi senden kann, wird ein interner Puffer benutzt um die Pakete zu speichern, die nicht unmittelbar gesendet werden können. Die Puffergöße beträgt 5 Mbytes. Die Pufferauslastungsanzeige im Remote Agent-Fenster zeigt den aktuellen Pufferstatus an. Zum Beispiel, wenn das Programm 2,5 Mbytes Daten gepuffert hat, ist die Pufferauslastung 50%. Falls das Programm eine Pufferauslastung von 100% erreicht, wird die Datenpufferung gestoppt und erfasste Pakete verworfen bis wieder etwas Pufferspeicher frei ist.

Sicherheit

CommView Remote Agent for WiFi wurde mit einem Blick auf Sicherheit entwickelt. Es ist nur über ein Passwort zugänglich, welches niemals in Klartext übertragen wird und durch Benutzung eines Anfrage-/Antwortprotokolls mit einer sicheren Zerhackerfunktion abgesichert ist. Ist die

Authentifizierung erfolgreich, wird der gesamte Verkehr komprimiert und und mit demselben Passwort verschlüsselt. Bitte treffen Sie Vorkehrungen zur Sicherung Ihres Passwortes. Sobald es durch eine unauthorisierte Person aufgedeckt wird, erlangt diese Person umfassende Fähigkeiten um Ihr Netzwerk zu untersuchen und Netzwerkverkehr des entfernten Computers abzufangen.

RPCAP verwenden

> Dieses Kapitel beschreibt eine experimentelle Funktionalität, die wie erwartet funktionieren kann oder auch nicht; dies hängt von der konkreten Implementierung in Soft- und Hardware von Drittherstellern ab. Für diese Funktionalität wird keine Unterstützung angeboten.

Zusätzlich zur Funktionalität der Daten-Fernerfassung, die **CommView Remote Agent** anbietet, kann CommView for WiFi mithilfe des RPCAP auch den Netzwerkverkehr entfernter Computer erfassen. Dieses Protokoll wird von Hardware (z.B. Aerohive Access Points) und Software (z.B. WinPcap) unterstützt.

Um den Fernbeobachtungsmodus einzuschalten, wählen Sie **Datei => Fernbeobachtungsmodus**. Es erscheint eine zusätzliche Werkzeugleiste neben der Hauptwerkzeugleiste im Hauptfenster von CommView for WiFi. Klicken Sie auf **Neue RPCAP-Verbindung**, um ein Fernster für die neue Verbindung zu öffnen.

Um sich mit einem Ferngerät zu vernetzen, geben Sie dessen **Hostnamen oder IP-Adresse** ein, bestimmen Sie die **Port**-Nummer (standardmäßig verwendet RPCAP Port 2002), aktivieren Sie die Checkbox **Benutzer-Authentifikation**, geben Sie **Benutzer-ID** und **Passwort** ein, falls eine Authentifikation erforderlich ist, dann aktivieren Sie die Checkbox **Vermischter Modus**, falls dies der Erfassungsmodus ist, den Sie benutzen möchten. Klicken Sie auf **Verbinden**, um die Verbindung aufzubauen. Wenn die Verbindung aufgebaut ist, zeigt die Dropdown-Liste **Adapter** die optionalen Schnittstellen. Um die Datenerfassung zu starten, klicken Sie auf **Paketerfassung starten**.

Aruba Remote Capture verwenden

> Dieses Kapitel beschreibt eine experimentelle Funktionalität, die wie erwartet funktionieren kann oder auch nicht; dies hängt von der konkreten Implementierung in Soft- und Hardware von Drittherstellern ab. Für diese Funktionalität wird keine Unterstützung angeboten.

Zusätzlich zur Funktionalität der Daten-Fernerfassung, die CommView Remote Agent bietet, kann CommView for WiFi auch den Netzwerkverkehr der Aruba-APs erfassen.

Um den Fernüberwachungsmodus einzuschalten, wählen Sie **Datei => Fernbeobachtungsmodus**. Es erscheint eine zusätzliche Werkzeugleiste neben der Hauptwerkzeugleiste im Hauptfenster von CommView for WiFi. Klicken Sie auf **Neue Aruba Remote Capture Verbindung**, um ein Fenster für die neue Verbindung zu öffnen.

Die Fernerfassung der Pakete kann man im AP durch die Befehlszeilenschnittstelle starten. Die Aruba-Fernerfassung benutzt die folgende Syntax:

```
pcap start <interface-mac> <target-ipaddr> <target-port> 4 <maxlen>
```

Beispiel:

```
pcap start 18:64:72:e3:6a:10 192.168.0.2 5000 4 2346
```

Nachdem Sie die Fernerfassung im AP konfiguriert haben, geben Sie die Port-Nummer an, die Sie ausgewählt haben, und klicken Sie auf **Verbinden**, um Pakete von Ihrem Aruba-AP zu erhalten.

Port Referenz

Das Fenster (**Ansicht => Port-Referenz**) zeigt eine Port-Nummerntabelle und die zugehörigen Servicenamen. Dieser Bezug wird aus der Datei SERVICES erhalten, die von Windows installiert wurde. Sie finden die Datei im Verzeichnis **C:\windows\system32\drivers\etc.** Sie können diese Datei manuell editieren, wenn sie mehr Portnummern/Services hinzufügen möchten. CommView for WiFi liest diese Datei beim Programmstart, so dass Ihre Änderungen erst nach einem Neustart des Programms aktiv werden.

Eisntellungen

Sie können einige Programmeinstellungen konfigurieren im Menü **Einstellungen**.

Allgemein

- **Autostart-Paketerfassung** – Aktivieren Sie diese Checkbox, wenn CommView for WiFi sofort nach dem Programmstart mit dem Empfang von Paketen beginnen soll. Den entsprechend zu überwachenden Kanal wählen Sie mit der Dropdown-Liste.
- **Keine DNS/Auflösung** – Mit dieser Checkbox verhindern Sie, dass CommView for WiFi "reverse DNS lookups" der IP-Adressen durchführt. Wenn die Checkbox aktiviert ist bleibt die Spalte **Hostname** im Register **Letzte IP Verbindungen** leer.
- **Portnummern in Servicenamen konvertieren** – Aktivieren Sie diese Checkbox, wenn CommView for WiFi Servicenamen statt Nummern anzeigen soll. Wenn die Checkbox

aktiviert ist, wird z. B. Port **21** als **ftp** und Port **23** als **telnet** angezeigt. Über die von Windows installierte SERVICES-Datei wandelt das Programm die numerischen Werte in Servicenamen um. Sie finden die Datei im Verzeichnis **C:\Windows\system32\drivers\etc.** Sie können diese Datei manuell editieren, wenn sie mehr Portnummern/Services hinzufügen möchten.

- **MAC-Adressen in Kennnamen konvertieren** – Wandelt im Register **Pakete** MAC/Adressen in Kennnamen um. Kennnamen können über das Menü **Einstellungen => MAC Kennnamen** MAC-Adressen zugeordnet werden.
- **IP-Adressen in Kennnamen konvertieren** – Wandelt in den Registern **Pakete** und **Statistiken** IP-Adressen in Kennnamen um. Kennnamen können über das Menü **Einstellungen => IP Kennname** IP-Adressen zugeordnet werden.
- **IP-Adressen im Register Pakete in Hostnamen konvertieren** – Wählen Sie diese Checkbox, wenn CommView for WiFi aufgelöste Hostnamen statt IP-Adressen im Register **Pakete** anzeigen soll. Wenn diese Checkbox aktiv ist, versucht CommView for WiFi zuerst einen Kennnamen für die genannte IP-Adresse zu finden. Wenn kein Kennname gefunden wird oder die vorhergehende Checkbox **IP-Adressen in Kennnamen konvertieren** nicht aktiviert wurde, wird CommView for WiFi den internen DNS-Cache nach einem Hostnamen absuchen. Wenn kein Hostname gefunden wird, wird die IP-Adresse in numerischer Form dargestellt.
- **Herstellernamen in MAC-Adressen anzeigen** – CommView for WiFi ersetzt standardmäßig im Register **Pakete** die ersten drei Oktets der MAC-Adresse durch den Adapterherstellernamen. Wenn Sie dies nicht wünschen müssen Sie die Checkbox deaktivieren.
- **Defekte Pakete erfassen** – Durch Faktoren wie lange Distanzen, Radiointerferenzen und andere physikalische Phänomene können einige von Ihrem Adapter empfangene Pakete beschädigt sein, z. B. ganz oder teilweise unbrauchbare Daten enthalten. Aktivieren Sie die Checkbox, wenn solche Pakete empfangen und vom Programm dargestellt werden sollen. Dies hat Vor- und Nachteile. Der Vorteil ist, wenn Sie weit von den WLAN-Stationen bzw. Accesspoints entfernt sind, ein großer Teil der Pakete beschädigt sein kann. Sie können mit dieser Option mehr Daten sehen, selbst wenn diese wirklich beschädigt sind. Der Nachteil ist jedoch, dass Sie Daten mit ungültigen Inhalten sehen, z. B. IP-Pakete von nicht existierenden IP-Adressen. Ferner wird das Programm versuchen, wenn diese Option aktiv ist, selbst die WEP- bzw. WPA-verschlüsselten Daten zu entschlüsseln, bei denen der so genannte "Integrity Check Value" falsch ist, die Header jedoch gültig zu sein scheinen.

Speicherauslastung

Anzeige

- **Maximale Anzahl Pakete im Puffer** – Definiert die maximale Anzahl von Paketen, die das Programm im Speicher haben kann und zeigt die Paketliste (Zweites Register). Sie können z.

B. den Wert auf 3000 setzen. Dann werden nur die letzten 3000 Pakete im Speicher bzw. in der Paketliste berücksichtigt. Je höher dieser Wert ist, desto mehr Computerressourcen benötigt das Programm. Beachten Sie, wenn Sie Zugang zu sehr vielen Paketen benötigen, dass Sie die Autospeicherungsfunktion nutzen (mehr dazu unter **Logging**). Damit können Sie alle Pakete in einer Logdatei auf der Festplatte ablegen.

- **Maximale Zeilenanzahl der aktuellen IP-Verbindungen** – Legt die Anzahl der Zeilen zur Anzeige der aktuellen IP- Verdingungen fest. Wenn die Anzahl der Verbindungen den Schwellenwert überschreitet, werden die Verbindungen die am längsten nicht aktiv waren aus der Liste entfernt.
- **Treiber-Puffer** – Definiert die Treiberpuffergröße. Diese Einstellung beeinflusst die Performance des Programms. Je mehr Speicher für den Treiberpuffer reserviert ist, desto weniger Pakete verliert das Programm. Für LAN's mit geringem Verkehr ist die Puffergröße nicht wichtig. Für WLAN's mit hohem Verkehr sollten Sie jedoch die Puffergröße erhöhen, wenn das Programm zu viele Pakete verliert. Die Anzahl der verlorenen Pakete ermitteln Sie mittels **Datei => Durchsatzdaten** wenn die Paketerfassung aktiviert ist.

Letzte IP-Verbindungen

- **Logik anzeigen** – Ermöglicht die Auswahl des Layouts der aktuellen IP-Verbindungen an Ihre Bedürfnisse anzupassen. Mit der Auswahl eines Objektes aus der Dropdown-Liste wird die ausgewählte Logik angezeigt.
- **Lokale IP-Adressen definieren** – Dieses Tool sollten Sie verwenden, wenn Sie WLAN-Verkehr beobachten, der viele Pass-through-Pakete und eine Mischung aus internen und externen IP-Adressen enthält. In solch einer Situation weiß CommView for WiFi nicht, welche IP-Adressen als lokale Adressen definiert werden sollen und könnte dann die IP-Adressen in den Quell- und Ziel-IP-Spalten vertauschen. Mit diesem Werkzeug definieren Sie die lokalen Netzwerkadressen und Subnet-Masken, um sicher zu sein, dass die aktuellen IP-Verbindungen richtig angezeigt werden. Dies funktioniert jedoch nur mit der standardmäßigen **Smart-Logik**.

Farben

- **Paketfarbe** – Definiert die Farben für die verschiedenen Paketarten (normal, schadhafte CRC, schadhafte ICV) im Register **Pakete**.
- **Paket-Header einfärben** – Aktivieren Sie diese Checkbox, wenn CommView for WiFi Paketinhalte einfärben soll. Wenn diese Checkbox aktiv ist, zeigt das Programm die ersten acht Paketschichten mit verschiedenen Farben an. Zum Ändern einer Farbe wählen Sie die zu ändernde Header-Art und klicken dann auf das farbige Rechteck.

- **Formelsyntax hervorheben** – Definiert die Farben zum Hervorheben der Schlüsselwörter in den Formeln für die **Erweiterte Regeln**.
- **Ausgewählte Bytesequenzfarbe** – Definiert den Font und die Hintergrundfarbe für die Darstellung der Bytesequenz, die im Decoderbaum gewählt wurde. Wählen Sie z. B. den TCP-Baumknoten, werden die entsprechenden Teile des Pakets mit diesen Farben hervorgehoben.
- **Rahmenfarbverwaltung** – Stellt die Farben für verschiedene Typen von Verwaltungsrahmen ein. Farbe wird in der Spalte **Protokoll** des Registers **Pakete** benutzt um zugehörige Rahmentypen anzuzeigen.

Decodierung

- **Inhalt aller Knoten im Decoderfenster anzeigen** – Aktivieren sie diese Checkbox, um alle Knoten im Decoderfenster automatisch geöffnet darzustellen wenn Sie ein neues Paket in der Paketliste wählen.
- **Letzten Knoten aufklappen** – Aktivieren Sie diese Checkbox, wenn Sie möchten, dass die letzten Knoten im Decoderfenster automatisch aufgeklappt werden, wählen Sie ein neues Paket in der Paketeliste aus und geben die Anzahl der aufzuklappenden Knoten ein.
- **Ebene ausklappen** – Bestimmen Sie die Anzahl der Ebenen, die Sie ausklappen möchten.
- **Für ASCII-Export nur bis zur ersten Ebene decodieren** – Diese Option beeinflusst das Decodierformat für den Export eines Paketlogs bzw. eines individuellen Paketes als ASCII-Datei mit Decodierung. Wenn diese Checkbox aktiv ist, werden nur die Knoten der höchsten Ebene abgespeichert. Wenn Sie z. B. ein TCP/IP-Paket speichern möchten, während diese Funktion deaktiviert ist, werden alle Arten von Service-Sub-Knoten auch gespeichert. Wenn die Option aktiv ist, werden die Sub-Knoten nicht mitgespeichert. Damit wird die Ausgabe der ASCII-Dateien weniger detailliert und kompakter.
- **Falsche Prüfsummen für die TCP-Sitzungsrekonstruktion ignorieren** – Hiermit beeinflussen Sie, wie CommView for WiFi mit schadhaften TCP/IP-Paketen umgeht, wenn das Programm TCP-Sitzungen rekonstruiert. Standardmäßig ist diese Option aktiviert, d.h. auch Pakete mit falscher Prüfsumme werden in der Rekonstruktion berücksichtigt und angezeigt. Wenn Sie diese Option abschalten, werden Pakete mit falscher Prüfsumme verworfen und nicht im TCP-Rekonstruktionsfenster angezeigt.
- **Paketnummern einbinden bei Sitzungsrekonstruktion** – Aktivieren Sie diese Checkbox, wenn Sie möchten, dass die Dateneinheiten im TCP-Sitzungsrekonstruktionsfenster mit zugehörigen, vorangestellten Paketnummern dargestellt werden.
- **Bei TCP-Sitzungsrekonstruktion nach dem Sitzungsstart suchen** – Wenn diese Checkbox aktiviert ist, wird das Programm versuchen, den Beginn der TCP-Sitzung zu finden, wenn Sie die Sitzung rekonstruieren. Ist die Checkbox nicht aktiviert, wird die Sitzung von dem gewählten Paket ausgehend rekonstruiert, d.h. früher Pakete werden verworfen.

- **GZIP-Inhalt entpacken** – Aktivieren Sie diese Checkbox damit CommView for WiFi GZIP-komprimierten HTTP-Inhalt in lesbaren Text innerhalb des TCP-Sitzungsrekonstruktionsfenster darstellt. GZIP-Inhalt wird nur dekomprimiert, wenn der Anzeigetyp im Fenster auf ASCII gesetzt ist.
- **Bilder rekonstruieren** – Aktivieren Sie diese Checkbox, wenn CommView for WiFi binäre HTTP-Streams, die Bilder darstellen, in betrachtungsfähige JPG-, BMP-, PNG- und GIF-Bilder im TCP-Sitzungsrekonstruktionsfenster verwandeln soll. Bilder werden nur angezeigt, wenn der Anzeigetyp im Fenster auf HTML gestzt ist. Bilder werden niemals innerhalb der HTML-Seite angezeigt, zu der sie gehören, sie werden durch den Server in einer separaten Sitzung übertragen.
- **IPv4-Formendungen in IPv6-Adressen verwenden** – Wenn diese Checkbox nicht angekreuzt ist, werden IPv6-Adressen nur in hexadezimaler Schreibweise dargestellt, z.B. fe80::02c00:26ff:fe2d:edb5. Ist die Checkbox angekreuzt, werden die letzten 4 Byte der IPv6-Adressen in der IPv4-Darstellungsart angezeigt, z.B. fe80::02c00:26ff:254.45.237.181.
- **Fragmentierte IP-Paket wieder zusammensetzen** - Aktivieren Sie diese Checkbox an, wenn das Programm fragmentierte IP-Pakets wieder zusammensetzen soll. Standardmäßig werden fragmentierte IP-Pakete angezeigt, wie Sie empfangen wurden, in ihrer Originalform. Ist diese Option eingeschaltet, wird das Programm einen internen Fragmentpuffer erhalten und versuchen, die Fragmente zusammenzufügen. Dabei werden nur erfolgreich zusammengesetzte Fragmente als Ergebnis angezeigt.
- **Signalstärke in dBm anzeigen** – Aktivieren Sie diese Checkbox wenn Sie möchten, dass die Signalstärke in dBM anstatt in Prozent angezeigt werden soll. Die Nutzbarkeit der Signalstärke in dBM ist abhängig vom benutzten drahtlosen Adapter. Weiterführende Informationen finden Sie im Kapitel Signalstärke.
- **Standard Anzeigetyp** – Wählen Sie aus der Dropdown-Liste den Anzeigetyp, den Sie als Standard für die TCP-Sitzungsrekonstruktion setzen wollen. Erlaubte Werte sind ASCII, HEX, HTML und EBCDIC.

VoIP

Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

- **VoIP-Analyse deaktivieren** – Deaktivierung der Erfassung und Analyse von VoIP-Daten. Aktivieren Sie diese Checkbox wenn Sie nicht mit VoIP arbeiten und wenn Sie die Benutzung der Computerressourcen duch die Applikation minimieren möchten.

- **Maximale Aufzeichnungen in der Liste** – Begrenzt die Anzahl der angezeigten und verarbeiteten VoIP-Vorgänge. Wenn die Anzahl der Aufzeichnungen die festgelegte Begrenzung übersteigt, werden ältere Aufzeichnungen aus der Liste gelöscht.
- **Verwaiste RTP-Ströme ignorieren** – Wenn diese Checkbox aktiviert ist, ignoriert der VoIP-Analyser RTP-Datenströme die keine Ausgangssignalsitzung haben. Verwaiste RTP-Ströme entstehen typischerweise wenn die Paketerfassung in der Mitte eines Telefonates gestartet wird oder das Signalprotokoll der Applikation unbekannt ist (z.B. kein SIP oder H.323) oder das Signalprotokoll wurde in einer nichtstandardisierten Art und Weise gesendet (z.B. verschlüsselt oder als Teil einiger anderer Sitzungen). Solche Ströme sind immer noch zur Analyse verfügbar und manchmal zur Wiedergabe. Schauen Sie bitte in das Kapitel **Telefonate wiedergeben** um detaillierte Informationen über die Wiedergabe von Telefonaten zu erhalten. Deaktivieren Sie diese Option, wenn Sie kein Interesse an solchen verwaisten Strömen haben und Computerressourcen sparen möchten. Beachten Sie, wenn verwaiste Ströme nicht ignoriert werden kann der VoIP-Analyser über das UDP-Protokoll übertragene Ströme irrtümlicherweise als RTP-Ströme identifizieren. Allgemein ist dies kein Fehler, weil RTP-Pakete keine standardisierte einheitliche Signatur besitzen, deshalb sind solche "Falschpositiven Ergebnisse" in Ordnung.
- **Beschädigte Pakete im VoIP-Analyser ignorieren** – Wenn diese Checkbox aktiviert wird, werden drahtlose Pakete mit schlechtem CRC durch das VoIP-Analysermodul verworfen. Dies hinderd die Applikation daran "Geistersignale" zu erstellen oder Medienströme, die wie Pakete mit schlechtem CRC erscheinen, werden nicht ausgeschieden.

Geo-Standort

Geo-Standort ist die Länderzuordnung für IP-Adressen. Wenn diese Funktionalität aktiviert ist, überprüft CommView for WiFi die interne Datenbank um die zugehörigen Ländernformationen für jede IP-Adresse. Sie können das Programm so konfigurieren, dass es den **ISO-Ländercode**, den **Landesnamen** oder die **Landesflagge** für jede IP-Adresse anzeigt. Sie können Geo-Standort auch deaktivieren. Für einige reservierte IP-Adressen (z. B. 192.168.*.* oder 10.*.*.*) kann keine Länderinforrmation zugeteilt werden. In solchen Fällen wird der Landesname nicht angezeigt, oder falls Sie die Option **Landesflagge** benutzen, wird eine Flagge mit einem Fragezeichen angezeigt.

Wenn die IP-Zuweisung ständig wechselt, ist es wichtig, dass Sie immer eine aktuelle Version von CommView for WiFi benutzen. Eine frische aktuelle Datenbank ist in jeder Ausgabe von CommView for WiFi. Eine frische Datenbank hat eine 98%ige Treffgenauigkeit. Ohne Updates fällt die Treffgenauigkeit jedes Jahr prozentual um ca. 15%.

Verschiedenes

- **Bei minimierter Darstellung nicht in der Taskleiste anzeigen** – Aktiveren Sie diese Checkbox, wenn beim Minimieren des Fensters der Button nicht in der Taskleiste angezeigt werden soll. Wenn diese Checkbox aktiv ist wird das Programm nach der Minimierung über ein System Tray-Icon erneut geöffnet.
- **Verlassen der Applikation bestätigen** – Aktivieren Sie diese Checkbox, wenn Sie die Programmbeendigung bestätigen möchten.
- **Auto-Scrollen im Register Pakete** – Wenn diese Checkbox aktiv ist, scrollt das Programm den Text im Register Pakete automatisch, wenn Sie ein neues Paket aus der Paketliste auswählen (nur wenn der Text nicht in das Fenster passt). Dies ist nützlich, wenn sie bei einem großen Paket die Inhalte ansehen wollen ohne manuell scrollen zu müssen.
- **Auto-Scrollen in Paketliste zum letzten Paket** – Wenn diese Checkox aktiv ist, scrollt das Programm automatisch im Register **Pakete** die Paketliste durch bis zum letzten erhaltenen Paket.
- **Sortieren neuester Datensätze der aktuellen IP-Verbindungen** – Wenn diese Checkbox aktiv ist, sortiert das Programm automatisch die neuen Einträge im Register **Aktuelle IP Verbindungen** nach einem benutzerdefinierten Kriterium (z. B. aufsteigende Reihenfolge der Remote-IP-Adressen).
- **Smart CPU-Control verwenden** – Wenn diese Checkbox aktiv ist versucht das Programm durch Senkung der Qualität und Frequenz der Bildschirm-Updates die CPU-Last beim Empfangen von sehr starkem Verkehr zu senken.
- **Mit Windows starten** – Wenn diese Checkbox aktiv ist startet das Programm jedesmal, wenn Windows gestartet wird. Unter Windows Vista und höher, ist diese Checkbox wirkungslos, wenn UAC aktiviert ist. Dies ist eine Einschränkung von Vista die letzten Windows-Versionen, die verhindern, dass Applikationen mit höheren Rechten beim Windowsstart geladen werden. Wenn diese Funktionalität wichtig ist, deaktivieren Sie UAC.
- **Minimiert starten** – Wenn diese Checkbox aktiv ist, wird das Programm minimiert gestartet und das Hauptfenster nicht angezeigt bis Sie das Systemtray-Icon oder den Taskleisten-Button gedrückt haben.
- **Gitternetz anzeigen** – Lässt das Programm Rasterlinien in den Pakete-, Kanäle-, und AP-Listen anzeigen.
- **Automatische Applikations-Updates aktivieren** – Mit dieser Checkbox lassen Sie das Programm sich regelmäßig mit der TamoSoft-Website verbinden und nach Updates suchen. Mit dem Eingabefeld **Intervall zwischen den Checks** definieren Sie in welchen Abständen diese Überprüfung durchgeführt werden soll.

Plug-Ins

Dieser Bereich wird für Plug-Ins von Drittherstellern benötigt um Konfigurationsaufgaben zu ermöglichen. Weitere Informationen finden sie unter **Maßgeschneidertes Decoding**.

Häufig gestellte Fragen

In diesem Kapitel finden Sie die Antworten auf einige der am häufigsten gestellten Fragen.

F1. Ich bin in einem WLAN und möchte meine eigenen ein- und ausgehenden Pakete ansehen. Welches Produkt brauche ich: Standard non-wireless CommView Edition oder CommView for WiFi?

A. Sie brauchen die Standard non-wireless CommView Edition. Damit können Sie Ihren eigenen Verkehr ansehen, können aber nicht den Verkehr anderer WLAN-Stationen sehen. Im Gegensatz zur Standard CommView Edition ermöglicht Ihnen CommView for WiFi andere WLAN-Stationen zu überwachen, Management frames zu erfassen, die Signalstärke anzuzeigen, usw.

F2. Brauche ich besondere Hardware um CommView for WiFi nutzen zu können?

A. Ja, Sie brauchen ein kompatibles WLAN-Adapter. Eine Liste kompatibler Adapter finden Sie unter **https://www.tamos.com/download/main/ca**. Zwecks Aktivierung der Überwachungsmöglichkeiten Ihres WLAN-Adapters, benötigen Sie die mit diesem Produkt mitgelieferten speziellen Treiber. Wenn CommView for WiFi nicht läuft, kann Ihr Adapter mit anderen WLAN-Hosts oder Accesspoints kommunizieren, so als würden Sie den Originaltreiber benutzen, den Sie vom Adapterhersteller bezogen haben. Wenn jedoch CommView for WiFi aktiviert ist, befindet sich Ihr Adapter in einem passiven, "promiskösen" Überwachungsmodus.

F3. Meine Karte ist nicht auf der Liste der unterstützten Hardware. Was kann ich tun?

A. Unsere Kompatibilitätsliste beinhaltet nur die Karten, die wir in unseren Labors getestet haben. Es gibt andere Karten, die mit CommView for WiFi kompatibel sein können. Der beste Weg, herauszufinden ob Ihre Karte kompatibel ist, ist unser **Adapter-Testprogramm** herunterzuladen und auf Ihrem Computer laufenzulasssen. Wenn ein kompatibler Adapter installiert ist, zeigt das Tool dessen Namen. Bevor Sie unser Testprogramm laufen lassen, stellen Sie bitte sicher, dass Sie den aktuellsten Treiber benutzen, der mit ihrem Computer oder Netzwerkadapter mitgeliefert wurde. Besuchen Sie deren Webseite, um die aktuellste Treiberversion herunterzuladen. Dies ist wichtig, weil der Test vom benutzten Treiber abhängig ist. Je neuer der Treiber ist, umso besser ist die Chance, dass er mit CommView for WiFi arbeitet. Zum Schluss, Sie können eine kompatibele Karte kaufen, die derzeitig nicht sehr teuer ist. Oder bestellen Sie eine verpackte CommView for WiFi-Version, die immer einen kompatiblen Adapter enthält.

F4. Welcher Adapter empfehlen Sie für die Verwendung mit Ihrer Anwendung?

A. Wir empfehlen, dass Sie die Liste der kompatiblen Hardware einsehen, die Sie hier finden https://www.tamos.com/download/main/ca. Bei Benutzung dieser Auflistung, wählen Sie den besten, auf der Anschlussform basierenden Adapter (USB, USB integriert usw.). Empfindlichkeit, unterstützte Windows-Version und unterstützte 802.11-Bänder. Ein 802.11ac-USB-Adapter ist allgemein die beste Wahl.

F5. Welche der unterstützten Adapter haben externe Antennenanschlüsse?

A. Alfa Networks AWUS1900 und Alfa Networks AWUS036ACM.

F6. Kann ich simultan Daten von mehreren Kanälen aufzeichnen?

A. Ja, wenn Sie verschieden unterstützte USB-Adater benutzen. Für weitere Informationen schauen Sie bitte ins Kapitel Mehrkanalerfassung.

F7. Ich habe einen speziellen Treiber für mein Adapter installiert und jetzt scheint mein Adapter abgeschaltet zu sein und ich kann mich nicht mit meinem Netzwerk verbinden, wenn ich CommView for WiFi geschlossen habe. Was kann das Problem sein?

A. Wenn Sie den Treiber für Ihr Adapter erneuern, können die Konfigurationseinstellungen (inkl. bevorzugte Netzwerke und Passwörter) verloren gehen, Sie müssen deshalb das Adapter rekonfigurieren. Wenn Ihr Adapter konfiguriert wurde und sich immer noch nicht verbinden kann, deaktivieren und aktivieren Sie es erneut im Gerätemanager, dies wird die Verbindungssfähigkeit wiederherstellen.

F8. Einige Kanäle im Fenster für die Kanalauswahl werden nicht aufgeführt. Ist das normal? Was ist, wenn ich will diese Kanäle überwachen?

A. Die Antwort hängt vom Adaptertyp und dem Betriebssystem ab.

- Empfohlene Ralink-, MediaTek- und Realtek-basierte USB-Adapter: Alle Kanäle sind immer verfügbar, wenn sie in CommView für WLAN verwendet werden.
- Empfohlene Intel-basierte Adapter: Die Kanalverfügbarkeit kann vom jeweiligen Modell abhängen. Wir versuchen auf jeden Fall alle Kanäle verfügbar zu machen.
- Andere Adapter (z. B. Dell oder Broadcom): Die Aktivierung der Kanäle 12 und 13 ist möglicherweise möglich. Öffnen Sie das CommView for WiFi-Anwendungsordner (normalerweise C:\Programme (x86)\CommViewWiFi). Dort sehen Sie die Datei mit dem Namen **ch1213.exe**. Doppelklicken Sie auf diese Datei, um sie auszuführen. Starten Sie CommView for WiFi neu und diese Kanäle stehen zur Auswahl zur Verfügung. Beachten Sie, dass die Fähigkeit des Adapters, Pakete auf den Kanälen 12 und 13 zu erfassen, von der vom Laptop-Hersteller festgelegten Regulierungsdomäne abhängt. Wenn der Anbieter sie

aktiviert hat, wird es kein Problem geben. Wir haben jedoch von vielen Beispielen gehört, bei denen Laptop-Anbieter die Kanäle 12 und 13 nicht aktiviert haben, sogar bei Laptops, die in einem Land verkauft wurden, in dem diese Kanäle legal waren.

F9. Kann man bei der überwachung eines WLANs sicher sein, dass man alle übertragenen Pakete empfängt?

A. Nein, und hier ist warum. Wenn eine WLAN-Station verbunden und authentifiziert ist, startet die Station bzw. der Accesspoint einen Prozess, Pakete erneut zu senden die nicht empfangen wurden oder auf dem Weg beschädigt wurden (z. B. durch Radiointerferenzen). Bei CommView for WiFi wird der WLAN-Adapter in einen passiven überwachungsmodus veresetzt. Deshalb kann das System keine Aufforderungen senden, bestimmte Pakete erneut zu versenden. Dies resultiert im Verlust einiger Pakete. Der Anteil der so verlorengegangenen Pakete variiert. Je näher Sie sich an der Station bzw. am Accesspoint befinden, desto weniger Pakete gehen verloren.

F10. Kann das Programm WPA- und WPA2-verschlüsselte Pakete entschlüsseln?

A. Ja, im WPA-PSK-Mode. Beide, TKIP (WPA) und AES/CCMP (WPA2) werden unterstützt. WPA3 kann nicht entschlüsselt werden. WPA3 benutzt die Passphrase nur zur Authentifizierung; Entschlüsselung ist unmöglich.

F11. Ich bin in einem WLAN mit hohem Verkehrsvolumen und es ist schwer einzelne Pakete zu untersuchen, wenn die Applikation hunderte oder tausende von Paketen pro Sekunde empfängt, weil die alten Pakete schnell aus der Pufferanzeige entfernt werden. Kann ich etwas dagegen tun?

A. Ja, Sie können den Button **Aktuellen Puffer in neuem Fenster öffnen** auf der kleinen Werzeugleiste des Registers **Pakete** benutzen. Das ermöglicht Ihnen bei jedem Intervall, soviele Schnappschüsse des aktuellen Puffers zu erstellen, wie Sie möchten. Sie werden dann in der Lage sein, die Pakete in den neuen Fenstern in Ihrer arbeitsfreien Zeit zu untersuchen.

F12. Ich habe das Programm gestartet, einen Kanal gewählt und mit der Erfassung begonnen, es werden jedoch keine Pakete angezeigt. Helfen Sie bitte!

A. Öffnen Sie zunächst das Register **Pakete**. Das Register **Aktuelle IP-Verbindungen** kann leer sein, wenn Sie keine korrekten WEP-Schlüssel eingegeben haben und Ihr WLAN WEP-Verschlüsselung anwendet. Wenn auch das Register **Pakete** leer ist, überprüfen Sie bitte die Statusleiste des Programms (status bar). Wenn der Paketzähler erhöht wird haben Sie aktive Regeln, die verhindern, dass das Programm Pakete anzeigt. Klicken Sie auf **Regeln => Alle Rücksetzen** und betätigen Sie dann die drei Werkzeugleisten-Buttons: **Datenpakete erfassen**, **Managementpakete erfassen** und **Kontrollpakete erfassen**. Wenn der Paketzähler in der Statusleiste nicht zunimmt, sind die WLAN-Stationen nicht aktiv oder es sind keine Accesspoints erkannt wurden. Wenn Sie

vollkommen sicher sind, dass WLAN-Stationen oder Accesspoints existieren, melden Sie das Problem bitte an uns weiter.

F13. Kann CommView for WiFi NCF-Logdateien lesen, die von der CommView Non-Wireless-Standardedition stammen? Wie wäre es umgekehrt?

A. Ja, CommView for WiFi kann die von der Non-Wireless-Standardedition erzeugten NCF-Logdateien lesen. Die Non-Wireless- Standardedition kann ebenso die von CommView for WiFi erzeugten NCF-Logdateien lesen (und bald wird das Programm die aktuellesten NCFX-Lofdateien auch lesen), aber Sie können keine wireless-spezifischen Spalten sehen, wie z. B. die Signalstärke oder die Kanalnummer.

F14. Arbeitet CommView for WiFi auf Multi-Prozessor-Computern?

A. Ja.

F15. Es scheint unmöglich zu sein, mehr als 5000 Pakete vom Paketpuffer zu speichern. Gibt es eine Abhilfe?

A. Aktuell exististiert keine solche Begrenzung. Die Applikation benutzt einen Umlaufpuffer zur Speicherung erfasster Pakete. Standardmäßig kann der Puffer die letzten 5000 Pakete aufnehmen, aber dieser Wert kann über die **Einstellungen** angepasst werden. Die maximale Puffergröße beträgt 20000 Pakete (der Puffer kann aus einem nahe liegenden Grund nicht unbegrenzt sein: Ihr Computer-RAM ist nicht unbegrenzt). Sie können den Pufferinhalt unter Benutzung des Registers **Protokolle** in eine Datei speichern. Diese Begrenzung der Puffergröße schränkt die Fähigkeit zur Speicherung einer Anzahl von Paketen keineswegs ein. Sie brauchen nur die automatische Protokollierung im Register **Protokolle** aktivieren. Eine solche automatische Protokollierung veranlasst die Applikation zur kontinuierlichen Ausgabe der erfassten Pakete in Dateien und Sie können eine Begrenzung der Gesamtgröße der erfassten Daten festlegen.

F16. Meine Firewall-Software warnt mich, dass CommView for WiFi versucht sich mit dem Internet zu verbinden. Ich weiß, dass manche Webseiten die Besucher tracken können, indem sie die Information sammeln, die durch das Programm über das Internet geschickt wird. Warum versucht CommView for WiFi sich mit dem Internet zu verbinden?

A. Drei Dinge können Ihre Firewall alarmiert haben. Das kann zum einen der Versuch sein, eine IP-Adresse in einen Hostnamen aufzulösen. Da CommView for WiFi Kontakt zu Ihrem DNS-Server hat um DNS-Anfragen durchzuführen, kann so unausweichlich ein Alarm ausgelöst werden. Dies können Sie unter **Einstellungen => Optionen => Keine DNS Auflösung** deaktivieren, dann werden aber keine Hostnamen mehr im Register Letzte IP-Verbindungen angezeigt. Es kann zweitens sein, dass Sie das Programm so konfiguriert haben, dass es nach Updates bzw. neueren Versionen sucht. Dabei verbindet sich CommView for WiFi mit www.tamos.com. Dies können Sie unter

Einstellungen => Optionen => Versch. => Automatische Applikations-Updates aktivieren/ deaktivieren. Drittens: Wenn Sie das Programm kaufen, müssen Sie es aktivieren. Falls Sie Online-Aktivierung wählen, muss CommView for WiFi sich mit www.tamos.com verbinden. Sie können dies umgehen, wenn Sie die manuelle Aktivierung auswählen. Dies sind die einzigen Gründe warum CommView for WiFi allenfalls eine Verbindung ins Internet herstellt. Es gibt keine versteckten Aktivitäten. Wir verkaufen keine Spyware.

F17. Ich bin oft als Benutzer und ohne administrative Rechte angemeldet. Muss ich mich um CommView for WiFi zu starten abmelden und als Administrator wieder anmelden?

A. Nein. Sie können das CommView for WiFi-Verzeichnis öffnen, rechtsklicken Sie dann auf CA.exe während Sie Shift gedrückt halten und wählen Sie dann **Ausführen als…** aus dem Kontextmenü. Geben Sie den administrativen Login und das Passwort ein und klicken Sie dann auf **OK** um das Programm zu starten. Unter Windows Vista und höher startet CommView for WiFi automatisch mit erhöhten Rechten.

F18. Bei der Rekonstruktion von TCP-Sitzungen die japanische oder chinesische HTML-Seiten beinhalten kann ich den Originaltext nicht sehen.

A. Zur Anzeige ostasiatischer Sprachen sollten Sie ostasiatische Fonts installieren. Öffnen Sie **Systemsteuerung => Ländereinstellungen**, wählen Sie das Register **Sprachen** und aktivieren Sie die Checkbox **Dateien für ostasiatische Sprachen installieren**.

F19. Ich bin etwas verwirrt durch die für CommView for WiFi verfügbaren Lizenztypen. Können Sie die Unterschiede zwischen den Lizenztypen erklären?

A. Zwei Lizenztypen sind gegenwärtig für CommView for WiFi verfügbar: die Standardlizenz und die VoIP-Lizenz. Die teurere VoIP-Lizenz erlaubt alle Applikationsfunktionen, inklusive des VoIP-Analysers, während die Standardlizenz den VoIP-Analyser nicht freigibt.

Zusätzlich ist die Standardlizenz auch als Jahresabonnement verfügbar, was eine zeitlich limitierte Lizenz darstellt, gültig für 1 Jahr ab Kaufdatum.

CommView for WiFi ist auch als verpacktes Produkt erhältlich. Verpackte Produkte beinhalten einen kompatiblen drahtlosen Adapter und einen USB-Stick. Im Preis enthalten ist der UPS-Basis-Versand.

Andere Lizenzbedingungen und Konditionen entnehmen Sie bitte der mit dem Produkt gelieferten Endbenutzerlizenz.

F20. Kann ich Ton vom VoIP-Analyser in eine Standard-.wav- oder .mp3-Datei speichern?

A. Nicht direkt, aber er gibt eine Menge Hilfsmittel auf dem Markt, die ein "virtuelles Audiokabel" anbieten, welches alles in eine Datei speichert, was Ihre Soundkarte abspielt. Versuchen Sie zum Beispiel, **Xilisoft Sound Recorder** (benutzen Sie den Modus "Was Sie hören").

VoIP-Analyse

> Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

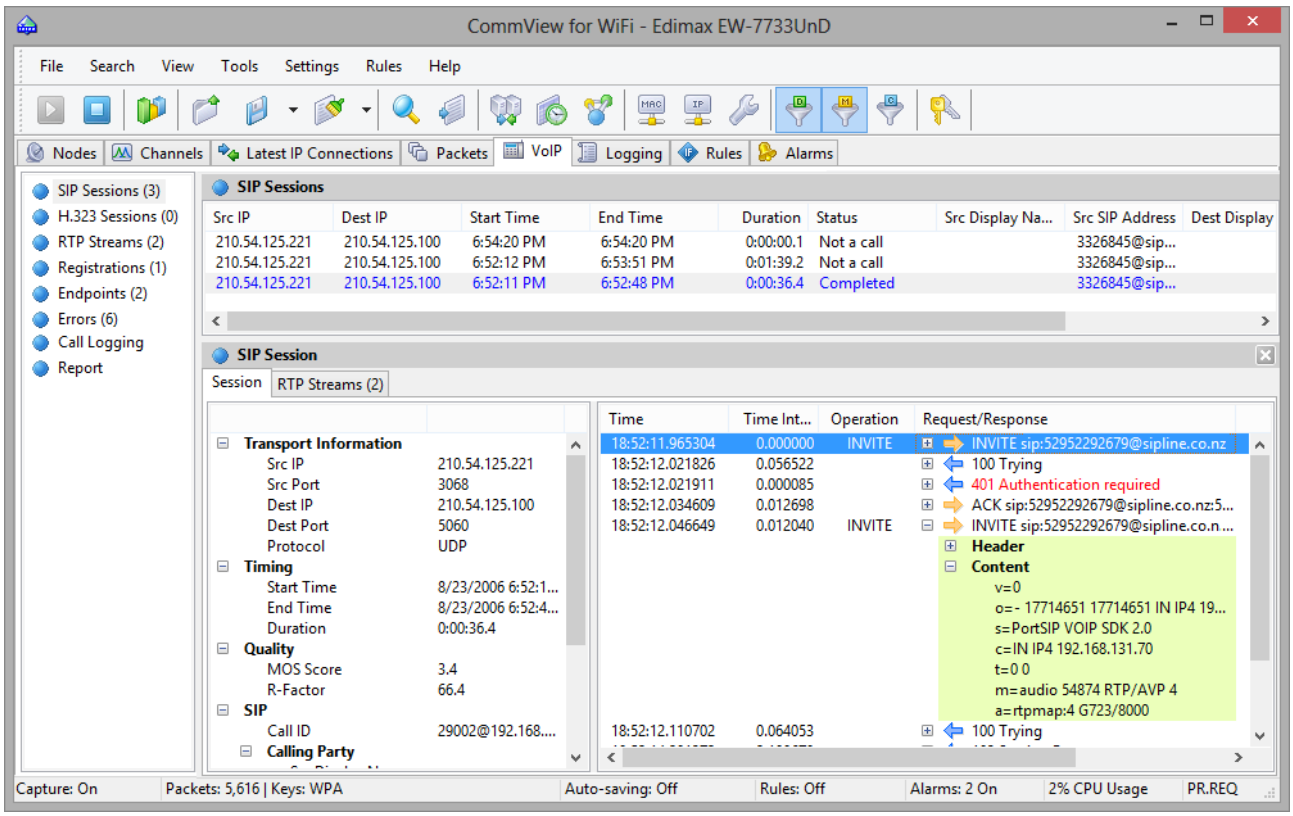
Der VoIP-Analyser ist ein eingebautes CommView-Modul, dass für die Echtzeiterfassung und Analyse von Internettelefonie (VoIP) geeignet ist, darunter fallen Anrufabläufe, Nahrichtenübermittlungen, Registrierungen, Medienströme, Fehler usw. Dieses Hilfsmittel hilft, durch die Sichtbarmachung dieser Daten und Beurteilung der Sprachqualität, Ihre Produktivität bei der Austestung von Netzwerken, Software und Hardware zu steigern. CommView's VoIP-Analyser unterstützt **SIP 2.0-** und **H.323**-Nachrichtenprotokolle und **RTP 2.0-**Medienströme und viele weitverbreitete Codecs. Zusätzlich zur Echtzeitanalyse, kann der Analyser für den nachträglichen Import der erfassten Daten und zur Analyse von Erfassungsprotokollen in einer Vielzahl von Formaten (z.B. Tcpdump, EtherPeek, usw.) genutzt werden.

Wenn Ihre drahtlose Netzwerk WEP oder WPA-Verschlüsselung benutzt, sollen Sie WEP oder WPA-Schlüssel korrekt konfigurieren, um den Netzwerkverkehr entschlüsseln zu können; anders, wird VoIP-Analyse nicht verfügbar sein. Siehe **WEP/WPA Schlüssel** und **Hintergründe der WPA-Entschlüsselung** nach mehr Information.

Arbeit mit dem VoIP Analysator

> Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Der VoIP-Analysator wird über das Register VoIP des Hauptfensters erreicht, in dem die Echtzeitanalyse erfasster Pakete aufgeführt wird oder durch das **VoIP-Protokoll-Betrachterfenster**, dass benutzt werden sollte, wenn Sie eine nachträgliche Analyse von Protokolldateien ausführen möchten. Der VoIP-Analyser arbeitet korrekt mit der Paketerfassung und zeigt die Ergebnisse in Echtzeit an:



Die Informationen im VoIP-Analyser-Fenster werden in verschiedenen Kategorien gegliedert. Die Kategorienauflistung wird im Fensterausschnitt angeordnet und ermöglicht die Auswahl und Ansicht detaillierter Analysedaten, welche im rechten Teil des Fensters dargestellt werden. Die folgenden Kategorien sind verfügbar:

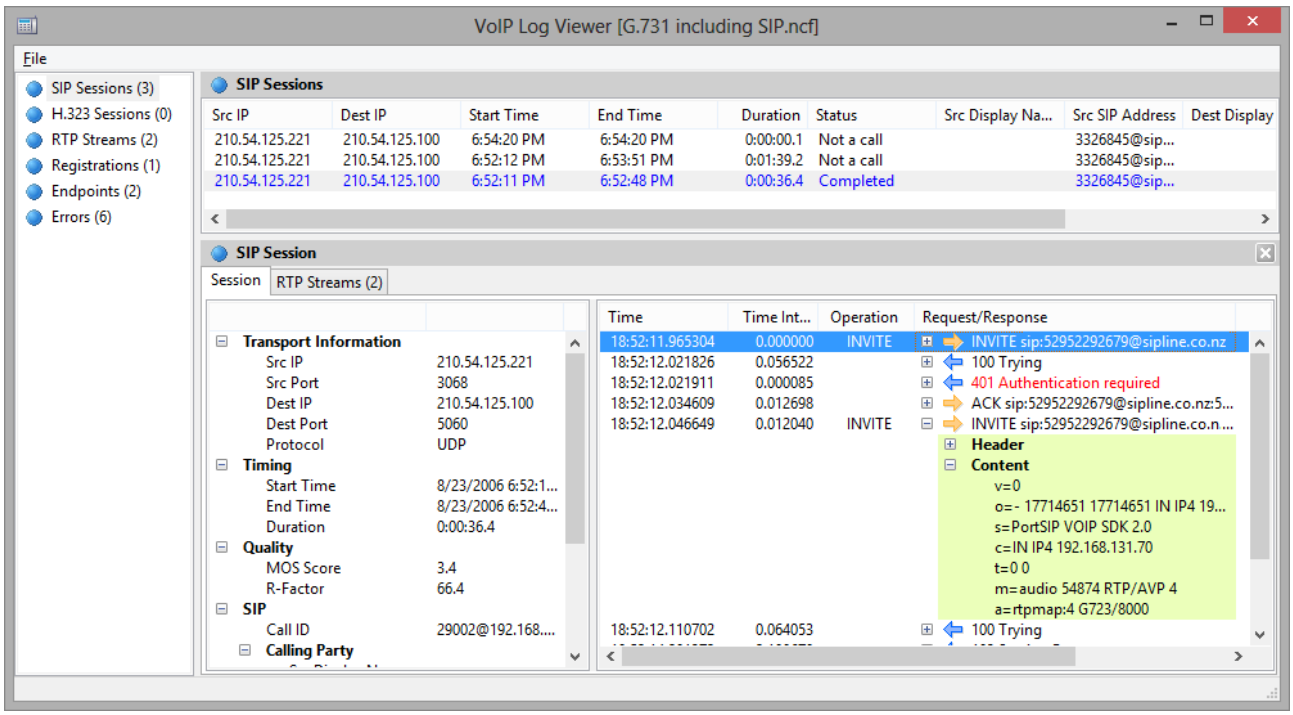
- **SIP-Sitzungen** – Auflistung erfasster SIP 2.0-Sitzungen.
- **H.323-Sitzungen** – Auflistung erfasster H.323-Sitzungen.
- **RTP-Ströme** – Auflistung erfasster RTP-Ströme.
- **Registrierungen** – Auflistung der am Registrations-Server registrierten Klienten und der Klienten-Registrierungsverlauf.
- **Endpunkte** – Auflistung der am VoIP-Datenaustausch beteiligten Arbeitsplätze.
- **Fehler** – Auflistung der während des VoIP-Datenaustausches registrierten Fehler.
- **Anrufprotokoll** – Protokollkonfiguration für erfasste VoIP-Daten.
- **Bericht** – Konfiguration der Berichtserstellung, inklusive des Automatikmodus.

Für detaillierte Informationen, über die Datenanordnung im VoIP-Analyser, verweisen wir auf das Kapitel **Arbeiten mit Auflistungen im VoIP-Analyser**.

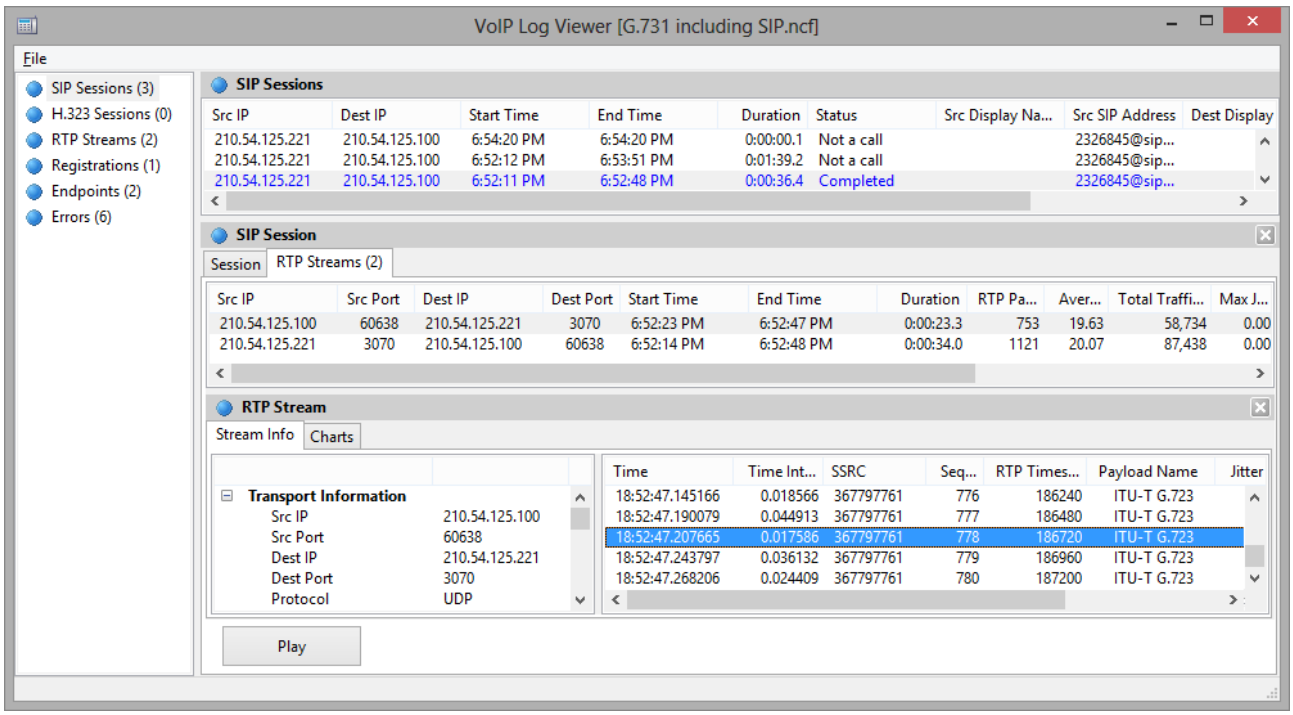
SIP- und H.323-Sitzungen

> Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Der VoIP-Analyser unterstützt aktuell zwei Typen von VoIP-Signalprotokollen, SIP und H.323. SIP- und H.323-Sitzungen werden als zwei separate Elemente im linken Fensterausschnitt dargestellt. Durch Auswahl eines der Elemente werden die zugehörigen, durch die Applikation erfassten Nachrichtensitzungen und detaillierte Informationen zu jeder Sitzung dargestellt:



Der obere Fensterausschnitt zeigt eine komplette Auflistung der erfassten SIP- oder H.323-Sitzungen. Wenn Sie eine SIP-/H.323-Sitzung aus der Liste auswählen, werden detaillierte Informationen der ausgewählten Sitzung im unteren Fensterausschnitt eingeblendet, inklusive eines detaillierten Sitzungsprotokolls, summierte und statistische Daten, sowie die RTP-Ströme bezogen auf die ausgewählte Sitzung.



Falls RTP-Ströme für die gewählte Nachrichtensitzung verfügbar sind, ist es möglich einen Anruf durch klicken auf **Wiedergabe** wiederzugeben.

Siehe auch:

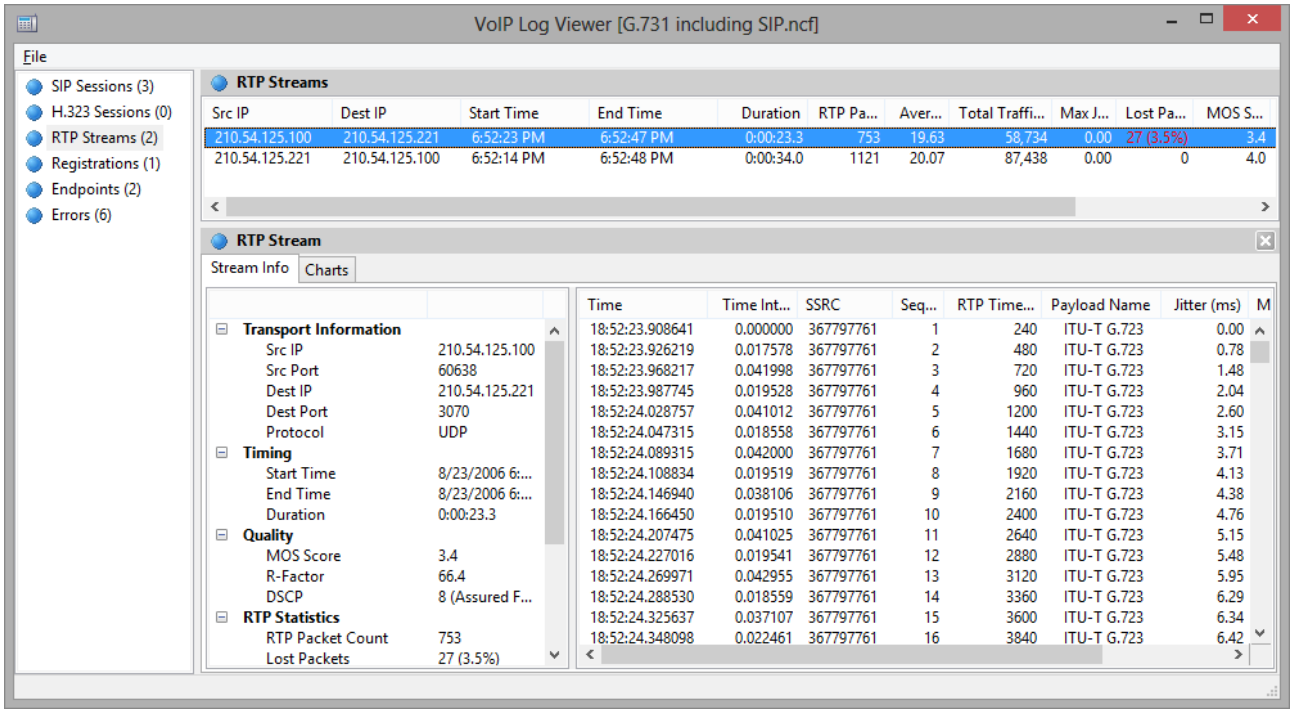
- **Arbeiten mit Auflistungen im VoIP-Analyser**
- **Anrufswiedergabe**
- **NVF-Dateien**

RTP-Ströme

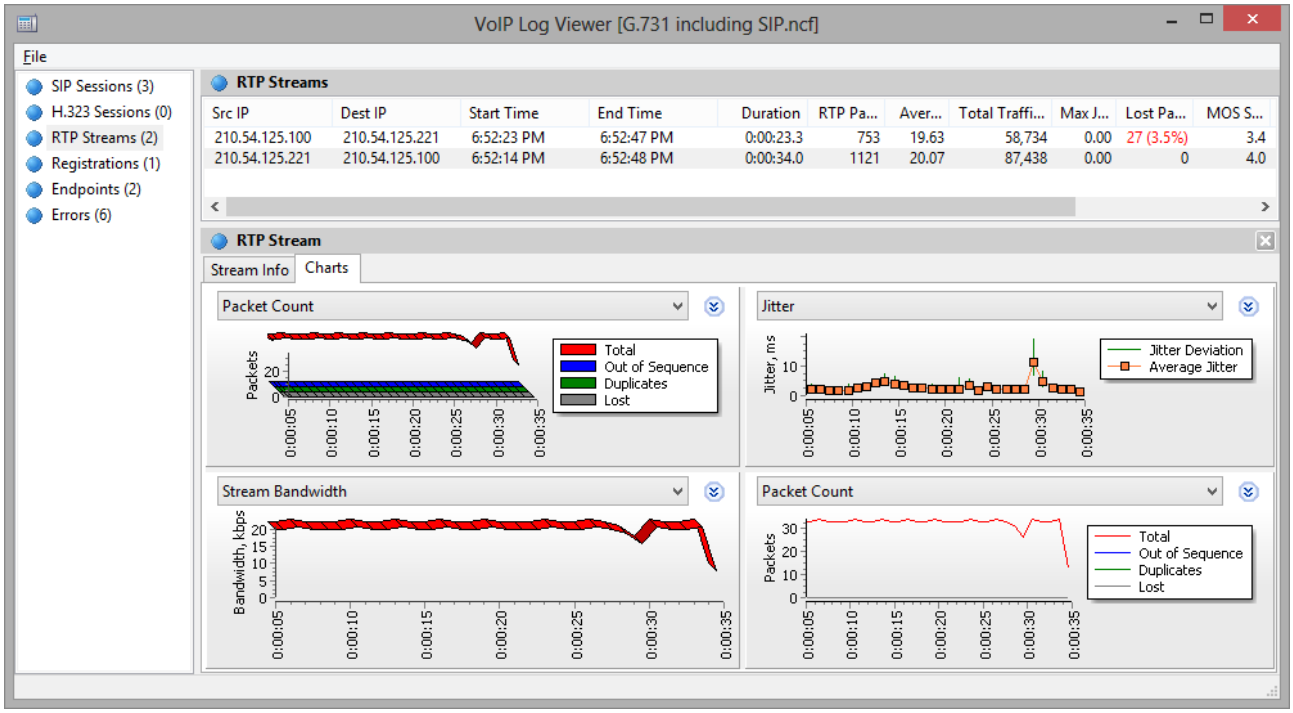
> Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Das Echtzeittransportprotokoll (RTP oder Real-time Transport Protocol) definiert ein standardisiertes Paketformat zum in Umlauf bringen von Audio und Video über das Internet. Während Protokolle wie SIP oder H.323 zur Kontrolle des Anrufs benutzt werden (z.B. zur Verbindungseinstellung, zum Wählen, zur Verbindungstrennung, usw.), wird RTP zur sicheren Übertragung von Datenpaketen und zur Erhaltung der Dienstqualität benutzt. In anderen Worten, RTP-Ströme befördern die aktuelle Sprachladung unter Benutzung eines Codecs aus einer Anzahl von Codecs und die Analyse der RTP-Daten stellt unschätzbare Informationen zur Beurteilung der Anrufsqualität und zur Fehlersuche in VoIP-Netzwerken bereit.

Zur Anzeige von durch die Applikation erfassten RTP-Strömen, wählen Sie **RTP-Ströme** im linken Fensterausschnitt des VoIP-Analyser-Fensters:



Der obere Teil zeigt eine komplette Auflistung aller RTP-Ströme. Wenn Sie einen RTP-Strom aus der Liste auswählen, werden detaillierte Informationen des ausgewählten Stroms im unteren Fensterausschnitt eingeblendet, inklusive der vollständigen RTP-Paketliste, summierte und statistische Daten, sowie die Diagramme:



Bis zu vier verschiedene Diagramme können für den ausgewählten Strom simultan, mit einem Fensterintervall von 5 bis 60 Sekunden, angezeigt werden. Beachten Sie bitte, dass durch Rechtsklicken und Ziehen das Schaubild nach links blättert oder entsprechend nach rechts. Die folgenden Diagrammtypen sind verfügbar:

- **Paketanzahl** – Anzahl der RTP-Pakete/Sekunde inklusive Duplikate, verlorener und defekter Pakete.
- **Strombandbreite** – Geschwindigkeit des Stroms in Kilobits/Sekunde.
- **Paketgröße** – Durchschnittliche Größe, der durch das Netzwerk, die RTP-Köpfe und die RTP-Ladung getrennte, RTP-Pakete.
- **Jitter** – Strom-Jitter.
- **R-Factor, MOS Score** – Stromqualitätsbeurteilung.
- **Paketintervalle** – Zeitliche Zuordnung von RTP-Paketen zu einem Strom.

Die RTP-Stromauflistung beinhaltet alle erfassten RTP-Ströme, zugehörig zu SIP- oder H.323-Nachrichtensitzungen und solche für nicht identifizierte Nachrichtensitzungen (s.g. Verwaiste Ströme, die z.B. zu keiner Hauptsitzung gehören). Für detaillierte Informationen, zum Ausschluss von RTP-Strömen, ohne zugehörige Nachrichtensitzungen, verweisen wir auf das Kapitel **Einstellungen**.

Siehe auch:

- **Arbeiten mit Auflistungen im VoIP-Analyser**
- **Anrufswiedergabe**
- **NVF-Dateien**

Registrierungen, Endpunkte, Fehler

> Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Zur Anzeige des mit dem Registrierungs-Server registrierten VoIP-Klienten wählen Sie das Element **Registrierung** im linken Fensterausschnitt des VoIP-Analyser-Fensters. Der obere Teil des rechten Ausschnittfensters zeigt eine Auflistung aller Registrierungen, inklusive des aktuellen Registrierungsstatus der VoIP-Klienten. Wenn Sie einen registrierten Datensatz auswählen, wird das Registrierungsprotokoll des VoIP-Klienten mit den gesendeten/empfangenen Mitteilungen des Registrierungs-Servers angezeigt.

Zur Anzeige aller am VoIP-Datenaustausch beteiligten Arbeitsplätze inklusiver statistischer Daten und einer Liste der Hauptanrufer wählen Sie das Element **Endpunkte** im linken Fensterausschnitt des VoIP-Analyser-Fensters. Die vollständige Liste der Arbeitsplätze wird im oberen Teil des Fensterausschnittes angezeigt. Wenn Sie einen Endpunkt auswählen, zeigt der untere Teil des Fensterausschnittes die eingeleiteten oder empfangenen Anrufe des ausgewählten Computers.

Zur Anzeige der letzten, während des Datenaustausches zwischen den VoIP-Clienten und Servern registrierten Fehler wählen Sie das Element **Fehler** im linken Fensterausschnitt des VoIP-Analyser-Fensters. Die Auflistung der letzten Fehler wird im oberen Teil des Fensterausschnittes angezeigt. Wenn Sie einen Datensatz auswählen, werden die zugehörigen Anrufinformationen im unteren Teil des Ausschnittfensters angezeigt.

Anrufprotokoll und Berichte

> Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Das **Anrufprotokoll** ermöglicht es Ihnen, automatisch alle VoIP-bezogenen Pakete als CommView for WiFi-Erfassungdatei zu speichern. Aktivieren Sie die Funktion **Automatische Speicherung** und wählen Sie die zu erfassenden Ausgabedaten, die in eine Protokolldatei gespeichert werden sollen. Im Bereich **Einzubindende Daten** können Sie die spezifischen Pakete konfigurieren, welche die Applikation protokollieren soll.

Das Ausschnittfenster **Berichte** ist für die automatische Erstellung von VoIP-Berichten vorgesehen. Ankreuzen der Checkbox **Berichte generieren** aktiviert die Berichterstellung. Im Bereich **Einzubindende Daten** können Sie die spezifischen Informationen konfigurieren, die Sie in die Berichte einbinden möchten. Sie können ebenso das Berichtsformat (CSV oder HTML) einstellen wie die Zeitintervalle, in denen die Berichte erstellt werden sollen. Neue Berichte können entweder ältere ersetzen oder angehängt werden.

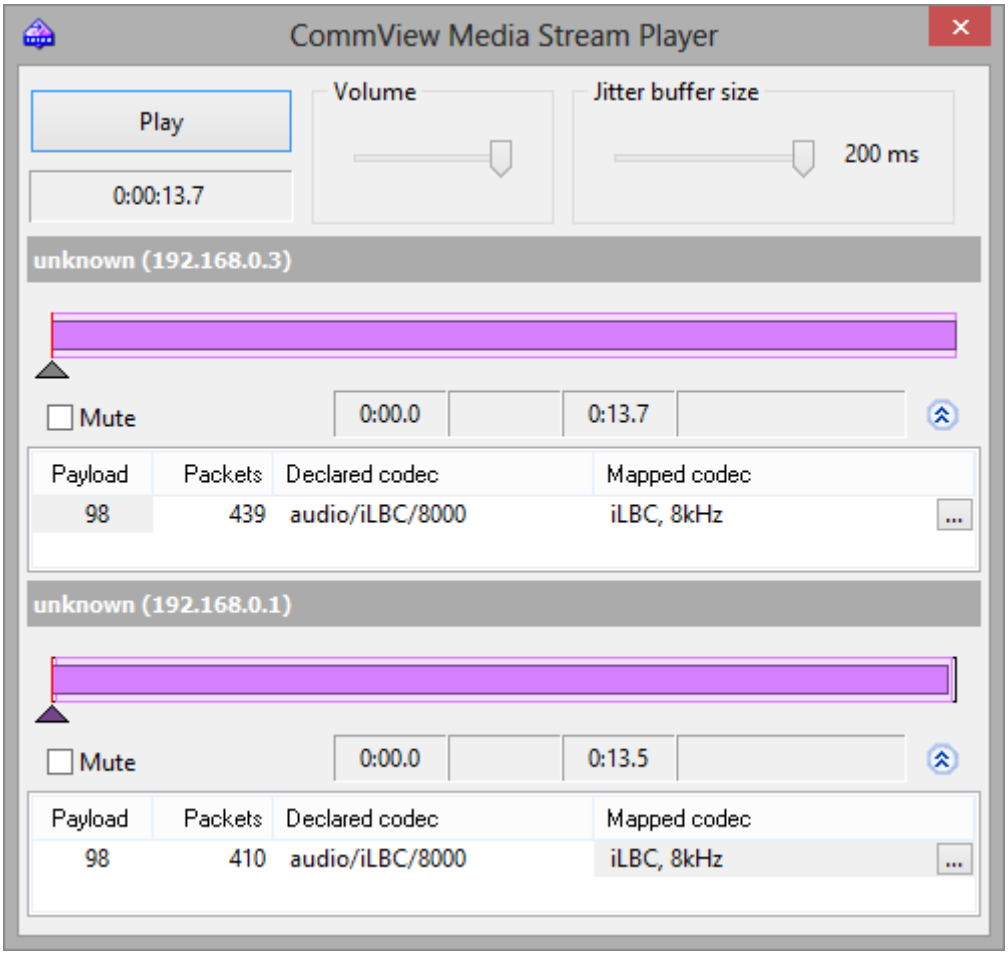
Anrufswiedergabe

> Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Die Funktionalität der Anrufswiedergabe kann erfahrungsgemäß zur Beurteilung der Audioqualität, der an einem VoIP-Anruf teilnehmenden Parteien genutzt werden. In den meisten Fällen, ermöglicht Ihnen der VoIP-Analyser erfasste Anrufe wiederzugeben (dies ist von der Unterstützung des bei dem vorgegebenen VoIP-Anruf verwendeten Codec's abhängig). Zur Wiedergabe eines Anrufs, wählen Sie die gewünschte Aufzeichnung im VoIP-Analyser-Fenster, wählen das Register **RTP-Ströme** und klicken auf den Button **Wiedergabe**. Alternativ können Sie ein beliebiges Element aus der Auflistung der RTP-Ströme (z.B. die **RTP-Stromkategorie**) im rechten Fensterausschnitt auswählen, wählen Sie ein oder mehrere Ströme, führen Sie einen Rechtsklick darauf aus und wählen Sie den Menüpunkt **Auswahl wiedergeben**. Auf diesem Weg ist es möglich Ströme mit fehlenden oder nichtunterstützten Signalsitzungen (z.B. das Protokoll ist kein SIP oder H.323) zu verbinden und wiederzugeben.

Simultane Wiedergabe von RTP-Strömen, die zu unterschiedlichen Anrufen gehören und die zu verschiedenen Zeiten ausgeführt wurden, ist nicht durchführbar. Das Hauptproblem ist die erhebliche Zeitdifferenz zwischen den Strömen, die zu unterschiedlichen VoIP-Anrufen gehören, abgesehen davon, macht es keinen Sinn, sich Audiosignale anzuhören, welche ein Teil von bezugslosen Anrufen sind. Die Funktionalität, zur Auswahl freiwählbarer RTP-Ströme für eine nachfolgende Wiedergabe, ist einzig und allein für die manuelle Wiederherstellung eines Anrufs aus mehreren Strömen vorgesehen, für den Fall, dass keine SIP- oder H.323-Stammsitzungen verfügbar sind.

Nach Betätigung des Buttons **Wiedergabe** wird das Medienstrom-Player-Fenster geöffnet:



Zur Anzeige weiterer detaillierter Informationen über die Audioströme und zum Aufruf der manuellen Codec-Zuordnung, klicken Sie auf den Button mit dem Doppelpfeil. Für jeden RTP-Strom können Sie:

- Manuell einen Strom über die Zeit sychronisieren, z.B. einstellen der Startzeit für die Wiedergabe in Bezug zu anderen Strömen. Zur Durchführung, bewegen Sie das kleine Dreieck nach links oder rechts.
- Wählen Sie den korrekten Sound-Codec für jeden Ladungstyp der RTP-Ströme. In den meisten Fällen, wählt der Medienstrom-Player den richtigen Codec automatisch. Allerdings, wenn Sie mit verwaisten RTP-Strömen arbeiten denen die SIP- oder H.323-Stammsitzungen fehlen, dann werden Informationen über den richtigen Codec benötigt, den Sie dann manuell aus der Ausklappliste auswählen müssen. Wenn Sie es schwierig finden, den richtigen Codec auszuwählen, klicken Sie auf den Button **Versuchen zu erraten** und der Medienstrom-Player wird selbst versuchen den Codec auszuwählen.

Beachten Sie bitte, dass es manchmal nicht möglich ist, den Ton von RTP-Strömen wiederzugeben, weil diese Ströme verschlüsselt sind, geschützte Codecs benutzen oder die Codecs von CommView for WiFi nicht unterstützt werden.

Der Lautstärkeregler ermöglicht Ihnen dieEinstellung der Lautstärke. Der Regler **Jitter-Puffergröße** erlaubt Ihnen einen Jitter-Puffer in VoIP-Endknoten zu simulieren, wie er in der realen Welt genutzt wird. Eine typische Jitter-Puffergröße ist 30 ms bis 50 ms. Eine Anhebung des Jitter-Puffers verbessert die Sprachqualität, erhöht aber auch die Wartezeit.

VoIP-Protokollbetrachter

> Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Der VoIP-Protokollbetrachter ist ein Werkzeug zur Anzeige und Auswertung durch CommView for WiFi und einigen Netzwerkanalysern von Drittherstellern erzeugter und erfasster Dateien. Er hat eine ähnliche Funktionalität wie der VoIP-Anylser, der Bestandteil des Programmhauptfensters ist; seine Zweckbestimmung ist die Analyse nach der Erfassung, z.B. lieber arbeiten mit Dateien als Pakete in Echtzeit erfassen. Für detaillierte Informationen, wie Sie mit diesem Werkzeug arbeiten, verweisen wir auf das Kapitel **Arbeiten mit dem VoIP-Analysator**.

Klicken Sie auf **Datei => VoIP-Protokollbetrachter** um den VoIP-Protokollbetrachter zu öffnen. Sie können so viele VoIP-Protokollbetrachterfenster öffnen wie Sie möchten und jedes Fenster kann für die Analyse einer oder mehrerer erfasster Dateien benutzt werden.

Der VoIP-Protokollbetrachter kann durch CommView for WiFi erfasste Dateien im NCF-Format laden, sowie andere durch Netzwerk-Analyser von Drittherstellern erzeugte Formate. Zusätzlich ist es möglich, **CommView-VoIP-Dateien (NFV)** in den VoIP-Protokollbetrachter zu laden.

VoIP-Protokollbetrachtermenü

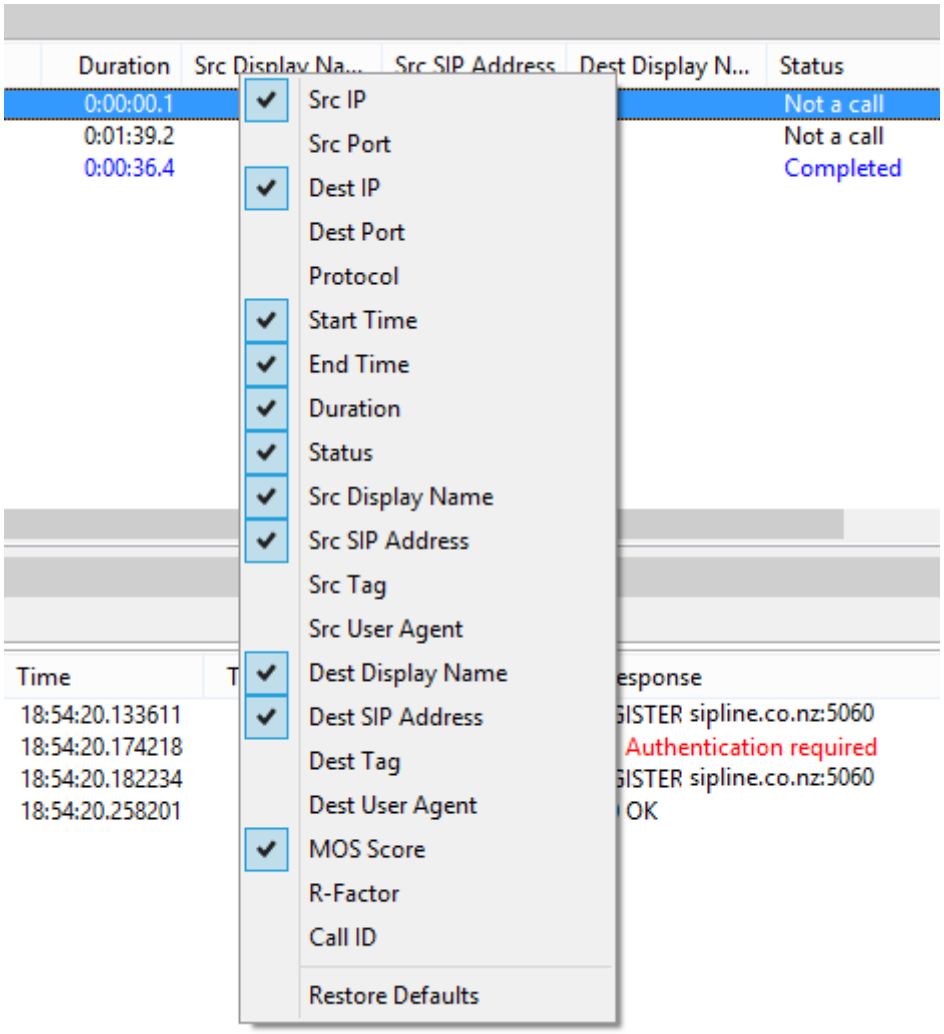
- **CommView-Protokolle laden** – Öffnet eine oder mehrere CommView-Erfassungsdateien.
- **Protokolle importieren** – Ermöglicht Ihnen von anderen Paketnanalysern erzeugte Erfassungsdateien zu importieren.
- **Bericht erzeugen** – Generiert einen Übersichtsbericht der in den VoIP-Protokollbetrachter geladenen Daten und speichert diesen auf Ihre Festplatte. Wenn Sie einen Bericht generieren, werden die Einstellungen des **Berichtsbedienfeldes** im Hauptfenster des VoIP-Analysator benutzt.
- **VoIP-Daten leeren** – Leert das aktuelle Fenster.
- **Fenster schliessen** – Schließt das Fenster.

Auflistungen im VoIP-Analysator

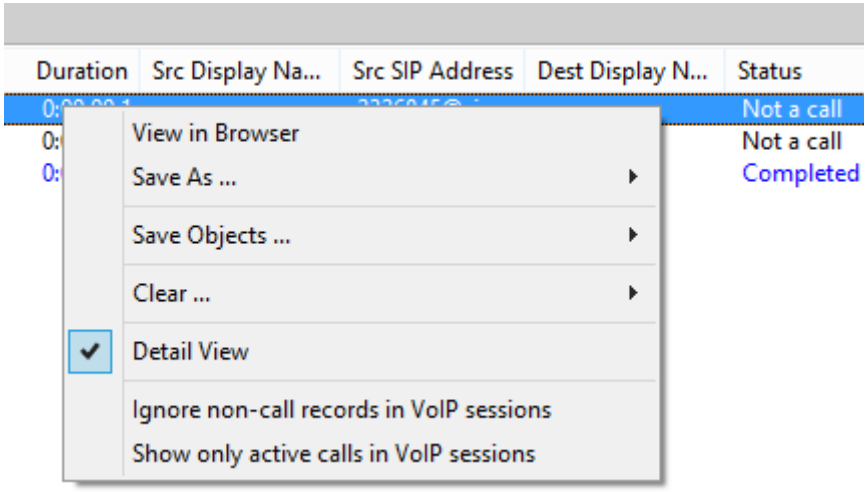
> Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Weil die im VoIP-Analysator gezeigten Informationsauflistungen Daten verschiedener Arten beinhalten, wird der gemeinsame Stil und das gemeinsame Datenpresentationsprinzip dieser Listen unten erklärt.

Standardmäßig beinhaltet die Auflistung nur die meistgenutzten Datenfelder, während alle anderen Felder ausgeblendet werden. Zur Auswahl der Felder, die Sie angezeigt bekommen möchten, rechtsklicken Sie auf den Listenkopf und aktivieren/deaktivieren die zugehörigen Optionen. Es ist ebenso möglich, die Spaltenweite und die Reihenfolge der darzustellenden Datenfelder durch Ziehen mit der Maus einzustellen.



Rechtsklicken auf eine Liste öffnet ein Kontextmenü mit den folgenden Elementen:



- **Ansicht im Browser** – Öffnet die aktuelle Ansicht als HTML-Datei im Web-Browser.
- **Speichern als…** – Exportiert alle oder ausgewählte Aufzeichnungen in eine Textdatei.
- **Objekt speichern…** – Speichert alle oder ausgewählte Objekte in eine NVF-Datei. Für detaillierte Informationen über das NVF-Format, verweisen wir auf das Kapitel **NVF-Dateien**.
- **Leeren…** – Entfernt alle oder ausgewählte Objekte/Listen. Das Löschen von Stammobjekten führt auch zur Löschung der untergeordneten Objekte; z.B. bei der Löschung eines SIP-Anrufs, wird der zugehörige RTP-Strom des Anrufs ebenfalls von der **RTP-Stromauflistung** gelöscht.
- **Detailansicht** – Wenn Sie mit einer Masterliste arbeiten, d.h. wenn mehr zugehörende Details des ausgewählten Objekts vorhanden sind, wird das Ein/Ausschalten dieser Option, das Programm veranlassen, die zugehörigen Details des Objekts Ein- bzw. Auszublenden. Z.B. die Auswahl **Detailansicht** in der **SIP-Sitzungsauflistung**, veranlasst das Programm detaillierte Informationen der ausgewählten SIP-Sitzung, wie die Anrufinformationsübersicht und zugehörige RTP-Ströme, ein- bzw. auszublenden.
- **Nicht-Anrufe in VoIP-Sitzungen ignorieren** – Verbirgt alle Eintragungen, die keine aktuellen Anrufe sind.
- **Nur ablauffähige Anrufe in VoIP-Sitzungen anzeigen** – Verbirgt alle Eintragungen ein, die nicht mehr aktiv sind.

NVF-Dateien

Das VoIP-Analysemodul ist nur für VoIP-Lizenz- oder Testversionsbenutzer verfügbar, die den VoIP-Testmodus gewählt haben.

Der VoIP-Analyser ermöglicht Ihnen ein oder mehrere VoIP-Datenobjekte in eine Containerdatei im NVF-Format zu speichern. Anders als gemeinsam erfasste Dateien, beinhaltet NVF keine erfassten Datenpakete. Stattdessen ist dies ein, in einer Einzeldatei gespeicherter Satz von VoIP-Objekten. NVF-Datein sind hilfreich, wenn Sie einen VoIP-Anruf für eine spätere Analyse speichern möchten.

VoIP-Objekte, die in eine NVF-Datei gespeichert werden können, sind:

- SIP-Sitzungen
- H.323-Sitzungen
- RTP-Ströme

Um ein Objekt in eine NVF-Datei zu speichern, wählen Sie bitte ein oder mehrere Objekte in der VoIP-Analyserliste aus, führen einen Rechtsklick zur Öffnung des Kontextmenüs aus und wählen das Menüelement **Objekte speichern als…**

SIP- oder H.323-Sitzungen und zugehörige RTP-Ströme (wenn überhaupt) werden in eine Datei gespeichert. Wenn Sie jedoch nur den RTP-Strom zur Speicherung auswählen, wird die zugehörige SIP- oder H.323-Stammsitzung nicht mitgespeichert.

Sie können die gespeicherte NVF-Datei in das **VoIP-Protokollbetrachterfenster** laden.

Weiterführende Themen

802.11n/ac/ax/be-Netzwerke überwachen

Trotz der Ähnlichkeiten zwischen den 802.11 a/b/g- und 802.11n/ac/ax/be-Technologien gibt es einige Besonderheiten in 802.11n/ac/ax/be-Netzwerken, die die Art und Weise beeinflussen, wie solche Netzwerke effektiv überwacht werden können. Ohne auf die spezifischen technischen Details dieses Standards einzugehen (diese sind in vielen öffentlichen Quellen im Internet publiziert), zeigt dieses Kapitel die besten Überwachungspraktiken und Hardwarevoraussetzungen für 802.11n-, 802.11ac-, 802.11ax- und 802.11be-Netzwerke.

Kompatibilität der Adapter

Die Erfassung von Paketen des spezifieschen Standards erfordert einen Adapter, der auf desselben oder den aktuellsten Standard sich basiert. Zum Beispiel, die Erfassung der 802.11ac-Pakete erfordert einen 802.11ac- oder 802.11ax-Adapter. Sie können die 802.11ac-Pakete nicht mit einem 802.11n-Adapter erfassen. Die Liste der kompatiblen Adapter kann auf der Download-Seite von CommView for WiFi auf unserer Webseite heruntergeladen werden. Je nach der Konfiguration des zu analysierenden 802.11n/ac/ax/be-Netzwerks bestehen zusätzliche Anforderungen an Ihren Adapter. Diese werden unten beschrieben.

MIMO und Transmit Beamforming

Die Benutzung von MIMO- und Transmit Beamforming-Technologie in 802.11n/ac/ax/be-Netzwerken ist eine ernsthafte Herausforderung für drahtlose Analyser. Solche Netzwerke erstellen ein sehr komplexes, lernfähiges Signalstärkenabbild, mit Abfällen und Erhebungen, manche so klein wie einige Zentimeter des Bandes. Weil ein Überwachungsgerät passiv ist, versucht das überwachte WLAN nicht sich dem Gerät anzupassen. Signale bewegen sich auf hohen Frequenzen und übertragen durch mehrere Antennen sind sie ebenso schwierig ohne CRC-Fehler aufzufangen. Dies alles meint, Sie sollten allgemein bei der Überwachung von 802.11n/ac/ax/be-Netzwerken gegenüber älteren 802.11 a/b/g-Netzwerken, einen deutlich höheren Anteil von beschädigten Frames erwarten. Da dies kein Problem darstellt, wenn Sie eine Standortaufnahme oder Signalstärkenmessung bestimmter Geräte ausführen, individuelle TCP-Streams oder Fehlermeldungen auf der Pro-Paket-Ebene untersuchen, kann es problematisch werden, wenn zuviele Frames beschädigt sind.

Zur Verminderung dieser 802.11n/ac/ax/be-spezifischen Faktoren, berücksichtigen Sie die Übernahme der folgenden Techniken:

- Finden Sie die beste Position für das Notebook mit dem laufenden CommView for WiFi. Drehen oder bewegen in verschiedene Richtungen kann eine enorme Zu- oder Abnahme der Signalstärke bewirken. Tatsächlich kann die Position Ihres Körpers oder ein gehobener Arm, Auswirkungen auf den Anteil von CRC-Fehlern nehmen.
- Versuchen Sie sicherzustellen, dass die WLAN-Geräte nicht mit ihren Maximal-Raten laufen. Erfolgreiche Paketerfassung mit Raten von 100 Mb/s und darunter ist weit mehr als erfolgreiche Paketerfassung mit höheren Datenraten. Dabei hört sich dies unmittelbar engegengesetzt an, wenn Ihr Notebookstandort in der Nähe eines AP befindet, führt Bewegung des Clients um einige Meter weiter vom AP weg, eher zur Erhöhung der Empfangsqualität, als zu deren Absenkung; ein nur 1- oder 2 m von einem AP entfernt stehender 802.11ax-Client wird zwangsläufig Pakete mit Raten von 720 oder 866 Mb/s annähernd übertragen, wobei mit demselben Gerät 5m weiter vom AP entfernt die Rate auf circa 200 Mb/s abfällt, was für unsere Zwecke vorteilhaft ist.

Es ist wichtig anzumerken, dass das Leistungsvermögen Ihres Überwachungsadapters in Hinblick auf die Zahl der unterstützten spatialen Ströme die Kapazitäten des zu überwachenden Netzwerks überschreiten oder ihnen entsprechen muss. Mit anderen Worten: Sie können vom Klient mit einem drei-Strom-AP gesendete Pakete nicht mit einem Adapter empfangen, der nur ein oder zwei spatiale Ströme benutzt (aber Sie können z. B. vom 2-Strom-Klient an einen 2-Strom-AP gesendete Pakete mit einem 3-Strom-Adapter empfangen). Man kann die Zahl der unterstützten spatialen Ströme leicht den Spezifikationen des Adapters entnehmen. Bei 802.11ac-Netzwerken, bedeutet eine maximale unterstützte Rate von 433 Mb/s einen 1-Strom-Adapter, 876 Mb/s einen 2-Strom-Adapter und 1,300 Mb/s einen 3-Strom-Adapter.

Kanalbündelung im 2,4-GHz-Band

In modernen Netzwerken wird die Datenrate wahlweise durch Bindung von zwei 20 MHz-Kanälen (40 MHz-Betrieb) erhöht. Der 40 MHz-Betrieb benutzt Breitbänder, verglichen zu 20 MHz-Bändern in 802.11 a/b/g, zur Unterstützung höherer Datenraten. Da ein mit einer 802.11n/ac/ax-Karte ausgerüsteter Wi-Fi-Analyser kein Problem mit der simultanen Erfassung von 2 Kanälen hat, ist es wichtig auf die Regulierungsdömäne der benutzten Hardware zu achten. Kurz dargestellt, die Frequenz des Sekundärkanals im 40 MHz-Modus ist abhängig von der Frequenz des Primärkanals. Zum Beispiel, Auswahl des Kanals 1 Ihrer Hardware bedeutet, dass der primäre 20 MHz-Kanal auf der Frequenz des Kanal 1 arbeitet, während der sekundäre 20 MHz-Kanal 4 Kanäle über dem Primärkanal arbeitet, z.B. auf der Frequenz des Kanal 5. Wenn in höher Kanalnummern gearbeitet wird, z.B. 10 oder 11, addieren Sie 4 zu der Kanalnummer bedeutet dass die Frequenz des sekundären Kanals ausserhalb der Grenzen der Regulationsdomäne liegt: in den USA, ist in 2,4 GHz-Bändern der oberste Kanal 11; in den meisten europäischen Ländern ist der oberste Kanal 13. In solchen Fällen benutzt der sekundäre Kanal die unterhalb des Primärkanals liegende Frequenz. Zum Beispiel: Auswahl des Kanals 10 in Ihrer Hardware bedeutet, dass der primäre 20 MHz-Kanal

auf der Frequenz des Kanal 10 arbeitet, weil der sekundäre 20 MHz-Kanal 4 Kanäle unterhalb des Sekundärkanals arbeitet, z.B. auf der Frequenz des Kanal 6.

Das potenzielle Problem auf das ein Aussendienstmitarbeiters treffen kann, wenn er international arbeitet, ist dass die Regulationsdomäne seines überwachenden Netzwerkadapters zu der Regulationsdomäne des zu überwachenden Wi-Fi-Netzwerkes differiert. Zum Beispiel, ein deutschbasiertes 802.11n-WLAN auf Kanal 9 arbeitend, würde die Kanäle 9 und 13 binden. Ein in Kanada gekaufter Überwachungsadapter würde den Sekundärkanal 5 erwarten. Dies wird den Adapter abhalten, die 40 MHZ-Ströme des drahtlosen Analysers zu "sehen". Zur Handhabung einer solchen Situation, berücksichtigen Sie, Hardware zu benutzen, die zur entsprechenden Regulationsdomäne gehört, oder nutzen Sie die Einstellung der Checkbox **Sekundärkanal ist unterhalb des Primärkanals im 40 MHz-Modus** im Ausschnitt **Erfassung** im Hauptfenster von CommView for WiFi. Die Aktivierung dieser Checkbox zwingt der Adapter eine Sekundärkanalfrequenz unterhalb der Primärkanalfrequenz zu benutzen, selbst wenn die Regulationsdomäne des Netzwerkadapters dies nicht erfordert.

Beachten Sie bitte, dass einige der von CommView for WiFi unterstützten Adapter wie auf Broadcom-Chipsets basierende Adapter, keine Kanalbindung unterstützen. Sie können die Pakete nur auf 20-MHz-Kanälen empfangen. Mehr dazu unter **Technische Informationen**. Wir empfehlen, einen der Adapter zu wählen, die auf unserer **Download-Seite** als "**Empfohlen**" markiert sind; solche Adapter unterstützen die Kanalbindung.

Kanalbündelung in Bändern 5 GHz und 6 GHz

Die Kanalbündeung in Bändern 5 GHz und 6 GHz ist der Kanalbündeung im 2,4 GHz-Band ähnlich, aber die Anzahl der verbundenen Kanäle kann in den 802.11ac/ax-Netzwerken bis zu acht sein und in den 802.11be-Netzwerken kann es sechzehn sein. Das heißt, dass die Kanalbreite 320 MHz erreichen kann. Anders als 2,4 GHz-Band, beim Standard, werden die Sätze der im 5 GHz- und 6-GHz-Band verbundenen Kanäle eindeutig definiert. Zum Beispiel, bei 40 MHz-Kanälen, wird Kanal 52 immer mit Kanal 56 verbunden; Der Kanal kann mit Kanal 48 verbunden werden. Aus diesem Grund, hat die Checkbox **Sekundärkanal ist unterhalb im 40 MHz-Modus** keine Wirkung, wenn Sie die Kanäle im 5 GHz-Band mit einem empfohlenen Adapter erfassen, weil der Adapter automatisch den richtigen Satz der Kanäle auswählt. Zum Beispiel, wenn Sie Kanal 36 wählen, arbeitet der Adapter im 80 MHz-Breitkanal (von 36 bis 48). Jedoch sind in diesem Beispiel die im 20-MHz-Breitkanal gesendeten Pakete sichtbar nur, wenn sie über den Kanal 36 gesendet werden. Mit anderen Worten, wenn Sie einen 802.11ac/ax-AP überwachen, der Kanäle 36-48 benutzt, und sein Primärkanal Kanal 36 ist, werden Sie die AP-Beacons und 80 MHz-Pakete sehen, wenn Sie die Daten im Kanal 36 erfassen; Sie werden nur die 80 MHz-Pakete (und keine Beacons) sehen, wenn Sie die Pakete in den Kanälen 40, 44 oder 48 erfassen.

BCC- und LDPC-Kodierung

Auf der Hardware-Ebene sind 802.11n/ac/ax-be-Pakete entweder mit Binary Convolutional Code (BCC)-Kodierung oder mit Low Density Parity Check (LDPC)-Kodierung verschlüsselt. BCC ist das Standardverfahren der Kodierung, das in den meisten neuen Geräten benutzt wird. LDPC ist ein optionales Kodierungsverfahren, das von einigen 802.11n-Geräten unterstützt wird. Wenn ein Klient sich mit dem AP verbindet, bestimmt das Element HT Capabilities Info in den Association-Request- und Association-Response-Paketen, welche von Kodierungsmethoden benuzt wird. Wenn z. B. das BCC-Standardverfahren benutzt wird, enthält HT Capabilities Info das Feld "**HT LDPC coding capability: Transmitter does not support receiving LDPC coded packets**". Wenn das WLAN-Netzwerk LDPC-Kodierung benutzt, muss Ihr Adapter auch die LDPC-Kodierung unterstützen; sonst werden die mit HT-Raten in einer oder beiden Richtungen gesendeten Pakete beschädigt oder gehen verloren. Momentan werden mit LDPC verschlüsselte Pakete nur von Atheros-basierenden mPCIe-Adaptern wie AR93xx, AR94xx und AR95xx unterstützt. Erfassung der LDPC-kodierten Pakete wird von allen empfohlenen 802.11ac/ax/be-Adaptern unterstützt.

Hintergründe von CRC- und ICV-Fehlern

CRC-Fehler

Jeder WLAN-Frame besteht aus den folgenden Basiskomponenten:

- Einem MAC-Header, der Informationen zur Framekontrolle, Dauer, Adresse und Sequenzsteuerung enthält.
- Einen unterschiedlich langen Framekörper, der Information über den Frametyp enthält.
- Eine Frame-Checksequenz (FCS), die einen zyklischen 4-Byte-Wiederholungscode (CRC) enthält.

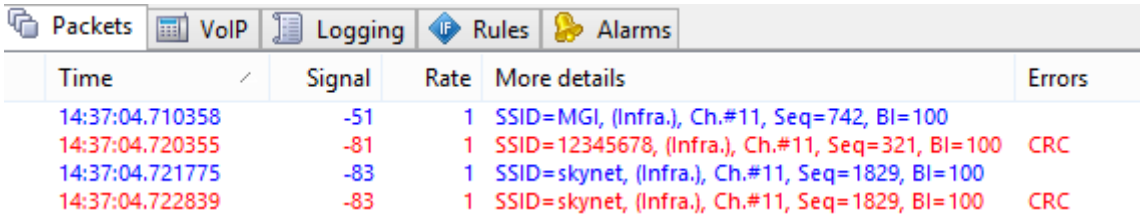
Die letzte Komponente (FCS) wird für den Integritätstest des Paketes auf der Empfängerseite benötigt. Der empfangende Teil berechnet den CRC-Wert aus dem erhaltenen Frame und vergleicht den berechneten Wert mit den aktuellen 4 Byte am Ende des Paketes. Wenn diese Werte differieren wird das Paket als beschädigt angesehen.

Wie CommView for WiFi mit solchen beschädigten Frames umgeht hängt von den durch den Anwender durchgeführten Einstellungen ab. Standardmässig werden solche Frames ignoriert, außer:

- Wenn sie die Gesamtzahl der Pakete und den Bytecounter erhöhen.
- Wenn sie den CRC Fehlerzähler im Register **Kanäle** erhöhen.
- Wenn sie im Register **Statistik** in der Paketgrößentabelle enthalten sind.

Aus folgendem Grund werden beschädigte Frames in anderen Listen und Tabellen nicht gezählt. Kein Frameteil mit einer falschen CRC-Summe ist vertrauenswürdig. Der Frame kann eine völlig falsche IP-Adresse, falschen Dateninhalt etc. beinhalten, wobei in der Realität solche Frames doch den Originalen ähneln. Aus diesem Grund können CRC-Fehler auch nicht einem WLAN-Accesspoint bzw. einer Station zugeordnet werden, da man auch nicht die MAC-Adresse des echten Absenders bestimmen kann.

Dennoch kann der Benutzer die Checkbox **Beschädigte Frames erfassen** in den Optionen aktivieren; in diesem Fall werden die beschädigten Frames auch in der Paketliste angezeigt. Standardmässig werden solche Frames rot markiert und haben den CRC-Marker in der Spalte **Fehler** im Register **Pakete** angezeigt:



Es ist wichtig zu verstehen, dass ein von CommView for WiFi empfangenes Frame mit CRC-Fehler am Zielknoten ohne Fehler ankam.

Nicht alle WLAN-Adapter können beschädigte Frames an den Applicationlevel weitergeben. Dies ist nur für die empfohlenen Adapter sichergestellt, die von CommView for WiFi unterstützt werden.

ICV-Fehler

Der sogenannte "Integrity Check Value" (ICV) ist eine 4-Byte-Checksumme, die von WEP- und WPA-verschlüsselten Frames zur Überprüfung des Vershlüsselungsergebnisses verwendet wird. Die Empfängerseite berechnet den ICV-Wert aus dem Datenteil des erhaltenen Frames und vergleicht diesen berechneten Wert mit den aktuellen 4 Bytes am Ende des Paketdatenteils. Wenn diese Werte differieren wird die Entschlüsselung als fehlerhaft definiert.

CommView for WiFi kann, sofern die richtigen **WEP-/WPA-Schlüssel** eingegeben worden sind, on-the-fly WEP-und WPA-Entschlüsselung durchführen. Das Programm zeigt die ICV-bezogenen Informationen in drei Orten an: In den Registern Knoten und Kanäle sowie in der Spalte Fehler im Register Pakete. Wie ICV-Fehler angezeigt und vom Programm gezählt werden hängt davon ab, ob ein Schlüssel eingegeben wurde und inwieweit d Schlüssel korrekt ist. Es gibt dabei drei Möglichkeiten:

1. Ein Schlüssel wurde eingegeben und er ist der Richtige für das WLAN.
2. Ein Schlüssel wurde eingegeben, ist aber falsch.
3. Es wurde kein Schlüssel eingegeben.

Im ersten Fall sollten nur wenige ICV-Fehler vom Programm gemeldet werden. Im zweiten Fall bekommen die gesammelten Datenframes ein ICV-Error-Flag, da die berechneten und gemessenen ICV-Werte nicht übereinstimmen, da ein falscher Schlüssel verwendet wurde. Im dritten Fall haben die Frames keine ICV-Fehler, da keine Entschlüsselungsversuche durchgeführt wurden.

Wie weiter oben erklärt wurde, sind ICV-Fehler im Gegensatz zu den "harten" CRC-Fehlern eher sogenannte Softfehler, die vom Entschlüsselungsschlüssel abhängig sind. Ihr WLAN kann vollfunktionsfähig sein, wenn Sie aber den falschen WEP-Schlüssel in CommView for WiFi eingegeben haben, werden Sie viele ICV-Fehler beobachten. Aufgrund dieser "Softness" werden die Pakete standardmässig in derselben Farbe, wie die anderen Pakete angezeigt. Mittels des Dialoges **Einstellungen** können Sie dies verändern.

Wenn ein Frame einen CRC-Fehler hat, macht das Erkennen von ICV-Fehlern keinen Sinn. Daher zeigt CommView for WiFi niemals ICV-Fehler für Frames mit CRC-Fehlern an.

Hintergründe der WPA-Entschlüsselung

Wie bereits erwähnt kann CommView for WiFi on-the-fly WEP-und WPA/WPA2-verschlüsselten Verkehr entschlüsseln. Um dies richtig nutzen zu können, sollten Sie die kryptographischen Grundlagen verstanden haben.

WEP (Wired Equivalent Privacy) ist ein Mechanismus zur Erzeugung von Datensicherheit in WLAN-Netzwerken. WEP ermöglicht dem Administrator einen Schlüsselsatz, oder auch nur einen Schlüssel, für das WLAN zu erzeugen. Diese Schlüssel werden für die Entschlüsselung der Daten vor der Übersendung benötigt und werden von den Clients und Accesspoints geteilt. Wenn ein Client keinen korrekten WEP-Schlüssel besitzt, kann er die empfangenen bzw. zu anderen Clients gesendeten Daten nicht entschlüsseln, was unautorisierten Netzwerkzugriff und Abhören verhindern soll. WEP-Entschlüsselung ist recht einfach, solange man den richtigen Schlüssel hat. WEP ist ein statisches Verschlüsselungssystem, welches – sofern der richtige Schlüssel im Dialog **WEP-/WPA-Schlüssel** eingegeben wurde – CommView for WiFi ermöglicht sofort mit dem Entschlüsseln der Pakete zu beginnen.

WPA (Wi-Fi Protected Access) ist der Nachfolger des weniger sicheren WEP-Standards. WPA-Adressen – mit vielen Sicherheitsaspekten – erhöhen signifikant den Datenschutz und die Zugriffskontrolle für WLAN's. Im Gegensatz zu WEP ist WPA ein dynamisches Verschlüsselungssystem, das u.a. sogenanntes Rekeying, stationseindeutige Schlüssel und einige andere Methoden zur Sicherheitserhöhung benutzt. WPA bietet zwei Modi an: PSK (Pre-Shared Key) und Enterprise, welche sich in vielen Punkten unterscheiden. CommView for WiFi unterstützt auch die WPA- und WPA2-Entschlüsselung im PSK-Modus.

Durch die dynamische Natur der WPA-Verschlüsselung hilft allein das Wissen um die WPA-Passphrase auch nicht dabei, den Verkehr sofort nach Eingabe dieser Passphrase entschlüsseln zu können. Um WPA-verschlüsselten Verkehr entschlüsseln zu können muss CommView for WiFi

laufen und während der Schlüsselaustauschphase schon Daten sammeln. Der Schlüsselaustausch läuft über das EAPOL-Protokoll. Dabei ist es wichtig, dass alle EAPOL-Schlüsselaustauschpakete erfolgreich empfangen wurden. Ein beschädigtes oder verlorenes EAPOL-Paket macht es CommView for WiFi unmöglich empfangene oder gesendete Pakete einer bestimmten Station zu entschlüsseln, so dass es warten muss bis es die nächste EAPOL-Kommunikation zwischen dem AP und der Station empfangen kann. Dies ist ein großer Unterschied in der Entschlüsselungsart von WEP- im Gegensatz zu WPA-Verkehr.

Das bedeutet, dass nach Eingabe der WPA-Passphrase und dem Schließen des Dialogs **WEP-/WPA-Schlüssel** mit dem dazu gehörenden Empfangsbeginn der Pakete Sie dennoch auf die nächste Authentifikation und den nächsten Schlüsselaustausch warten müssen, bevor Pakete der erkannten Station entschlüsselt werden können. Deshalb ist es nicht ungewöhnlich, wenn das Programm Pakete in Richtung zu oder von einem Client entschlüsseln kann, nicht aber von oder zu einem anderen, da es bis dahin noch nicht alle EAPOL-Pakete des Clients empfangen hat.

Eine Neu-Authentifikation kann über das **Knotenzuordnung wiederherstellen**-Werkzeug ausgelöst werden, indem man den AP neustartet (für alle authentifizierten Stationen) oder indem man sich für den jeweiligen Client, an das Netzwerk neu anmeldet.

> WICHTIG. Bitte beachten Sie, dass **der mit WPA3 verschlüsselte Paketverkehr nicht entschlüsselt werden kann**. WPA3 verwendet die Passphrase nur zur Authentifizierung. Entschlüsselung ist unmöglich.

Signalstärke

Die drahtlose Signalstärke wird tradionell entweder in Prozent oder in dBM gemessen (dem Leistungsverhältniswert in Dezibel, der gemessenen Leistung bezogen auf 1 Milliwatt). Standardmäßig zeigt CommView for WiFi die Signalstärke in dBm an. Der Pegel von 100% entspricht einem Signalpegel von –35 dBm, z.B. beide, -25 dBm und –15 dBm, werden als 100% angezeigt, weil dieser Signalpegel sehr hoch sind. Der Signalpegel von 1% entspricht einer Signalstärke von –95 dBm. Zwischen –95 dBm und –35 dBm ist die Prozentskala linear, z.B. 50% entspricht –65 dBm.

Wenn Sie Messungen in Prozentrang-Werten bevorzugen, können Sie mit der Option **Signalstärke in dBm anzeigen** in **Einstellungen => Optionen => Decodierung** auf Prozentrang umschalten. Wenn die Option **Signalstärke in dBm anzeigen** eingeschaltet ist, wird die Signalhöhe in den Registern **Knoten**, **Kanäle** und **Pakete** angezeigt. Im Paketdekoderbaum wird die Signalhöhe immer in Prozentrang und dBm angezeigt.

A-MPDU- und A-MSDU-Pakete erfassen

Die 802.11n-, 802.11ac-, und 802.11ax-Standards ermöglichen das Senden mehrfacher Frames pro Einzelzugang zum Medium durch Zusammenführung der Frames in einen größeren Frame. Es existieren zwei Formen der Framezusammenführung: Aggregated Mac Protocol Data Unit (A-MPDU) und Aggregated Mac Service Data Unit (A-MSDU). CommView for WiFi kann beide zusammengeführte Pakettypen erfassen, wie unten beschrieben.

Empfangene A-MPDU-Frames werden auf Hardwareebene in Einzelpakete gesplittet. A-MPDU's können eine Größe von 64 Kbytes erreichen. Wenn ein A-MPDU erfasst wurde, wird es als eine Anzahl nicht zusammengeführter Pakete, die wie jedes andere Paket aussehen, durch die Hardwareebene genehmigt. Diese Pakete werden durch CommView for WiFi in keiner speziellen Weise markiert. Die Unterstützung für A-MPDUs ist verbindlich in modernen WiFi-Standards festgelegt und ist weit verbreitet. A-MPDU wird weitgehend in 802.11n- und 802.11ac-Geräten benutzt. A-MPDU's können mit jedem von CommView for WiFi unterstützten Adapter erfasst werden.

Empfangene A-MSDU-Frames werden auf Softwareebene in Einzelpakete gesplittet. A-MSDU's können eine Größe von 7,935 Bytes erreichen. Wenn ein A-MSDU erfasst wurde, wird es als ein einzelnes, zusammengeführtes Paket, durch die Hardwareebene genehmigt, - z.B. in der Originalform, wie es empfangen wurde. Ist das zusammengeführte Paket nicht beschädigt und wenn es entschlüsselt werden kann (wenn Entschlüsselung erforderlich ist), wird CommView for WiFi das A-MSDU wieder zerlegen und die Einzelpakete in der Paketeauflistung anzeigen. Solche Pakete werden in der Spalte "Mehr Details" als "Subframe #... of A-MSDU #..." gekennzeichnet. Zusätzlich wird den Subframes das original zusammengeführte A-MSDU nachgestellt, welches als "A-MSDU #...." gekennzeichnet ist. Wenn das zusammengeführte Paket beschädigt oder verschlüsselt ist, wird nur das original A-MSDU angezeigt. A-MSDUs können mit jedem empfolenen 802.11ac- und 802.11ax-Adapter erfasst werden.

Beachten Sie, dass große Frames, wie A-MSDUs, häufig beschädigt sind, besonders wenn Sie mit hohen Datenraten gesendet worden sind.

CommView for WiFi innerhalb virtueller Maschine benutzen

Sie können CommView for WiFi innerhalb eines virtualisierten Windows-Betriebssystems installieren und benutzen, das als Gastbetriebssystem auf Mac (oder PC, wenn Sie aus irgendeinem Grund die virtuelle Umgebung vorziehen) betrieben wird. Um dies zu realisieren, brauchen Sie eine Virtualisierungssoftware wie **VMWare**, **Parallels Desktop für Mac** oder **Virtual Box**.

Gastbetriebssystem

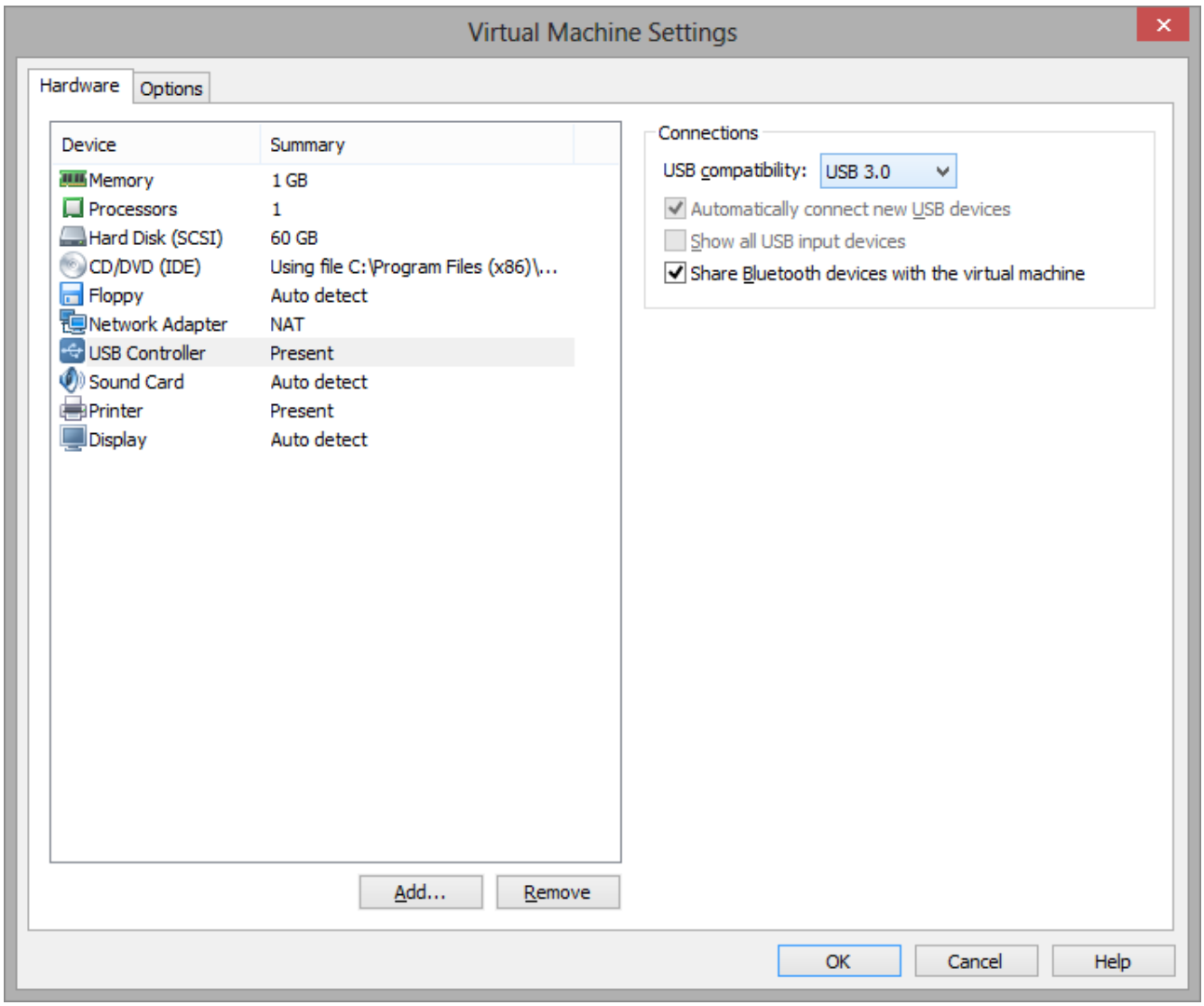
Als Windows-Gastbetriebssystem können Sie Windows 10 oder Windows 11 benutzen.

Hardware

Um CommView for WiFi für passive Erfassungen zu benutzen, benötigen Sie einen kompatiblen Adapter. Wenn Sie unsere Software auf einem Windows-Notebook laufen lassen, können Sie einen beliebigen kompatiblen Adapter mit verschiedenen Formfaktoren verwenden. Eine Aufstellung der kompatiblen Adapter finden Sie **hier**. Wenn Sie CommView for WiFi innerhalb einer virtualisierten Windows-Maschine betreiben, können Sie **nur USB-Adapter** benutzen. Bitte sehen Sie in der Aufstellung der kompatiblen Adapter nach, ob der USB-Adapter, den Sie verwenden möchten, dort zu finden ist. Wir empfehlen dringend, einen Adapter zu wählen, der als „empfohlen“ gekennzeichnet ist. Die Adapter sind jederzeit auch direkt bei uns erhältlich, wenn Sie die verpackte Version kaufen.

Virtualisierungssoftware konfigurieren

Falls Ihre Virtualisierungssoftware USB 3.0 Emulation unterstützt (es ist der Fall, wenn Sie VMWare oder Parallels Desktop für Mac verwenden), sicherstellen Sie, dass Sie USB 3.0 Emulation eher als USB 2.0 verwenden, auch dann, wenn Ihre USB-Port und Wi-Fi Adapter 2.0 sind. USB-Konfiguration in VMWare (siehe Illustration unten).



Die USB-3.0-Emulation ist vorzuziehen, da sie die Kommunikationsgeschwindigkeit zwischen dem Wi-Fi-Adapter und dem Gastbetriebssystem drastisch erhöht. So dauert zum Beispiel bei einigen Adaptern die Anschaltung eines Wi-Fi Kanals 500 und sogar 1000 Millisekunden, wenn die USB-2.0-Emulation verwendet wird, bei Verwendung der USB-3.0-Emulation hingegen nur 100 Millisekunden. Bedenkt man, dass CommView for WiFi normalerweise alle 250 Millisekunden die Kanäle umschaltet, ist dieser Unterschied dramatisch. Die Verwendung einer USB-2.0-Emulation könnte die Geschwindigkeit der Applikation wesentlich reduzieren.

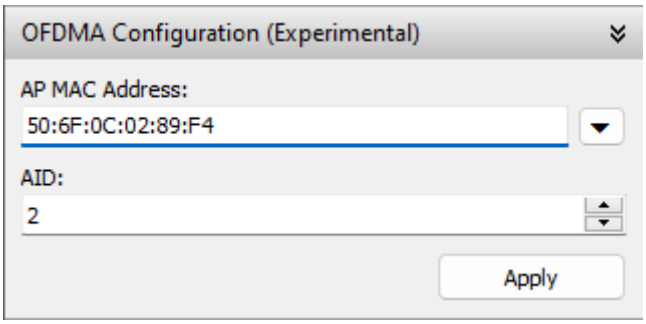
Aus diesem Grund, empfehlen wir, dass Sie **VirtualBox** als Virtualisierungssoftware nicht benutzen sollen. Zum Zeitpunkt der Abfassung dieses Textes unterstützt VirtualBox USB 3.0 nicht. Wenn Sie noch immer VirtualBox benutzen möchten, verwenden Sie zumindest die Option **USB 2.0 (EHCI) Controller aktivieren**. Sonst wird Ihr drahtloser USB-Adapter nicht funktionieren.

Installation des Adapters

Schließen Sie den USB-Adapter an Ihren Computer an. Wenn der Adapter angeschlossen ist, müssen Sie Ihre Virtualisierungssoftware konfigurieren, um das erkannte USB-Gerät zu verwenden, indem Sie den Adapter vom Host-Betriebssystem trennen und mit dem Gastbetriebssystem verbinden. Das Konfigurationsverfahren hängt von der konkret verwendeten Virtualisierungssoftware ab – bitte sehen Sie in der betreffenden Dokumentation nach. Nachdem die virtuelle Maschine die Kontrolle über den Adapter übernommen hat, benachrichtigt Sie Windows, dass ein neues USB-Gerät erkannt wurde und die benötigten Treiber dafür gesucht werden. Klicken Sie im CommView for WiFi Programmenü auf **Hilfe => Treiberinstallationsanweisung**, um die Anweisungen zur Installation unseres speziellen Treibers für die Erfassung der Datenpakete zu finden. Nach erfolgreicher Installation des Treibers können Sie die Applikation neu starten und benutzen.

OFDMA Erfassung

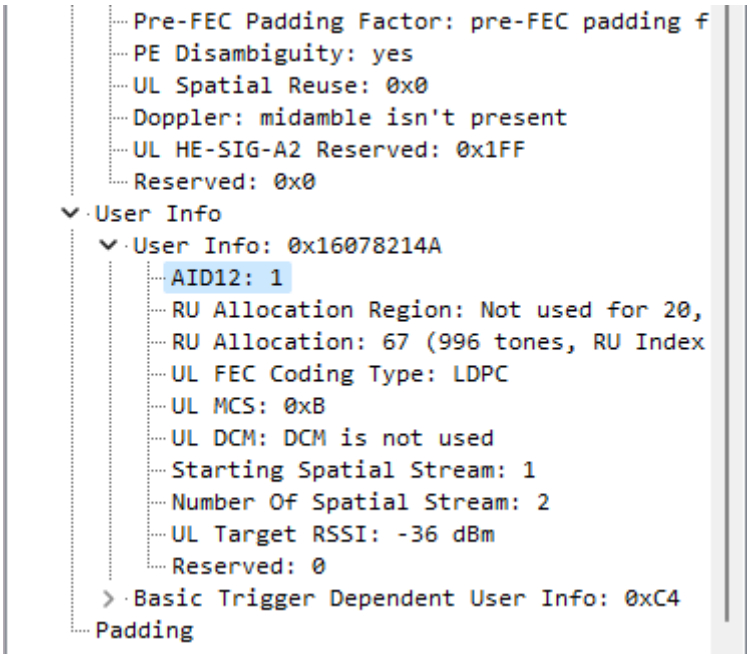
CommView for WiFi ist in der Lage, OFDMA-Pakete zu erfassen, die von APs an STAs gesendet werden. Diese Funktionalität ist nur verfügbar, wenn Sie einen Intel-Adapter mit Wi-Fi 802.11ax (Wi-Fi 6)-Unterstützung verwenden, d. h. Sie benötigen Intel AX200 oder ein neueres Modell. Wenn ein solcher Adapter erkannt wird, wird im Hauptanwendungsfenster ein zusätzliches OFDMA-Panel angezeigt:



Aufgrund der Einschränkungen der Hardware werden OFDMA-Pakete erst erfasst, wenn Sie die MAC-Adresse des überwachten AP sowie die Zuordnungs-ID (AID oder AID12) der STA eingeben, die Sie überwachen möchten. Sie können nur die OFDMA-Pakete erfassen, die mit der angegebenen MAC-Adresse und den AID-Parametern übereinstimmen. Sie können nicht den gesamten OFDMA-Verkehr zwischen beliebigen APs und STAs erfassen.

Die MAC-Adresse finden Sie virtuell in jedem Paket, oder Sie können die Pfeilschaltfläche rechts neben dem MAC-Adressfeld verwenden, um einen der APs auszuwählen, die die Anwendung derzeit „sieht“.

Die AID ist in CTRL/TRIGGER-Paketen zu finden (bitte beachten Sie, dass CTRL-Pakete standardmäßig nicht von CommView for WiFi angezeigt werden, Sie müssen die entsprechende Schaltfläche in der Symbolleiste drücken). Sobald Sie ein CTRL/TRIGGER-Paket vom AP zu der spezifischen STA gefunden haben, an der Sie interessiert sind, können Sie die AID im Decoder-Baum sehen:



Da es bei hoher Verkehrslast nicht immer einfach ist, CTRL/TRIGGER-Pakete zu finden, können Sie in **Erweiterte Regeln** die folgende Formel verwenden, um solche Pakete zu filtern: (ftype=1 und fsubtype=2).

Nachdem Sie die MAC-Adresse des AP und die AID der STA eingegeben haben, klicken Sie auf **Übernehmen**. Dadurch erfasst die Anwendung den OFDMA-Verkehr (falls vorhanden) zwischen dem angegebenen AP und dem Client mit der angegebenen AID.

Mehrkanalerfassung

CommView for WiFi ist in der Lage, Daten von mehreren Kanälen gleichzeitig zu erfassen, wenn mehrere kompatible USB-Adapter verwendet werden.

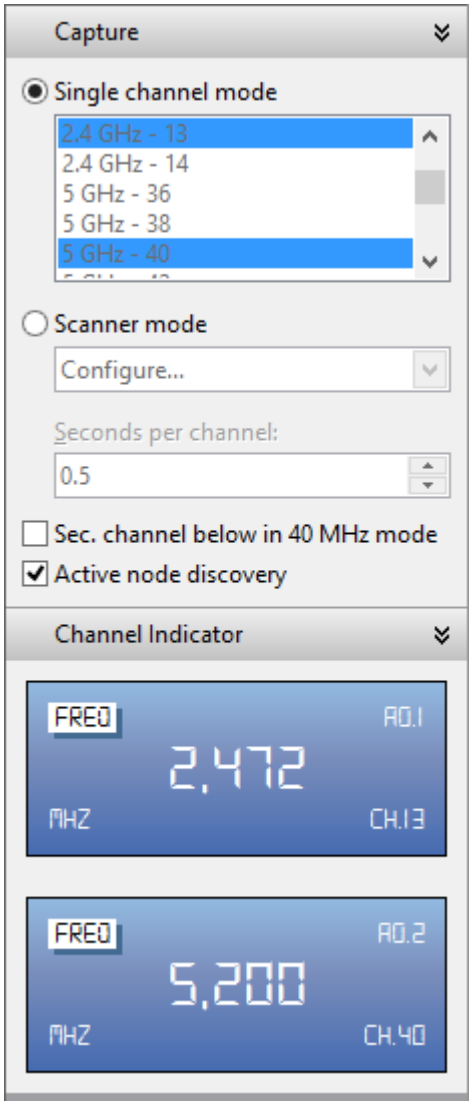
Die folgenden 802.11ac-USB-Adapter können für die Mehrkanalerfassung verwendet werden: ASUS USB-AC68, Belkin F9L1109 v1, D-Link DWA-180 rev A1, D-Link DWA-182 rev C1 oder D1, Edimax EW-7822UAC, Edimax EW-7833UAC, EnGenius EUB1200AC, Linksys WUSB6300, Linksys WUSB6400M, NETGEAR A6210, Proxim ORiNOCO 9100, Rosewill RNX-AC1200UB, TP-LINK Archer T4U, TP-LINK Archer T4UH, TP-LINK Archer T9UH v2, TRENDnet TEW-805UB, ZyXEL NWD6605 und ZyXEL AC240. Die folgenden 802.11ax-USB-Adapter können für die Mehrkanalerfassung verwendet

werden: ASUS USB-AX56, D-Link DWA-X1850, FusionFutures AX1800, NETGEAR A8000 und Alfa AWUS036AXML.

Beachten Sie bitte, dass verschiedene Adaptertypen nicht vermischt benutzt werden können; alle Adapter sollten das gleiche Modell sein. Wenn mehrere Adapter angeschlossen sind, verändern sich die folgenden Elemente der Bedienfläche:

- Der Bereich Kanalauswahl im Ausschnitt **Erfassung** ermöglicht es Ihnen, mehrere Kanäle zu wählen. Sie können mehrere Kanäle mit gedrückter **Ctrl**-Taste auswählen. Die Zahl der ausgewählten Kanäle kann die Zahl der angeschlossenen USB-Adapter nicht überschreiten.
- Der Ausschnitt **Kanal-Anzeige** zeigt mehrere **Markers**; ihre Zahl entspricht der Zahl der angeschlossenen USB-Adapter.

Dies wird in folgendem Bildschirmfoto illustriert.



Wenn Sie mehrere Adapter verwenden, beachten Sie bitte folgende Punkte:

1. **Energieverbrauch**. Ein einzelner Adapter kann bis zu 450 mA verbrauchen. Ein einzelner USB-2.0-Anschluss kann bis zu 500 mA bereitstellen. Ein einzelner USB-3.0-Anschluss kann bis zu 900 mA bereitstellen. Ein moderner Laptop hat zwei USB-3.0-Anschlüsse, also können Sie entweder einen Adapter pro Anschluss verwenden oder einen USB-Hub benutzen; aber wenn Sie drei Adapter in den USB-Hub einstecken, wird die Begrenzung von 900 mA überschritten, was unerwünschte Wirkungen haben könnte – z. B. könnten die Adapter ohne Warnung mit der Erfassung von Paketen aufhören.
2. **Kanal-Umschaltzeit**. Wenn CommView for WiFi im Scannermodus läuft, dauert die Kanal-Umschaltung einige Zeit – zwischen 20 und 80 Millisekunden pro Adapter. Stellen Sie sich vor, dass 12 Kanäle mit dem Scannerintervall von 250 ms pro Kanal gescannt werden und die Kanal-Umschaltzeit 60 ms beträgt. Die Gesamtzeit wäre (250 + 60) * 12 = 3,72 Sekunden, wenn Sie einen

Adapter verwenden. Wenn Sie drei Adapter verwenden, wäre die Gesamtzeit 250 + 60 *3) * 4 = 1,72 Sekunden. Dies ist 2,16-mal besser, nicht 3-mal. Je mehr Adapter Sie also benutzen, desto größer ist die Kanal-Umschaltzeit. Wenn Sie 12 Adapter benutzen, was theoretisch auch möglich ist, beträgt die Gesamtzeit 250 + 60 * 12 = 0,97 Sekunden, um 12 Kanäle zu scannen – Sie gewinnen also nicht so viel Zeit.

Daher empfehlen wir, nicht mehr als zwei oder drei Adapter zu verwenden.

Spektralanalyse

Spektralanalyse beinhaltet den Gebrauch von speziellem RF-Equipment für das Abhören und die Analyse der von Wi-Fi-Geräten benutzten Frequenzbänder. Weil diese Bänder unlizensiert sind, werden Sie oft von RF-Signalen von Nicht-Wi-Fi-Quellen mitgenutzt, wie drahtlosen Videokameras, Mikrowellenöfen oder drahtlosen Telefonen, wodurch Interferenz verursacht wird. Der Zweck der Spektralanalyse ist es, solche Interferenzquellen zu entdecken, sie zu beseitigen und/oder die WLAN-Kanäle mit minimaler Interferenz zu ermitteln.

Hardwareanforderungen

CommView für WiFi kann durch die Verbindung mit den USB-basierten Spektrumanalysatoren **WiPry** oder Wi-Spy gleichzeitig mit der Paketerfassung eine Spektralanalyse durchführen. WiPry kann bei **TamoSoft** oder bei **Oscium** erworben werden.

CommView for WiFi unterstützt die folgenden Wi-Spy-Modelle:

- Wi-Spy DBx (Dual-Band, 2,4 GHz und 5 GHz)
- Wi-Spy 2.4x (Einzelband, 2,4 GHz)
- Wi-Spy 2.4i (Einzelband, 2,4 GHz)

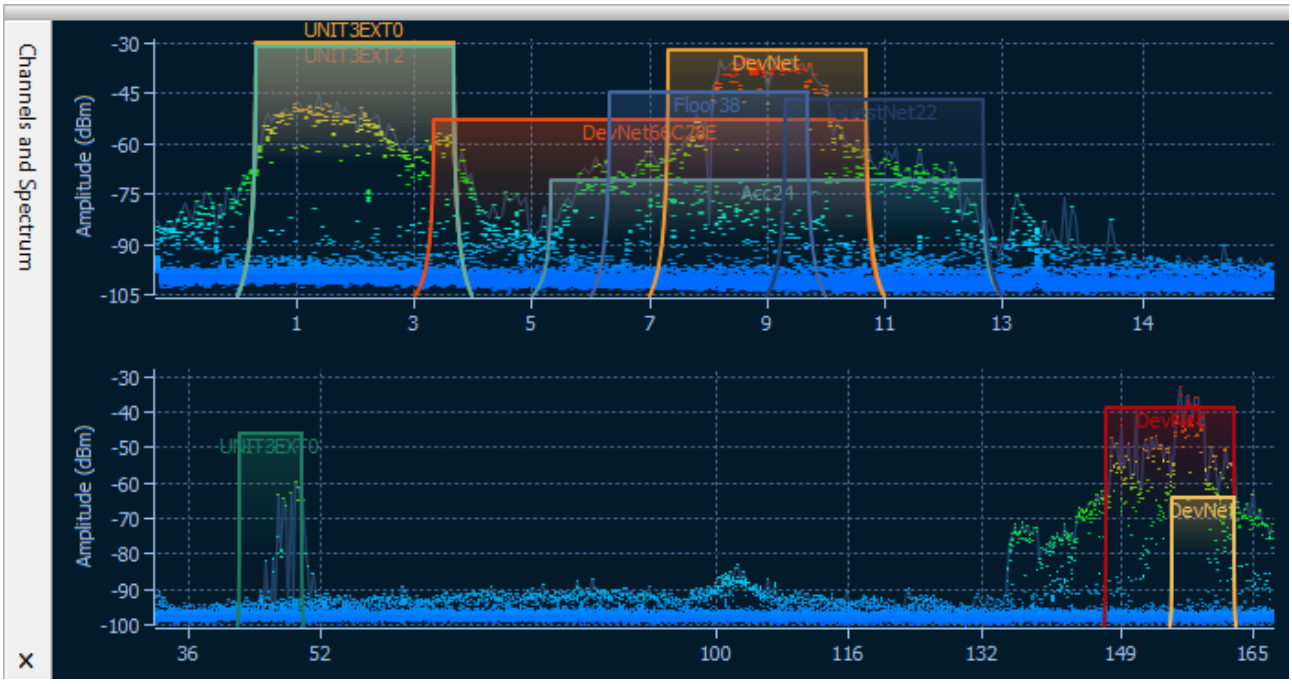
CommView for WiFi unterstützt die folgenden WiPry-Modelle:

- WiPry Clarity (Tri-Band, 2,4 GHz, 5 GHz und 6 GHz)
- WiPry 2500x (Dual-Band, 2,4 GHz und 5GHz)

Wenn ein Multiband-Modell verwendet wird, werden kontinuierlich mehrere Bänder nacheinander durchsucht. Die gleichzeitige Verwendung von zwei Wi-Spy DBx-Geräten könnte die Datenqualität verbessern, da CommView for WiFi jedes der Geräten nur einem Band zuordnen würde. Beachten Sie, dass Sie nicht zwei WiPry-Geräte desselben Typs gleichzeitig verwenden können. Sie können jedoch WiPry Clarity und WiPry 2500x kombinieren und Wi-Spy- und WiPry-Geräte kombinieren.

Spektraldatendiagramme

Wenn ein USB-Spektrumanalysator angeschlossen ist, wird ein aktives Spektrumabbild im Ausschnitt **Kanäle und Spektrum** des Hauptfensters von CommView for WiFi angezeigt, wie im Folgenden gezeigt wird.



Der Spektrumausschnitt ist ähnlich dem von **Chanalyzer**, einer Spektralanalyseapplikation von MetaGeek, die mit Wi-Spy ausgeliefert wird. Standardmäßig zeigt der Ausschnitt **Kanäle und Spektrum** jeweils ein oder zwei Flächendiagramme für Einzel- oder Dualband-Wi-Spy-Modelle.

Das Aussehen der Diagramme kann über das Kontextmenü gesteuert werden. Wählen Sie **2,4 GHz**, **5 GHz**, **6 GHz** oder **Dual**, damit im Spektrumbereich eines der einzelnen Frequenzbänder oder zwei von drei verfügbaren Bändern gleichzeitig angezeigt werden (**5 GHz**, **6 GHz** und **Dual** sind nur verfügbar, wenn Sie über ein Dual- oder Tri-Bandanalysator verfügen). Wählen Sie **Aktuelles Niveau** zur Einblendung einer Linie, welche die aktuelle Signalamplitude anzeigt; wählen Sie **Max. Niveau** zur Einblendung einer Linie, welche die maximale Signalamplitude zeigt. Das Element **X-Achse** ermöglicht es Ihnen, die Maßeinheit für die Horizontalachse zu wählen; Sie können zwischen **Frequenz** in MHz und **Kanalnummern** wählen. Bei Aktivierung der **Wasserfall**-Ansicht erhalten Sie die Applikationskurve der Amplitude im Zeitablauf. Wählen Sie **1/3**-, **1/2**- oder **2/3-Fenstergröße** zur Festlegung der Fenstergröße für das Wasserfall-Diagramm. Der Spektrumausschnitt kann von der Hauptapplikation gelöst und als ein separates schwebendes Fenster angezeigt werden. Benutzen Sie **Fenster lösen** und **Fenster anhängen** um die entsprechenden Funktionen auszuführen. Sie können den Spektrumausschnitt durch Aktivieren oder Deaktivieren des Elementes **Ansicht => Kanäle und Spektrum** im Hauptmenü der Applikation ausblenden.

Beachten Sie, um Spektraldaten in CommView for WiFi anzuzeigen, müssen Sie Chanalyzer schließen, falls er läuft; Wi-Spy kann nicht simultan von mehreren Applikationen erreicht und kontrolliert werden.

Erfassung von intensivem Verkehr

Wenn Sie Daten aus einem grossen und stark benutzten Netzwerksegment erhalten, sollten Sie berücksichtigen, dass die Verarbeitung von tausenden Paketen/Sekunde durchaus die CPU-Auslastung erhöhen und das Programm träger reagieren kann. Zur Erhöhung der Programmperformance sollten Sie Regeln benutzen, um nichtbenötigte Pakete auszufiltern. Das Senden einer 50 MB grossen Datei zwischen zwei Maschinen innerhalb Ihres WLANs erzeugt ungefähr 40.000 NetBIOS Pakete mit einem Datentransfervolumen von 5 MB/Sekunde, was doch eine starke Belastung für das Programm darstellen kann. Normalerweise brauchen Sie aber nicht jedes NETBIOS-Paket zu überwachen, so dass Sie CommView for WiFi so konfigurieren könnten, dass es nur IP-Pakete erfasst. CommView for WiFi bietet ein flexibles Filtersystem, mit dem Sie die Anwendung so feintunen können, dass sie nur die wirklich benötigten Pakete anzeigt. Wenn Sie nur statistische Funktionen brauchen (grüne Histogramme, Kuchengrafiken, Hosttabellen) können Sie des Weiteren mittels des Menüs „Paketausgabe unterbrechen“ die statistischen Informationen gewinnen, ohne eine Echtzeitanzeige zu benötigen.

Die Programmperformance wird verbessert durch:

- Eine schnelle CPU (Intel Core i7 wird empfohlen)
- RAM Größe (8 GB und mehr wird empfohlen)
- Die Verwendung von Filtern, zur Ausfilterung von unnötigem Verkehr

CommView for WiFi im nichtsichtbaren Modus

Es gibt zwei Möglichkeiten CommView for WiFi als versteckten Prozess laufen zu lassen:

1. Starten Sie CommView for WiFi mit dem Switch hidden (verborgen), z.B.:
   CV.EXE hidden
2. Wenn CommView for WiFi bereits läuft können Sie mit es ein-/ausblenden, indem Sie einen Hotkey verwenden. Zum Ausblenden drücken Sie bitte die Tastenkombination [ALT]+[SHIFT]+[h].

Vergessen Sie nicht, dass Sie Windows-Applikationen nicht vollständig verstecken können. Im unsichtbaren Modus kann man den CommView for WiFi-Prozess immer noch im Task-Manager sehen.

Kommandozeilen Parameter

Bei laufendem Programm können Sie mit folgenden Kommandozeilenparameter bestimmten Aktionen starten lassen:

- Lade und aktiviere ein Regelset aus einer Datei. Verwenden Sie den Schalter /ruleset mit nachfolgendem Dateinamen und dem vollen Pfad, z.B.:

```
CV.EXE /ruleset "C:\Program Files\CommViewWiFi\Rules\POP3Rules.rls"
```

  Wenn ein Dateiname oder dessen Pfad Leerzeichen enthält, muß dieser in Anführungszeichen (" ") gesetzt werden.

- Lade und aktiviere einen WEP-/WPA-Schlüsselsatz aus einer Datei. Verwenden Sie den Schalter /keyset mit nachfolgendem Dateinamen und dem vollen Pfad, z.B.:

```
CV.EXE /keyset "C:\Program Files\CommViewWiFi\WLAN3Keys.wep"
```

  Wenn ein Dateiname oder dessen Pfad Leerzeichen enthält, muß dieser in Anführungszeichen (" ") gesetzt werden.

- Wählen Sie das ausgesuchte Verzeichnis für die Logdateispeicherung. Verwenden Sie den Schalter /logdir gefolgt vom vollen Pfad zur Datei, z.B.:

```
CV.EXE /logdir "C:\Program Files\CommView\Logs"
```

- Starten Sie die Applikation ohne die Eingabeaufforderung den Treiber zu installieren. Dies ist brauchbar, wenn Sie CommView for WiFi benutzen um Protokolle anderer Computer zu laden oder für Verbindungen zu Remote Agents. Benutzen Sie den Schalter /noprompt, z.B.:

```
CV.EXE /noprompt
```

- Verbinden Sie zu einem oder mehreren Remote Agents. Benutzen Sie den Schalter "/ra" mit nachfolgender IP-Adresse oder Hostnamen des Remote Agents zu dem Sie sich verbinden möchten, gefolgt vom Passwort in Anführungszeichen und der zuüberwachenden Kanalnummer (der Kanalindex ist 1-basierend, z.B. wenn Sie die Überwachung im Scanner-Modus durchführen müssen, benutzen Sie die "1"; wenn Sie den ersten Kanal überwachen müssen, benutzen Sie "2") z.B.:

```
CV.exe /ra 192.168.0.5 "MeinPasswort" 2
```

- Zur Verbindung zu mehreren Remote Agents aus einem CommView for WiFi-Lauf, benutzen Sie dann eine Stapelverarbeitungsdatei ähnlich der folgenden:

```
START "CV" "C:\Program Files\CommViewWiFi\CV.exe" /noprompt
PING 1.1.1.1 -n 1 -w 5000 >NUL
START  "CV"  "C:\Program  Files\CommViewWiFi\CV.exe" /ra  192.168.0.1
"pwd1" 5
PING 1.1.1.1 -n 1 -w 1000 >NUL
START  "CV"  "C:\Program  Files\CommViewWiFi\CV.exe" /ra  192.168.0.2
"pwd2" 5
PING 1.1.1.1 -n 1 -w 1000 >NUL
START  "CV"  "C:\Program  Files\CommViewWiFi\CV.exe" /ra  192.168.0.3
"pwd3" 5
PING 1.1.1.1 -n 1 -w 1000 >NUL
```

Dieses Script startet CommView for WiFi, wartet 5 Sekunden um sichzustellen, dasss die Applikation geladen wurde (wir benutzen das Kommando PING zum pausieren, da es keine Möglichkeit gibt, in einer BAT-Datei eine Pause zu progammieren), dann üergeben wir der Applikation die IP-Adresse, Passwörter und Adapternummern von 3 Remote Agents (mit 1-Sekunden-Pausen).

Sie können alle diese Parameter gleichzeitig anwenden, ausgenommen den letzten Parameter.

Datenaustausch mit Ihrer Anwendung

CommView for WiFi bietet ein einfaches TCP/IP-Interface, dass es Ihnen ermöglicht von CommView for WiFi empfangene Pakete zu verarbeiten, während Sie gleichzeitig Ihre eigene Applikation in Echtzeit verwenden. Ab Version 5.0 können Sie mit diesem Interface auch Pakete senden (analog zur Paketgeneratorfunktion in CommView).

So geht das

CommView for WiFi sollte mit dem speziellen Kommandozeilenargument MIRROR gestartet werden, welches das Programm auffordert, empfangene Pakete an eine bestimmte IP-Adresse und einen TCP-Port Ihrer Wahl zu spiegeln.

Beispiele:

```
CV.EXE  mirror:127.0.0.1:5555 //  spiegelt  die  Pakete  in  die
Loopbackadresse, TCP Port 5555
```

```
CV.EXE mirror:192.169.0.2:10200 // spiegelt die Pakete nach 192.169.0.2,
TCP Port 10200
```

Wenn CommView for WiFi mit einem solchen Schalter gestartet wurde, versucht es eine TCP-Session durch Verbinden zu der definierten IP- Adresse bzw. Portnummer zu generieren. Das bedeutet, dass Sie bereits die Anwendung laufen lassen und einen bestimmten Port abhören lassen. Wenn CommView for WiFi keine Verbindung erzeugen kann, versucht das Programm alle 15 Sekunden eine Neuverbindung herzustellen. Dies geschieht auch bei einem Verbindungsabbruch. Auch hier versucht CommView for WiFi alle 15 Sekunden eine Neuverbindung herzustellen. Wenn diese Verbindung erfolgreich hergestellt wurde sendet CommView for WiFi die gesammelten Pakete in Echtzeit zu dieser definierten IP-Adresse.

Daten Format

Die Daten werden im NCF-Format übertragen. Mehr dazu unter **CommView Logdateiformat**.

Pakete senden

Pakete können von Ihrer Anwendung nicht nur empfangen, sondern auch mittels des Paketgenerators gesendet werden. Dabei sendet CommView for WiFi die Daten über dieselbe TCP-Verbindung, über die Sie auch die Daten erhalten. Das Datenformat ist einfach. Sie sollten die Paketlänge (2 Byte lange unsignierte Integer in Little-endian-Standardreihenfolge), den Datenraten-Index (2 Byte lange unsignierte Integer in Little-endian-Standardreihenfolge) und danach das Paket selbst senden. Die Paketlänge sollte nicht die 4 Byte enthalten, die dem Paketkörper vorangehen. Der Datenraten-Index basiert auf Null; er soll den Raten-Index enthalten, wie er im **Paketgenerator** angezeigt wird. Beachten Sie das folgende Beispiel:

Der im Hex gesendete String: D4 00 00 00 80 1F 02 66 C2 8E. Die Länge dieses Strings ist 10 Byte.

Die benutzte Rate: 5,5 Mbit/s. Es ist das dritte Element in der Drop-down-Liste "802.11-Datenrate" im **Paketgenerator**.

Der daraus resultierende zu sendende Puffer lautet: 0A 00 02 00 D4 00 00 00 80 1F 02 66 C2 8E.

Wenn der Adapter nicht geöffnet wurde oder keine Paketinjektion erlaubt, wird das Paket ohne Hinweis verworfen.

Beispielprojekte

Zwei einfache Demoanwendungen, die auf eingehende Verbindungen hören extrahieren Pakete aus dem Stream und zeigen sofern vorhanden die Rohdaten.

- **https://www.tamos.com/products/commwifi/samp_mirr_c7.zip**. Dies ist ein Visual Studio Projekt mit C++ Quellcode.

- https://www.tamos.com/products/commwifi/samp_mirr_d7.zip. Dies ist ein Delphi-Project mit Pascal Sourcecode. Wenn Sie das Projekt kompilieren wollen benötigen Sie die bekannten ICS-Komponentensuite von Francois Piette, erhältlich unter http://www.overbyte.be.

Bandbreite

Wenn Sie Daten auf einem entfernten Computer spiegeln, sollten Sie sicherstellen, dass der Link zwischen CommView for WiFi und dem Ziel der Spiegelung schnell genug ist, um die empfangenen Daten zu transportieren. Wenn CommView for WiFi 500 KBytes/sec empfängt und Ihr Link nur 50 KBytes/sec versenden kann, werden Sie zwangsläufig einen Datenstau bekommen, der verschiedene Probleme erzeugen kann. Z. B. könnte Winsock bei einigen Windowsversionen aufhören Daten zu senden.

Maßgeschneidertes Decoding

CommView for WiFi ermöglicht die Verwendung von zwei selbstdefinierten Decoder-Arten.

Einfacher Decoder

Wenn Sie diesen Decodertyp wählen wird die Decoder-Ausgabe in einer Extraspalte im Register **Pakete** angezeigt. Der Decoder sollte dabei eine 32-bit DLL-Datei namens "Custom.dll" sein, die nur eine Prozedur namens "Decode" exportiert. Der Prototyp dieser Prozedur wird unten in C und Pascal dargestellt:

```
extern "C" {

    void __stdcall Decode(unsigned char *PacketData, int PacketLen, char *Buffer, int BufferLen);

} procedure Decode (PacketData: PChar; PacketLen: integer; Buffer: PChar; BufferLen: integer); stdcall;
```

Die DLL muß sich dabei im CommView for WiFi Installationsverzeichnis befinden. Beim Start von CommView for WiFi sucht es nach der Custom.dll im Installationsverzeichnis und lädt diese in den Speicher. Wenn der Eingangspunkt für Decode gefunden wurde, fügt CommView for WiFi eine neue Spalte namens Custom (Selbstdefiniert) der Paketliste hinzu.

Wird ein neues Paket empfangen und angezeigt, ruft CommView for WiFi die Decode-Prozedur auf und gibt die Paketinhalte an die DLL weiter. Die Decode-Prozedur muß nun die Paketinformation verarbeiten und kopiert dann das Ergebnis in den Puffer. Das erste Argument ist der Paket-Pointer zu den Paketdaten, das zweite Argument die Datenlänge und das dritte Argument der Pointer zum

Puffer, in den die Ergebnisse des Decodings kopiert werden sollen. Das vierte Argument ist die Puffergröße (derzeit stets 1024 Bytes). Der gesamte Puffer ist für CommView for WiFi zugeteilt und freigegeben. Sie sollten nicht versuchen diese Zuteilung zu ändern. Das in den Speicher kopierte Ergebnis wird dann als String in der Spalte Custom angezeigt.

Ihre Prozedur sollte schnell genug sein um tausende von Paketen/Sekunde zu verarbeiten. Sonst wird die Anwendung unnötig langsam. Bitte halten Sie sich auch an die Konvention STDCALL.

Zwei Demo-DLL's sind verfügbar. Sie zeigen eine einfache Operation: Die Ausgabe der Decode-Funktion ist der Hexcode der letzten Byte des Paketes. Ihr eigener Decoder kann natürlich beliebig komplex sein:

- **https://www.tamos.com/products/commview/cust_decoder_c.zip**. Dies ist ein Visual Studio Projekt mit C++ Quellcode.
- **https://www.tamos.com/products/commview/cust_decoder_d.zip**. Dies ist ein Delphi-Project mit Pascal Sourcecode.

Komplexer Decoder

Bei der Verwendung dieses Decodertypes wird die Decoderausgabe als zusätzliche Objekte im Paketdecoderbaum angezeigt. Mehr zur Implementation dieses Decoders erhalten Sie durch das Herunterladen folgender Datei:

https://www.tamos.com/products/commview/complex_decoder_c7.zip

Diese Decoderart kann nur in Microsoft Visual C++ geschrieben werden, da es mit C++ erzeugte Klassen benutzt.

Technischer Support

Technischen Support für maßgeschneiderte Decoder gibt es auf der Basis von "Besten Ergebnissen".

CommView Logdateien Format

CommView und CommView for WiFi verwenden das unten beschriebene Datenformat um empfangene Pakete als NCF-Datei abspeichern zu können. Dies ist ein offenes Datenformat, das Sie zur Verarbeitung von Logdateien verwenden können, aber auch für den direkten Datenaustausch mit Ihrer Applikation. Dies ist in der Hilfedatei beschrieben.

Format NCFX

Dieses neue Format wurde in CommView für WiFi 7.3 eingeführt. Ältere CommView for WiFi-Versionen und aktuelle CommView-Versionen (ohne Wi-Fi) verwenden das alte NCF-Format, das im entsprechenden Abschnitt unten beschrieben wird.

Pakete werden nacheinander aufgezeichnet. Zwei oder mehr Header, deren Struktur unten angegeben ist, stellen jeden Paketkörper voran. Alle Header-Felder mit einer Länge von mehr als einem Byte verwenden die Little-Endian-Reihenfolge und sind ohne Vorzeichen.

General Header – Pflichtfeld. Länge = 20 Byte.

Feldname	Länge (Bytes)	Beschreibung
Datenlänge	4	Die Länge des Pakets, einschließlich der Länge dieses und der folgenden Header und einschließlich der Länge des Paketinhalts (Body).
Jahr	2	Paketdatum (Jahr)
Monat	1	Paketdatum (Monat)
Tag	1	Paketdatum (Tag)
Stunden	1	Paketdatum (Stunden)
Minuten	1	Paketdatum (Minuten)
Sekunden	1	Paketdatum (Sekunden)
Mikrosekunden	4	Paketdatum (Mikrosekunden)
Medientyp	1	Der Typ des Paketmediums.0x01 für Wi-Fi-Pakete, 0x00 für Ethernet-Pakete.
Entschlüsselungsflag	1	0x01 wenn das Paket bereits von CommView for WiFi entschlüsselt wurde und wird in entschlüsselter Form gespeichert. Sonst ist der Wert 0x00.
Richtung	1	Paketrichtung für Ethernet-Pakete: 0x00 bei Pass-through, 0x01 bei Inbound, 0x02 bei Outbound. WiFi-Pakete: immer 0x00.
Reserviert1	1	Derzeit ungenutzt

Reserviert2	1	Derzeit ungenutzt

RF Header – Pflichtfeld. Länge = 20 Byte.

Feldname	Länge (Bytes)	Beschreibung
RF Header Länge	2	Die Länge dieses Header, einschließlich der Länge aller zusätzlichen Erweiterungen (Header), falls vorhanden.
Paketstatus und Modulation	2	Eine Bitmaske, bei der eines oder mehrere der folgenden Bits gesetzt sind: ▪ Bit 0 – Das Paket ist beschädigt (falsches FCS) ▪ Bit 1 – Das Paket wurde mit einer HT PHY Rate gesendet (802.11n) ▪ Bit 2 – Das Paket wurde mit einer VHT PHY Rate gesendet (802.11ac) ▪ Bit 3 – Das Paket wurde mit einer HE PHY Rate gesendet (802.11ax) ▪ Bit 4 – HE Modulation, 0 – OFDM, 1 – OFDMA, nur gültig, wenn Bit 3 ist eingestellt
Band	2	0x40 für 5 GHz, 0x80 für 2,4 GHz, 0x100 für 6 GHz
Kanal	2	Wi-Fi-Kanal
Geräuschstärke (dBm)	1	Geräuschstärke in dBm, als vorzeichenloser Wert; z.B. -90 dBm wird als 90 gespeichert.
Signalstärke (dBm)	1	Signalstärke in dBm, als vorzeichenloser Wert; z.B. -30 dBm wird als 30 gespeichert.
Signal Level (Prozente)	1	Signal level als Prozentsatz
Reserviert	1	Derzeit ungenutzt
PHY Rate	4	PHY Datenübertragungsrate in Mbit/s mal 10

Präsenz von Erweiterungen	4	Eine Bitmaske, die das Vorhandensein zusätzlicher Erweiterungen (Header) nach diesem RF-Header anzeigt. Zum Beispiel, wenn die Bits 3, 2 und 0 sind gesetzt, wird der RF Header von einer Erweiterung des Typs 0 gefolgt, dann kommt die Erweiterung des Typs 2 und die Erweiterung des Typs 3.

Derzeit unterstützte Erweiterungen

MCS-Headertype 0 – Optional. Size = 4 Byte.

Beachten Sie, dass der MCS-Headertyp 0 niemals hinzugefügt wird, wenn Sie Pakete mit einem 802.11ac Adapter erfassen. MCS-Informationen werden nur hinzugefügt, wenn zum Erfassen 802.11ac-Adapter und neuere Adapter verwendet werden.

Feldname	Länge (Bytes)	Beschreibung
MCS Index	1	MCS index
Anzahl der Ströme	1	Anzahl der MIMO spatialen Ströme minus 1; z.B. der Wert 0x00 bezeichnet ein Strom.
Kanalbreite	1	Kanalbreite Wenn Bit 4 im Feld **Paketstatus und Modulation** gleich 0 wird (OFDM Modulation): 0x00 – 20 MHz, 0x01 – 40 MHz, 0x02 – 80 MHz, 0x03 – 160 MHz, 0x05 – 320 MHz. Wenn Bit 4 im Feld **Paketstatus und Modulation** gleich 1 wird (OFDMA Modulation): 0x00 - 26-tone RU, 0x01 – 52-tone RU, 0x02 – 106-tone RU, 0x03 – 242-tone RU, 0x04 – 484-tone RU, 0x05 – 996-tone RU, 0x06 – 1992-tone RU (996x2-tone RU)
GI	1	Schutzintervall (Guard Interval): 0x00 - 0.8µs, 0x01 - 0.4µs, 0x02 - 1.6µs, 0x03 - 3.2µs

Beispiel 1

Ein 350 Byte langes Beacon-Paket, das mit der legacy PHY-Rate von 6 Mbit/s gesendet wird, wird gespeichert als:

[20 Byte für General Header, wo das Feld **Datenlänge** auf 390 gesetzt wird] + [20 Byte für RF Header, wo das Feld **RF Header Länge** auf 20 und das Feld **Präsenz von Erweiterungen** auf 0x00000000 gesetzt werden] + [350 Byte für das Paketkörper]

Beispiel 2

Ein 1002 Byte langes Paket, das mit VHT PHY-Rate von 72,2 Mbit/s gesendet wird, wird gespeichert als:

[20 Byte für General Header, wo das Feld **Datenlänge** auf 1046 gesetzt wird] + [20 Byte für RF Header, wo das Feld **RF Header Länge** auf 24 und das Feld **Präsenz von Erweiterungen** auf 0x00000001 gesetzt werden] + [4 Byte für MCS Header] + [1002 Byte für das Paketkörper]

Format NCF

Dieses Format wird in CommView (jede Version) und CommView für WiFi Version 7.2 und älter verwendet. Neuere CommView for WiFi-Versionen (7.3 und neuer) verwenden das im entsprechenden Abschnitt oben beschriebene NCFX-Format.

Die Pakete werden nacheinander aufgenommen. Ein 24-Byte-Header, der unten beschrieben wird, geht jedem Paket voran. Alle Header-Felder, die länger als 1 Byte sind, verwenden sogenannte Little-endian-Bytefolgen.

Feldname	Länge (Bytes)	Beschreibung
Datenlänge	2	Die Länge des Paketkörpers nach dem Header
Ausgangslänge	2	Originallänge des Paketkörpers nach dem Header (ohne Kompression). Wenn keine Kompression benutzt wird, ist der Wert identisch mit dem aus dem vorherigen Feld.
Version	1	Paketformat Version (0 für die aktuelle Implementation)
Jahr	2	Paketdatum (Jahr)
Monat	1	Paketdatum (Monat)
Tag	1	Paketdatum (Tag)
Stunden	1	Paketdatum (Stunden)
Minuten	1	Paketdatum (Minuten)

<table>
<tr><td>Sekunden</td><td>1</td><td>Paketdatum (Sekunden)</td></tr>
<tr><td>Mikrosekunden</td><td>4</td><td>Paketdatum (Mikrosekunden)</td></tr>
<tr><td>Flags</td><td>1</td><td>Bitflags:<table>
<tr><td>Medium</td><td>0...3</td><td>Mediumtyp für das Paket (0 - Ethernet, 1 - WiFi, 2 - Token Ring)</td></tr>
<tr><td>Entschlüsselt</td><td>4</td><td>Das Paket wurde entschlüsselt (nur für Wi-Fi-Pakete anwendbar)</td></tr>
<tr><td>Beschädigt</td><td>5</td><td>Das Paket ist beschädigt, z.B. das Paket hat einen falschen CRC-Wert (nur für Wi-Fi-Pakete anwendbar)</td></tr>
<tr><td>Komprimiert</td><td>6</td><td>Das Paket wurde komprimiert abgespeichert</td></tr>
<tr><td>Reserviert</td><td>7</td><td>Reserviert</td></tr>
</table></td></tr>
<tr><td>Signal Level</td><td>1</td><td>Signal Level als Prozentsatz (nur für Wi-Fi-Pakete anwendbar)</td></tr>
<tr><td>Übertragungsrate</td><td>1</td><td>Datenübertragungsrate in Mbit/s mal 2 (nur für Wi-Fi-Pakete anwendbar)</td></tr>
<tr><td>Band</td><td>1</td><td>Transmissionsband. 0x01 für 802.11a, 0x02 für 802.11b, 0x04 für 802.11g, 0x08 für 802.11a-turbo, 0x10 für 802.11 SuperG, 0x20 für 4,9 GHz Public Safety, 0x40 für 5 GHz 802.11n/ac, 0x80 für 2,4 GHz 802.11n/ac (nur für WiFi-Pakete anwendbar).</td></tr>
<tr><td>Kanal</td><td>1</td><td>Kanalnummer (nur für Wi-Fi Pakete anwendbar)</td></tr>
<tr><td>Richtung</td><td>1</td><td>Für Nicht-WiFi-Pakete, Richtung. 0x00 bei Pass-through, 0x01 bei Inbound, 0x02 bei Outbound Für Wi-Fi-Pakete, das höherwertige Byte für das Feld PHY-Rate, wenn das Feld für die Ein-Byte-Rate den Wert nicht aufnehmen kann (d. h. der Wert ist höher als 255 ist).</td></tr>
<tr><td>Signal Level (dBm)</td><td>1</td><td>Signal Level in dBm (nur für Wi-Fi Pakete anwendbar)</td></tr>
</table>

Geräuschstärke (dBm)	1	Geräuschstärke in dBm (nur für Wi-Fi Pakete anwendbar)
Daten	Variabel	Paketkörper (unmodifiziert, so wie es über das Medium übertragen wurde). Wenn das Kompressionsflag gesetzt wurde, werden die Daten mittels der öffentlich zugänglichen Zlib 1.1.4 Library komprimiert. Die Länge dieses Feldes wird unter **Datenlänge** aufgezeichnet.

Die Headergesamtlänge ist 24 Byte.

Wenn Pakete komprimiert gespeichert werden enthält das Feld **Datenlänge** die Länge nach der Kompression, während die Ausgangslänge die Originallänge beschreibt. Ist ein Paket unkomprimiert, beinhalten beide Felder denselben Wert.

Wie kann man CommView for WiFi kaufen

Das Programm ist eine 30-Tage-Probeversion. Sie können eine vollfunktionierende, nicht eingeschränkte Version des Programms über unsere Webseite kaufen. Zwei Lizenztypen sind gegenwärtig für CommView for WiFi verfügbar: die Standardlizenz nd die VoIP-Lizenz. Die teuere VoIP-Lizenz erlaubt alle Applikationsfunktionen, inklusive des VoIP-Analysers, wogegen die Standardlizenz den VoIP-Analyser nicht freigibt.

Überprüfen Sie unsere **Webseite** für die Einzel-Anwender- und Mehrfachanwenderlizenpreise. Eine lizensierte Kopie von CommView for WiFi kann von einer Einzelperson, auf einem Computer persönlich genutzt werden. Eine zweite Kopie kann auf einem zusätzlichen mobilen Computer installiert werden. Schauen Sie bitte für detaillierte Beschreibungen unserer Lizenzrichtlinien in das Endanwenderlizenzabkommen, welches während der Installation eingeblendet wird.

Als registrierter Benutzer erhalten Sie:

- Eine vollfunktionale, unbeschränkte Ausgabe der Software
- Kostenlose Updates innerhalb eines Jahres nach Kaufdatum
- Informationen über Updates und neue Produkte
- Kostenlosen technischen Support

Wir akzeptieren Bestellungen über Kreditkarte, telefonische und Faxbestellungen, Schecks und Überweisung. Preise, Definitionen und Konditionen können sich ändern, überprüfen Sie daher unsere Webseite auf die neuesten Produktangebote und Preise.

https://www.tamos.com/order