
# WIRE**SHARK** Newsletter Juli 2014

Dieser Wireshark Newsletter von Leutert NetServices informiert Sie regelmässig in Kürze über wichtige Neuerungen im Zusammenhang mit dem führenden Open Source Analyser Wireshark und weiteren sinnvollen Netzwerkanalyse-Produkten.

## Schlagzeilen:

- Neuerungen in Wireshark ab Version 1.10.0
- Gigabit Ethernet zu USB 3.0 Adapter als Capture Interface
- Datenabgriff & Analyse an einem VLAN Trunk
- WLAN 802.11ac Analyse mit AirPcap Nx
- Cisco Nexus 1000V Virtual Switch mit Ethanalyzer
- Hinweise: Wireshark Kurse und Präsentationen

## Neue Features der Wireshark Versionen 1.10.0 bis 1.10.8

Die Versionen 1.10.0 bis 1.10.8 enthalten zahlreiche Protokollerweiterungen und Bug Fixes jedoch nur wenige Funktionserweiterungen.
Ab Version 1.10.6 ist jedoch neu die IPv4 Checksum Verification per Default ausgeschaltet. Die Checksum Verification von UDP und TCP ist ja bereits seit Version 1.2 per Default ausgeschaltet. Die meisten neuen Ethernet Adapter haben die Funktion Checksum Offloading aktiviert; d.h. die Berechnung der Feld- und Frame Checksum wird vom Adapter erst kurz vor dem Aussenden eines Frames berechnet und eingetragen. Dies führte zu zahlreichen Checksum-Error Falschmeldungen von Wireshark, wenn die Daten auf dem sendenden Gerät aufgezeichnet werden.

Unser Newsletter Archiv finden sie unter: http://www.wireshark.ch/de/wireshark-infos/newsletter

## Gigabit Ethernet zu USB 3.0 Adapter als Capture Interface

Bereits seit Version 1.8 unterstützt Wireshark das Aufzeichnen von Daten von mehreren Interfaces gleichzeitig. Dadurch stieg die Nachfrage nach einem zweiten Ethernet Interface für Notebooks, da diese normalerweise nur einen Anschluss (oder sogar nur noch WLAN) anbieten.

Wir suchten nach einem Produkt, welches folgende Anforderungen unterstützt:

- 10/100/1000 Ethernet
- USB 3.0
- VLAN 802.1q Tagging
- Wireshark WinPcap kompatibel
- Unterstützung mehrerer Betriebssysteme
- In der Schweiz lieferbar

Wir haben uns für folgendes Produkt entschieden und entsprechende Test durchgeführt:

## StarTech.com USB31000SW USB 3.0 zu Gigabit Ethernet NIC Network Adapter

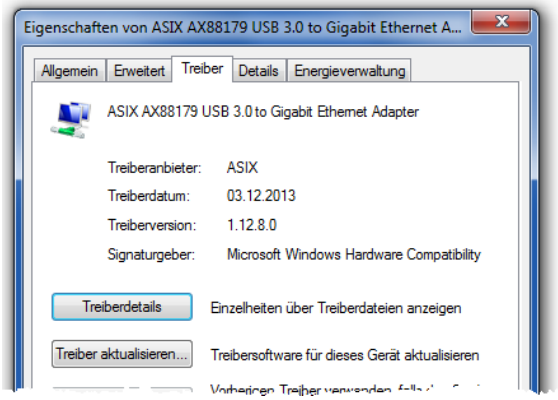

*Gigabit Ethernet zu USB 3.0 Adapter*

Dieser Adapter erfüllt die obigen Kriterien. Er ist über Amazon in verschiedenen Ländern lieferbar und unterstützt die Betriebssysteme Windows 7 (32/64), 8.1 (32/64), Mac OS® 10.6 - 10.9 und Linux Kernel 2.6.25 - 3.5.0.

Für Ästheten ist der Adapter sogar in den Farben Schwarz oder Weiss erhältlich 😊.
Folgende Tests haben wir mit diesem Adapter durchgeführt:

- VLAN Tag Unterstützung
- Performance Messung
- Windows und MAC OS Unterstützung

## Adapter Installation und empfohlene Einstellungen




*Aktueller Driver*

Der Adapter basiert auf einem Chipsatz von ASIX.

Auf der beigelegten CD befindet sich unter Umständen nicht der aktuellste Driver, unter Windows wurde mit „Treiber aktualisieren“ automatisch der neuste Driver gefunden und installiert. Bei einem älteren Driver wurden die VLAN Tags in den Ethernet Frames entfernt und entsprechend im Wireshark nicht angezeigt.

Ein zweiter Ethernet Adapter im Notebook kann auf verschiedene Arten sinnvoll verwendet werden.

1. Zur gleichzeitigen Aufzeichnung von Daten an verschiedenen Messpunkten, z.B. vor und nach einem Router, Firewall usw. Wireshark speichert die Daten von diesen Messpunkten im selben Trace File und markiert die Frames mit einer Interface ID. Diese kann in einer zusätzlichen Kolonne angezeigt werden. Zudem müssen die Frames nach ihrem absoluten Zeittstempel sortiert werden.
Details über die Installation und die notwendigen Einstellungen finden Sie in unserem Newsletter vom September 2012.

2. Zur Aufzeichnung von Daten nur über den zweiten Adapter. Dies hat den Vorteil, dass der Notebook gleichzeitig über den ersten Adapter weiterhin mit dem Netzwerk verbunden sein kann und damit z.B. die DNS Namensauflösungen von Wireshark weiterhin funktionieren.

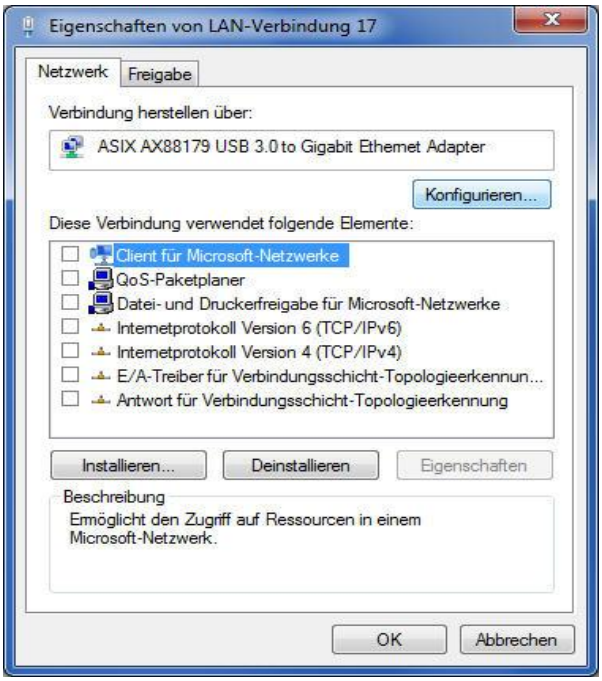

## Verhindern von eigenen Frames

Beim Aufzeichnen von Daten mit Wireshark ist es oft unerwünscht, dass Pakete vom eigenen Notebook ausgesendet und mit aufgezeichnet werden. Bei Messungen an einem Trunk sollte dies sogar gezielt verhindert werden, da die eigenen Pakete ohne Tag ausgeschickt werden und damit vom nächsten Switch ins sogenannte „Native VLAN" weitergeleitet werden.

Manche Switches nehmen an einem „Monitor Port" deshalb keine eingehenden Frames entgegen, trotzdem sind diese eigenen Pakete dann im Trace File vorhanden und müssen ausgefiltert werden.

Eine zuverlässige Methode das Aussenden eigener Pakete zu verhindern, ist das Ausschalten aller Optionen unter den Einstellungen des zum Aufzeichnen gewählten Adapters.

Wireshark benötigt für das Aufzeichnen von Daten keine dieser Optionen, solange keine aktive Namensauflösung von Wireshark über DNS gewünscht ist.
Ist der Notebook, auf welchem Wireshark läuft, gleichzeitig über ein weiteres Interface mit dem Netz verbunden und konfiguriert, wird von Wireshark automatisch diese Verbindung für die Namensauflösungen verwendet.




*Einstellung für einen reinen Capture Adapter*

# Datenabgriff & Analyse an einem VLAN Trunk

Die Bezeichnung Trunk steht hier für die physische Verbindung zwischen zwei Switches, bestehend aus einem einzigen physischen Link (Kupfer oder Glas). Die Ethernet Frames sind mit zusätzlichen 4 Bytes, dem 802.1q VLAN Tag versehen. (Einige Hersteller verwenden die Bezeichnung Trunk beim Bündeln mehrerer physischer Verbindungen in eine logische).

Zum Abgreifen der Daten eines Trunks stehen verschiedene Methoden zur Verfügung:

1. Konfigurieren eines Monitor Ports, welcher die Daten eines Trunks spiegelt.

   Vorteile:
   - Kein Unterbruch der Trunk Verbindung notwendig
   - Trunk Port kann Kupfer oder Glasmedium sein

   Nachteile:
   - Setzt Zugriffsrechte auf dem Switch voraus (nicht immer gegeben)
   - Einige Switches entfernen den VLAN Tag beim Kopieren auf den Monitor Port


2. Einfügen eines Taps oder Switches in die Trunk Verbindung

Vorteile:
- Keine Zugriffsrechte auf Netzwerkkomponenten notwendig
- Trunk Port kann Kupfer oder Glasmedium sein
- Keine zusätzliche Belastung des Switches

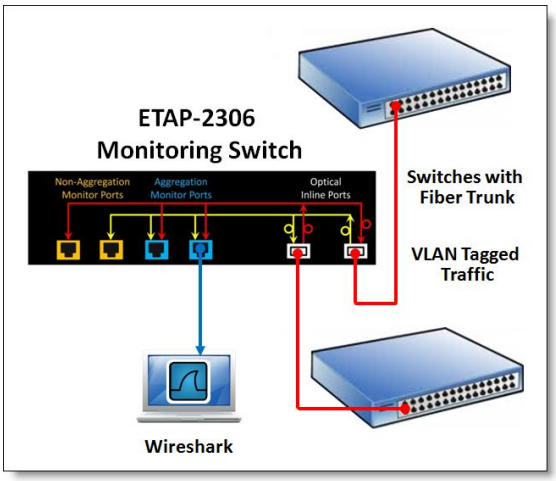
Nachteile:
- Unterbruch beim Einfügen des Taps oder Switches

Es existieren zwei Arten von Monitoring Ports: Aggregating und Non-Aggregating.

Aggregating Ports kopieren Sende- **und** Empfangsrichtung auf den einen Port. Dieser kann überlastet werden, da jede Richtung bis 1 Gigabit/sec übertragen kann, also total 2 Gigabit/sec.
Non-Aggregating Switches bieten je einen Port für jede Richtung (Tx und Rx).

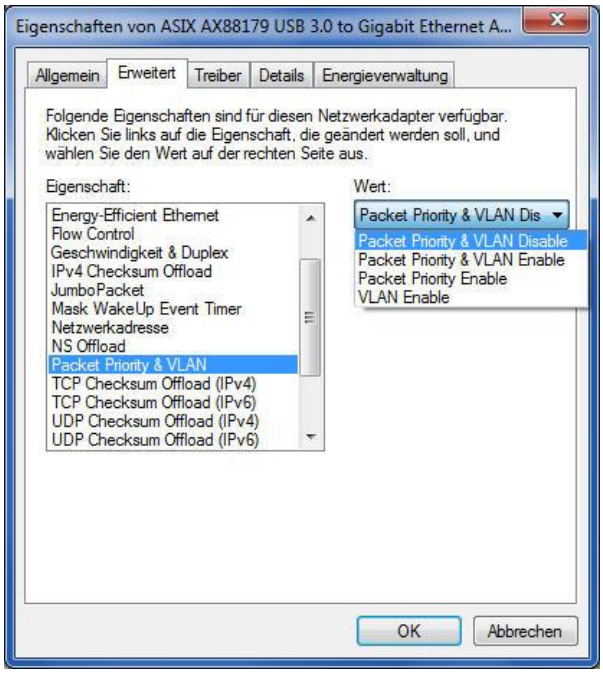
Unser Monitoring Switch ETAP-2306 unterstützt beide Port-Typen und Trunks mit Kupfer oder Glas.

Mehr Informationen auf unserer Webseite.




*Trunk Abgriff mit Monitoring Switch*

## Aufzeichnen der VLAN Tags mit dem Ethernet-USB Adapter




*Ausschalten der Priority & VLAN Option*

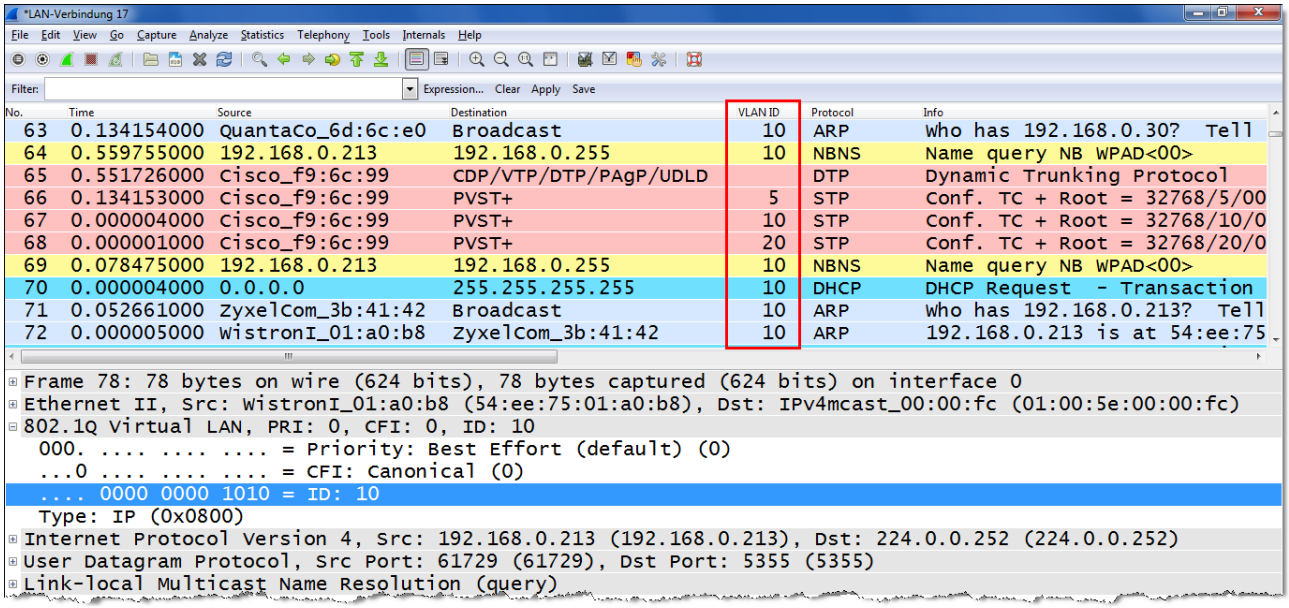
Damit die VLAN Tags vom Ethernet Adapter an Wireshark weitergeleitet werden, muss die Option „Packet Priority & VLAN“ ausgeschaltet werden.

Ist diese Option eingeschaltet, werden die VLAN Tags vom Adapter interpretiert und entfernt, sie sind damit im Wireshark nicht sichtbar.


## Darstellen der VLAN Tags

Die aufgezeichneten VLAN Tags sind im Packet Detail Fenster zu sehen und können als spezielle Kolonne dargestellt werden → rechte Maus auf der VLAN ID → Apply as Column

Frames ohne VLAN Tags gehören zum Native VLAN




*VLAN Tags als Kolonne (oben) und im Packet Details Fenster (unten)*

## Performance Messungen des StarTech Ethernet-USB Adapters

Die Leistungsfähigkeit des StarTech.com USB 3.0 zu Gigabit Ethernet Adapters wurde für die Verwendung als Wireshark Capture Interface rudimentär getestet. Dabei ging es nicht um detaillierte und aufwändige Tests, sondern um eine grobe Beurteilung, ob sich der StarTech Adapter als Capture Interface für Wireshark eignet.

Unter Verwendung von Iperf wurde ein Gigabit Ethernet Link in eine Richtung zu 100% mit Frames voller Länge (1518 Bytes) ausgelastet und mit Wireshark über den StarTech Adapter aufgezeichnet. Der limitierende Faktor bei der Aufzeichnung liegt in der Praxis sowieso nicht beim Ethernet Adapter, sondern bei der Schreibgeschwindigkeit des Speichermediums (Harddisk). Für die Aufzeichnung wurde deshalb ein leistungsfähiger Notebook (Lenovo ThinkPad T540p) mit SSD verwendet:

Mit dem StarTech Adapter konnte der volle Gigabit Link ohne Frameverlust aufgezeichnet werden.

## Unterstützte Betriebssysteme des StarTech Ethernet-USB Adapters

Gemäss StarTech Datenblatt werden folgende Betriebssysteme unterstützt: Windows 7 (32/64), 8.1 (32/64), Mac OS® 10.6 - 10.9 und Linux Kernel 2.6.25 - 3.5.0.

Getestet wurde der Adapter unter Windows 7 (64 Bit) und MAC OS X 10.9.4, dabei wurden keine Probleme festgestellt.

# WLAN 802.11ac Analyse mit AirPcap Nx

Der neue WLAN 802.11ac Standard erweitert den Durchsatz gegenüber dem 802.11n Standard noch einmal markant. Der n-Standard erreicht mit 2 Channels und 4 Spacial Streams bis 600 Mbit/s.

Der ac-Standard wird in Phasen, sogenannten Waves, in Produkten implementiert werden. Zurzeit sind die ersten Access Points nach Wave 1 mit 2 oder 3 Streams verfügbar.

Für die Unterscheidung der verschiedenen Techniken hat sich folgende Kurzbezeichnung etabliert:

2 x 2 : 2

Anzahl Transmitter ↗ ↑ ↖ Anzahl Streams

Anzahl Receiver

| | | | |
|---|---|---|---|
| **IEEE 802.11n:** | Bonding bis zu 2 Channels und 4 Streams | < 600 Mbit/s | 2x2:4 |
| **ac Wave 1:** | Bonding bis zu 4 Channels und 2 Streams | < 867Mbit/s | 2x2:2 |
| **ac Wave 1:** | Bonding bis zu 4 Channels und 3 Streams | <1'300 Mbit/s | 4x4:3 |
| **ac Wave 1:** | Bonding bis zu 4 Channels und 8 Streams | <3'470 Mbit/s | 4x4:8 |
| **ac Wave 2:** | Bonding bis zu 8 Channels und 8 Streams | <6'930 Mbit/s | 8x8:8 |

Die angegebenen Mbit/s sind physikalische Bruttoraten, welche Bandbreite netto für den Benutzer nutzbar ist, hängt von vielen Faktoren ab und wird sich im Bereich 30-50% bewegen.

Wir haben Tests mit einem der ersten Enterprise Access Points, dem Cisco 3702, durchgeführt. Der AP unterstützt 4x4:3 mit einer maximalen Bruttorate von 1'300 Mbit/s.

Leider gibt es noch wenige Endgeräte, welche ac-WLAN Adapter eingebaut haben. Zur Verfügung stand ein Lenovo ThinkPad T540p mit dem Intel 7260 Dual Band Chipset, dieser erreicht mit 2x2:2 maximal 867 Mbit/s brutto.

Weitere Tests zeigten, wie weit der Wireshark AirPcap Nx Adapter im ac-Umfeld weiterhin verwendet werden kann.

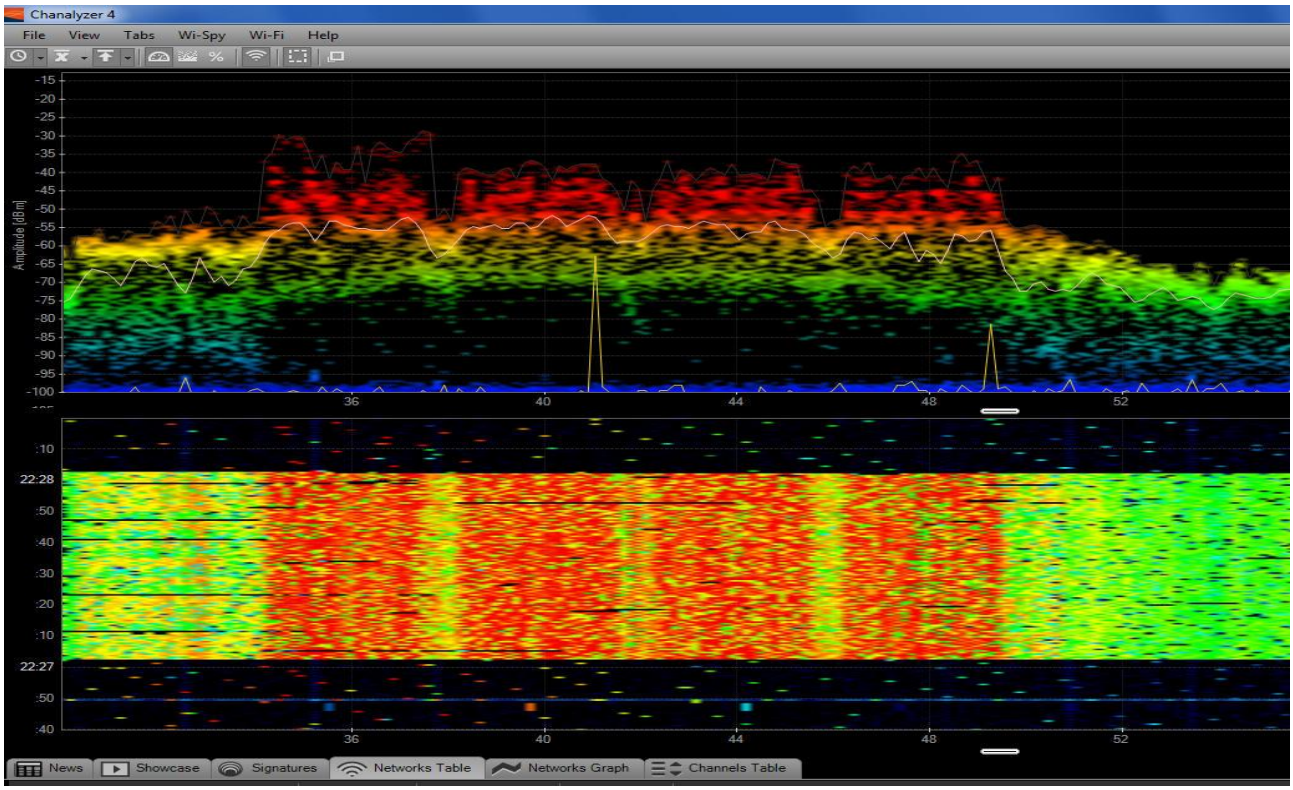
Cisco AP 802.11ac 4x4:3

Erste Messungen mit Iperf ergaben eine netto Bandbreite von bis zu **350 Mbit/s**, dies unter Verwendung von 4 Kanälen und 2 Streams. Dies entspricht rund 40% der physikalischen Bruttorate von 867 Mbit/s.

Diese Angabe dient als maximaler Wert, erreichbar nur in Laborumgebung und mit nur einem WLAN Client. In der Praxis wird dieser Wert geringer sein und zudem zwischen den anwesenden WLAN Clients noch aufgeteilt (shared Media).

→ Hinweis: Der 802.11ac Standard bietet je nach Land im 5GHz Band von 19 bis 24 non-overlapping Kanäle zu je 20MHz Bandbreite. Einige Produkte, welche den ac-Stempel tragen unterstützen jedoch nur die untersten 4 Kanäle 36, 40, 44 und 48. Grund liegt warscheinlich daran, dass die oberen Kanäle nur mit zusätzlich technischen Auflagen wie DFS und TPC benutzt werden dürfen.


Der 802.11ac Standard funkt(ioniert) ausschliesslich im 5GHz Band; es können bis zu 4 Kanäle zu je 20MHz Bandbreite gleichzeitig benutzt werden. Der Spektrumanalyser Wi-Spy DBx und die Software Chanalyzer zeigen die gleichzeitige Übertragung in den 4 Kanälen.




*Channel Bonding mit den Kanälen 36, 40, 44 und 48*

## Verwendung des AirPcap Nx Adapters im 802.11ac Umfeld?

Wireshark unter Windows kann die in den Notebooks eingebauten WLAN Adapter nicht nutzen. Diese unterstützen keinen promiscuous Mode und liefern auch die wichtigen WLAN Management- und Control-Frames nicht an Wireshark weiter.
Für die WLAN Analyse und Fehlersuche sind jedoch genau diese Frames ausschlaggebend, sie liefern detaillierte Informationen über die Kommunikation zwischen den WLAN Clients und dem Access Point.

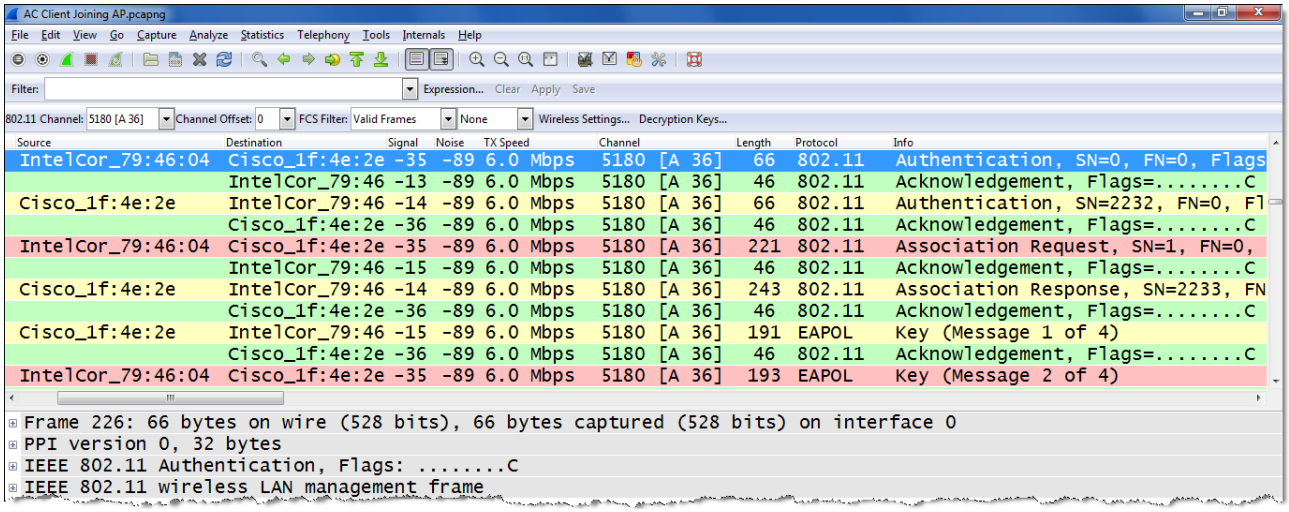

*AirPcap Nx analysiert 2.4 und 5 GHz*

Der AirPcap Nx unterstützt den 802.11n Standard. Zurzeit steht noch kein Adapter für 802.11ac zur Verfügung, und gemäss dem Hersteller www.riverbed.com ist auch noch kein Lieferdatum geplant.

Q: Wie weit kann der für 802.11n entwickelte AirPcap Nx für die ac-Analyse verwendet werden?

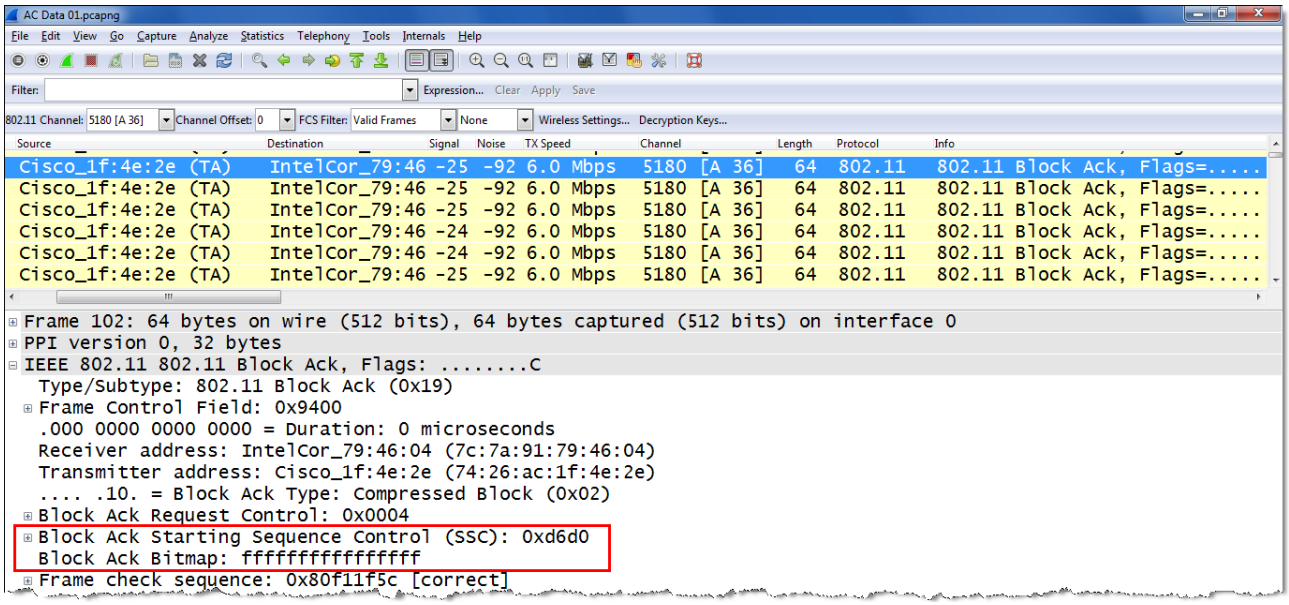
A: Weitgehend! Der ac-Standard verwendet dieselben Management- und Control-Frames wie der n-Standard. Diese Frames werden ausschliesslich im Basis-Kanal und in der n-Modulation gesendet und können mit dem Nx Adapter analysiert werden. Nicht aufgezeichnet werden lediglich die über 4 Kanäle verteilt gesendeten Daten-Frames.


Mit dem AirPcap Nx Adapter können auch im ac-Umfeld die Management- und Control-Frames aufgezeichnet werden. Diese werden weiterhin nur im Basis Kanal gesendet.




*Anmeldeprozess eines ac-Clients an einen ac-Access Point mit WPA Key Negotiation*

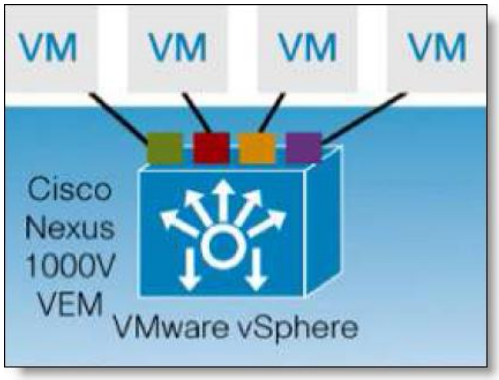
Die Daten-Frames werden im ac-Standard auf 4 Kanälen und mit der neuen ac-Modulation 256-QAM gesendet. Da der AirPcap Nx Adapter nur 2 Kanäle und 64-QAM Modulation unterstützt, sind diese bei der Aufzeichnung nicht sichtbar. Sichtbar hingegen sind weiterhin die im Basiskanal übertragenen Block Acknowledges. Durch die Analyse der Felder Starting Sequence Control und Block Ack Bitmap kann trotzdem die erfolgreiche Übertragung der Daten-Frames überprüft werden.




*Die Daten-Frames sind unsichtbar, sichtbar jedoch die entsprechenden Block Acks*

Mehr Details erfahren sie in unserem WLAN Analysekurs, welcher bereits den ac-Standard abdeckt.


## Cisco Nexus 1000V Virtual Switch mit Ethanalyzer




*Quelle: Cisco Systems*

Zahlreiche High-End Hardware Switches besitzen bereits eingebaute Aufzeichnungsmöglichkeiten, welche es erlauben Frames zu speichern und mit Wireshark zu analysieren.
Immer mehr besteht jedoch auch das Bedürfnis in virtualisierten Umgebungen Daten aufzeichnen zu können. Der virtuelle Switch Nexus 1000V von Cisco bietet mit dem Tool Ethanalyzer diese Möglichkeit.
Ethanalizer ist die Implementation des Command Line basierenden TShark in Cisco's NX-OS. Die TShark Files können mit Wireshark analysiert werden.

Mehr zu Ethanalyzer erfahren sie unter diesem Link.

Nexus1000V ist erhältlich für die Virtualisierungs-Plattformen VMware vSphere und Microsoft Hyper-V. Wir werden in zukünftigen Newslettern noch vermehrt auf das Thema Datenaufzeichnung im virtualisierten Umfeld eingehen. Vorschläge, Beiträge und Erfahrungen sind willkommen.

## Hinweise:

## Öffentliche Präsentationen und Wireshark Kurse

Gönnen Sie sich und Ihren Mitarbeiter etwas Sinnvolles und buchen Sie uns z.B. für eine eintägige Einführung zu IPv6, einem Update zu Wireshark oder dem Thema Ihrer Wahl aus den aufgeführten Kursen. Wir garantieren Ihnen einen lehrreichen Anlass.

## Wireshark Einführungen und Kurse

Gerne offerieren wir Ihnen zu den aufgeführten Themen firmeninterne Kurse oder Tech-Sessions nach ihren Wünschen (mit oder ohne Lab-Sessions):

- Netzwerkanalyse allgemein
- TCP/IP Netzwerkanalyse mit Wireshark
- WLAN Netzwerkanalyse mit Wireshark und AirPcap → Neu ergänzt mit 802.11ac
- VoIP Analyse mit Wireshark
- IPv6 Netzwerkanalyse mit Wireshark

Die komplette Liste aller öffentlichen Kurse auch in Österreich und Deutschland finden Sie auf unserer Webseite http://www.wireshark.ch/de/wireshark-kurse/oeffentliche-kurse

Es würde uns freuen, Sie in einem unserer Kurse begrüssen zu können.

Besten Dank für Ihr Interesse
Mit freundlichen Grüssen Rolf Leutert

LEUTERT NetServices
Phone +41 79 430 55 23
leutert@wireshark.ch
www.wireshark.ch
Postfach
CH-8058 Zürich-Flughafen