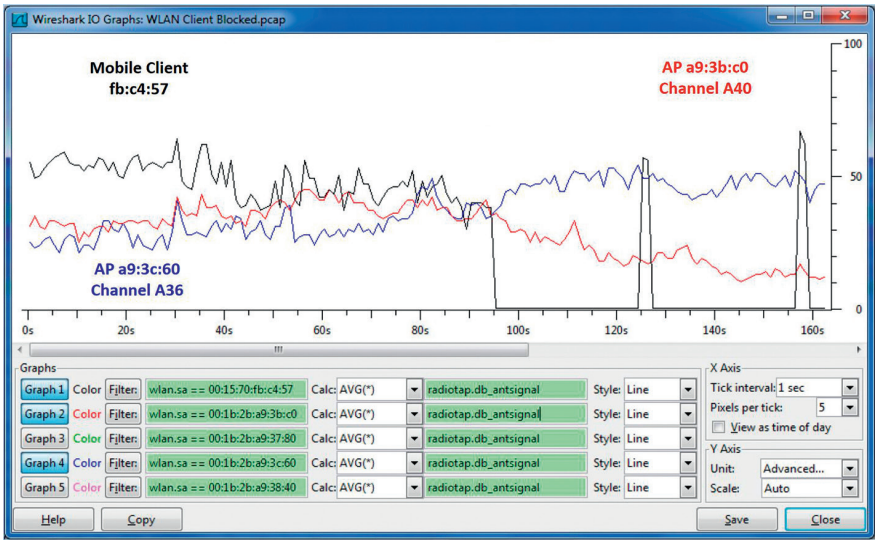
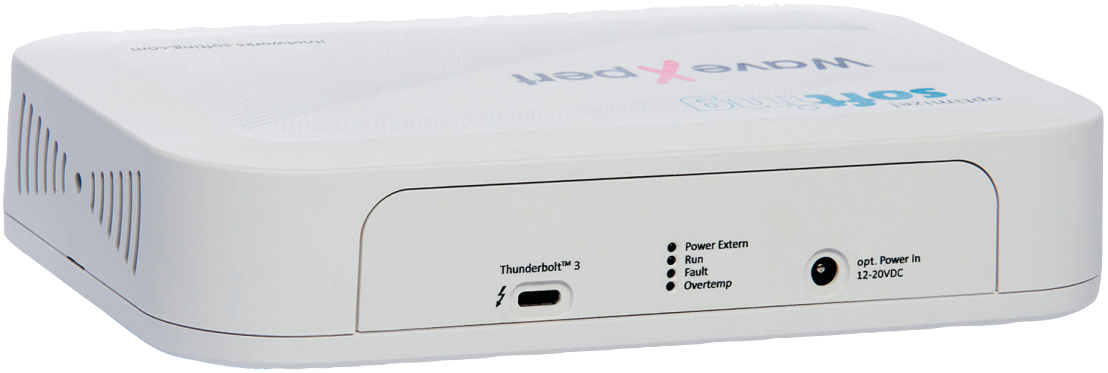
Sonderdruck aus
»de« 3.2020

das elektrohandwerk
Vorsprung ▪ Wissen ▪ Mehrwert

Fehler im WLAN erkennen und beheben





Fehler im WLAN erkennen und beheben

PROBLEME AUF DER DATENAUTOBAHN Beim Datenverkehr über WLAN ist es ähnlich wie auf einer Autobahn: Sind viele Autos unterwegs, erhöht sich die Wahrscheinlichkeit, dass Probleme auftreten. Anstelle von Fahrzeugen sprechen wir hier von der steigenden Anzahl der Geräte im Netzwerk, wie Laptops, Handys und Zeiterfassungssysteme. Somit wächst auch die Anfälligkeit für Fehler und Probleme. Schnell ist es passiert, dass Dienste wie Voice over WLAN, nicht mehr richtig funktionieren. Doch wie geht man der Ursache solcher Problematiken auf den Grund?

AUF EINEN BLICK

DIE ERFASSUNG UND ANALYSE aller übertragenen Daten ist die Voraussetzung für eine Identifizierung vorhandener Fehler in WLAN-Netzwerken

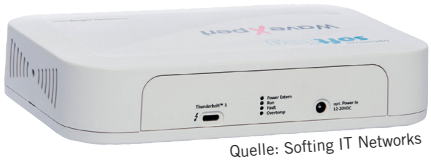
LANGZEITERFASSUNG UND LIVE-ÜBERWACHUNG sind zwei Möglichkeiten zur Datenanalyse mit der »Wireshark«-Software zur grafischen Aufbereitung von Datenprotokollen

Die Anforderungen, die ein WLAN-Netzwerk in einem Unternehmen erfüllen muss, werden mehr und komplexer. Denn das kabellose lokale Netzwerk ist längst zum Standard für modernes, flexibles Arbeiten geworden. Die Anzahl an Geräten im Firmennetzwerk nimmt stetig zu, damit verbunden wächst auch die Fehleranfälligkeit.

Da kann es schnell zu Problemen kommen: Applikationen arbeiten nicht mehr richtig oder ein Anruf über Voice over WLAN ist nicht möglich. Diese Szenarien sind IT-Spezialisten bestens bekannt. Um der Fehlerquelle auf den Grund zu gehen und die Problematik zu beheben, ist eine Möglichkeit die übertragenen Datenpakete zu analysieren. Doch davor müssten die Daten zunächst erfasst werden. Das ist zum einen über die Nutzung von USB-WLAN-Karten möglich. Und zum anderen mit einem WLAN-Sniffer, also einem Tool zur verlustfreien WLAN-Datenerfassung.

WLAN-Karten oder Sniffer?

Bei der Paketerfassung stellt sich natürlich auch die Frage: Benötige ich hierfür wirklich einen WLAN-Sniffer, oder ist hier die Erfassung über USB-WLAN-Karten bereits ausreichend? Aufgrund der heutigen Anforderungen an das Netzwerk ist eine Erfassung von mehreren Kanälen notwendig. Verwendet man hierbei nur USB-WLAN-Karten, kann schnell ein »Antennenwald« entstehen. Setzt man hingegen auf eine Hardware-Lösung, also z.B. auf einen WLAN-Sniffer wie den »Wavexpert« von Softing IT Networks, hat man nur ein handliches Gerät zur Datenerfassung, welches ebenfalls in der Lage ist, mehrere Kanäle gleichzeitig zu erfassen (**Bild 1**).



Quelle: Softing IT Networks

Bild 1: WLAN-Sniffer »Wavexpert« mit Stromversorgung über eine Thunderbolt-Schnittstelle

Ein weiterer Nachteil bei dem Einsatz von USB-WLAN-Karten – vor allem, wenn mehrere davon benötigt werden – liegt darin, dass nicht immer eine ausreichende Stromversorgung vorhanden ist. Bricht diese ab, hat das zur Folge, dass WLAN-Pakete nicht vollständig aufgezeichnet werden. Bei dem bereits erwähnten WLAN-Sniffer hingegen ist die ausreichende Stromversorgung über eine Thunderbolt-Schnittstelle garantiert.

Ein weiterer Vorteil dieser Schnittstelle ist, dass sie eine Datenübertragungsrate von bis zu 40 Gbit ermöglicht. Bei USB-WLAN-Karten hingegen erfolgt die Übertragung der Daten über einen USB-Port, welcher allerdings wie ein Flaschenhals funktioniert und möglicherweise für die Analyse relevante Daten verliert. Es zeigt sich also, dass der Einsatz eines WLAN-Sniffers durchaus sinnvoll ist.

Aktive oder passive Tools?

Im Bereich der WLAN-Sniffer wird unterschieden zwischen aktiven und passiven Tools. Aktive, zeichnen sich, wie der Name schon sagt, über ihre Aktivität aus. Sie senden Probe-Request-Pakete an die Access Points und diese senden Probe-Response-Pakete zurück. Man kann sich das ungefähr so vorstellen: Person A fragt, ob jemand da ist, und alle in Reichweite antworten mit »Ja«.

Passive WLAN-Sniffer hingegen arbeiten im Monitormodus. Sie senden keine Abfragen aus und benötigen auch keine Antwort. Sie erkennen und erfassen die Übertragungen von WLAN-Netzwerken in ihrer Umgebung. Zudem können sie auch aktive WLAN-Sniffer erkennen, andersherum aber nicht.

Nach der Theorie bewegen wir uns in das Feld. Denn hier lauern an der einen oder anderen Stelle Herausforderungen, bei denen ein WLAN-Sniffer unterstützen kann. Moderne WLAN-Netzwerke optimieren mit technischen Methoden wie Mehrfachverbindungen und Kanalbündelungen die Übertragungsgeschwindigkeiten, um heutige Anforderungen

zu erfüllen. Beide Methoden stellen WLAN-Sniffer vor eine Herausforderung.

Bei Mehrfachverbindungen (Multiple Input Multiple Output, kurz: MIMO) werden neben direkt eingehenden Funkwellen auch reflektierte Funkwellen eingesetzt, um die Übertragungsraten zu erhöhen. Möchte man beim eingesetzten Übertragungsverfahren MIMO-Daten aufzeichnen, müssen somit mehrere Streams erfasst werden.

Bei Kanalbündelung werden, wie der Name schon sagt, mehrere Kanäle zu einem breiten Kanal zusammengefasst. Somit wird eine Erhöhung des Datendurchsatzes im WLAN ermöglicht. Setzt man bei der Datenerfassung bei dieser Technologie auf eine WLAN-Karte, ist es notwendig, dass diese über mehrere Antennen verfügt, welches wiederum zu dem oben erwähnten Antennenwald führen kann.

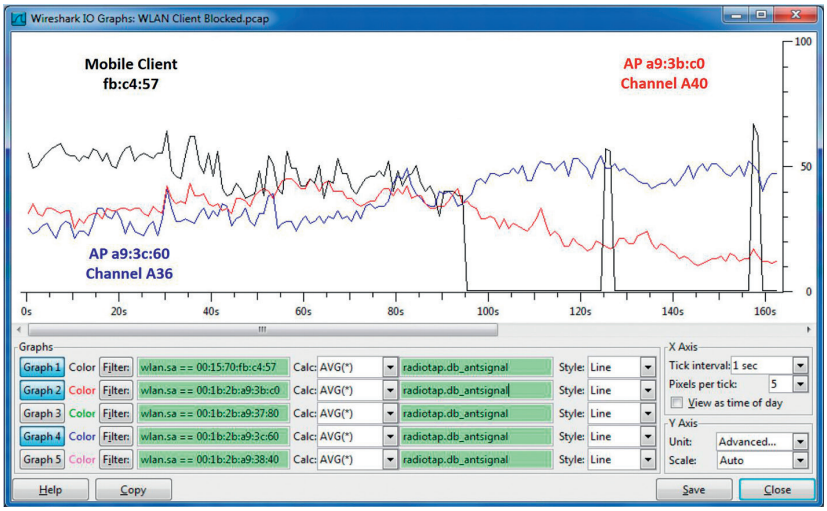
Eine weitere Herausforderung, liegt darin, wenn mehrere Kanäle gleichzeitig erfasst werden müssen. Der Fall tritt ein, wenn Roaming-Prozesse sichtbar gemacht werden sollen. Die Erfahrung von WLAN-Dienstleistern hat gezeigt, dass beim Roaming sehr häufig Fehler entstehen: Der Client verliert beispielweise die WLAN-Verbindung komplett, oder die Übergabe von einem Access Point zu einem neuen dauert zu lange.

Außerdem ist es aufgrund der Fülle an Geräten in WLAN-Netzwerken oftmals notwendig, mehrere Kanäle gleichzeitig zu erfassen. Hier sollte man darauf achten, dass der verwendete WLAN-Sniffer intern über mehrere WLAN-Karten sowie die entsprechende Anzahl von Antennen verfügt. Natürlich ist es auch möglich, mit mehreren Geräten die erfasste Anzahl der Kanäle zusätzlich zu erhöhen. Zudem können mit passiven WLAN-Sniffern nicht nur die Nutzdaten, sondern auch die Management- und Kontrollinformationen verlustfrei empfangen werden.

Das Detektivspiel beginnt

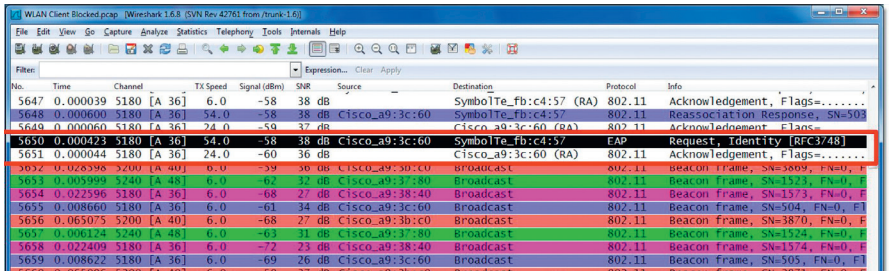
Sobald Probleme in den WLAN-Netzwerken auftreten, ist eine WLAN-Paketanalyse notwendig. Bevor diese jedoch durchgeführt werden kann, müssen Daten erfasst werden. Wenn beispielsweise die WLAN-Verbindung abbricht, sobald man sich mit dem Client (im nachfolgenden Beispiel ein Barcode-Scanner) bewegt, erfasst der WLAN-Sniffer alle übertragenen WLAN-Daten. Sie werden anschließend auf dem PC gespeichert.

Nun beginnt die eigentliche Analyse der Daten. In den meisten Fällen wird hier die kostenlose Software »Wireshark« eingesetzt. Hierzu gibt es zwei Analysemöglichkeiten: die Langzeiterfassung und die Live-Überwachung. Bei ersterer werden die Daten erfasst und zu einem späteren Zeitpunkt analysiert. Wird die Live-Überwachung zur Analyse genutzt, werden die Daten direkt in die Software gespielt und analysiert.



Quelle: Leutert Netservices

Bild 2: Der WLAN-Client war zu Beginn mit der MAC-Adresse »BSSID Cisco_a9:3b:c0« und zum Ende mit »BSSID Cisco_a9:3c:60« verbunden



Quelle: Leutert Netservices

Bild 3: ID-Abfrage des Access Points (»Request Identity«) und Empfangsbestätigung des Clients (»Acknowledgement«)

Beispiel aus der Praxis

Es wurden im Praxisbeispiel die erfassten Daten auf die MAC-Adresse des WLAN-Clients, des Barcode-Readers, gefiltert und betrachtet, mit welchem Access Point der WLAN-Client am Anfang und am Ende der Aufnahme verbunden war (**Bild 2**). Die Signalstärke der beiden Access Points und des Clients verdeutlichten in einem Graphen den Roaming-Vorgang vom Client. Im Anschluss wurden die zuletzt gesendeten Pakete zwischen WLAN-Client und Access Point betrachtet, wodurch Rückschlüsse auf die Fehlerursache gezogen werden konnten. In diesem Fall hatte sich der WLAN-Client am ersten Access Point wegen zu schwacher Signalstärke abgemeldet und bereits mit dem zweiten Access Point mit besserem Empfang verbunden. Der zweite Access Point fragte nach einer ID, worauf der Client nicht geantwortet hat und die Verbindung daher nach 30 sec. getrennt wurde.

Der Fehler wurde gefunden. Doch wo liegt nun die Schuld? Beim Access Point, beim Client oder lag eine Störung der WLAN-Verbindung vor? Der Access Point hat nach einer ID gefragt, sichtbar am Paket »Request Identity«, und somit seine Arbeit getan. Der Client hat den Empfang dieses Pakets fehlerfrei mit »Acknowledgement« bestätigt (**Bild 3**), weswegen der Access Point das Paket also nicht noch einmal senden musste. Eine Störung des WLANs lag auch nicht vor, da der Client die ID-Abfrage empfangen konnte und entsprechend, wie zuvor beschrieben, bestätigt hat. Das Problem lag daher beim Client. Denn er hätte dem Access Point mit der ID antworten müssen, was allerdings nicht geschehen ist. Die Ursache des Problems lag somit in einem Fehler in der Firmware. Nach Meldung des Problems an den Client-Hersteller wurde dieses mit einem Firmware-Update behoben. Nun ist es wieder möglich, störungsfrei Barcodes zu scannen.

AUTOR

Frank Neuhoff
Produktmanagement Wavexpert,
Softing IT Networks, Haar