



WLAN Analyse Webinar (Site Survey – Troubleshooting – Management)

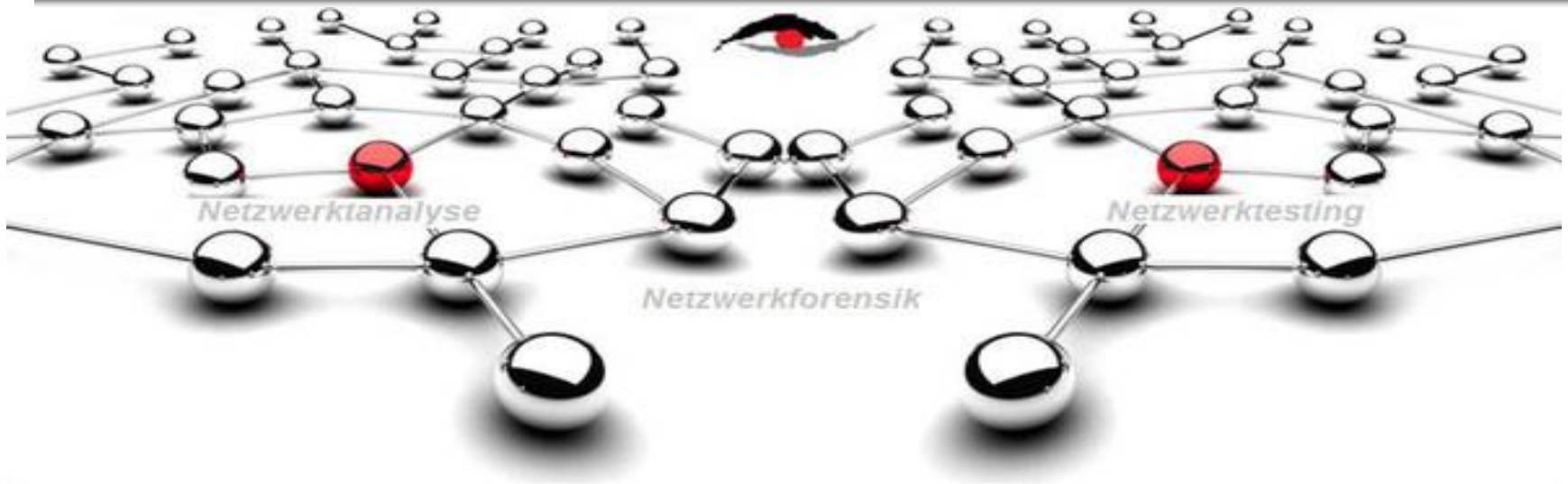


Patrick Petersson
CEO | CIO
HEXCOM UG

[Tel.: +49\(0\)89-35852970](tel:+49(0)89-35852970)
mail@hexcom.de

In Kooperation





Was können Sie von HEXCOM Events erwarten?

Überzeugung und Glaubwürdigkeit, wir bringen es auf den Punkt
Wir sind praxisnah und polarisierend, weil wir gegen Mainstream sind.
Wir bieten Nachhaltigkeit und Messbarkeit, weil wir lieben was wir tun.

Sie wollen mehr über die HEXCOM erfahren?
Dann besuchen Sie uns doch einfach unter www.hexcom.de





I.) Wireless Life Cycle

II.) Netzwerk Design

- >> Erwartungen an einen Netzwerk – Designer.
- >> Wireless Standards.
- >> Wireless Kanäle.
- >> 802.11n im Fokus.
- >> Arbeitsweise einer WLAN Planer Software (Ekahau).

III.) Bereitstellung und Verifikation

- >> Erste Schritte für die Bereitstellung eines Wireless Netzwerkes.
- >> Spektrumsanalyse.
- >> Arbeitsweise einer Wireless Site Survey Software (TamoGraph).

IV.) Troubleshooting und Management

- >> Wireless Troubleshooting und Management Möglichkeiten.
- >> Wofür Troubleshooting und Management Überhaupt.
- >> Arbeitsweise eines Wireless Netzwerk Analyzer (CommView WiFi).

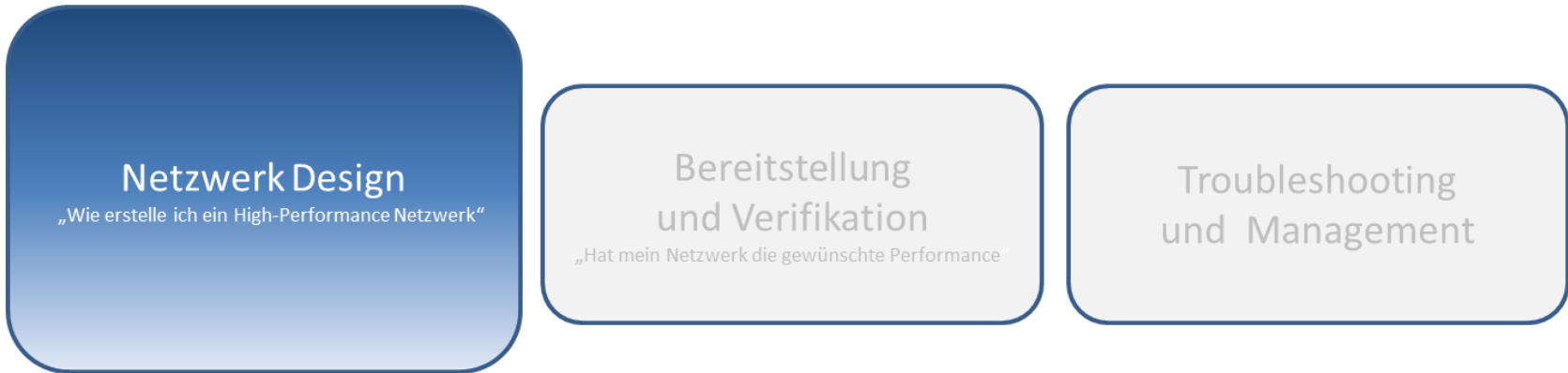
V.) Fragen und Antworten



Lebenslauf eines Wireless Netzwerkes

„Mit seinen wichtigsten Aufgaben“







Was ist von ein Wireless - Designer zu erwarten?

Die bestmögliche WLAN Leistung ist zu errechnen:

- >> Netzwerkleistung für eine Vielzahl von Anwendungen optimieren.
- >> Die Minimierung von Kanalüberlappungen und Kanalstörungen.
- >> Bestimmung der Menge, Typ und Ausrichtung von Access Points und Antennen.
- >> Sicherstellen der Sicherheitsrichtlinien und Sicherheitsvorkehrungen.

- # Überprüfung der Installation „Funktionalität“.
- # Vollständige Dokumentation des Netzwerkes.



Praxisbeispiel

Universitäts – Campus

10.000 User --> 265 Gebäude --> 6.000 Access Points 802.11n

- # Readyness für Multi-channel und IP-based video (IPTV) over wireless..
- # Erhöhtes Traffic aufkommen durch Social Media und File Sharing unter Studenten.
- # Hörsäle (10) müssen die Wireless - Kapazität von 600 Usern gleichzeitig besitzen.
- # Sicherheitsrichtlinien und Sicherheitsvorkehrung müssen ALLE erfüllt sein



Wireless Standards und Wireless Kanäle



802.11a

Datentransfer:

brutto 54 MBit/s (netto maximal 50 %).

Frequenzband:

5 GHz (seit 13. 11. 02 freigegeben - lizenzfrei).

Modulationsverfahren:

OFDM (Orthogonal Frequency Division Multiplexing).

Akzeptanz:

gering verbreitet.

802.11b

Datentransfer:

brutto 11 MBit/s (netto maximal 50 %).

Frequenzband:

2,400 bis 2,4835 GHz (lizenzfrei).

Modulationsverfahren:

DSSS (Direct Sequence Spread Spectrum).

Akzeptanz:

noch relativ weit verbreitet.

802.11g

Datentransfer:

brutto 54 MBit/s (netto maximal 40 %).

Frequenzband:

2,400 bis 2,4835 GHz (lizenzfrei).

Modulationsverfahren:

OFDM und DSSS.

Akzeptanz:

der am weitesten verbreitete Standard.

802.11n

Datentransfer:

brutto 600 MBit/s.

Frequenzband:

2,400 bis 2,4835 GHz (lizenzfrei), auch 5 GHz.

Modulationsverfahren:

MIMO Technologie.

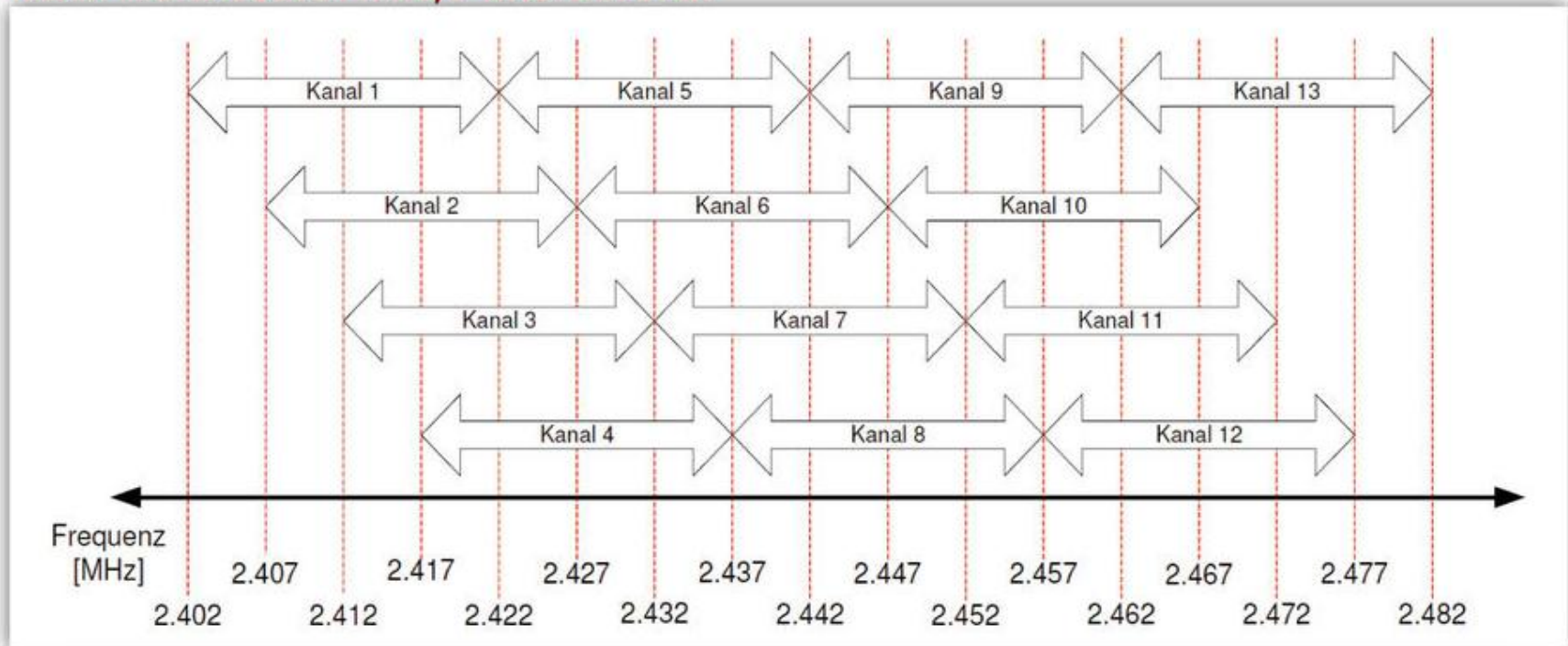
Akzeptanz:

noch gering verbreitet.

1999(802.11a) ->> 1999 (802.11b) ->> 2003 (802.11g) ->> 2009 (802.11n)



WLAN-Kanalraster im 2,4-GHz-Bereich



WLAN-Geräte nutzen im 2,4 GHz-Bereich die Kanäle 1 (2,412 GHz) bis 13 (2,472 GHz). Nachdem WLAN eine Bandbreite von ca. 20 bzw. 40 MHz nutzt, der Abstand zwischen benachbarten WLAN-Kanälen jedoch nur 5 MHz beträgt, überlappen sich benachbarte Kanäle. Bei einer Bandbreite von 20 MHz sind daher nur 4 (und nicht 13) Kanäle praktisch nutzbar, etwa die Kanäle 1, 5, 9 und 13. Bei einer Bandbreite von 40 MHz sind lediglich zwei Kanäle praktisch nutzbar (zB Mittenfrequenz bei Kanal 3 bzw. 11).



WLAN-Kanäle im 5-GHZ-Bereich



Typische WLAN-Geräte unterstützen die Kanäle 36 (5,18 GHz), 40 (5,20 GHz), 44 (5,22 GHz) und 48 (5,24 GHz), manche Geräte unterstützen darüber hinaus auch die Kanäle 100 (5,50) 104 (5,52) 108 (5,54), 112 (5,56), 116 (5,58), 120 (5,60), 124 (5,62), 128 (5,64), 132 (5,66), 136 (5,68) und 140 (5,70).



Vor- und Nachteile der einzelnen WLAN Kanäle

2,4-GHz-Vorteile

- >> Gebührenfreies freigegebenes ISM-Frequenzband.
- >> Keine aufwändigen Spektrum-Management-Funktionen wie TPC oder DFS nötig, um volle Ausschöpfungen zu ermöglichen.
- >> Hohe Verbreitung und geringe Gerätekosten.

2,4-GHz-Nachteile

- >> Frequenzband muss mit anderen Funktechniken geteilt werden. (Bluetooth, Mikrowellenherde, Babyphones, etc.).
- >> Störungsfreier Betrieb von nur maximal 3 Netzwerken am selben Ort möglich, da effektiv nur 3 brauchbare (kaum Überlappende) Kanäle zur Verfügung stehen (in Deutschland: Kanäle 1, 7 und 13).

5-GHz-Vorteile

- >> weniger genutztes Frequenzband „störungsärmerer Betrieb“ in Deutschland insgesamt 19 nicht überlappende Kanäle vorhanden.
- >> höhere Reichweite, da in Zusammenhang mit 802.11h bis zu 1000 mW Sendeleistung möglich ist.

5-GHz-Nachteile

- >> Starke Regulierungen in Europa: auf den meisten Kanälen ist DFS nötig; auf einigen Kanälen kein Betrieb im Freien erlaubt; falls kein TPC benutzt wird, muss die Sendeleistung reduziert sein.
- >> Ad-hoc-Modus wird von den meisten Geräten nicht unterstützt.
- >> Geringere Verbreitung, daher wenig verfügbare Geräte auf dem Markt.



802.11n Performance im Fokus



MIMO (Multiple Input Multiple Output)

„Systeme mit mehreren Eingangs- und Ausgangsgrößen“

Unterscheidung in technischen Kategorien:

Systeme, die über genau eine Eingangs- und eine Ausgangsgröße bzw. -variable verfügen, werden als **SISO**-System (Single Input Single Output) bezeichnet.

Verfügt ein System über mehrere Eingangs- und Ausgangsgrößen, spricht man von einem **MIMO**-System.

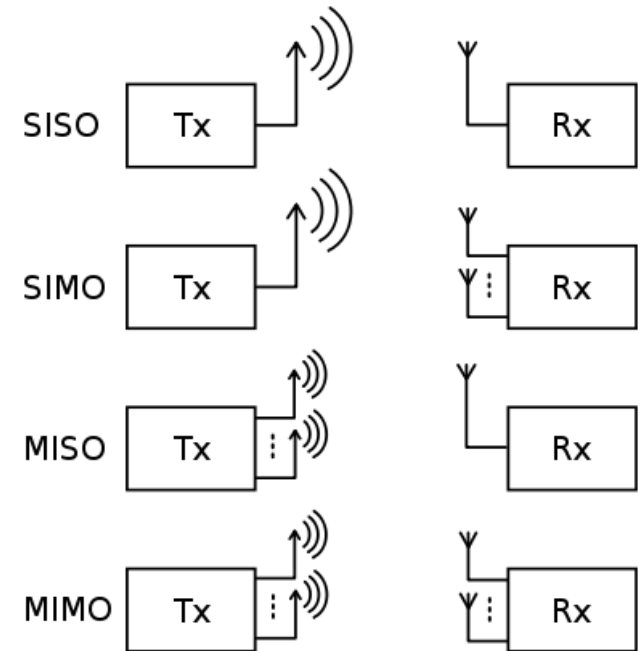
Analog werden auch die Begriffe **SIMO** (Single Input Multiple Output) und **MISO** (Multiple Input Single Output) verwendet.

Berechnung der Kanalkapazität

$$C_a \approx \min \{n_T, n_R\} \log_2(1 + \rho)$$

Berechnung für die Erhöhung der Kanalkapazität

$$C = \log_2 \left[\det \left(\mathbf{I}_{n_R} + \frac{\rho}{n_T} \mathbf{H} \mathbf{H}^H \right) \right]$$





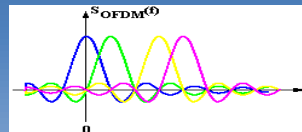
Channel Bonding

„Belegung der doppelten Bandbreite“

In Kürze:

>> Benutzung der doppelten Bandbreite statt 20MHz 40MHz
 (Übertragung doppelter OFDM Träger (Orthogonal Frequency-Division Multiplexing))

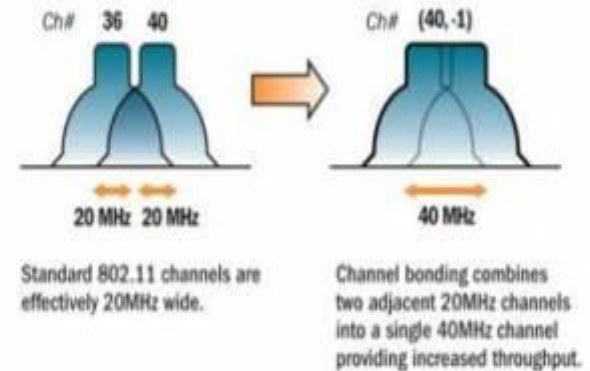
Die zu übertragende Nutzinformation mit hoher Datenrate wird auf mehrere Teildatenströme mit niedriger Datenrate aufgeteilt (Möglich in 2,4 Ghz Bereich oder im 5Ghz Bereich)



Berechnung der OFDM-Signale
 (nach diskreten Fouriertransformationen (IDFT))

$$f_v = \frac{v}{T}, \quad f_w = \frac{w}{T}, \quad w, v \in \mathbb{N}$$

$$\frac{1}{T} \int_0^T e^{j2\pi f_v t} e^{-j2\pi f_w t} dt = \begin{cases} 1, & \text{wenn } v = w \\ 0 & \text{sonst} \end{cases}$$





802.11n Frame Aggregation

„Erlaubt WLAN deutlich längere Frames (2304 statt 1518 Byte)“

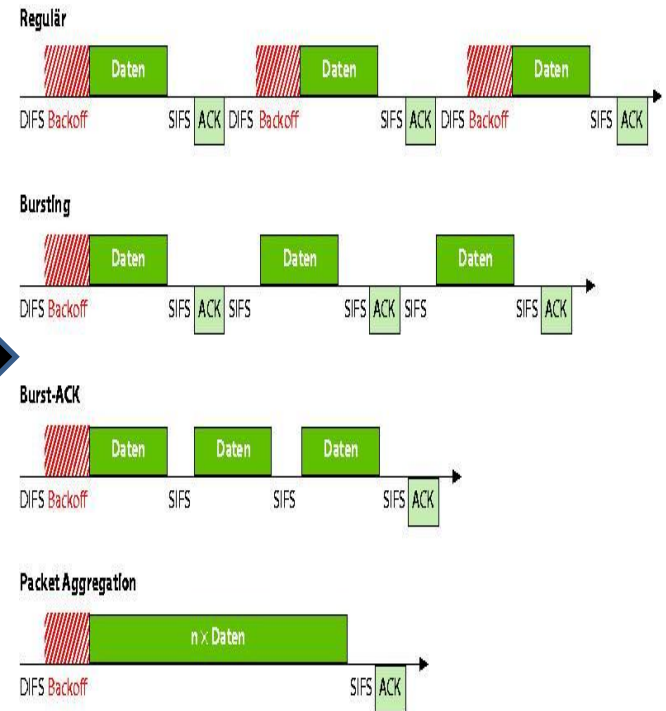
Unterscheidung zwischen

MSDU Aggregation „Packet Aggregation“

- >> Single MAC Frame, multiple PDU (Protocol Data Units).
- >> Bearbeitung in der MAC-Schicht, Umwandlung zu einem einzigen Header.
- >> Entschlüsselung (Decodierung) ist nicht individuell durch Empfänger möglich.

MPDU Aggregation „Block Aggregation“

- >> Multiple MAC Frame.
- >> Bearbeitung in der MAC-Schicht, Umwandlung in mehrere kleinen Headern.
- >> Entschlüsselung (Decodierung) ist individuell je nach „Block“ möglich.



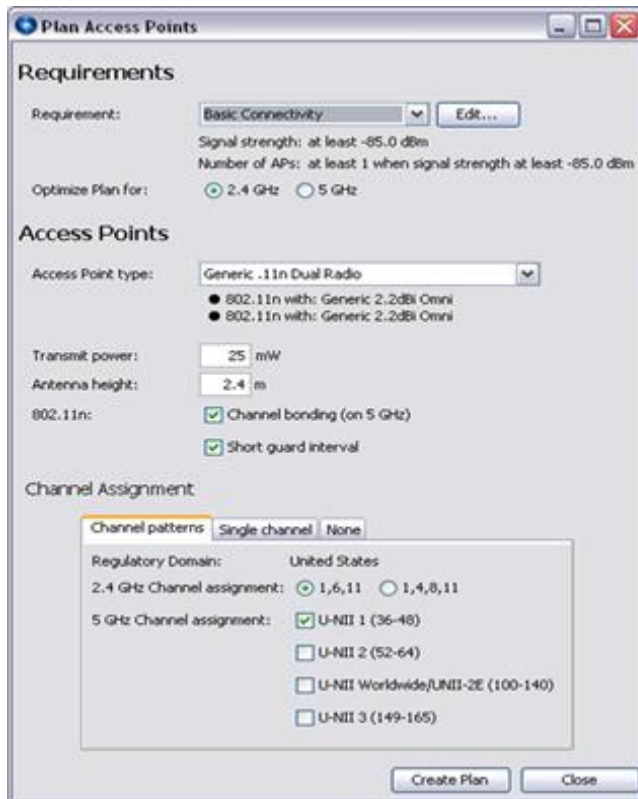


Wie arbeitet eine WLAN Planungssoftware? Beispiel Ekahau



Mittels automatischer Netzwerkplanung...

Automatisches finden der optimalen Anzahl der APs,
sowie automatische Konfiguration anhand der vorgegebenen Voraussetzungen.



Auswahl der Anforderung wie z.B. VOIP

Auswahl der APs mit Ihrem Parameter



Auswahl der Fläche



...mittels manueller Netzwerkplanung!

Example Project Pro.exe - Ekahau Site Survey

File Edit View Site Device Help

Access Points Surveys Building

Showing: 12/12

Quick Select Actions

Not placed on any Map (1/1)

Floor 1 (2/2)

My Cisco AP1250 (1)

n 6 2.4 m 0° Edit...

n 40 2.4 m 0° Edit...

Floor 1

My Nortel AP-2332 (1)

a 40 2.4 m 0° Edit...

g 1 2.4 m 0° Edit...

Floor 1

Floor 2 (1/1)

My Aruba AP-125 (1)

n 11 2.4 m 0° Edit...

n 52 2.4 m 0° Edit...

Floor 2

Floor 9-Survey (5/5)

Show Signal Strength for My Access Points

Options

Custom

Aruba AP-70

Bandspeed AM3100AG

Belair 100

Bluesocket 1500/1540

Bluesocket 1700

Bluesocket 1800

Cisco AP 1000

Cisco AP 1100/1121

Generic 2.2dBi Omni

Planning Survey

Floor 1

-80.0dBm -20.0dBm





Wireless Site Survey

„Der erste Schritt für die Bereitstellung eines drahtlosen Netzes.“

Messung von Störquellen

Begehung

- > Einlesen von Gebäudeplänen (Skalieren von Plänen, Ausrichtung der einzelnen Räume).
- > Einstellungen für die Vermessungen sind zu beachten (Messadapter, Frequenzbänder, Scanzeiten auswählen).

Visualisierung

- > Feldstärke, Interferenzen, Round Trip Zeiten und weitere...

Optimierung

- > Einplanung zusätzlicher Kanäle, APs. oder Änderungen von Einstellungen

Dokumentierung

Bereitstellung und Verifikation

„Hat mein Netzwerk die gewünschte Performance“

Überprüfung der Leistungsfähigkeit.

Überprüfung der Flächenabdeckung.

(Unter Berücksichtigung höchstmöglicher Sicherheit .)

- >> Kontrolle von Einstellungen u. Ausrichtungen der APs.
- >> Durchführung von Lasttests und Sicherheitstests.
- >> Dokumentation, Übergabe und Wartung des Netzes.

Planung zusätzlicher Kapazitäten!



Netzwerk Design

„Wie erstelle ich ein High-Performance Netzwerk“

Bereitstellung
und Verifikation

„Hat mein Netzwerk die gewünschte
Performance“

Troubleshooting
und Management

Spektrumsanalyse



Messung von Störquellen

Findung von Störsignalen im Bereich 2,4 GHz und 5 GHz.

Identifizierung der Art der Störer.

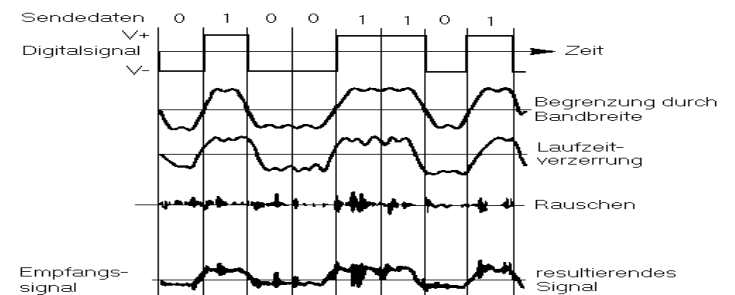
- > Bluetooth
- > Telefone
- > Mikrowellen
- > Audio.- und Videoüberträger

Standortlokalisierung der Störquellen.

Analyse über einen längeren Zeitraum.

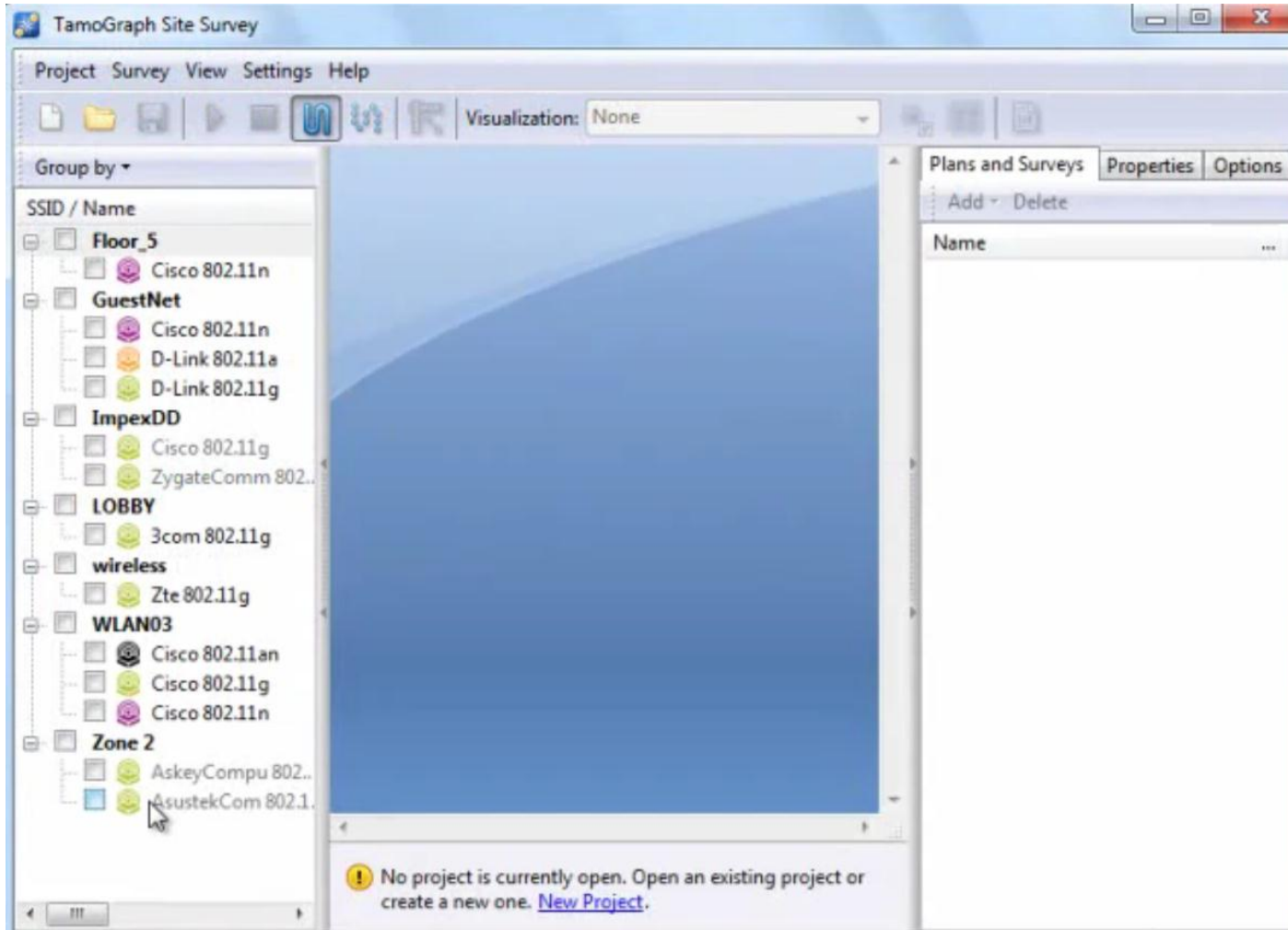
- > Findung von zeitlich intermittierenden Störquellen .

Einfache Dokumentation für die Bereitstellung des Netzes .





Wireless Site Survey mit TamoGraph





TamoGraph Site Survey

Project Survey View Settings Help

Visualization: None

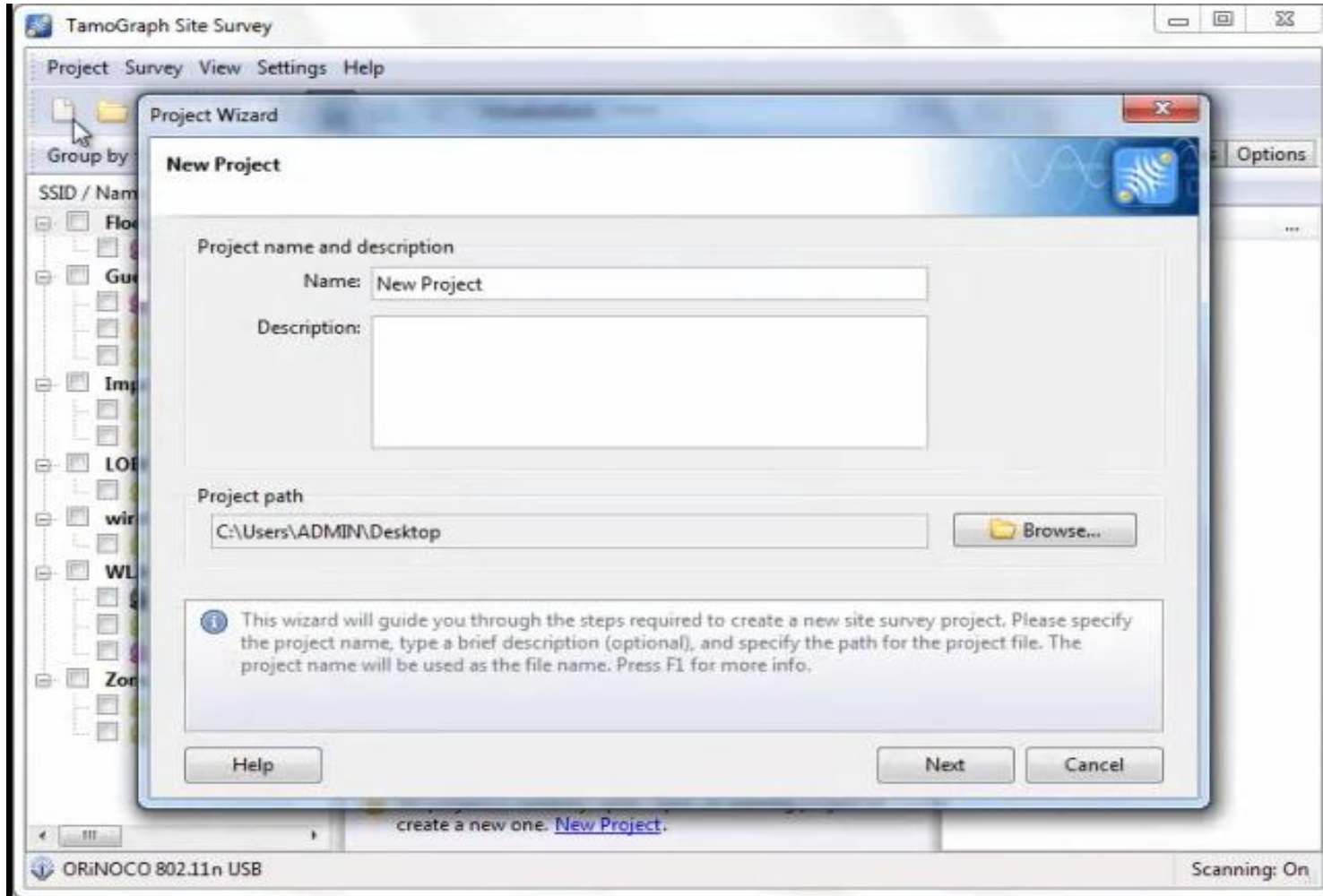
Group by ▾

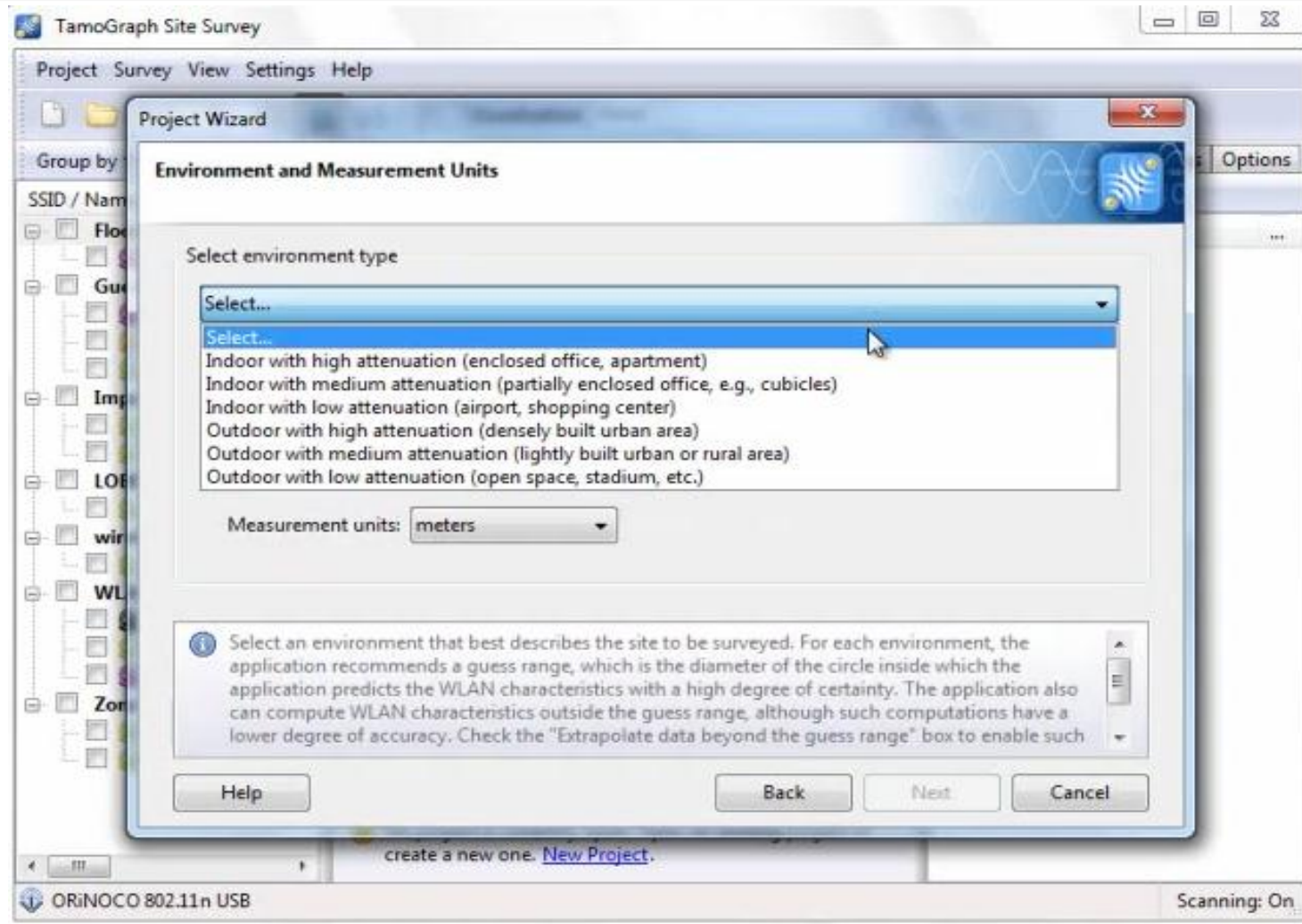
SSID / Name	Ch	Band	Signal	Encryption	Max ...	Spati...	MAC Address
Floor_5							
Cisco 802.11n	1	802.11n	-80	WPA-CCMP,...	300.0	2	00:23:04:03:FE:7E
GuestNet							
Cisco 802.11n	2 (6)	802.11n	-68	WEP	270.0	2	00:23:04:1B:81:01
D-Link 802.11a	36	802.11a	-37	WPA-TKIP	54.0	1	00:0F:3D:E9:05:01
D-Link 802.11g	11	802.11g	-27	WEP	54.0	1	00:0F:3D:E9:05:01
ImpexDD							
Cisco 802.11g	11	802.11g	N/A	WPA-CCMP	54.0	1	00:22:90:78:0D:CD
ZygateComm 802....	8	802.11g	N/A	WPA-TKIP	54.0	1	00:02:CF:AE:80:4F
LOBBY							
3com 802.11g	11	802.11g	-84	WEP	54.0	1	00:1A:C1:36:B5:15
wireless							
Zte 802.11g	8	802.11g	-47	WPA-CCMP	54.0	1	00:22:93:1F:E7:64
WLAN03							
Cisco 802.11an	161 (157)	802.11an	-65	None	300.0	2	00:23:04:79:5B:31
Cisco 802.11g	6	802.11g	-78	WPA-TKIP	54.0	1	00:22:90:49:F2:7F
Cisco 802.11n	2 (6)	802.11n	-50	WPA-CCMP	300.0	2	00:23:04:89:C6:91
Zone 2							
AskeyCompu 802....	11	802.11g	N/A	WPA-TKIP	54.0	1	00:21:63:1C:F7:89
AsustekCom 802.1...	11	802.11g	N/A	WPA-TKIP	54.0	1	90:E6:BA:A9:9D:4C

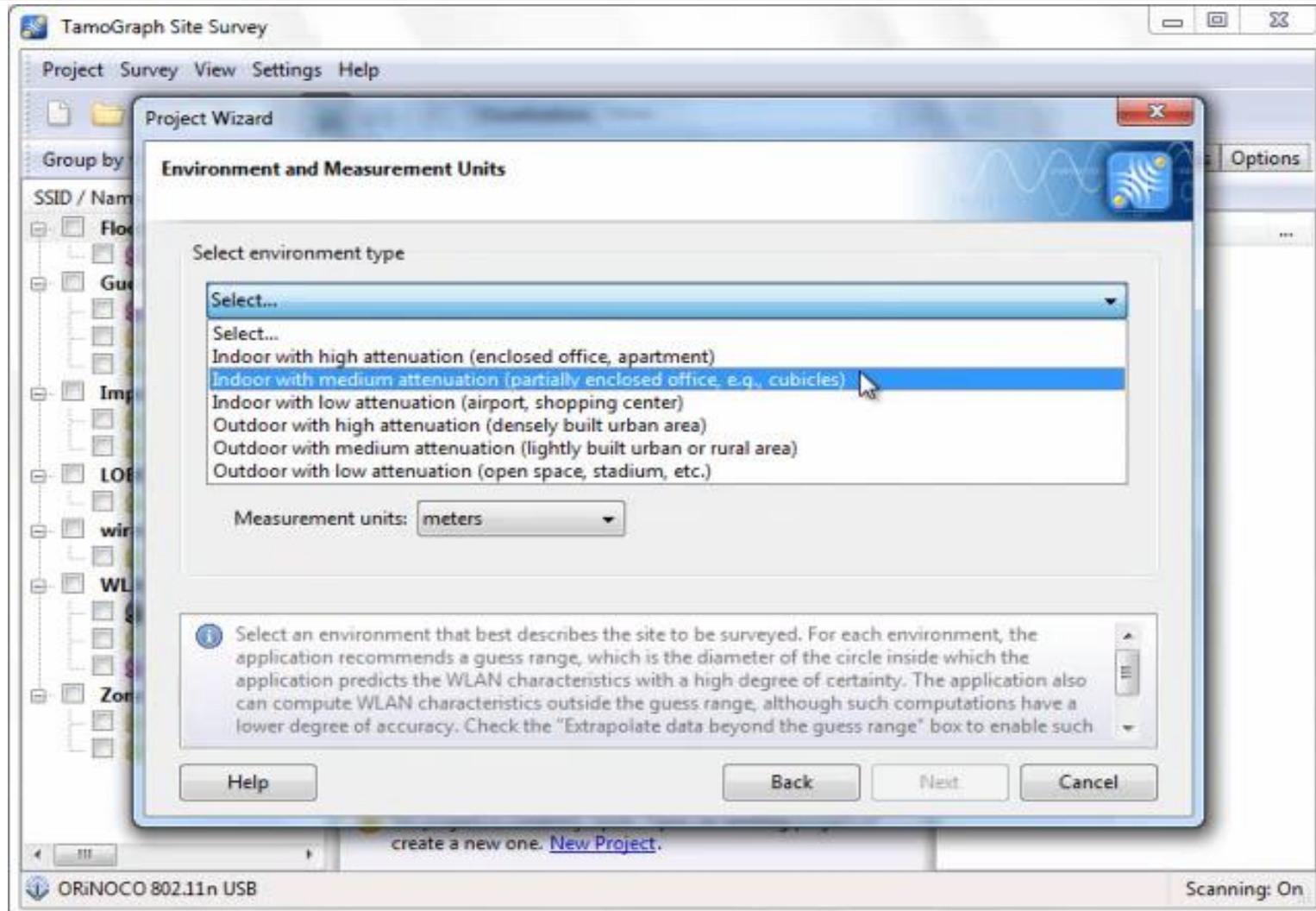
ORiNOCO 802.11n USB

Scanning: On

! No project is currently open. Open an existing project or create a new one. [New Project.](#)









The screenshot shows the 'Project Wizard' dialog box in the 'Scanner Settings' step. The 'Channels to scan' table is as follows:

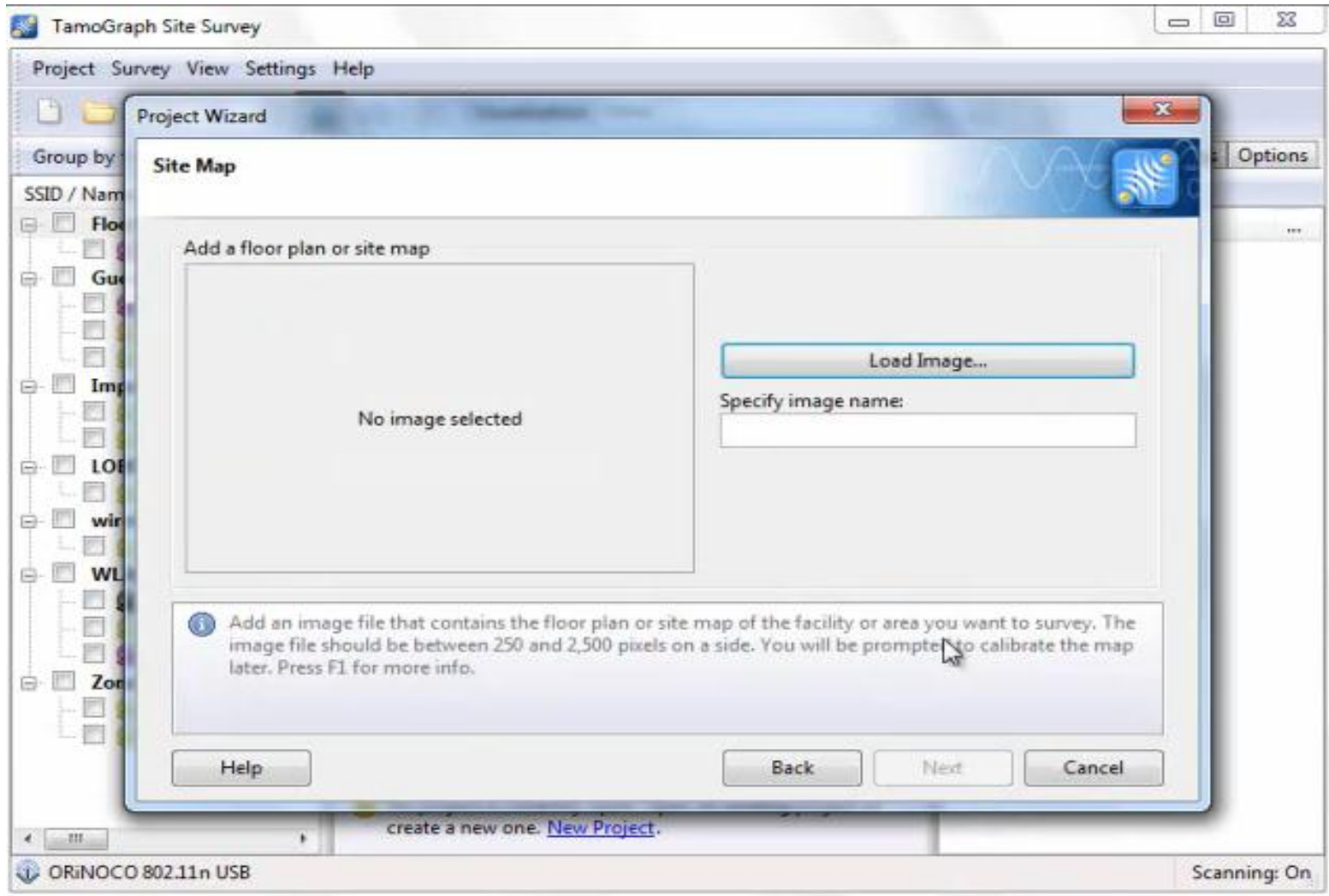
Channel	Interval
<input checked="" type="checkbox"/> 2.4 GHz 802.11b/g/n	
<input checked="" type="checkbox"/> 1	250
<input checked="" type="checkbox"/> 2	250
<input checked="" type="checkbox"/> 3	250
<input checked="" type="checkbox"/> 4	250
<input checked="" type="checkbox"/> 5	250
<input checked="" type="checkbox"/> 6	250
<input checked="" type="checkbox"/> 7	250
<input checked="" type="checkbox"/> 8	250
<input checked="" type="checkbox"/> 9	250

Additional settings in the dialog include:

- Scan interval: 250 ms
- Use the same interval for all channels
- Buttons: Help, Back, Next, Cancel

Background information from the main window:

- Project: Survey
- SSID / Name: Floo, Guu, Imp, LOF, wir, WL, Zon
- Device: ORiNOCO 802.11n USB
- Status: Scanning: On





Zone A.ssprj* - TamoGraph Site Survey

Project Survey View Settings Help

Visualization: None

To calibrate the map, you need to know the distance between two points on the map. This could be the distance between two walls or windows. Click on the first point and, while holding down the left mouse button, move the mouse pointer to the second point. Release the left mouse button when the mouse pointer is over the second point. A red line indicating the distance will be shown. Now enter the length of the red line and click "Apply".

The measured distance is 0.00 m

Apply

ORiNOCO 802.11n USB Scanning: On



Zone A.ssprj* - TamoGraph Site Survey

Project Survey View Settings Help

Visualization: None

0 10 20

0 10

Reception

Office A

Office B

Break Room

Conference Room

Walk along the planned path at a steady pace in a straight line. Every time you need to change direction, click on the map again to mark your current location. When done, click "Stop" to finish the survey.

ORiNOCO 802.11n USB 12.84 x 13.47 m 5.92 : 9.79 m Zoom 82% Scanning: On



The screenshot shows the TamoGraph Site Survey software interface. The window title is "Zone A.ssprj* - TamoGraph Site Survey". The menu bar includes "Project", "Survey", "View", "Settings", and "Help". The toolbar contains icons for file operations and a "Visualization" dropdown set to "None".

The left sidebar shows a tree view of the survey data, grouped by "Floor_5". The "WLAN03" group is highlighted with a red box and contains the following items:

- 3com 802.11n
- Cisco 802.11n
- Cisco 802.11g
- Cisco 802.11n

The main area displays a floor plan of "Floor 5" with various rooms labeled: "Reception", "Office A", "Office B", "Lobby", "Break Room", and "Conference Room". Blue arrows indicate the survey path. The status bar at the bottom shows "ORiNOCO 802.11n USB", dimensions "14.93 x 15.66 m", "Zoom 70%", and "Scanning: On".



The screenshot shows the TamoGraph Site Survey software interface. The main window displays a floor plan of a building with various rooms labeled: Reception, Office A, Office B, Break Room, Conference Room, and LOBBY. A blue signal strength heatmap is overlaid on the floor plan, with arrows indicating signal paths. A mouse cursor is hovering over a signal strength icon in Office B, which has triggered a tooltip with the following details:

- Name: Cisco 802.11n
- SSID: WLAN03
- MAC: 00:23:04:79:58:31
- Vendor: Cisco
- Channel: 161 (157)
- Max Rate: 300.0 Mbps
- Encryption: None

The left sidebar shows a tree view of detected SSIDs and devices, grouped by floor (Floor_5) and zone (Zone 2). The WLAN03 group is expanded, showing several Cisco 802.11n and Cisco 802.11g devices. The bottom status bar indicates the current device is an ORINOCO 802.11n USB, with a signal strength of -79 dBm and a distance of 13.90 m. The zoom level is set to 70% and scanning is on.



Zone A.ssprj* - TamoGraph Site Survey

Project Survey View Settings Help

Visualization: None

- None
- Signal Level
- Signal-to-Noise Ratio
- Signal-to-Interference Ratio
- AP Coverage Areas
- Number of APs
- Expected PHY Rate
- Frame Format
- Channel Bandwidth
- Requirements

Group by

SSID / Name

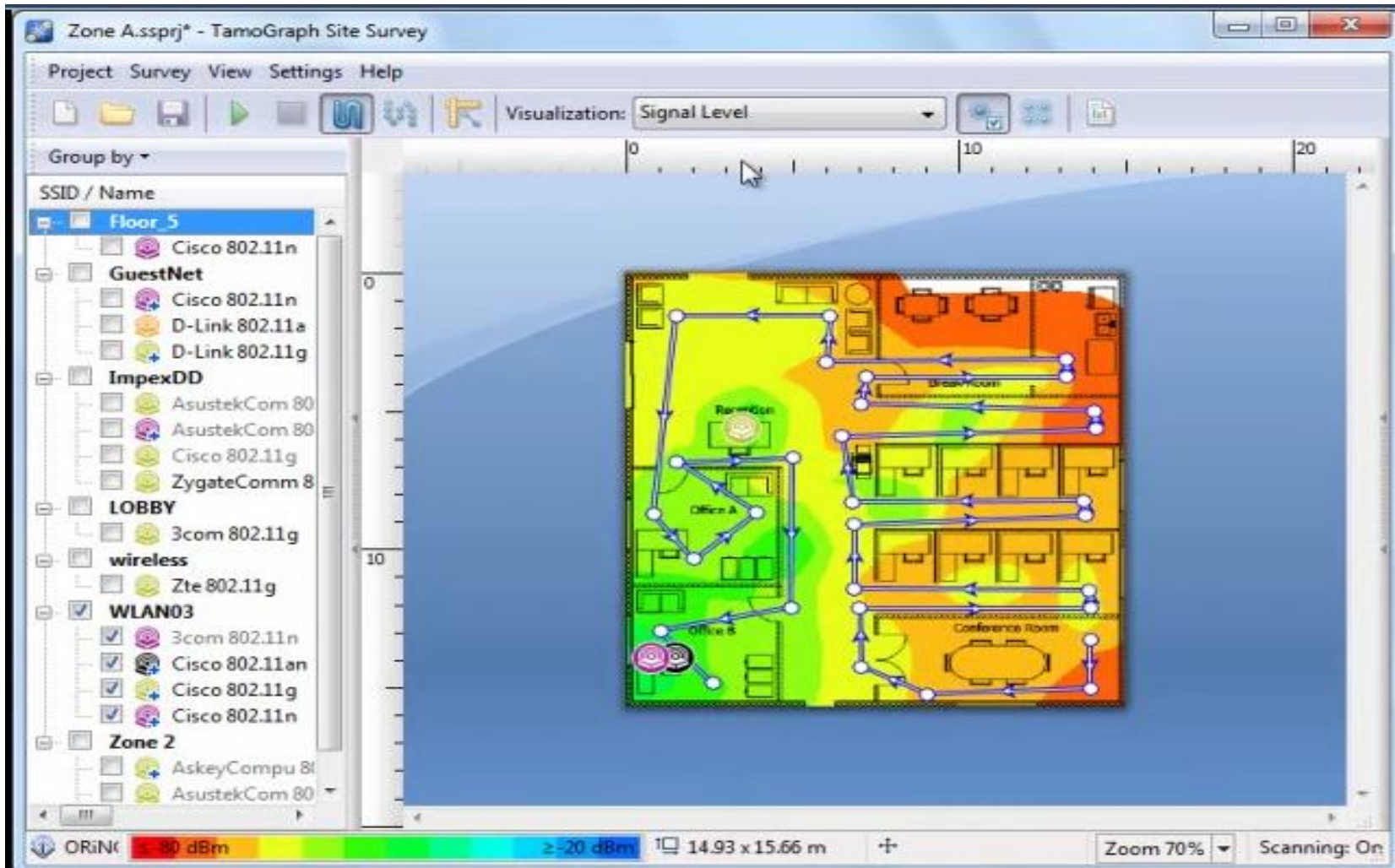
- Floor 5
 - Cisco 802.11n
 - GuestNet
 - Cisco 802.11n
 - D-Link 802.11a
 - D-Link 802.11g
 - ImpexDD
 - AsustekCom 80
 - AsustekCom 80
 - Cisco 802.11g
 - ZygateComm 8
 - LOBBY
 - 3com 802.11g
 - wireless
 - Zte 802.11g
 - WLAN03
 - 3com 802.11n
 - Cisco 802.11an
 - Cisco 802.11g
 - Cisco 802.11n
 - Zone 2
 - AskeyCompu 8l
 - AsustekCom 80

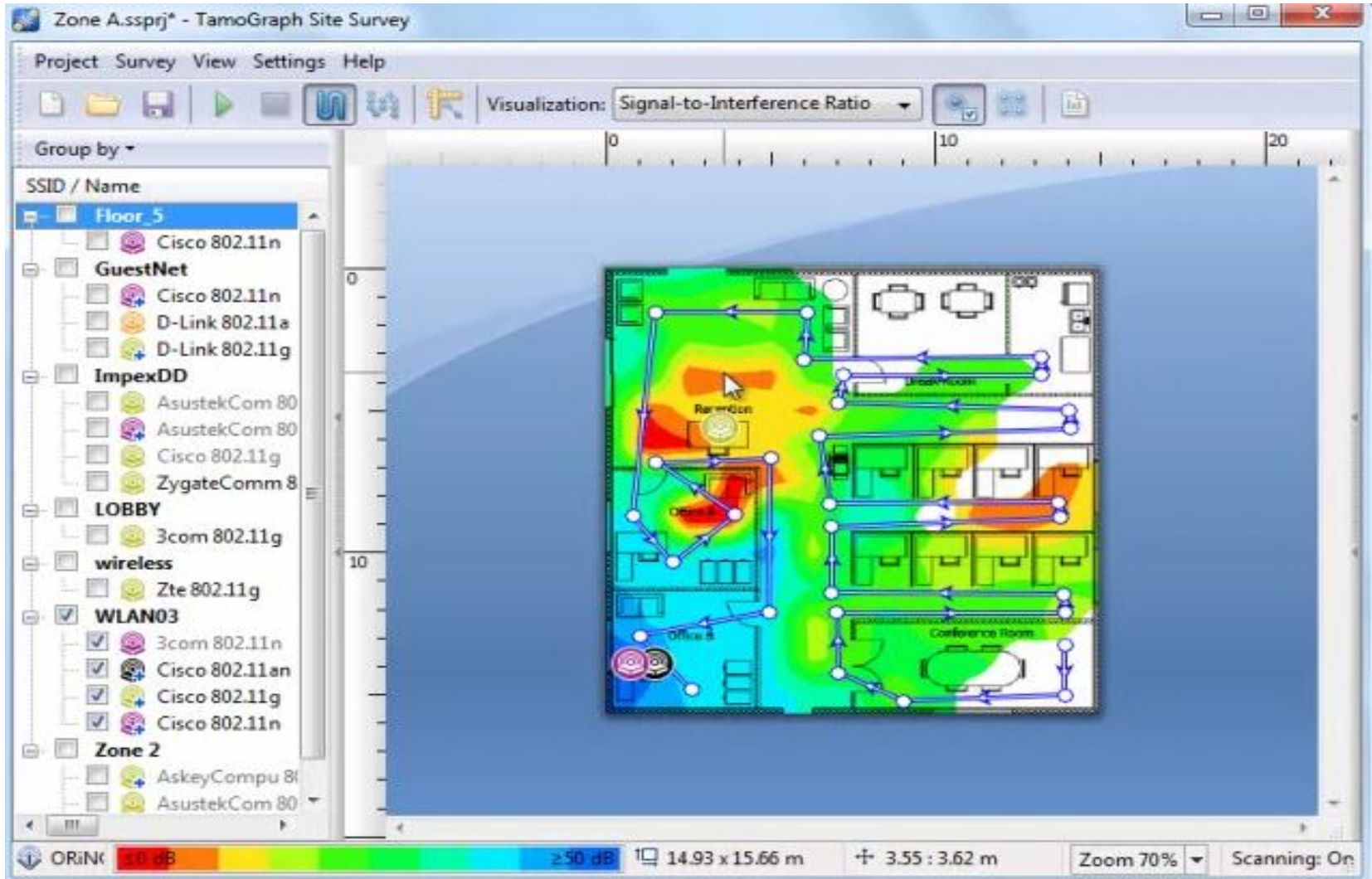
ORiNOCO 802.11n USB

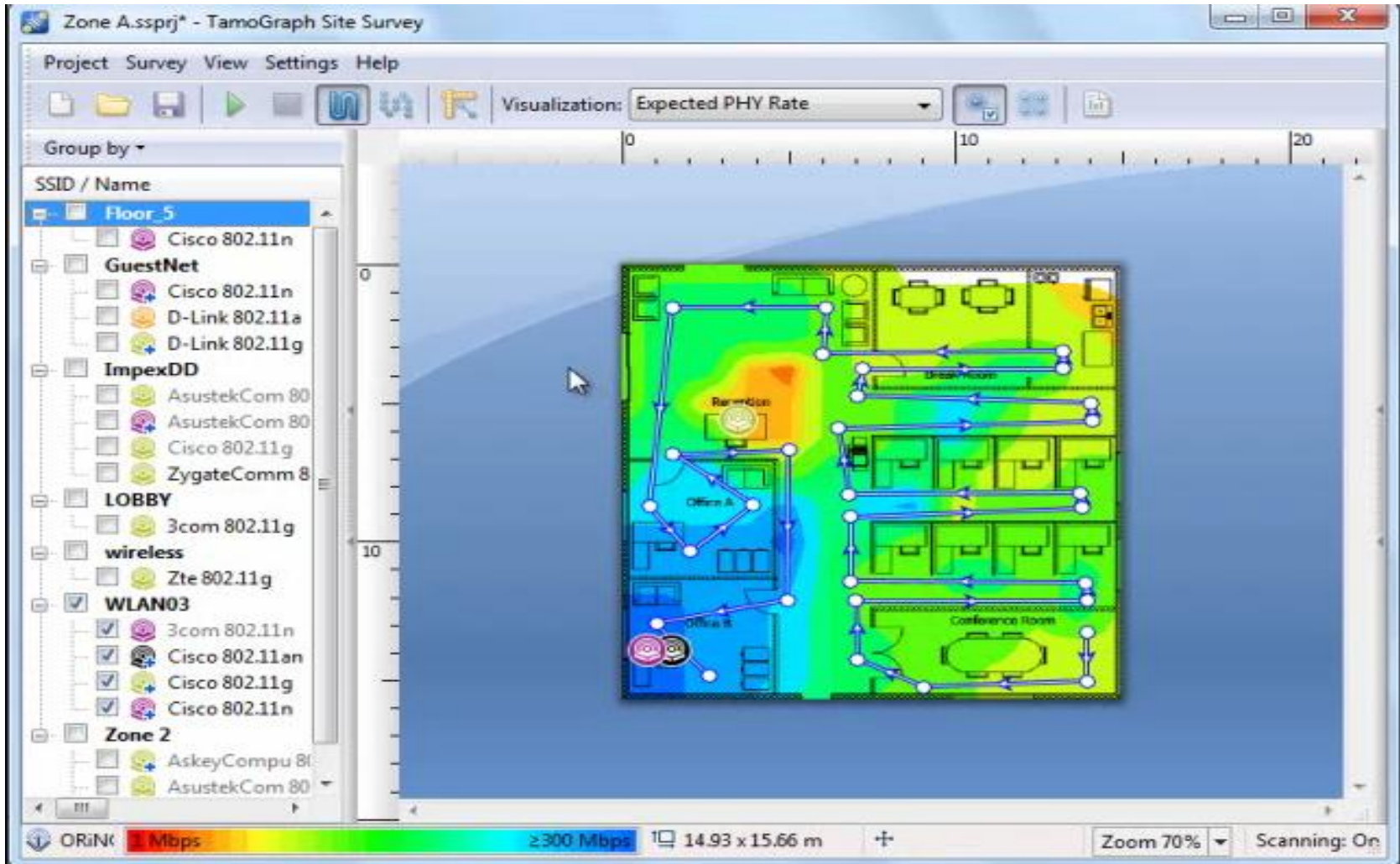
14.93 x 15.66 m

Zoom 70%

Scanning: On










Zone A.sprj* - TamoGraph Site Survey

Project Survey View Settings Help

Visualization: Requirements



Plans and Surveys Properties Options

Plan / Map

Environment

Requirements

Requirement preset: Advanced

Description	Threshold
<input checked="" type="checkbox"/> Min. signal...	-70 dBm
<input checked="" type="checkbox"/> Min. signal...	15 dB
<input checked="" type="checkbox"/> Min. signal...	20 dB
<input checked="" type="checkbox"/> Min. APs r... with si...	2 -70 dBm
<input checked="" type="checkbox"/> Min. PHY r...	11 Mbps
<input checked="" type="checkbox"/> Min. allow...	HT-mixed
<input checked="" type="checkbox"/> Min. chan...	20 MHz HT

Scanner

ORiNK SL SNR SIR PHY FF CB 14.93 x 15.66 m Zoom 70% Scanning: On



Zone A.sprj* - TamoGraph Site Survey

Generate Report

Plans and Surveys

- sample office no margins
 - Survey 9/9/2010 1:39:06 PM
 - Survey 9/9/2010 2:28:52 PM

Current AP selection mode: Selected APs

Project information

Surveyor: ADMIN

Location:

Description:

Visualizations

- Map with no visualizations
- Signal Level
- Signal-to-Noise Ratio
- Signal-to-Interference Ratio
- AP Coverage Areas
- Number of APs
- Expected PHY Rate
- Frame Format
- Channel Bandwidth
- Requirements

Additional items to include

- Walkabout paths
- AP list
- Map descriptions
- Survey comments

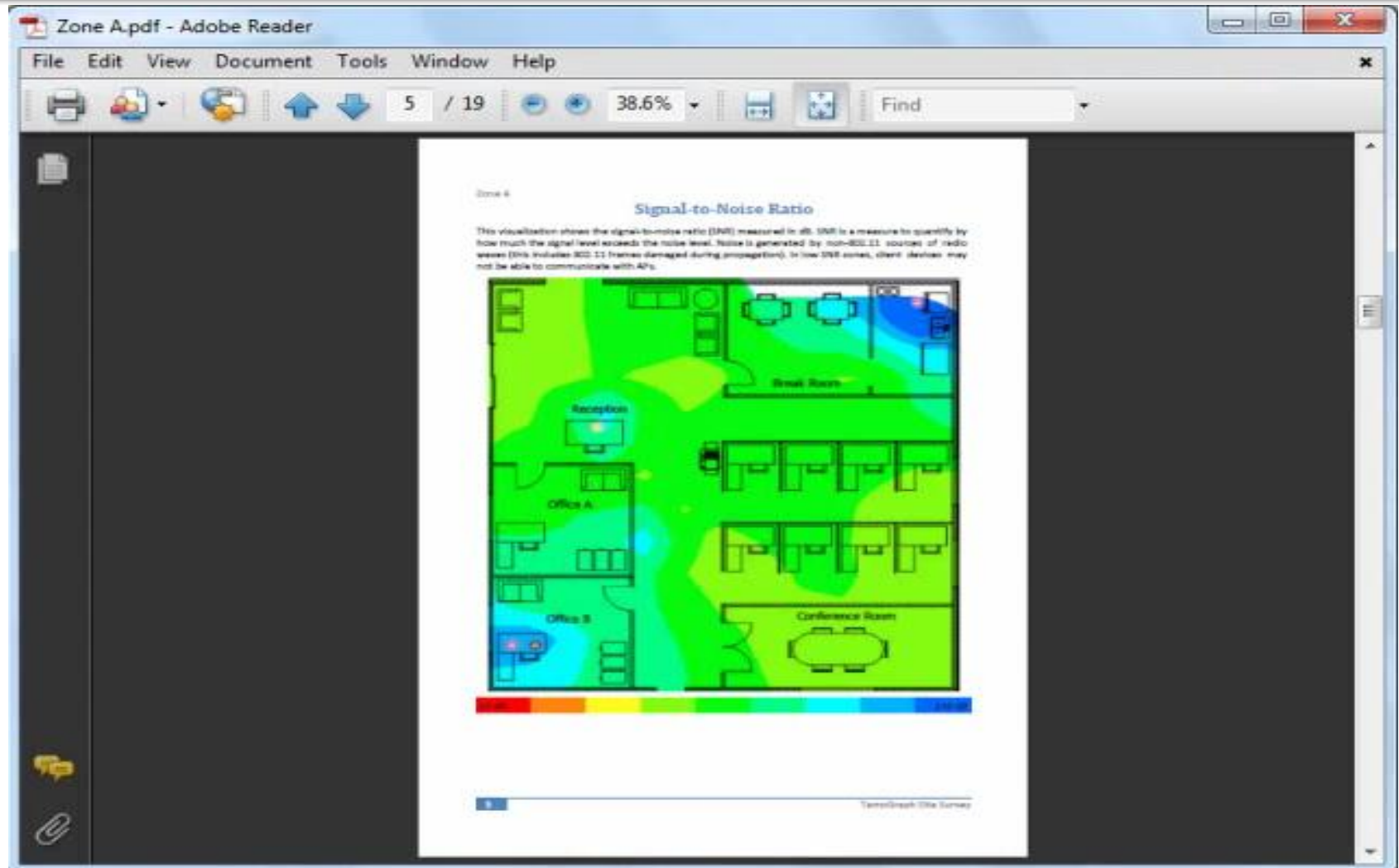
Output settings

Format: PDF

Paper size: A4

Help Open report after generation Save Print... Cancel

ORiNc SL SNR SIR PHY FF CB 14.93 x 15.66 m Zoom 70% Scanning: On





Netzwerk Design

„Wie erstelle ich ein High-Performance Netzwerk“

Bereitstellung und Verifikation

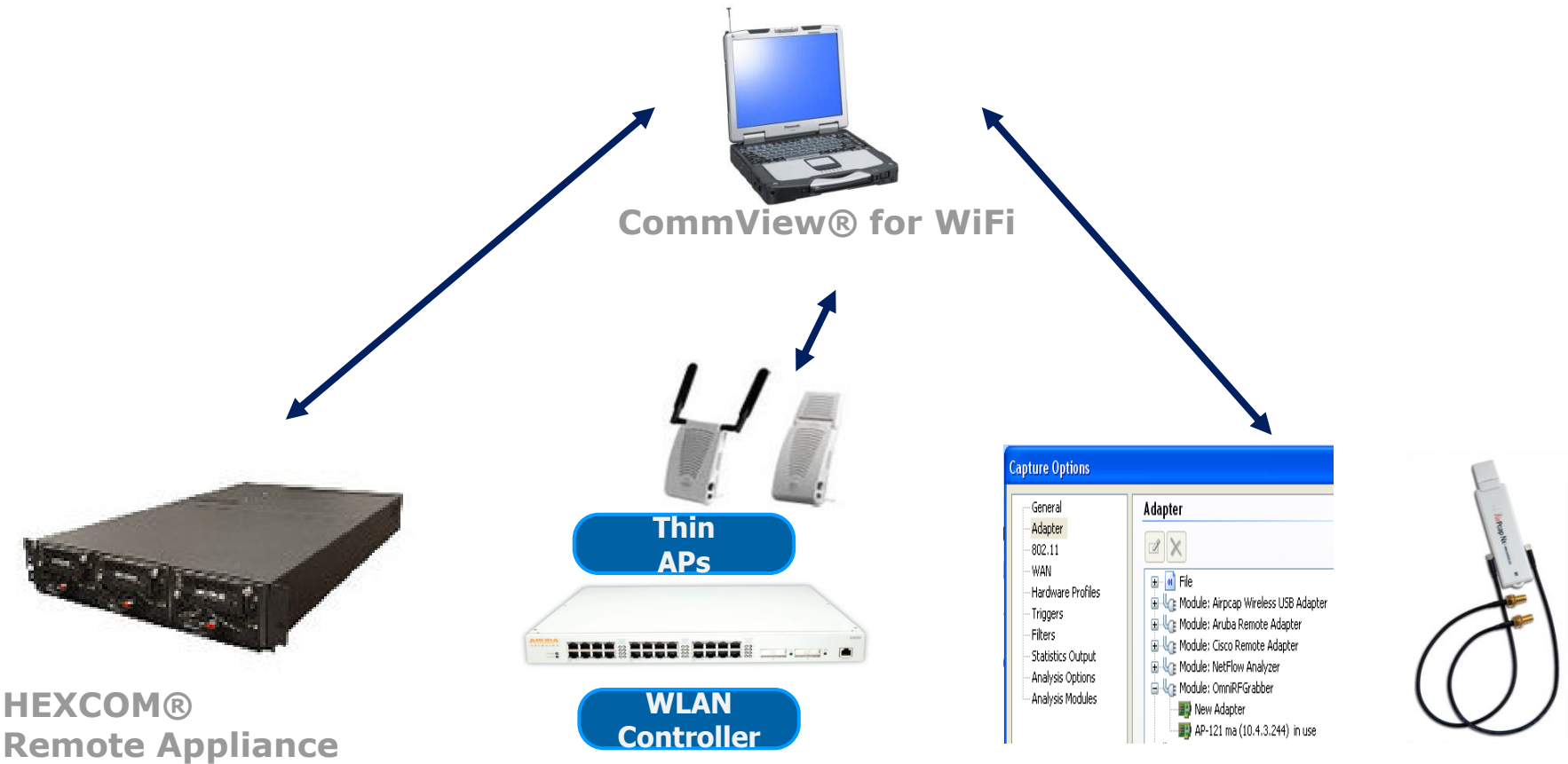
„Hat mein Netzwerk die gewünschte Performance“

Troubleshooting und Management



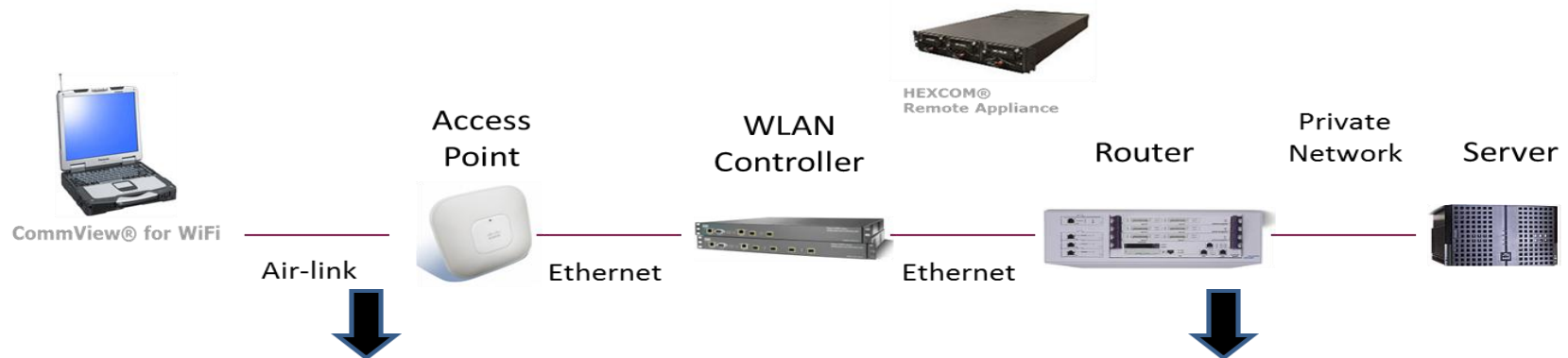
Wireless Troubleshooting und Management Möglichkeiten

Übersicht!





Wireless Analyse und Management Möglichkeiten. Wofür überhaupt?



- >> Um Sicherheitsrichtlinien zu Überprüfen.
- >> Um Rogue APs und Clients auswendig zu machen.
- >> Um Wireless security Attacken zu verhindern
- >> Um Performance und Qualität zu Überwachen
- >> Um Tiefgehende Protokollanalysen zu starten.

- >> Zum Nachverfolgen der WLAN Pakete
- >> Zum Sicherstellen des "QOS"
- >> Zum Betrachten von VPN/MPLS "Wahlverfahren"
- >> Zum Überblick gesamter Netzwerklatenzen.



Netzwerk Design

„Wie erstelle ich ein High-Performance Netzwerk“

Bereitstellung
und Verifikation

„Hat mein Netzwerk die gewünschte Performance“

Troubleshooting
und Management

Beispiele der Mobilten Wireless Analyse



Wireless Capture Adapter für CommView WiFi

„The big brother from AirPcap Adapter“



Der selbe Hersteller, wie für den AirPcap NX.

Die gleiche Leistung wie der AirPcap NX.

Doch der Preis macht den Unterschied.

AirPCAP NX = Durchschnitt 590,00 EUR*

CommView WiFi Adapter = Festpreis 100,00 EUR*

* = netto



Scanner
✕

Scanning

Options

Access Points & Hosts	Signal
[-] Channel 5	
BelkinComp:60:CC:0D	■ ■ ■ ■ ■
GemtekTech:00:A4:92	■ ■ ■ ■ ■
[-] Channel 9	
3com:93:98:86	■ ■ □ □ □
3comEurope:A4:80:CE	■ ■ ■ ■ ■
Intel:50:3F:16	■ ■ ■ ■ ■
Netgear:41:B4:2D	■ ■ □ □ □
D-Link:5B:C5:C2	■ ■ ■ □ □
BelkinComp:60:CC:0D	■ ■ ■ □ □

Details:

Is Access Point: No

Is Wireless Host: Yes

WEP/WPA: No

SSID: office (Ad Hoc)

Signal Level: 50

MAC Address: 00:30:BD:60:CC:0D

IP Address: 169.254.109.28

Scanner

Select a channel and click "Capture" to close the scanner window and start capturing

Band: 802.11b/g

Channel: 5

802.11b/g: Scanning channel 9 ...



CommView for WiFi - D-Link AirXpert DWL-AG520 Wireless PCI Adapter

File Search View Tools Settings Rules Help

Nodes Channels Latest IP Connections Packets Logging Rules Alarms

MAC Address	Channel	Type	SSID	Encryption	Signal	Rate	Bytes	Packets	Retry	ICV Err...
AP_DLINK	11	AP	PINO...	WPA-CCMP	51/69/81	1/5.78/54	122,801	1,249	66	0
LinksysGro:60:89:D5	11	STA		WPA	1/69/78	1/32.44/48	27,549	377	0	0
AP_DLINK	161	AP	PINO...	WEP	23/50/63	6/46.41/54	2,299,698	53,090	551	0
Proxim	161	STA		WEP	41/61/80	6/53.2/54	1,907,059	25,669	124	0

Capture: On | Packets: 61,071 | Keys: WEP,WPA | Auto-saving: Off | Rules: Off | Alarms: Off | 0% CPU Usage



CommView for WiFi - D-Link AirXpert DWL-AG520 Wireless PCI Adapter

File Search View Tools Settings Rules Help

Nodes Channels Latest IP Connections Packets Logging Rules Alarms

Channel	Packets	Data	Mngt	Ctrl	Signal	Rate	Encryption	Retry	ICV Errors	CRC Errors
6	2	0	2	0	93/96/98	1/1/1	0	0	0	0
7	2	0	2	0	93/94/95	1/1/1	0	0	0	0
8	6	0	6	0	61/73/80	1/1/1	0	0	0	1
9	8	2	6	0	50/56/63	1/1/1	2	0	0	0
11	1,505	216	1,056	233	1/69/86	1/9.91/54	216	75	2	33
12	44	9	35	0	63/70/80	1/1/1	9	4	0	1
13	24	0	23	1	50/64/80	1/5.17/54	0	1	0	2
161	57,828	28,195	1,911	27,722	18/55/81	6/34.66/54	27,224	941	2,805	3,085

Capture: Off | Packets: 62,063 | Keys: WEP,WPA | Auto-saving: Off | Rules: Off | Alarms: Off | 1% CPU Usage



CommView for WiFi - D-Link AirPremier DWL-AG530 Wireless PCI Adapter

File Search View Tools Settings Rules Help

Nodes Channels Latest IP Connections Packets Logging Rules Alarms

Source IP	Destination IP	In	Out	Sessions	Ports	Hostn...	Bytes
192.168.0.1	192.168.0.3	1899	1542	2	netbios-ssn,3017,3...		2,009,081
12.13.14.15	192.168.0.3	0	1	0	3016,net		
192.168.0.16	192.168.0.3	0	2	0	3018,net		
192.168.0.50	192.168.0.3	1751	1699	0			
192.168.0.3	192.168.0.255	0	2	0	netbio		
192.168.0.1	238.239.238.239	0	15	0	netbios-dg		
▶ 192.168.0.1	192.168.0.22	537	492	2	microsoft-c		
192.168.0.22	192.168.0.50	14	12	2	1044,ht		
192.168.0.1	192.168.0.255	0	8	0	netbios-ns,		
192.168.0.22	192.168.0.255	0	3	0	netbi		

Quick Filter

- Copy ▶
- Show All Ports ...
- Data Transfer ...
- Jump To ▶
- SmartWhois ▶
- Create Alias ▶
- Save Latest IP Connections As ...
- Clear Latest IP Connections
- More Statistics ...

Capture: On | Packets: 25,932 | Keys: WPA | Auto-saving: Off | Rules: Off | Alarms: Off | 1% CPU Usage



CommView for WiFi - D-Link AirPremier DWL-AG530 Wireless PCI Adapter

File Search View Tools Settings Rules Help

Nodes Channels Latest IP Connections Packets Logging Rules Alarms

Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port	Dest Port	Signal	Rate	More details
IP/TCP	GemtekTe...	Intel:96:0...	192.168.0.4	192.168.0.1	micros...	3019	68	54	WEP: Decrypted...
MNGT/BEA...	MyAP	Broadcast	N/A	N/A	N/A				
IP/UDP	GemtekTe...	01:00:5E:...	192.168.0.4	239.255.2...	1900				
IP/UDP	GemtekTe...	33:33:00:...	158.22.250.0	0.0.0.12	1900				
ARP REQ	GemtekTe...	Broadcast	192.168.0.4	192.168.0.1	N/A				
MNGT/BEA...	MyAP	Broadcast	N/A	N/A	N/A				

0x0000	08 41 2C 00 00 0F 3D E9-05 00 00 14 A5 2D 61 2F .A
0x0010	00 02 B3 96 0C EC 20 AE-AA AA 03 00 00 00 08 00 ..
0x0020	45 00 00 4F 2C F7 40 00-80 06 4C 5C C0 A8 00 04 E.
0x0030	C0 A8 00 01 01 BD 0B CB-EE D9 65 0C F1 6F E8 02 A"
0x0040	50 18 40 D5 06 6D 00 00-00 00 00 23 FF 53 4D 42 P.

Wireless Packet Info

- Signal level: 0x44 (68)
- Rate: 54.0 Mbps
- Band: 802.11g
- Channel: 11 - 2462 MHz
- Date: 7-Jul-2006
- Time: 13:21:55.677507

Capture: Off | Packets: 29,693 | Keys: WEP,WPA | Auto-saving: Off | Rules: Off

Reconstruct TCP Session

- Quick Filter
- Open Packet(s) in New Window
- Create Alias
- Copy Address
- Copy Packet
- Send Packet(s)
- Save Packet(s) As ...
- SmartWhois
- Clear Packet Buffer
- Decode As
- Font



TCP Session

File Edit Settings

Contents | Session Analysis

```
GET /wiki/Computer_network HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword,
application/x-silverlight, */*
Referer:
http://www.google.com/search?sourceid=navclient&ie=UTF-8&rlz=1T4GFRC_enRU220
RU225&q=networking
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR
2.0.50727; .NET CLR 1.1.4322)
Host: en.wikipedia.org
Connection: Keep-Alive

HTTP/1.0 200 OK
Date: Mon, 17 Dec 2007 09:50:04 GMT
```

MyIP:1068 => rr.pmtpa.wikimedia.org:80 * 1,472 bytes in 4 packet(s) Display type: ASCII
 rr.pmtpa.wikimedia.org:80 => MyIP:1068 * 24,372 bytes in 19 packet(s)
 Total 25,844 bytes in 23 packet(s), Session time: 3 second(s) Navigation: << >> >>>

TCP Session

File Edit Settings

Contents | Session Analysis

Web Images Maps News Shopping Gmail more | Blogs Books Calendar Documents Fir | Sign in

Google

networking Search [Advanced Search Preferences](#)

Web Books Scholar Results 1 - 10 of about 25,000,000 for networking [definition]. (0.14 seconds)

[Computer network - Wikipedia, the free encyclopedia](#)
 A computer network is an interconnection of a group of computers. Networks ma classified by what is called the network layer at which they operate ...
[en.wikipedia.org/wiki/Computer_network](#) - 70k - [Cached](#) - [Similar pages](#)

[Network - Wikipedia, the free encyclopedia](#)
 In general, the term network can refer to any interconnected group or sys specifically, a network is any method of sharing information between two
[en.wikipedia.org/wiki/Network](#) - 25k - [Cached](#) - [Similar pages](#)
 [More results from en.wikipedia.org]

Sponsored Links

[IESE Executive Education](#)
 International Management Programs for senior Executives. Sign up now!
[www.iese.edu](#)


MyIP:1065 => lm-in-f104.google.com:80 * 818 bytes in 1 packet(s) Display type: HTML
 lm-in-f104.google.com:80 => MyIP:1065 * 6,870 bytes in 6 packet(s)
 Total 7,688 bytes in 7 packet(s), Session time: 0 second(s) Navigation: << >> >>>

TCP Session

File Edit Settings

Contents | Session Analysis

```
GET /images?q=tbm:JtYSr1oE1JXCMhttp://jayeragon.com/blog/wp-content/uploads/2007/10/online_business_f
http://images.google.com/images?sourceid=navclient&ie=UTF-8&rlz=1T4GFRC_enRU220RU225&q=networking&
x86 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.
Connection: Keep-Alive Cookie: PREF=ID=38aaa705a1a45060.TB=2.TM=1184937720.LM=1184957928.S=k1MjWj
NID=7=BFDbjwvxsKtrkEigMJOB19Zq3v48uQhLZXeN_L4j87QhNzduGwi78G2OULPwv219d9GhnyFcJ1Hmz161BLc
HTTP/1.1 200 OK Content-Type: image/jpeg Cache-Control: max-age=604800 Server: ltf Content-Length: 2406
```



```
GET /images?q=tbm:lb7slpCJwVZ1cMhttp://assets.xbox.com/en-us/support/_images/Networking_Use3.jpg HTTP
http://images.google.com/images?sourceid=navclient&ie=UTF-8&rlz=1T4GFRC_enRU220RU225&q=networking&
x86 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.
Connection: Keep-Alive Cookie: PREF=ID=38aaa705a1a45060.TB=2.TM=1184937720.LM=1184957928.S=k1MjWj
NID=7=BFDbjwvxsKtrkEigMJOB19Zq3v48uQhLZXeN_L4j87QhNzduGwi78G2OULPwv219d9GhnyFcJ1Hmz161BLc
HTTP/1.1 200 OK Content-Type: image/jpeg Cache-Control: max-age=604800 Server: ltf Content-Length: 2137
```

MyIP:1102 => 216.239.59.104:80 * 6,398 bytes in 9 packet(s) Display type: HTML
 216.239.59.104:80 => MyIP:1102 * 33,326 bytes in 29 packet(s)
 Total 39,724 bytes in 38 packet(s), Session time: 1 second(s) Navigation: << >> >>>

TCP Session

File Edit Settings

Contents | Session Analysis

14:14:38.561804 0.000284	Seq: 1 (2853554876) Ack: 1 (2827424013) Data: 565 Flags: [PSH ACK] Seq: 1 (2853554876) Ack: 1 (2827424013)	3	Connection Time: 0.186835 Server Response Time: 0.000964 Data Transfer Time: 2.839024
14:14:38.750393 0.188589	Seq: 1 (2827424013) Ack: 566 (285355441) Data: 1460 Flags: [ACK]	4	
14:14:38.753424 0.003031	Seq: 1 (2827424013) Ack: 566 (285355441) Data: 1460 Flags: [ACK]	5	
14:14:38.755387 0.001963	Seq: 1461 (2827425473) Ack: 566 (285355441)	6	
14:14:38.755418 0.000031	Seq: 566 (285355441) Ack: 2921 (2827426933) Data: 1460 Flags: [ACK]	7	
		8	
		9	

MyIP:1068 => rr.pmtpa.wikimedia.org:80 * 1,472 bytes in 4 packet(s) Display type: HTML
 rr.pmtpa.wikimedia.org:80 => MyIP:1068 * 24,372 bytes in 19 packet(s)
 Total 25,844 bytes in 23 packet(s), Session time: 3 second(s) Navigation: << >> >>>



Alarm Setup ✕

General

Name: Enabled

Alarm type

Packet occurrence (enter a formula):

`ipproto=tcp and dport=1080`

Bytes per second >

Unknown MAC address: Configure ...

Unknown IP address: Configure ...

Rogue APs: Configure ...

Ad Hoc Networks: Configure ...

Event occurrences

Events needed to trigger:

Times to trigger this alarm:

Action

Display message:

Pronounce message:

Play sound:
 📁

Launch application:
 📁

Parameters:

Send e-mail to:
 ⚙️

Add text:

Enable capturing rules:

Disable other alarms:

Start logging

Stop logging



Send Packet

Wireless Packet Info

- 802.11
- Probe request
 - SSID
 - Supported rates
 - Extended Supported Rat

Templates

- ARP
- Beacon
- ProbeRequest

0x00: FF FF FF FF FF 00 20 A6 4F F4 C2 @...yyyyyy. !06Ã

0x10: FF 50 11 00 00 01 08 02 04 0B 16 yyyyyyP.....

0x20: 04 12 24 60 6C ..OH2...\$`1

Packet Generator

Packet size: 42

Packets per second: 580

802.11 rate, Mbps: 48

Continuously

1 time(s)

Long Preamble

Send



CommView for WiFi - D-Link DWA-552 Xtreme N Desktop Adapter

File Search View Tools Settings Rules Help

Nodes Channels Latest IP Connections Packets Logging Rules Alarms VoIP

- SIP Sessions (3)
- H.323 Sessions (0)
- RTP Streams (2)
- Registrations (1)
- Endpoints (2)
- Errors (6)
- Call Logging
- Report

Src IP	Dest IP	Start Time	End Time	Duration	Status
210.54.125.221	210.54.125.100	6:52:11 PM	6:52:48 PM	0:00:36.4	Completed
210.54.125.221	210.54.125.100	6:52:12 PM	6:53:51 PM	0:01:39.2	Not a call
210.54.125.221	210.54.125.100	6:54:20 PM	6:54:20 PM	0:00:00.1	Not a call

SIP Session

Call Info | RTP Streams (2)

Time	Operat...	Request/Response
18:52:1...	INVITE	INVITE sip:8495...
18:52:1...		100 Trying
18:52:1...		401 Authentic...
18:52:1...		ACK sip:8495249...
18:52:1...	INVITE	INVITE sip:8495...
18:52:1...		100 Trying
18:52:1...		183 Session Pro...

Timing

Start Time	8/23/2006 6:52:11 PM
End Time	8/23/2006 6:52:48 PM
Duration	0:00:36.4

Quality

MOS Score	3.4
R-Factor	66

SIP

Capture: Off | Packets: 391 | Keys: WPA | Auto-saving: Off | Rules: 1 On | Alarms: Off | 4% CPU Usag | PR.REQ



VoIP Log Viewer [G.723 including SIP.ncf]

File

- SIP Sessions (3)
- H.323 Sessions (0)
- RTP Streams (2)
- Registrations (1)
- Endpoints (2)
- Errors (6)

SIP Sessions

Src IP	Dest IP	Start Time	End Time	Duration	Status
210.54.125.221	210.54.125.100	6:52:11 PM	6:52:48 PM	0:00:36.4	Completed
210.54.125.221	210.54.125.100	6:52:12 PM	6:53:51 PM	0:01:39.2	Not a call
210.54.125.221	210.54.125.100	6:54:20 PM	6:54:20 PM	0:00:00.1	Not a call

SIP Session

Call Info | RTP Streams (2)

Time	Request/Response
18:52:11.965000	INVITE sip:12345678901@tamos.c...
18:52:12.021000	100 Trying
18:52:12.021000	401 Authentication required
Header SIP/2.0 401 Authenticatic Via: SIP/2.0/UDP 192.168.131... From: <sip:2326845@tamos.cc...> To: <sip:12345678901@tamos.cor...> Call-ID: 29002@192.168.131.7... CSeq: 20 INVITE WWW-Authenticate: Digest realm="sip.tsft.loc",nonce="CC... Server: CommuniGatePro/5.0.1... Content-Length: 0	
18:52:12.034000	ACK sip:12345678901@tamos.cor...
18:52:12.046000	INVITE sip:12345678901@tamos...

Transport Infor...

- Src IP: 210.54.125.221
- Src Port: 3068
- Dest IP: 210.54.125.100
- Dest Port: 5060
- Protocol: UDP

Timing

- Start Time: 8/23/2006 6:52:11 PM
- End Time: 8/23/2006 6:52:48 PM
- Duration: 0:00:36.4

Quality

- MOS Score: 3.4
- R-Factor: 66

SIP

- Call ID: 29002@192.168.131.7...
- Calling Party**
 - Src Display Name: PortSIP softpho...
 - Src SIP Address: 2326845@tamo...
 - Src Tag: 16403
 - Src User Agent: PortSIP softpho...



VoIP Log Viewer [G.723 including SIP.ncf]

File

- SIP Sessions (3)
- H.323 Sessions (0)
- RTP Streams (2)**
- Registrations (1)
- Endpoints (2)
- Errors (6)

RTP Streams

Src IP	Dest IP	Start Time	Duration	RTP...	Avera...	Lost Packets	Max Jitte...	MOS
210.54.125.100	210.54.125.221	6:52:23 PM	0:00:23.3	753	19.63	27 (3.5%)	56.26	
210.54.125.221	210.54.125.100	6:52:14 PM	0:00:34.0	1121	20.07	0	19.16	

RTP Stream

Stream Info | Charts

Time	SSRC	...	Payload Na...	Jitter ...	RTI
18:52:23.908000	367797761		1 ITU-T G.723	0.00	
18:52:23.926000	367797761		2 ITU-T G.723	0.75	
18:52:23.968000	367797761		3 ITU-T G.723	1.45	
18:52:23.987000	367797761		4 ITU-T G.723	2.05	
18:52:24.028000	367797761		5 ITU-T G.723	2.61	
18:52:24.047000	367797761		6 ITU-T G.723	3.13	
18:52:24.089000	367797761		7 ITU-T G.723	3.69	

Transport Infor...

- Src IP: 210.54.125.100
- Src Port: 60638
- Dest IP: 210.54.125.221
- Dest Port: 3070
- Protocol: UDP

Timing

- Start Time: 8/23/2006 6:...
- End Time: 8/23/2006 6:...
- Duration: 0:00:23.3

Quality

- MOS Score: 3.4
- R-Factor: 66

RTP Statistics

- RTP Packet Co...: 753
- Lost Packets: 27 (3.5%)
- Duplicate Pack...: 0
- Sequence Errors: 0

Network Utilizat...

- Total Traffic (byt...): 58,734
- Network Tra: 31,626 (53.8%)

RTP Stream

Stream Info | Charts

Packet Count

Jitter

Stream Bandwidth

Packet Intervals



VoIP Log Viewer [G.723 including SIP.ncf]

File

- SIP Sessions (3)
- H.323 Sessions (0)
- RTP Streams (2)
- Registrations (1)
- Endpoints (2)
- Errors (6)**

Errors

Time	IP Address	Call ID	Error Class	Error Description
18:52:12.021000	210.54.125.100	29002@192.168...	Authorization	401 Authentication required
18:52:12.126000	210.54.125.100	2896@192.168...	Authorization	401 Authentication required
18:52:30.568000	210.54.125.100	2896@192.168...	Authorization	401 Authentication required
18:53:09.861000	210.54.125.100	2896@192.168...	Authorization	401 Authentication required
18:53:51.184000	210.54.125.100	2896@192.168...	Authorization	401 Authentication required
18:54:20.174000	210.54.125.100	8956@192.168...	Authorization	401 Authentication required

SIP Session

Call Info | RTP Streams (0)

Time	Request/Response
18:52:12.049000	REGISTER sip:tamos.com:5060
18:52:12.126000	401 Authentication required
18:52:12.130000	REGISTER sip:tamos.com:5060
18:52:12.186000	200 OK
18:52:30.317000	REGISTER sip:tamos.com:5060
18:52:30.568000	401 Authentication required
18:52:30.580000	REGISTER sip:tamos.com:5060
18:52:30.762000	200 OK
18:53:09.819000	REGISTER sip:tamos.com:5060
18:53:09.861000	401 Authentication required
18:53:09.866000	REGISTER sip:tamos.com:5060
18:53:09.937000	200 OK
18:53:51.143000	REGISTER sip:tamos.com:5060
18:53:51.184000	401 Authentication required
18:53:51.190000	REGISTER sip:tamos.com:5060
18:53:51.252000	200 OK

Transport Information

- Src IP: 210.54.125.221
- Src Port: 3068
- Dest IP: 210.54.125.100
- Dest Port: 5060
- Protocol: UDP

Timing

- Start Time: 8/23/2006 6:52...
- End Time: 8/23/2006 6:53...
- Duration: 0:01:39.2

Quality

- MOS Score: ?
- R-Factor: ?

SIP

- Call ID: 2896@192.168...

Calling Party

- Src. Display:



Vielen Dank für Ihre Aufmerksamkeit !!!



Patrick Petersson
CEO | CIO
HEXCOM UG

[Tel.: +49\(0\)89-35852970](tel:+4908935852970)
mail@hexcom.de



www.hexcom.de



www.xing.com/net/wireshark



www.admin-magazin.de



Fragen und Antworten