# 3.14 WLAN- und Funkverbindungsfehler analysieren

Eine WLAN-Verbindung besteht nicht nur aus „verbunden“ oder „nicht verbunden“. Zwischen Client und Anwendung liegen Funkübertragung, Authentifizierung, Zuordnung zu einem Access Point, VLAN-Zuweisung, IP-Konfiguration, Routing, DNS und der eigentliche Netzwerkdienst.

Die zentralen Fragen dieser Seite lauten:

> Kann der Client das gewünschte WLAN zuverlässig empfangen, sich korrekt authentifizieren und anschließend über das zugewiesene Netzwerk störungsfrei kommunizieren?

---

## 1. Sicherheits- und Aktionskennzeichnungen

| Kennzeichnung | Bedeutung |
|---|---|
| [RO] | Rein lesender Befehl, der normalerweise keine Konfiguration verändert |
| [TEST] | Aktiver Test, der Funk- oder Netzwerkverkehr erzeugt |
| [PRIV] | Administrator- oder Root-Rechte können erforderlich sein |
| [FILE] | Der Befehl schreibt Ausgaben in eine Datei |
| [SENS] | Die Ausgabe kann sensible Informationen enthalten |
| [CHANGE] | Der Befehl verändert eine Konfiguration |
| [DISRUPT] | Der Befehl kann eine Verbindung oder Funkversorgung beeinträchtigen |

WLAN-Diagnosen können SSIDs, BSSIDs, MAC-Adressen, Standorte, Benutzernamen, interne Netze und Authentifizierungsinformationen enthalten. Kennwörter und private Schlüssel dürfen niemals exportiert oder dokumentiert werden.

---

## 2. WLAN-Fehler in Schichten aufteilen

| Ebene | Zentrale Frage |
|---|---|

| | |
|---|---|
| Hardware | Ist der WLAN-Adapter vorhanden und betriebsbereit? |
| Funk | Ist das gewünschte WLAN mit ausreichender Qualität empfangbar? |
| 802.11-Verbindung | Kann sich der Client mit dem Access Point verbinden? |
| Authentifizierung | Werden Kennwort, Zertifikat oder 802.1X-Anmeldung akzeptiert? |
| Netzwerkzuweisung | Erhält der Client das richtige VLAN und die richtige IP-Konfiguration? |
| Routing | Ist das Standardgateway erreichbar? |
| DNS | Funktioniert die Namensauflösung? |
| Internetzugang | Ist ein externer Zugriff möglich? |
| Anwendung | Funktioniert der tatsächlich benötigte Dienst? |
| Stabilität | Bleibt die Verbindung bei Bewegung und Last erhalten? |

**Grundregel:**

Mit WLAN verbunden
≠
gültige IP-Konfiguration
≠
Internetzugang
≠
Anwendung funktioniert

## 3. Wichtige WLAN-Begriffe unterscheiden

| Begriff | Bedeutung |
|---|---|
| SSID | Sichtbarer beziehungsweise konfigurierter WLAN-Netzwerkname |
| BSSID | Kennung einer konkreten Funkzelle, üblicherweise eine MAC-Adresse |
| Access Point | Stellt die WLAN-Funkzelle bereit |
| Band | Frequenzbereich, beispielsweise 2,4 GHz, 5 GHz oder 6 GHz |
| Kanal | Genutzter Teil des Frequenzbereichs |

| Begriff | Bedeutung |
| --- | --- |
| Kanalbreite | Beispielsweise 20, 40, 80 oder 160 MHz |
| RSSI | Empfangssignalstärke, häufig in dBm angegeben |
| Noise | Gemessener beziehungsweise geschätzter Rauschpegel |
| SNR | Abstand zwischen Nutzsignal und Rauschen |
| PHY-Rate | Ausgehandelte Bruttodatenrate der Funkverbindung |
| Durchsatz | Tatsächlich nutzbare Datenübertragungsrate |
| Roaming | Wechsel eines Clients zwischen Funkzellen |
| Band Steering | Access Point versucht, Clients in ein geeignetes Frequenzband zu lenken |
| Airtime | Anteil der Funkzeit, den Geräte für Übertragungen verwenden |
| DFS | Dynamische Kanalauswahl zum Schutz bestimmter Radarsysteme |
| Hidden SSID | SSID wird nicht regulär in Beacon-Frames angekündigt |
| 802.1X | Portbasierte Authentifizierung, häufig in Unternehmens-WLANs |
| Captive Portal | Webbasierte Freischaltung, häufig in Gastnetzen |

Mehrere Access Points können dieselbe SSID anbieten, aber jeweils eine eigene BSSID verwenden.

---

## 4. Störungsumfang zuerst bestimmen

Vor technischen Änderungen ist zu klären:

- Ist nur ein Client betroffen?
- Sind mehrere Clients am gleichen Standort betroffen?
- Ist nur eine SSID betroffen?
- Ist nur ein Access Point beziehungsweise eine BSSID betroffen?
- Tritt der Fehler nur in einem bestimmten Raum auf?
- Sind 2,4 GHz, 5 GHz oder 6 GHz unterschiedlich betroffen?
- Funktioniert die Verbindung in unmittelbarer Nähe zum Access Point?
- Tritt der Fehler nur während hoher Auslastung auf?
- Tritt er nur beim Roaming auf?
- Funktioniert Ethernet am selben Standort?
- Funktioniert das WLAN, aber nicht der Internetzugang?
- Erhalten andere Clients eine gültige DHCP-Konfiguration?

- Tritt der Fehler seit einer Treiber-, Firmware- oder Richtlinienänderung auf?
- Sind ältere oder nur neuere WLAN-Geräte betroffen?
- Betrifft der Fehler nur ein Benutzerkonto?

**Sinnvolle Vergleichsmatrix:**

| Vergleich | Erkenntnis |
|---|---|
| Gleiches Gerät, anderer Standort | Funkzelle oder Standortproblem |
| Gleiches Gerät, andere SSID | SSID-, Authentifizierungs- oder VLAN-Problem |
| Anderes Gerät, gleiche Position | Client- oder allgemeines Funkproblem |
| WLAN gegenüber Ethernet | Funkebene gegenüber allgemeinem Netzwerkproblem |
| Betroffener gegenüber funktionierendem Client | Konfigurationsunterschiede |
| Nähe zum AP gegenüber Randbereich | Signal-, Störungs- oder Roamingproblem |

## 5. Signalstärke in dBm richtig interpretieren

WLAN-Signalstärken werden häufig als negative dBm-Werte angegeben.

```
-45 dBm ist stärker als -75 dBm
```

Eine näher an null liegende Zahl bedeutet ein stärkeres Signal.

| RSSI-Beispiel | Grobe praktische Einordnung |
|---|---|
| -30 dBm | Extrem stark, meist in unmittelbarer Nähe |
| -40 bis -50 dBm | Sehr stark |
| -50 bis -60 dBm | Häufig gut für anspruchsvolle Anwendungen |
| -60 bis -67 dBm | Häufig noch brauchbar bis gut |
| -67 bis -70 dBm | Je nach Anwendung und Umgebung grenzwertig |
| -70 bis -80 dBm | Schwach, geringere Datenraten und Wiederholungen wahrscheinlich |
| unter -80 dBm | Häufig instabil oder nicht mehr sinnvoll nutzbar |

Diese Werte sind keine universellen Garantien. Antennen, Clienthardware, Kanalbreite, Störungen, Anwendung und Messverfahren beeinflussen das Ergebnis.

**Signal-Rausch-Abstand näherungsweise:**

```
SNR = Signalpegel − Rauschpegel
```

Beispiel:

```
Signal:  -60 dBm
Rauschen: -90 dBm

SNR = 30 dB
```

Ein starkes Signal kann trotzdem schlecht nutzbar sein, wenn das Rauschen oder die Kanalbelegung ebenfalls hoch ist.

---

## 6. PHY-Rate und tatsächlichen Durchsatz unterscheiden

Die angezeigte Verbindungsrate ist eine ausgehandelte Bruttodatenrate und nicht der tatsächlich nutzbare Anwendungsdurchsatz.

Abzüge entstehen unter anderem durch:

- WLAN-Protokoll-Overhead,
- Management- und Kontrollframes,
- Verschlüsselung,
- gemeinsam genutzte Funkzeit,
- Wiederholungen,
- Störungen,
- Halbduplexbetrieb,
- Entfernung,
- Kanalbreite,
- Anzahl der Spatial Streams,
- Leistungsfähigkeit des Clients,
- Auslastung des Access Points,
- TCP- und Anwendungs-Overhead.

**Deshalb gilt:**

```
PHY-Rate 866 Mbit/s
≠
866 Mbit/s nutzbarer Datendurchsatz
```

Ein Internet-Speedtest misst zusätzlich Internetanschluss, WAN, Testserver und Providerpfad. Zur reinen WLAN-Beurteilung ist ein lokaler Testserver im kabelgebundenen LAN besser geeignet.

---

## 7. Windows: WLAN-Schnittstelle und Verbindung prüfen

**WLAN-Schnittstellen und aktuelle Verbindung:**

```
[RO][SENS] netsh wlan show interfaces
```

Typische Angaben:

```
Name
Beschreibung
GUID
Physische Adresse
Status
SSID
BSSID
Netzwerktyp
Funktyp
Authentifizierung
Verschlüsselung
Kanal
Empfangsrate
Übertragungsrate
Signal
Profil
```

**Alle relevanten WLAN-Informationen:**

```
[RO][SENS] netsh wlan show all
```

**Windows-Netzwerkadapter:**

```
[RO] Get-NetAdapter |
    Format-Table Name, InterfaceDescription, Status, LinkSpeed, MacAddress
```

**IP-Konfiguration:**

```
[RO][SENS] Get-NetIPConfiguration
```

**Adapterstatistik:**

```
[RO] Get-NetAdapterStatistics |
    Format-Table Name, ReceivedBytes, SentBytes,
                 ReceivedDiscardedPackets, OutboundDiscardedPackets,
                 ReceivedPacketErrors, OutboundPacketErrors
```

Paketfehler und verworfene Pakete müssen über einen Zeitraum beziehungsweise im Vergleich zu einem funktionierenden Zustand bewertet werden.

---

## 8. Windows: sichtbare Netze, BSSIDs und Kanäle prüfen

**Sichtbare WLAN-Netze:**

```
[RO][SENS] netsh wlan show networks
```

**Sichtbare Netze einschließlich BSSIDs:**

```
[RO][SENS] netsh wlan show networks mode=bssid
```

Damit lassen sich unter anderem vergleichen:

- SSID,
- BSSID,
- Signal,
- Funktyp,
- Kanal,
- mehrere Access Points derselben SSID,
- Authentifizierungsverfahren,
- Verschlüsselungsverfahren.

**Wichtige Fragen:**

- Ist die gewünschte SSID sichtbar?
- Sind mehrere BSSIDs derselben SSID vorhanden?
- Mit welcher BSSID ist der Client verbunden?
- Ist diese BSSID am Standort sinnvoll?
- Verwendet der Client das erwartete Frequenzband?
- Befinden sich viele starke Nachbarn auf demselben Kanal?
- Wechselt die BSSID während des Fehlers?

Ein einfacher Scan ist nur eine Momentaufnahme und erkennt nicht jede Störung oder Auslastung.

---

## 9. Windows: Treiber und Fähigkeiten prüfen

**WLAN-Treiberinformationen:**

```
[RO][SENS] netsh wlan show drivers
```

Mögliche Angaben:

- Hersteller,
- Anbieter,
- Datum,
- Version,
- unterstützte Funktypen,
- unterstützte Authentifizierungs- und Verschlüsselungsverfahren,
- Treibermodell,
- unterstützte WLAN-Funktionen.

**Wireless Capabilities:**

```
[RO][SENS] netsh wlan show wirelesscapabilities
```

**PowerShell-Treiberinformationen:**

```
[RO][SENS] Get-CimInstance Win32_PnPSignedDriver |
    Where-Object DeviceClass -eq "NET" |
    Select-Object DeviceName, DriverProviderName,
```

```
DriverVersion, DriverDate
```

Treiberstände sollten mit der offiziellen Freigabe des Geräte- oder Adapterherstellers verglichen werden. Ein neuerer generischer Treiber ist nicht automatisch besser als der vom Systemhersteller freigegebene Treiber.

---

## 10. Windows: gespeicherte WLAN-Profile prüfen

**Gespeicherte Profile:**

```
[RO][SENS] netsh wlan show profiles
```

**Bestimmtes Profil anzeigen:**

```
[RO][SENS] netsh wlan show profile name="SSID-ODER-PROFILNAME"
```

Zu kontrollieren sind:

- Profilname,
- SSID,
- Verbindung automatisch oder manuell,
- Authentifizierungsverfahren,
- Verschlüsselungsverfahren,
- Richtlinienquelle,
- zufällige Hardwareadresse,
- unternehmensweite oder benutzerbezogene Bereitstellung.

**Nicht verwenden:**

```
key=clear
```

Dadurch könnte ein gespeicherter WLAN-Schlüssel im Klartext ausgegeben werden. Das ist für eine normale Fehleranalyse nicht erforderlich und darf nicht in Dokumentationen verwendet werden.

---

## 11. Windows-WLAN-Bericht erstellen

**WLAN-Bericht erzeugen:**

```
[RO][PRIV][FILE][SENS] netsh wlan show wlanreport
```

Windows zeigt nach der Erstellung den konkreten Speicherort des Berichts an. Dieser Pfad sollte aus der Ausgabe übernommen und nicht angenommen werden.

Der Bericht kann unter anderem enthalten:

- WLAN-Sitzungen,
- Verbindungs- und Trennereignisse,
- Adapterinformationen,
- Treiberdaten,
- Netzwerkprofile,
- Fehlerursachen,
- Zeitverlauf,
- Ereignisse aus relevanten Windows-Protokollen.

Der Bericht enthält sensible Netzwerkdaten und muss entsprechend geschützt werden.

**WLAN-Ereignisprotokoll prüfen:**

```
[RO][PRIV][SENS] Get-WinEvent `
    -LogName "Microsoft-Windows-WLAN-AutoConfig/Operational" `
    -MaxEvents 100
```

**Zeitlich begrenzen:**

```
[RO][PRIV][SENS] Get-WinEvent `
    -FilterHashtable @{
        LogName   = "Microsoft-Windows-WLAN-AutoConfig/Operational"
        StartTime = (Get-Date).AddMinutes(-30)
    }
```

---

## 12. Linux: WLAN-Schnittstellen und Verbindungsstatus prüfen

**Netzwerkgeräte:**

```
[RO] ip -br link
```

**NetworkManager-Gerätestatus:**

```
[RO] nmcli device status
```

**Aktive Verbindungen:**

```
[RO][SENS] nmcli connection show --active
```

**WLAN-Schnittstellen mit iw:**

```
[RO] iw dev
```

**Aktuelle Verbindung einer bestimmten Schnittstelle:**

```
[RO][SENS] iw dev wlan0 link
```

`wlan0` muss durch den tatsächlich ermittelten Schnittstellennamen ersetzt werden.

Typische Angaben von `iw dev wlan0 link`:

```
BSSID
SSID
Frequenz
RX-Daten
TX-Daten
Signal
RX-Bitrate
TX-Bitrate
```

**Stationsinformationen:**

```
[RO][SENS] iw dev wlan0 station dump
```

Abhängig von Treiber und Betriebsmodus können zusätzliche Werte wie Signal, Bitrate, Wiederholungen und übertragene Daten angezeigt werden.

---

## 13. Linux: sichtbare Netze und Funkumgebung prüfen

**WLAN-Scan mit NetworkManager:**

```
[TEST][SENS] nmcli device wifi list
```

**Scan für eine bestimmte Schnittstelle:**

```
[TEST][SENS] nmcli device wifi list ifname wlan0
```

**Ausgewählte Felder anzeigen:**

```
[TEST][SENS] nmcli -f IN-USE,SSID,BSSID,MODE,CHAN,FREQ,RATE,SIGNAL,SECURITY \
  device wifi list
```

**Regulierungsdomäne prüfen:**

```
[RO] iw reg get
```

**WLAN-Fähigkeiten des Adapters:**

```
[RO][SENS] iw list
```

`iw list` kann eine sehr umfangreiche Ausgabe erzeugen. Relevant sind unter anderem:

- unterstützte Bänder,
- Frequenzen,
- Kanalbreiten,
- Schnittstellenmodi,
- Verschlüsselungsfähigkeiten,
- räumliche Streams,
- regulatorische Einschränkungen.

Die Regulierungsdomäne darf nicht willkürlich verändert werden. Zulässige Kanäle und Sendeleistungen sind landesabhängig reguliert.

---

## 14. Linux: NetworkManager-Protokolle auswerten

**Aktuelle NetworkManager-Protokolle:**

```
[RO][PRIV][SENS] sudo journalctl -u NetworkManager --since "-30 minutes"
```

**WLAN-bezogene Kernelmeldungen:**

```
[RO][PRIV][SENS] sudo journalctl -k --since "-30 minutes" |
    grep -Ei 'wlan|wifi|wireless|80211|firmware'
```

**Treiberzuordnung der Netzwerkschnittstellen:**

```
[RO][SENS] lspci -k |
    grep -A 4 -Ei 'network|wireless'
```

Bei USB-WLAN-Adaptern:

```
[RO][SENS] lsusb
```

Zu suchen sind unter anderem:

- Firmware konnte nicht geladen werden,
- Authentifizierung fehlgeschlagen,
- Verbindung wurde getrennt,
- DHCP fehlgeschlagen,
- Access Point nicht erreichbar,
- regulatorische Einschränkung,
- Treiberabsturz,
- Energiesparzustand,
- Roamingereignis.

---

## 15. macOS: WLAN-Schnittstelle und Verbindung prüfen

**Hardwareports und Gerätenamen anzeigen:**

```
[RO] networksetup -listallhardwareports
```

Dadurch wird ermittelt, welche Schnittstelle zum WLAN gehört, beispielsweise `en0` oder `en1`. Der Name darf nicht ohne Prüfung vorausgesetzt werden.

**Aktuell verbundenes WLAN:**

```
[RO][SENS] networksetup -getairportnetwork en0
```

`en0` muss durch die tatsächlich ermittelte WLAN-Schnittstelle ersetzt werden.

**Ausführliche WLAN- und Hardwareinformationen:**

```
[RO][SENS] system_profiler SPAirPortDataType
```

**IP-Konfiguration:**

```
[RO][SENS] ifconfig en0
```

**Netzwerkdienstkonfiguration:**

```
[RO][SENS] networksetup -getinfo "Wi-Fi"
```

`Wi-Fi` muss durch den tatsächlichen Namen des Netzwerkdienstes ersetzt werden.

---

## 16. macOS: aktuelle WLAN-Diagnoseinformationen prüfen

Auf aktuellen macOS-Versionen kann `wdutil` WLAN-Diagnoseinformationen bereitstellen.

**Verfügbarkeit und Hilfe prüfen:**

```
[RO] command -v wdutil
```

```
[RO] wdutil help
```

**Aktuelle Diagnoseinformationen, sofern von der installierten Version unterstützt:**

```
[RO][PRIV][SENS] sudo wdutil info
```

Die verfügbaren Unterbefehle und Ausgaben können sich zwischen macOS-Versionen unterscheiden. Deshalb muss zuerst die lokale Hilfe geprüft werden.

Mögliche Informationen sind:

- SSID,
- BSSID,
- Kanal,
- Signal,
- Rauschpegel,
- Übertragungsrate,
- Sicherheitsverfahren,
- Schnittstelle.

Ältere Anleitungen verwenden häufig das interne `airport`-Werkzeug. Dessen Verfügbarkeit und Verhalten ist auf aktuellen macOS-Versionen nicht zuverlässig vorauszusetzen; deshalb wird es hier nicht als Standardbefehl verwendet.

---

## 17. macOS Wireless Diagnostics verwenden

Apple stellt die grafische Anwendung „Diagnose für drahtlose Umgebungen“ beziehungsweise „Wireless Diagnostics“ bereit.

**Aufruf:**

1. Mit dem problematischen WLAN verbinden, soweit möglich.
2. Wahltaste beziehungsweise `Option` gedrückt halten.
3. Auf das WLAN-Symbol in der Menüleiste klicken.
4. „Diagnose für drahtlose Umgebungen öffnen“ auswählen.
5. Den Anweisungen folgen.

Apple gibt an, dass die Diagnose selbst die Netzwerkeinstellungen nicht verändert.

Die Diagnose kann ein komprimiertes Archiv erzeugen. Apple dokumentiert dafür:

```
/var/tmp
```

Der Dateiname beginnt mit:

```
WirelessDiagnostics
```

und endet mit:

```
.tar.gz
```

Das Archiv kann umfangreiche und sensible System- und Netzwerkdaten enthalten und darf nur geschützt weitergegeben werden.

---

## 18. Frequenzbänder praktisch unterscheiden

| Eigenschaft | 2,4 GHz | 5 GHz | 6 GHz |
|---|---|---|---|
| Reichweite | Häufig größer | Häufig geringer als 2,4 GHz | Häufig stärker durch Entfernung und Hindernisse beeinflusst |
| Kanalkapazität | Begrenzter | Mehr verfügbare Kanalressourcen | Große zusätzliche Frequenzressourcen |
| Störquellen | Viele WLAN- und Nicht-WLAN-Geräte | Häufig weniger Nicht-WLAN-Störungen | Abhängig von regionaler Freigabe und Nutzung |
| Wanddurchdringung | Häufig günstiger | Häufig geringer | Häufig geringer |
| Geräteunterstützung | Sehr weit verbreitet | Weit verbreitet | Nur geeignete neuere Geräte |
| Kanalbreiten | Häufig 20 oder 40 MHz | Häufig 20 bis 160 MHz | Abhängig von Standard und Gerät auch sehr breite Kanäle |

Die tatsächlich nutzbaren Frequenzen und Kanalbreiten hängen von Land, Gerät, Treiber, Access Point und WLAN-Standard ab.

**Typischer Zielkonflikt:**

```
Breitere Kanäle
→ potenziell höhere Datenrate
```

→ benötigen mehr Frequenzspektrum

→ höhere Wahrscheinlichkeit von Überlappungen oder Störungen

## 19. Kanalbelegung und Störungen beurteilen

Ein WLAN-Kanal ist ein gemeinsam genutztes Medium. Alle Geräte auf demselben oder überlappenden Kanal teilen sich die verfügbare Funkzeit.

Mögliche Störquellen:

- benachbarte WLANs,
- Bluetooth,
- Mikrowellengeräte,
- Funkkameras,
- drahtlose Audio- oder Videoübertragung,
- USB-3-Geräte und schlecht abgeschirmte Kabel im 2,4-GHz-Umfeld,
- Radarerkennung auf DFS-Kanälen,
- defekte oder stark sendende Geräte,
- sehr breite Kanalbelegung,
- versteckte Stationen.

**Co-Channel-Interference:**

Mehrere WLANs verwenden denselben Kanal und müssen sich die Funkzeit teilen.

**Adjacent-Channel-Interference:**

Überlappende Kanäle beeinflussen sich, ohne sauber koordiniert zu werden.

Im 2,4-GHz-Band werden bei 20-MHz-Kanalbreite häufig überlappungsarme Planungen verwendet. Welche Kanäle zulässig und sinnvoll sind, hängt von der regionalen Regulierung und dem vorhandenen Kanalplan ab.

Ein Scan zeigt andere WLANs, aber nicht zuverlässig alle Nicht-WLAN-Störquellen. Dafür kann ein geeigneter Spektrumanalysator erforderlich sein.

## 20. DFS-Ereignisse berücksichtigen

Bestimmte 5-GHz-Kanäle unterliegen Dynamic Frequency Selection. Erkennt ein Access Point ein relevantes Radarsignal, kann er den Kanal wechseln oder die Aussendung vorübergehend

einstellen.

**Mögliche Symptome:**

- WLAN verschwindet kurzfristig,
- Clients werden gleichzeitig getrennt,
- Access Point wechselt den Kanal,
- nur bestimmte 5-GHz-Kanäle sind betroffen,
- Verbindung kehrt nach einer Wartezeit zurück,
- Ereignis tritt standortabhängig auf.

Zu prüfen sind:

- Access-Point-Ereignisprotokolle,
- Controllerereignisse,
- Kanalverlauf,
- DFS- beziehungsweise Radarereignisse,
- automatischer Kanalwechsel,
- Clientunterstützung des neuen Kanals.

DFS darf nicht pauschal als Fehler betrachtet werden. Es handelt sich um eine regulatorisch vorgesehene Schutzfunktion.

---

## 21. Authentifizierung und Verschlüsselung prüfen

Mögliche WLAN-Sicherheitsverfahren:

- WPA2-Personal,
- WPA3-Personal,
- WPA2-Enterprise,
- WPA3-Enterprise,
- Übergangsmodi,
- 802.1X/EAP,
- Enhanced Open beziehungsweise OWE,
- offene Gastnetze mit Captive Portal.

Zu kontrollieren sind:

- unterstützt der Client das Verfahren,
- stimmt das Kennwort,
- wird ein altes Profil verwendet,
- ist WPA3 erforderlich oder optional,
- ist Protected Management Frames erforderlich,

- funktioniert die 802.1X-Authentifizierung,
- ist das Serverzertifikat vertrauenswürdig,
- stimmt der Servername im Zertifikat,
- ist das Benutzer- oder Gerätezertifikat gültig,
- ist das Benutzerkonto gesperrt,
- ist das Gerät durch Richtlinie zugelassen,
- ist die Systemzeit korrekt.

**Systemzeit:**

| Betriebssystem | Befehl |
|---|---|
| Windows | [RO] Get-Date -Format o |
| Linux | [RO] date --iso-8601=seconds |
| macOS | [RO] date "+%Y-%m-%dT%H:%M:%S%z" |

Bei Zertifikats- und Kerberos-basierten Verfahren kann eine falsche Systemzeit die Anmeldung verhindern.

---

## 22. 802.1X- und Enterprise-WLAN eingrenzen

Ein Enterprise-WLAN kann mehrere Komponenten enthalten:

```
WLAN-Client
   ↓
Access Point
   ↓
WLAN-Controller
   ↓
RADIUS-Server
   ↓
Identitätsdienst
   ↓
VLAN- und Zugriffsrichtlinie
```

Zu dokumentieren sind:

- Benutzer- oder Geräteauthentifizierung,
- EAP-Verfahren,
- Zertifikatsaussteller,

- Identität beziehungsweise anonyme Identität,
- RADIUS-Antwort,
- zugewiesenes VLAN,
- angewendete Rolle,
- Access-Control-List,
- Zeitpunkt,
- Access Point und BSSID.

**Typische Fehler:**

| Beobachtung | Mögliche Ursache |
|---|---|
| Kennwortabfrage wiederholt sich | Zugangsdaten, EAP oder Zertifikatsprüfung |
| Zertifikatswarnung | Vertrauenskette oder Serveridentität |
| Verbindung hergestellt, falsches Netz | Dynamische VLAN-Zuweisung oder Richtlinie |
| Nur Gerätetunnel vor Anmeldung fehlt | Computerzertifikat oder Geräteauthentifizierung |
| Benutzer funktioniert auf anderem Gerät | Gerätezertifikat, Profil oder Gerätekonformität |
| Alle Benutzer an einem AP betroffen | AP-, Controller- oder Netzwerkpfad zum RADIUS |

Client-, Controller- und RADIUS-Protokolle müssen zeitlich miteinander verglichen werden.

---

## 23. Nach der WLAN-Verbindung DHCP prüfen

**Windows:**

```
[RO][SENS] Get-NetIPConfiguration
```

```
[RO][SENS] ipconfig /all
```

**Linux:**

```
[RO][SENS] ip -br address
```

```
[RO] ip route show
```

**macOS:**

```
[RO][SENS] networksetup -getinfo "Wi-Fi"
```

```
[RO][SENS] ifconfig en0
```

Zu kontrollieren sind:

- gültige IP-Adresse,
- Präfix beziehungsweise Subnetzmaske,
- Standardgateway,
- DHCP-Server,
- DNS-Server,
- Lease-Zeit,
- richtige VLAN-Zuweisung,
- IPv4- und IPv6-Konfiguration.

**Typisches Fehlerbild:**

```
WLAN-Authentifizierung erfolgreich
↓
Client wird dem falschen VLAN zugeordnet
↓
DHCP-Server nicht erreichbar oder falscher Adressbereich
↓
Kein nutzbarer Netzwerkzugang
```

Eine IPv4-Adresse aus `169.254.0.0/16` weist häufig darauf hin, dass keine reguläre IPv4-DHCP-Zuweisung erfolgt ist.

---

## 24. Gateway, DNS und Internet getrennt testen

### Stufe 1 – eigene IP-Konfiguration prüfen

```
IP-Adresse
Subnetzmaske beziehungsweise Präfix
Standardgateway
DNS-Server
```

**Stufe 2 – Standardgateway testen**

Windows:

```
[TEST] Test-Connection GATEWAY_IP -Count 4
```

Linux und macOS:

```
[TEST] ping -c 4 GATEWAY_IP
```

**Stufe 3 – externe IP-Adresse testen:**

Windows:

```
[TEST] Test-NetConnection 1.1.1.1 -Port 443
```

Linux und macOS:

```
[TEST] nc -vz -w 5 1.1.1.1 443
```

**Stufe 4 – DNS-Auflösung testen**

Windows:

```
[TEST] Resolve-DnsName example.com
```

Linux und macOS:

```
[TEST] dig example.com
```

**Stufe 5 – Anwendung testen**

```
[TEST] curl -I https://example.com/
```

Öffentliche Testziele dürfen nur verwendet werden, wenn dies durch die betrieblichen Richtlinien erlaubt ist.

## 25. Captive Portal erkennen

Gast-, Hotel- und öffentliche WLANs verlangen häufig eine browserbasierte Freischaltung.

**Typische Symptome:**

- WLAN ist verbunden,
- IP-Adresse und Gateway sind vorhanden,
- Internetzugriff funktioniert nicht,
- Browser wird auf eine Anmeldeseite umgeleitet,
- HTTPS-Seiten zeigen Fehler,
- VPN-Verbindung kann nicht aufgebaut werden,
- DNS-Antworten werden verändert.

Zu prüfen sind:

- wurde die Nutzungsseite vollständig bestätigt,
- ist die Sitzung abgelaufen,
- wurde das Gerät anhand seiner MAC-Adresse registriert,
- verwendet der Client eine zufällige MAC-Adresse,
- blockiert ein VPN oder Proxy die Portalerkennung,
- ist die Systemzeit korrekt,
- wurde die maximal zulässige Gerätezahl erreicht?

Zertifikatswarnungen auf HTTPS-Seiten dürfen nicht einfach bestätigt werden. Für die Portalanmeldung sollte die vom Betreiber vorgesehene sichere Methode verwendet werden.

---

## 26. Zufällige MAC-Adressen berücksichtigen

Moderne Betriebssysteme können pro WLAN eine private beziehungsweise zufällige MAC-Adresse verwenden.

Das kann folgende Auswirkungen haben:

- DHCP vergibt eine neue Adresse,
- Captive Portal erkennt ein neues Gerät,
- MAC-basierte Freigabe greift nicht,
- NAC behandelt das Gerät als unbekannt,
- Gerät erscheint mehrfach im Controller,
- statische DHCP-Reservierung passt nicht,
- Inventarisierung wird erschwert.

**Windows-Status anzeigen:**

```
[RO][SENS] netsh wlan show randomization
```

**Windows-Schnittstellenadresse:**

```
[RO] Get-NetAdapter |
    Format-Table Name, MacAddress, Status
```

**Linux:**

```
[RO] ip link show
```

**macOS:**

```
[RO] ifconfig en0
```

Die aktuelle Schnittstellenadresse allein zeigt nicht zwingend, ob und nach welchem Verfahren sie für ein bestimmtes WLAN erzeugt wurde. Die Einstellung sollte zusätzlich in der WLAN-Konfiguration des Betriebssystems geprüft werden.

Private MAC-Adressen dürfen nicht pauschal deaktiviert werden. Ihre Nutzung ist eine Datenschutz- und Netzwerkdesignentscheidung.

---

## 27. Roamingprobleme analysieren

Beim Roaming entscheidet der Client normalerweise selbst, wann er zu einer anderen Funkzelle wechselt. Access Points und Controller können diese Entscheidung unterstützen oder beeinflussen.

**Typische Symptome:**

- Verbindung bricht beim Wechsel zwischen Räumen ab,
- Sprach- oder Videokonferenz stockt beim Laufen,
- Client bleibt an einem weit entfernten Access Point hängen,
- BSSID wechselt häufig hin und her,
- Problem tritt nur bei bestimmten Clientmodellen auf,
- Anmeldung wird bei jedem AP-Wechsel wiederholt,
- IP-Adresse ändert sich beim Roaming.

Zu dokumentieren sind:

- SSID,
- alte BSSID,
- neue BSSID,
- Kanal und Band,
- Signal vor dem Wechsel,
- Signal nach dem Wechsel,
- Zeitpunkt und Dauer der Unterbrechung,
- zugewiesenes VLAN,
- IP-Adresse vor und nach dem Wechsel,
- unterstützte Roamingfunktionen,
- Clienttreiber und Firmware.

**Wichtige Standards und Funktionen:**

| Funktion | Aufgabe |
|---|---|
| 802.11k | Informationen über benachbarte Funkzellen |
| 802.11v | Unterstützung bei Netzwerkauswahl und Übergängen |
| 802.11r | Beschleunigte Übergänge zwischen Access Points |
| PMK-Caching | Wiederverwendung bestimmter Authentifizierungsinformationen |

Unterstützung und Verhalten hängen von Client, Access Point, Sicherheitsverfahren und Konfiguration ab.

---

## 28. Sticky Clients und Ping-Pong-Roaming erkennen

**Sticky Client:**

> Client bleibt mit schwacher BSSID verbunden
> obwohl eine nähere BSSID verfügbar ist

Mögliche Ursachen:

- Roamingentscheidung des Clients,
- Treibereinstellung,
- Sendeleistung der Access Points,
- ungünstige Zellüberlappung,
- fehlende beziehungsweise inkompatible Roamingunterstützung,

- zu niedrige Datenraten weiterhin erlaubt.

**Ping-Pong-Roaming:**

```
Client wechselt wiederholt zwischen zwei BSSIDs
```

Mögliche Ursachen:

- ähnliche Signalstärke,
- schwankende Funkbedingungen,
- ungeeignete Schwellenwerte,
- übermäßige Zellüberlappung,
- Band-Steering-Konflikte,
- Clienttreiber.

Ein erzwungenes Trennen des Clients kann kurzfristig helfen, beweist aber keine nachhaltige Fehlerbehebung.

---

## 29. Energiesparfunktionen berücksichtigen

WLAN-Adapter und Betriebssysteme können die Funkhardware zum Energiesparen in reduzierte Betriebszustände versetzen.

**Typische Symptome:**

- Verbindung bricht im Akkubetrieb ab,
- nach Standby kein Netzwerkzugang,
- hoher erster Paketverlust nach Inaktivität,
- Verbindung ist nach Deaktivieren und Aktivieren des Adapters wieder vorhanden,
- Problem tritt nur bei bestimmten Energiesparprofilen auf.

**Windows-Energiezustände:**

```
[RO] powercfg /getactivescheme
```

**Windows-WLAN-Bericht:**

```
[RO][PRIV][FILE][SENS] netsh wlan show wlanreport
```

**Linux:**

```
[RO] iw dev wlan0 get power_save
```

Nicht jeder Treiber unterstützt dieselbe Abfrage.

**macOS:**

```
[RO] pmset -g
```

Energiesparfunktionen sollten nicht dauerhaft deaktiviert werden, bevor Treiber, Firmware und das konkrete Fehlerbild geprüft wurden.

---

## 30. Paketverlust und Latenz lokal messen

Zuerst wird das lokale Standardgateway getestet. Dadurch bleiben Internetprovider und externe Netze zunächst außerhalb der Messung.

**Windows:**

```
[TEST] Test-Connection GATEWAY_IP -Count 50
```

Alternativ:

```
[TEST] ping -n 50 GATEWAY_IP
```

**Linux und macOS:**

```
[TEST] ping -c 50 GATEWAY_IP
```

Zu bewerten sind:

- Paketverlust,
- minimale Latenz,
- durchschnittliche Latenz,
- maximale Latenz,
- starke Schwankungen,
- zeitlicher Zusammenhang mit Bewegung oder Last.

**Wichtig:** Access Points oder Gateways können ICMP niedriger priorisieren. Ein Ping-Test ist deshalb ein Hinweis, aber keine vollständige Qualitätsmessung.

---

## 31. Durchsatz im lokalen Netz mit iperf3 testen

Ein lokaler kabelgebundener `iperf3`-Server hilft, WLAN und Internetanschluss voneinander zu trennen.

**Auf dem autorisierten kabelgebundenen Testserver:**

```
[TEST] iperf3 -s
```

**Auf dem WLAN-Client:**

```
[TEST] iperf3 -c SERVER_IP
```

**Gegenrichtung testen:**

```
[TEST] iperf3 -c SERVER_IP -R
```

**Bestimmte Testdauer:**

```
[TEST] iperf3 -c SERVER_IP -t 30
```

**UDP-Test mit begrenzter Zielrate:**

```
[TEST] iperf3 -c SERVER_IP -u -b 20M -t 30
```

UDP-Tests erzeugen gezielt Last und müssen mit einer angemessenen Bandbreite begonnen werden.

Zu dokumentieren sind:

- Standort des Clients,
- SSID und BSSID,
- Frequenzband,
- Kanal,

- Signal,
- PHY-Rate,
- TCP-Durchsatz in beide Richtungen,
- UDP-Verlust und Jitter,
- Anzahl paralleler Clients,
- Uhrzeit.

---

## 32. Internet-Speedtest nicht mit WLAN-Messung verwechseln

Ein Internet-Speedtest umfasst:

```
WLAN
+ lokales LAN
+ Router
+ Firewall
+ Internetanschluss
+ Provider
+ Routing zum Testserver
+ Testserver
```

Ein schlechtes Ergebnis kann daher auch bei einem fehlerfreien WLAN entstehen.

**Empfohlene Reihenfolge:**

1. WLAN-Signal und Verbindungsparameter prüfen.
2. Lokales Gateway testen.
3. Lokalen kabelgebundenen `iperf3`-Server testen.
4. Erst danach Internetdurchsatz messen.
5. WLAN- und Ethernetmessung zum selben Ziel vergleichen.
6. Messung zu mehreren Zeitpunkten wiederholen.

Die Aussage „WLAN liefert nur 50 Mbit/s“ ist ohne lokalen Vergleich nicht ausreichend belegt.

---

## 33. Airtime und hohe Clientdichte berücksichtigen

WLAN ist ein geteiltes Medium. Auch langsam sendende Clients verbrauchen Funkzeit.

Mögliche Ursachen hoher Airtime-Auslastung:

- viele aktive Clients,
- langsame oder weit entfernte Clients,
- viele Wiederholungen,
- niedrige Basisdatenraten,
- Broadcast- und Multicastverkehr,
- breite Kanäle mit Störungen,
- Legacy-Geräte,
- hohe Datenübertragungen,
- mehrere SSIDs mit Management-Overhead,
- schlecht platzierte Access Points.

**Typische Symptome:**

- starkes Signal, aber geringer Durchsatz,
- hohe Latenz unter Last,
- Problem nur zu bestimmten Uhrzeiten,
- alle Clients einer Funkzelle betroffen,
- andere Funkzellen funktionieren,
- viele Wiederholungen und wechselnde Datenraten.

Für eine zuverlässige Bewertung werden Controllerstatistiken oder geeignete WLAN-Analysewerkzeuge benötigt.

---

## 34. Access Point, Switch und VLAN gemeinsam prüfen

Ein Access Point benötigt selbst eine funktionierende kabelgebundene Infrastruktur.

Zu prüfen sind:

- AP-Stromversorgung beziehungsweise PoE,
- Ethernet-Link,
- Linkgeschwindigkeit,
- Switchportfehler,
- VLAN-Trunk,
- native beziehungsweise untagged VLAN-Zuweisung,
- Management-VLAN,
- SSID-zu-VLAN-Zuordnung,
- DHCP-Relay,
- Controllererreichbarkeit,
- AP-Firmware,
- Uplink-Auslastung.

**Typisches Fehlerbild:**

```
Client verbindet sich erfolgreich mit SSID
↓
Access Point ordnet Client falschem VLAN zu
↓
Client erhält keine oder falsche IP-Konfiguration
```

**Switchportzähler beachten:**

- CRC-Fehler,
- Drops,
- Duplexprobleme,
- Link-Flaps,
- PoE-Unterbrechungen,
- Port-Security-Ereignisse,
- Spanning-Tree-Ereignisse.

Ein scheinbares Funkproblem kann tatsächlich auf dem kabelgebundenen AP-Uplink entstehen.

---

## 35. Mesh- und Repeater-Probleme erkennen

Bei Mesh-Systemen und Repeatern wird Verkehr zusätzlich über einen drahtlosen oder kabelgebundenen Backhaul übertragen.

```
Client
  ↓ WLAN
Mesh-Knoten oder Repeater
  ↓ Backhaul
Haupt-Access-Point
  ↓ LAN
Ziel
```

Zu prüfen sind:

- Qualität des Clientlinks,
- Qualität des Backhauls,
- kabelgebundener oder drahtloser Backhaul,
- verwendetes Frequenzband,
- mehrere Funkübertragungen desselben Datenpakets,
- Position des Repeaters,

- Roaming zwischen Hauptgerät und Repeater,
- Kanalplanung,
- Uplink-Auslastung,
- Firmwarestand.

Ein Repeater mit starkem Signal zum Client kann trotzdem eine schlechte Gesamtverbindung liefern, wenn sein eigener Uplink schwach ist.

---

## 36. Versteckte SSIDs und Netzwerkprofile beurteilen

Eine versteckte SSID verbessert die Verschlüsselung nicht. Clients müssen möglicherweise aktiv nach dem bekannten Netz suchen.

Mögliche Nachteile:

- erschwerte Diagnose,
- zusätzliche Probe Requests,
- Verbindungsprobleme bei fehlerhaftem Profil,
- Datenschutzprobleme durch aktive Suche,
- nicht einheitliches Verhalten verschiedener Clients.

Zu prüfen sind:

- SSID exakt geschrieben,
- Sicherheitsverfahren korrekt,
- Netzwerkprofil aktuell,
- automatische Verbindung vorgesehen,
- Richtlinienprofil vorhanden,
- Access Point sendet die erwartete Konfiguration.

Das Löschen und Neuerstellen eines Profils ist eine Änderung. Vorher sollten Profilquelle, Unternehmensrichtlinie und Zugangsdaten geklärt werden.

---

## 37. Keine vorschnellen WLAN-Änderungen durchführen

Nicht unkontrolliert:

- WLAN-Profil löschen,
- Kennwort im Klartext exportieren,
- Access Point neu starten,
- Kanal oder Kanalbreite beliebig ändern,

- Regulierungsdomäne verändern,
- Sendeleistung maximieren,
- WPA3 oder 802.1X deaktivieren,
- Zertifikatsprüfung umgehen,
- private MAC-Adresse pauschal deaktivieren,
- Treiber ungeprüft ersetzen,
- Controllerkonfiguration ändern,
- Roamingfunktionen abschalten,
- Funknetz während der Geschäftszeit neu planen.

**Sicherer Ablauf:**

1. Istzustand und Standort dokumentieren.
2. SSID, BSSID, Kanal, Band und Signal erfassen.
3. Fehler reproduzieren.
4. Client und Vergleichsgerät prüfen.
5. Authentifizierung und VLAN-Zuweisung kontrollieren.
6. DHCP, Gateway und DNS testen.
7. Lokalen Durchsatz messen.
8. Client-, AP-, Controller- und RADIUS-Protokolle vergleichen.
9. Ursache nachweisen.
10. Änderung genehmigen lassen.
11. Auswirkung auf andere Funkzellen und Clients berücksichtigen.
12. Nachprüfung am ursprünglichen Fehlerort durchführen.

---

## 38. Systematischer Diagnoseablauf

| Schritt | Prüfung | Leitfrage |
|---|---|---|
| 1 | Störungsumfang bestimmen | Client, Standort, BSSID, SSID oder gesamtes WLAN? |
| 2 | Hardwarestatus prüfen | Wird der WLAN-Adapter korrekt erkannt? |
| 3 | Treiber und Fähigkeiten prüfen | Unterstützt der Client Band und Sicherheitsverfahren? |
| 4 | Funkumgebung erfassen | Ist die SSID sichtbar und wie stark ist das Signal? |
| 5 | BSSID und Kanal dokumentieren | Mit welcher Funkzelle ist der Client verbunden? |
| 6 | Authentifizierung prüfen | Wird Personal- oder Enterprise-Anmeldung akzeptiert? |

| Schritt | Prüfung | Leitfrage |
|---|---|---|
| 7 | VLAN-Zuweisung prüfen | Landet der Client im vorgesehenen Netz? |
| 8 | IP-Konfiguration prüfen | Sind Adresse, Gateway und DNS korrekt? |
| 9 | Gateway testen | Funktioniert der lokale Netzwerkpfad? |
| 10 | DNS testen | Werden Namen korrekt aufgelöst? |
| 11 | Anwendung testen | Funktioniert der tatsächlich benötigte Dienst? |
| 12 | Paketverlust messen | Ist die Funkverbindung stabil? |
| 13 | Lokalen Durchsatz messen | Welche Leistung liefert nur das WLAN? |
| 14 | Roaming prüfen | Tritt der Fehler beim BSSID-Wechsel auf? |
| 15 | Kanal und Auslastung prüfen | Ist die Funkzelle gestört oder überlastet? |
| 16 | AP-Uplink prüfen | Funktioniert die kabelgebundene Infrastruktur? |
| 17 | Protokolle vergleichen | Welche Komponente lehnt ab oder trennt? |
| 18 | Minimale Änderung planen | Welche konkrete Korrektur stellt den Sollzustand her? |
| 19 | Nachprüfung | Funktioniert es am ursprünglichen Standort unter Last? |
| 20 | Dokumentation | Sind Ursache, Messwerte und Änderung festgehalten? |

## 39. Kompakte Befehlstabelle

| Aufgabe | Windows | Linux | macOS |
|---|---|---|---|
| WLAN-Verbindungsstatus | `[RO][SENS] netsh wlan show interfaces` | `[RO][SENS] iw dev wlan0 link` | `[RO][SENS] networksetup -getairportnetwork en0` |
| Netzwerkschnittstellen | `[RO] Get-NetAdapter` | `[RO] ip -br link` | `[RO] networksetup -listallhardwareports` |
| Sichtbare WLANs | `[RO][SENS] netsh wlan show networks mode=bssid` | `[TEST][SENS] nmcli device wifi list` | Wireless Diagnostics beziehungsweise `[RO][PRIV][SENS] sudo wdutil info`, falls unterstützt |

| Aufgabe | Windows | Linux | macOS |
|---|---|---|---|
| WLAN-Treiber | `[RO][SENS] netsh wlan show drivers` | `[RO][SENS] lspci -k` beziehungsweise `[RO][SENS] lsusb` | `[RO][SENS] system_profiler SPAirPortDataType` |
| WLAN-Fähigkeiten | `[RO][SENS] netsh wlan show wirelesscapabilities` | `[RO][SENS] iw list` | `[RO][SENS] system_profiler SPAirPortDataType` |
| Gespeicherte Profile | `[RO][SENS] netsh wlan show profiles` | `[RO][SENS] nmcli connection show` | Über WLAN-Einstellungen beziehungsweise MDM prüfen |
| IP-Konfiguration | `[RO][SENS] Get-NetIPConfiguration` | `[RO][SENS] ip -br address` | `[RO][SENS] networksetup -getinfo "Wi-Fi"` |
| Standardroute | `[RO] Get-NetRoute -DestinationPrefix "0.0.0.0/0"` | `[RO] ip route show default` | `[RO] route -n get default` |
| DNS-Konfiguration | `[RO][SENS] Get-DnsClientServerAddress` | `[RO][SENS] resolvectl status` | `[RO][SENS] scutil --dns` |
| Adapterstatistik | `[RO] Get-NetAdapterStatistics` | `[RO][SENS] iw dev wlan0 station dump` | Abhängig von macOS-Version: `wdutil` prüfen |
| WLAN-Protokoll | `[RO][PRIV][SENS] Get-WinEvent -LogName "Microsoft-Windows-WLAN-AutoConfig/Operational"` | `[RO][PRIV][SENS] sudo journalctl -u NetworkManager` | Wireless Diagnostics |
| WLAN-Bericht | `[RO][PRIV][FILE][SENS] netsh wlan show wlanreport` | Protokolle und Befehlsausgaben getrennt sichern | Wireless Diagnostics erzeugt Diagnosearchiv |
| Gatewaytest | `[TEST] Test-Connection GATEWAY_IP -Count 20` | `[TEST] ping -c 20 GATEWAY_IP` | `[TEST] ping -c 20 GATEWAY_IP` |
| Lokaler Durchsatz | `[TEST] iperf3 -c SERVER_IP` | `[TEST] iperf3 -c SERVER_IP` | `[TEST] iperf3 -c SERVER_IP` |

`wlan0`, `en0`, `Wi-Fi`, `GATEWAY_IP` und `SERVER_IP` müssen durch die tatsächlich ermittelten Werte ersetzt werden.

---

## 40. Dokumentationsvorlage für WLAN-Fehler

Störung:

Zeitpunkt:

Zeitzone:

Standort:

Raum beziehungsweise Bereich:

Benutzer:

Client:

Betriebssystem:

WLAN-Adapter:

Treiberversion:

SSID:

BSSID:

Access Point:

Frequenzband:

Frequenz:

Kanal:

Kanalbreite:

WLAN-Standard:

Signal beziehungsweise RSSI:

Rauschpegel:

SNR:

TX-PHY-Rate:

RX-PHY-Rate:

Sicherheitsverfahren:

Authentifizierung erfolgreich:

802.1X-Verfahren:

RADIUS-Ergebnis:

Zugewiesenes VLAN:

Client-IP-Adresse:

Präfix:

Standardgateway:

DHCP-Server:

DNS-Server:

IPv6-Konfiguration:

Gatewaytest:

Paketverlust:

Latenz:

DNS-Test:

Anwendungstest:

Lokaler iperf3-Test:

Internettest:

Captive Portal:

Private MAC-Adresse:

Alte BSSID vor Roaming:

Neue BSSID nach Roaming:

Unterbrechungsdauer:

Roamingzeitpunkt:

Vergleichsgerät:

Vergleich an anderem Standort:

Vergleich über Ethernet:

Andere Clients betroffen:

Andere SSIDs betroffen:

Access-Point-Protokoll:

Controllerprotokoll:

RADIUS-Protokoll:

Switchportstatus:

PoE-Status:

Uplinkfehler:

DFS-Ereignis:

Kanalauslastung:

Festgestellte Ursache:

Genehmigte Änderung:

Rückfallplan:

Ergebnis der Nachprüfung:

---

## 41. Kontrollfragen nach der Diagnose

- Ist nur ein Client, Standort, Access Point oder die gesamte SSID betroffen?
- Wird der WLAN-Adapter fehlerfrei erkannt?
- Unterstützt der Client das verwendete Band und Sicherheitsverfahren?
- Ist die gewünschte SSID sichtbar?
- Mit welcher BSSID ist der Client verbunden?
- Stimmen Frequenzband, Kanal und Kanalbreite?
- Wie hoch sind Signal, Rauschen und SNR?
- Ist die angezeigte PHY-Rate plausibel?
- Wird die Authentifizierung erfolgreich abgeschlossen?

- Ist bei Enterprise-WLAN das Zertifikat gültig?
- Wird das vorgesehene VLAN zugewiesen?
- Erhält der Client eine gültige IP-Konfiguration?
- Ist das Standardgateway erreichbar?
- Funktioniert DNS?
- Funktioniert die Anwendung über IP-Adresse und Hostname?
- Tritt Paketverlust bereits zum lokalen Gateway auf?
- Wurde der lokale Durchsatz unabhängig vom Internet gemessen?
- Tritt der Fehler nur bei hoher Auslastung auf?
- Tritt er beim Wechsel der BSSID auf?
- Bleibt der Client an einer weit entfernten BSSID hängen?
- Wurden DFS- und Kanalwechselereignisse geprüft?
- Ist der kabelgebundene Uplink des Access Points fehlerfrei?
- Wurden Client-, AP-, Controller- und RADIUS-Protokolle zeitlich verglichen?
- Wurde die Ursache vor einer Kanal-, Profil- oder Sicherheitsänderung nachgewiesen?
- Wurde nach der Änderung am ursprünglichen Fehlerort erneut gemessen?

---

## 42. Quellen und weiterführende Dokumentation

- Microsoft Learn – `netsh wlan`: https://learn.microsoft.com/windows-server/administration/windows-commands/netsh-wlan
- Microsoft Support – WLAN-Bericht unter Windows analysieren: https://support.microsoft.com/windows/analyze-the-wireless-network-report-76da0daa-1db2-6049-d154-7bb679eb03ed
- Microsoft Learn – WLAN-AutoConfig-Dienst: https://learn.microsoft.com/windows-server/networking/technologies/extensible-authentication-protocol/network-access
- Linux Wireless Documentation – `iw`: https://wireless.docs.kernel.org/en/latest/en/users/documentation/iw.html
- NetworkManager – `nmcli`: https://networkmanager.dev/docs/api/latest/nmcli.html
- NetworkManager – WLAN-Einstellungen: https://networkmanager.dev/docs/api/latest/settings-802-11-wireless.html
- Apple – Diagnose für drahtlose Umgebungen verwenden: https://support.apple.com/de-de/guide/mac-help/mchlf4de377f/mac
- Apple – Wenn der Mac keine WLAN-Internetverbindung herstellt: https://support.apple.com/de-de/101588
- Apple – `networksetup` in Remote Desktop: https://support.apple.com/de-de/guide/remote-desktop/apdd0c5a2d5/mac
- Wi-Fi Alliance – Discover Wi-Fi: https://www.wi-fi.org/discover-wi-fi

- IEEE 802.11 Working Group: https://www.ieee802.org/11/
- RFC 5416 – CAPWAP Protocol Binding for IEEE 802.11: https://www.rfc-editor.org/rfc/rfc5416.html
- iPerf3 – Offizielle Dokumentation: https://software.es.net/iperf/