Konfiguration, Überprüfung und Fehlerbehebung von Intel Connectivity Analytics auf einem Wireless-Controller der Serie 9800

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration und den Betrieb der Intel Connectivity Analytics-Funktion auf einem Wireless-Controller der Serie 9800.

Hintergrundinformationen

Intel Wi-Fi-Adapter können jetzt Diagnoseinformationen an Controller der Serie 9800 senden, um die Geräteanalysefunktion von Cisco Enterprise Wireless nutzen zu können. Dazu gehören:

- Informationen zu Client-Geräten, darunter:

    - PC-Hersteller/-Modell
    - Betriebssystemversion, Adaptertreiberversion
- Informationen zur Funkumgebung, einschließlich RSSI des zugehörigen Access Points (AP) und benachbarter APs

Voraussetzungen

- Wireless Controller der Serie 9800
- Intel Wi-Fi-Adapter (AC9560, AX200, AX201, AX210 oder höher)
- Aironet Wave 2/Wi-Fi 6/6E/7 APs

Anforderungen

- Auf dem 9800 muss Cisco IOS-XE® 17.6.1 oder höher installiert sein.
- Auf dem Intel Wi-Fi-Adapter muss der Treiber 22.50 oder höher installiert sein.
- Der Client muss für die Verwendung des nativen Windows Supplicant oder von AnyConnect NAM konfiguriert sein.
    - Wenn Sie NAM verwenden, finden Sie weitere Informationen unter CSCwc57807für die minimalen NAM- und Windows-Versionen, die für die Arbeit mit PMF erforderlich sind

Verwendete Komponenten

In dieser Übung:

- 9800-L-C mit 17.6.3
- Lenovo X1 Carbon Gen 9 PC mit Windows 11, mit Intel AX201 Adapter mit 22.150 Treiber
- AP4800, C9105, C9120, C9130

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

CLI bei 9800

1. Netzwerksicherung aktivieren

```
9800-L#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
9800-L(config)#network-assurance enable
```

2. Geräteklassifizierung aktivieren

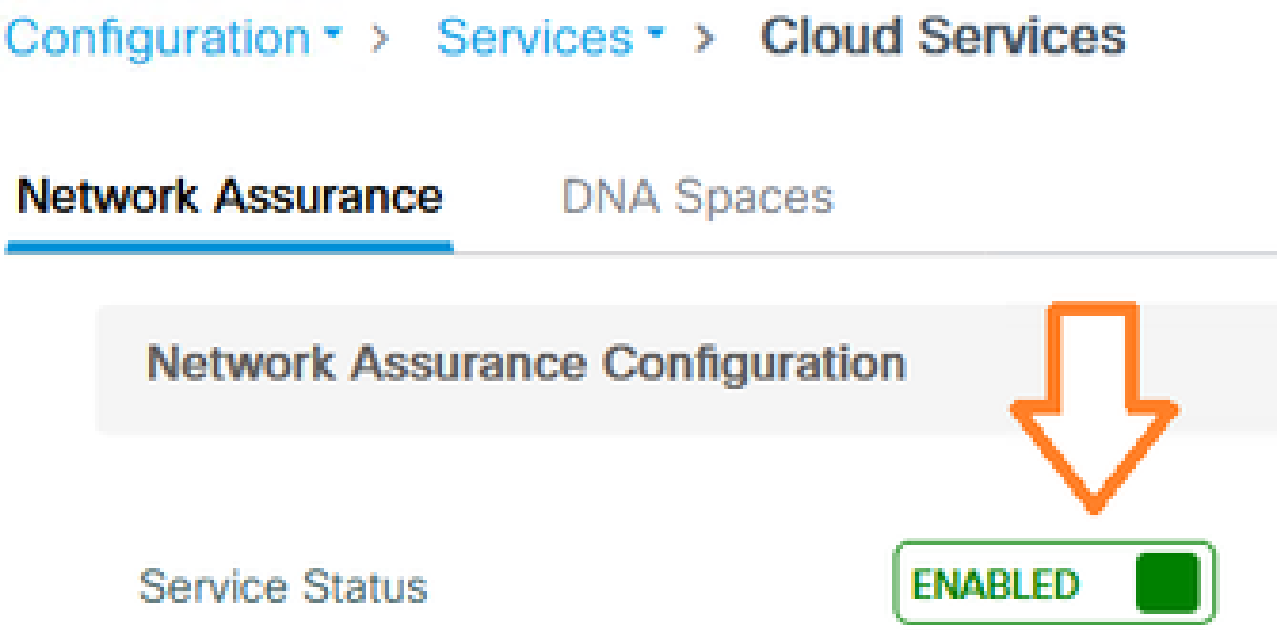
```
9800-L(config)#device classifier
```

3. Aktivieren Sie Geräteanalysen für jedes WLAN. Beachten Sie, dass "device-analytics" und "device analytics pc-analytics" standardmäßig aktiviert sind. Der Export von Geräteanalysen ist optional. Aktivieren Sie außerdem optional oder obligatorisch PMF (was sich auf die Client-Konnektivität und/oder die Leistung auswirken kann).

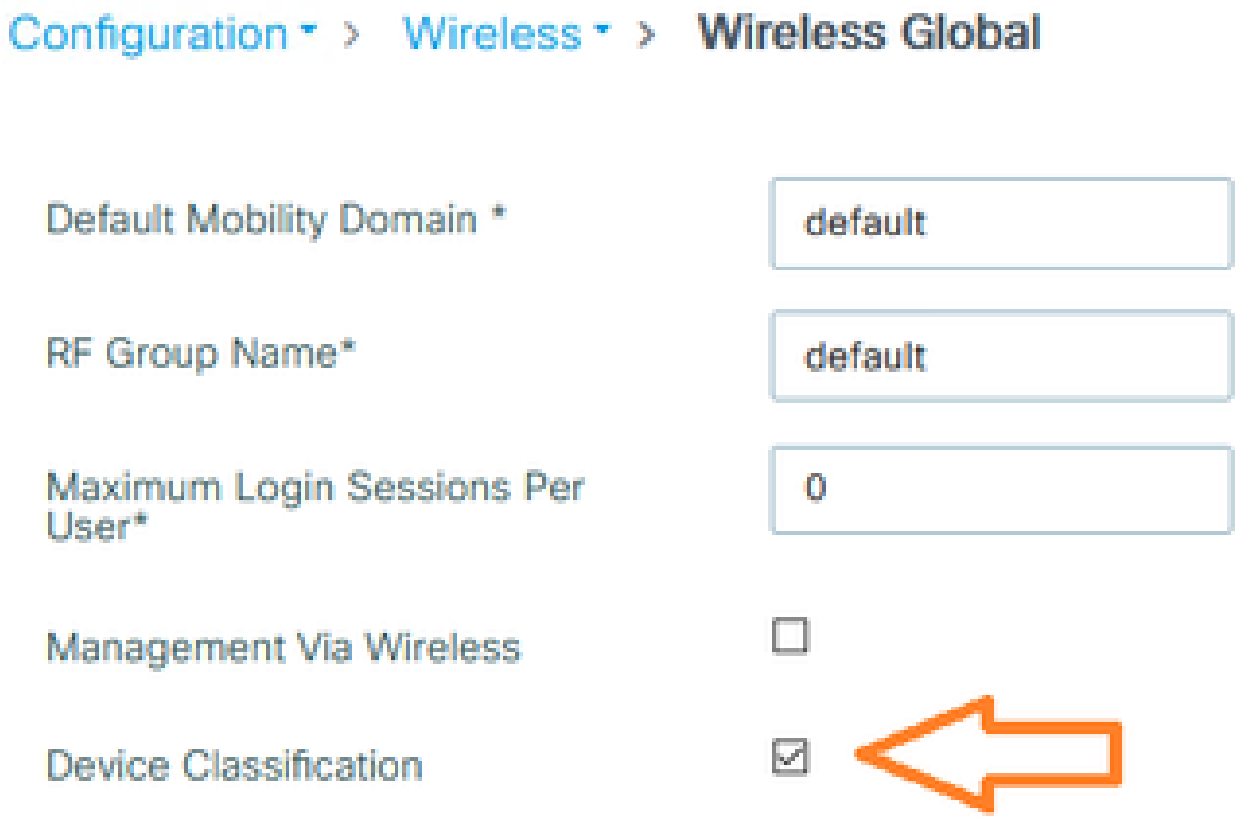
```
9800-L(config)#wlan TUCSONLAB 1 TUCSONLAB
9800-L(config-wlan)#shutdown
9800-L(config-wlan)#device-analytics
9800-L(config-wlan)#device-analytics pc-analytics
9800-L(config-wlan)#device-analytics export     # optional
9800-L(config-wlan)#security pmf optional       # or "mandatory"
9800-L(config-wlan)#no shutdown
```

Benutzeroberfläche des 9800

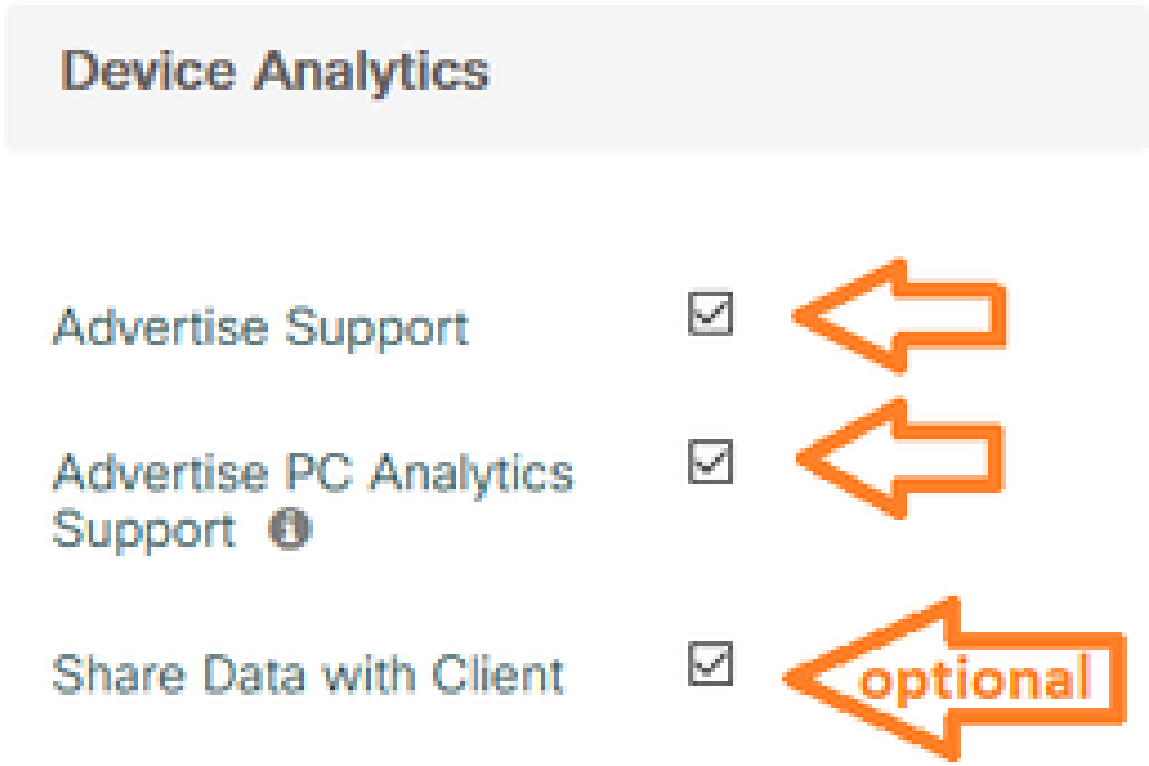
1. Netzwerksicherung aktivieren



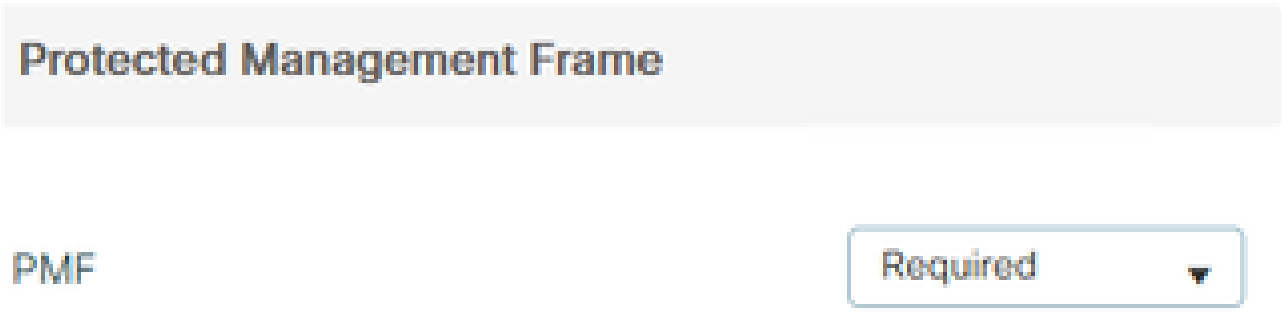
2. Geräteklassifizierung aktivieren



3. Aktivieren Sie für jedes WLAN unter Erweitert > Geräteanalysen die Unterstützung für Geräteanalysen, die Unterstützung für PC-Analysen und (optional) die Datenfreigabe mit dem Client.



4. Stellen Sie die PMF für jedes WLAN auf Optional oder Required ein (Hinweis: Dies kann sich auf die Client-Verbindung und/oder -Leistung auswirken.)



Überprüfung

Verknüpfen Sie den Intel Client mit dem Wireless-Netzwerk.

CLI bei 9800

- STA-INFO-Bericht für die Client-MAC-Adresse anzeigen

```
9800-L#show device classifier mac-address 36da.2624.f622 detail
Client Mac: 36da.2624.f622
Device Type: LENOVO 20XXS3JC01
Confidence Level: 40
Day Zero Classification: LENOVO
Device Name: Unknown Device
Software Version: 22.150.00.03
Device OS: Windows 10
Device Vendor: Intel
Power Type: AC Powered
Hardware Model: AX201 160MHz
```

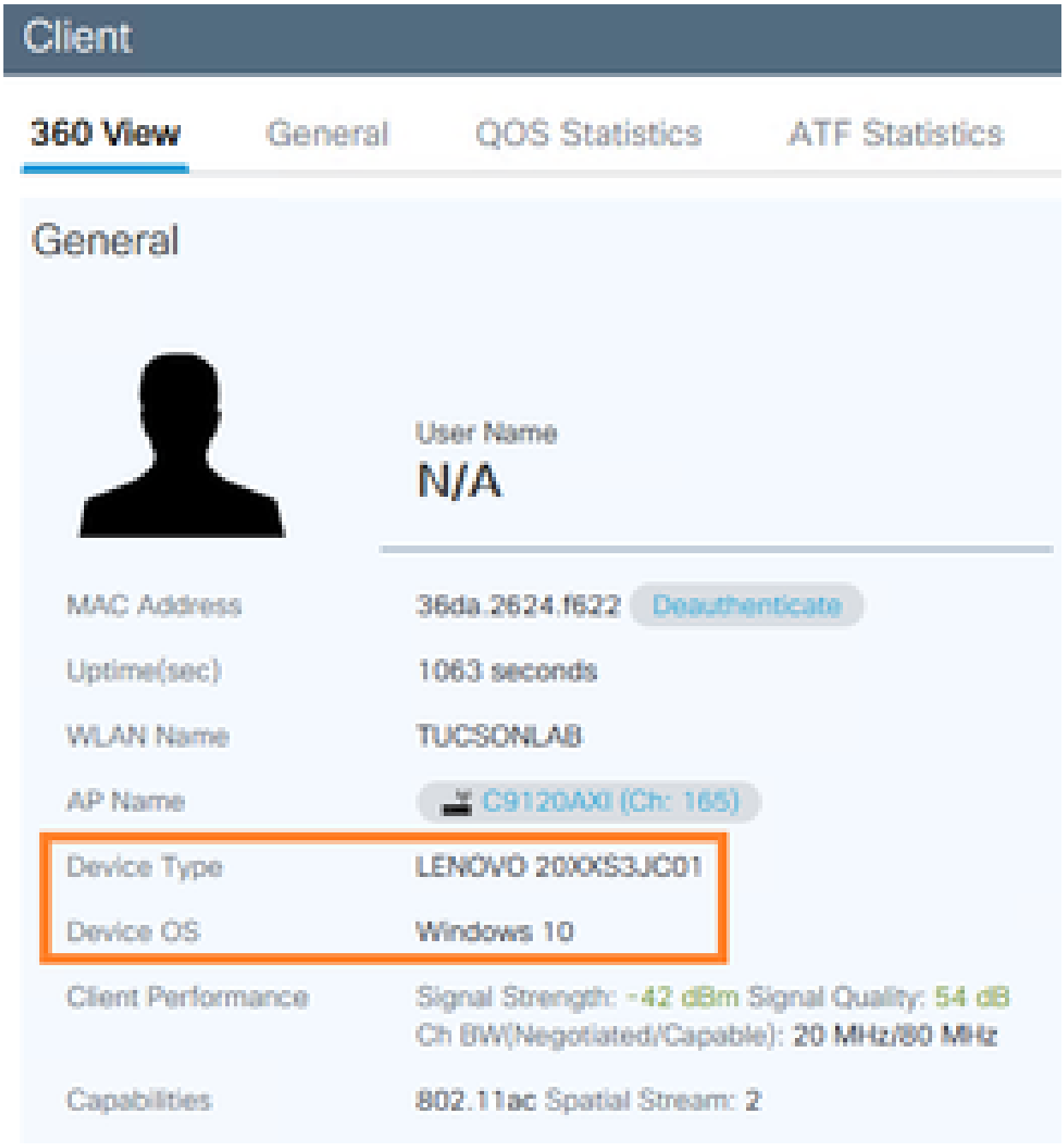
- Anzeige der PC Analytics-Informationen vom Client

```
9800-L#show wireless client mac-address 36da.2624.f622 stats pc-analytics
------------------------
Neighbor APs Info:
------------------------
Reported time:: 08/02/2022 22:40:39
------------------------
Roaming Reasons:
------------------------
Selected AP RSSI:: -55
Candidate BSSIDs:
-----------------
Neighbor AP                     RSSI(dB)
683b.78aa.230e                  -62
04eb.409f.0d6e                  -55
3c41.0e3b.0d6e                  -64
------------------------
Failed AP Report:
------------------------
Last Reported Time:: 08/02/2022 22:40:39
APs with Invalid IEs: None
APs not sending response:
------------------------
BSSID                           Frame Type
```

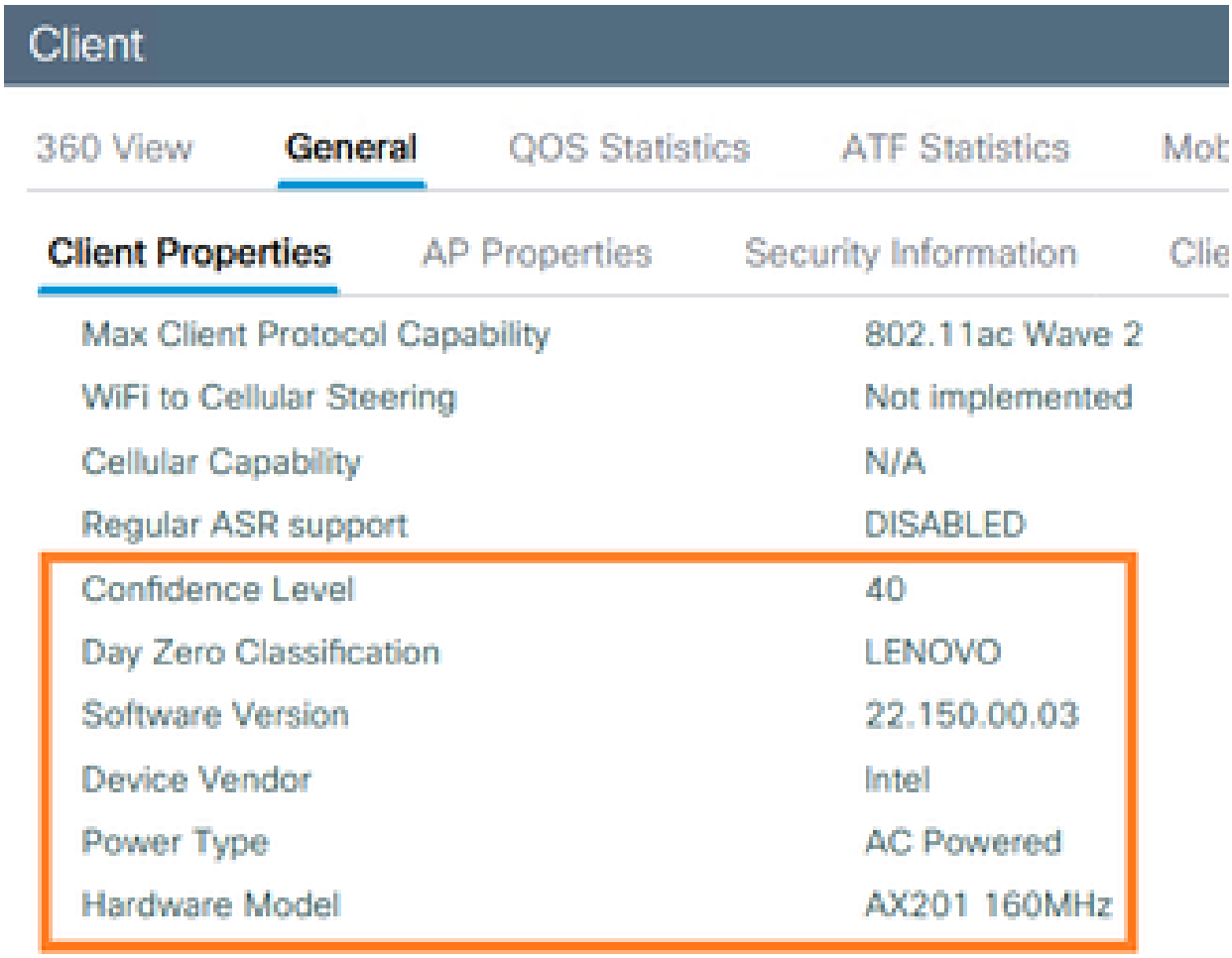
```
084f.f983.4a4e                  Authentication Response
04eb.409f.0d6e                  Other Frame types
-------------------------
PC Analytics report stats
-------------------------
-----------------------------------------------------------------------
    Report Type            Processed Reports          Dropped Reports
-----------------------------------------------------------------------

    STA Info                     1                          0
    Neigh AP                     1                          0
    Low RSSI                     0                          0
    Beacon Miss                  0                          0
    Failed AP                    1                          0
    Unknown APs                  0                          0
```

Benutzeroberfläche des 9800

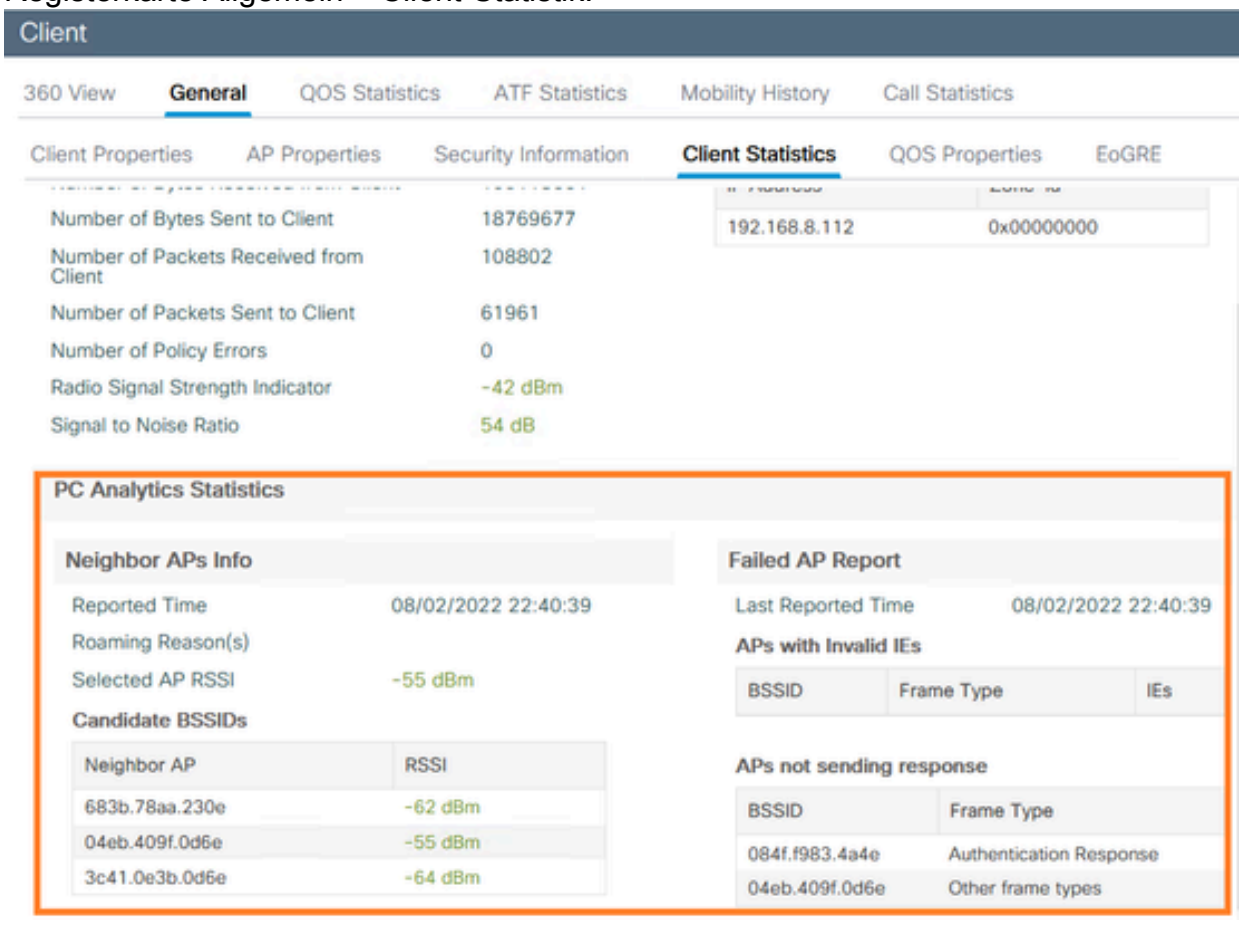
- Zeigen Sie den STA INFO-Bericht unter Überwachung > Wireless > Clients > Client-MAC an:
    - Auf der Registerkarte 360 Ansicht:



- Auf der Registerkarte Allgemein > Client-Eigenschaften:



- Registerkarte Allgemein > Client-Statistik:



Fehlerbehebung

Sie können Folgendes sammeln:

- Client-RA-Nachverfolgungen des 9800
- EPC des 9800, gefiltert nach Client-MAC
- Client-Debugging vom Access Point
- Over-the-Air (OTA)-Paketerfassung

Die folgenden Beispiele zeigen einen Arbeitsfall (Windows-Komponente) und einen nicht-Arbeitsfall (AnyConnect NAM)

RA-Ablaufverfolgungen

RA-Ablaufverfolgungen auf dem 9800 aktivieren

```
debug wireless mac 38:87:D5:09:33:EB interner Monitor-Zeit 2085978494
```

(Verbindung des getesteten Clients mit dem Access Point herstellen)

RA-Traces deaktivieren und auf TFTP-Server kopieren

```
no debug wireless mac 38:87:D5:09:33:EB internal monitor-time 2085978494
```

(Suchen Sie die neueste ra_trace-Datei)

```
dir bootflash: | ra_trace einschließen
```

```
copy
bootflash:ra_trace_MAC_38:87:d5:09:33:eb_211303_UTC_Fri_Aug_05_2022.log
tftp://192.168.10.2/ra_trace.log
```

Was Sie in den RA-Traces beachten sollten

Wenn PC Analytics mit dem Intel Client arbeitet, zeigt RA Traces die Funktion an, die die Daten aus dem empfangenen Aktionsrahmen analysiert:

```
2022/08/05 21:12:14.083830 {wncd_x_R0-0}{1}: [client-orch-sm] [24548]: (debug)
2022/08/05 21:12:14.083831 {wncd_x_R0-0}{1}: [dot11-validate] [24548]: (debug)
2022/08/05 21:12:14.083836 {wncd_x_R0-0}{1}: [dot11-validate] [24548]: (debug)
```

Dann sollten Sie Daten sehen, wie vom Client gemeldet, zum Beispiel die Treiberversion:

```
2022/08/05 21:12:14.083917 {wncd_x_R0-0}{1}: [dot11-validate] [24548]: (debug)
```

Integrierte Paketerfassung

Starten Sie EPC auf dem 9800

```
MYCAP klar erfassen
Monitor Capture MYCAP Schnittstelle Ten0/1/0 beide
MYCAP-Puffergröße 100 überwachen
MYCAP-Übereinstimmung mit allen
monitor erfassen MYCAP innere mac 38:87:D5:09:33:EB
MYCAP Start überwachen
```

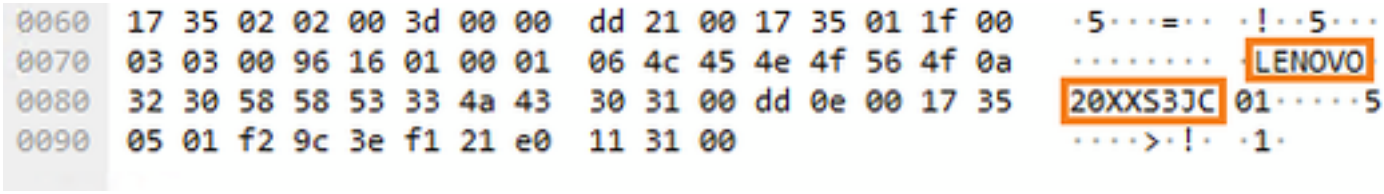
(Verbindung des getesteten Clients mit dem Access Point herstellen)

EPC anhalten und auf TFTP-Server exportieren

```
MYCAP-Stopp überwachen
MYCAP-Export erfassen tftp://192.168.10.2/MYCAP.pcap
Keine Monitorerfassung MYCAP
```

Was ist im EPC zu beachten?

Suchen Sie in Wireshark nach einem Action-Frame (wlan.fc.type_subtype == 0x000d), dessen Kategoriecode "Vendor-specified Protected" lautet (wlan.fixed.category_code == 126). Die Nutzlast sollte die PC-Marke/das PC-Modell in ASCII anzeigen:



Client-Debugging am Access Point

Starten von Debugging

```
Terminalmonitor

debug client 38:87:D5:09:33:EB
```

(Verbindung des getesteten Clients mit dem Access Point herstellen)

Debuggen beenden

```
Unbug alle

Terminalüberwachungssperre
```

Worauf Sie bei den AP-Debugging-Aufgaben achten sollten
Suchen Sie nach einer INTEL_DEO_ANALYTICS-Zeile, da der Access Point einen eingehenden ACTION-Frame vom Client analysiert. Beispiel:

```
Aug 5 21:12:13 kernel: [*08/05/2022 21:12:13.0674] [1659733933: 67444] [AP4800

      [U:W] DOT11_ACTION : Category Code: 23, Action Code: 53

Aug 5 21:12:13 kernel: [*08/05/2022 21:12:13.0675] CLSM[38:87:D5:09:33:EB]: US

Aug 5 21:12:13 kernel: [*08/05/2022 21:12:13.0676] CLSM[38:87:D5:09:33:EB]: IN
```

OTA-Paketerfassung

In diesem Beispiel wurde ein MacBook mit Wireless-Diagnose verwendet. Siehe Collect Packet Captures Over the Air auf einem MacBook.

Sie sollten sehen, dass der Client einen oder mehrere ACTION-Frames sendet, die CCMP-geschützt sind (wlan.ccmp.extiv && wlan.fc.type_subtype == 0x000d). Da diese Frames verschlüsselt sind, können Sie die Nutzlast nicht lesen (schauen Sie dazu auf den EPC oder eine Zeitspanne vom Switch-Port des Access Points.)

Wenn der Client keine CCMP-geschützten Management-Frames sendet, stellen Sie sicher, dass PMF auf optional oder obligatorisch festgelegt ist.

Um sicherzustellen, dass der 9800 richtig konfiguriert ist, um Intel Analytics anzukündigen, sehen Sie sich den Beacon-Frame oder die Antwort auf die Anfrage an. Suchen Sie mit der Cisco OUI nach einem anbieterspezifischen Tag (00:40:96 - d. h. wlan.tag.oui == 0x004096). Das nächste Oktett (im Feld "Vendor Specific OUI Type" (anbieterspezifischer OUI-Typ) hat den Wert 0x2c - dies ist DEO_IE. Das folgende Oktett ist bitcodiert. sein viertgeringstes Bit ist das Intel Analytics-Bit.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.