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

## Inhalt

Einleitung
<u>Hintergrundinformationen</u>
<u>Voraussetzungen</u>
Anforderungen
Verwendete Komponenten
Konfigurieren
<u>CLI bei 9800</u>
Benutzeroberfläche des 9800
Überprüfung
<u>CLI bei 9800</u>
Benutzeroberfläche des 9800
Fehlerbehebung
RA-Ablaufverfolgungen
RA-Ablaufverfolgungen auf dem 9800 aktivieren
RA-Traces deaktivieren und auf TFTP-Server kopieren
Was Sie in den RA-Traces beachten sollten
Integrierte Paketerfassung
Starten Sie EPC auf dem 9800
EPC anhalten und auf TFTP-Server exportieren
Was ist im EPC zu beachten?
Client-Debugging am Access Point
Starten von Debugging
Debuggen beenden
OTA-Paketerfassung

# 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 f
  ür die Verwendung des nativen Windows Supplicant oder von AnyConnect NAM konfiguriert sein.
  - Wenn Sie NAM verwenden, finden Sie weitere Informationen unter <u>CSCwc57807</u>für 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
```

 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

Configuration -> Wireless -> Wireless Global

Default Mobility Domain *	default
RF Group Name*	default
Maximum Login Sessions Per User*	0
Management Via Wireless	
Device Classification	

Device Analytics	
Advertise Support	
Advertise PC Analytics Support 10	
Share Data with Client	D optional

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.)

### Protected Management Frame

### PMF

Required

## 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: \_\_\_\_\_ Frame Type BSSID

084f.f983.4a4e 04eb.409f.0d6e	Authentication Response 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:

Client			
360 View	General	QOS Statistics	ATF Statistics
General			
		User Name N/A	
MAC Address		36da.2624.f622 Deauth	enticate
Uptime(sec)		1063 seconds	
WLAN Name		TUCSONLAB	
AP Name		🗳 C9120AXI (Ch: 165)	
Device Type		LENOVO 2000KS3JC01	
Device OS		Windows 10	
Client Perform	ance	Signal Strength: -42 dBm Ch BW(Negotiated/Capab	Signal Quality: 54 dB le): 20 MHz/80 MHz
Capabilities		802.11ac Spatial Stream:	2

• Auf der Registerkarte Allgemein > Client-Eigenschaften:

C	Client					
2	360 View	General	QOS Statistic	:s /	ATF Statistics	Mot
	Client Proper	ties	AP Properties	Securi	ty Information	Clie
	Max Client F	Protocol C	apability		802.11ac Wave 2	
	WiFi to Cellu	ular Steerin	ng		Not implemented	
	Cellular Cap	ability			N/A	
	Regular ASF	R support			DISABLED	
	Confidence	Level			40	
	Day Zero Cl	assificatio	n		LENOVO	
	Software Ve	rsion			22.150.00.03	
	Device Vend	dor			Intel	
	Power Type				AC Powered	
	Hardware M	lodel			AX201 160MHz	

### Registerkarte Allgemein > Client-Statistik:

360 View Gene		QOS Statis	tics	ATF Statistics	Mobility History	Call Statistics				
lient Prope	erties A	AP Properties Security Information			Client Statistics	QOS	EoGRE			
Number of Bytes Sent to Client						Long to				
				8/090//	192.168.8.112		000			
Number of Client	f Packets Re	ceived from	1	08802						
Number of	f Packets Se	nt to Client	6	1961						
Number of	f Policy Error	'S	0	1						
Radio Sigr	hal Strength I	Indicator	-	42 dBm						
Signal to Noise Ratio										
PC Analy	voise Ratio	ics	5	4 dB						
PC Analy Neighbo	voise Ratio vtics Statist	ics	5	4 dB	Failed AP Re	port				
PC Analy Neighbo Reporte	vtics Statist or APs Info	ics 0	5 8/02/202	4 dB 2 22:40:39	Failed AP Re	port 1 Time	08/02	/2022 22:40:3		
PC Analy Neighbor Reporte Roaming	voise Ratio vtics Statist or APs Info ed Time g Reason(s)	ics 0	5 8/02/202	4 dB 2 22:40:39	Failed AP Re Last Reported APs with Inva	port 1 Time alid IEs	08/02	/2022 22:40:3		
PC Analy Neighbo Reporte Roaming Selecter	voise Ratio vtics Statist or APs Info vd Time g Reason(s) d AP RSSI	ics 0	5 8/02/202 55 dBm	4 dB 2 22:40:39	Failed AP Re Last Reported APs with Inva BSSID	port 1 Time alid IEs Fram	08/02, ne Type	/2022 22:40:3		
PC Analy Neighbo Reporte Roaming Selecter Candida	voise Ratio vtics Statist or APs Info ed Time g Reason(s) d AP RSSI ate BSSIDs	lics 0	5 8/02/202 55 dBm	4 dB 2 22:40:39	Failed AP Re Last Reported APs with Inva BSSID	port 1 Time alid IEs Fram	08/02 ne Type	/2022 22:40:3 IEs		
PC Analy PC Analy Neighbor Reporte Roaming Selecter Candida Neighb	vtics Statist or APs Info ed Time g Reason(s) d AP RSSI ate BSSIDs por AP	ics 0	5 8/02/202 55 dBm RSSI	4 dB 2 22:40:39	Failed AP Re Last Reported APs with Inva BSSID APs not send	port I Time alid IEs Fram	08/02 ne Type oonse	/2022 22:40:3 IEs		
PC Analy PC Analy Neighbo Reporte Roaming Selecter Candid Neighb 683b.7	voise Ratio vtics Statist or APs Info ed Time g Reason(s) d AP RSSI ate BSSIDs oor AP '8aa.230e	lics 0	5 8/02/202 55 dBm RSSI -62 dBm	4 dB 2 22:40:39	Failed AP Re Last Reported APs with Inva BSSID APs not send BSSID	port 1 Time alid IEs Fram ling resp	08/02, ne Type onse Frame Type	/2022 22:40:3 IEs		
PC Analy PC Analy Neighbo Reporte Roaming Selecter Candida Neighb 683b.7 04eb.4	voise Ratio vtics Statist or APs Info ed Time g Reason(s) d AP RSSI ate BSSIDs oor AP 28aa.230e .09f.0d6e	ics 0	5 8/02/202 55 dBm RSSI -62 dBm -55 dBm	4 dB 2 22:40:39	Failed AP Re Last Reported APs with Inva BSSID APs not send BSSID 084f,f983.4a	port 1 Time alid IEs Fram fing resp	08/02, ne Type onse Frame Type Authentication	/2022 22:40:3 IEs		

# 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

сору

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 "Vendorspecified Protected" lautet (wlan.fixed.category\_code == 126). Die Nutzlast sollte die PC-Marke/das PC-Modell in ASCII anzeigen:

0060	17	35	02	02	00	3d	00	00	dd	21	00	17	35	01	1f	00	·5···=··	·!··5···
0070	03	03	00	96	16	01	00	01	06	4c	45	4e	4f	56	4f	Øa		LENOVO
0080	32	30	58	58	53	33	4a	43	30	31	00	dd	0e	00	17	35	20XXS3JC	015
0090	05	01	f2	9c	3e	f1	21	e0	11	31	00						····>·!·	·1·

#### **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]: II

### **OTA-Paketerfassung**

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

Sie sollten sehen, dass der Client einen oder mehrere ACTION-Frames sendet, die CCMPgeschützt 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.