

HowTo: Einschalten Debug-Modus und Capture Wireless Pakete am DWC-1000/DWC-2000

[Voraussetzungen]

- 1. DWC-1000/2000 mit aktueller Firmware
 - DWC-1000 mit FW 4.4.1.2 und höher
 - DWC-2000 mit FW 4.4.0.3 und höher
- 2. Kompatibler Unified-AP mit aktueller Firmware
 - DWL-8610AP/8600AP/6700AP/6600AP/6610AP/3600AP/2600AP mit FW 4.2.0.x und höher

[Szenario]

Es soll ein Unified-AP, welcher durch einen DWC-1000/2000 gemanaged wird, in den Debug-Modus versetzt werden um WLAN Pakete zur Fehlersuche/Analyse mitzuschneiden.





[Vorbereiten des DWC-1000/2000]

 Verbinden Sie sich auf den DWC-1000/2000 und wechseln Sie zu "Wireless -> Access Point -> Managed APs List"

🕰 s	tatus 🤶 Wir	eless 📃 Netw	rork 🕼 VPN	Security	O Maintenance	
Status » Dashboard	General General	Access Point Discovered AP List	Peer Group Peer Configuration	ACL IP ACL	DiffServ DiffServ Class) @
The Traffic Overvie	Channel Algorithm	Managed APs List	Peer Status	IP ACL Rules	DiffServ Policy	
and Active Info for	Power Algorithm	AP Poll List		MAC ACL	DiffServ Policy Class	011 /
Dashboard	WIDS	AP Profile		MAC ACL Rules	Defination	
Dashboard	Distributed Tunnels	SSID Profiles				ard
	WLAN Deployment	WDS Groups				
Traffic Overview	WLAN Visualization					
	HTTP 41.17%	30 22.5		20 16 12		

a. Wechseln Sie in den Reiter "Managed APs"

Wireless » Access Point » Managed APs List » Managed APs 20											00			
Valid APs Managed APs AP Provisioning														
AP managed by the Wireless Controller is listed by its MAC address and location.When the AP is in Managed mode, remote access to the AP is disabled. However,we can enable Telnet access by enabling the Debug feature. We can also manually change the RF channel and power for each radio on an AP.														
Managed APs List	t													
Show 10 💌 entri	es [Right click or	n record to get mor	e op	tions]										٩
Model Name 🔂	Location \ominus	MAC Address	€	IP Address	⊜	Channel	⇔	Power %	⊜	Firmware	⊜	Debug	⊜	Profile 😌
dwl6610ap		3C:1E:04:F3:DC:80		192.168.10.109		0/6		0/100		4.3.0.2_B042		Disable		1 - Default
dwl8610ap		B0:C5:54:E7:A0:00		192.168.10.128		0/1		100/100		4.3.0.2_B042		Enable		1 - Default
Showing 1 to 2 of 2 en	Showing 1 to 2 of 2 entries													

b. Mittels "Rechtsklick" auf den zu konfigurierenden AP erhalten Sie weitergehende Unterpunkte

Vireless » Access Point » Managed APs List » Managed APs									
Valid APs Managed APs AP Provisioning									
AP managed by the Wireless Controller is listed by its MAC address and location.When the AP is in Managed mode, remote access to the AP is disabled. However,we can enable Telnet access by enabling the Debug feature. We can also manually change the RF channel and power for each radio on an AP.									
Managed APs List									
Show 10 - entries [Right click on record to get more op	tions]					٩			
Model Name $\ \Omega$ Location $\ \Theta$ MAC Address $\ \Theta$	IP Address ⊖	Channel ⊖	Power % 😌	Firmware 😌	Debug ⊖	Profile \varTheta			
dw16610ap	192.168.10.109	0/6	0/100	4.3.0.2_B042	Disable	1 - Default			
wil8610a Channel and Power Radio Uff :00	192.168.10.128	0/1	100/100	4.3.0.2_B042	Enable	1 - Default			
Sowing AP Debug				K First Previo	ous 1 Next	> Last >			



- c. Wählen Sie nun "AP Debug" aus
 - i. Aktivieren/Deaktivieren Sie die Option "Enable Debug"
 - ii. Tragen Sie das AP Administratorenpasswort f
 ür den Telnetzugriff ein
 1. Standardmässig lautet dieses "admin
 - iii. Bestätigen Sie Ihr Passwort
 - iv. Bestätigen Sie Ihre Anpassungen mit "Save"

Managed AP Debug Configuratio	n				Wizard	System Search U	×
MAC Address Location	3C: 11	E:04:F3:DC:80					
IP Address	192.1	68.10.109					
Status	Not 9	started					
Enable Debug	ON						
rassword	••••	•					
Confirm Password	••••	•					
Wireless » Access Point » Manager	d APs List » Managed	APs					Save ? Ø
		Opera	tion Succee	ded			
Valid APs Managed APs A	AP Provisioning						
AP managed by the Wireless Contr disabled. However,we can enable radio on an AP.	oller is listed by its Telnet access by en	MAC address and abling the Debug	d location.Whe g feature. We c	n the AP is in I an also manual	Managed mode, ly change the R	remote access to the F channel and power	AP is for each
Managed APs List							
Show 10 💌 entries [Right click	on record to get more	e options]					٩
Model Name ☆ Location ↔	MAC Address 🕀	IP Address ⊖	Channel 🖯	Power % ⊜	<u>Fi</u> rmware ⊖	Debug ⊖	Profile ⊖
dwl6610ap	3C:1E:04:F3:DC:80	192.168.10.109	0/6	0/100	4.3.0.2_B042	Enable - Requested	1 - Default
dwl8610ap	B0:C5:54:E7:A0:00	192.100.10.120	0/1	1007 100	4.3.0.Z_B042	Enable	1 - Default
Showing 1 to 2 of 2 entries					K First	J Previous 1 Next	> Last >J

Nach der Aktivierung des Debug-Modus ist ein TELNET/SSH Zugriff auf den aktivierten AP möglich.

Dieser Zugriff ist solange möglich, bis der AP neu gestartet oder die Option deaktiviert wurde.



2) Verbinden Sie sich nun per "Telnet/SSH" auf den aktivierten Unified AP



Tragen Sie das in Punkt 1 c vergeben Passwort zur Authentifizierung am Accesspoint ein.



3) Mittels "get radio" bekommen Sie einen Überblick über die zur Verfügung stehenden Radios.

🛃 192.168.10.109 - PuTTY		
DLINK-WLAN-AP#		
DLINK-WLAN-AP# get ra	dio	
Property	Value	
Iname	wlan0	
status	up	
mac	3C:1E:04:F3:DC:80	
channel-policv	best	
appe	bg-n	
static-channel	O THE PARTY OF THE	
channel	6	
tx-rx-status	up	
multicast-to-unicast	off	
dhcp-to-unicast	off	
Property	Value	
	Value	
Tame	wlanl	
status	aown	
mac	3C:1E:04:F3:DC:90	
channel-policy	best	
mode	a-n-ac	
static-cnannei	52	
channel	36	
tx-rx-status	up	
multicast-to-unicast	off	=
dhcp-to-unicast	off	
DLINK-WLAN-AP#		
DLINK-WLAN-AP#		
DLINK-WLAN-AP#		-



 4) Sie können nun diverse Einstellungen bezüglich des Paket Capture auswählen (DWL-6600AP/8600AP 5G: radio1, 2.4G: radio2) (DWL-8610AP 5G: radio2, 2.4G: radio1)

! Je nach vorhandenem Accesspointtyp können unterschidliche Optionen verfügbar sein !

- a) set packet-capture file-capture-interface radio1
 - i) definiert Radio1 als Capture-Interface
- b) set packet-capture start-remote-capture up/down
 - i) startet/beendet das Remote-PCAP
- c) mittels "get packet-capture" bekommen Sie eine Übersicht über die Funktion



- 5) Starten Sie an Ihrer Messstation den Wireshark und definieren ein entsprechendes "Remote Interface"
 - a) Gehen Sie auf Interface List => Options

	e World's Most Popular Ne rsion 1.12.7 (v1.12.7-0-g7fc8978 fro	etwork Protocol Analyzer om master-1.12)			
	Wireshark: Capture Interfaces				_ D _ X
	Device	Description	IP	Packets Packe	ets/s
Interface List	E VMware Network Adapter VMnet	8 411/ware Wraat Etitemet Ndapte.	1000119471696410919100440	9 1	Details
Live list of the capture inter (counts incoming packets)	🔲 🔎 Drahtlosnetzwerkverbindung 2	Minnet	<u> </u>	0 0	Details
Start	🔲 🖈 Drahtlosnetzwerkverbindung 3	<u></u>	- C 00 0 1 14 55 70 00b	0 0	Details
Choose one or more interfa	🔲 <section-header> LAN-Verbindung 3</section-header>	Watchouard Secure Client Virtuar NDISO Adapter	10003012.0003.5101.0107	• 0 0	Details
John Mare Network Adapter	🔲 🔊 Drahtlosnetzwerkverbindung	Microsoft	192.168.10.168	20 3	Details
Drahtlosnetzwerkverbindur	🔲 <section-header> LAN-Verbindung 2</section-header>	R H L DEL EREE ", C + H	C 00 0000 5761 000 J 5 J	218 33	B Details
Drahtlosnetzwerkverbindur	🔲 🗊 LAN-Verbindung 5	No Mindons Haapter VS for Eynes SecaEntender	1000/0021/100 1000210021	0 0	Details
LAN-Verbindung 3	Bluetooth-Netzwerkverbindung 3	Miner		0 0	Details
 Drahtlosnetzwerkverbindur LAN-Verbindung 2 	Help		<u>S</u> tart Stor	p Option	<u>C</u> lose
🖉 LAN-Verbindung 5			IKING IV change/071/01/18	VISI ncanna /68	K VR)



b) Gehen Sie auf Manage Interfaces

Wireshar	k: Capture Options	TABLE INC.						
Capture								
Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]		Capture Filter	A
	VMware Network Adapte	 Ethernet	enabled	262144	2			*
•						III		
🗆 Captu	re on all interfaces							Manage Interfaces
🗹 Use p	romiscuous mode on all inte	erfaces						

c) Definieren Sie ein neues "Remote Interface" mittels "add"

Interface Management		
Pipes Local Interfaces	note Interfaces	
Remote Interfaces		
Host	 Name 	•
•		Þ
<u>A</u> dd <u>D</u> elete		<u>A</u> pply <u>C</u> lose

- i) Tragen Sie die IP-Adresse des capturing APs ein
- ii) Tragen Sie Port 2002 ein (Standard)
- iii) Bestätigen Sie die Eingabe mit "OK"

	Wires	shark: Re							
0	Host:	192.168.10.19							
	Port: 2002								
	Authentication								
	Null authentication								
	© Pass	sword authentication							
	Userna	me:							
	Passwo	ord:							
		<u>O</u> K <u>C</u> ancel							

! Sollten Sie zu lange Zeit zwischen aktivieren des Capture Modus am AP und Definition am Wireshark Client benötigt haben, so erscheint eine Fehlermeldung am Wireshark. Deaktivieren und Aktivieren Sie den Capture Modus am AP neu um dies zu korrigieren.



- d) Wählen Sie die Interfaces aus die "verborgen" (nicht angezeigt) werden sollen
- e) Bestätigen Sie Ihre Auswahl mit "apply"

Interface Managemen	t		_ 0 X
Pipes Local Interfaces	Remote Interfaces]
Host	 Name 		▲ Hide
□ 192.168.10.109			
	rpcap	//[192.168.10.109]:2002/brtrunk	
	rpcap	://[192.168.10.109]:2002/eth0	
	rpcap	://[192.168.10.109]:2002/wlan0	
	rpcap	://[192.168.10.109]:2002/wlan0vap1	
	rpcap	://[192.168.10.109]:2002/wlan0vap2	
	rpcap	://[192.168.10.109]:2002/radio1	
	rpcap	://[192.168.10.109]:2002/any	
	rpcap	://[192.168.10.109]:2002/lo	
Add Delete		Apply	Close

In der Interface Übersicht des Wireshark werden jetzt alle entsprechenden Optionen angezeigt.

Captur	e Interface	Link-laver header	Prom. Mode	Snaplen (B) B	uffer [MiB]		Capture	Filter
	LAN-Verbindung 5 fe80::cc21:4094:8061:bb17 192.168.200.2	Ethernet	enabled	262144	2			
	Bluetooth-Netzwerkverbindung 3 fe80::25b4:d6d1:9e1b:69cb 0.0.0.0	Ethernet	enabled	262144	2			
	VMware Network Adapter VMnet1 fe80::d119:dcfc:d176:6c5f 192.168.217.1	Ethernet	enabled	262144	2			
	rpcap://[192.168.10.109]:2002/brtrunk 192.168.10.109	Ethernet	enabled	262144	2			
	rpcap://[192.168.10.109]:2002/eth0	Ethernet	enabled	262144	2			
	rpcap://[192.168.10.109]:2002/wlan0	Ethernet	enabled	262144	2			
	rpcap://[192.168.10.109]:2002/wlan0vap1	Ethernet	enabled	262144	2			
	rpcap://[192.168.10.109]:2002/wlan0vap2	Ethernet	enabled	262144	2			
M	rpcap://[192.168.10.109]:2002/radio1	802.11 plus radiotap header		262144	2	>		
	rpcap://[192.168.10.109].2002/any	Linux cooked	enableu	202144	2			
	rpcap://[192.168.10.109]:2002/lo (loopback) 127.0.0.1	Ethernet	enabled	262144	2			
∢ 📃				111				
Cap	ture on all interfaces							Manage
🛛 Use	promiscuous mode on all interfaces							
<u>C</u> aptur	e Filten							▼ Compile select
pture	Files							Display Options
ile:							Browse	☑ Update list of packets in real
Lico	multiple files I Use pcap-ng format							Automatically scroll during li
Z Nov	tila avanz							Hide capture info dialog
Nex	tile every							News Develotion
_ Ring	buffer with 2 tiles							Resolve MAC addresses
op Cap	oture Automatically After							Resolve <u>n</u> etwork-layer name
1	packet(s) 1 megabyte(s)	*						Resolve transport-layer name
	file(s)	~						☑ Use <u>e</u> xternal network name r
<u>H</u> elp								Start



In diesem Vorgang wurde das Radio-Interface ausgewählt um die WLAN Frames mitzulesen.

Die entsprechenden Daten werden nun im lokalen Wireshark angezeigt und können entsprechend weiterbearbeitet werden.

*rpcap://[192.168.10.109]:2002/radio1 [Wireshark 1.12.	7 (v1.12.7-0-g7fc8978 from master-1.12)]							
Eile Edit View Go Capture Analyze Statistics Telephony Iools Internals Help								
● ● ▲ ■ ₫ ⊟ 🗋 X 😂 ٩, + + • • 7	\$ ■■ 444 8 8 8 8 % \$							
Filter:	Expression Clear Apply	Save HTC WLAN, ADDR						
No. Time 547 2015-09-24 13:29:02 147834000	Source 26:fb:94:15:01:1f	Spanning-tree-(for-1802	tocol Length Info 2 11 93 Data SN=0, EN=0, Elaos= pE.	^				
548 2015-09-24 13:29:02.1575404000 549 2015-09-24 13:29:02.165703000 550 2015-09-24 13:29:02.165703000 551 2015-09-24 13:29:02.194547000 552 2015-09-24 13:29:02.20457000 553 2015-09-24 13:29:02.20479000 554 2015-09-24 13:29:02.27273000 555 2015-09-24 13:29:02.27273000 557 2015-09-24 13:29:02.27273000 557 2015-09-24 13:29:02.27273000 557 2015-09-24 13:29:02.27273000	D-LinkIn,287:32:90 D-LinkIn,23:0d:e0 D-LinkIn,27:54:d0 D-LinkIn,267:530 D-LinkIn,267:530 D-LinkIn,18:58:32 D-LinkIn,100:fd:f0 C67:38:1d:cb:5f:85 D-LinkIn,100:fd:f2 D-LinkIn,100:fd:f2 D-LinkIn,267:63:10	Broadcast 802. Broadcast 802.	2.11 275 Beacon frame, SN=656, FN-0, Flags, BI-100, 2.11 276 Beacon frame, SN=2147, FN-0, Flags, BI-100, 2.11 275 Beacon frame, SN=2147, FN-0, Flags, BI-100, 2.11 275 Beacon frame, SN=60, FN-0, Flags, BI-100, 2.11 276 Beacon frame, SN=369, FN-0, Flags, BI-100, 2.11 275 Beacon frame, SN=369, FN-0, Flags, BI-100, 2.11 276 Beacon frame, SN=3262, FN-0, Flags, BI-100, 2.11 249 Beacon frame, SN=3252, FN-0, Flags, BI-100, 2.11 242 Beacon frame, SN=1159, FN-0, Flags, BI-100, 2.11 276 Beacon frame, SN=3562, FN-0, Flags, BI-100, 2.11 276 Beacon frame, SN=365, FN-0, Flags, BI-100, 2.11 276 Beacon frame, SN=365, FN-0, Flags, BI-100, 2.11 276 Beacon frame, SN=365, FN-0, Flags, BI-100, 2.11 276 Beacon frame, SN=358, FN-0, Flags, BI-100, 2.11 276 Beacon frame, SN=358, FN-0, Flags, BI-100,	SSID-dlonline[Malfo SSID-dlonline SSID-dlonline SSID-dlonline[Malformed SSID-Cude[Malformed SSID-Cud-G020-5832 SSID-CMM_CP_PAS[Ma SSID-dlink_DMR-730 SSID-Gude SSID-Gude				
559 2015-09-24 13:29:02.323768000 560 2015-09-24 13:29:02.339789000 561 2015-09-24 13:29:02.339640000 562 2015-09-24 13:29:02.362367000 563 2015-09-24 13:29:02.370511000 564 2015-09-24 13:29:02.372851000	D-LinkIn_b0:fd:f0 G6:a8:laich:5f:85 D-LinkIn_b0:fd:f1 D-LinkIn_8f:32:90 D-LinkIn_2a:0d:e0 D-LinkIn_8f:54:d0	Broadcast 802. Broadcast 802. Broadcast 802. Broadcast 802. Broadcast 802. Broadcast 802. Broadcast 802.	2.11 249 Beacon frame, SN-2363, FN-0, Flags, BI-100 2.11 249 Beacon frame, SN-1160, FN-0, Flags, BI-100 2.11 288 Beacon frame, SN-259, FN-0, Flags, BI-100 2.11 275 Beacon frame, SN-658, FN-0, Flags, BI-100 2.11 276 Beacon frame, SN-249, FN-0, Flags, BI-100 2.11 275 Beacon frame, SN-259, FN-0, Flags, BI-100 2.11 275 Beacon frame, SN-259, FN-0, Flags, BI-100 2.11 275 Beacon frame, SN-559, FN-0, Flags, BI-100	, SSID-CHM[Malformed , SSID-CHM[Malformed , SSID-CLM_CP_DOP[Ma SSID-CLM_CP_DOP[Ma SSID-GLde[Malforme SSID-GLde]Malforme				
 Frame 1: 276 bytes on wire (2208 bits Radiotap Header v0, Length 25 IEEE 802.11 Beacon frame, Flags: IEEE 802.11 wireless LAN management f [Malformed Packet: IEEE 802.11]), 276 bytes captured (2208 bits) or rrame	n interface O						
0000 00 00 19 00 6f 08 00 00 26 70 53 0010 00 02 85 09 a0 00 ec a7 50 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 78 54 26 b0 78 54 00 00 00 00 64 04 00	8 20 00 00 00 00			* *				
● K File: "C\Users\mlinde\AppData\Loca Packets: 574 -	Displayed: 574 (100,0%) · Dropped: 0 (0,0%)		Profile: Default					