

# Specialized Attacks: Hardware Product Testing

---

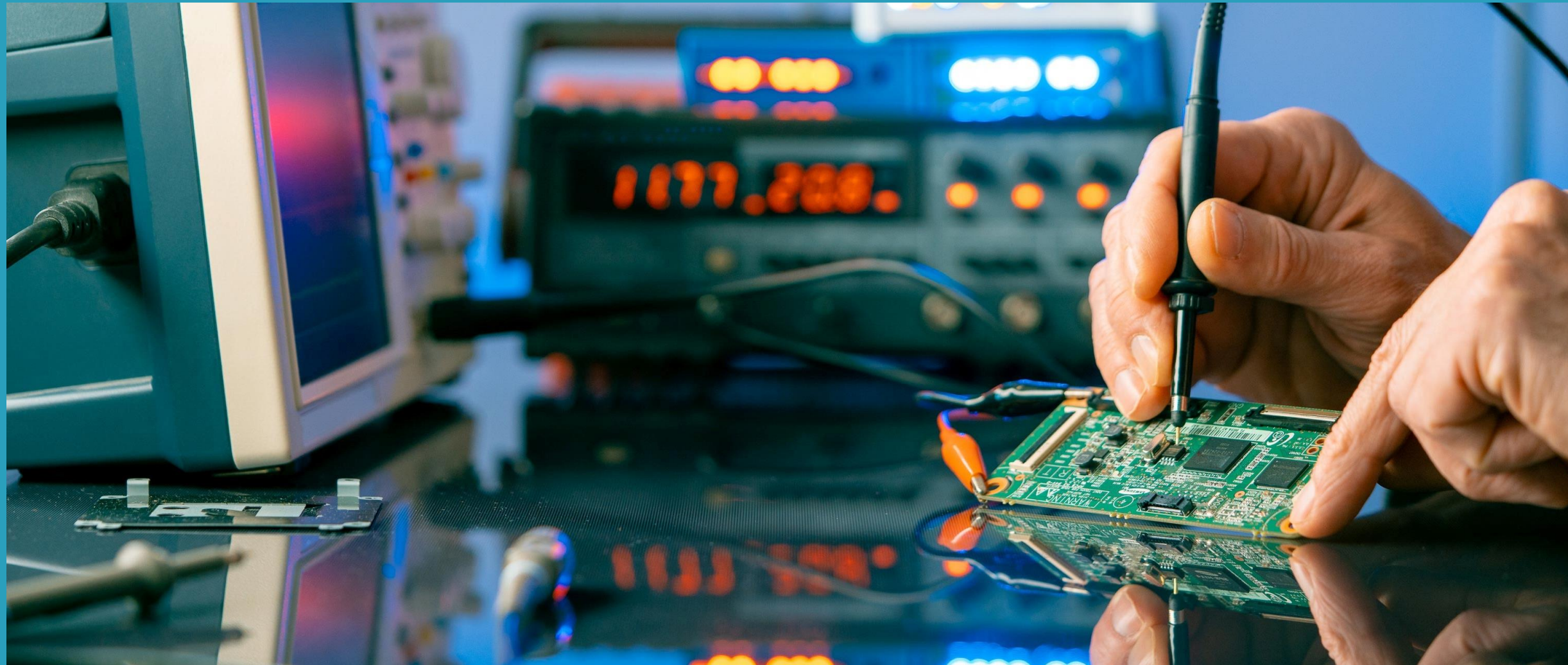
Exploring Hardware Attacks



**Matt Lloyd Davies**

Capability Development Lead





# Hardware Product Testing

Identifying vulnerabilities and determining the resilience of hardware by physically interacting with it.



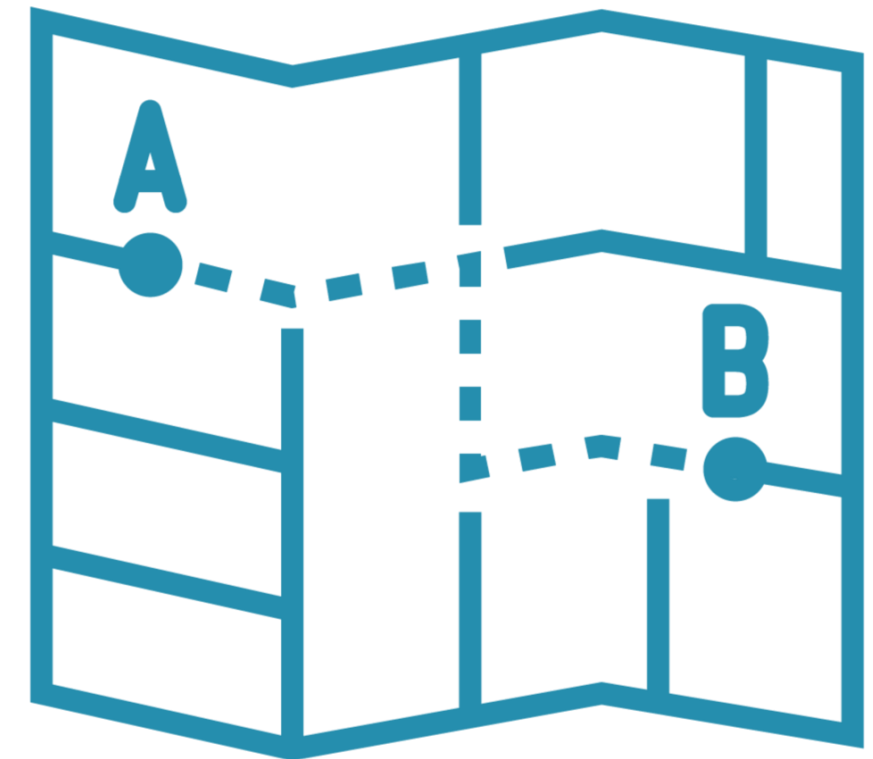
# Hardware Product Testing



**Exfiltrate sensitive  
data**

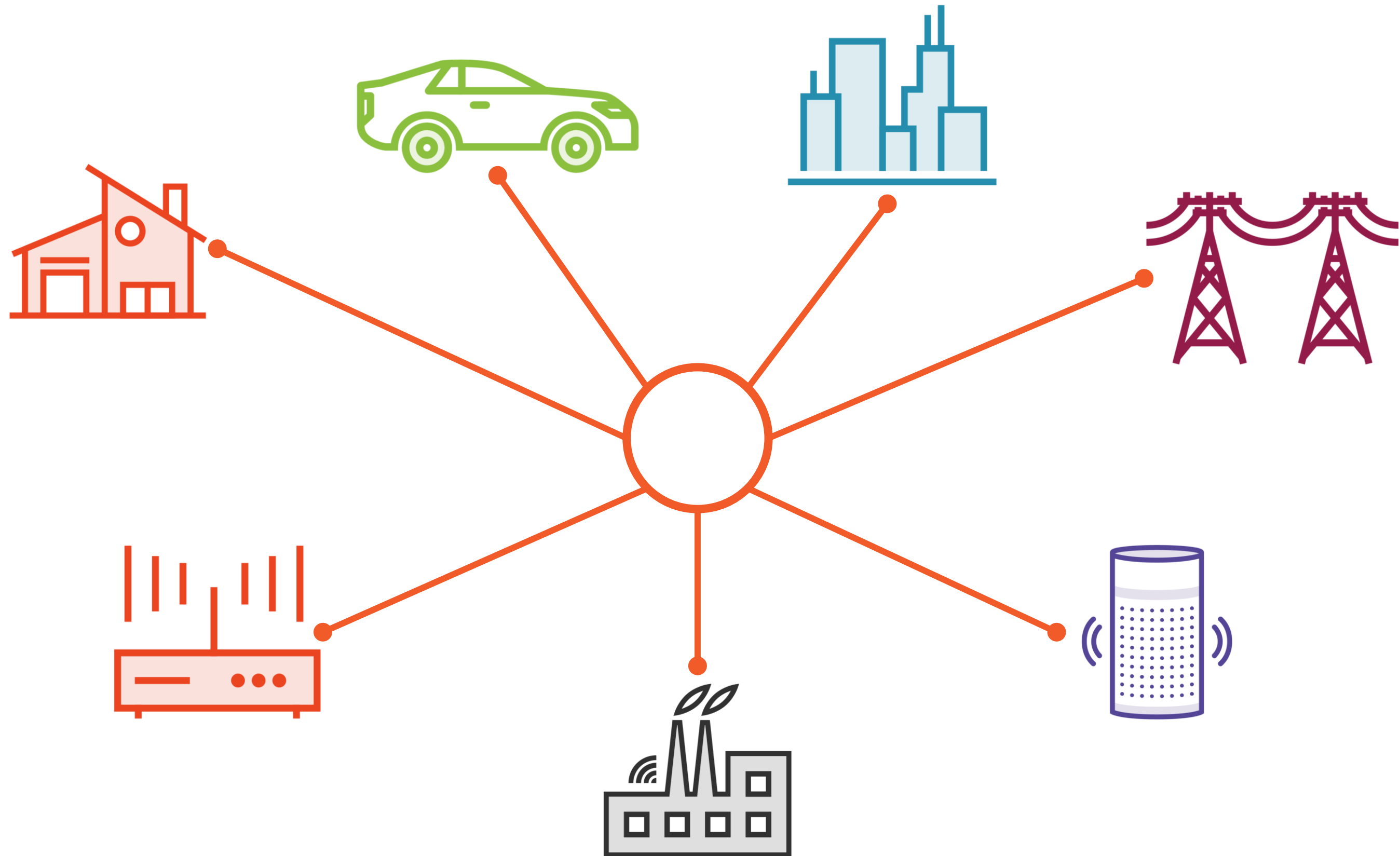


**Gain privileged  
access**

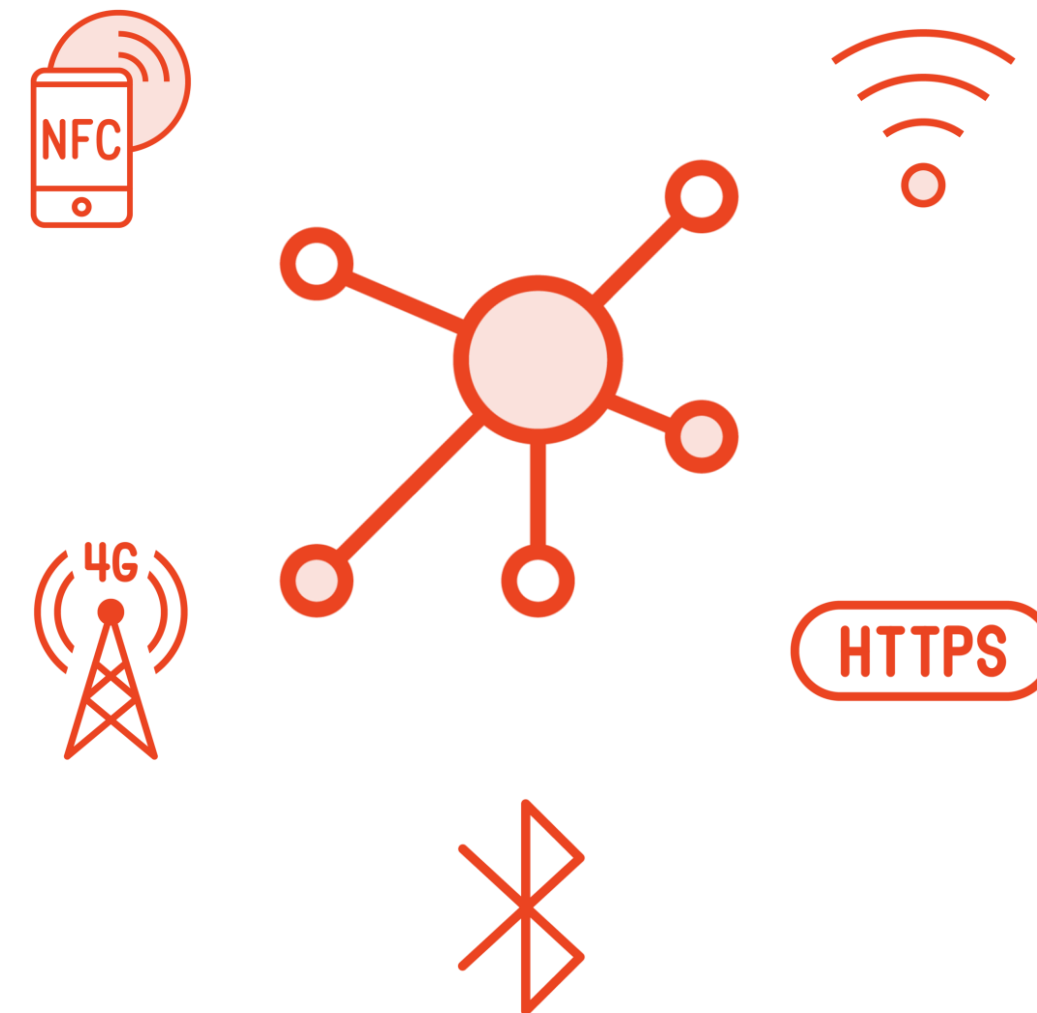
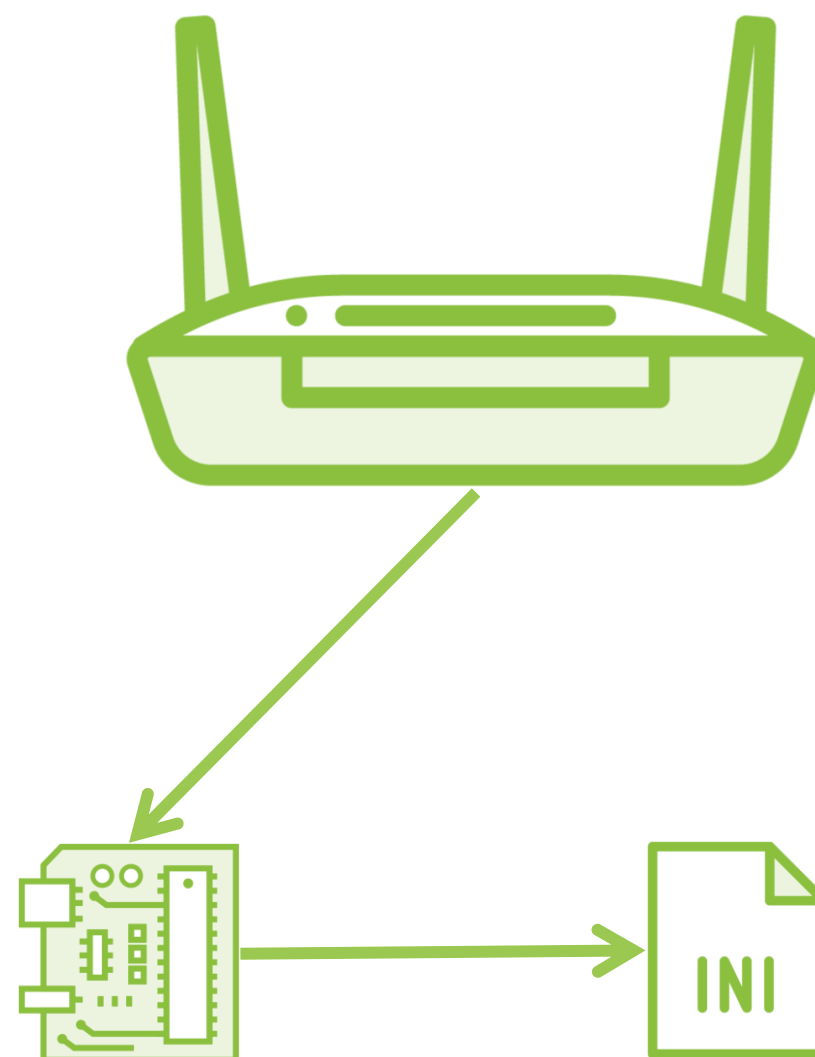


**Pivot and move  
laterally**

# The Smart World



# The Attack Surface





# Hardware Product Testing



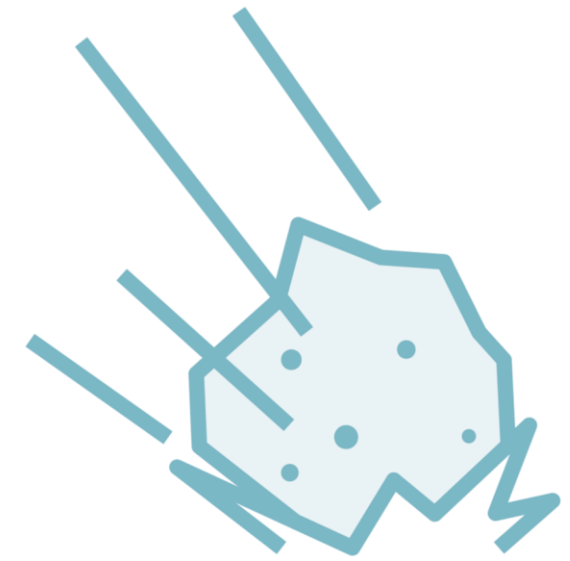
**Target**



**Access**



**Position**



**Impact**



# Identifying Hardware Components and Interfaces

---





# The TL-WR841N Home Router

A 300 Mbps entry level home router  
that retails for under \$20.





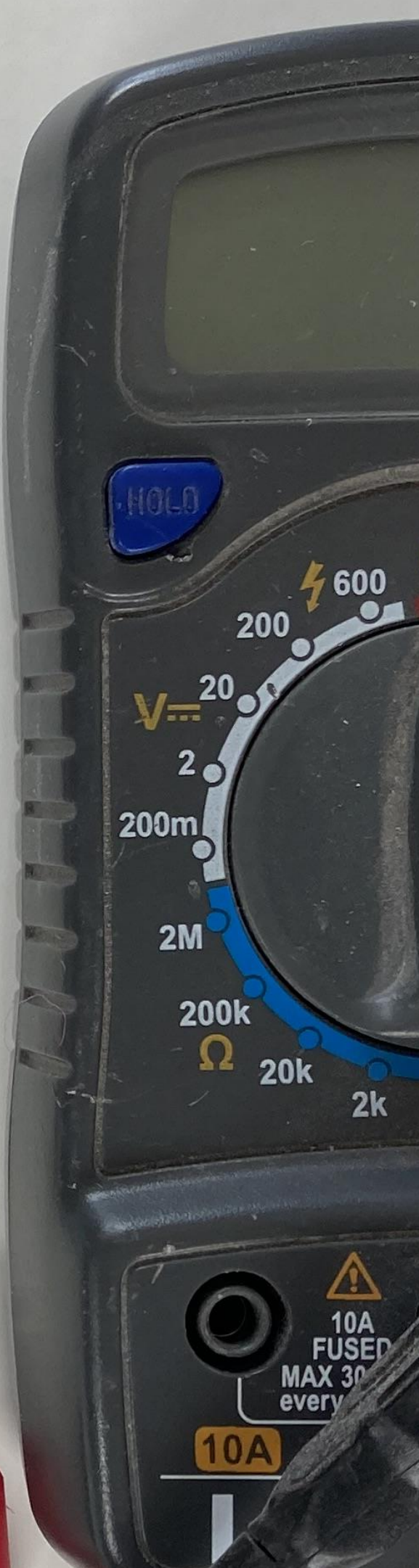


# The TL-WR841N Home Router

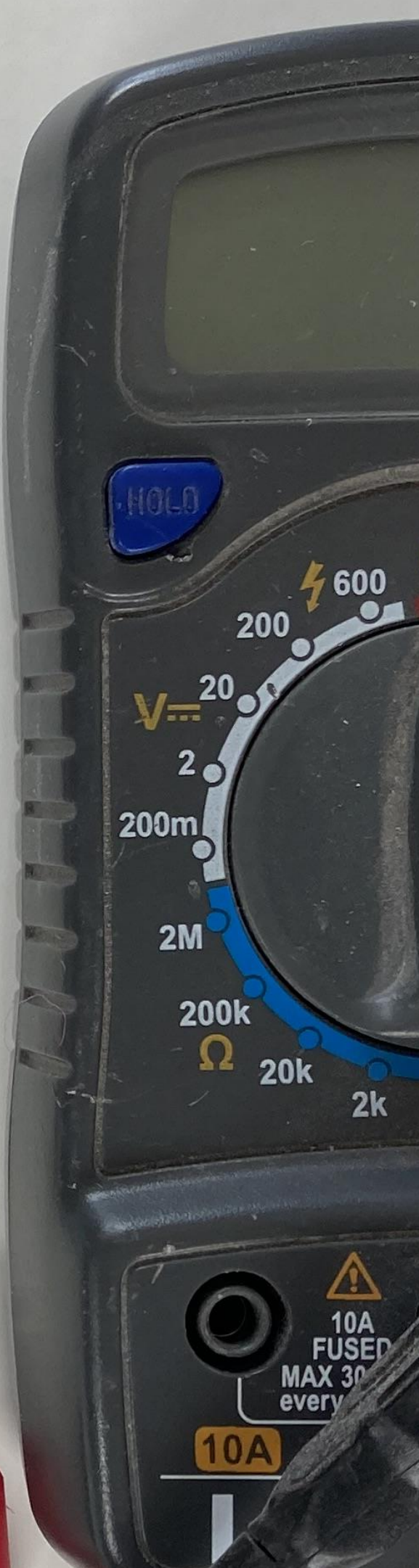
A 300 Mbps entry level home router  
that retails for under \$20.



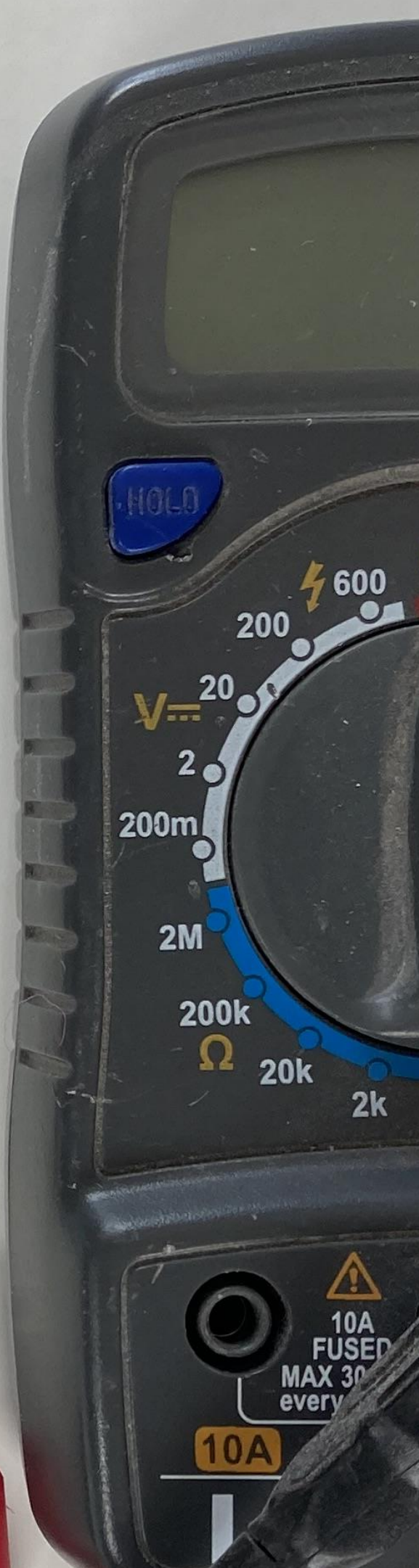




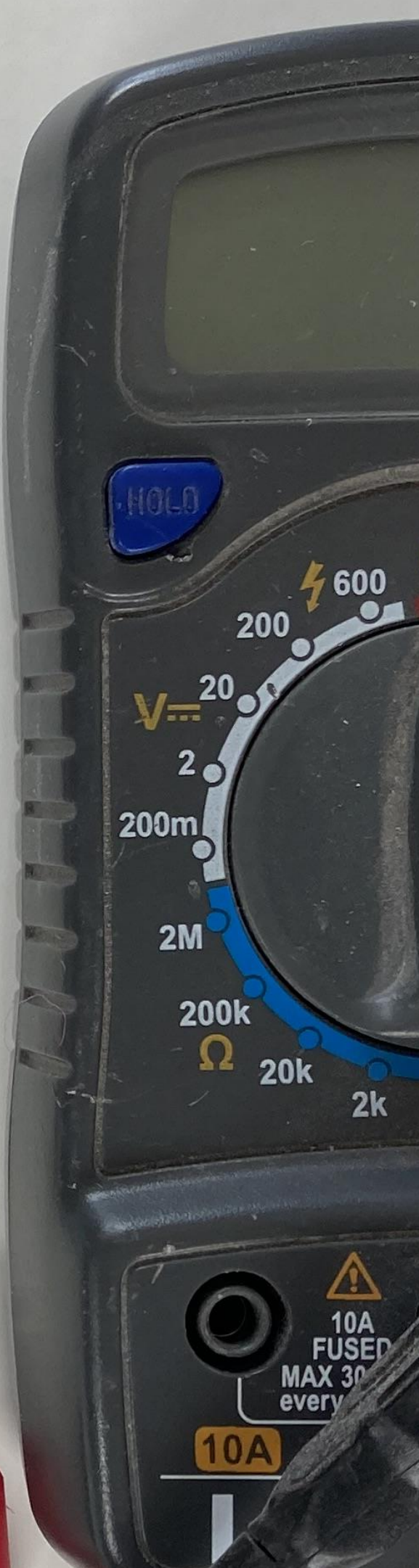




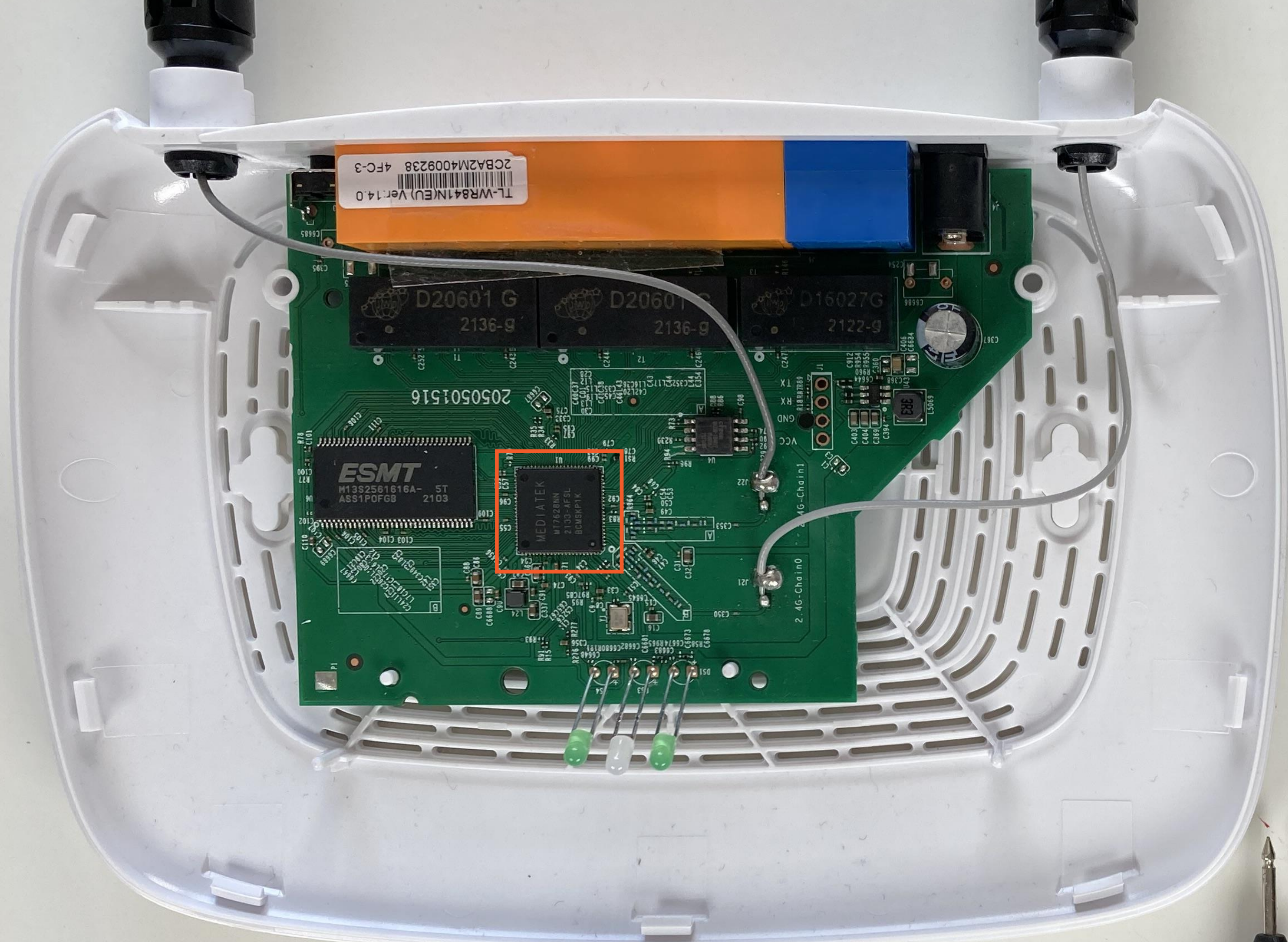












TL-WR841N(EU) Ver:1.4.0  
2CBA2M4009238 4FC-3

D20601 G  
2136-G

D20601 G  
2136-G

D16027G  
2122-G

2050501516

ESMT  
M13S2561616A- 5T  
ASS1P0FGB 2103

MEDIATEK  
MT7620N  
2133-AFSL  
BCM5KPK

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

VCC

GND

TX

RX

IF

2.4G-Cha in0

2.4G-Cha in1

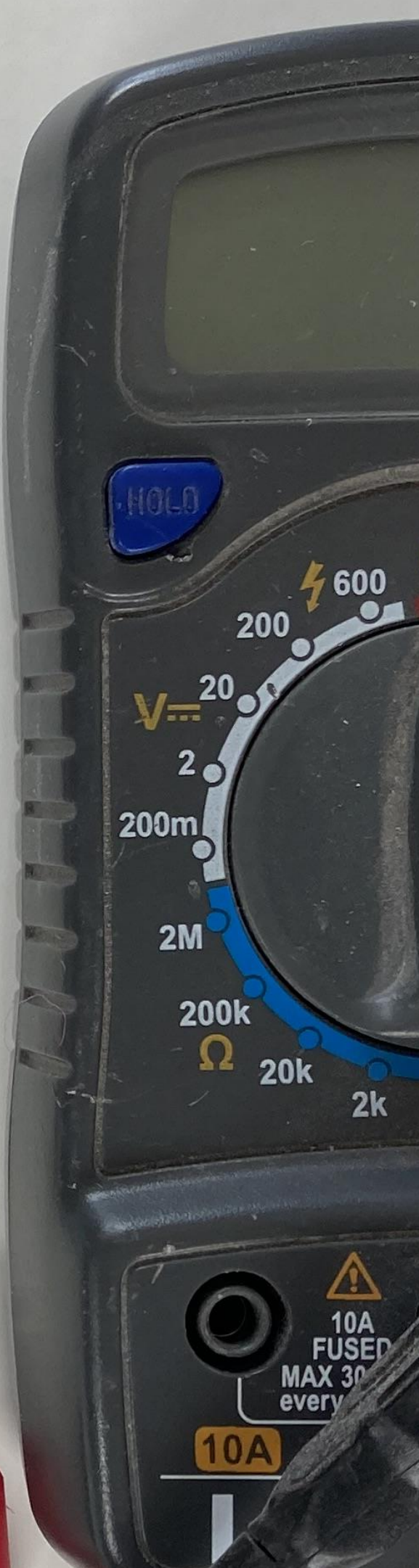
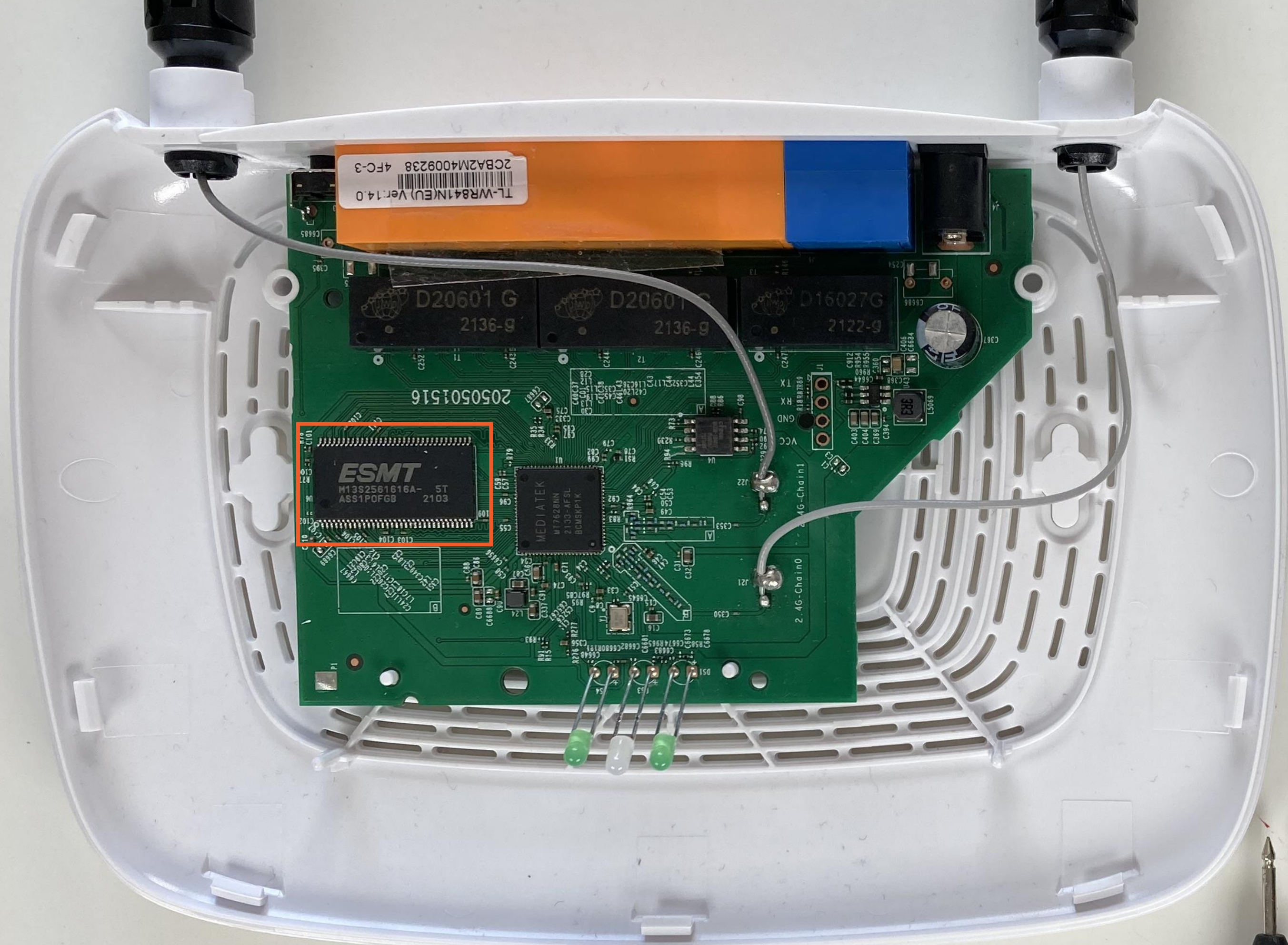
VCC

GND

TX

RX









2.4G-Chain0

2.4G-Chain1

VCC  
GND  
RX  
TX



2050501516

2136-9

2136-9

2122

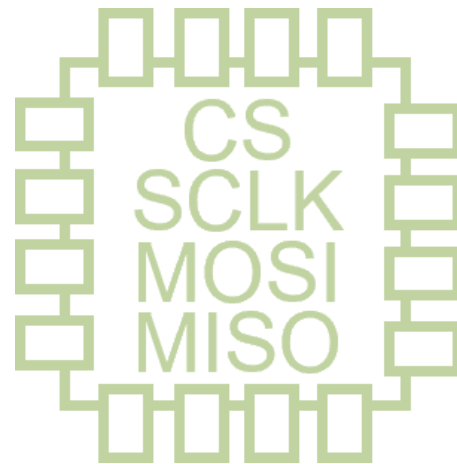


# Hardware Interfaces and Communication Protocols



## UART

Universal Asynchronous  
Receiver-transmitter



## SPI

Serial Peripheral Interface



## I2C

Inter-integrated Circuit



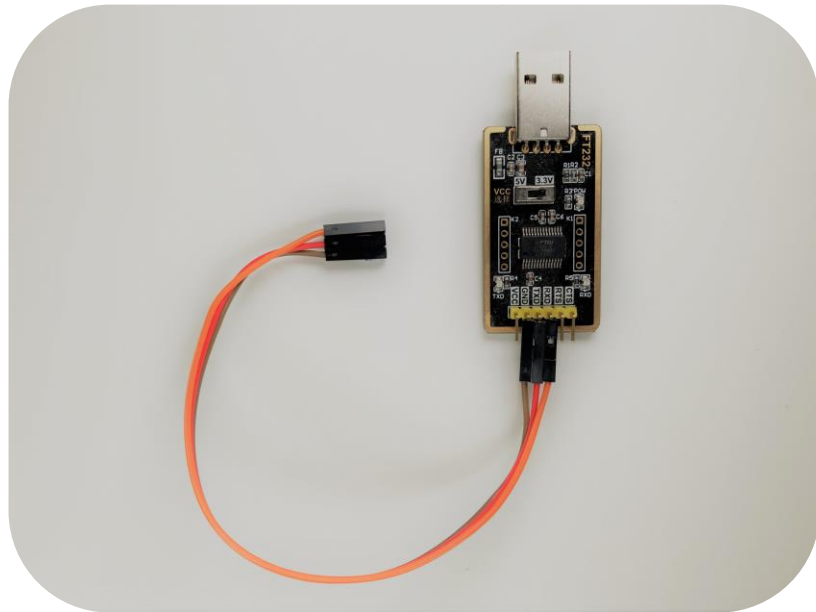
# Hardware Testing Tools

---

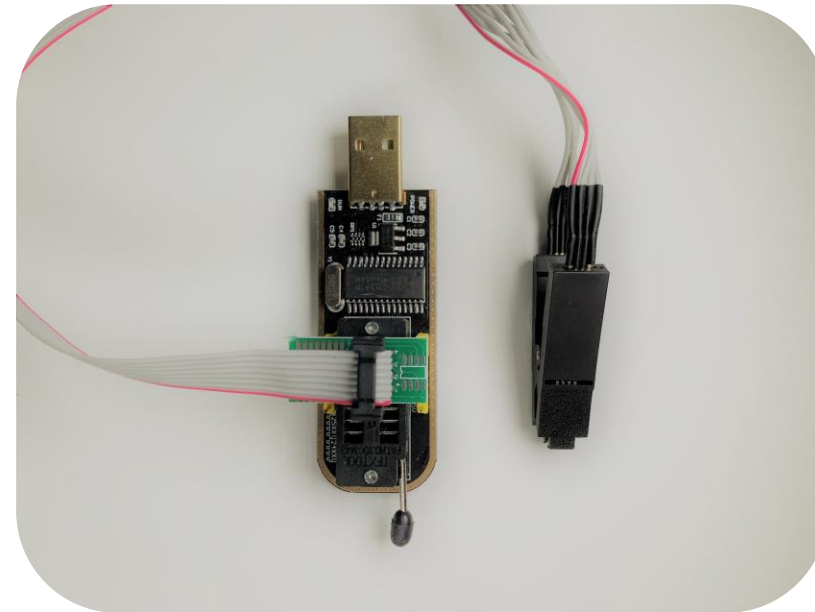




# Hardware



**TTL to USB  
cable**



**Flash memory  
programmer**



**Multi-meter**



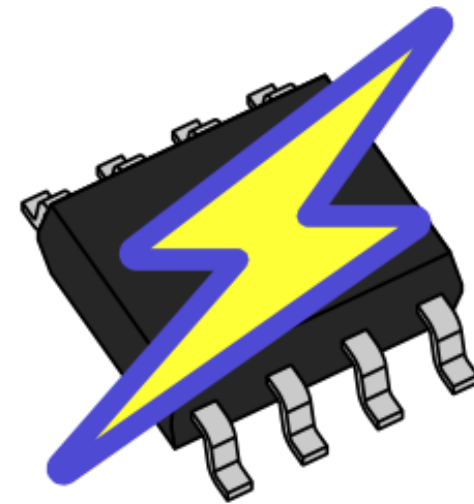
**Logic analyzer**



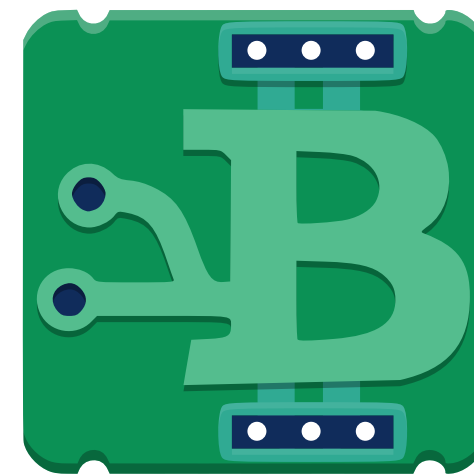
# Software



**Connect to  
serial ports**



**Read and write  
to memory**



**Interrogate  
binaries**



**Reverse  
engineer**



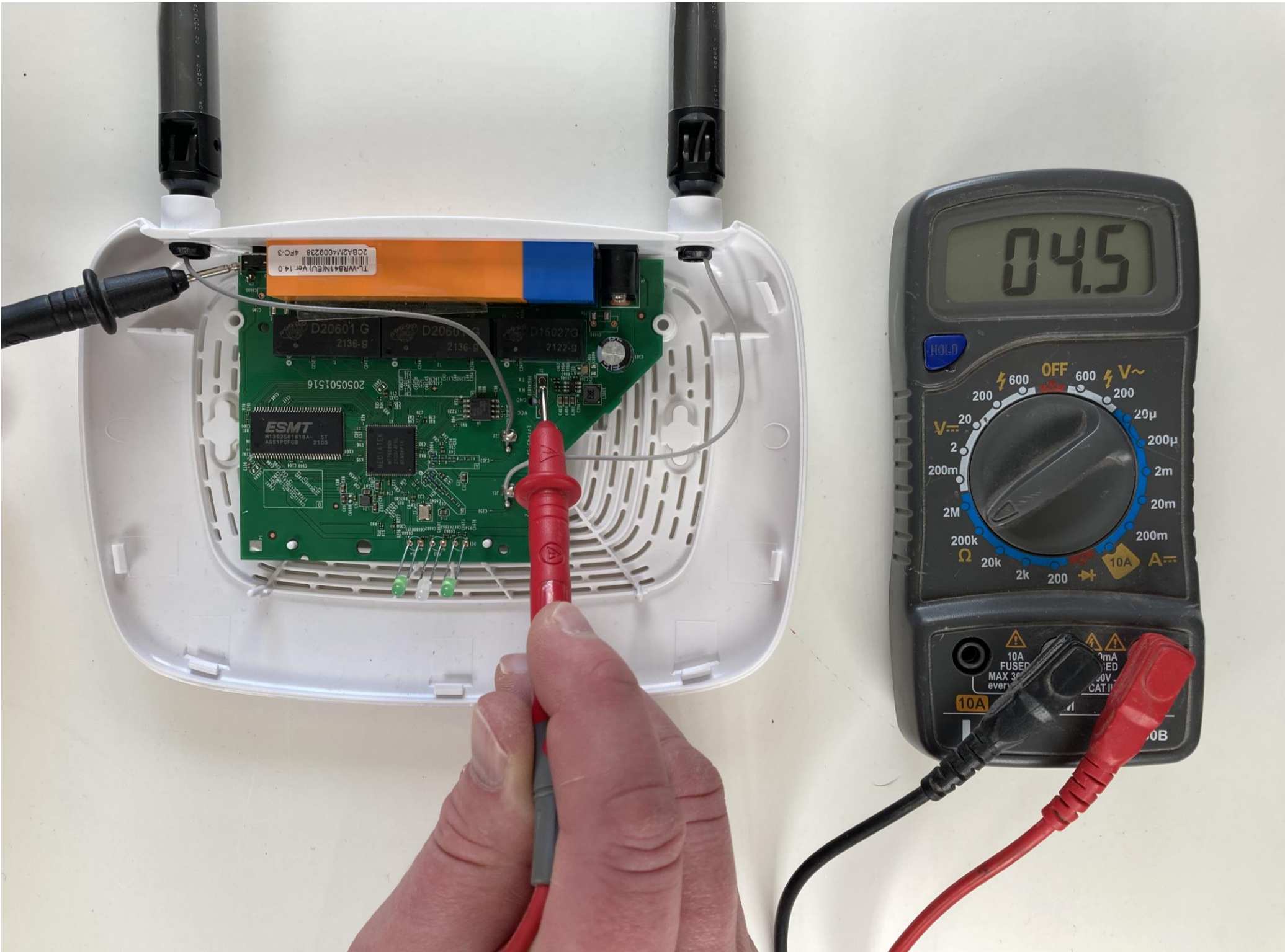
# Identifying UART Serial Pins

---



# Electrical Measurements

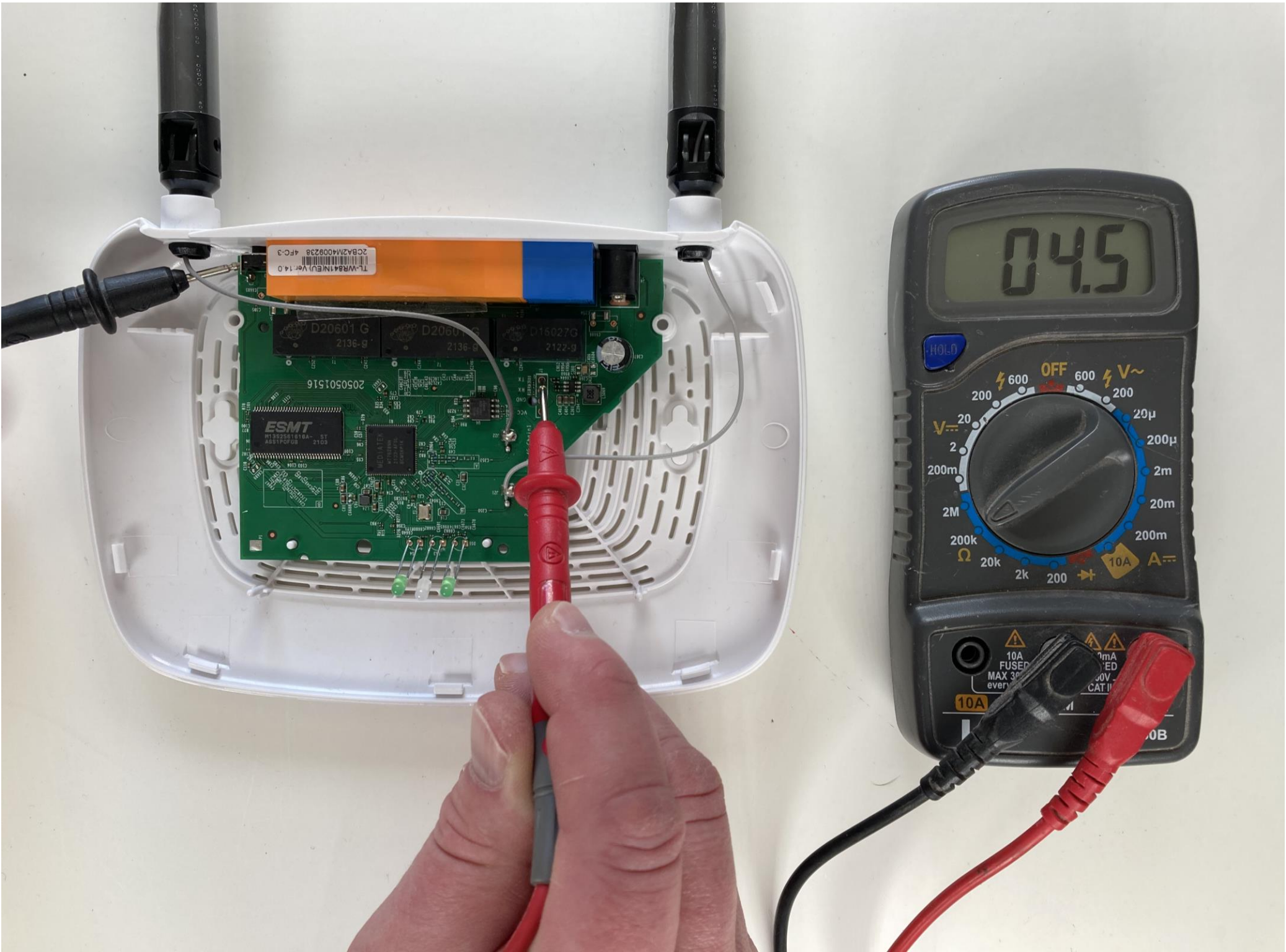
Pin	$R_{GND}$	$R_{VCC}$	V
1			
2			
3			
4			





# Electrical Measurements

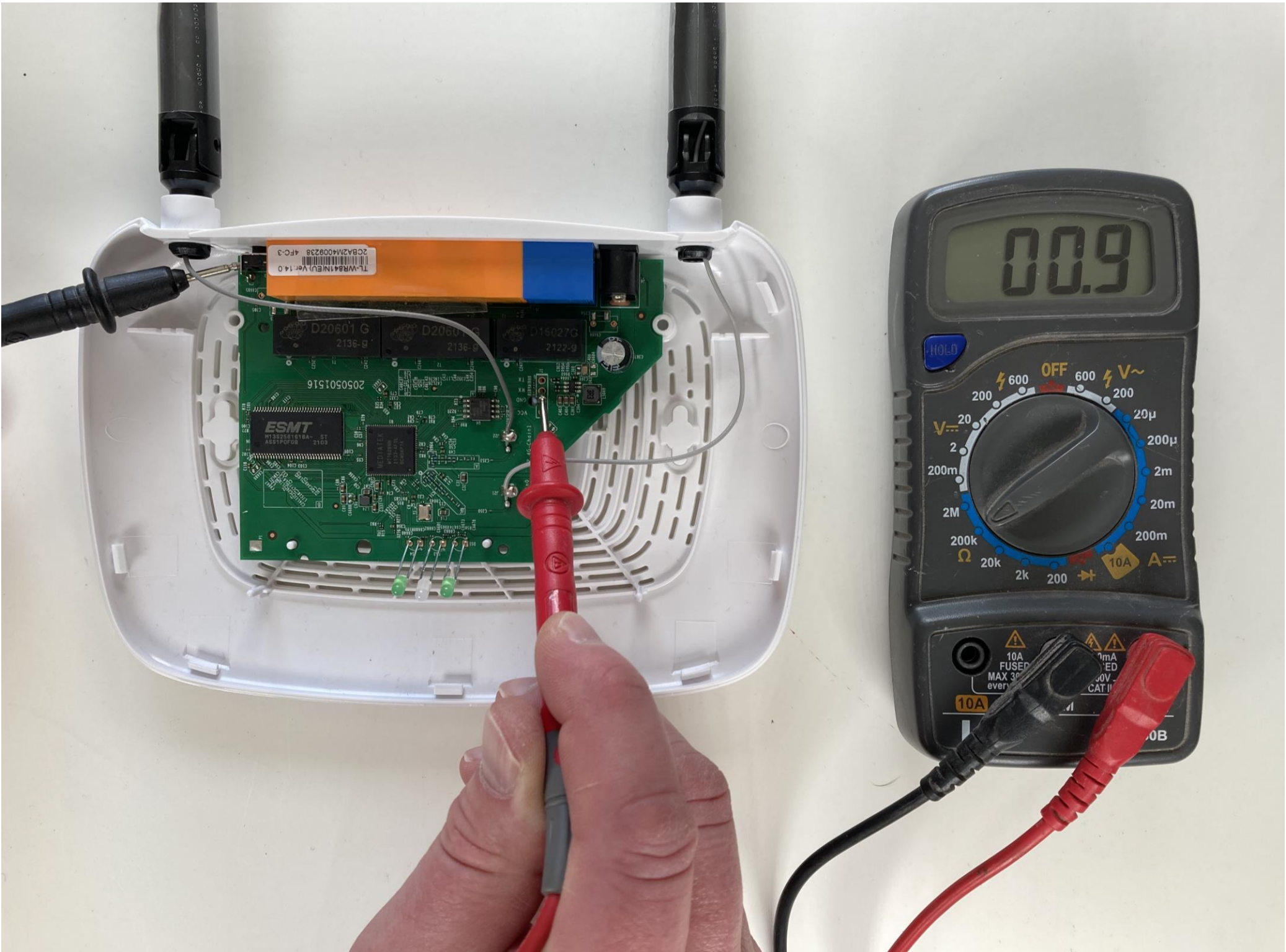
Pin	R <sub>GND</sub>	R <sub>VCC</sub>	V
1	4.5kΩ		
2			
3			
4			





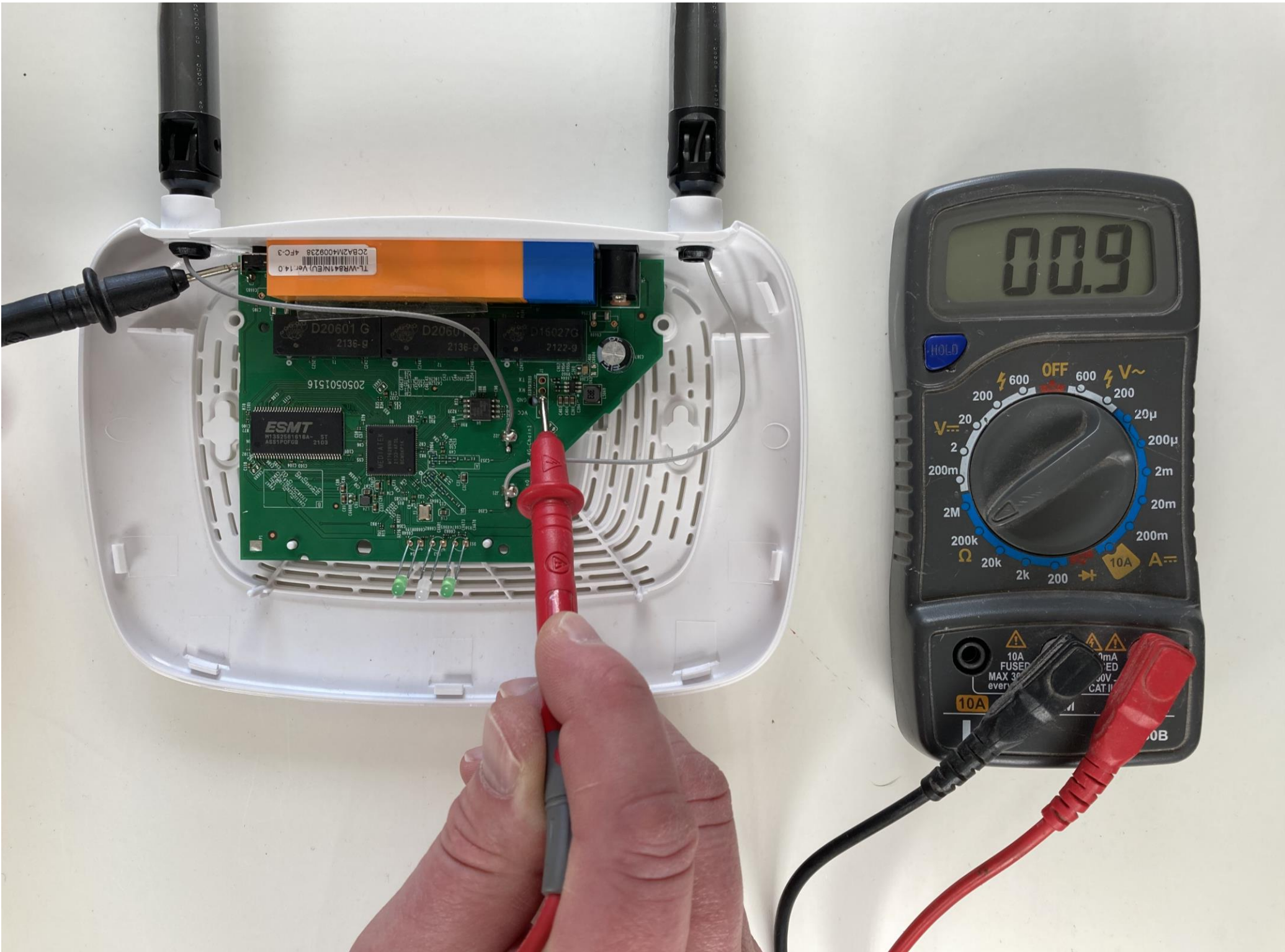
# Electrical Measurements

Pin	R <sub>GND</sub>	R <sub>VCC</sub>	V
1	4.5kΩ		
2			
3			
4			



# Electrical Measurements

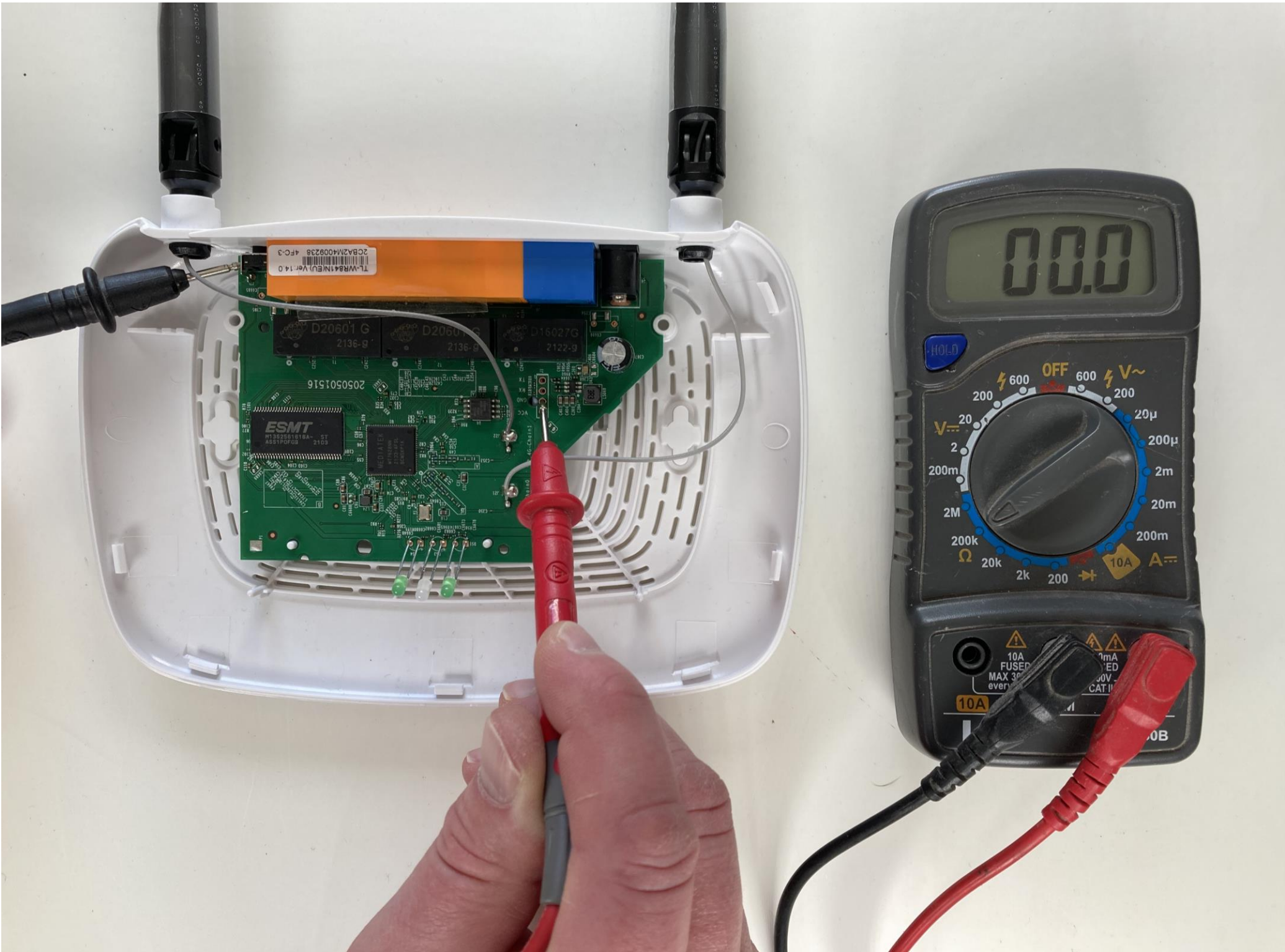
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$		
2	0.9k $\Omega$		
3			
4			





# Electrical Measurements

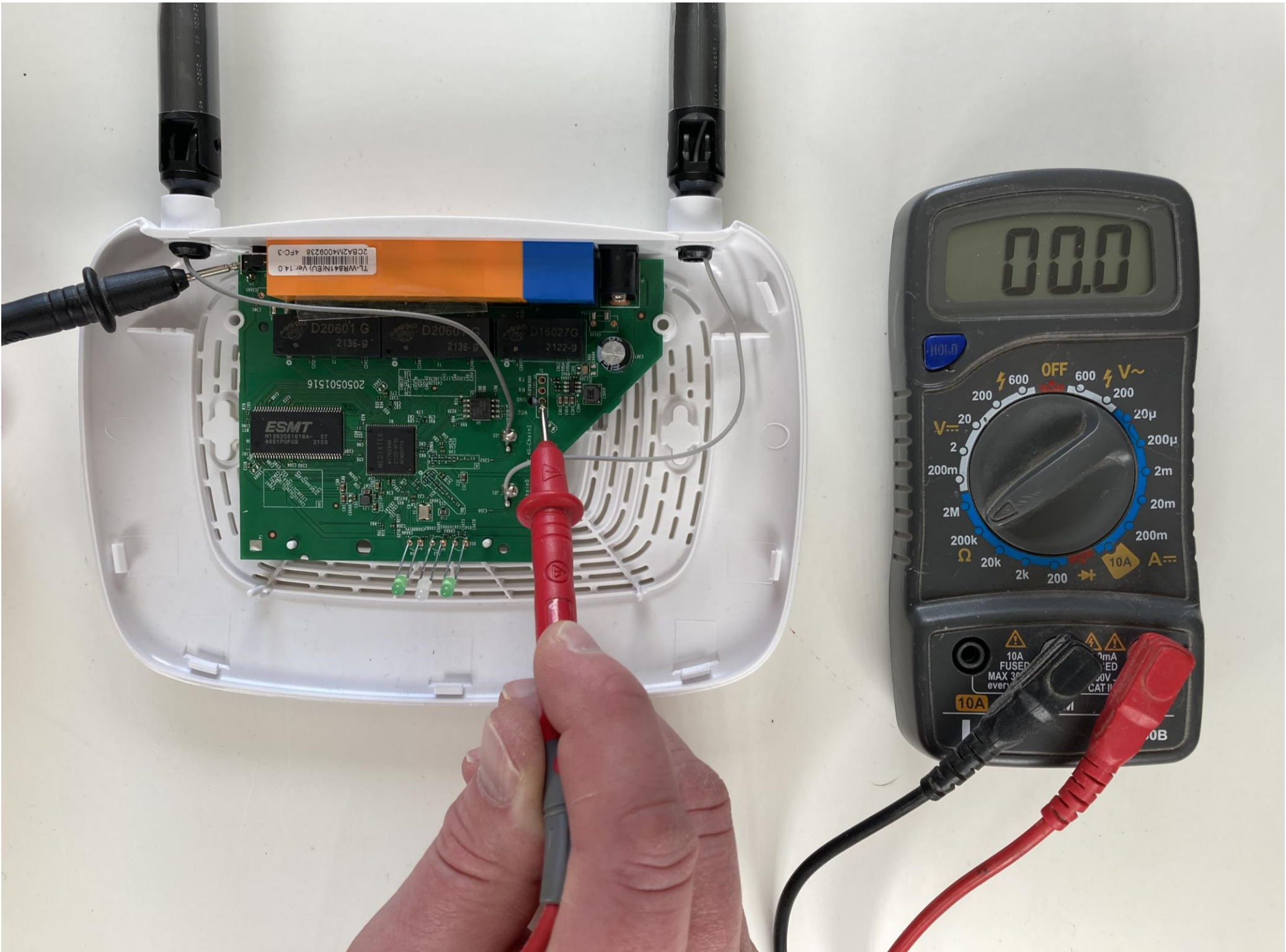
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$		
2	0.9k $\Omega$		
3			
4			





# Electrical Measurements

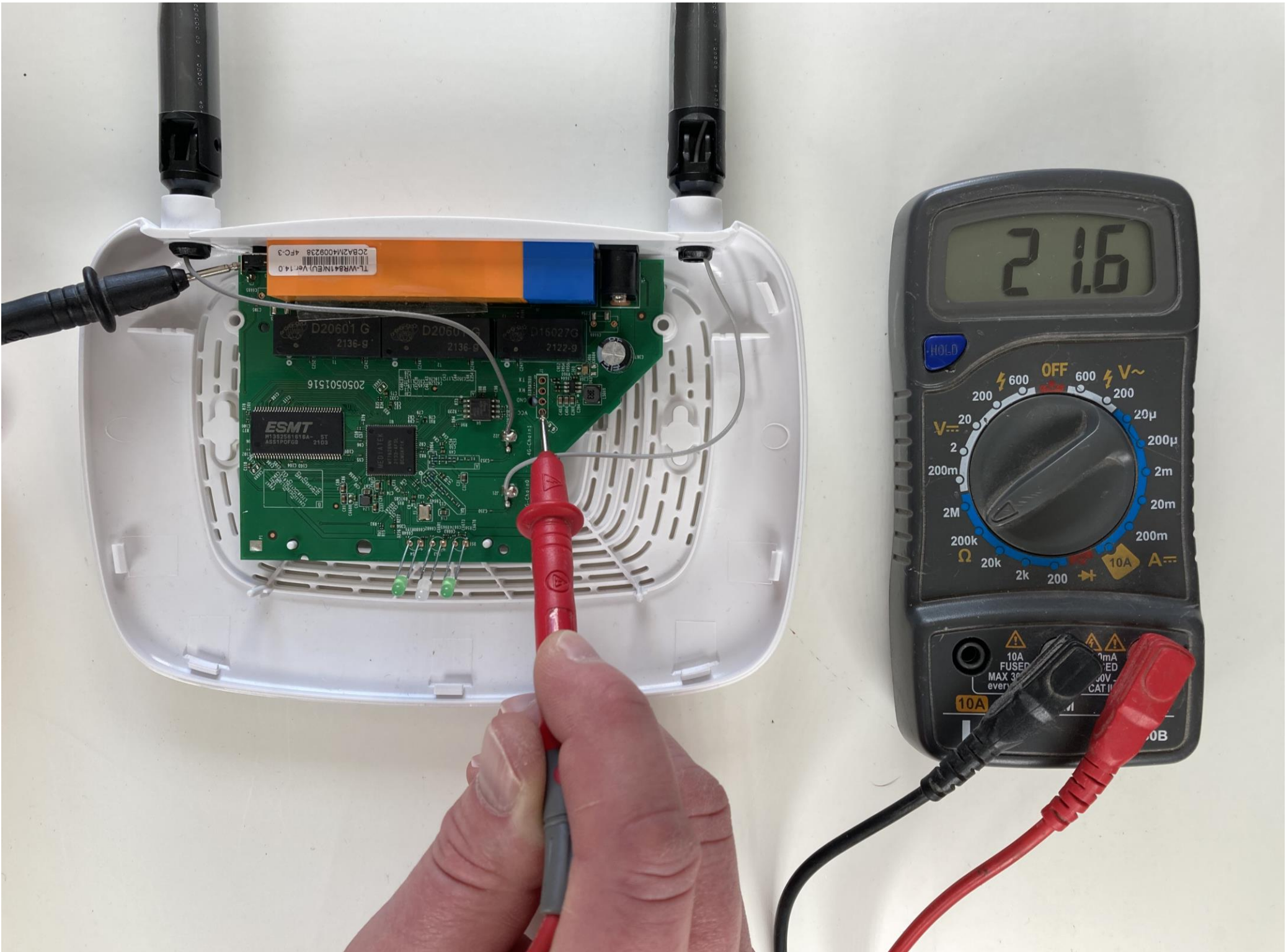
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$		
2	0.9k $\Omega$		
3	0.0k $\Omega$		
4			





# Electrical Measurements

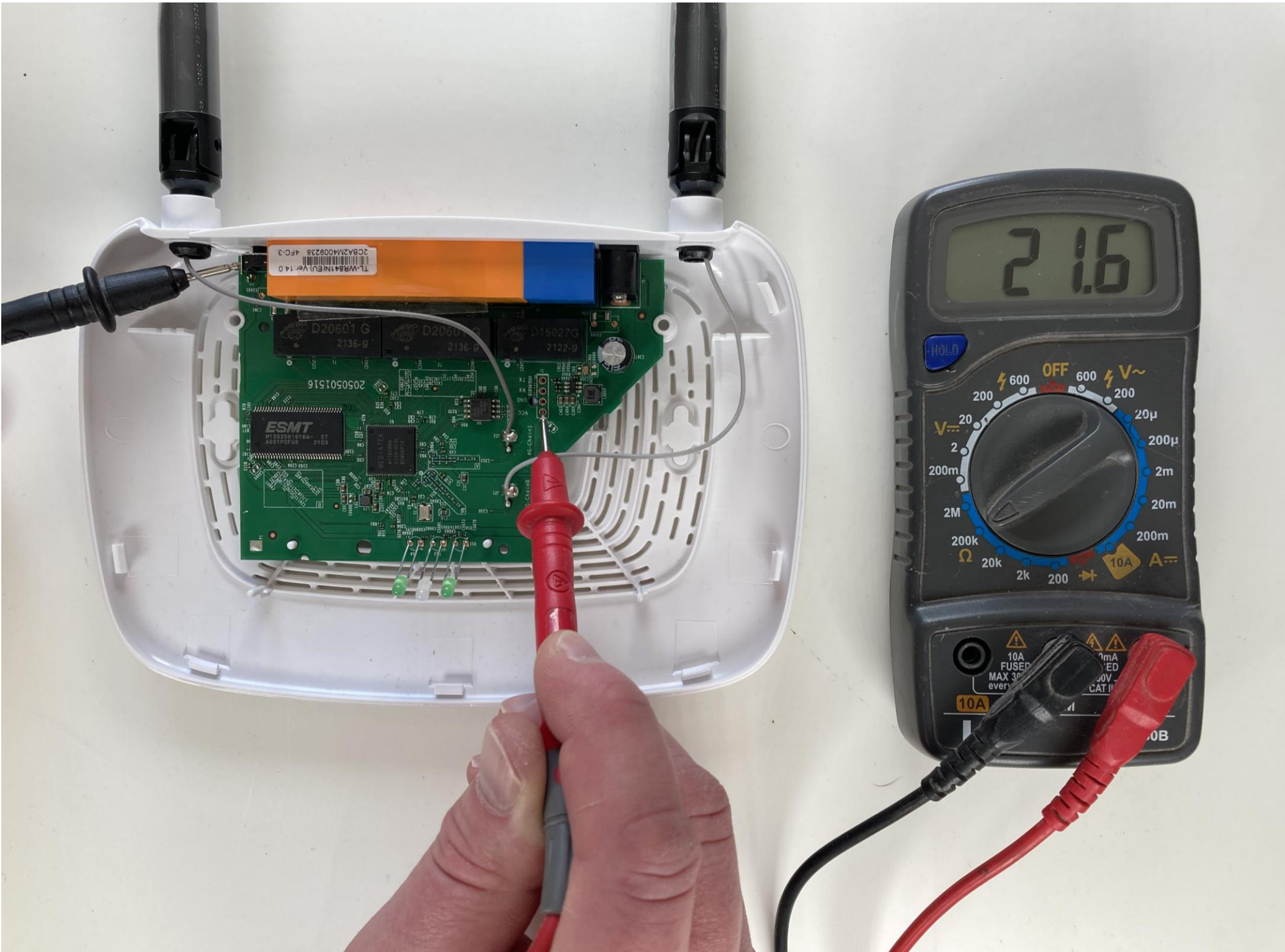
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$		
2	0.9k $\Omega$		
3	0.0k $\Omega$		
4			





# Electrical Measurements

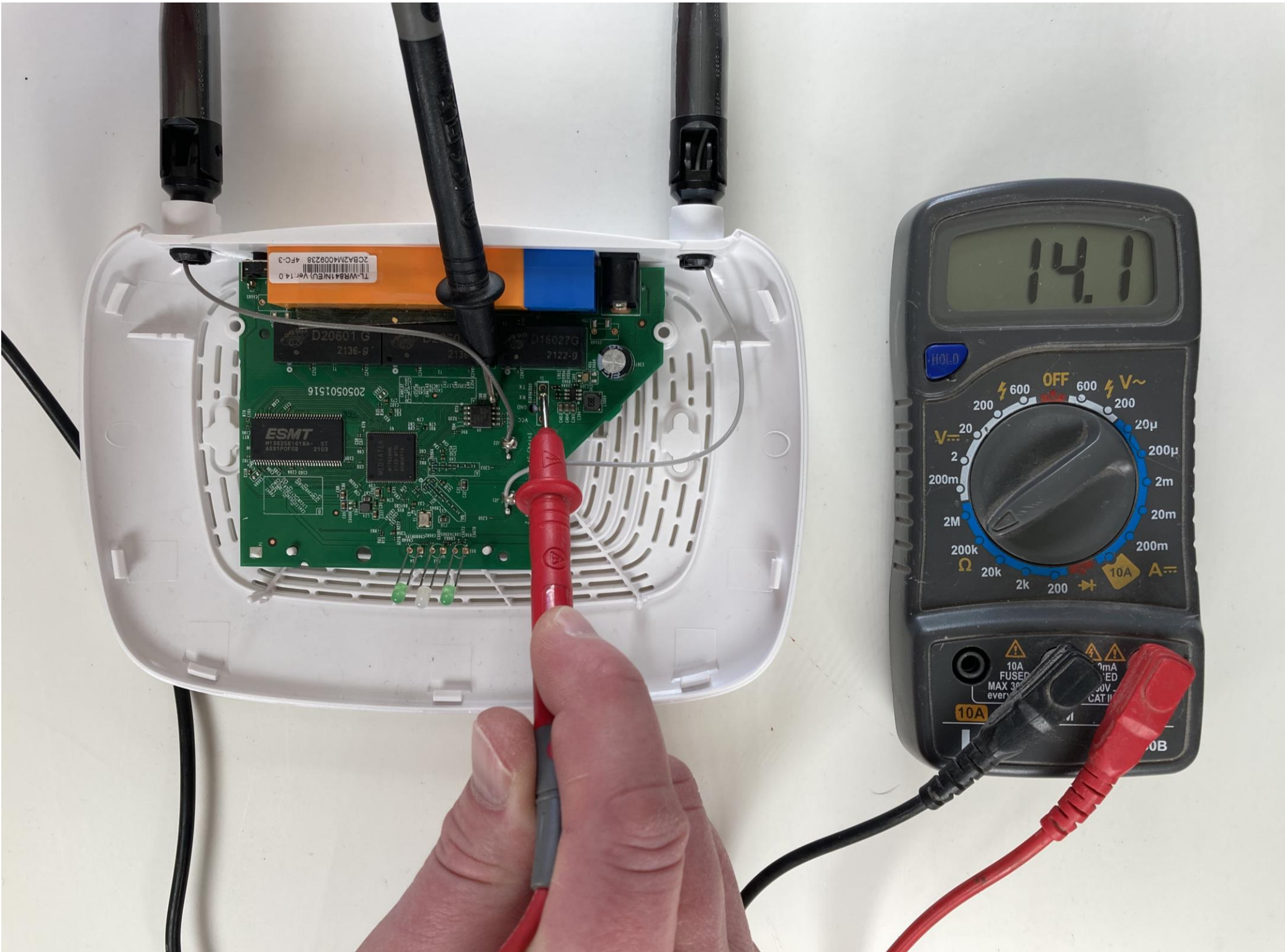
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$		
2	0.9k $\Omega$		
3	0.0k $\Omega$		
4	21.6k $\Omega$		





# Electrical Measurements

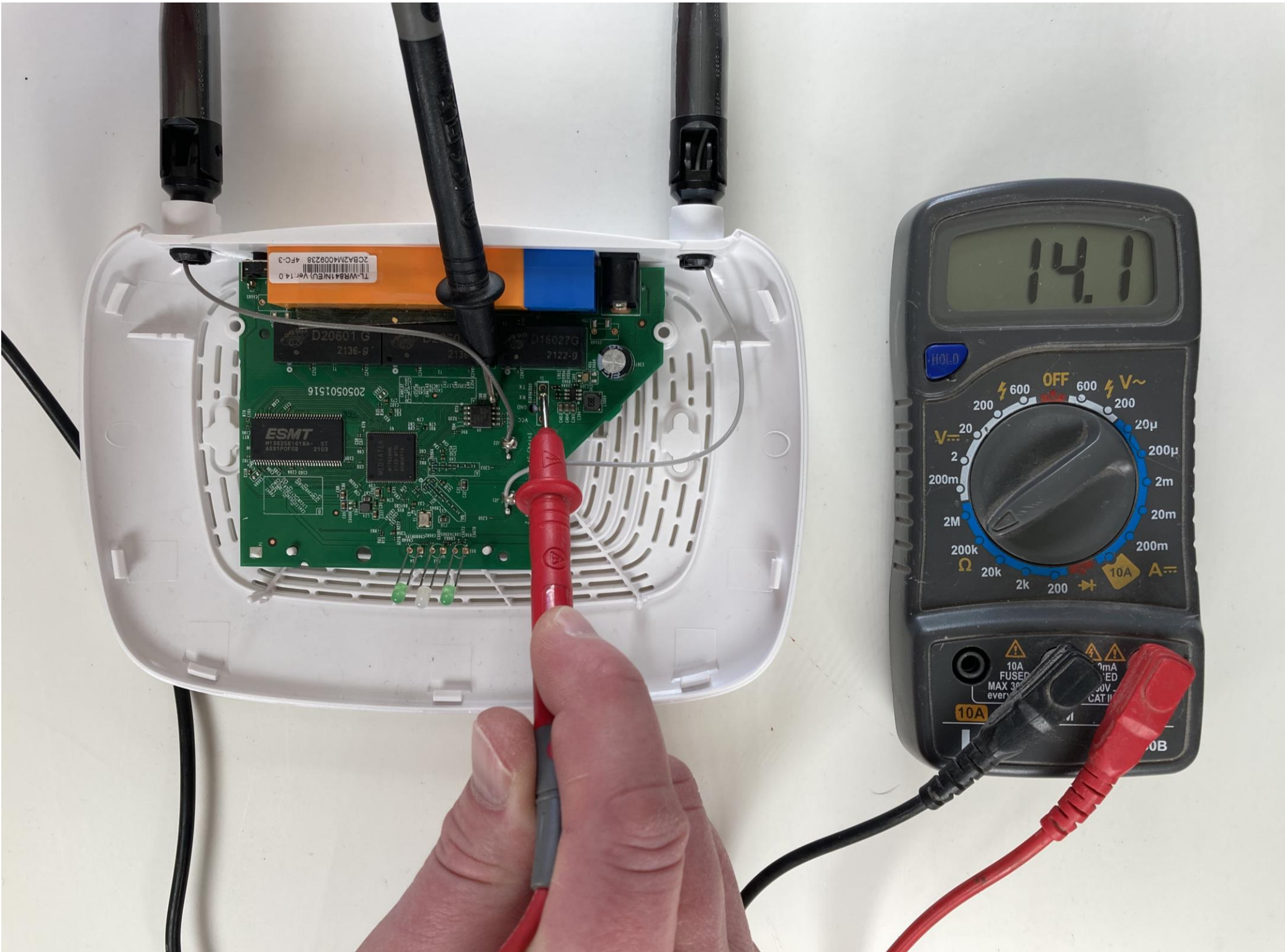
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$		
2	0.9k $\Omega$		
3	0.0k $\Omega$		
4	21.6k $\Omega$		





# Electrical Measurements

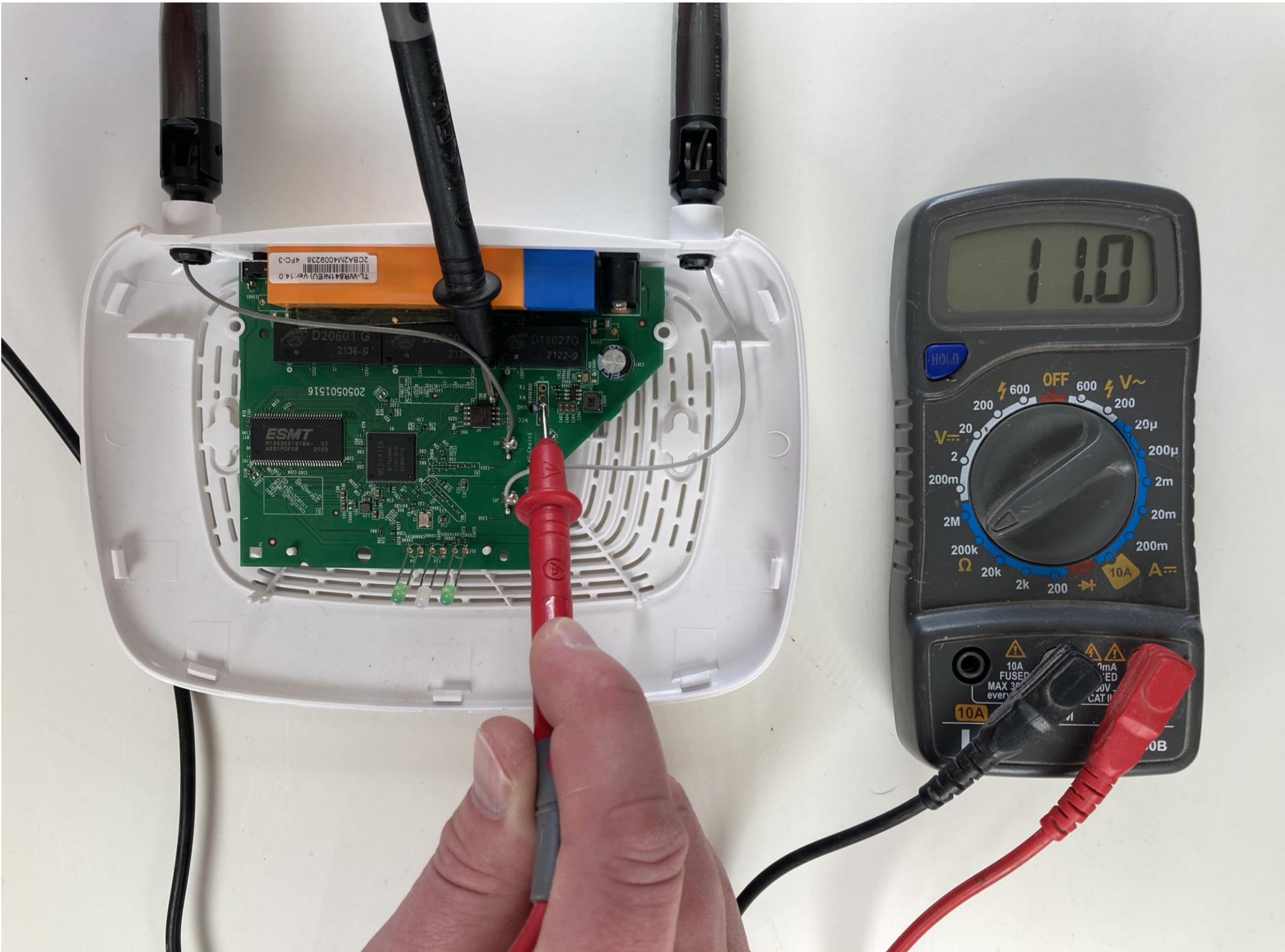
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	
2	0.9k $\Omega$		
3	0.0k $\Omega$		
4	21.6k $\Omega$		





# Electrical Measurements

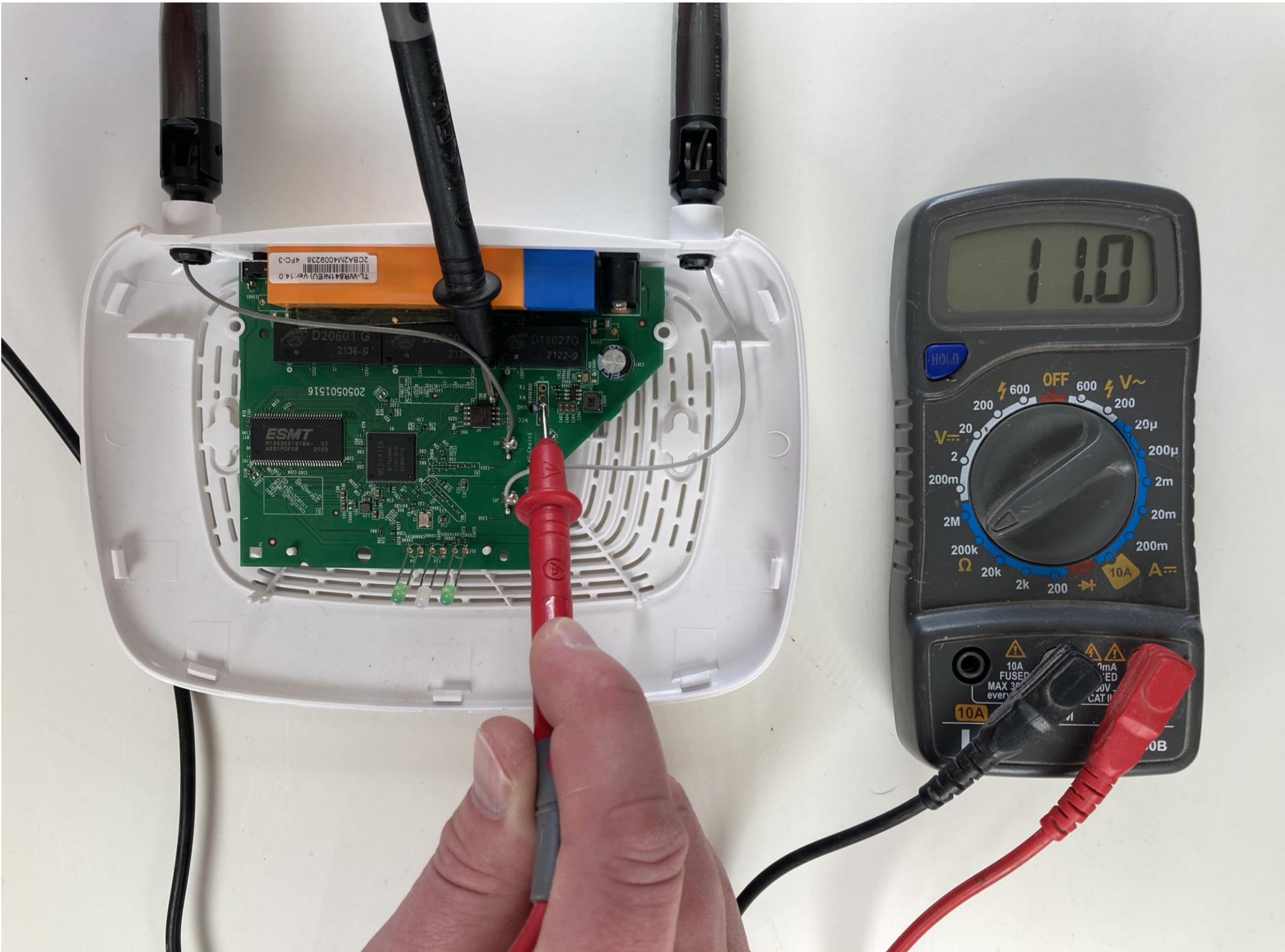
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	
2	0.9k $\Omega$		
3	0.0k $\Omega$		
4	21.6k $\Omega$		





# Electrical Measurements

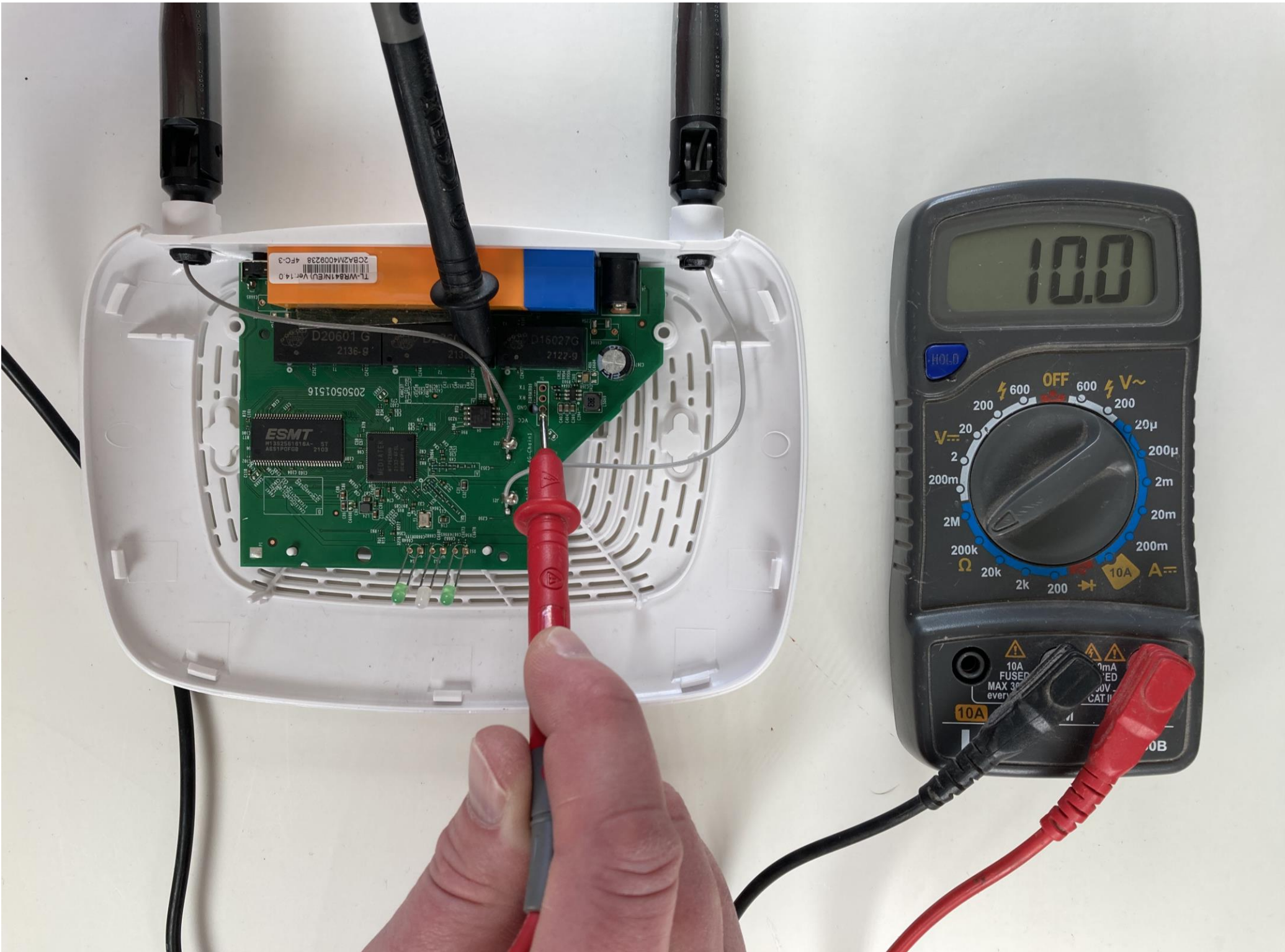
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	
2	0.9k $\Omega$	11.0k $\Omega$	
3	0.0k $\Omega$		
4	21.6k $\Omega$		





# Electrical Measurements

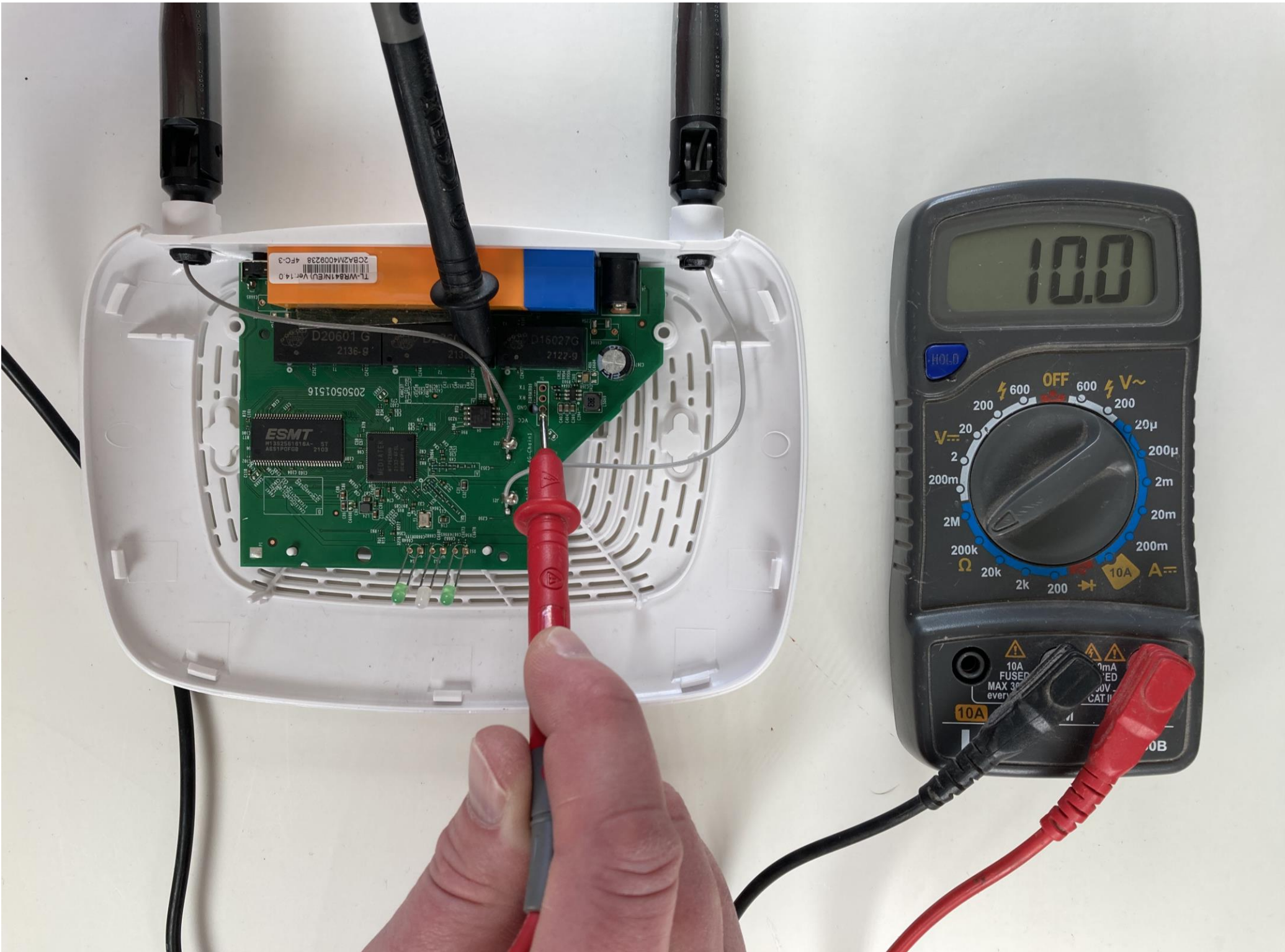
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	
2	0.9k $\Omega$	11.0k $\Omega$	
3	0.0k $\Omega$		
4	21.6k $\Omega$		





# Electrical Measurements

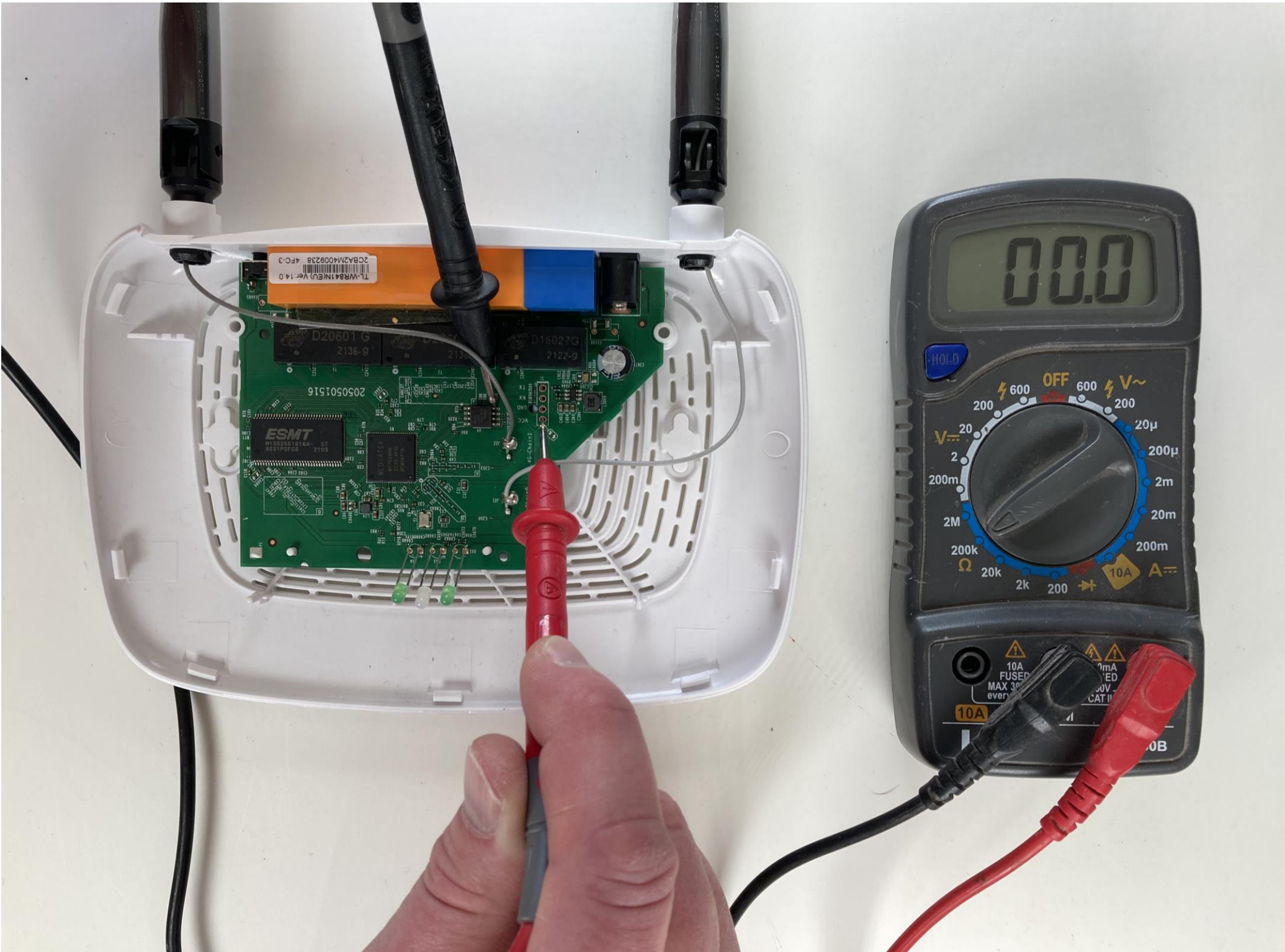
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	
2	0.9k $\Omega$	11.0k $\Omega$	
3	0.0k $\Omega$	10.0k $\Omega$	
4	21.6k $\Omega$		





# Electrical Measurements

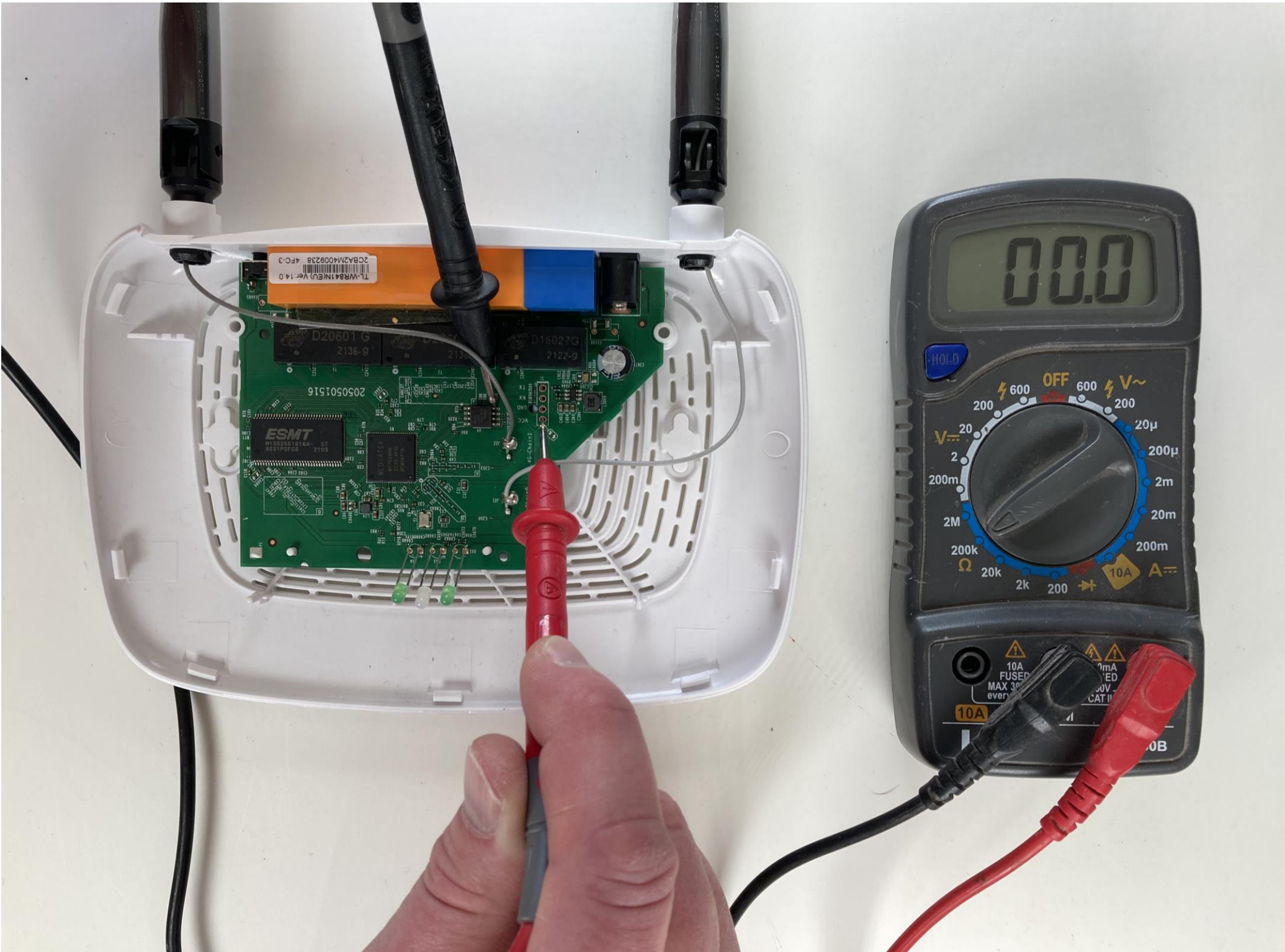
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	
2	0.9k $\Omega$	11.0k $\Omega$	
3	0.0k $\Omega$	10.0k $\Omega$	
4	21.6k $\Omega$		





# Electrical Measurements

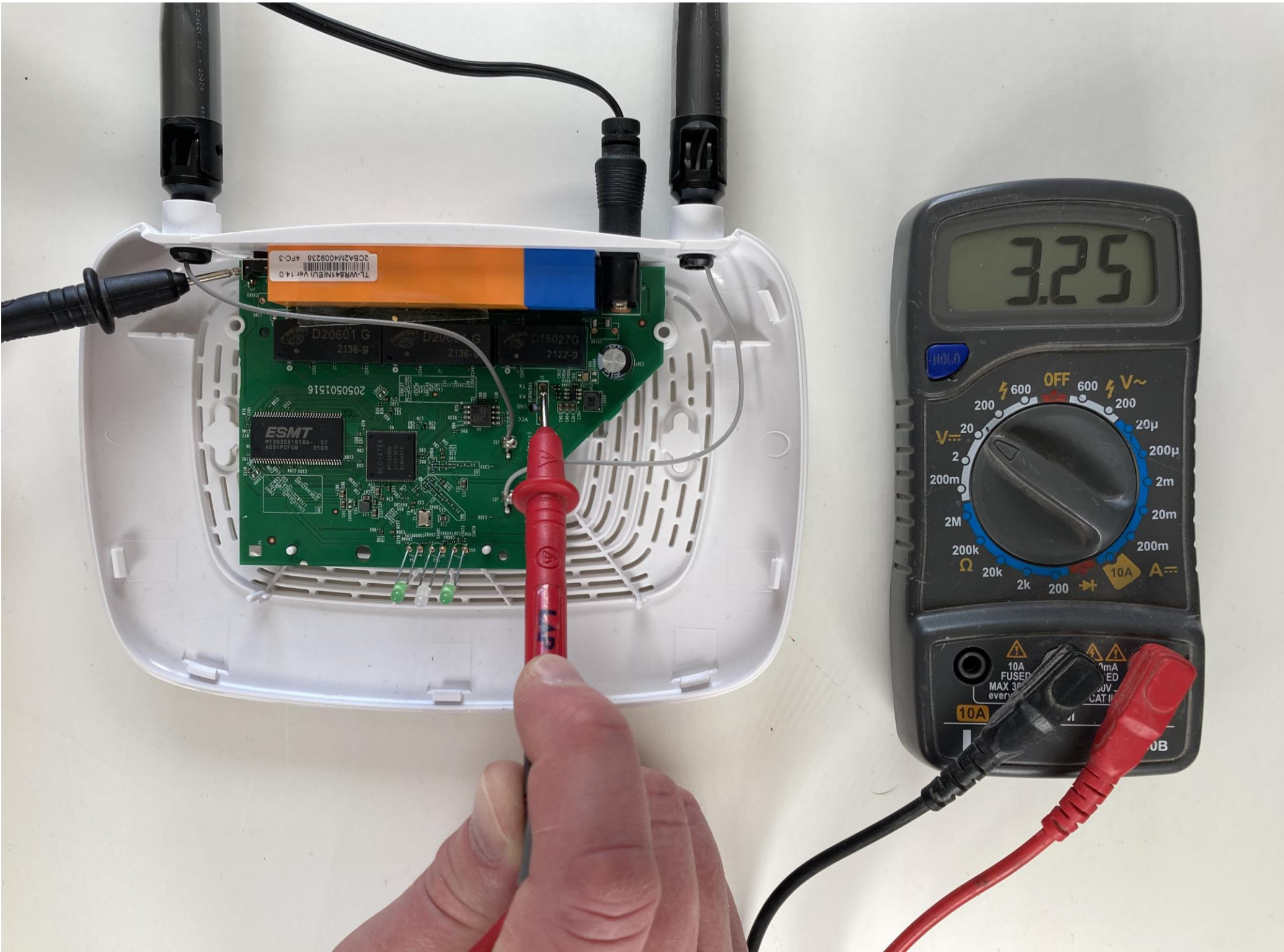
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	
2	0.9k $\Omega$	11.0k $\Omega$	
3	0.0k $\Omega$	10.0k $\Omega$	
4	21.6k $\Omega$	0.0k $\Omega$	





# Electrical Measurements

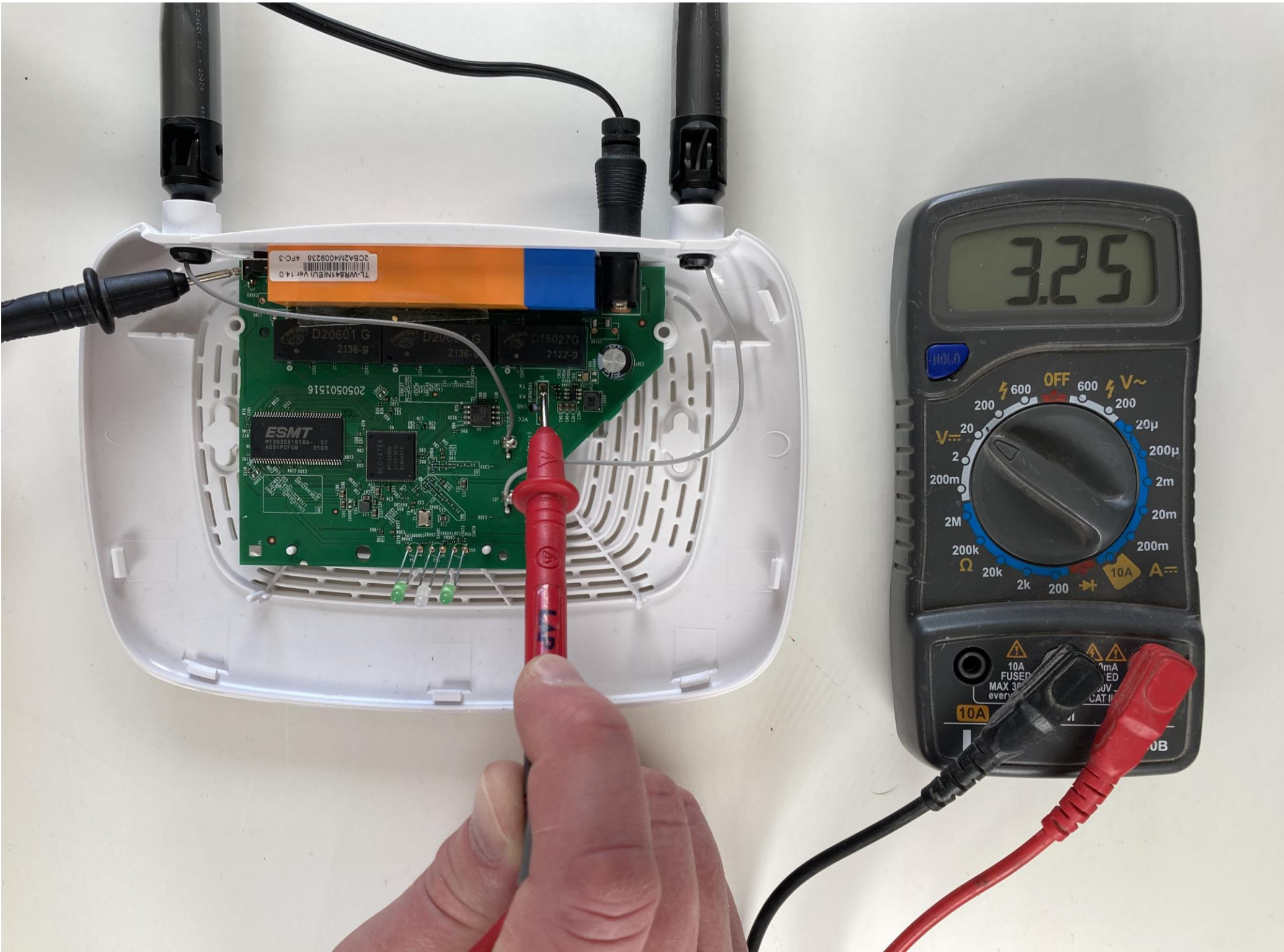
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	
2	0.9k $\Omega$	11.0k $\Omega$	
3	0.0k $\Omega$	10.0k $\Omega$	
4	21.6k $\Omega$	0.0k $\Omega$	





# Electrical Measurements

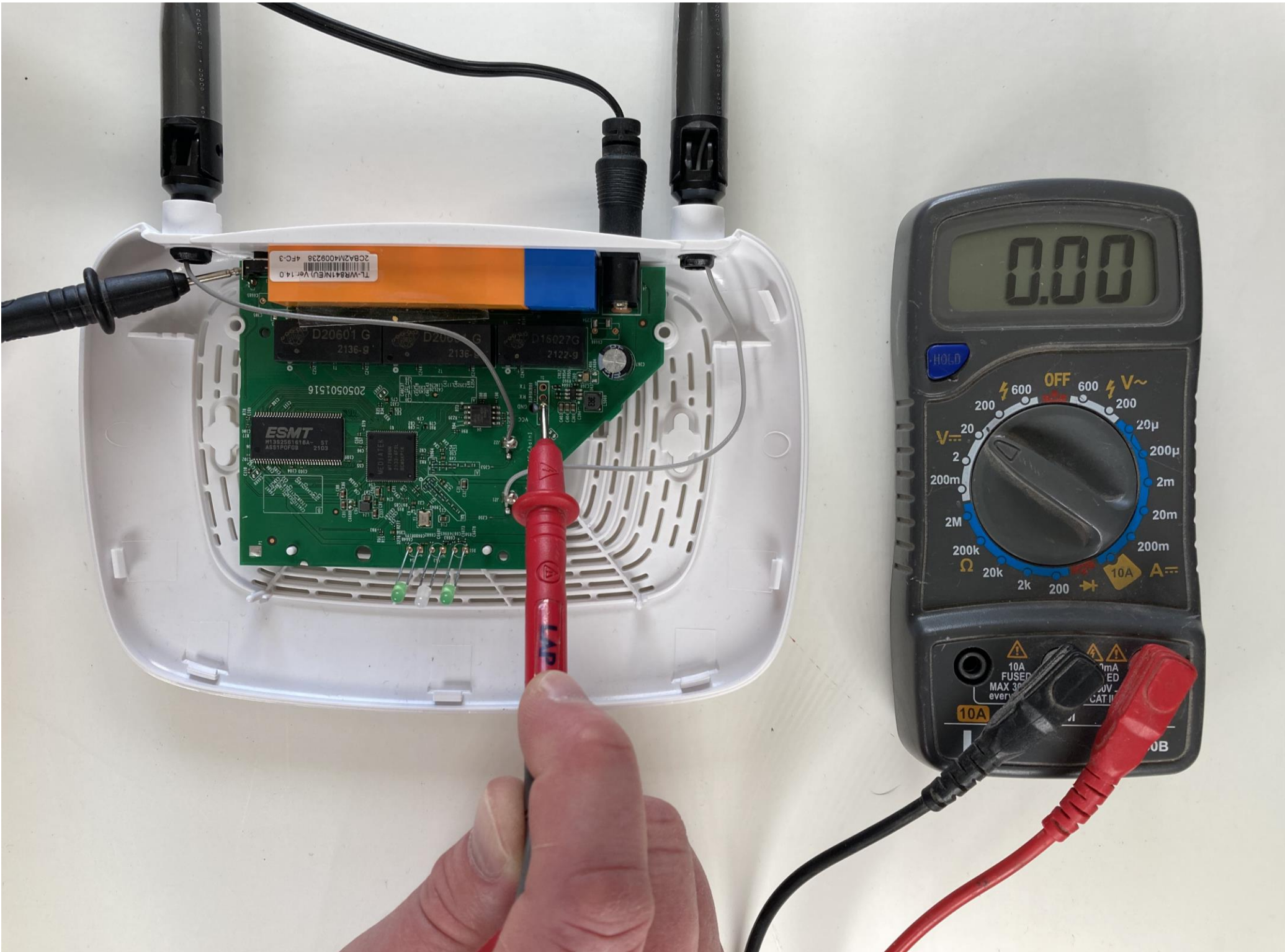
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	3.25V
2	0.9k $\Omega$	11.0k $\Omega$	
3	0.0k $\Omega$	10.0k $\Omega$	
4	21.6k $\Omega$	0.0k $\Omega$	





# Electrical Measurements

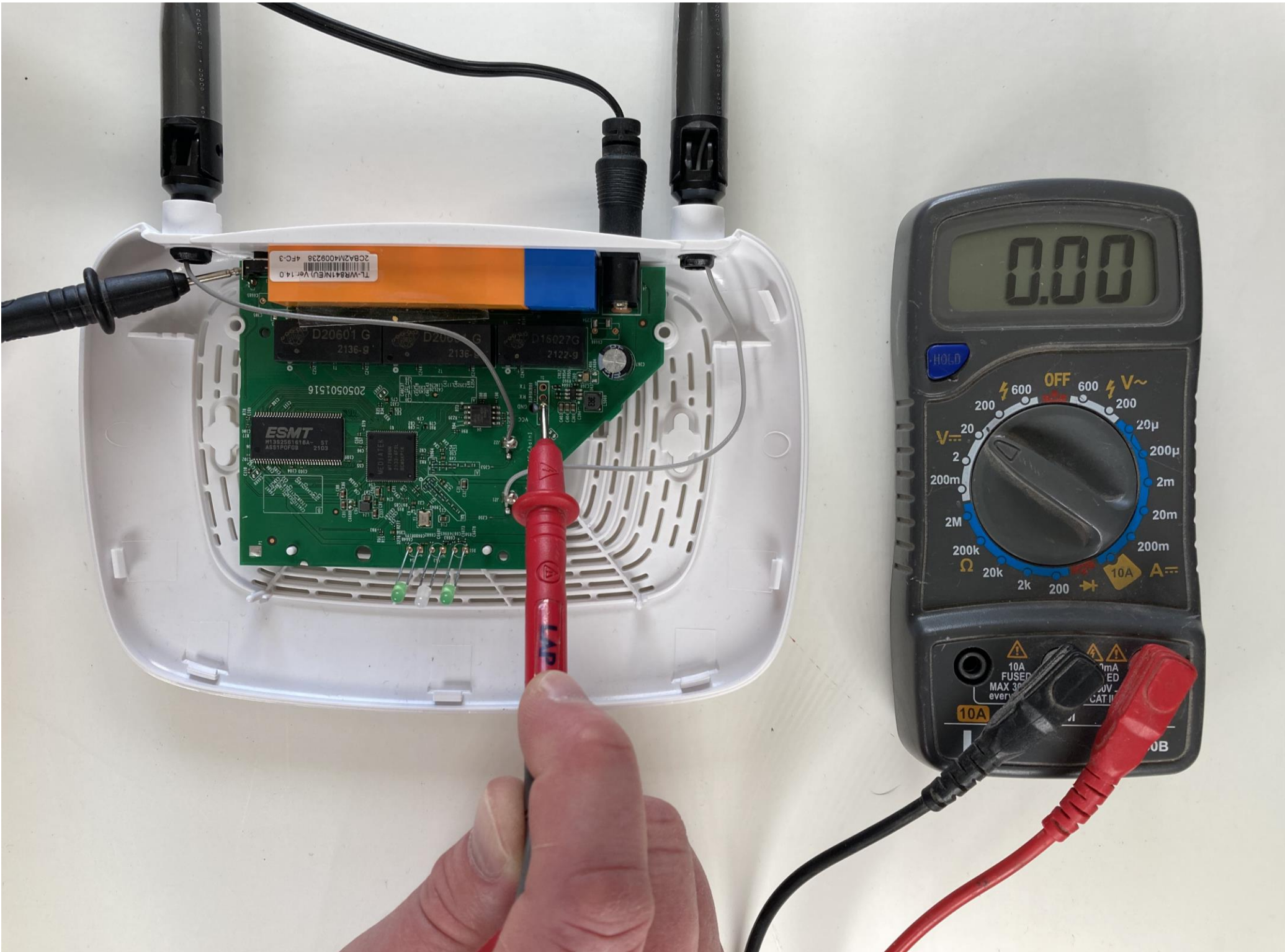
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	3.25V
2	0.9k $\Omega$	11.0k $\Omega$	
3	0.0k $\Omega$	10.0k $\Omega$	
4	21.6k $\Omega$	0.0k $\Omega$	





# Electrical Measurements

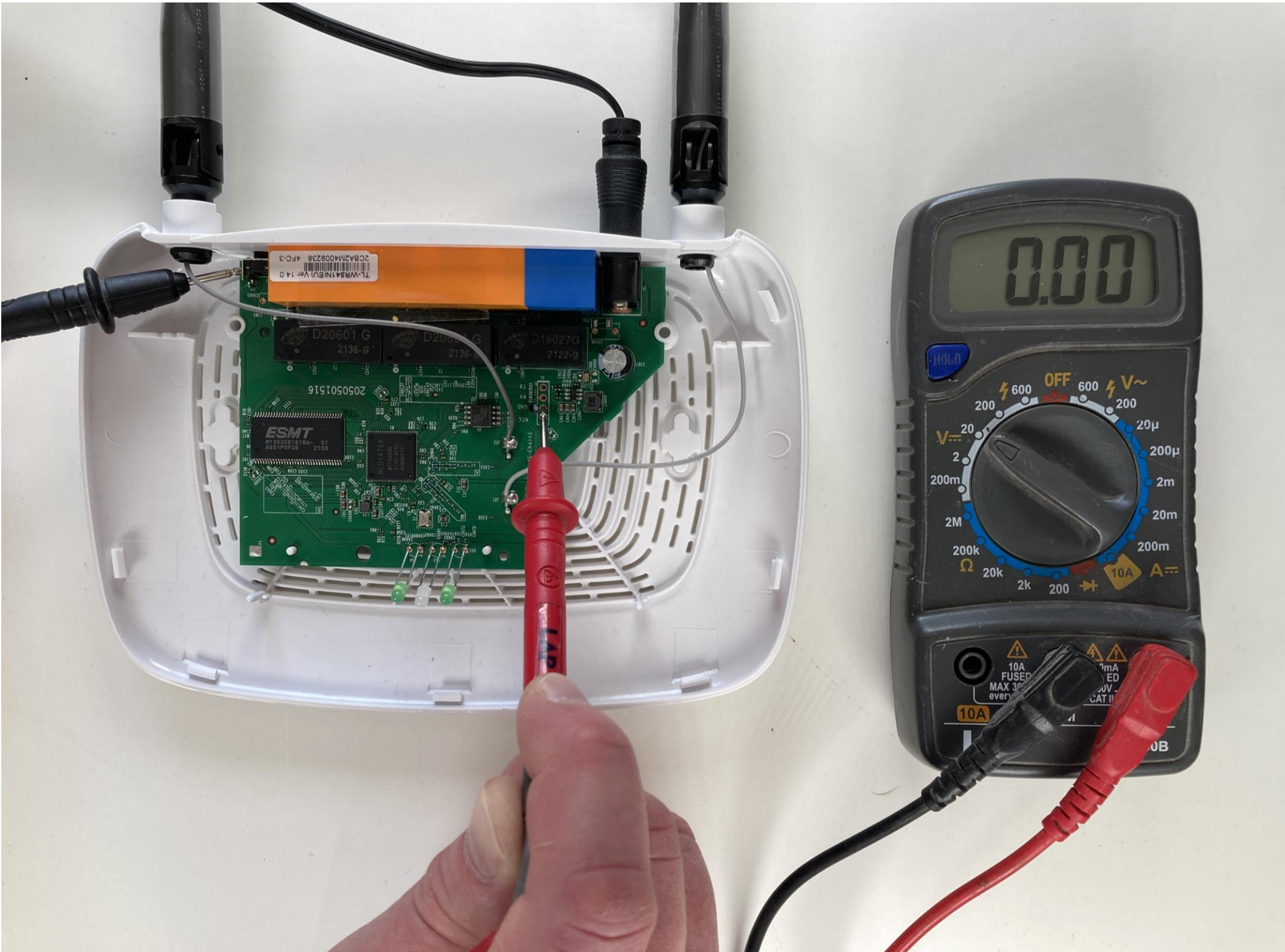
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	3.25V
2	0.9k $\Omega$	11.0k $\Omega$	0.0V
3	0.0k $\Omega$	10.0k $\Omega$	
4	21.6k $\Omega$	0.0k $\Omega$	





# Electrical Measurements

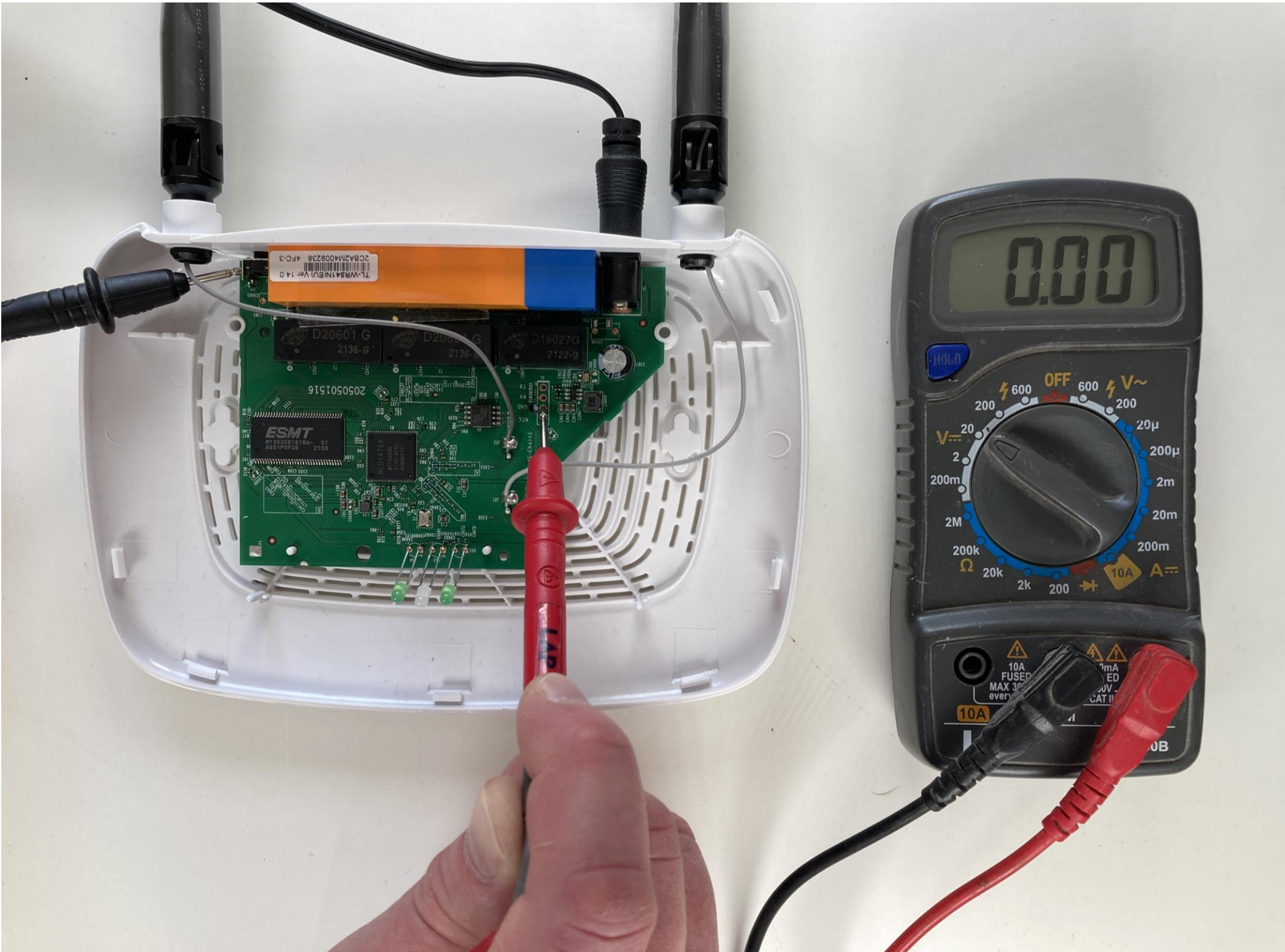
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	3.25V
2	0.9k $\Omega$	11.0k $\Omega$	0.0V
3	0.0k $\Omega$	10.0k $\Omega$	
4	21.6k $\Omega$	0.0k $\Omega$	





# Electrical Measurements

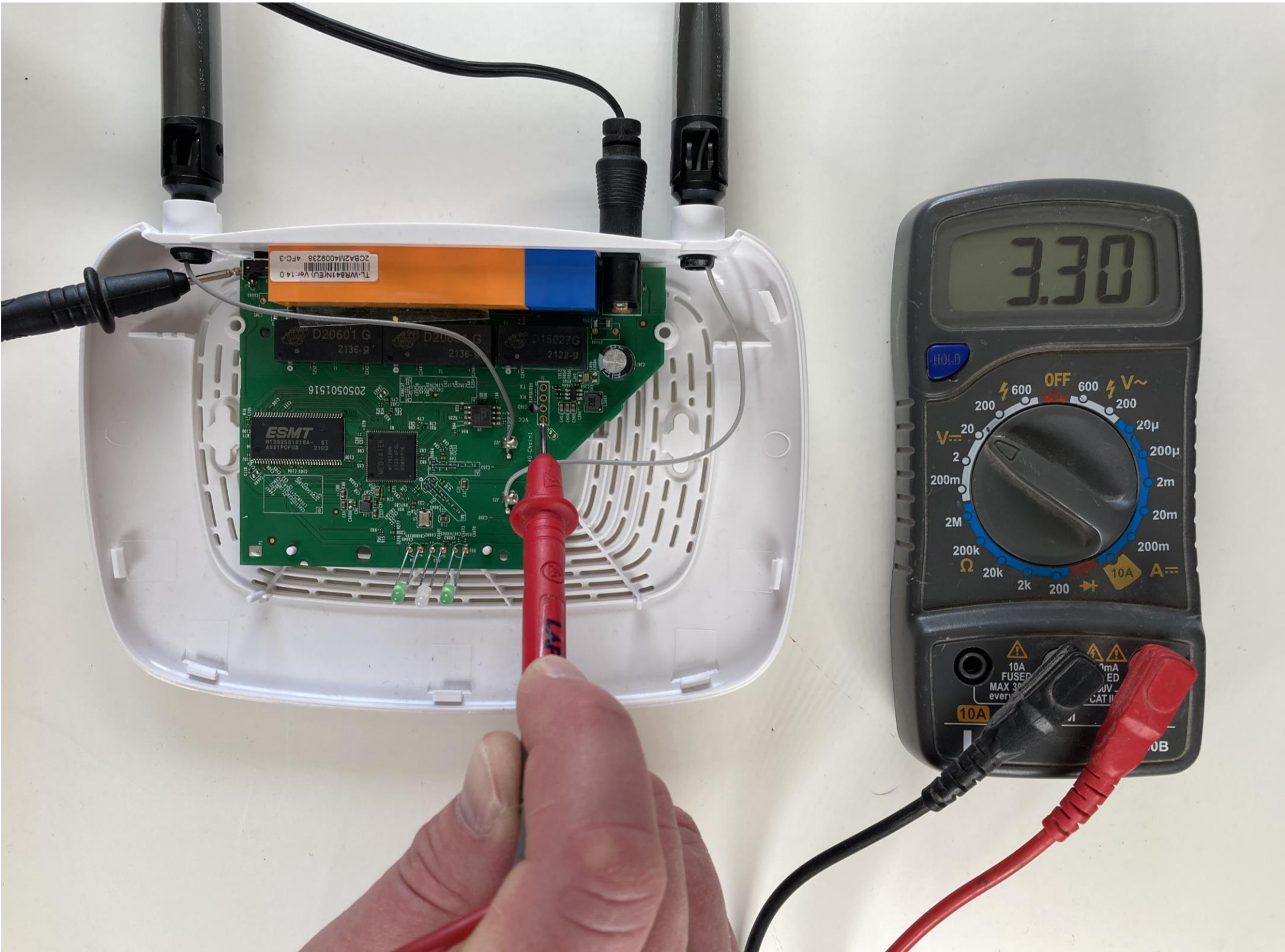
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	3.25V
2	0.9k $\Omega$	11.0k $\Omega$	0.0V
3	0.0k $\Omega$	10.0k $\Omega$	0.0V
4	21.6k $\Omega$	0.0k $\Omega$	





# Electrical Measurements

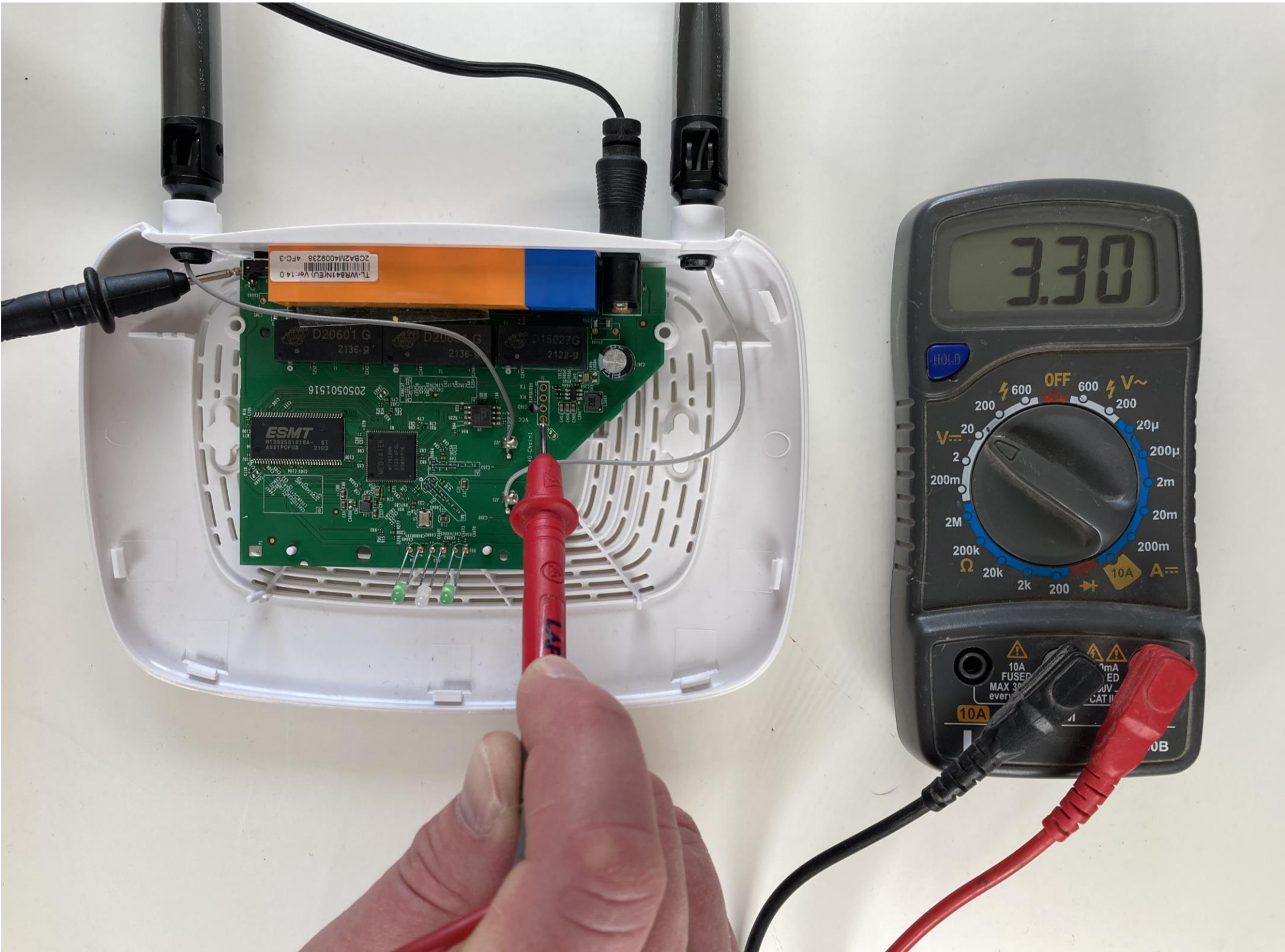
Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	3.25V
2	0.9k $\Omega$	11.0k $\Omega$	0.0V
3	0.0k $\Omega$	10.0k $\Omega$	0.0V
4	21.6k $\Omega$	0.0k $\Omega$	





# Electrical Measurements

Pin	$R_{GND}$	$R_{VCC}$	V
1	4.5k $\Omega$	14.1k $\Omega$	3.25V
2	0.9k $\Omega$	11.0k $\Omega$	0.0V
3	0.0k $\Omega$	10.0k $\Omega$	0.0V
4	21.6k $\Omega$	0.0k $\Omega$	3.3V





# Identifying UART Serial Pins

Pin	$R_{\text{GND}}$	$R_{\text{VCC}}$	V
1	4.5k $\Omega$	14.1k $\Omega$	3.25V
2	0.9k $\Omega$	11.0k $\Omega$	0.0V
3	0.0k $\Omega$	10.0k $\Omega$	0.0V
4	21.6k $\Omega$	0.0k $\Omega$	3.3V





# Identifying UART Serial Pins

Pin	$R_{\text{GND}}$	$R_{\text{VCC}}$	V	Tx
1	4.5k $\Omega$	14.1k $\Omega$	3.25V	
2	0.9k $\Omega$	11.0k $\Omega$	0.0V	
3	0.0k $\Omega$	10.0k $\Omega$	0.0V	
4	21.6k $\Omega$	0.0k $\Omega$	3.3V	





# Identifying UART Serial Pins

Pin	$R_{\text{GND}}$	$R_{\text{VCC}}$	V	
1	4.5k $\Omega$	14.1k $\Omega$	3.25V	Tx Rx
2	0.9k $\Omega$	11.0k $\Omega$	0.0V	
3	0.0k $\Omega$	10.0k $\Omega$	0.0V	
4	21.6k $\Omega$	0.0k $\Omega$	3.3V	





# Identifying UART Serial Pins

Pin	$R_{GND}$	$R_{VCC}$	V	
1	4.5k $\Omega$	14.1k $\Omega$	3.25V	Tx
2	0.9k $\Omega$	11.0k $\Omega$	0.0V	Rx
3	0.0k $\Omega$	10.0k $\Omega$	0.0V	Gnd
4	21.6k $\Omega$	0.0k $\Omega$	3.3V	





# Identifying UART Serial Pins

Pin	$R_{GND}$	$R_{VCC}$	V	
1	4.5k $\Omega$	14.1k $\Omega$	3.25V	Tx
2	0.9k $\Omega$	11.0k $\Omega$	0.0V	Rx
3	0.0k $\Omega$	10.0k $\Omega$	0.0V	Gnd
4	21.6k $\Omega$	0.0k $\Omega$	3.3V	V <sub>cc</sub>



# Up Next: Obtaining Firmware

---

