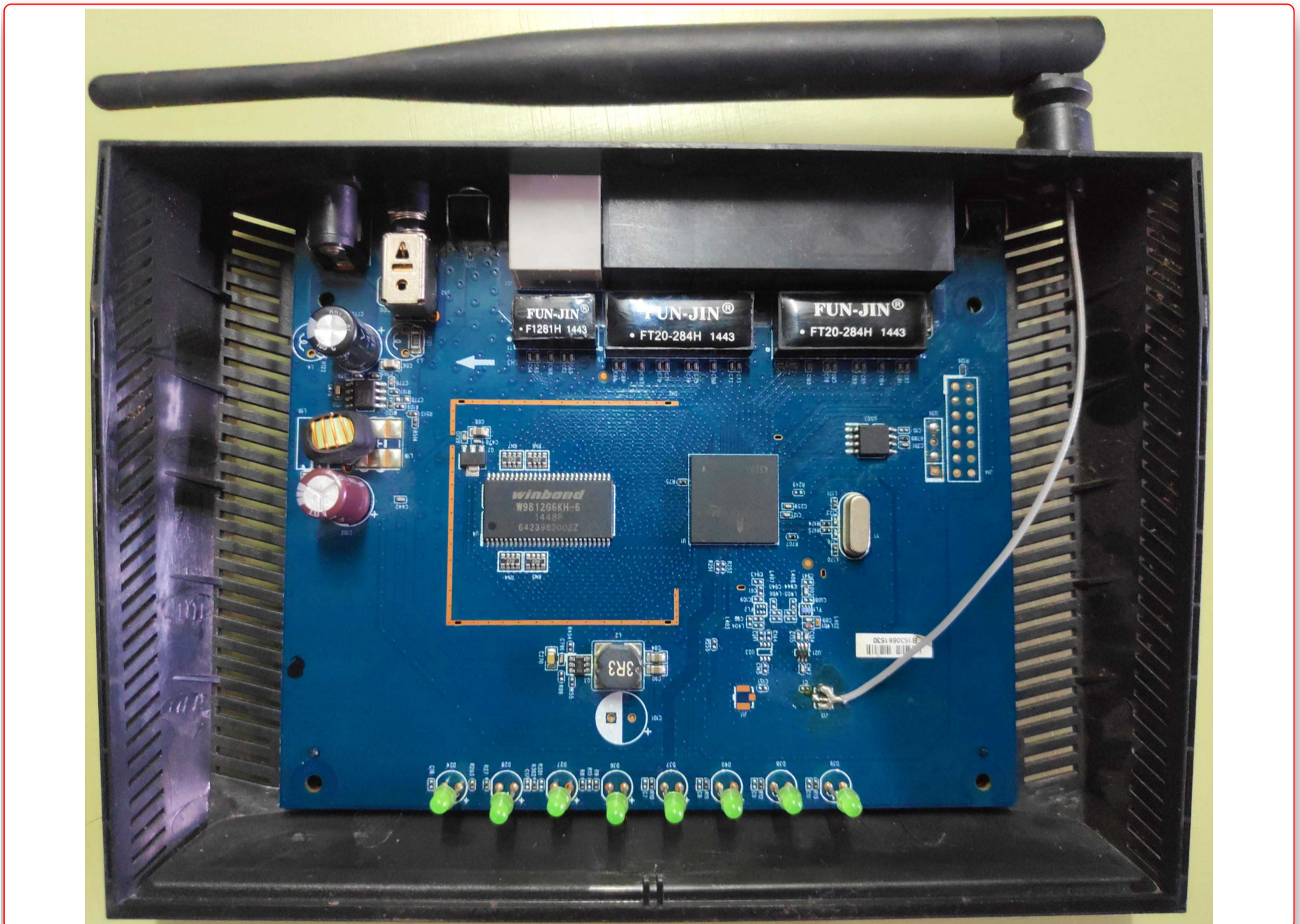


IoT Security-Part 13 (Introduction To Hardware Recon)



Shakir

1-September-2020



IoT Security Part 13 (Introduction to Hardware Recon)

This blog is part of the IoT Security series where we discuss the basic concepts pertaining to the IoT/IIoT eco-system and its security. If you have not gone through the previous blogs in the series, I would urge you to go through those first. In case you are only interested in the basics of Hardware recon, feel free to continue.

[IoT Security - Part 1 \(101 - IoT Introduction And Architecture\)](#)

[IoT Security - Part 12 \(MQTT Broker Security - 101\)](#)

In this blog, we will discuss how to perform reconnaissance on hardware. The hardware comprises physical electronics components that include micro-controller, microprocessor, resistor, capacitor, LEDs, etc. which make a device work. The hardware reconnaissance process

consists of several steps like device disassembly, looking at the various components, debug ports like UART, JTAG/SWD, identifying the chips, finding the respective datasheet, and finding the information from the datasheet. so let's get into each of them.

Importance of Hardware Recon

During the process of pentesting or security research in general, before starting to attack the target we have to have a complete understanding of the system even if it is a blackbox. The recon process helps in identifying different components that make up the system so we can gear our attacks towards what we know and what loopholes we have identified while understanding the system. During the recon, we identify pieces and connect those pieces to derive intelligent information that will help in compromising the security of the system. When attacking a hardware device, we need to first understand what is the hardware made up of i.e. what are the different components of the hardware to be able to create an effective threat model and mis-use cases to be used while finding vulnerabilities. We will see below what is the basic information derived during this process.

Hardware Tools

We will need some key pieces of physical equipment to perform hardware reconnaissance.

1. Multimeter:

A multimeter is a very important tool for circuit probing. It will help us to test all the components and to measure resistance, voltage, and current level and electric continuity between two points.

2. A soldering iron, Solder, Flux, Tweezer, Soldering wick, Cutter, Wire stripper:

These are soldering tools, useful to add and remove the components from the PCB.

3. Screwdriver set:

Necessary for disassembling the device. Nowadays device disassembly is quite a tough job sometimes manufacturers use tamper protection to prevent people from gaining access to internal components of the device.

4. Jumper wires:

Useful to connect two devices electrically.

5. Desoldering Pump/Hot Air Rework:

The Desoldering pump requires removing SMD components without destroying the PCB with a suitable temperature.

6. Magnifying Glass:

Useful to see the components clearly and helps in recognizing the components model, make, and part numbers. Usually, they are written in very small sizes that are difficult to read with the naked eye.

7. Vise Stand:

Useful to hold PCB while soldering or desoldering components. or while inspecting PCB



Fig 1. Hardware tools

Basic knowledge of electronics:

Basic Electronics is one of the most important things to understand if you want to get into hardware hacking. you will need to understand what is happening in the device and how any given component can be exploited. So here we will look at some basic electronic components and the purpose of using them in circuits.

1. Resister: It adds resistance between two components. It is measured in ohms.
2. Capacitor: It charges and discharges in specific Interval of time and used to stabilize the power supply in Circuit. It is measured in farad.
3. Inductors: They are used for filtering and smoothing high-frequency noise in the circuit using electromagnetic discharge. It is measured in Henry.
4. IC: Integrated Circuits is a set of electronic circuits on small pieces of silicon.
5. LED: Light Emitting Diode.
6. EEPROM (Electrically Erasable Programmable Read-Only Memory): Embedded devices use these as a means of storage.
7. Crystals: These oscillate at a given frequency, similar to a timer.
8. Transformers: They are used to convert voltage levels. Mostly used for converting AC mains to DC supply with some extra circuitry.
9. Diodes: Used to restrict current flow in one direction.
10. Relay: It is a switch that controls (open and close) circuits electromechanically.

11. Microcontroller/Microprocessor: It is a tiny little computer on a single metal-oxide-semiconductor (MOS) integrated circuit (IC) chip.
12. SoC (System on Chip): They can be just a Processor or Processor + memory + peripherals.
13. Transister: It is used to amplify and switch the signals and electrical power.
14. Battery: It converts chemical energy into electrical energy.
15. Motor: It converts electrical energy into mechanical energy.
16. Switch: It interrupts the current.
17. PCB: Printed circuit board (PCB) is a non-conductive material with conductive lines printed or etched.

Different types of packages of components:

The packages are divided into two types based on the how the mounted on a Printed circuit board(PCB).

Through-hole mount package:

This type of component is designed in such a way that the pins of the component are inserted in the PCB and another side of the PCB pin can be solderable. These types of components are bigger than surface-mount packages. These components are cheaper as compared to SMD components. See the different types of Through-hole gull-wing components below the photo.



Fig 2. IC Package-Through-hole

[Image source](#)

Surface Mount Package:

The surface-mount package component mounts directly on the PCB surface. This type of component takes minimum size and takes less time to assemble but it also increases the chances of defects. Below are the type of SMD package components



Fig 3. IC Package-Surface Mount

[Image source](#)

Types of SMD components:

- Small Outline L-leaded Packages (SOP) This type has gull-wing type leads that come out from the body in the L shape and can be mounted directly on the PCB
- Quad flat L-shape packages (QFP) This is the same to SOP only difference is that pins come out from 4 direction instead of 2 and can be mounted directly on the PCB.
- Ball Grid Array(BGA) These types of packages have a solder ball array on the backside of Component.

Printed Circuit Board (PCB)

Now we have a good understanding of electronic components and its different packages. So what next?

Here we will discuss PCB, Printed circuit board (PCB) is a nonconductive material with conductive lines printed or etched. Electronic components mounted on the PCB board such as Transistors, resistors, capacitors, integrated circuits(ICs) and the traces connect the components to form a working circuit. PCBs are most commonly made of fiberglass, composite epoxy, or other composite material. PCBs are made up of multiple layers. Even a simple single sided (one layer) board is made up of a conductive metal layer and a substrate layer composited together. As the complexity of the PCB increases, so will the amount of layers within it.



Fig 4. PCB Top side



Fig 5. PCB Bottom side

There are a lot of software tools available for designing a PCB like Kicad, Eagle, Orcad. We use Kicad for PCB design. It's easy to use and has the feature to view PCB in 3d.

PCB gives us a lot of information like different components, debug ports, test pads, etc. used. It helps researchers create a threat model/mind map of attack scenarios for the device.

FCC ID:

An FCC ID is a unique identifier assigned to hardware products registered with the United States Federal Communications Commission (Hence, the name FCC ID). Most of the smart devices have an FCC ID which will give you a lot of details about the device like internal photos of the device, operating frequency, etc. This information is crucial for identifying the components as well as understanding the RF technology used in the device. You can search for the details of the devices by their FCC IDs on [fcc.gov](https://www.fcc.gov).

Let's search for the details of an Edimax Camera device for example. It's FCC ID is NDD9530401309. As you can see we get a lot of interesting device-related information.



Fig 6. Edimax Camera

11 Matches found for FCC ID NDD9530401309

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
DOC letter	Cover Letter(s)	11/27/2013	pdf	11/27/2013
ad hoc mode letter	Cover Letter(s)	11/27/2013	pdf	11/27/2013
LTC request	Cover Letter(s)	11/27/2013	pdf	11/27/2013
PoA	Cover Letter(s)	11/27/2013	pdf	11/27/2013
ext photos	External Photos	11/27/2013	pdf	11/27/2013
label	ID Label/Location Info	11/27/2013	pdf	11/27/2013
int photos	Internal Photos	11/27/2013	pdf	11/27/2013
MPE	RF Exposure Info	11/27/2013	pdf	11/27/2013
test report	Test Report	11/27/2013	pdf	11/27/2013
test setup photos	Test Setup Photos	11/27/2013	pdf	11/27/2013
user manual	Users Manual	11/27/2013	pdf	11/27/2013

Fig 7. FCC ID Table

Disassembly:

Depending on the device that has been put together we have to use appropriate tools to take apart all different parts. We also recommend that you have a good screwdriver toolkit for the entire hardware assessment process as varying devices will have different kinds of screws used in them. So, here we will perform hardware recon on the ASUS RT-N10E wifi router. we will disassemble the router to access the Printed circuit board. There are 4 screws on the backside of the device that should be removed, then the plastic enclosure can pull apart.

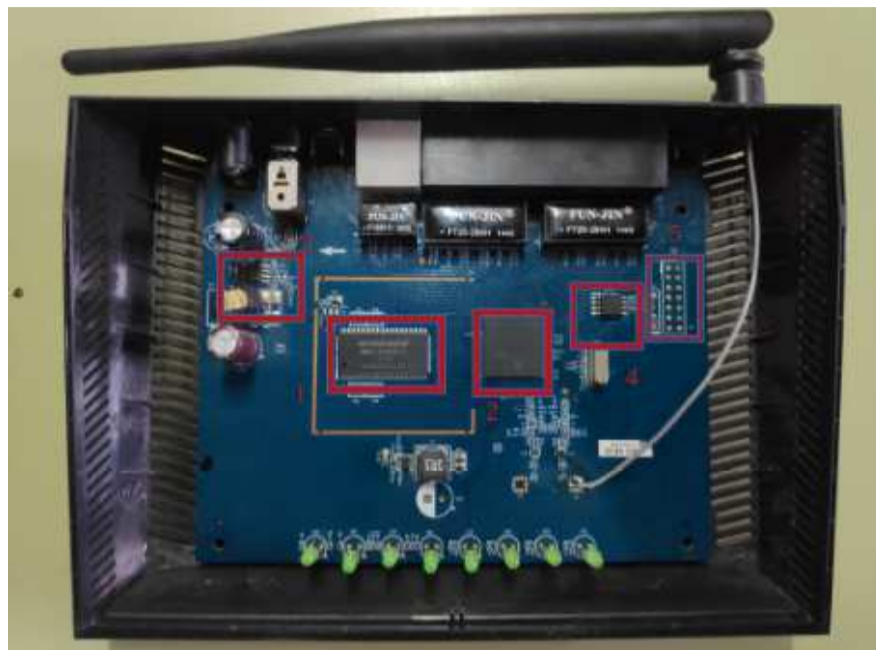


Fig 8. ASUS router

PCB Board Analysis

This is a very simple board with very few components and a header for debugging. More complicated devices will have many different components, multiple processors, CLPDs and/or FPGAs, multiple flash memories for different firmware and settings, cryptography co-processors, and various debugging ports and interfaces. In this PCB board, there are 4 ICs that we highlighted in the red box and some pinouts(headers). we need to identify what the ICs are and what are the pinouts and why they are important,

1. WINBOND
2. BROADCOM
3. Fiti power
4. Macronix
5. Pinouts (Header)

Chip Analysis

Let's take a closer look at the ICs and see what we can unearth.

1. WINBOND:

- Here we can see clearly what is written on the IC.
- Winbond is the manufacturer and W9812G6KH-6 IS the Part number of the IC.



Fig 9. Winbond IC

- let's google the part number and download the datasheet. **Datasheet**



Fig 10. Datasheet

From the datasheet, we get to know that W9812G6KH is a high speed synchronous dynamic random access memory. We will get more information from the datasheet like memory size, clock frequency pin diagram power supply, packages.

2. BROADCOM:

- The part number of the IC is BCM5356 KFBG.



Fig 11. Broacom IC


- Let's google the part number **Datasheet**

BCM5356x Family

[CONTACT SALES](#) [REQUEST INFO](#)

802.11b/g and Single-Stream 802.11n 2.4-GHz Router

[OVERVIEW](#) [SPECIFICATIONS](#) [OPTIONAL PRODUCTS](#)



Incorporates IEEE 802.11b/g and single-stream IEEE 802.11n MAC and baseband and a 2.4GHz radio transceiver to achieve data rates of up to 150 Mb/s.

"The BCM5356 processor is Broadcom's lowest cost and most integrated entry level router. Also on chip is a powerful 333-MHz MIPS 74K CPU core with 32-KB instruction cache and a 32K data cache and an optimized memory subsystem architecture that delivers system performance of over 100Mb/s TCP throughput. In addition, the BCM5356 integrates a highly reliable 2.4 GHz power amplifier that delivers the equivalent performance as external power amplifiers. The BCM5356 includes a variety of components on chip, thereby reducing the Bill of Materials (BOM), and enabling smaller form factor and lower cost PCB solutions. The BCM5356 is implemented in 65nm CMOS technology that enables lower overall power consumption compared to previous generations. Further, it implements a Green Wi-Fi mode that dynamically switches off components of the chip thereby reducing active power consumption. This solution comes with two options which include:

BCM5356: Single-chip 2.4G single stream IEEE 802.11n retail router
BCM5356U: Single-chip 2.4G single stream IEEE 802.11n retail router with USB support"

Fig 12. Datasheet

- BCM5356 is a Baseband Micro-processor with 2.4 GHz radio transceiver. For more information about this chip check given link.

3. FR9886

- FR9886 is manufactured by fitipower integrated technology

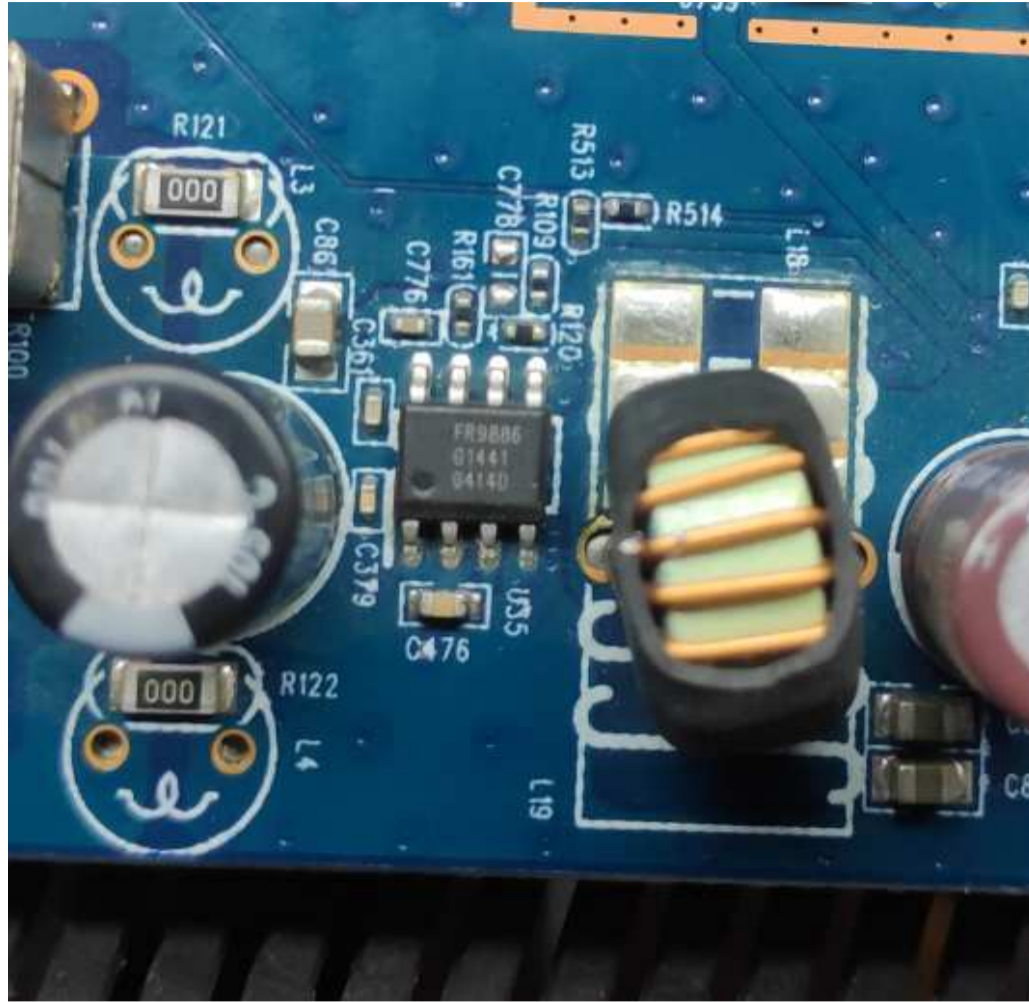


Fig 13. Power IC

- Let's google the part number **Datasheet**



FR9886

**23V, 2.5A, 340KHz Synchronous Step-Down
DC/DC Converter**

Fig 14. Datasheet

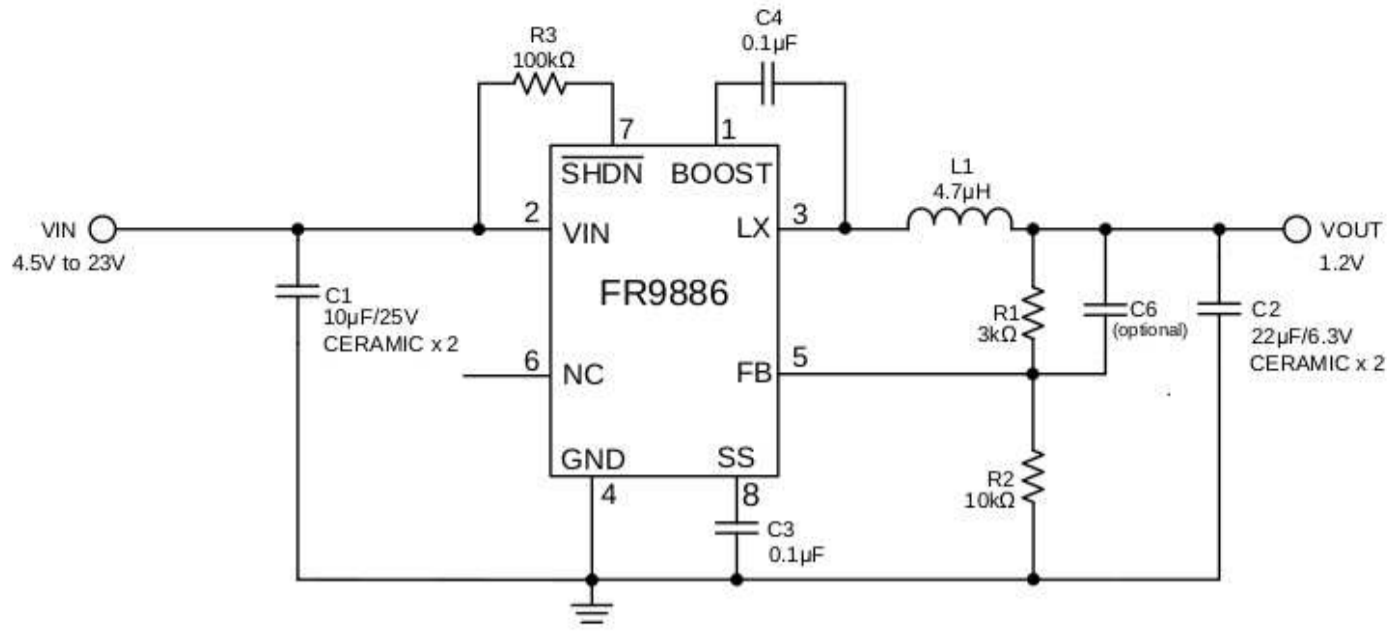


Fig 15. Circuit Diagram

- FR9886 is a synchronous step-down DC/DC convertor
- This is the typical schematic diagram of fr9886 step down dc-dc convertor
- The input range is in between 4.5V to 23v DC and we will get the fixed output that is 1.25V

4. MXIC

- The IC is manufactured by Macronix.
- The part number is 25l3206e.



Fig 16. Memory IC

- Let's download the datasheet and we know what this part is. **Datasheet**



Fig 17. Datasheet

- This IC is an 8-Mb serial flash.
- This chip may store Linux based firmware for the target device.
- Pin Identification: This IC comes in different packages as shown below. In our case, the ic package is 8-LAND WSON (6*5MM).

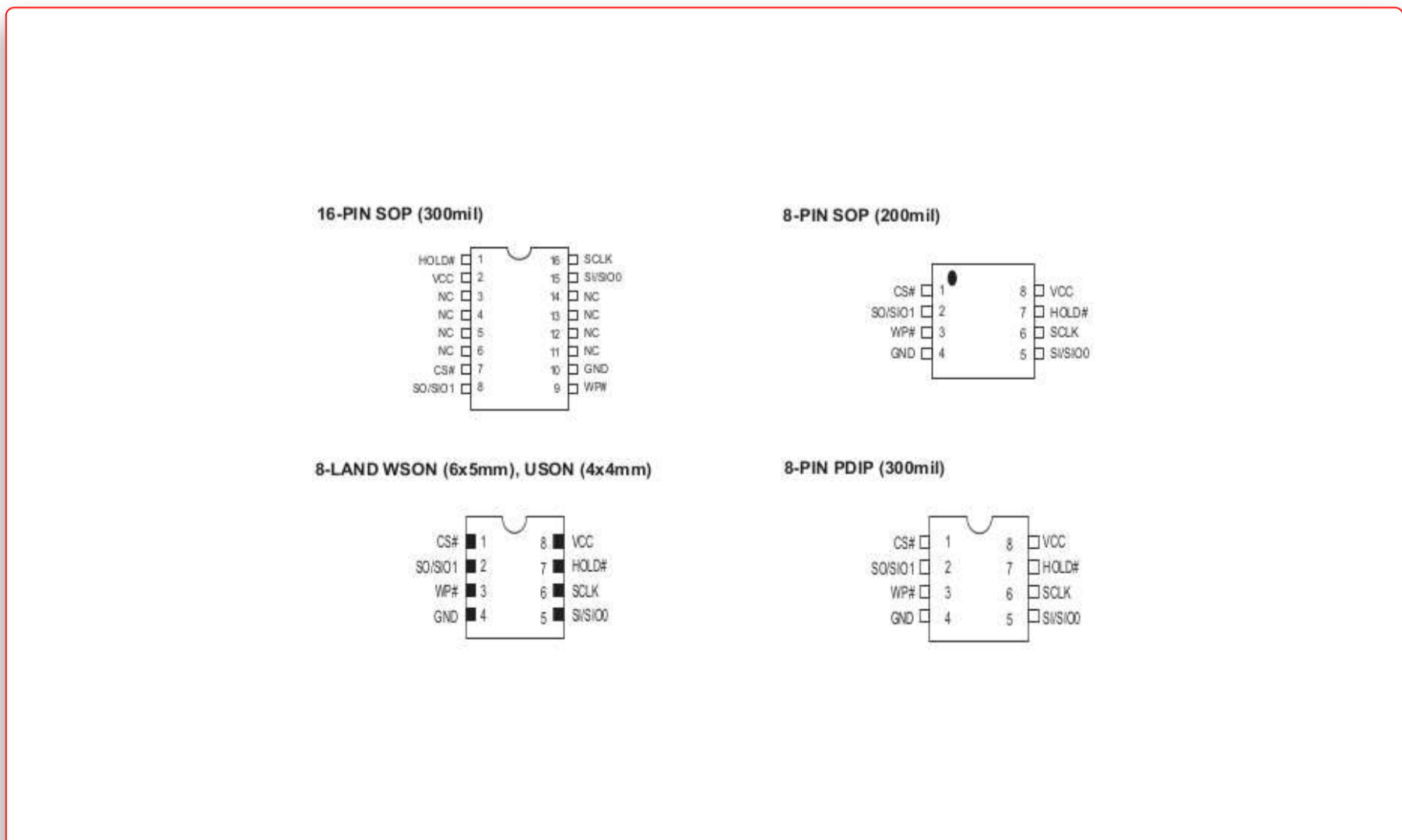


Fig 18. IC Package

- Pin description Here is the pin description taken from the datasheet. It is useful for making a connection with the hardware tool for reading and writing the firmware.

PIN DESCRIPTION

SYMBOL	DESCRIPTION
CS#	Chip Select
SI/SIO0	Serial Data Input (for 1 x I/O)/ Serial Data Input & Output (for Dual Output mode)
SO/SIO1	Serial Data Output (for 1 x I/O)/ Serial Data Output (for Dual Output mode)
SCLK	Clock Input
WP#	Write protection
HOLD#	Hold, to pause the device without deselecting the device
VCC	+ 3.3V Power Supply
GND	Ground

Fig 19. IC Pinout

Serial Flash Recon

Out of the four components identified, let's look at the serial flash and how to extract data from the chip. * Remove serial flash using soldering iron or hot air station from the router PCB. * While desoldering DO NOT heat it too much as it may damage the chip * We need a PCB adapter for soldering removed ICs as we can see in the image below. * Be careful when soldering the IC, check the round notch that is PIN 1.



Fig 20. IC desolder

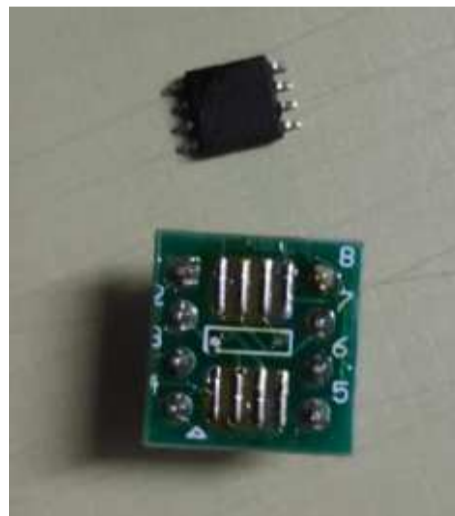


Fig 21. IC Adapter

Interfacing IC with our computer

To read or write the IC we need can use commercial or open source software. However, we need to interface the IC with our PC for the software to be able to communicate with the IC. We can use EXPLIoT-Nano (<https://explot.io/products/explot-nano>) or any other hardware connector that speaks SPI protocol for reading and writing firmware from Serial flash.

- Explot-Nano is a compact hacker-friendly multi-purpose, multi-protocol hardware tool mainly used to debug and program microcontrollers/processors and flash chips.
- Explot-Nano can be configured to support hardware protocols including, UART, I2C, SPI, ARM SWD, and JTAG. Even though it runs on 3.3V, all I/O pins are 5V tolerant.
- After soldering the IC on the PCB adapter make the connection properly as shown below.
- Now you can extract the data (firmware in our case) and further analyze the information in the firmware. we will see in details in upcoming SPI blog.

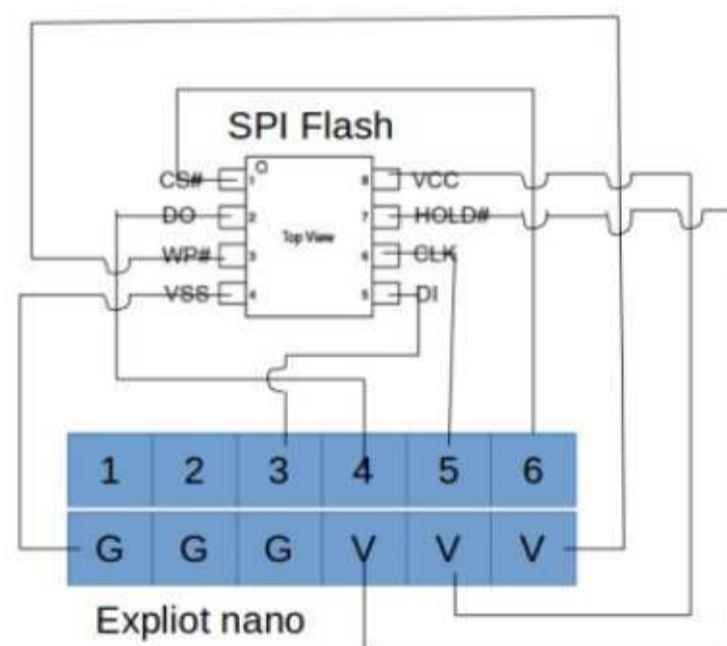


Fig 22. Connection Diagram



Fig 23. EXPLIoT Connection

5. Pinouts (headers)

Device manufacturers need a way to program the device with their firmware, so they generally use debug headers or test points to either debug or flashing firmware or recovering bricked devices.. As we have seen in this router, a PCB pin header has many pin headers, it's very important to know about what these headers contain. it may be a UART port, JTAG, SWD, anything who can directly talk with the main chip, rarely these pin headers are labelled. In the next blog series we will see what are the different debug ports , how to identify debug ports, different methods of identifying debug ports and its use cases.

Conclusion:

We hope this blog post gives you an overview of the basics of hardware recon, how PCB analysis, component identification, its datasheets give you useful information to perform hardware assessment. This is a very basic overview of what you can and should do. In later blog posts, we will cover more details of analysing the different microcontrollers, memory chips, and hardware protocols commonly used in devices.

Continue to the next part - [IoT Security-Part 14 \(Introduction To And Identification Of Hardware Debug Ports\)](#)