# Recuperação de HGU Travado

GPT2742GX4X5v6

# Resumo

Entende-se por HGU travado aquele cujo sistema é incapaz de realizar o processo de *boot* de seu *software* de forma integral, levando a um equipamento com presença parcial, ora nula, de suas funcionalidades. Para analisar o funcionamento do equipamento em tempo real, faz-se uso do seu canal pré-estabelecido (*built-in*) de comunicação serial, o que nos permite identificar as causas do travamento e traçar linhas de solução (*troubleshooting*). As informações demonstradas neste documento referem-se a um equipamento MitraStar plataforma Econet / Zyxel EN7523/EN7529, modelo GPT2742GX4X5v6.

## Acesso ao *Console*

Para o acesso ao *console* do equipamento, utiliza-se uma placa JTAG com chip MAX3232, vide Figura 1:

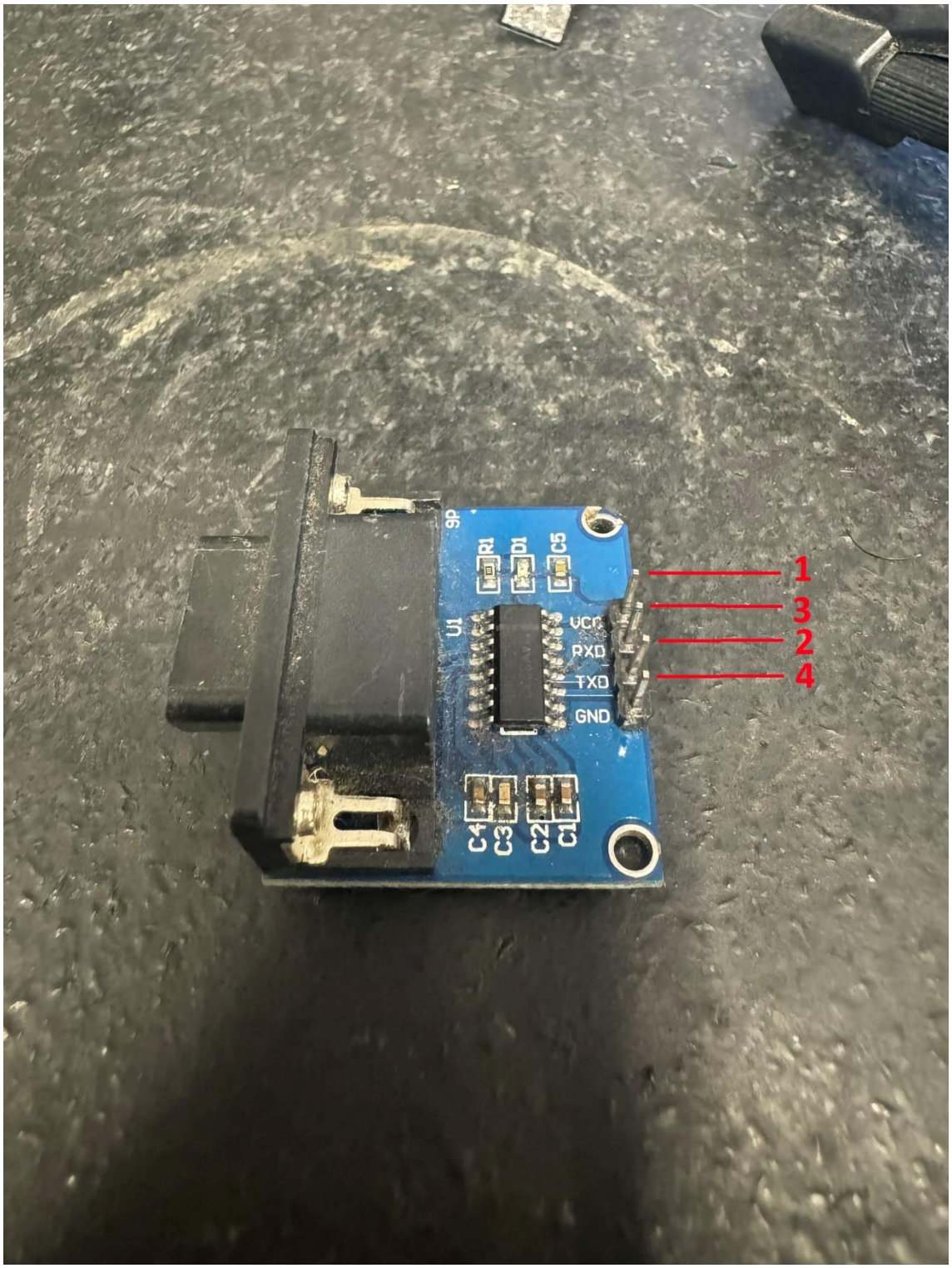


Figura 1: Placa JTAG

A placa possui quatro terminais, VCC (1), TX (2), RX (3) e GND (4), que devem ser conectados à placa do equipamento, preferencialmente soldados, vide Figuras 2-4:

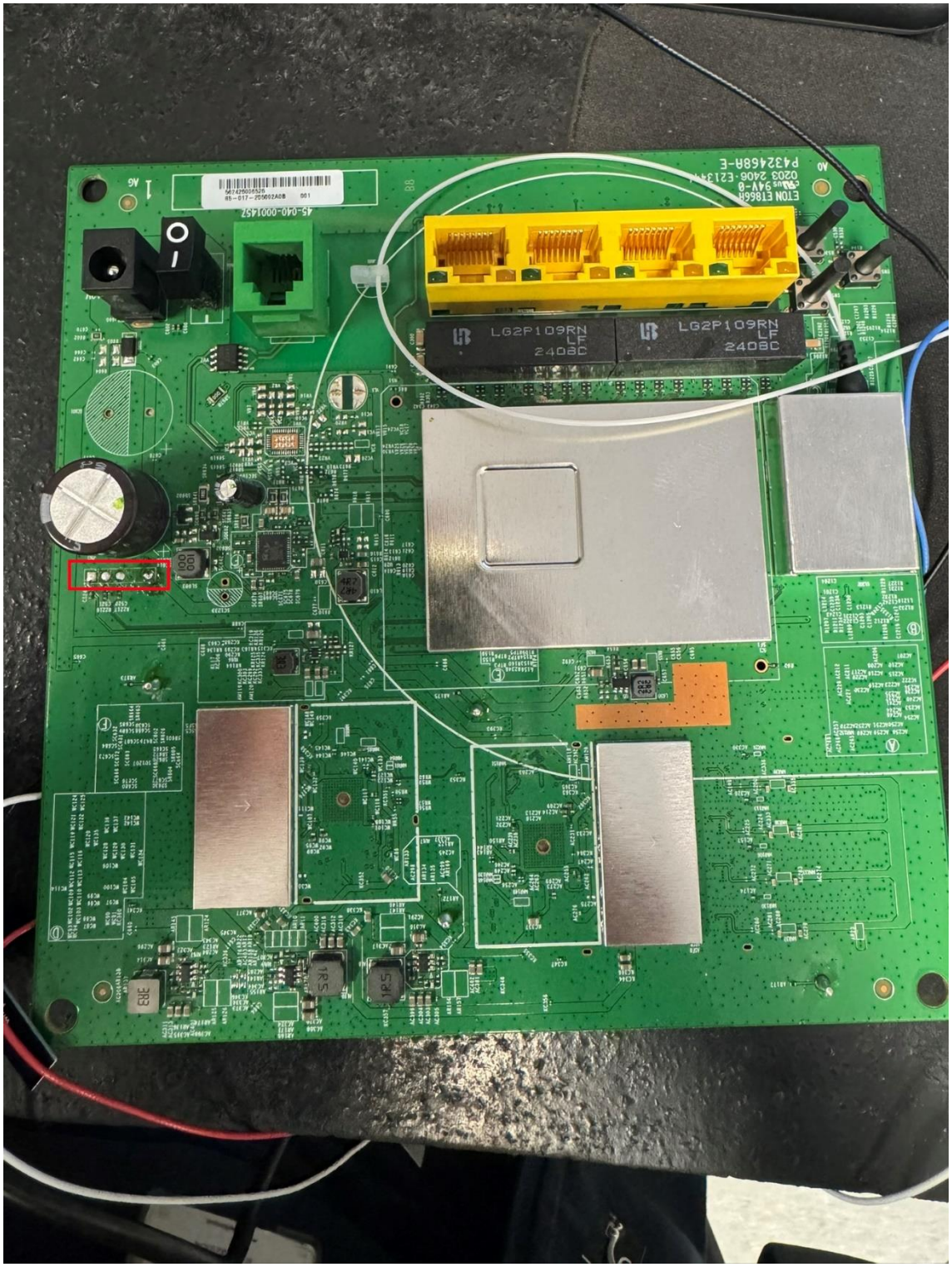


Figura 2: Placa do HGU

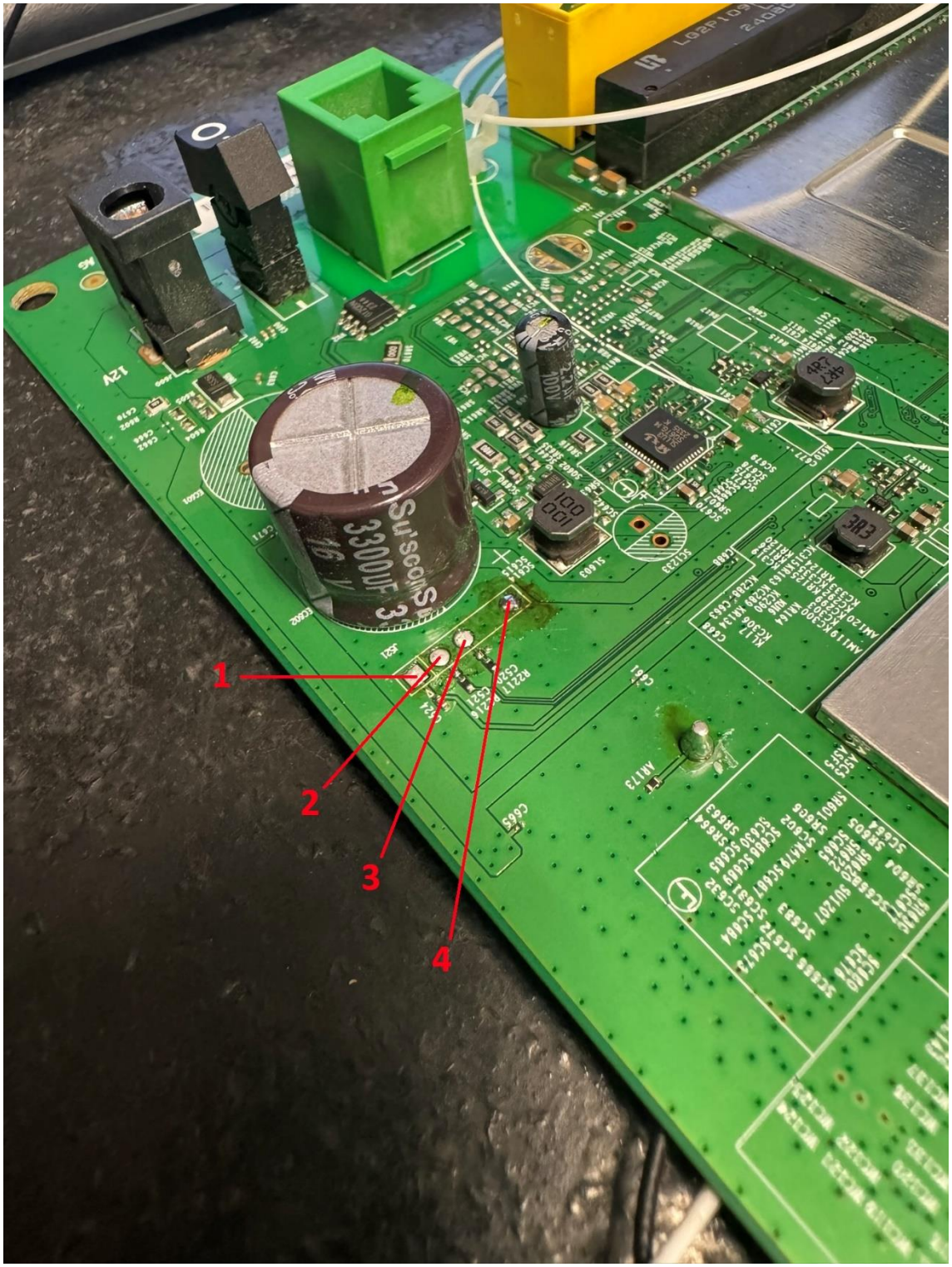


Figura 3: Terminais do *Console*

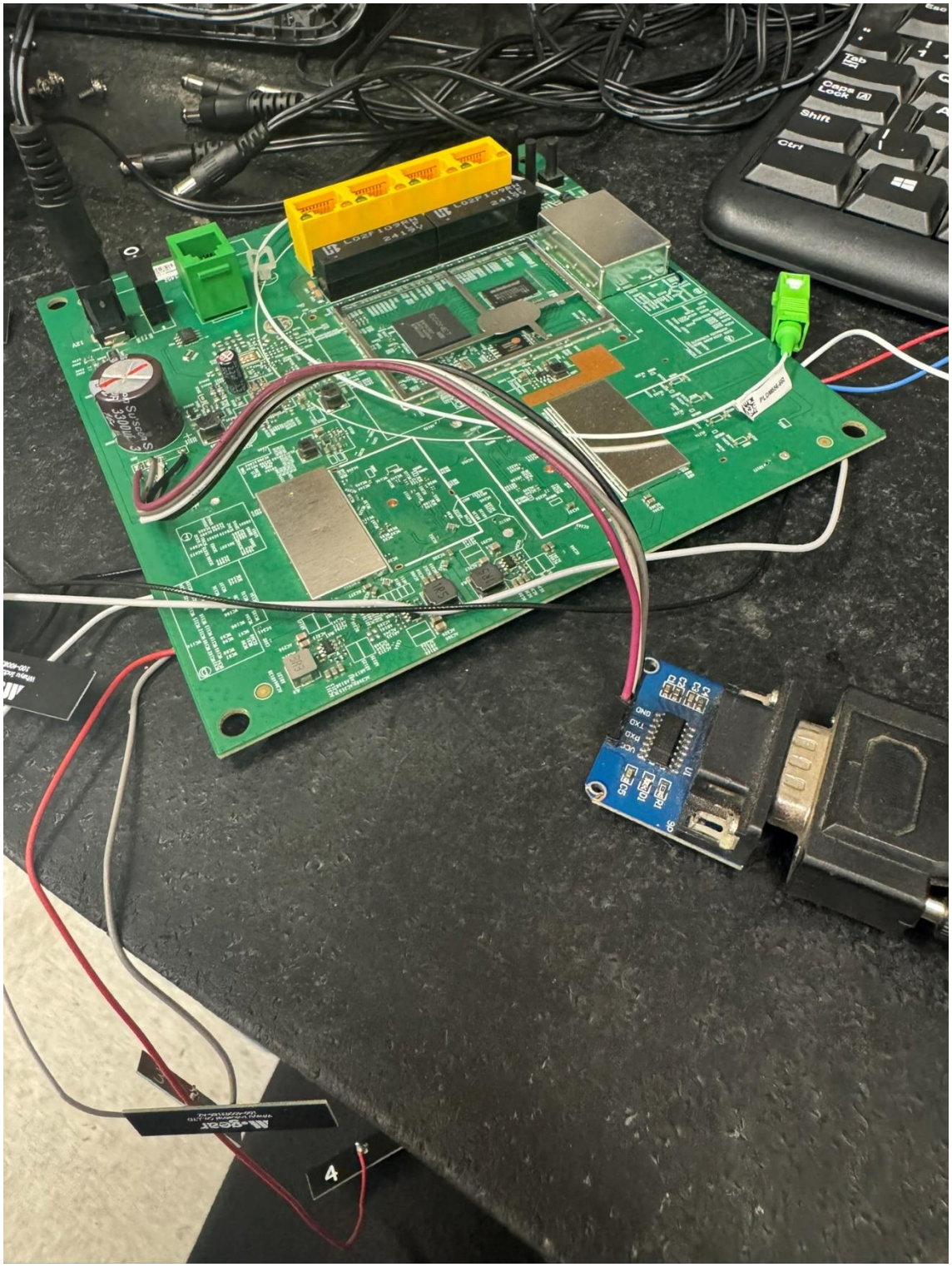


Figura 4: Conexão serial completa

## Configuração da Comunicação

Com a conexão física devidamente realizada, a comunicação entre o dispositivo e a porta serial do computador pode ser feita de forma simples por meio de um *hyperterminal*. PuTTY e Teraterm são opções comuns, sendo o PuTTY a escolha para o prosseguimento neste documento. Acessando, com Win + x (Figura 5), o menu de opções de gerenciamento do sistema do Windows, vide abaixo como identificar a porta que deve ser utilizada para o acesso (aquela que apresentar algo similar a “USB para Serial” em seu nome no sistema, vide Figura 6), após conectar o cabo serial em uma das portas USB da máquina utilizada:


Figura 5: Menu de gerenciamento

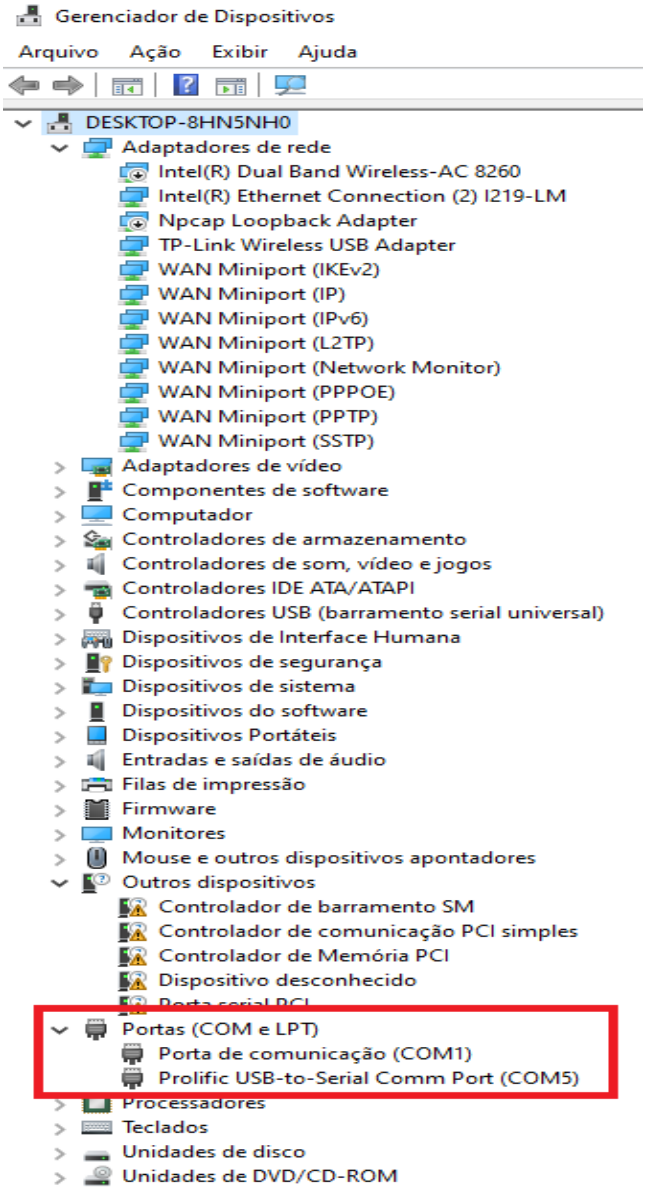


Figura 6: Portas COM

Após identificar a porta COM a ser utilizada, deve-se lembrar sempre de atribuir à conexão configurada no *hyperterminal* um *baud rate* (taxa de transmissão serial assíncrona) de 115200 para que os dados da comunicação com o HGU sejam devidamente interpretados pelo mesmo e pela máquina, vide Figura 7:

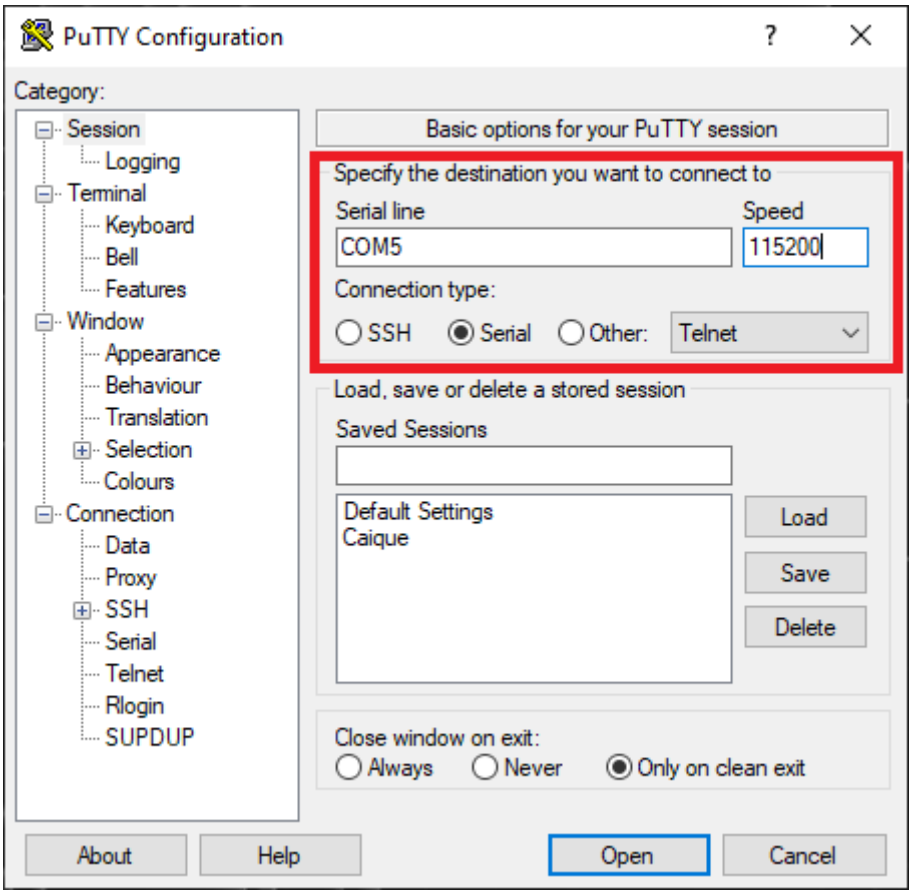


Figura 7: Configuração do PuTTY
A janela de *console* é aberta ao clicar no botão *Open*

# Utilização do *Console*

Uma vez iniciada, a janela do *console* estará atrelada à porta serial (COM5 no exemplo) e será responsável por exibir o *log* do dispositivo, isto é, um “depósito” em tempo real de todas as informações e quaisquer erros referentes ao seu funcionamento. Da mesma forma, o usuário do *hyperterminal* pode inserir informações manualmente utilizando o teclado e enviá-las ao equipamento, que fará o processamento destes dados conforme lógicas internas. Vide abaixo as primeiras informações enviadas pelo HGU para *log* (Figura 8):

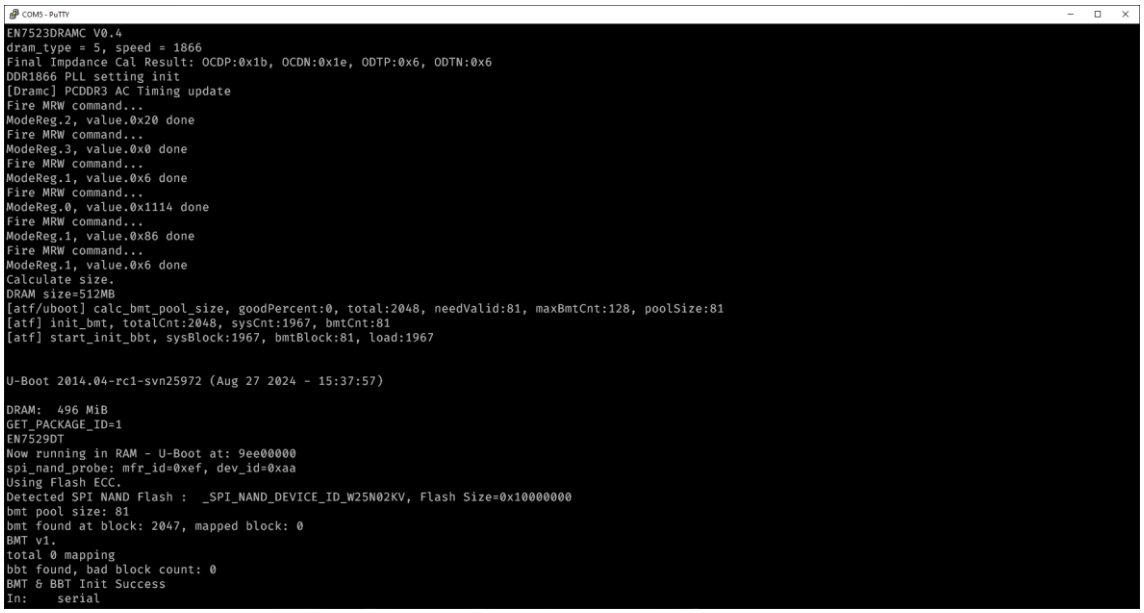


Figura 8: Janela do *console* com *logs* iniciais do HGU

# Identificando Erros

Defeitos típicos de um equipamento travado podem ser identificados ainda nos estágios iniciais do processo de *boot*. Vide abaixo exemplos de linhas comuns ao *log* de um HGU apresentando LED rosa que merecem atenção em casos de equipamento travado em geral:

## *imageSequence*

---

*tclinux_main->imageSequence= 1000001*

*tclinux_slave->imageSequence= 1000001*

---

Estes valores representam uma sequência serial de atualização de firmware, aparecem sempre nesta sequência e são uma **indicação direta de defeito relacionado à corrupção de memória quando ambos os valores são 1000001.**

## Erros do bootloader

Os conjuntos de linhas a seguir indicam erros expostos pelo *bootloader*, o software cuja função é inicializar o núcleo do sistema Linux sobre o qual o HGU opera.

• *Hash check fail*

---

*Can't get image data/size for '' hash node in 'fdt@1' image node*

*ERROR: tclinux hash check fail!*

*update 0x5ac0000 imageSequence= 1000001*

*...verify kernel:0x5ac0000 error*

*Verify image fail*

---

• *Flash command fail*

---

flash - flash - flash command

Usage:

flash flash usage:

flash init

flash erase [addr] [len]

flash read [src] [len] *[dst]

flash write [dst] [len] *[src]

---

• *bootm command fail*

---

Wrong Image Format for bootm command

ERROR: can't get kernel image!

bootm - boot application image from memory

---

Quando um equipamento apresenta um ou todos os conjuntos de linhas acima durante o processo inicial de boot, normalmente o faz repetidamente (em *loop*), até atingir um número máximo de tentativas, fatalmente chegando ao *log* abaixo

---

!!! Fail to booting kernel !!!

Not support LED number 0 on this board!

Reset your board! system halt...

---

que indica que o bootloader não fará mais nenhuma tentativa e corresponde ao equipamento visivelmente travado.

## Realizando o Reparo

O reparo adequado neste caso é a reinstalação do firmware do equipamento, possível através do *prompt* intermediário do processo de *boot*. Para acessar este *prompt*, pressione qualquer tecla repetidamente na janela do *console* após ligar o equipamento até ver o *prompt* ZHAL>. Em seguida, envie o comando ATHE para ver a lista de comandos disponíveis, que deverá ser como na Figura 9. Os comandos ATUR, ATSH e ATSP são os destaques deste *prompt*.

```
ZHAL> ATHE
ATUR    [y:]x       upgrade RAS image (x=file name, y=host ip)
ATSH                dump manufacturer related data in ROM
ATEN    x[,y]       set BootExtension Debug Flag (y=password)
ATSE    x           show the seed of password generator
ATSP    x           show user password
ATSR    [x]         system reboot
ATGO                boot up whole system
ATMB    [x,y]       upgrade firmware image by multiboot
ATHE                show command list
ZHAL>
```

Figura 9: Resposta a ATHE; Comandos notáveis destacados

- ATUR: Instalação de firmware
- ATSH: Exibir dados de manufatura do equipamento
- ATSP: Exibir senha de acesso (senha admin/support)

Vide abaixo as respostas a estes comandos (Figuras 10-12):

```
ZHAL> ATSH
Firmware Version        : 100XNT0b1
External Version        : GL_g1.13_100XNT0b17_2
Bootbase Version        : V1.6 | 08/27/2024 15:35:00
Vendor Name             : MitraStar Technology Corp.
Product Model           : GPT-2742GX4X5v6
Serial Number           : E8458B2D1C51
Gpon Serial Number      : 4D535443FFFDBCC8
First MAC Address       : E8458B2D1C50
Last MAC Address        : E8458B2D1C57
MAC Address Quantity    : 08
Default Country Code    : D0
Boot Module Debug Flag  : 00
RootFS      Checksum    : 8B0AC247
Kernel      Checksum    : C402FD8E
Main Feature Bits       : 00
Other Feature Bits      :
                5a 59 a0 0f 00 00 20 37-35 32 39 00 00 00 00 01
                02 00 00 00  0 00 00 00-00 00 00 00 00 00
```

Figura 10: Resposta a ATSH

```
ZHAL> ATSP
User Password: pVkV7Via
ZHAL>
```

Figura 11: Resposta a ATSP

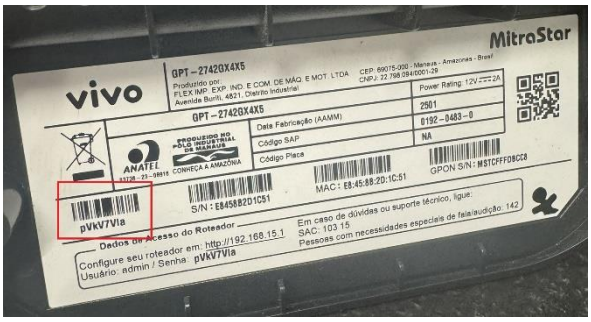


Figura 12: Etiqueta do equipamento de exemplo

Como descrito na resposta a ATHE, o comando ATUR obedece à seguinte estrutura:

---

ATUR [**IP_DO_SERVIDOR**]:**NOME_DO_ARQUIVO_DO_FIRMWARE**

---

Isto é, consiste em digitar ATUR, um espaço, o IP do servidor de protocolo TFTP, dois pontos e o nome do arquivo do firmware a ser instalado, que será servido pelo servidor no IP designado, que deve estar configurado para ouvir e servir na porta 69 (padrão do protocolo TFTP).

Após o envio do comando na devida estrutura, o arquivo será servido pelo servidor para o equipamento, que em seguida dará prosseguimento à instalação.

Vale informar que o servidor deve ter acesso à rede do HGU, que, nesta etapa de seu funcionamento, tem IP 192.168.1.1/24 e que, caso IP_DO_SERVIDOR não seja especificado, será considerado o valor padrão de 192.168.1.100.

Finalizada a instalação do firmware, deve-se observar novamente o processo de *boot* pelo *console* em busca de erros e, em particular, verificar se houve incremento em um dos valores de *imageSequence*.

## Modelo Askey RTF8225VW

Em seguida utilizaremos a base adquirida no estudo do GPT2742GX4X5v6, que habilita o estudo pontual de qualquer equipamento da linha HGU, para brevemente discutir o mesmo processo de recuperação de firmware no caso do modelo Askey RTF8225VW, também da série Wi-Fi 6. As principais diferenças em relação ao modelo MitraStar estão na configuração dos terminais de comunicação serial assíncrona, vide Figuras 1;13-14, e na implementação prática de sua interface de interação, isto é, os comandos que o equipamento expõe ao técnico.

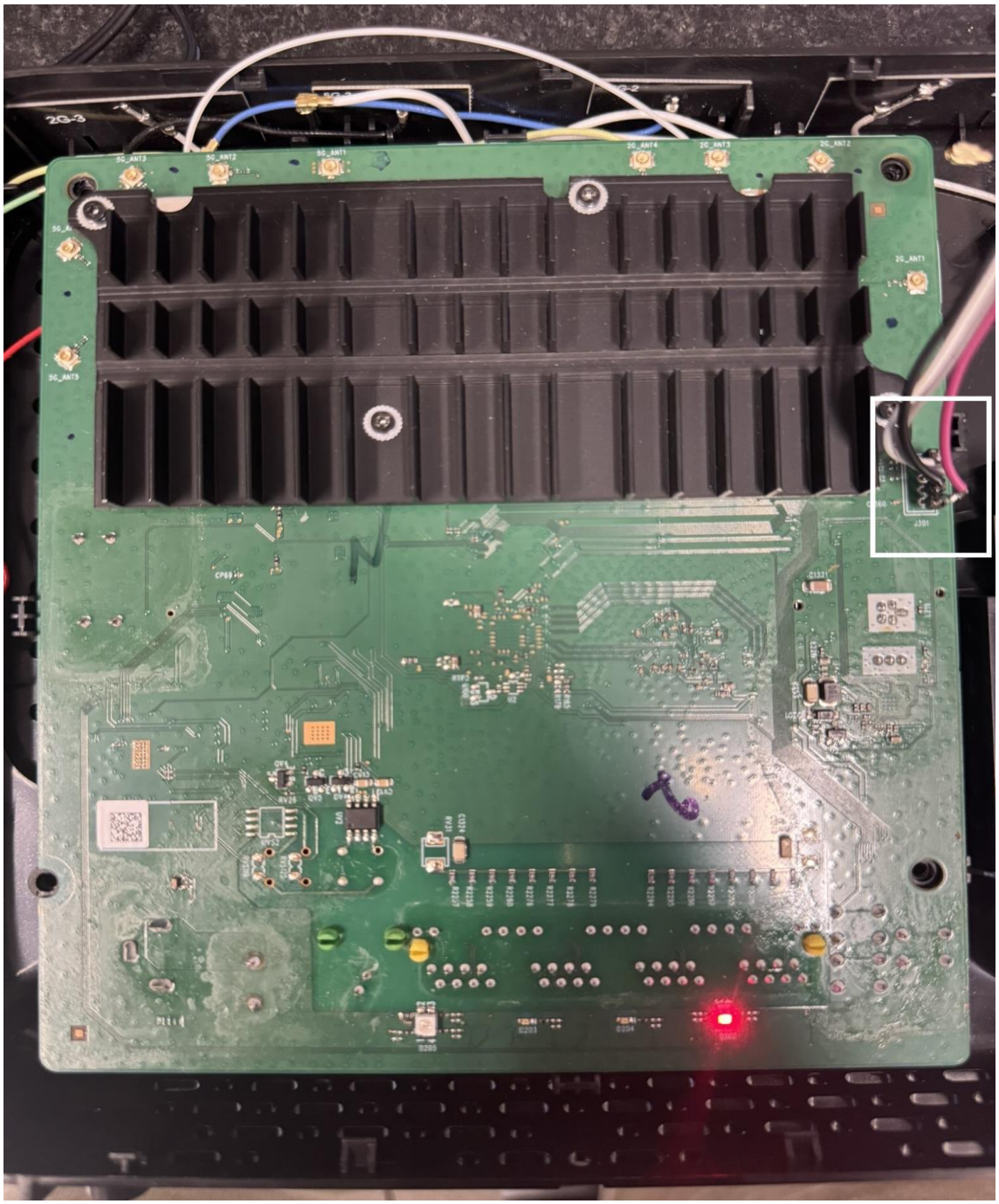

Figura 13: Placa do HGU – Askey RTF8225VW

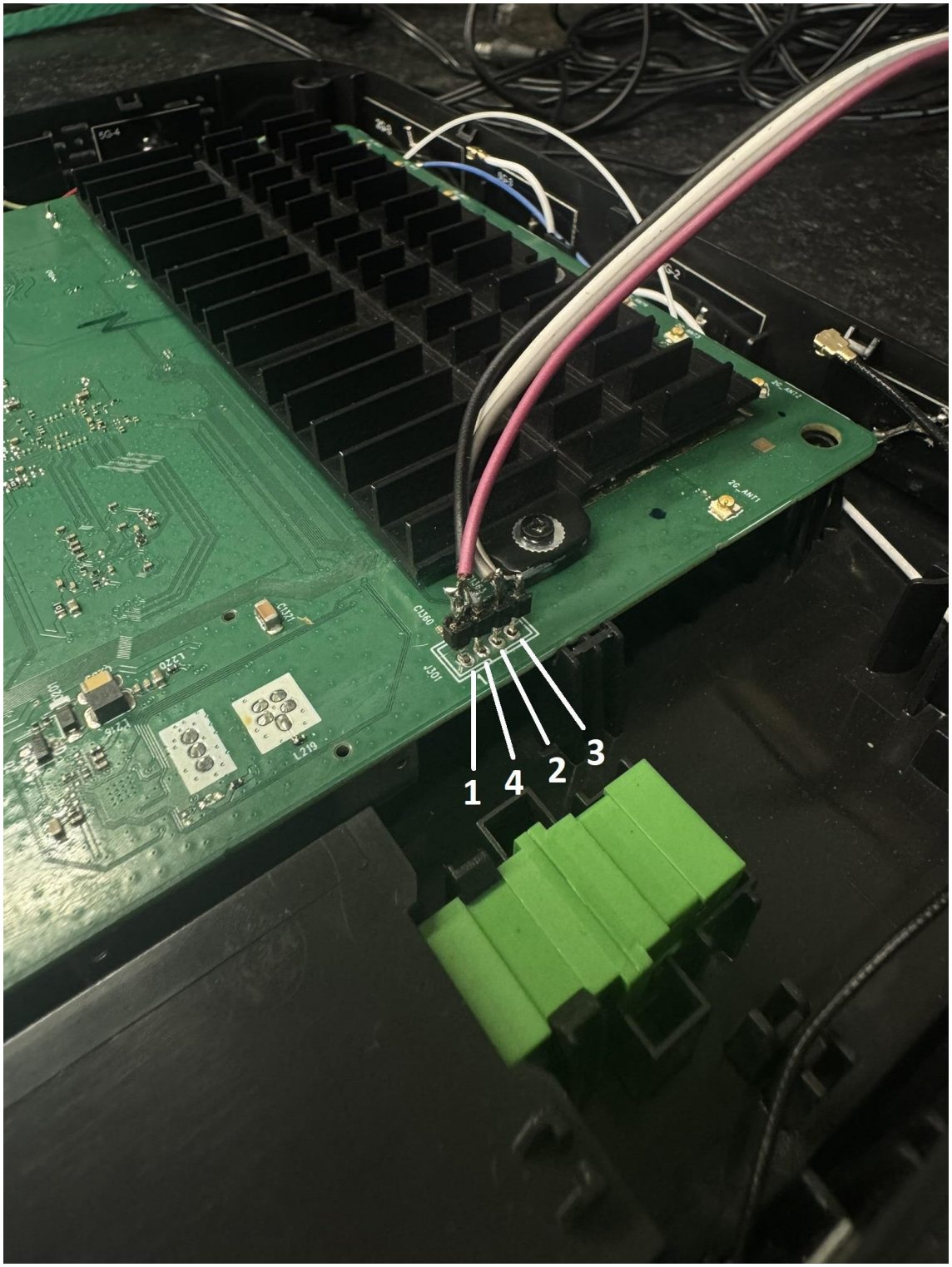


Figura 14: Terminais do *Console* – Askey RTF8225VW

Diferentemente do modelo MitraStar, o equipamento é identificado como travado via console dado que seu console interativo U-Boot, de *prompt* “ECNT>”, é acionado automaticamente após falhas tentativas de inicialização, deixando claro que não há uma imagem de sistema operacional válida em sua memória.

Uma questão importante no tratamento deste caso é que, quando o equipamento realiza tentativas de inicialização e não obtém sucesso, levando ao console U-Boot automaticamente, sua interface LAN é **desativada**, impossibilitando a comunicação com o computador e, consequentemente, com o servidor TFTP, sendo **obrigatório** acessar o console antes da primeira tentativa de inicialização, **pressionando repetidamente a tecla ENTER após a energização do dispositivo**.

Da mesma forma, no entanto, é também possível extrair dados úteis do sistema neste *console*, bem como realizar diversas ações sobre o sistema por meio de seus comandos.

A lista de comandos disponíveis no console U-Boot deste modelo é extensa, e pode ser visualizada em https://github.com/istkai/docHGU/blob/main/RTF8225VW/Console%20U-Boot%20RTF8225VW.pdf, juntamente com a lista de variáveis de ambiente disponíveis para consulta, como, por exemplo, o serial e a senha de acesso do equipamento. Estas variáveis podem ser visualizadas por meio do comando *printenv*, vide Figura 18.

Utiliza-se então a mesma abordagem de reinstalação da imagem de sistema do equipamento via servidor TFTP que no caso do dispositivo MitraStar. Para isso, basta saber o comando a se utilizar, asp_update, sua estrutura, e os IPs padrão do equipamento e do servidor, que são diferentes do outro modelo, vide Figuras 16-17.

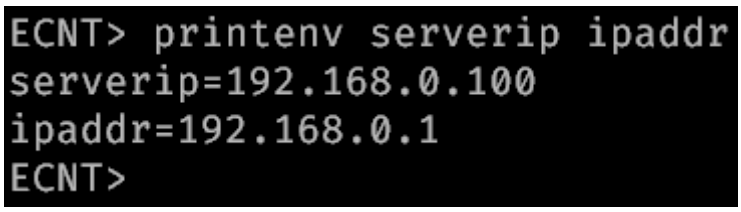


Figura 16: IPs padrão – Askey RTF8225VW

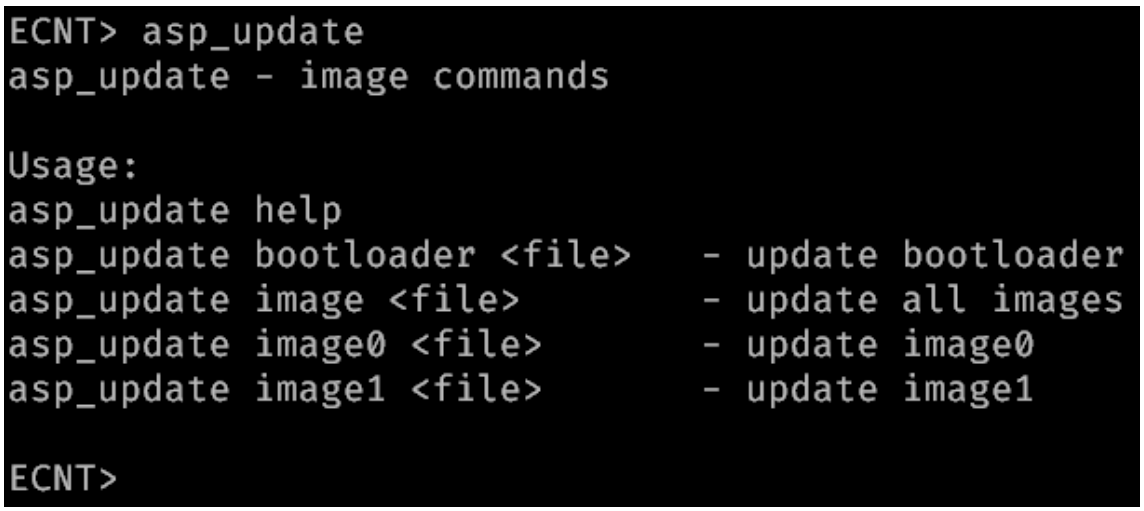


Figura 17: Estrutura do comando asp_update

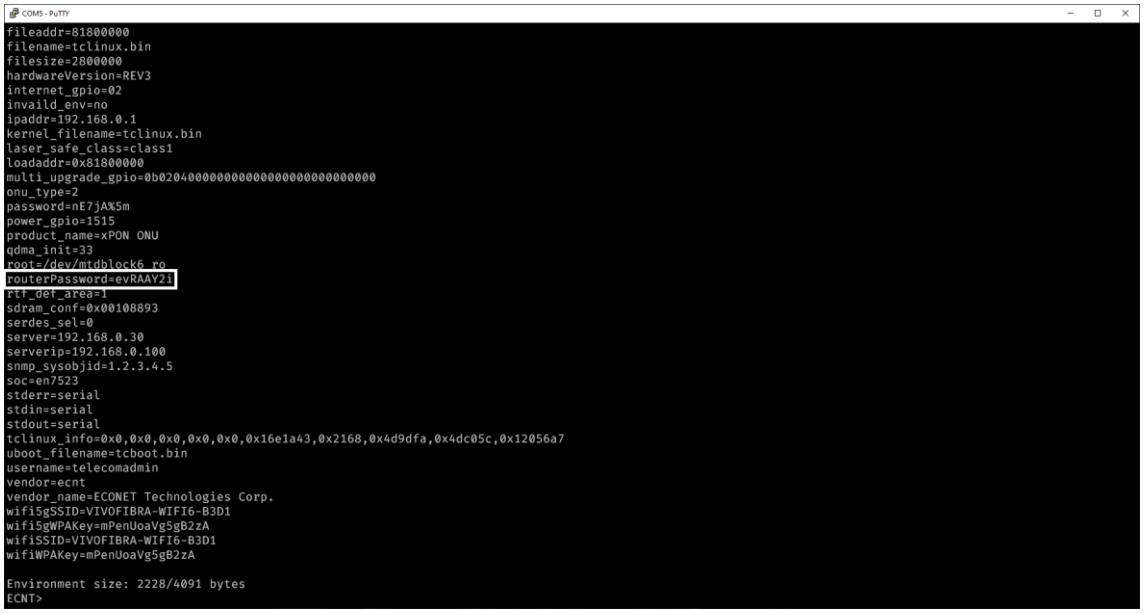


Figura 18: Exemplo de resposta a printenv. Destaque para *routerPassword*

Da Figura 17, pode-se visualizar que é possível, utilizando o comando asp_update, instalar ou atualizar o *bootloader*, a imagem de sistema principal(*image0*), a imagem de sistema reserva(*image1*), ou ambas imagens de sistema(image).

Por exemplo, para atualizar ambas imagens de sistema, seria utilizada a seguinte estrutura:

---

asp_update image <file>

---

Onde <file>, o nome do arquivo, é um argumento opcional e, caso não informado, utiliza o valor padrão de “RTF8225VW_TEF.tclinux.bin”.

Finalmente, é importante saber que esta imagem de sistema NÃO é a mesma utilizada para atualização via interface web(página /padrao). Trata-se da imagem do próprio sistema Linux utilizado pelo dispositivo, que pode ser extraída, também via TFTP, de um outro equipamento em bom funcionamento, dado acesso à sua própria interface de comunicação serial assíncrona.