공유기 커스텀 펌웨어 개발의 이해

김승주

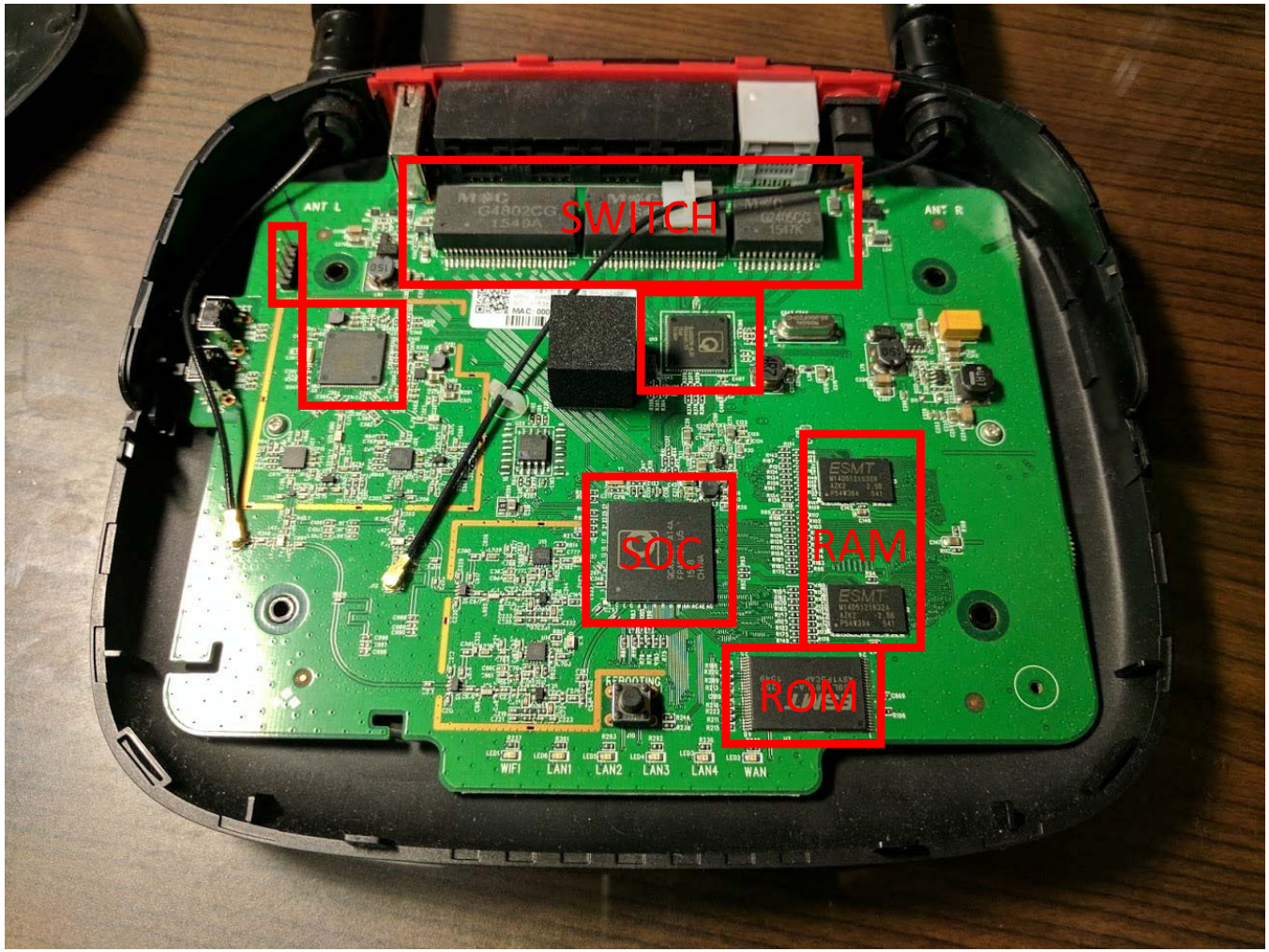
manatails@mananet.net

OpenWRT

- WRT54G에서 시작된 임베디드용 리눅스 배포판
- 최근 LEDE로 분리되었다가 병합
- 관련 문서의 부재로 진입장벽이 높은 편

OpenWrt
Wireless Freedom

기판 부품 확인



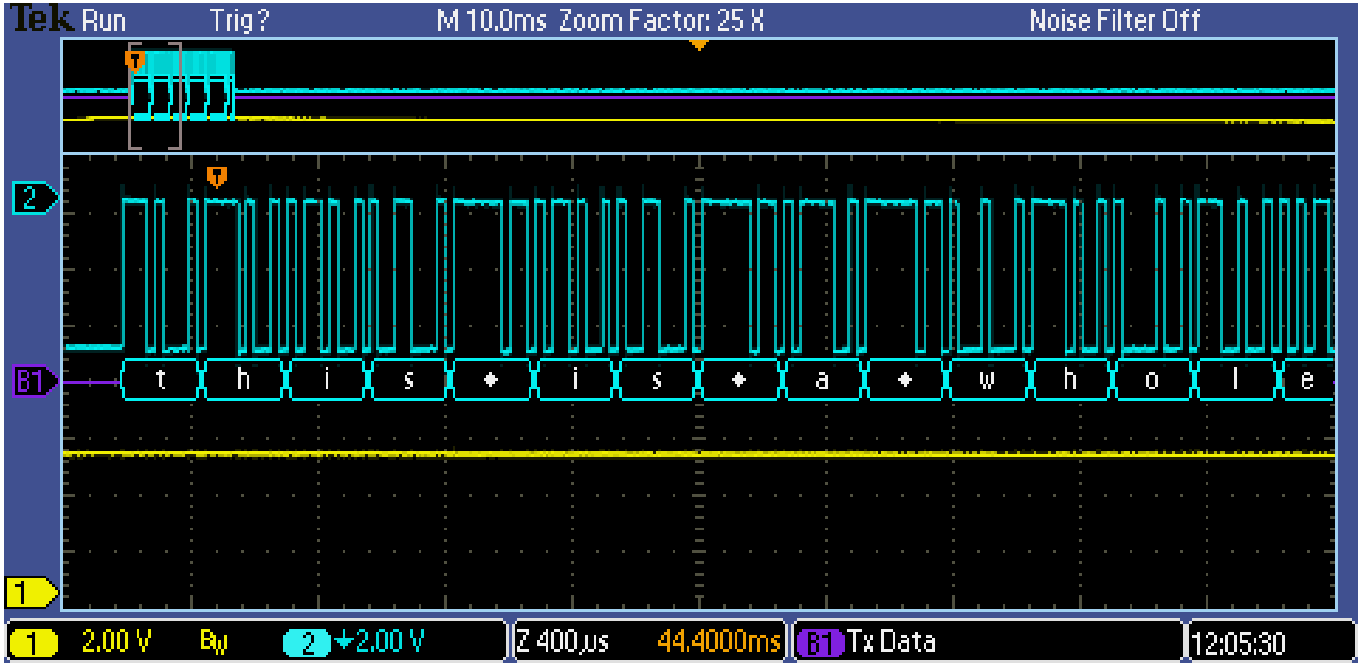
시리얼 접근

- TX : 출력시 변화
- RX : 다양
- GND : 프레임과 비교
- VCC : 일정

- 일반적인 가정용 기기의 경우 서비스용 포트가 대부분 존재

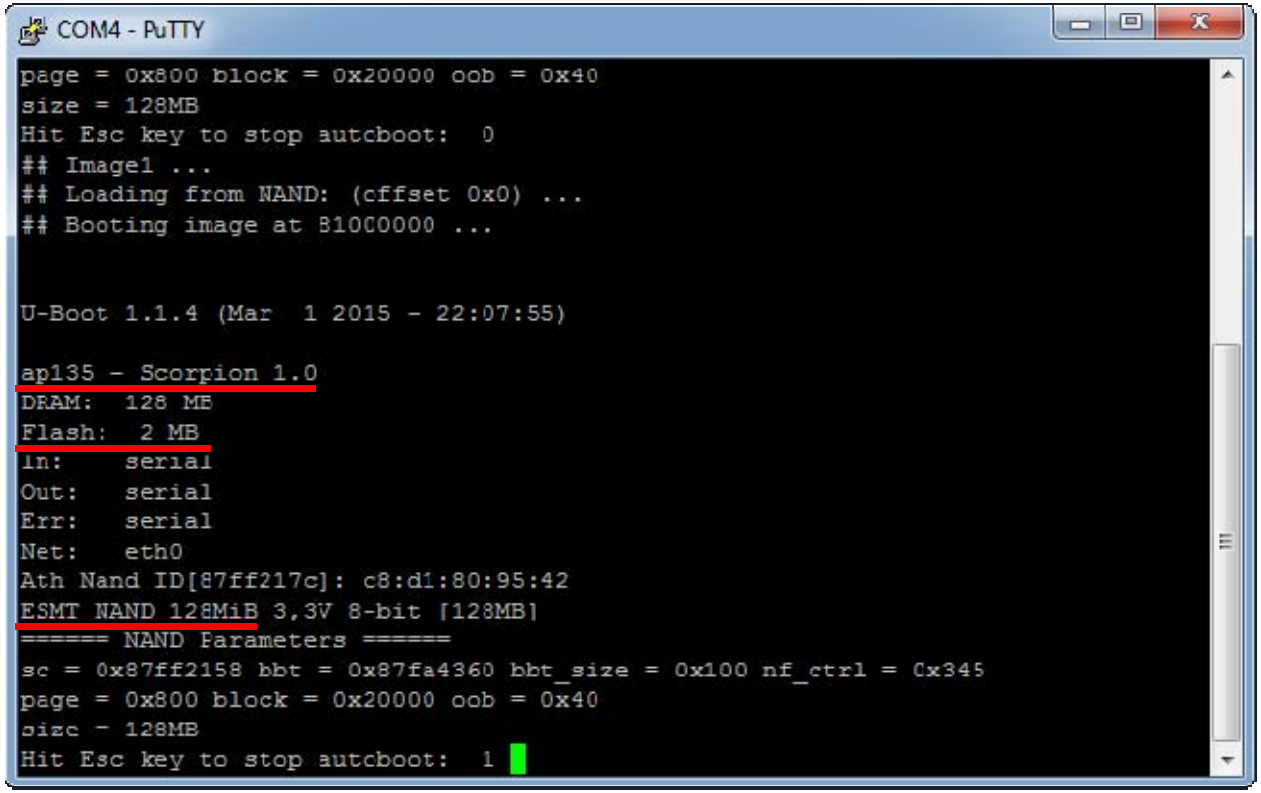
시리얼 접근

- 포트가 숨겨진 경우 오실로스코프 이용



부팅 로그 확인

- 플랫폼 종류
- NAND
- RAM
- NOR



U-boot

- GPL 라이센스 오픈소스 부트로더
- 부팅 이미지 정보 표시
  - bootinfo
- TFTP를 통해 부팅 혹은 다운로드
  - tftpboot
- NAND, 메모리 작업
  - nand, md
- 커널 파라미터 수정
  - setenv, printenv

커널 로그 확인

- MTD 구성
- 랜카드 정보
- 주변기기 장치명
- 로그 파일은 항상 백업

```
wmi_unified_vdev_stop_send for vap 0 (87150000)
OL vap_stop -
STOPPED EVENT for vap 0 (87150000)
wmi_unified_scan_start_send for vap 0 (87150000)
OL vap_start +
wmi_unified_vdev_start_send for vap 0 (87150000)
OL vap_start -
ol_vdev_start_resp_ev for vap 0 (87150000)
ol_ath_vap_join: join operation is only for STA/IBSS mode
wmi_unified_vdev_up_send for vap 0 (87150000)
Notification to UMAC VAP layer
Init in progress. Delay vap_stop
wmi_unified_vdev_stop_send for vap 0 (87150000)
STOPPED EVENT for vap 0 (87150000)
device ath0 entered promiscuous mode
 DEVICE IS DOWN ifname=ath0
 DEVICE IS DOWN ifname=ath0
OL vap_stop +
wmi_unified_vdev_stop_send for vap 0 (87150000)
OL vap_stop -
STOPPED EVENT for vap 0 (87150000)
OL vap_start +
wmi_unified_vdev_start_send for vap 0 (87150000)
OL vap_start -
ol_vdev_start_resp_ev for vap 0 (87150000)
ol_ath_vap_join: join operation is only for STA/IBSS mode
wmi_unified_vdev_up_send for vap 0 (87150000)
Notification to UMAC VAP layer
br0: port 3(ath0) entering forwarding state
setup wanif dev(eth0.2)
setup wan2if dev(eth0.3)
<cwmp_utility.c>Set No Debug Message[1]
<main.c>Set No Debug Message!
<cwmp_utility.c>Set using certificate auth[1]
<main.c>Set using certificate auth.

DW02-412H login: root
```

펌웨어 덤프

- U-boot: Flash -> RAM -> TFTP이용
  - nand read 0x81000000 0x1000000 0x617dc5
  - tftp 0x81000000 nand.backup 0x370000

- OS: mtd 이용
  - dd if=/dev/mtd0 of=/tmp/part.backup

펌웨어 덤프

- 콘솔 로그 저장후 스크립트로 변환

```
manatails@W230SS: ~
File  Edit  View  Search  Terminal  Help
boot> md.b 0x1000000 0x160
01000000: 04 a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
01000010: ab a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
01000020: 05 05 02 03 49 53 51 2d 34 30 30 30 00 00 00 00    ....ISQ-4000....
01000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
01000040: ab a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
01000050: ab a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
01000060: c0 22 9b 58 96 55 67 6f 74 14 e4 c2 81 b5 38 ce    .".X.Ugot.....8.
01000070: 8f b7 87 be c2 c8 be e9 47 c4 44 73 9e f5 0d 9e    ........G.Ds....
01000080: ab a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
01000090: ab a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
010000a0: ef 99 1a ad dc e6 03 f0 79 df 41 e0 46 db 26 79    ........y.A.F.&y
010000b0: 58 58 e2 0f c8 21 8d 6b 81 bc 75 28 38 d7 99 59    XX...!.k..u(8..Y
010000c0: ab a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
010000d0: ab a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
010000e0: 5a 4a 3e 91 a4 de f7 bb e0 e0 d4 10 e1 4d 7b 03    ZJ>..........M{.
010000f0: a9 3c 35 2e 33 87 d2 a6 94 7b 2b 7c 7f aa d6 38    .<5.3....{+|...8
01000100: ab a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
01000110: ab a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
01000120: 0b 68 1f 6a dd 3a d6 80 ef f9 2a 7c 1c b3 9b 48    .h.j.:....*|...H
01000130: 8d 2f 78 92 0b 5b d4 c4 58 e6 e2 67 7b 83 7d 85    ./x..[..X..g{.}.
01000140: ab a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
01000150: ab a0 3c cd 54 5f c3 32 ab a0 3c cd 54 5f c3 32    ..<.T_.2..<.T_.2
boot>
```

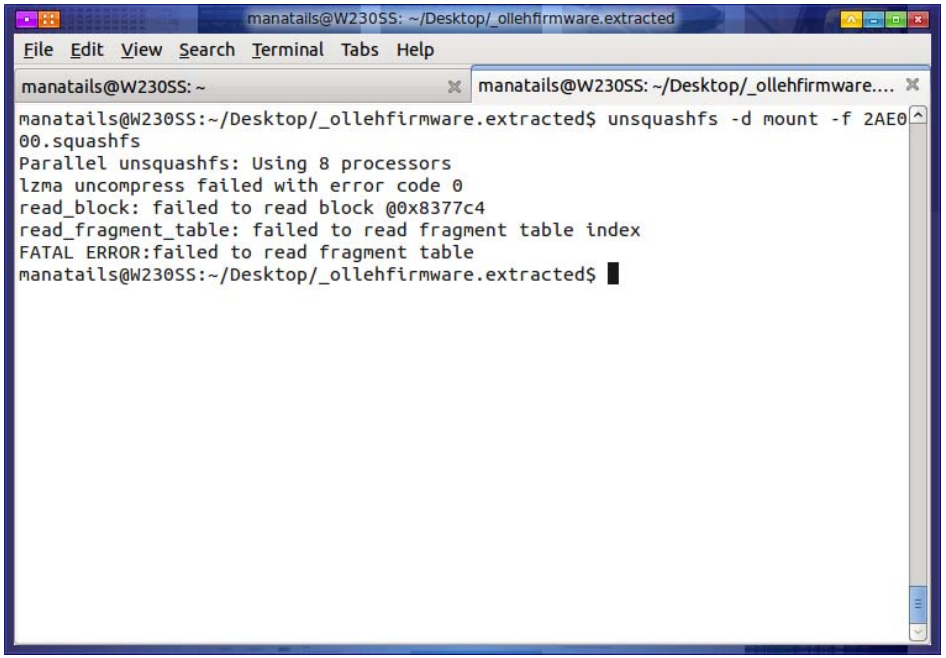
덤프파일 분석

- file
- binwalk
  - 펌웨어 분석에 특화
  - 시그니쳐 검색

```
manatails@W230SS:~/Desktop$ binwalk ollehfirmware

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
2125856       0x207020        Linux kernel version "2.6.31-svn2007 (gcc version
4.3.3 (GCC) ) #5 Tue Nov 17 19:25:5.3 (GCC) ) #5 Tue Nov 17 19:25:56 KST 2015"
2753031       0x2A0207        LZMA compressed data, properties: 0x66, dictionary
 size: 16777216 bytes, uncompressed size: -1 bytes
2753059       0x2A0223        LZMA compressed data, properties: 0x66, dictionary
 size: 33554432 bytes, uncompressed size: -1 bytes
2809856       0x2AE000        Squashfs filesystem, little endian, version 4.0, c
ompression:lzma, size: 8617464 bytes,  633 inodes, blocksize: 16384 bytes, creat
ed: Tue Nov 17 19:25:52 2015
```

Security by obscurity

- Nonstandard squashfs
  - Sasquatch
- Nonstandard compression
  - LZ77, LZ78
  - LZMA
- Nonstandard uboot
- ..and so on



F/OSS

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

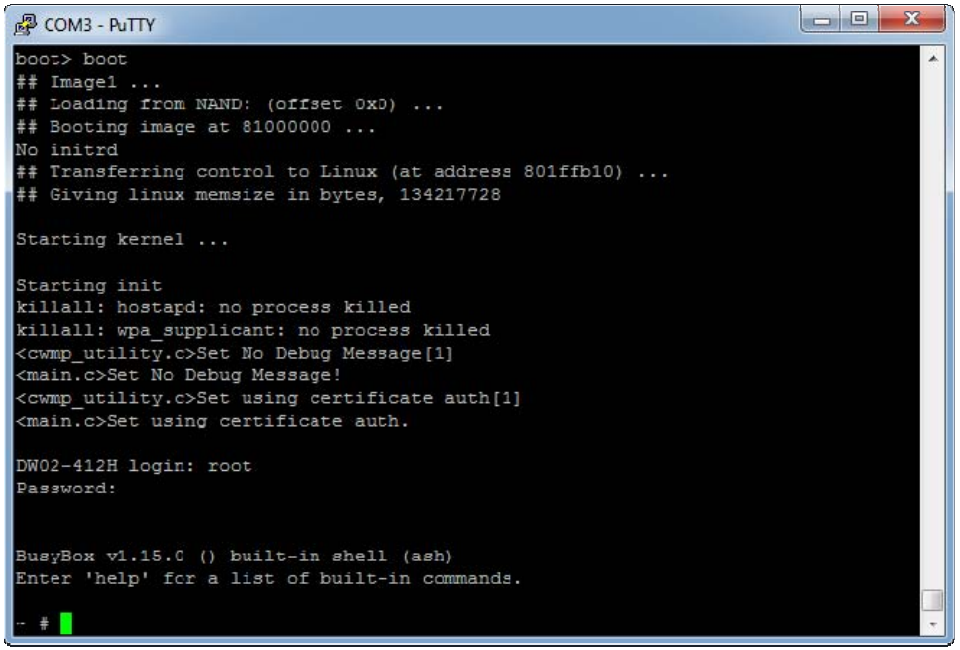
GNU license compliance

- Kernel source
- Underlying applications
- Delivery media with manual

루트권한 얻기

- setenv 사용하여 싱글모드 부팅

- setenv bootargs ${bootargs} 1



시스템 분석

- 기본 비밀번호 5자리
  - 브루트포스 이용하여 쉽게 복원
- /bin/rc에서 맥어드레스에 기반한 비밀번호 생성

```
.text:00404614 write_passwd:                          # CODE XREF: sub_404560+78↑j
.text:00404614                 lui     $v0, 0x44
.text:00404618                 addiu   $a0, $v0, (aVarEtcPasswd - 0x440000)  # "/var/etc/passwd"
.text:0040461C                 lui     $v0, 0x44
.text:00404620                 addiu   $a1, $v0, (aW - 0x440000)  # "w"
.text:00404624                 la      $t9, fopen
.text:00404628                 nop
.text:0040462C                 jalr    $t9 ; fopen
.text:00404630                 nop
.text:00404634                 lw      $gp, 0x2B0+var_2A0($fp)
.text:00404638                 sw      $v0, 0x2B0+stream($fp)
.text:0040463C                 lw      $v0, 0x2B0+stream($fp)
.text:00404640                 nop
.text:00404644                 beqz    $v0, loc_4046B4
.text:00404648                 nop
.text:0040464C                 jal     generate_password
.text:00404650                 nop
.text:00404654                 lw      $gp, 0x2B0+var_2A0($fp)
.text:00404658                 move    $a0, $v0
.text:0040465C                 jal     sub_40447C
.text:00404660                 nop
.text:00404664                 lw      $gp, 0x2B0+var_2A0($fp)
.text:00404668                 move    $v1, $v0
.text:0040466C                 lw      $a0, 0x2B0+stream($fp)  # stream
.text:00404670                 lui     $v0, 0x44
.text:00404674                 addiu   $a1, $v0, (aSS00RootBinSh - 0x440000)  # "%s:%s:0:0:root:/:/bin/sh₩n"
.text:00404678                 lw      $a2, 0x2B0+var_290($fp)
.text:0040467C                 move    $a3, $v1
.text:00404680                 la      $t9, fprintf
.text:00404684                 nop
.text:00404688                 jalr    $t9 ; fprintf
.text:0040468C                 nop
.text:00404690                 lw      $gp, 0x2B0+var_2A0($fp)
.text:00404694                 lw      $a0, 0x2B0+stream($fp)  # stream
.text:00404698                 la      $t9, fclose
.text:0040469C                 nop
.text:004046A0                 jalr    $t9 ; fclose
.text:004046A4                 nop
```

OpenWRT 빌드환경 준비

- 필수 패키지 설치
- OpenWRT 소스 준비
- Package feed 설치
- 환경설정

Feeds 설치

```
manatails@home-linux: ~/openwrt
File  Edit  View  Search  Terminal  Tabs  Help
manatails@W230SS: ~        manatails@home-linux: ~/openwrt
WARNING: No feed for package 'libyuv' found, maybe it's already part of the stan
dard packages?
WARNING: No feed for package 'libilbc' found, maybe it's already part of the sta
ndard packages?
WARNING: No feed for package 'libmemcached' found, maybe it's already part of th
e standard packages?
WARNING: No feed for package 'libsilk' found, maybe it's already part of the sta
ndard packages?
WARNING: No feed for package 'libg7221' found, maybe it's already part of the st
andard packages?
WARNING: No feed for package 'freeradius-client' found, maybe it's already part
of the standard packages?
Installing package 'freeswitch-stable' from telephony
Installing package 'freeswitch-stable-mod-bcg729' from telephony
Installing package 'kamailio-5.x' from telephony
Installing package 'libosip2' from telephony
Installing package 'miax' from telephony
Installing package 'pcapsipdump' from telephony
Installing package 'restund' from telephony
Installing package 'rtpproxy' from telephony
Installing package 'sipp' from telephony
Installing package 'siproxd' from telephony
Installing package 'yate' from telephony
manatails@home-linux:~/openwrt$
```

- 여러 패키지 소스를 일률적으로 분류하여 관리

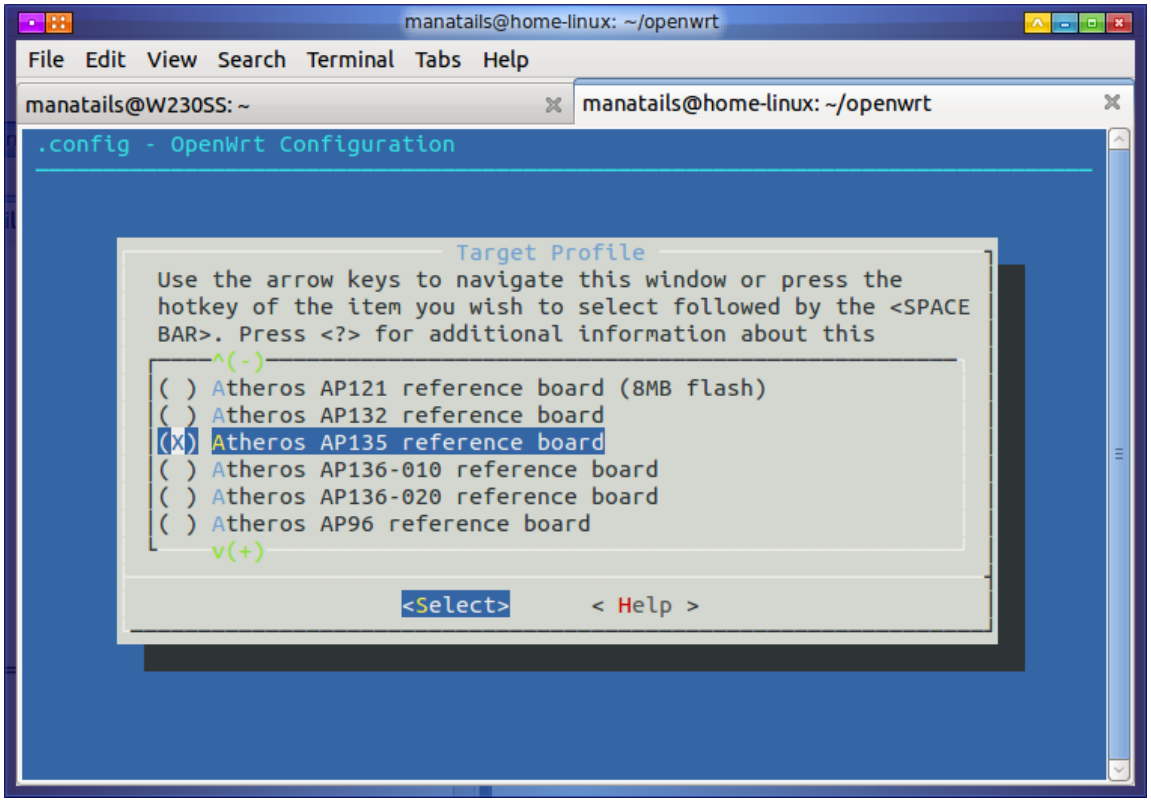
기본 설정

- sed --in-place=.bak -e 's/=m$/=n/g' .config
  - 모든 선택적 패키지 비활성화

- Make –j4 V=s IGNORE_ERRORS=m
  - 선택적 패키지 오류 무시

기본 설정

- 기기 종류
- 이미지 타입
- 커널 모듈
- 패키지

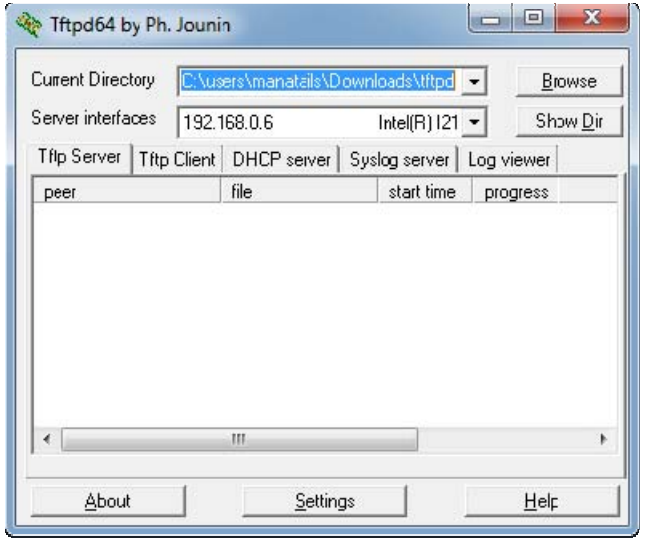


빌드 결과

- kernel
  - 기본 커널 이미지
- uimage
  - 커널 이미지에 uboot 헤더가 추가된 이미지
- rootfs
  - 루트 파일시스템
- Initramfs image
  - 램디스크를 루트 파티션처럼 사용
  - LiveCD
  - Kernel+rootfs

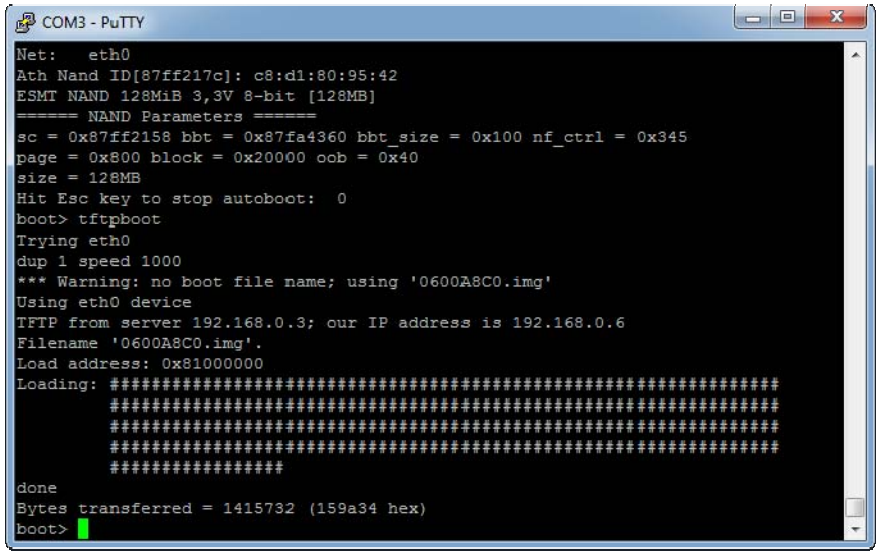
Firmware flashing

- TFTP 서버 이용
  - Tftpd64



- Common recovery method

- Uboot 환경변수에 설정



U-boot image format

- 64바이트 (0x40)
- 매직넘버
- 헤더영역 해쉬
- 데이터영역 해쉬
  - 데이터영역 사이즈

```
/*
 * Legacy format image header,
 * all data in network byte order (aka natural aka bigendian).
 */
typedef struct image_header {
        uint32_t        ih_magic;       /* Image Header Magic Number    */
        uint32_t        ih_hcrc;        /* Image Header CRC Checksum    */
        uint32_t        ih_time;        /* Image Creation Timestamp     */
        uint32_t        ih_size;        /* Image Data Size              */
        uint32_t        ih_load;        /* Data  Load  Address          */
        uint32_t        ih_ep;          /* Entry Point Address          */
        uint32_t        ih_dcrc;        /* Image Data CRC Checksum      */
        uint8_t         ih_os;          /* Operating System             */
        uint8_t         ih_arch;        /* CPU architecture             */
        uint8_t         ih_type;        /* Image Type                   */
        uint8_t         ih_comp;        /* Compression Type             */
        uint8_t         ih_name[IH_NMLEN];      /* Image Name           */
} image_header_t;
```

U-boot image format

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000  27 05 19 56 9D BF D2 6B 5A 52 3E 05 00 15 99 F4  '..V.¿ÒkZR>...™ô
00000010  80 06 00 00 80 06 00 00 B0 06 6C 5E 05 05 02 03  €...€...°.l^....
00000020  4D 49 50 53 20 4F 70 65 6E 57 72 74 20 4C 69 6E  MIPS OpenWrt Lin
00000030  75 78 2D 34 2E 39 2E 37 33 00 00 00 00 00 00 00  ux-4.9.73.......
00000040  6D 00 00 80 00 BC A8 46 00 00 00 00 00 00 00 6F  m..€.¼¨F.......o
00000050  FD FF FF A3 B7 7F 4C 39 C2 95 01 19 7A 6E DB C8  ýÿÿ£·.L9Â•..znÛÈ
00000060  2A E0 D8 9D 79 01 F2 FE 19 8D D0 E0 D0 89 63 2D  *àØ.y.òþ..ÐàÐ‰c-
00000070  7E C9 9D 34 D4 B7 00 FA E2 78 A5 3D C9 26 87 B9  ~É.4Ô·.úâx¥=É&‡¹
00000080  FB A5 5E 40 E6 3D 9C 8E F9 40 AA 02 65 C4 51 0E  û¥^@æ=œŽù@ª.eÄQ.
```

매직넘버

CRC 해쉬

빌드시간

데이터 크기

로드 주소

시작주소

데이터 CRC

펌웨어 이름

펌웨어 헤더 수정

- 68바이트 (0x44)

- 버전을 나타내는 32비트 값 존재

매직넘버 CRC해쉬 ??? 빌드시간

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000  27 05 19 56 0A F4 C1 95 00 02 04 00 56 4A FA A0  '..V.ôÁ•....VJú
00000010  00 94 9A 3A 80 00 20 00 80 1F FB 10 82 58 8D 6B  .”š:€. .€.û.‚X.k
00000020  05 05 02 03 49 53 51 2D 34 30 30 30 00 00 00 00  ....ISQ-4000....
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000040  00 00 00 00 5D 00 00 00 01 50 5C B0 00 00 00 00  ....].....P\°....
00000050  00 00 00 6F FD FF FF A3 B7 7F 63 C5 55 7E B6 B7  ...oýÿÿ£·.cÅU~¶·
00000060  C0 22 9B 58 96 55 67 6F 74 14 E4 C2 81 B5 38 CE  À"›X–Ugot.äÂ.µ8Î
00000070  8F B7 87 BE C2 C8 BE E9 47 C4 44 73 9E F5 0D 9E  .·‡¾ÂÈ¾éGÄDsžõ.ž
00000080  A5 A5 EF 7F 7A 1B 1F 8B BD D5 12 C8 AA 75 76 D1  ¥¥ï.z..‹½Õ.È ªuvÑ
```

펌웨어 헤더 수정

- 스크립트를 사용하여 자동화
- dd와 crc, xxd 이용

```
manatails@linux16: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 2.5.3              File: olleh.sh

FILENAME=bin/targets/ar71xx/generic/openwrt-15.05.1-r5691-f089b1f-ar71xx-generi$
SUFFIX=.olleh

dd if=$FILENAME of=orig_header.bin count=64 bs=1

dd if=orig_header.bin of=header.bin count=4 bs=1
printf '\x00\x00\x00\x00\x00\x02\x04\x00' | dd of=header.bin bs=1 seek=4 conv=n$
dd bs=1 skip=8 if=orig_header.bin >> header.bin

crc32 header.bin > crc.txt
xxd -r -p crc.txt crc.bin

dd if=crc.bin | dd of=header.bin bs=1 seek=4 conv=notrunc

dd if=header.bin of=$FILENAME$SUFFIX

dd bs=64 skip=1 if=$FILENAME of=$FILENAME$SUFFIX oflag=append conv=notrunc

cp $FILENAME$SUFFIX 0600A8C0.img
                          [ Read 19 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Linter ^_ Go To Line
```

기능 확인

- GPIO 조명
- 플래쉬 드라이버
- 무선랜 / 5GHz무선랜
- 스위치 / CPU 포트

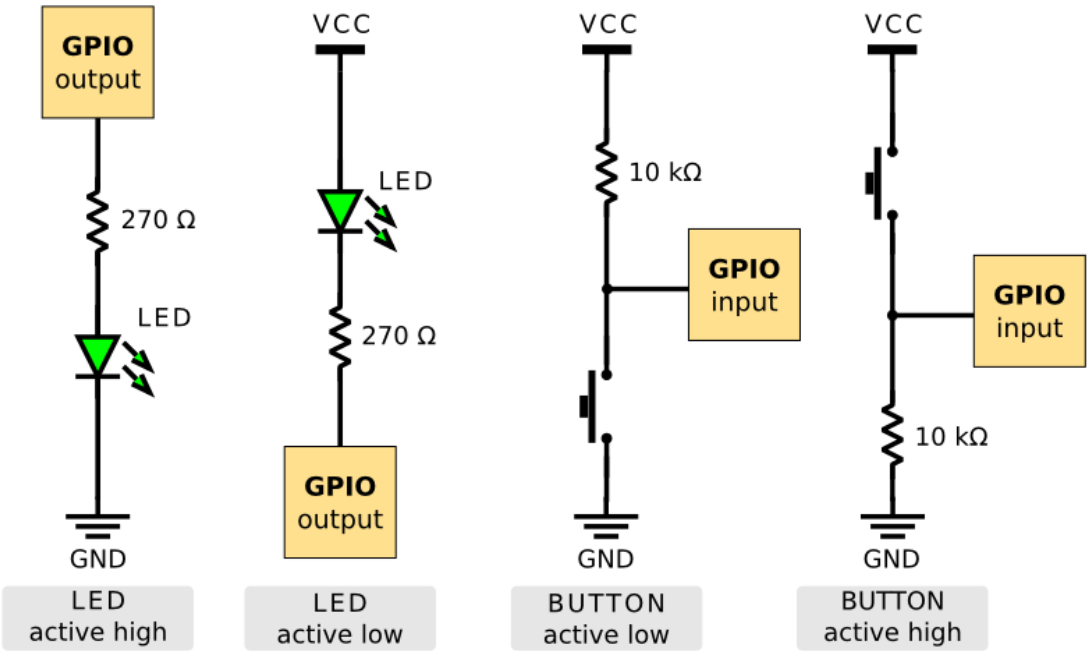
커널 로그 확인

COM3 - PuTTY

```
[    0.610000] NET: Registered protocol family 2
[    0.610000] TCP established hash table entries: 1024 (order: 0, 4096 bytes)
[    0.610000] TCP bind hash table entries: 1024 (order: 0, 4096 bytes)
[    0.620000] TCP: Hash tables configured (established 1024 bind 1024)
[    0.630000] TCP: reno registered
[    0.630000] UDP hash table entries: 256 (order: 0, 4096 bytes)
[    0.640000] UDP-Lite hash table entries: 256 (order: 0, 4096 bytes)
[    0.640000] NET: Registered protocol family 1
[    6.350000] futex hash table entries: 256 (order: -1, 3072 bytes)
[    6.360000] squashfs: version 4.0 (2009/01/31) Phillip Lougher
[    6.370000] jffs2: version 2.2 (NAND) (SUMMARY) (LZMA) (RTIME) (CMODE_PRIORIT
Y) (c) 2001-2006 Red Hat, Inc.
[    6.380000] msgmni has been set to 234
[    6.390000] io scheduler noop registered
[    6.390000] io scheduler deadline registered (default)
[    6.400000] Serial: 8250/16550 driver, 1 ports, IRQ sharing disabled
[    6.410000] console [ttyS0] disabled
[    6.430000] serial8250.0: ttyS0 at MMIO 0x18020000 (irq = 11, base_baud = 250
0000) is a 16550A
[    6.440000] console [ttyS0] enabled
[    6.440000] console [ttyS0] enabled
[    6.450000] bootconsole [early0] disabled
[    6.450000] bootconsole [early0] disabled
[    6.460000] m25p80 spi0.0: unrecognized JEDEC id 8c2115
```

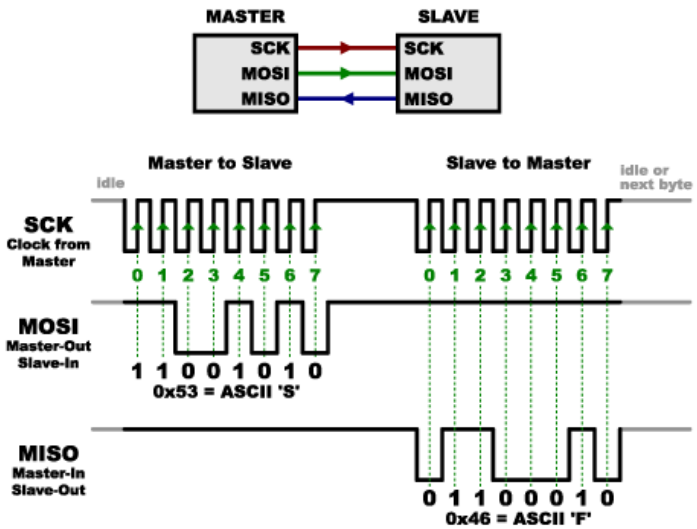
GPIO

- General Purpose Input Output
- SYSFS로 접근 가능: /sys/class/gpio



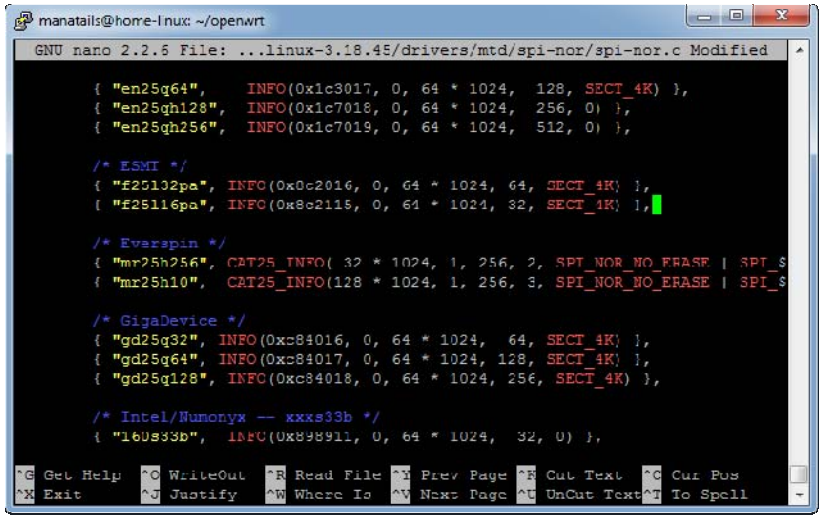
SPI

- *de-facto standard*
- 직렬 연결 기반의 단순한 제어 프로토콜
- Synchronous connection
- 저장장치, 센서



SPI-NOR

- 데이터시트 참조
- 커널 드라이버 수정



ESMT **F25L32PA**

Flash **3V Only 32 Mbit Serial Flash Memory with Dual**

■ FEATURES

- Single supply voltage 2.7~3.6V
- Standard and Dual SPI
- Speed
  - Read max frequency: 33MHz
  - Fast Read max frequency: 50MHz / 86MHz / 100MHz
  - Fast Read Dual max frequency: 50MHz / 86MHz / 100MHz (100MHz / 172MHz / 200MHz equivalent Dual SPI)
- Low power consumption
  - Active current: 35 mA
  - Standby current: 30 μA
  - Deep Power Down current: 5 μA
- Reliability
  - 100,000 typical program/erase cycles
  - 20 years Data Retention
- Program
  - Byte programming time: 7 μs (typical)
  - Page programming time: 1.5 ms (typical)
- Erase
  - Chip erase time 25 sec (typical)
  - Block erase time 1 sec (typical)
  - Sector erase time 90 ms (typical)
- Page Programming
  - 256 byte per programmable page
- Lockable 512 bytes OTP security sector
- SPI Serial Interface
  - SPI Compatible: Mode 0 and Mode 3
- End of program or erase detection
- Write Protect ($\overline{WP}$)
- Hold Pin ($\overline{HOLD}$)
- All Pb-free products are RoHS-Compliant

■ ORDERING INFORMATION

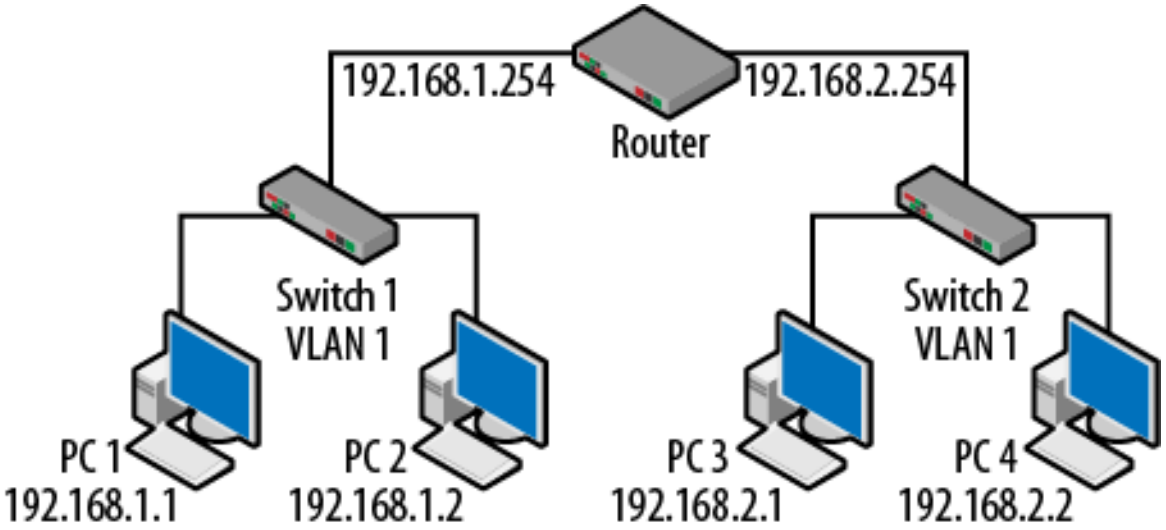
Product ID	Speed	Package		Comments
F25L32PA –50PAG	50MHz	8 lead SOIC	200mil	Pb-free
F25L32PA –86PAG	86MHz	8 lead SOIC	200mil	Pb-free

설정 편집

- lib/wifi/80211.sh

- Wi-Fi 연결에 대한 기본 설정

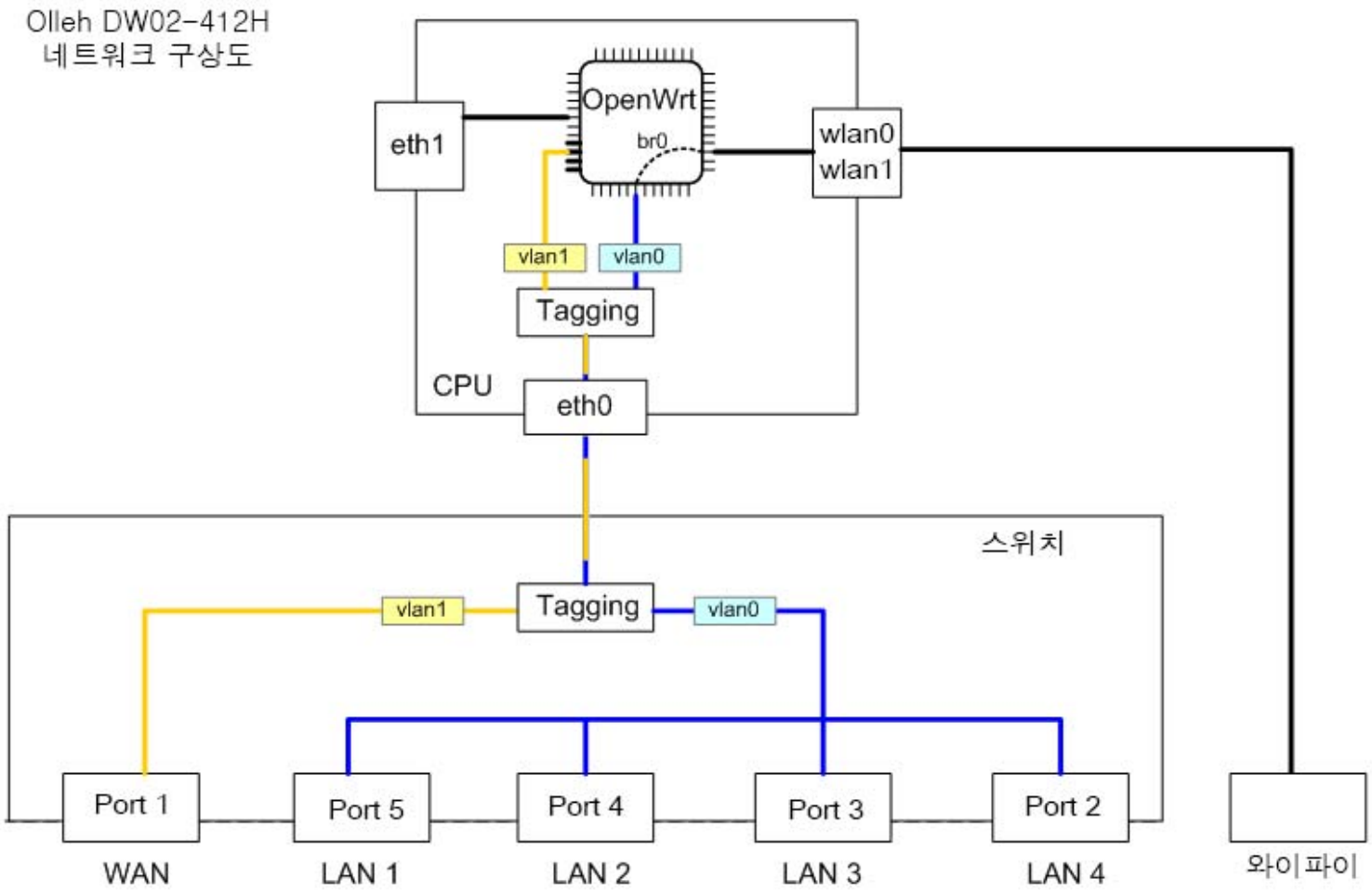
스위치 구성



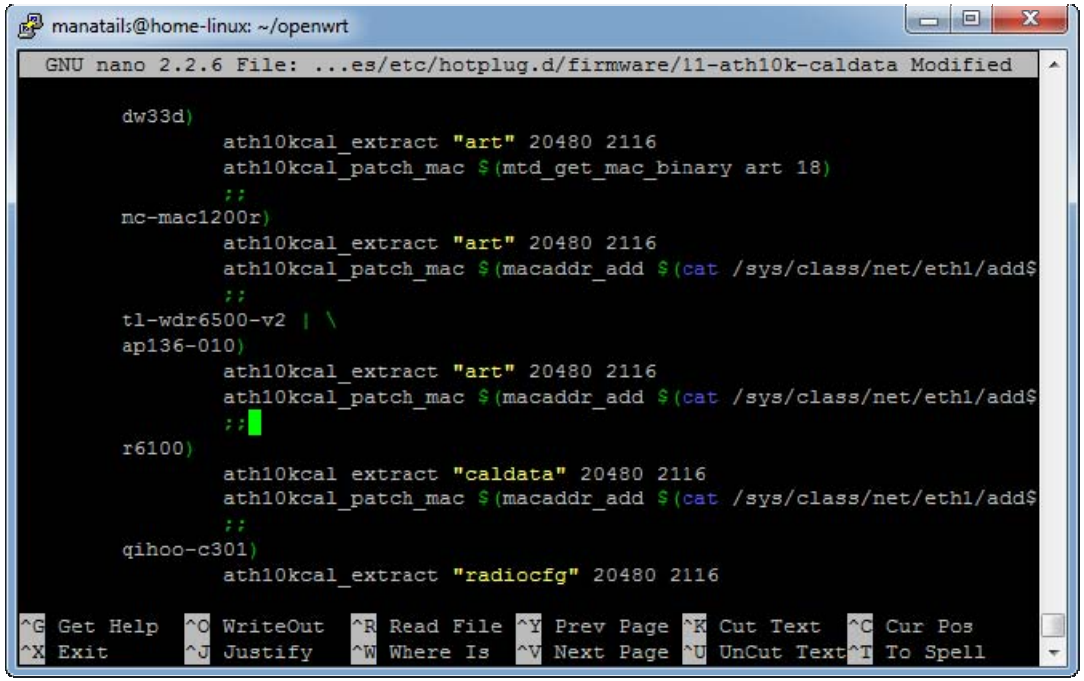
- 공유기 = 라우터 + 스위치 + (무선 AP)

- CPU 포트가 스위치에 연결되어있는 형태

스위치 구성


Olleh DW02-412H
네트워크 구상도
OpenWrt
br0
eth1
wlan0
wlan1
vlan1
vlan0
Tagging
CPU
eth0
스위치
vlan1
Tagging
vlan0
Port 1
Port 5
Port 4
Port 3
Port 2
WAN
LAN 1
LAN 2
LAN 3
LAN 4
와이파이

5GHz 칩셋 활성화



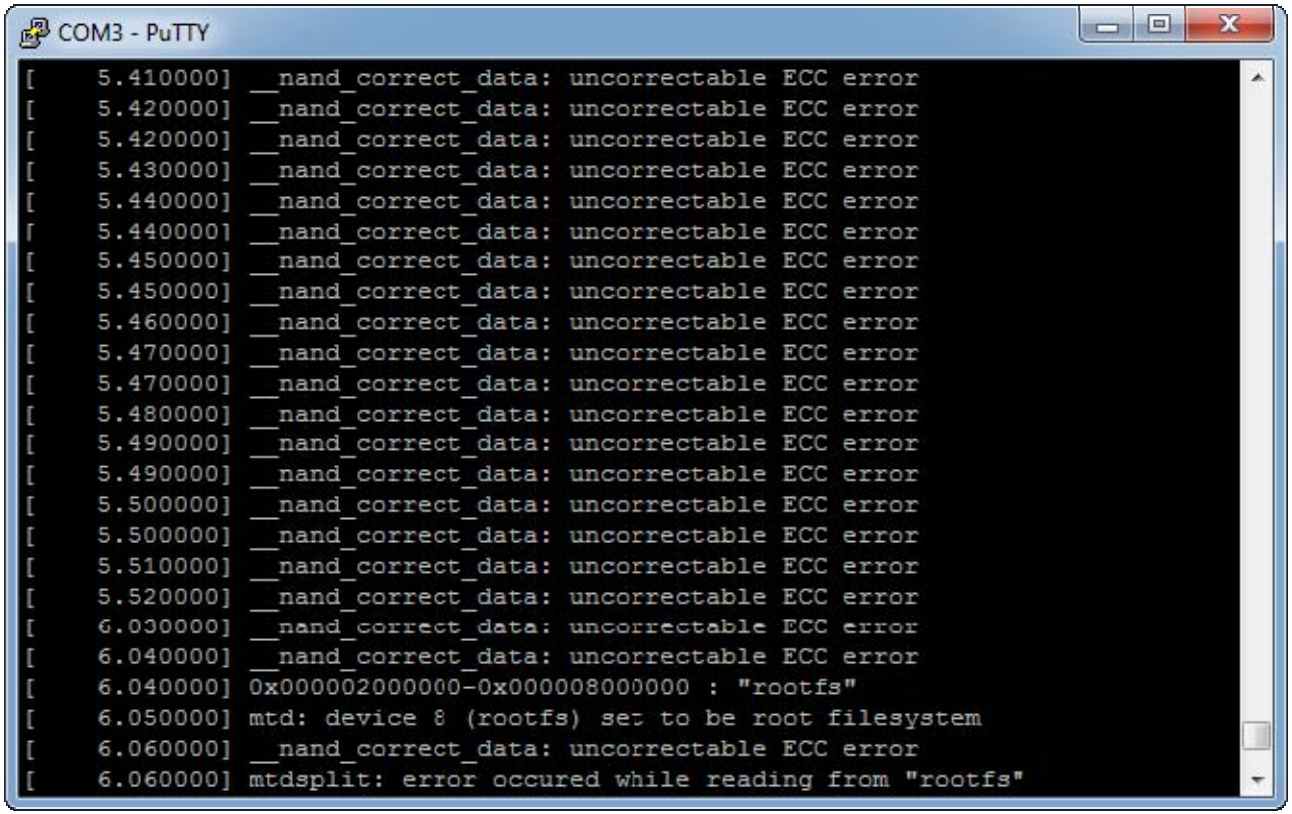
- 바이너리 드라이버 설치
- NOR 의 art영역 사용

Atheros ART

Size (byte)	Type	Name	Description
1	Unsigned Int	EEPROM Version	Eg: 0x02
1	Unsigned Int	Template Version	Eg: 0x02
6	Unsigned Int	MAC Address	Eg: 0x00 0x02 0x03 0x04 0x05 0x06
20	Unsigned Int	Customer Data	
			Base EEEPROM Header
2	Unsigned LE Int	Regulatory Domain 1	length in bytes
2	Unsigned LE Int	Regulatory Domain 2	length in bytes
1	4 bit/4 bit	TX RX Mask	First 4 bit TX Mask, last 4 bit RX Mask
1	Unsigned Int	Operatoin Flags	
1	Unsigned Int	EEP Misc	
1	Unsigned Int	RF Silent	
1	Unsigned Int	BlueTooth Options	
1	Unsigned Int	Device Capabilities	
1	Unsigned Int	Device Type	

- MAC주소, TRX설정, 규제정보 등..

NAND 설정



- Hardware ECC 설정

NAND 설정

manatails@home-linux: ~/openwrt

File Edit View Search Terminal Help

GNU nano 2.2.6 File: .../linux-3.18.45/arch/mips/ath79/mach-ap136.c

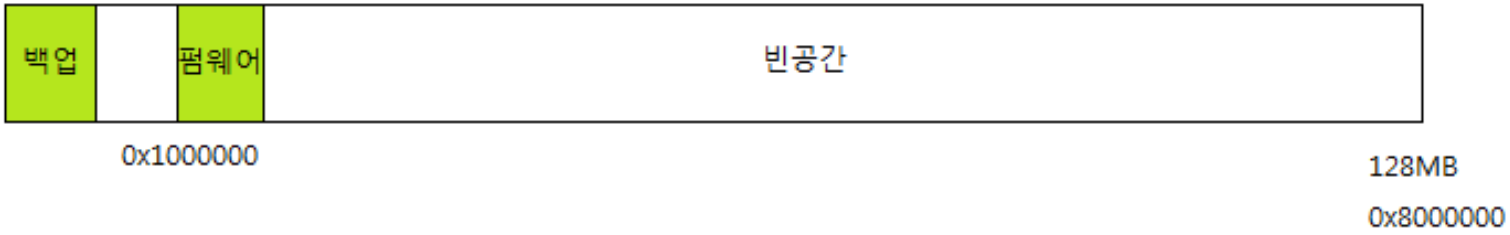
```
        ath79_register_leds_gpio(-1, ARRAY_SIZE(ap136_leds_gpio),
                                 ap136_leds_gpio);
        ath79_register_gpio_keys_polled(-1, AP136_KEYS_POLL_INTERVAL,
                                        ARRAY_SIZE(ap136_gpio_keys),
                                        ap136_gpio_keys);

        ath79_register_usb();

        //ath79_nfc_set_swap_dma(true);
        ath79_nfc_set_ecc_mode(AR934X_NFC_ECC_HW);
        ath79_register_nfc();

        ath79_register_wmac(art + AP136_WMAC_CALDATA_OFFSET, NULL);

        ath79_setup_qca955x_eth_cfg(QCA955X_ETH_CFG_RGMII_EN);

        ath79_register_mdio(0, 0x0);
        ath79_init_mac(ath79_eth0_data.mac_addr, art + AP136_MAC0_OFFSET, 0);
```

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

NAND 구성

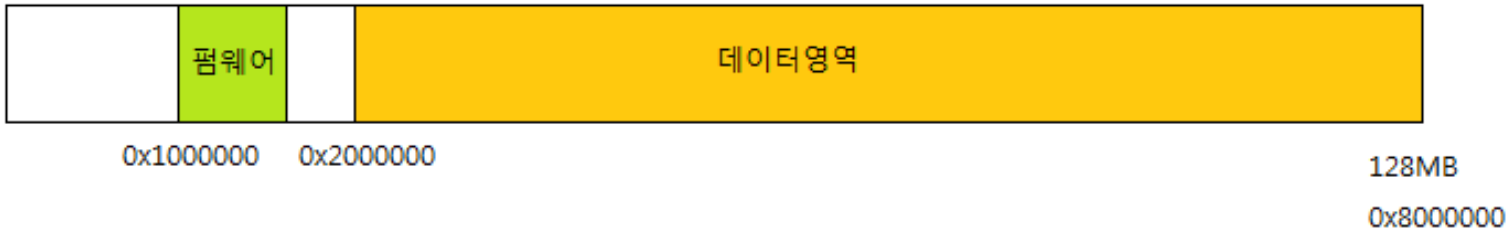
DW02-412H NAND

F59L1G81LA



DW02-412H NAND

F59L1G81LA



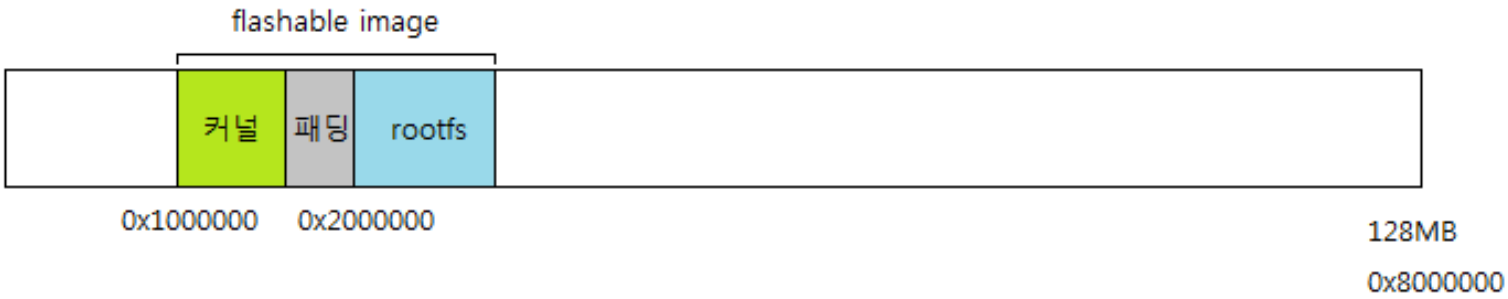
Filesystem Format

- SquashFS
  - 공간 효율이 좋음
  - Read-only
  - JFFS2와 병용

SquashFS + JFFS2

- JFFS2
  - Journaling
  - Wear leveling
  - Compressed

실제 이미지



- uImage + zero pad + jffs2
- 스크립트 이용 자동화

Final boot process

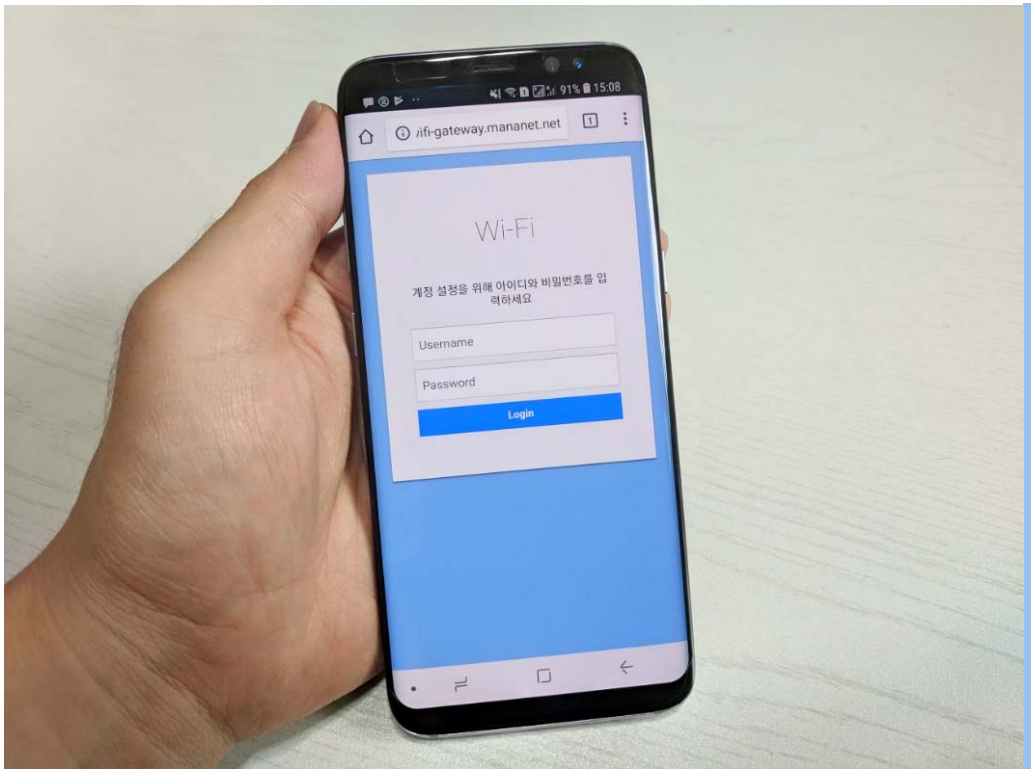
COM3 - PuTTY

```
[    0.740000] console [ttyS0] enabled
[    0.750000] bootconsole [early0] disabled
[    0.750000] bootconsole [early0] disabled
[    0.760000] m25p80 spi0.0: found f25l16pa, expected m25p80
[    0.770000] m25p80 spi0.0: f25l16pa (2048 Kbytes)
[    0.770000] 6 cmdlinepart partitions found on MTD device spi0.0
[    0.780000] Creating 6 MTD partitions on "spi0.0":
[    0.780000] 0x000000000000-0x000000040000 : "boot"
[    0.790000] 0x000000040000-0x000000050000 : "benv"
[    0.790000] 0x000000050000-0x000000060000 : "log"
[    0.000000] 0x0000001d0000-0x0000001e0000 : "nvram"
[    0.810000] 0x0000001e0000-0x0000001f0000 : "nvbackup"
[    0.810000] 0x0000001f0000-0x000000200000 : "art"
[    0.820000] nand: device found, Manufacturer ID: 0xc8, Chip ID: 0xd1
[    0.830000] nand: Unknown NAND 128MiB 3,3V 8-bit
[    0.830000] nand: 128MiB, SLC, page size: 2048, OOB size: 64
[    0.840000] Scanning device for bad blocks
[    0.890000] 3 cmdlinepart partitions found on MTD device ar934x-nfc
[    0.890000] Creating 3 MTD partitions on "ar934x-nfc":
[    0.900000] 0x000000000000-0x000001000000 : "current"
[    0.900000] 0x000001000000-0x000008000000 : "firmware"
[    2.080000] random: nonblocking pool is initialized
[    3.870000] 0x000002000000-0x000008000000 : "rootfs"
[    3.880000] mtd: device 8 (rootfs) set to be root filesystem
```

Usage

- MIPS 기반 임베디드 컴퓨터
- OpenWRT ipkg 이용

Usage



- Iptables 를 이용한 Wi-Fi 로그인 시스템

Security concerns

- Remote vulnerabilities
  - dhcpd 원격 명령어 실행 취약점
    - ISC-DHCP
    - Busybox dhcpd
  - Shellshock 권한 상승 취약점
- 제조사 백도어
  - Iptime
  - TP-Link, D-link, NETGEAR…

Security concerns

- 자동 (강제) 펌웨어 업데이트
  - 매 부팅시 스크립트로 실행

- TR-069
  - SOAP-HTTP 기반의 원격 관리 프로토콜
  - 통신사에서 임의적 설정 변경 가능

NAT Hardware acceleration

- WAN – LAN 사이 패킷은 라우팅 필요
- Closed source
- HW
  - 칩셋에서 바로 처리
  - 좋은 효율
  - 간단한 라우팅에 한정
- SW
  - 방화벽
  - CPU 처리 속도에 영향

국내 개발이 부진한 이유

- 국산 업체들의 반(反)오픈소스적 태도
  - GPL 무시
- 저가형 모델 다수
  - ipTIME 등
  - Realtek SoC – crippled MIPS
  - RAM 16MB 이하
  - Flash 4MB 이하
- 개발자, 커뮤니티의 부재

Q&A