Free Technology Workshop

Hacking Wi Fi

Hands on with wireless LAN routers,
packet capture and wireless security

Organised by Steven Gordon
Bangkadi 3rd floor IT Lab
10:30-13:30 Friday 18 July 2014
http://ict.siit.tu.ac.th/moodle/

WIRELESS FREEDOM

Aims

- Understand what is a “wireless router”
- See the internals (hardware)
- Know about (open source) firmware
- Understand what is a “wireless LAN”
- Setup a wireless LAN
- Aware of security features in wireless LANs
- Capture wireless packets (“sniffing”)
- Bypass security features in wireless LANs

Sources

- openwrt.org
- wikipedia.org
- and others

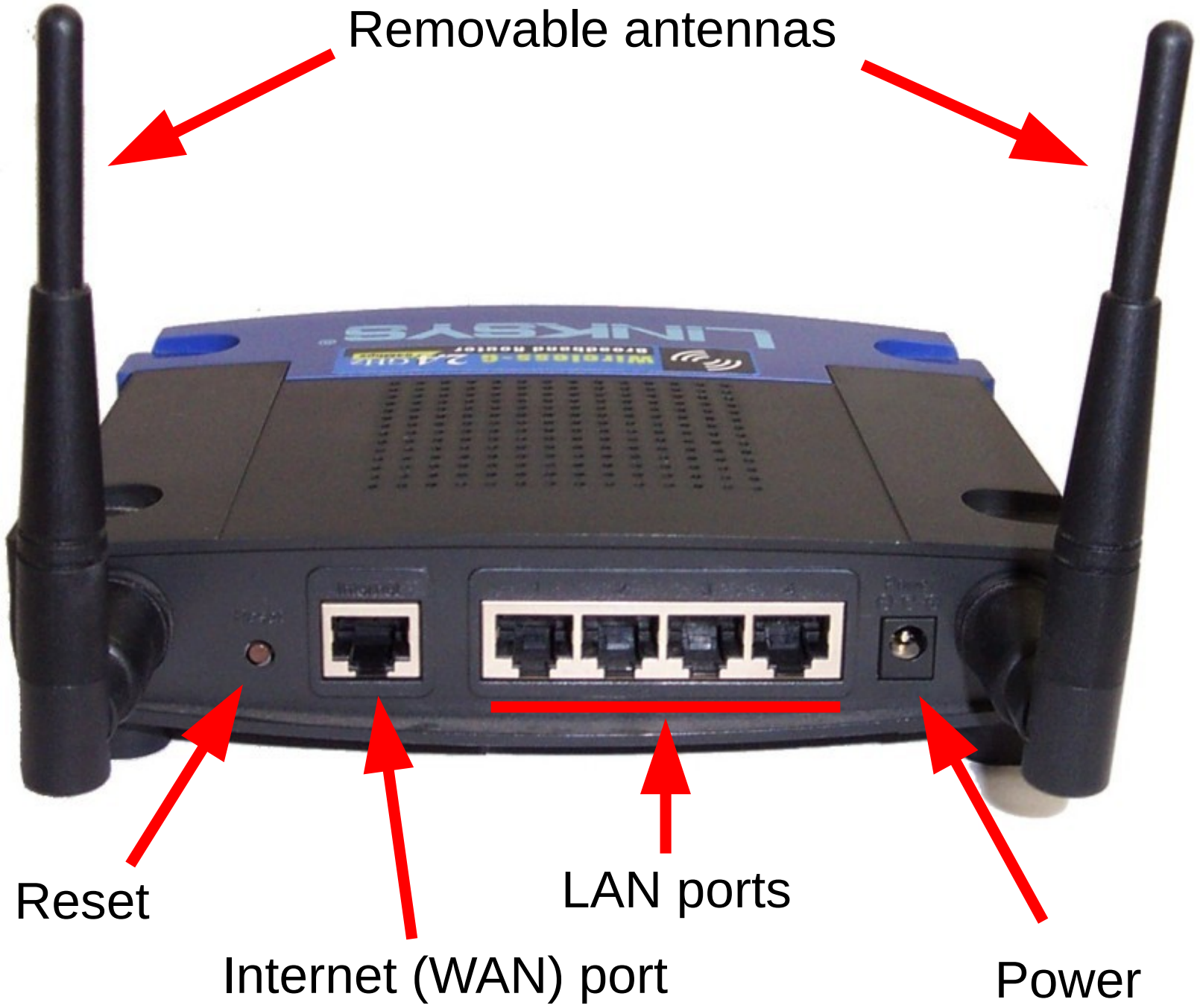
Naming, Acronyms, etc.

- AP - access point
- BSSID - basic SSID — *identifies AP*
- CTS - clear to send
- ESSID - extended SSID — *identifies network (also SSID)*
- LAN - local area network
- MAC - medium access control (layer) — *defines how to share channel with others*
- NAT - network address translation — *allows private addressing in internal network*
- PHY - physical (layer) — *defines data rate, channels, power, signals, ...*
- RTS - request to send
- SSID - service set identifier
- WAN - wide area network
- WEP - wired equivalent privacy — *insecure encryption*
- WLAN - wireless LAN — *also WiFi, IEEE 802.11*
- WMM - wireless multimedia mode — *priority for voice, video packets*
- WPA - WiFi protected access — *secure encryption*
- WRT - wireless router

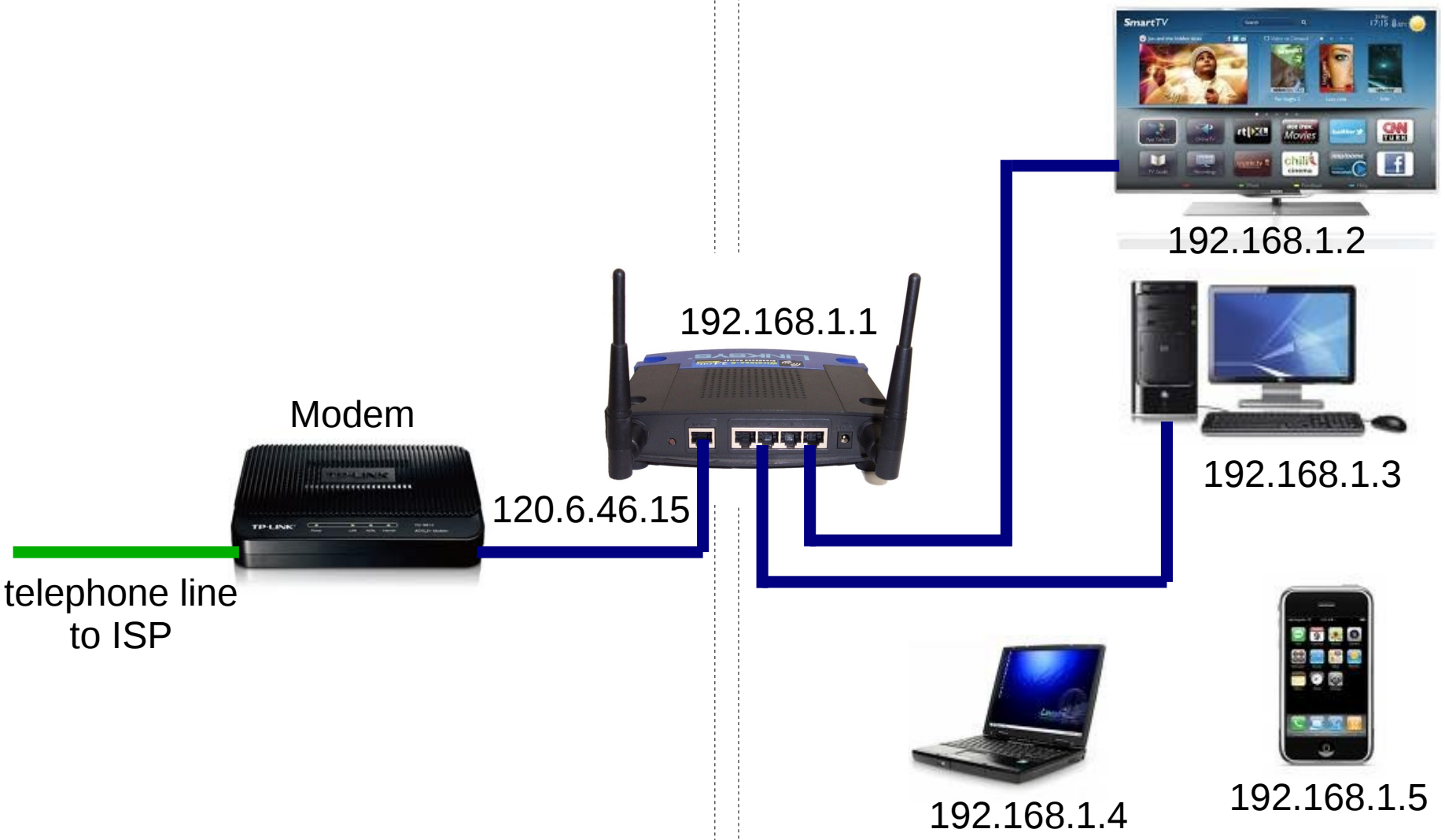
Quick Reference

- Router IP: 192.168.1.1
- Router username: root
- Router password: s11tnetw0rk
- Router name and SSID: ICTR*xx* (*xx*=10, 11, ...)
- iMac username: student
- iMac password: student
- Software: http://ict.siit.tu.ac.th/software/
- Workshop: http://ict.siit.tu.ac.th/moodle/

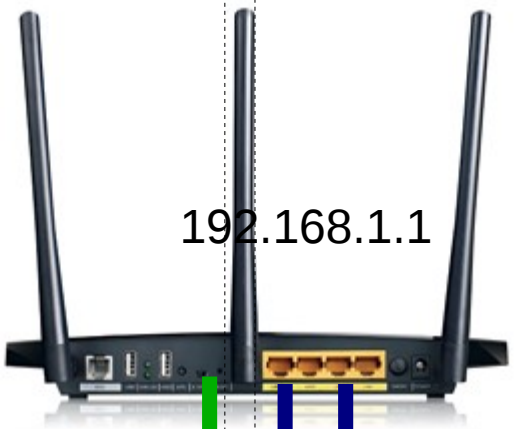
Wireless Routers


Removable antennas
Reset
Internet (WAN) port
LAN ports
Power

Wireless Router at Home



Wireless All-in-one Router at Home



192.168.1.1

120.6.46.15

telephone line
to ISP

192.168.1.2

192.168.1.3

192.168.1.4

192.168.1.5

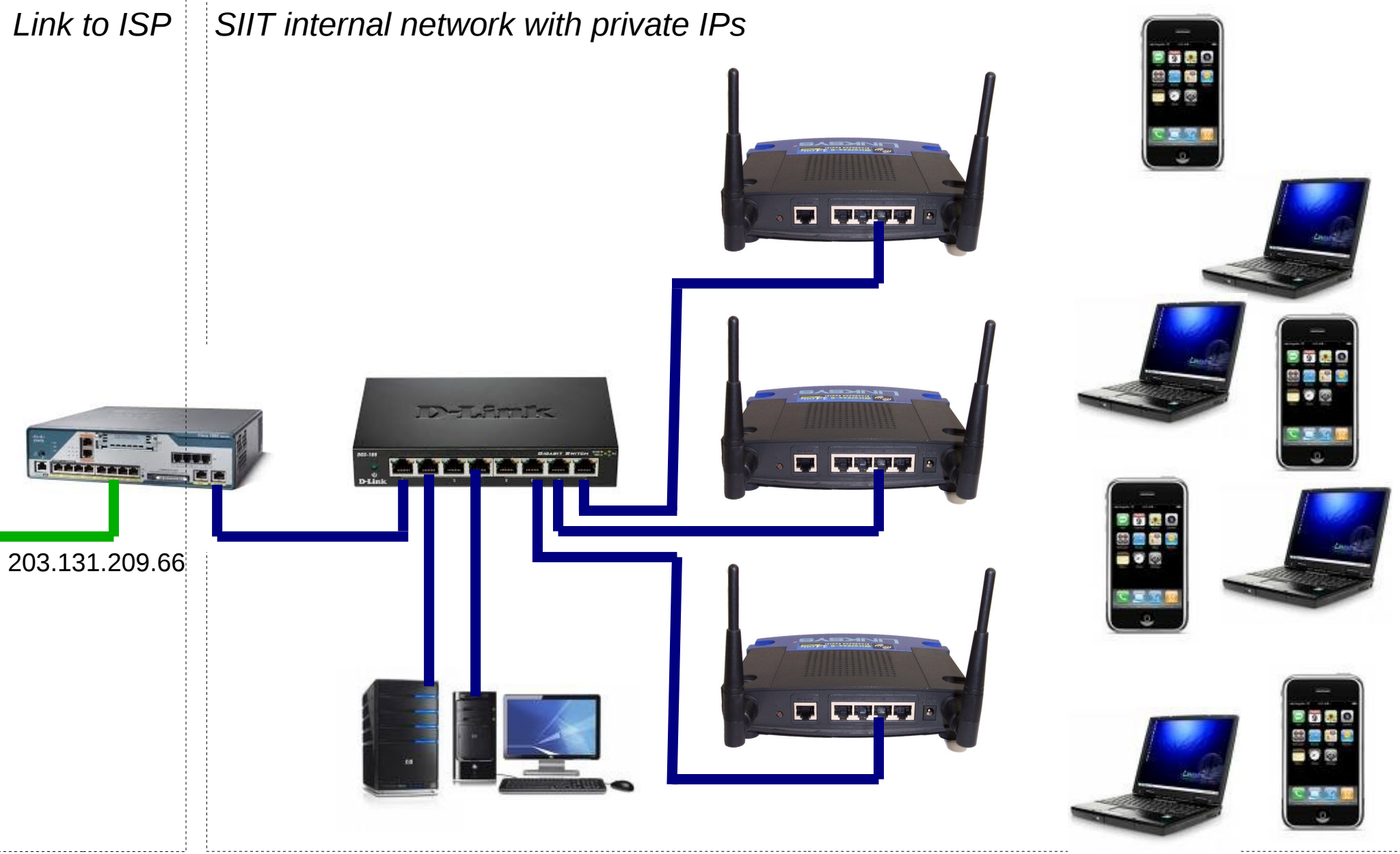
Internet connection with public IP

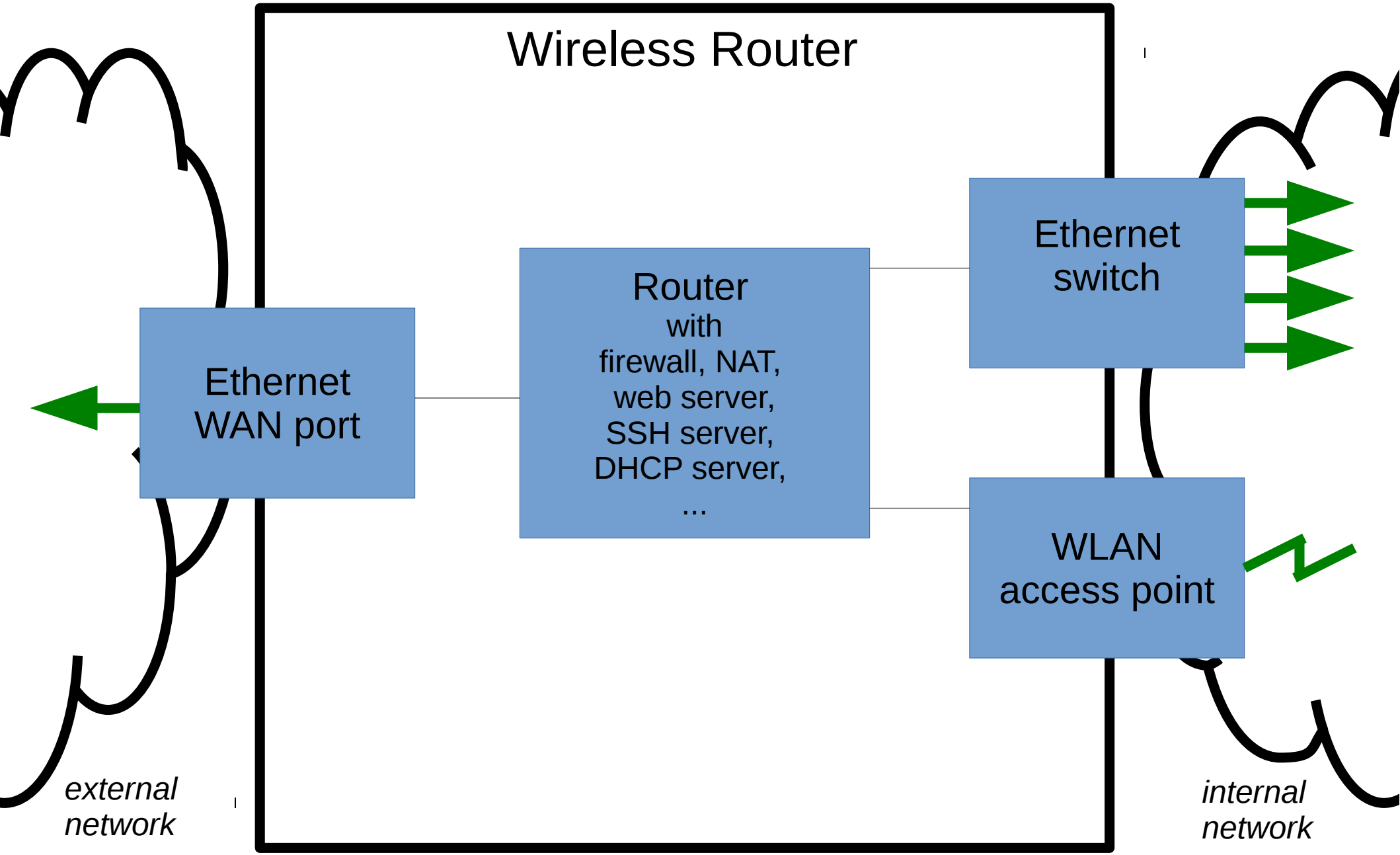
internal LAN with private IPs

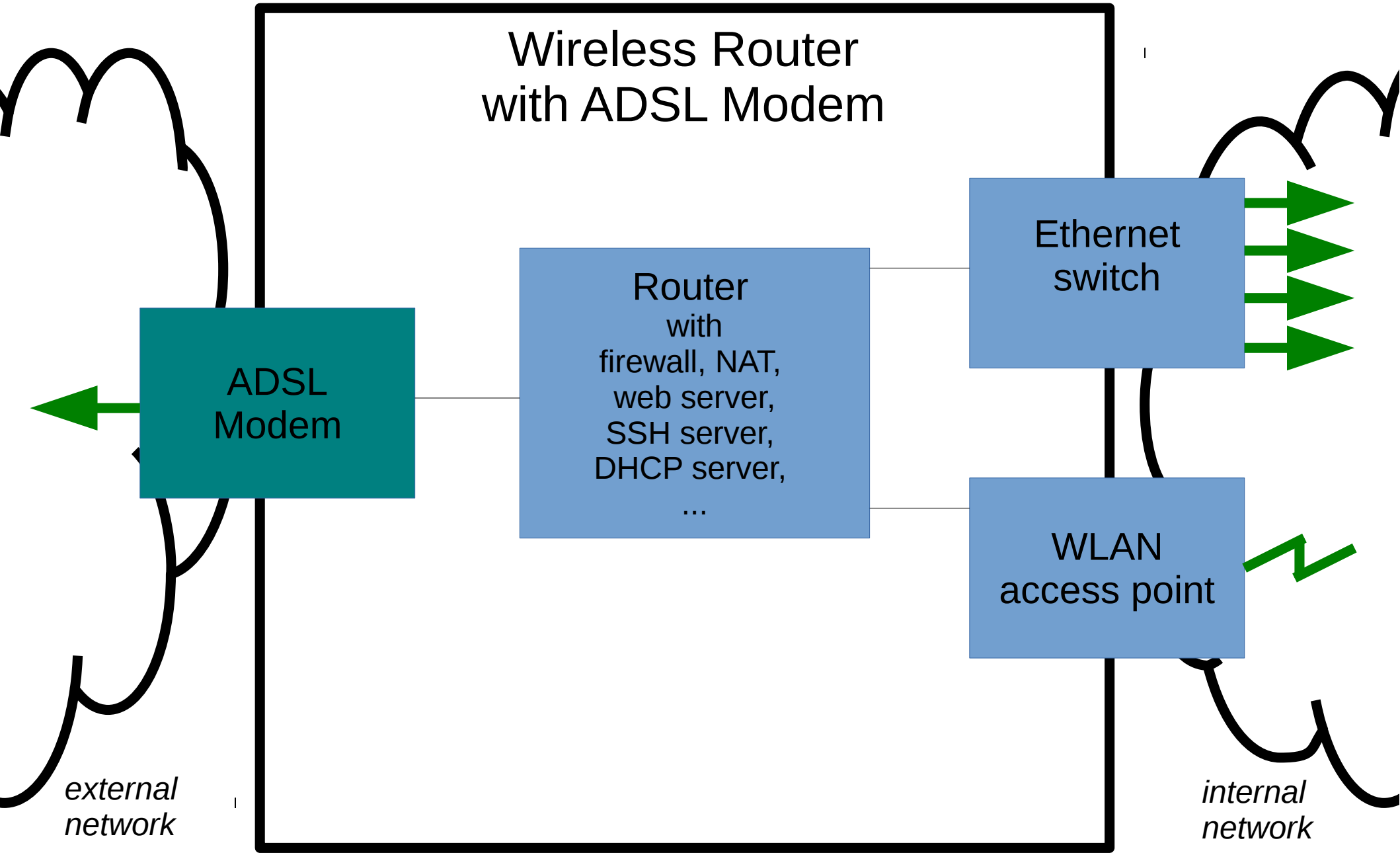
Wireless LAN AP at SIIT

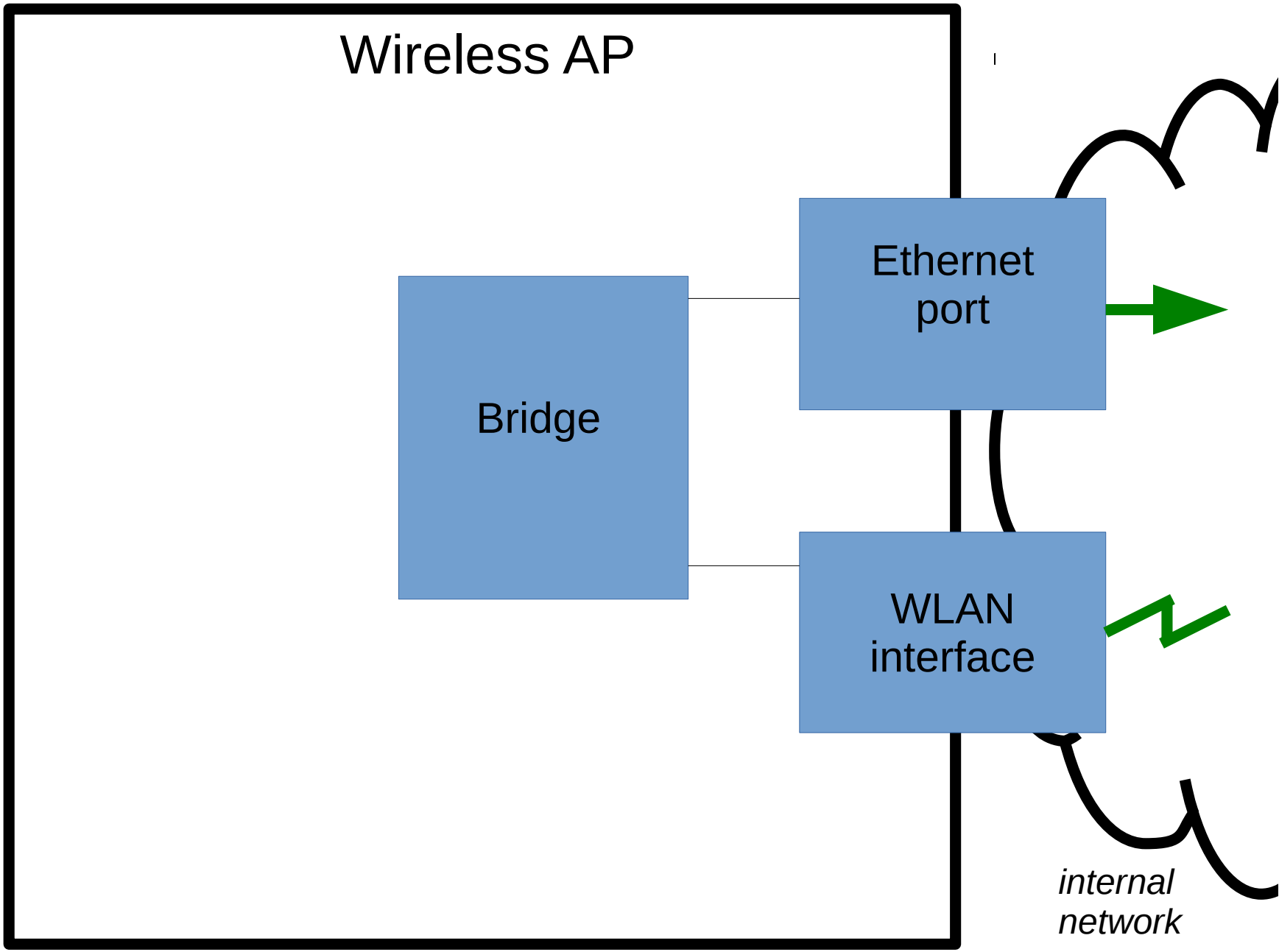
Link to ISP

SIIT internal network with private IPs




Wireless Router
Ethernet
WAN port
Router
with
firewall, NAT,
web server,
SSH server,
DHCP server,
...
Ethernet
switch
WLAN
access point
external
network
internal
network

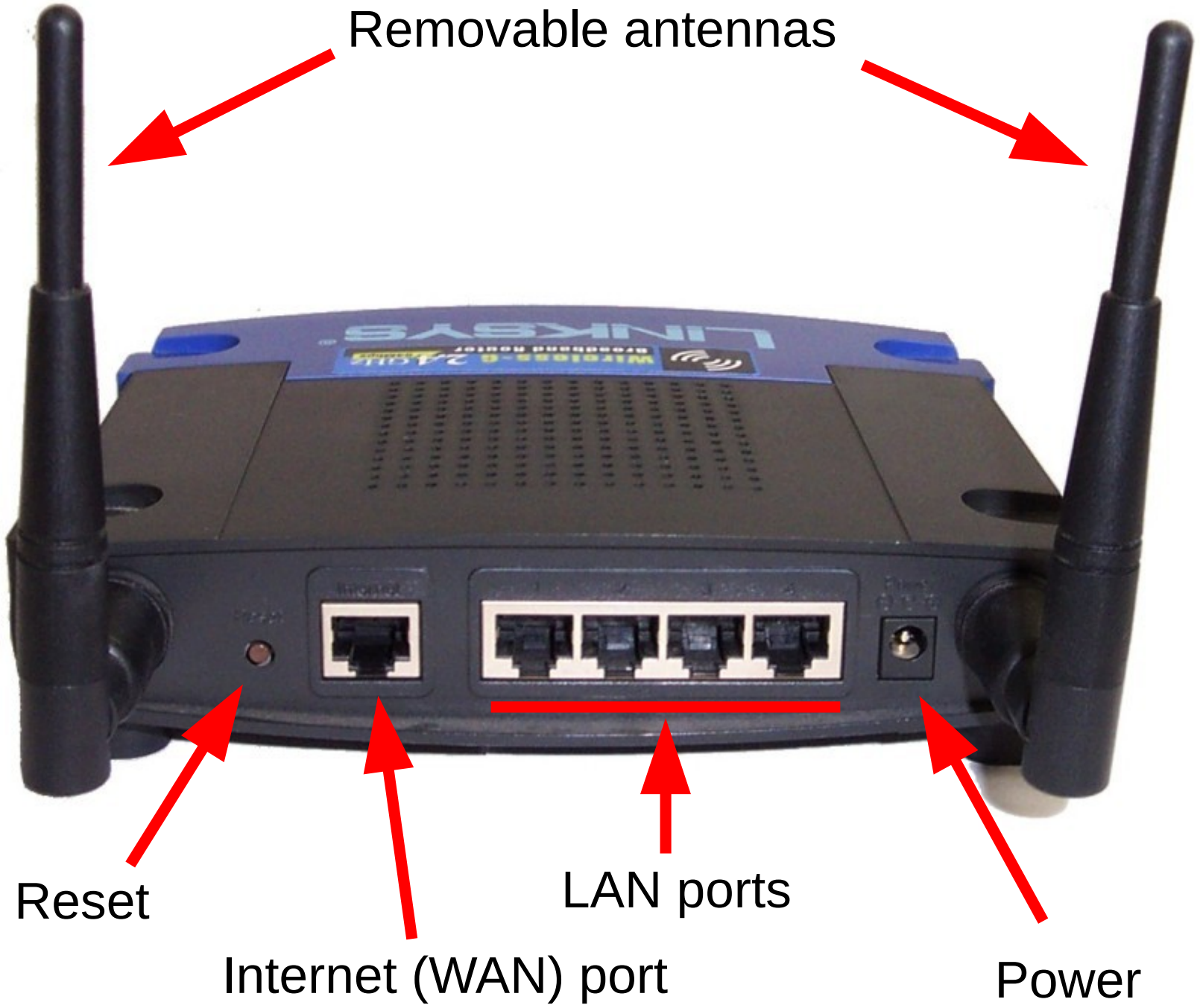

Wireless Router
with ADSL Modem
ADSL
Modem
Router
with
firewall, NAT,
web server,
SSH server,
DHCP server,
...
Ethernet
switch
WLAN
access point
external
network
internal
network


Wireless AP
Bridge
Ethernet port
WLAN interface
internal network

Router

All-in-one

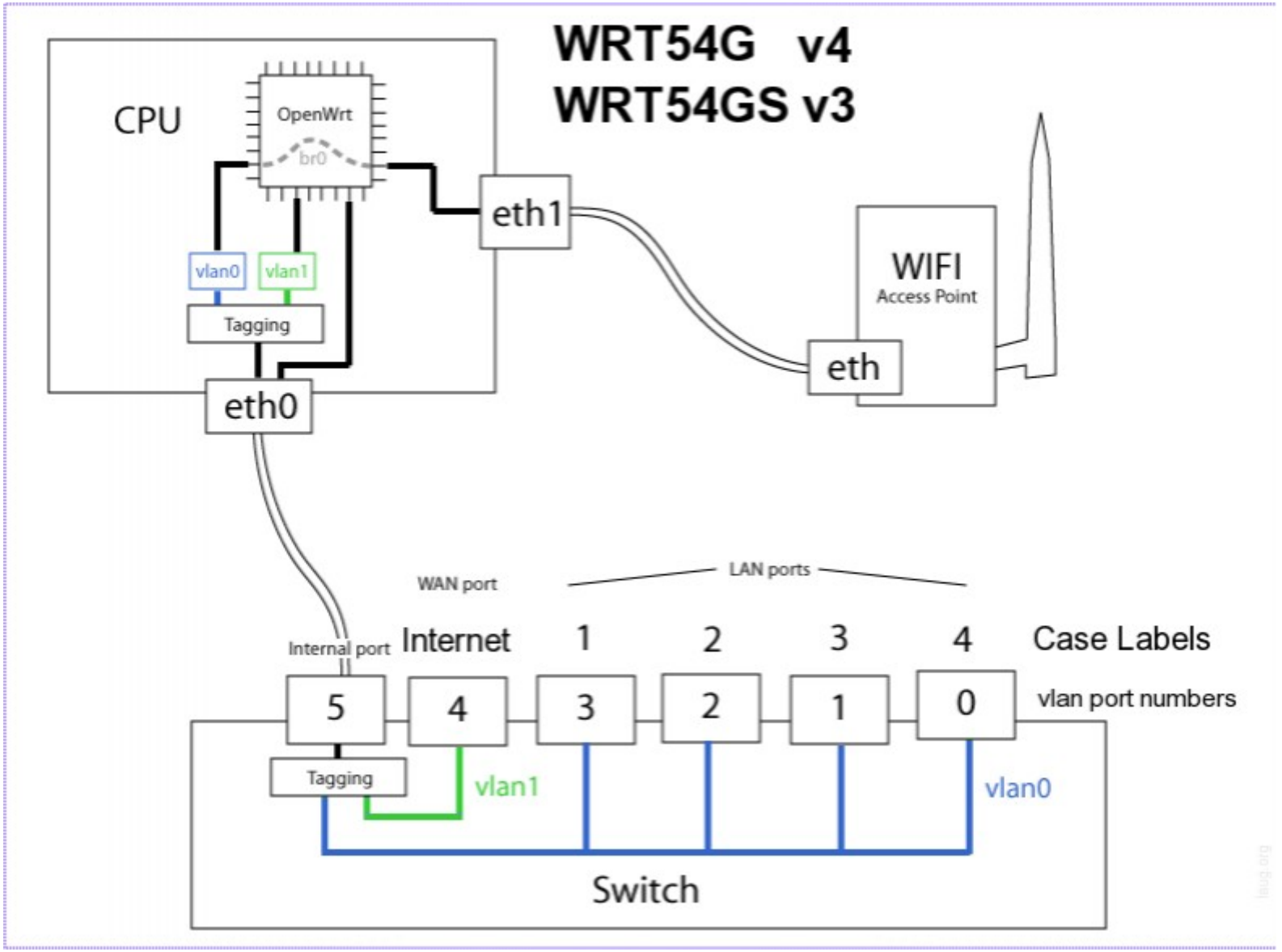
AP

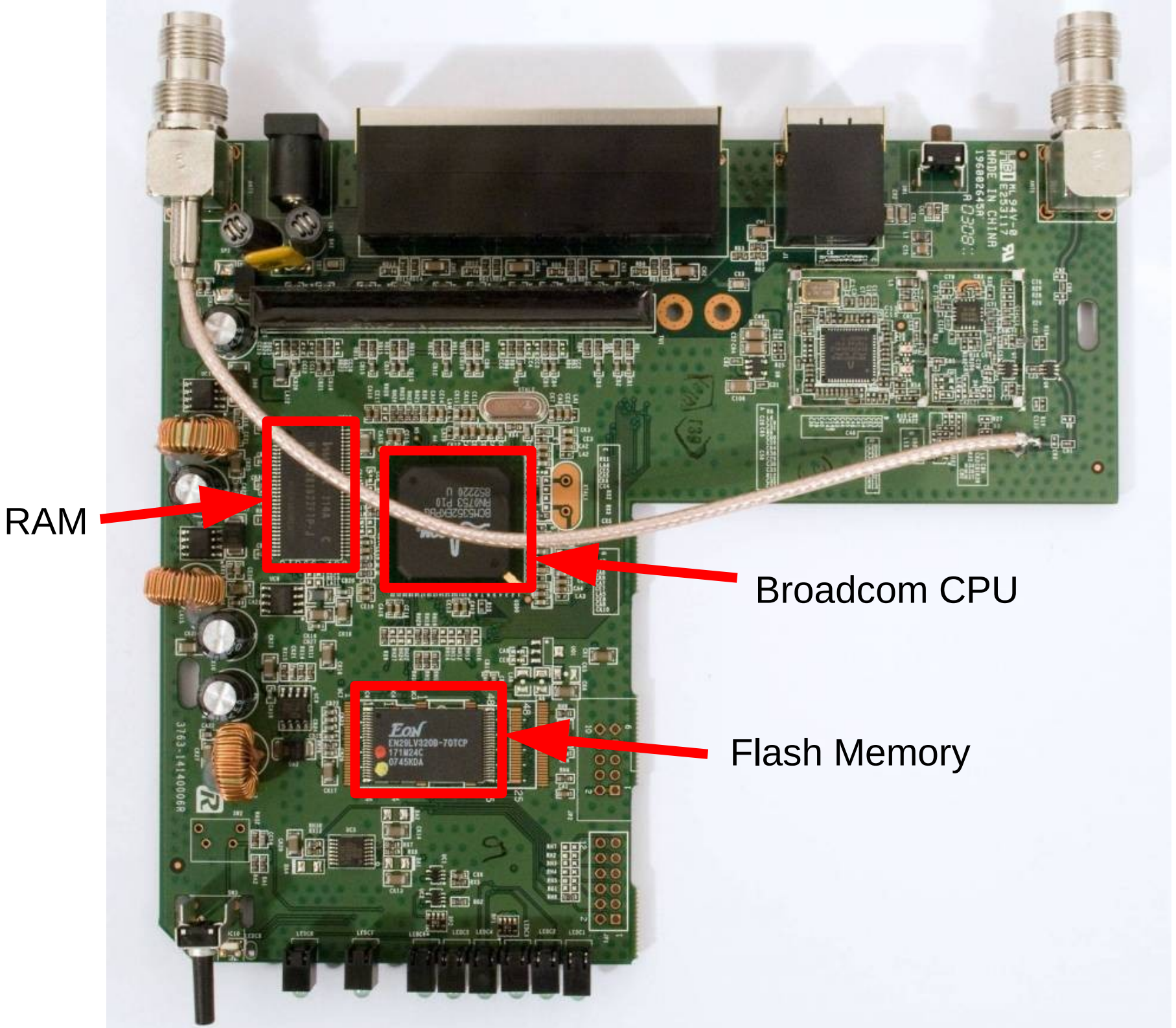

Removable antennas
Reset
Internet (WAN) port
LAN ports
Power

Linksys WRT54G(L)

Since 2003, popular wireless router with Linux firmware supports 3rd party firmware

• CPU: Broadcom 200MHz	*32-bit MIPS*
• Flash: 4MB	*Non-volatile storage*
• RAM: 16MB	*Volatile storage*
• Wireless chip: Broadcom (integrated)	*CPU + WiFi + Switch*
• Wireless PHY: 11b, 11g	*Up to 54 Mb/s*
• Wireless Tx Power: 63 mW	*Adjustable*
• Antenna: 2 x 2.2dBi dipole	*Removable RP-SMA*
• Wired ports: 5 x 10/100Mb/s	*4 x LAN + 1 x WAN*


WRT54G v4
WRT54GS v3
CPU
OpenWrt
br0
eth1
vlan0
vlan1
Tagging
eth0
WIFI
Access Point
eth
WAN port
LAN ports
Internal port
Internet
1
2
3
4
Case Labels
5
4
3
2
1
0
vlan port numbers
Tagging
vlan1
vlan0
Switch

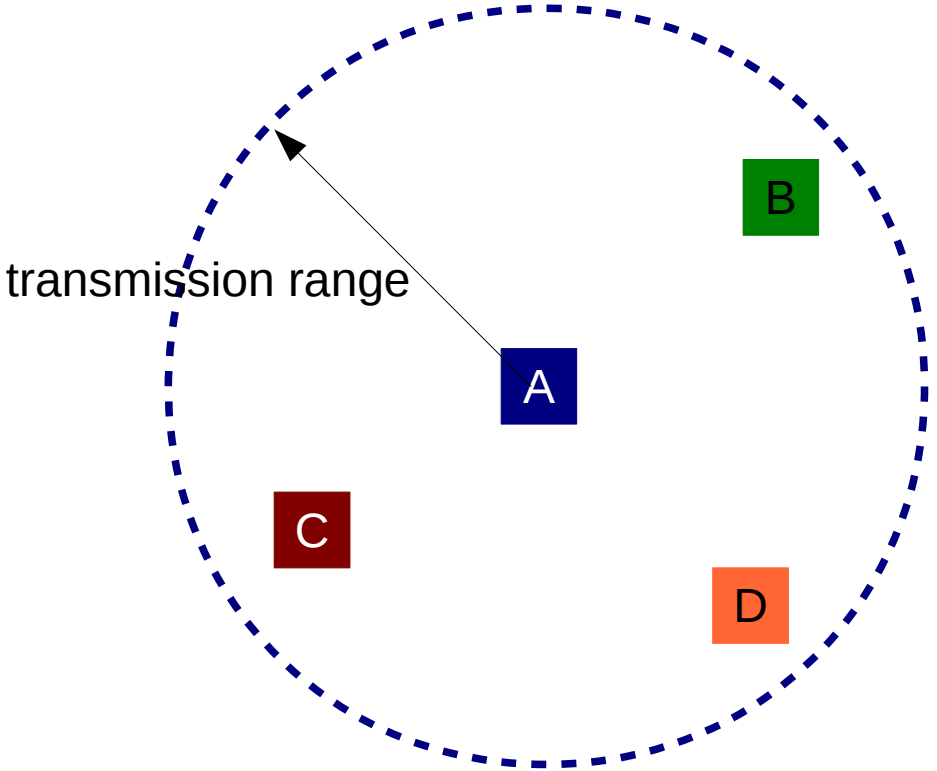

RAM
Broadcom CPU
Flash Memory
EON
EN29LV320B-70TCP

Wireless LANs

Wireless LANs

- IEEE 802.11 (standards), WiFi (marketing)
- Aim: Provide equivalent functionality to wired Ethernet
- Advantages of wireless:
  - No wires
  - Mobility
- Disadvantages of wireless:
  - More errors, varying delay: hard to achieve same performance as wires
  - Spectrum/frequencies available is limited: cannot just add more wires
  - Radio transmissions are broadcast: No “physical” security

Wireless LANs: Broadcast Radio



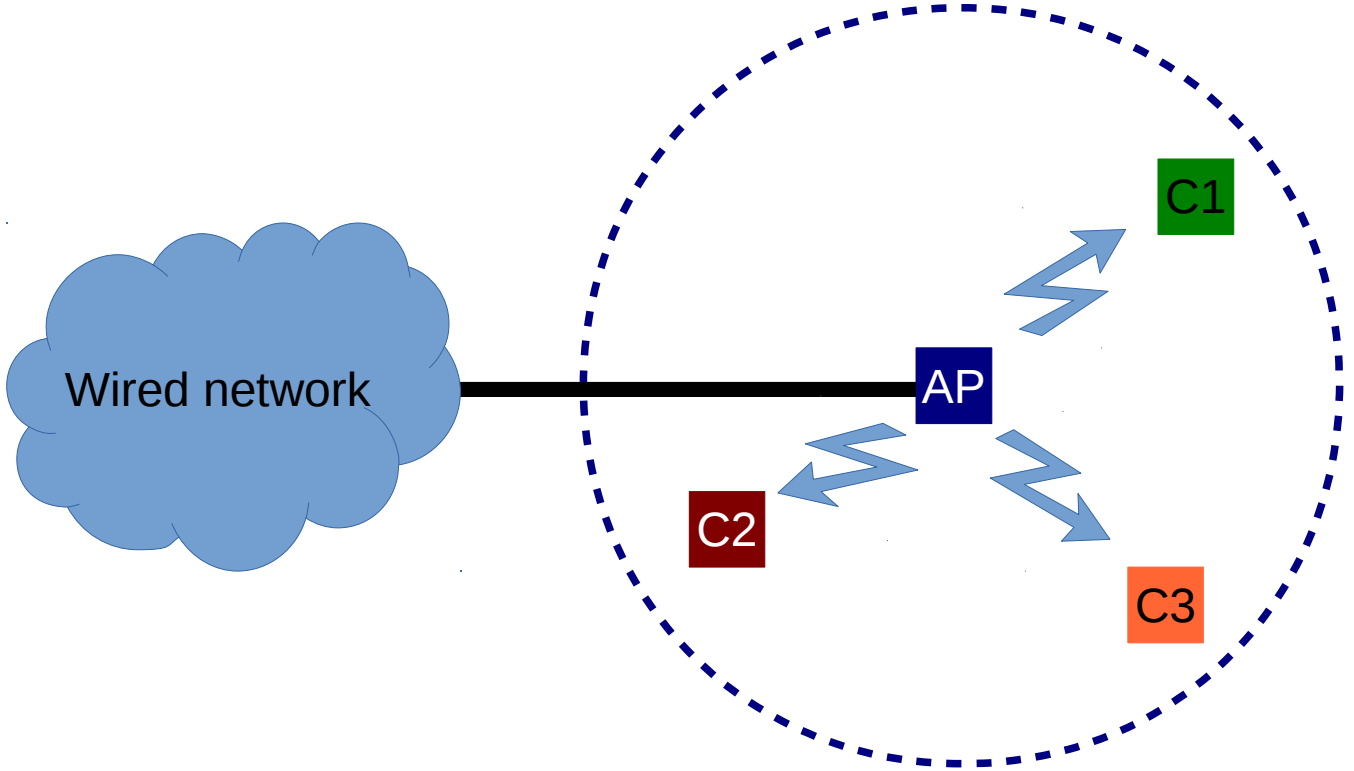
- Transmit signal at center frequency *f*, with bandwidth *BW*
- Devices with receives tuned to frequency *f* will receive the signal (if it has strong enough power)
- “Strong enough power”: depends on transmit power, receiver characteristics, antennas, frequency, obstructions
- Assume maximum distance some signal can be transmitted is range

Wireless LANs: Broadcast Radio

- Everyone within range of transmitter receives the signal
- If two (or more) signals received at same time, then neither can be understood
  - Interference, a “collision” occurs
- IEEE 802.11 MAC protocol aims to ensure only one device transmits at a time
  - Good: No (or few) collisions
  - Bad: Each device must wait for other devices before it can send
    - Shared medium: divide the data rate by number of devices wanting to share

IEEE 802.11 Wireless LANs

- Access Point (AP): acts as a bridge between wireless segment (WiFi) and wired segment (Ethernet)
- Client: wireless communications to AP



IEEE 802.11 Wireless LANs

- Physical (PHY) Layer:
  - Defines how to send wireless signals between devices
  - Data rate, frequency, bandwidth, power, modulation, ...
  - Different standards: 802.11a, 802.11b, 802.11g, ...
- Medium Access Control (MAC) Layer:
  - Defines how to efficiently send data between devices while sharing the medium
  - Common across different PHY standards

Wireless LAN PHY Characteristics

TABLE I

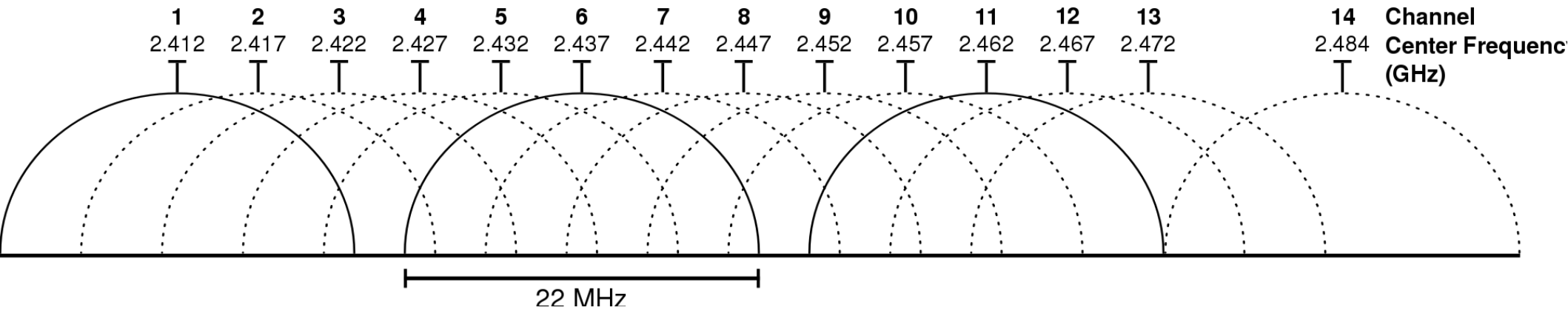
THE EVOLUTION OF THE 802.11 STANDARDS

Protocol	Year Introduced	Maximum Data Transfer Speed	Frequency	Highest Order Modulation	Channel Bandwidth	Antenna Configurations
802.11a	1999	54 Mbps	5 GHz	64 QAM	20 MHz	1×1 SISO
802.11b	1999	11 Mbps	2.4 GHz	11 CCK	20 MHz	1×1 SISO
802.11g	2003	54 Mbps	2.4 GHz	64 QAM	20 MHz	1×1 SISO
802.11n	2009	65 to 600 Mbps	2.4 or 5 GHz	64 QAM	20 and 40 MHz	Up to 4×4 MIMO
802.11ac	2012	78 Mbps to 3.2 Gbps	5 GHz	256 QAM	20, 40, 80 and 160 MHz	Up to 8×8 MIMO; MU-MIMO

www.microwavejournal.com

Channels in 2.4 GHz Band

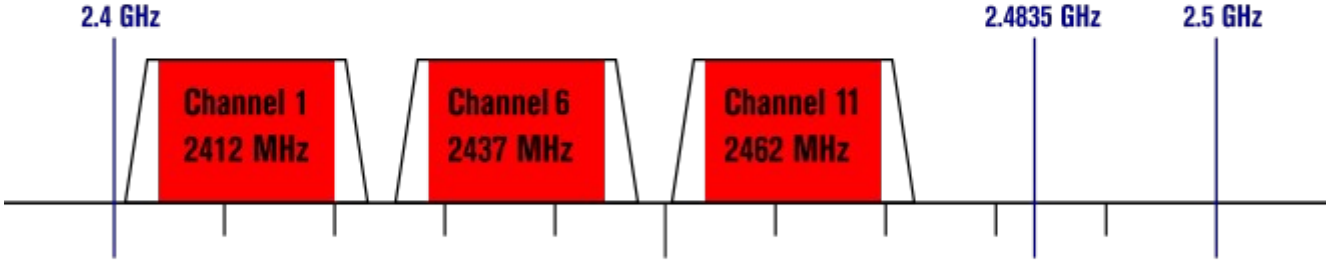
- 2.4 GHz ISM Band: 2.400 - 2.485 GHz
- Channel Bandwidth: ~20 MHz
- 11n, 11ac use larger bandwidth for higher data rate



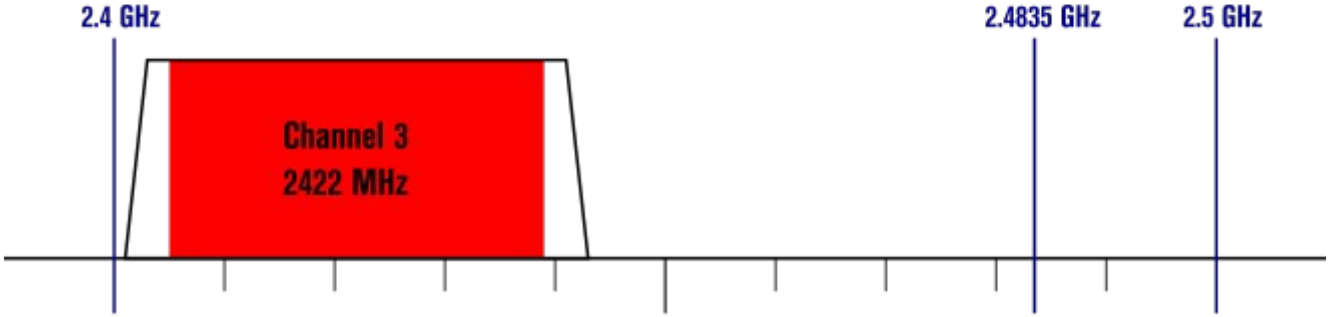
Non-Overlapping Channels for 2.4 GHz WLAN

802.11b (DSSS) channel width 22 MHz

802.11g/n (OFDM) 20 MHz ch. width – 16.25 MHz used by sub-carriers



802.11n (OFDM) 40 MHz ch. width – 33.75 MHz used by sub-carriers



5 GHz band allows for more non-overlapping channels and has less interference

Wireless LANs: Key Points

- Data Rate
  - Speed at which data sent between 2 devices
  - Varies according to PHY and distance
- Throughput:
  - MAC Overheads, e.g. headers, ACKs: 20-40%
    - 54 Mb/s - 25% overhead = 4 Mb/s
  - Waiting for others: divide by number of users
    - 10 users associated with AP: 4 Mb/s per user

Wireless LANs: Key Points

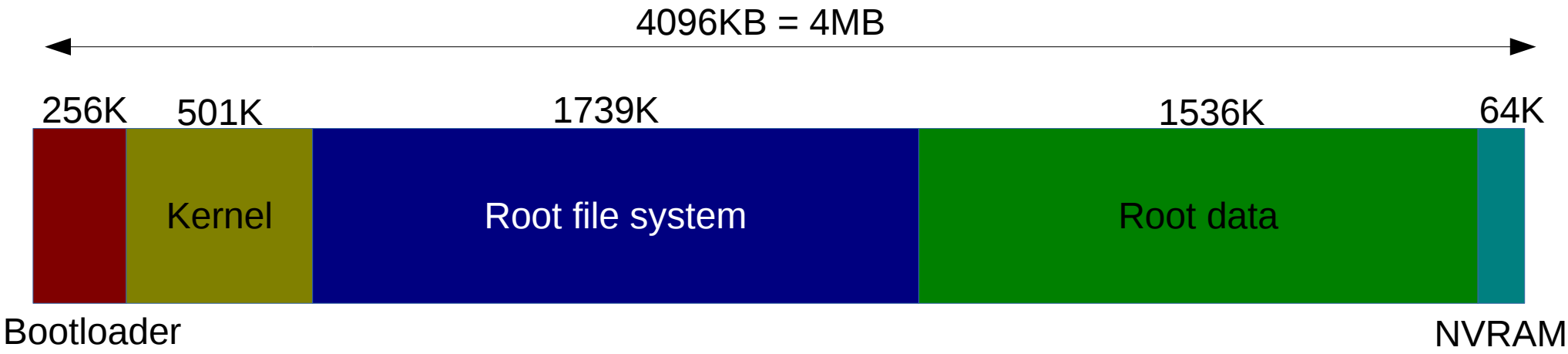
- Frequency Bands:
  - 2.4 GHz: supported by all devices; crowded
  - 5 GHz: not all APs, clients support; shorter range; less interference
- Channels:
  - Important when many nearby APs
  - 2 APs, 20 clients split amongst the APs
  - APs use same channel: 2 Mb/s per user
  - APs use non-overlapping channels: 4 Mb/s per user
  - 2.4 GHz band: channels 1, 6 and 11 (and 14)
  - 5 GHz band: 8 non-overlapping channels

Wireless LANs: Key Points

- Security:
  - None: no authentication or encryption
  - WEP: shared secret key, flawed
  - WPA: shared secret key (client and AP)
  - WPA Enterprise: authentication performed between client and separate server, encryption between client and AP

Wireless Router Firmware

WRT54GL Flash Memory



- Bootloader: loads firmware image into RAM, reads parameters from NVRAM
- Firmware image:
  - Linux Kernel
  - Root file system, e.g. permanent applications and libraries
  - Root data, e.g. config files, installed applications
- NVRAM: configurable parameters only used by bootloader

How to see this info? cat /proc/mtd and/or dmesg

Wireless Router Firmware - Normal Operation

- When router boots, bootloader loads firmware (kernel + root + data) into RAM and executes kernel
- Permanent changes can be written to “root data” on Flash
  - Edit configuration files
  - Install new applications
- Non-permanent changes can be written to temporary file system in RAM
  - Log files

Wireless Router Firmware - Flashing New Firmware

- Bootloader can be used to write a new firmware image
  - Replace kernel + root file system
- Two common options:
  - Existing firmware image has option to replace itself
  - Bootloader includes simple application (TFTP) to allow transfer of firmware image to device upon boot
- Next time the device boots, bootloader loads the new kernel + root file system

Wireless Router Firmware

- All wireless routers come with manufacturer provided firmware
  - Based on Linux and other embedded OS
- 3rd party firmware projects, usually Linux-based
  - OpenWRT: configurable with latest developments, free, open source software
  - DD-WRT: based on OpenWRT, ready-to-use, includes proprietary components
  - Tomato: ready-to-use, includes proprietary components
  - and others

OpenWRT

- Open source Linux distribution for embedded network devices
- Base packages provided as downloadable firmware image for many different devices
- Package manager (opkg) allows additional packages to be installed
- Different versions:
  - 14.07 Barrier Breaker
  - 12.09 Attitude Adjustment
  - 10.03 Backfire
  - 8.09 Kamikaze

Challenges with OpenWRT (and other 3rd party firmware)

- Only work for selected wireless routers, primarily those that use Linux-based manufacturer firmware
- Delay between release of new router and firmware image release
- Without open source drivers (or binary drivers provided by chip manufacturers) router features may not work
  - E.g. 802.11ac drivers are not yet common
- Performance with open source drivers may be worse (or better!) then manufacturer drivers

Mac OSX Command Line

Mac OSX File Sharing

- File Sharing
  - System Preferences → Sharing
  - File Sharing: On
- Connect to another iMac:
  - Finder → Shared → iMac_xx
- Public Shared Directory:
  - Yours: `/Users/student/Public`
  - Theirs: `/Volumes/student's Public Folder`
- Create 20 MB random file in Terminal:

```
$ dd if=/dev/urandom of=rand.bin bs=20m count=1
```

Mac OSX Commands

- Time a command on Terminal:

```
$ cd /Volumes/students' Public Folder
$ time cp rand.bin ~/
real  0m8.804s
...
```

- View interfaces (en0 Ethernet, en1 WiFi):

```
$ ifconfig en1
```

- Change MAC address:

```
$ sudo ifconfig en1 ether aa:bb:cc:11:22:33
```

Mac OSX Software Installs

- http://ict.siit.tu.ac.th/software/osx/
- XQuartz (needed by Wireshark)
- Wireshark

Mac OSX Packet Capture

- Link to airport: (only needed once)

```
sudo ln -s
/System/Library/PrivateFrameworks/Apple80211.fr
amework/Versions/Current/Resources/airport
/usr/local/bin/airport
```

- Search for active channels:

```
$ sudo airport en1 -s
```

- Start capture on channel 6:

```
$ sudo airport en1 sniff 6
```

(Ctrl-C to quit)

- View the .cap file with tcpdump or Wireshark

Example Wireless Networks

Setup the Wireless Router

- Explore OpenWRT web interface
  - View Stats: Status → Realtime Graphs → ...
  - Config Wifi: Network → Wifi → Edit → ...
  - Install software: System → Software →...
  - Edit firewall: Network → Firewall → ...

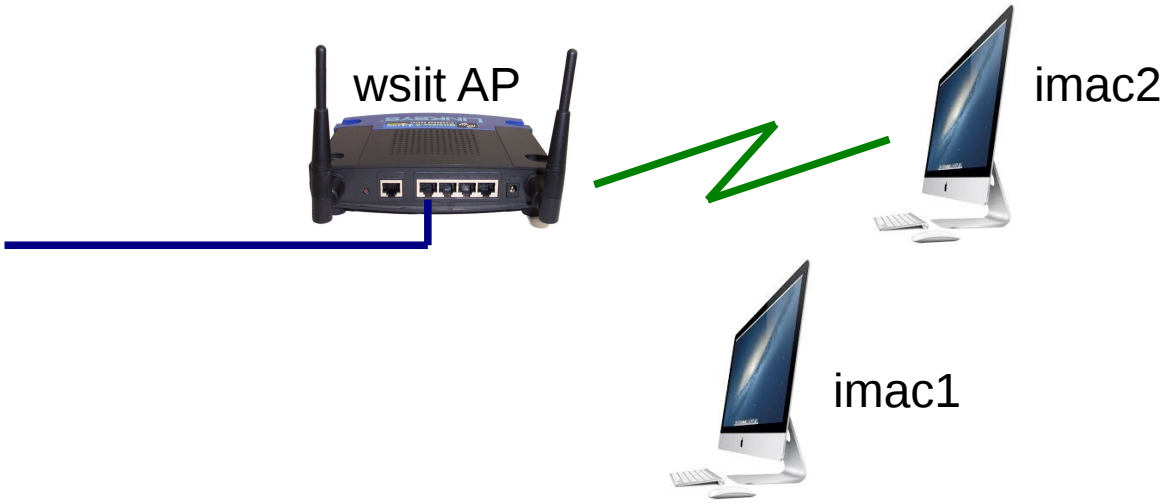
Measure Performance

- Compare delay across Ethernet vs WiFi
  - imac1: `ping 192.168.1.1`
  - imac2: `ping 192.168.1.1`
- Measure throughput across WiFi
  - Setup File Sharing on iMacs
  - imac1: Create 20MB random file in Public directory

    ```
    $ dd if=/dev/urandom of=rand.bin bs=20m count=1
    ```
  - imac2: Copy file from imac1 shared directory to home

    ```
    $ time cp /Volumes/students' Public Folder/rand.bin ~/
    ```

Intercept Other Peoples Data



- iMac1: Start packet capture
- iMac2: Access website (via SIIT internet)
- iMac1: Stop packet capture and view .cap file in Wireshark
  - Filter by 'http' and/or 'ip==10.10.x.y'

Use Wireless Router as Client

- In OpenWRT web interface:
  - Network → Wifi → Scan
    - Join Network
    - Default parameters (wwan, …)
    - Save and Apply
- Now use iMac to access SIIT internet via router

Setup a Rogue AP and Redirect HTTPS Login Web Pages to Unencrypted HTTP Logins

?