Candela
TECHNOLOGIES Network Testing and Emulation Solutions

Virtual STA and AP interfaces with ath5k, ath9k and ath10k

NOTE: This assumes you are using a recent kernel (3.9.0+) up-to-date wireless tools (hostap, iw, iwconfig, etc). Ath10k requires use of patched 3.14+ kernel and modified (CT) firmware.

The ath10k CT firmware images should now work on standard kernels, but multiple virtual stations may not work without the kernel driver patches. For normal ath10k station or AP use, just download the firmware, copy it into place, and reboot.

This documents how to use features in the latest kernels to implement implement virtual WiFi station and AP interfaces.

1. Recent upstream kernels version 3.0.0 or higher should work without modification, but you may wish to try out one of Candela's patched kernels.
   https://github.com/greearb?tab=repositories

2. Configure your kernel: Enable ath5k, ath9k, ath10k, and the debugging features for each. Enable the mac80211 debugging as well.

   ### Specific steps for Ubuntu 13.10 64-bit

   1. Install Ubuntu, let OS update packages, create a user with which to log in, etc.

   2. Install some tools:

   ```
   sudo apt-get install openssh-server git libqt4-dev g++
   sudo apt-get install build-essential kernel-package fakeroot libncurses5-dev
   ```

   3. Clone CT kernel and get it ready, and build. You may also see this page for some details:
      https://wiki.ubuntu.com/KernelTeam/GitKernelBuild

   ```
   mkdir git
   cd git
   git clone https://github.com/greearb/linux-ct-3.14.git linux-3.14.dev.y
   cd linux-3.14.dev.y
   cp configs/ct-x64.cfg .config
   make -j8 deb-pkg LOCALVERSION=-ct
   cd ..
   sudo dpkg -i linux-image-3.14.2-ct_3.14.2-ct-2_amd64.deb
   sudo dpkg -i linux-headers-3.14.2-ct_3.14.2-ct-2_amd64.deb
   sudo dpkg -i linux-image-3.14.2-ct-dbg_3.14.2-ct-2_amd64.deb
   sudo reboot
   ```

   When the system comes back up, double-check that `uname -a` shows the kernel version ends with '-ct', such as: 3.14.2-ct

3. For ath10k, you must also get a customised firmware image (henceforth, 'CT' firmware). See the Ath10k CT Firmware Page for downloads and information.

4. Fedora 19 (at least) comes with the tools needed to run virtual STA interfaces. You may have to compile hostapd yourself. We test with some modifications to hostapd, though the upstream code should work fine for most scenarios:
   `git clone https://github.com/greearb/hostap-ct.git hostap`
    or upstream project:
   `git clone https://w1.fi/srv/git/hostap.git`

5. Disable HW encryption, since that cannot work with multiple virtual interfaces. **For ath10k, this requires kernel driver changes ase well.**:
   `echo options ath5k nohwcrypt=1 >> /etc/modprobe.d/ath5k.conf`
   `echo options ath9k nohwcrypt=1 >> /etc/modprobe.d/ath9k.conf`
   `echo options ath10k_core nohwcrypt=1 >> /etc/modprobe.d/ath10k.conf`

6. Disable Network Manager. It usually gets in the way trying to manage the virtual interfaces.

7. Tell udev to keep away from your virtual interfaces. This can be more difficult to accomplish on more recent OSs (and/or versions of udev):

```
vi /lib/udev/rules.d/75-persistent-net-generator.rules

#KERNEL!="eth*|ath*|wlan*[0-9]|ra*|sta*|ctc*|lcs*|hsi*", GOTO="persistent_net_generator_end"
KERNEL!="eth*|ath*|ra*|ctc*|lcs*|hsi*", GOTO="persistent_net_generator_end"

# Optional, udev can be a pain, this may help make it less obtrusive.
# Skip virtual interfaces of all types.  This doesn't actually do
# anything for wifi interfaces, by the way.
SUBSYSTEM=="net", ACTION=="add", ATTR{iflink}!=ATTR{ifindex}, GOTO="persistent_net_generator_end"
```

8. Remove existing udev rules for ath5k/ath9k/ath10k devices:

```
# delete lines similar to this in 70-persistent-net.rules, if it exists.
# PCI device 0x168c:0x0013 (ath5k)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="00:0b:6b:83:5f:a6", ATTR{type}=="1", NAME=
```

9. **NOTE: The radio-dev-name is 'phy0' by default, but it will change if you reload the module or if you explicitly rename it.**
   To create/delete virtual interfaces:
   ```
   iw dev [radio-dev-name] interface add [virtual-sta-name] type station
   iw dev [radio-dev-name] interface add [virtual-ap-name] type __ap
   ip link set [interface-name] address [unique-mac-addr]
   ```
   To delete virtual interface:
   ```
   iw dev [dev-name] del
   ```

10. After the devices are created, they may be configured like any other wifi device. We have successfully tested more than 200 stations and up to 4 APs per radio/NIC using ath9k and our code trees. Ath10k is limited to 36 stations due to firmware limitations.

11. If you would like a pre-packaged testing solution, consider Candela Technologies' WiFi load-testing products. For more options, see: LANforge WiFi page and contact sales@candelatech.com

    - CT520: 32-station 802.11a/b/g/n ath9k system

    - CT523-600: 600-station 802.11a/b/g/n ath9k system

    - CT525-1200-6n: 1200-station 802.11a/b/g/n ath9k system

    - CT523-328-2ac-1n: 3-Radio 328-station 802.11a/b/g/n/AC system

    - CT525-792-3ac-3n: 6-radio /a/b/g/n/AC system.