Madwifi Repeaters with WPA2 and OPENVPN tunneling

With Thanks to Kel & Mike

INTRODUCTION

This document outlines the construction of a Non-WDS backbone repeater array using MadWifi, OpenVPN and Shorewall. Datastream integrity and security is managed using OpenVPN and WPA2. Shorewall manages netfilters and iptables to control routing and tunnels. An optional CPE AP is setup using WRAP3 as a station. This AP is secured by WPA2 and routes to the VPN on WRAP3.

This design places the openvpn server and client on the WRAPS themselves. One can effect about a 25% throughput improvement by not running the openvpn software on the WRAPS this way, but instead using other machines to provide the tunnel endpoints. That design is not explicitly documented here. As set up here, the OpenVPN servers reside on the WRAPS and create a secure wireless connection, with clear text packets on the wired LAN.

The example here uses MadWifi with a Debian distribution called Voyage on PC Engine's WRAP boards, but one can use any platform supported by Voyage, from WRAPS to PC's. You will need a development machine with a compact flash (CF) card writer and CF cards of at least 128 meg RAM in addition to the WRAP hardware and 4 Atheros radio miniPCI cards. You may want to use 512M cards, for the reasons detailed in the next paragraph.

The design shown here uses 512 meg CF cards with four 128M partitions. This provides a more robust installation while providing the means to reliably test the WRAPS from a remote location. The default installation lies in hda1, and the fallback is hda4, hda2 & 3 can be used to acquire and test new installations. Use **remountrw ;grub-reboot 1** to make a one time boot to partition hda2 instead of hda1. In the instance that the network fails to come up, the WRAP will reboot back to hda1 (see /etc/crontab for the chk_links.sh call). By logging in to each WRAP and invoking the **remountrw ;grub-reboot 1** all at the same time, the WRAPS will all try to boot from hda2. If it works and you have a stable net, the system will not reboot automatically. NB: the **next** time any WRAP in the array does, it will revert the entire array back to hda1. The entire system of WRAPs should recover in 5-14 minutes in the event of a failed test. If you do not want to trigger reboots when the links fail, comment out the /etc/crontab line calling chk_links.sh and/or edit the contents of that script to not ping a link. NB: the crontab interval changes with the # of WRAPs in the array- more WRAPS means longer intervals on the repeaters to accomodate all the reboots that get triggered in the array.

This example assumes the internet gateway is 192.168.4.1, and that the networks 192.168.100.0 (WRAP1-2), 192.168.101.0 (WRAP2 eth0), 192.168.110.0 (WRAP2-3), 192.168.111.0 (WRAP3 eth0), 192.168.112.0 (WRAP3 ath1) and 192.168.140.0 (tun0) are available and have no prior settings (like old routes) in your network system. You'll need to change the configuration settings to adapt to your own circumstances. You can certainly use subnets to reduce this demonstrative waste of address space.

WRAP1 is the front end (internet GW side) of the repeater array, connecting the wired internet gateway to the wireless repeater array thru an OpenVPN tunnel. You may choose to install the OpenVPN elsewhere, as it does take some CPU power. See **http://openvpn.net/howto.html** for more about OpenVPN. WRAP2 is the two radio repeater. If you need more repeaters, clone WRAP2 and arrange the crontab call to chk_links.sh, Channels, SSIDs, TxPower, networks, NATting and routing to fit. WRAP3 is the terminal end of the repeater backbone and OpenVPN tunnel, providing a wired interface out of the OpenVPN client to networks behind the tunnel. You can also opt to add a second radio (ath1), and provide a wireless AP as well.

If you do not implement the WRAP3's ath1 interface and it's WPA connection to an AP (and don't provide a wireless hub at the end of the repeater array, but instead only a wired hub on eth0), then comment out all references to the 192.168.112.0 net. You will have to edit the WRAP3 shorewall files and remove the wpa_supplicant call in **init**, and the a1 references in the **interface**, **rules**, **policy** & **zone** files.

The WRAPS should be fully assembled with short range test antennas before proceeding to the CF card setup.

Do not enable the **/etc/crontab** calls to **/usr/local/sbin/chk_links.sh** until you have Completely Finished the final installation. The chk_links.sh script will reboot

the WRAPS unless the adjacent networks are up and ping-able.

VOYAGE INSTALLATION

* I found it easiest to manage Voyage on a Debian PC with a similar kernel release (currently 2.6.15).

* Download Voyage: http://wiki.voyage.hk/dokuwiki/doku.php

* Create a directory under /usr/src called /usr/src/voyage. Create subdirectory called WRAP1, a subdirectory called WRAP2, a subdirectory called WRAP3, and a subdirectory called BASE.

* Install Voyage to /usr/src/voyage/BASE. Follow these instructions [from PREPARATIONS all the way thru to the end of CHROOTING] to install Voyage http://wiki.voyage.hk/dokuwiki/doku.php?id=temp_customization

* To automatically reboot on **kernel panic**, insert

```
kernel.panic=2
```

into the file **/etc/sysctl.conf**

* You'll need a working internet connection for the next steps before you can proceed. From within the chroot, ping a known host (ie: www.google.com) to prove the working connection.

* Next key in (and accept all related packages, agree with any defaults)
   apt-get update
   apt-get install -f
   apt-get upgrade
   apt-get install ethtool
   (optional) **apt-get install mc**
   (optional) **apt-get install iptraf**

* change to the /var/cache/apt/archives directory and then download shorewall 3.07 from: http://packages.debian.org/cgi-bin/download.pl?arch=all&file=pool%2Fmain%2Fs%2Fshorewall%2Fshorewall_3.0.7-1_all.deb&md5sum=9c0365454668c45876ecfe5114c4f0ae&arch=all&type=main

* Now key in:
  dpkg -i shorewall_3.0.7-1_all.deb
and accept all related packages.

* Use **mc** or the command line to create /bak and then backup the existing /etc/network directory and subdirectories to /bak/network .

* Edit the /etc/network/if* dirs and delete all lines except those containing "openvpn"

or "wireless-tools", this defeats the not-very-helpful-in-our-case scripts that normally control wpa_supplicant and madwifi.

* Create the file /ro/var/log/messages with a single blank line in it.

* Copy the file /var/lib/shorewall to /rw/tmp. Move the file /var/lib/shorewall to /ro/tmp, create a link from /rw/tmp/shorewall to /var/lib -this allows shorewall a writeable log file at start up.

* Copy all the files in /usr/share/doc/shorewall/default-config to /etc/shorewall

 * Add the following line to /etc/modules to enable loading the watchdog (wd1100) driver at startup:

    wd1100 sysctl_wd_graceful=0 sysctl_wd_timeout=60

* Key in **umount /proc** then **exit** and leave the chroot.

CLONE VOYAGE TO MAKE THE WRAPS

* Use **mc** or another means and copy the entire /usr/src/voyage/BASE directory to /usr/src/voyage/WRAP1, and again to /usr/src/voyage/WRAP2, and to /usr/src/voyage/WRAP3.

* WRAP1 is the front end of the repeater array, connecting the wired internet gateway to the wireless repeater array.

* WRAP2 is the two radio repeater. If you need more repeaters than one, clone WRAP2 and arrange the networks, NATting and routing to fit.

* WRAP3 is the terminal end of the repeater backbone, providing a wired interface to the internet, you can also opt to add a second radio, and provide a wireless AP as well (not yet documented here).

CUSTOMIZE THE WRAPS

* Use **mc** or your preferred editor to set the hostname on each of the WRAPs by editing /usr/src/voyage/WRAPx/ro/etc/hostname - do this for all three WRAPS

WRAP1

* Copy this text to WRAP1's **/etc/wpa_0.conf** file:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=root
ap_scan=1
#eapol_version=2

network={
        ssid="Wrap1ToWrap2"
        psk=fe871f00de4e0fea8feedbadbeeff00ddeadbeafbadf0E
        scan_ssid=1
        key_mgmt=WPA-PSK
        proto=RSN
        pairwise=TKIP
        group=TKIP
}
```

* Run wpa_passphrase and generate your own key. Replace the SSID & key in the file above. Use the same SSID & key in the WRAP2's **/etc/hostapd0.conf** file.

* Copy this text to WRAP1's **/etc/network/interfaces** file:

```
# Used by ifup(8) and ifdown(8). See the interfaces(5) manpage or
# /usr/share/doc/ifupdown/examples for more information.
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.4.10
        netmask 255.255.255.0
        network 192.168.4.0
        broadcast 192.168.4.255
        gateway 192.168.4.1
        up ethtool -s eth0 wol d

auto ath0
iface ath0 inet static
        address 192.168.100.10
        netmask 255.255.255.0
        network 192.168.100.0
        broadcast 192.168.100.255
#       pre-up wlanconfig ath0 create wlandev wifi0 wlanmode adhoc
        pre-upsysctl -w dev.wifi0.diversity=0
        pre-up sysctl -w dev.wifi0.txantenna=1
        pre-up sysctl -w dev.wifi0.rxantenna=1
        pre-up wlanconfig ath0 create wlandev wifi0 wlanmode ahdemo
# turn of 2nd antenna
        pre-up iwpriv ath0 mode 1
        pre-up iwpriv ath0 bgscan 0
        pre-up iwconfig ath0 channel 161

##      up iwconfig ath0 rate 54M auto

        pre-up iwconfig ath0 essid "Wrap1ToWrap2"
        up iwconfig ath0 txpower 5
        up iwpriv ath0 cwmin 0 1 1

#       up iwconfig ath0 enc off
```

 # set the ack timeouts for a long range connection (in meters) (mayking to courthouse 8km, to e911 4 km)
 # up athctrl -i wifi0 -d 8000
post-down wlanconfig ath0 destroy

* Edit the interfaces file (above) to set the channel, mode, essid and txpower values for ATH0.

* Copy these files to WRAP1's /etc/shorewall files of the same name:

/etc/shorewall/init

##
pkill wpa_supplicant
sleep 1
/usr/sbin/wpa_supplicant -B -D madwifi -i ath0 -c /etc/wpa_0.conf
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE

* NB: remove the 3 active lines above if you are not implementing WPA.

etc/shorewall/interfaces

##
#ZONE INTERFACE BROADCAST OPTIONS
a0 ath0 detect
#a1 ath1 detect
e0 eth0 detect
vpn tun+
#
#
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
Note that the wildcard ("+") on the **tun** interface: vpn zone applies to all **tun** interfaces - important if you want to support more than one openvpn client.

/etc/shorewall/ tunnels
##
#TYPE ZONE GATEWAY GATEWAY
 # ZONE
openvpnserver:1194 a0 192.168.140.5
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE

/etc/shorewall/masq
##
#INTERFACE SUBNET ADDRESS PROTO PORT(S) IPSEC
eth0 ath0
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE

/etc/shorewall/zones
##

```
#ZONE   TYPE          OPTIONS        IN                  OUT
#                                    OPTIONS             OPTIONS
# a0 is the ath0 lan, vpn is the VPN tunnel & nets behind the client, e0 is the etho lan
a0      ipv4
e0      ipv4
vpn     ipv4
fw      firewall
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

/etc/shorewall/policy

```
#############################################################################
#SOURCE        DEST          POLICY        LOG           LIMIT:BURST
#                            LEVEL

a0      vpn     REJECT
a0      e0      REJECT
a0      $FW     REJECT

vpn     all     ACCEPT
e0      all     ACCEPT
$FW     all     ACCEPT

all     all     REJECT   info
#LAST LINE -- DO NOT REMOVE
```

/etc/shorewall/rules

```
#############################################################################
#ACTION SOURCE         DEST          PROTO   DEST    SOURCE         ORIGINAL
RATE           USER/
#                                    PORT    PORT(S)        DEST           LIMIT          GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW

#ACCEPT e0      a0      udp     1194    -       -       -       -
#kill any ipp:631, netbios 137 138 comming in from eth0

DROP    a0      e0      udp     631     -       -       -       -
DROP    a0      $FW     udp     631     -       -       -       -
DROP    a0      vpn     udp     631     -       -       -       -

ACCEPT  a0      e0      udp     ntp     -       -       -       -
ACCEPT  a0      e0      tcp     ntp     -       -       -       -
ACCEPT  a0      e0      udp     53      -       -       -       -
ACCEPT  a0      e0      icmp    8       -       -       -       -
ACCEPT  a0      e0      udp     5001    -       -       -       -
ACCEPT  a0      e0      tcp     5001    -       -       -       -
ACCEPT  a0      e0      udp     1194,1026       -       -       -       -
ACCEPT  a0      e0      tcp     ssh     -       -       -       -

ACCEPT  a0      $FW     udp     1194,1026       -       -       -       -
ACCEPT  a0      $FW     tcp     ssh     -       -       -       -
ACCEPT  a0      $FW     icmp    8       -       -       -       -


#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

* Copy this text to WRAP1's **/usr/local/sbin/chk_links.sh** file:

```
#!/bin/sh
#################################################################
################
# Check for a ping reponse from any number of interfaces.
# Respond to 100% packet loss with a reboot
#
# Use cron to run this script- set the run interval to be at least 2x
# the reboot time/latency/delay of the slowest (to reboot) link.
#
#################################################################
################
 ping -c 1 192.168.4.1 |grep "100% packet" >/tmp/test_
 ping -c 1 192.168.100.20 |grep "100% packet" >>/tmp/test_
 if [ -s /tmp/test_ ] ; then
   remountrw
   cp /tmp/test_ /ro/var/log/.
   echo " chk_links forced reboot. \n" > /ro/var/log/chk_links.log
   date >> /ro/var/log/chk_links.log
    ping -c 1 192.168.4.1  >/ro/var/log/chk_links.log
   ping -c 1 192.168.100.20  >>/ro/var/log/chk_links.log
    fastreboot
 fi
 exit 0
```

* To reboot WRAP1 when the adjacent networks are down, add this line to **/etc/crontab** <u>but don't yet remove the # at the left of the line</u>. Do that **LAST**, after all other steps and the networks are all up and running. Otherwise, the WRAPS will reboot themselves every few minutes. Cron runs the wireless link check from WRAP1 to WRAP2 every 5 minutes.

```
#*/5 *   * * *   root   test -x /usr/sbin/anacron || /usr/local/sbin/chk_links.sh
```

* To reset the system clock daily on WRAP1 to an NTP date server add this line to **/etc/crontab**

```
3  1  * * *      root     test -x /usr/sbin/anacron || ntpdate -b -s pool.ntp.org
```

NB: the second term above should be the same hour as the default boot time. It may vary by WRAP. It takes about 2 minutes to boot and associate, so getting the day's time fix a minute later is good.

WRAP2

* Copy this text to WRAP2's **/etc/hostapd0.conf** file:

```
##### hostapd0 configuration file
##############################################
# Empty lines and lines starting with # are ignored
ssid="Wrap1ToWrap2"
wpa_psk=fe871f00de4e0fea8feedbadbeeff00ddeadbeafbadf0E
```

```
interface=ath0
driver=madwifi
logger_syslog=-1
logger_syslog_level=-1
logger_stdout=-1
logger_stdout_level=-1
debug=2
dump_file=/tmp/hostapd.dump
eapol_key_index_workaround=0
eap_server=1
wpa=3
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP CCMP
```

* Copy this text to WRAP2's **/etc/hostapd1.conf** file:

```
##### hostapd1 configuration file
##############################################
# Empty lines and lines starting with # are ignored
ssid="Wrap2ToWrap3"
psk=fee0fea8feedbadbeeff00ddeadbeafbadf0E
interface=ath0
driver=madwifi
logger_syslog=-1
logger_syslog_level=-1
logger_stdout=-1
logger_stdout_level=-1
debug=2
dump_file=/tmp/hostapd.dump
ssid=
eapol_key_index_workaround=0
eap_server=1
wpa=3
wpa_psk=
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP CCMP
```

* Copy this text to WRAP2's **/etc/network/interfaces** file:

```
# Used by ifup(8) and ifdown(8). See the interfaces(5) manpage or
# /usr/share/doc/ifupdown/examples for more information.
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
      address 192.168.101.10
      netmask 255.255.255.0
      broadcast 192.168.101.255

auto ath0
iface ath0 inet static
       address 192.168.100.20
       netmask 255.255.255.0
       network 192.168.100.0
       broadcast 192.168.100.255
# turn of 2nd antenna
       up sysctl -w dev.wifi0.diversity=0
       up sysctl -w dev.wifi0.txantenna=1
```

```
        up sysctl -w dev.wifi0.rxantenna=1
         pre-up wlanconfig ath0 create wlandev wifi0 wlanmode adhoc
# Set it to A band
        up iwpriv ath0 mode 1
# turn off background scanning
        up iwpriv ath0 bgscan 0
        up iwconfig ath0 channel 161
        up iwconfig ath0 essid Wrap1ToWrap2
        up iwconfig ath0 txpower 5
#         up iwconfig ath0 enc off
#         up iwconfig ath0 rate auto
# set the ack timeouts for a long range connection  (in meters)
#        up athctrl -i wifi0 -d 8000
#         up nat.sh ath0 eth0 "191.168.4.0/24"


auto ath1
iface ath1 inet static
        address 192.168.110.10
        netmask 255.255.255.0
        network 192.168.110.0
        broadcast 192.168.110.255
# turn of 2nd antenna
        up sysctl -w dev.wifi1.diversity=0
        up sysctl -w dev.wifi1.txantenna=1
        up sysctl -w dev.wifi1.rxantenna=1
         pre-up wlanconfig ath1 create wlandev wifi1 wlanmode adhoc
# Set it to A band
        up iwpriv ath1 mode 1
# turn off background scanning
        up iwpriv ath1 bgscan 0
        up iwconfig ath1 channel 52
        up iwconfig ath1 essid Wrap2ToWrap3
        up iwconfig ath1 txpower 5
#         up iwconfig ath0 enc off
#         up iwconfig ath0 rate auto
        up route add default gw 192.168.100.10
# set the ack timeouts for a long range connection  (in meters)
#        up athctrl -i wifi0 -d 8000
```

* Edit the WRAP2 /etc/network/interfaces file (above) to set the channel, mode and txpower values for ATH0. Use the same channel, mode and essid as the WRAP1 interfaces file. Be sure that you have the ATH0 radio's antenna correctly wired so you can direct it towards WRAP1 when you do the final installation.

* Continue to edit the interfaces file to set the channel, mode and txpower values for ATH1. Use a different channel and essid from the above. Be sure that you have the ATH1 radio's antenna correctly wired.

* Copy these files to WRAP2's /etc/shorewall files of the same name:

/etc/shorewall/init

```
############################################################################
#############################
pkill hostapd
```

sleep 1
/usr/local/bin/hostapd -B /etc/hostapd1.conf /etc/hostapd0.conf
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
#
 # Shorewall version 3.0 - Init File
#

* NB: remove the line hostapd line above if you are not implementing WPA.

/etc/shorewall/masq

```
#######################################################################
#INTERFACE              SUBNET          ADDRESS         PROTO   PORT(S) IPSEC
ath0    ath1
ath0    eth0
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

/etc/shorewall/zones

```
#######################################################################
#ZONE   TYPE            OPTIONS         IN                      OUT
#                               OPTIONS                 OPTIONS
# a0 is the gw, a1 is the  lan, e0 is the etho lan
a0      ipv4
a1      ipv4
e0      ipv4

fw      firewall
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

/etc/shorewall/policy

```
#######################################################################
#SOURCE         DEST            POLICY          LOG             LIMIT:BURST
#                                       LEVEL
a1      e0      ACCEPT
a1      fw      ACCEPT
a1      a0      ACCEPT
a0      e0      ACCEPT
a0      fw      ACCEPT
a0      a1      ACCEPT
e0      a0      ACCEPT
e0      fw      ACCEPT
e0      a1      ACCEPT
fw      e0      ACCEPT
fw      a0      ACCEPT
fw      a1      ACCEPT
all     all     ACCEPT
#LAST LINE -- DO NOT REMOVE
```

/etc/shorewall/started

```
#######################################################################
route add default gw 192.168.100.10
ntpdate -b -s pool.ntp.org
```

```
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
#
# Shorewall version 3.0 - Started File
#
```

* Copy this text to WRAP2's **/usr/local/sbin/chk_links.sh** file:

```
#!/bin/sh
############################################################################
###############
# Check for a ping reponse from any number of interfaces.
# Respond to 100% packet loss with a reboot
#
# Use cron to run this script- set the run interval to be at least 2x
# the reboot time/latency/delay of the slowest (to reboot) link.
#
############################################################################
###############
 ping -c 1 192.168.100.10 |grep "100% packet" >/tmp/test_
 ping -c 1 192.168.110.20 |grep "100% packet" >>/tmp/test_
 if [ -s /tmp/test_ ] ; then
   remountrw
   cp /tmp/test_ /ro/var/log/.
   echo " chk_links forced reboot. \n" > /ro/var/log/chk_links.log
   date >> /ro/var/log/chk_links.log
   ping -c 1 192.168.100.10 >/ro/var/log/chk_links.log
   ping -c 1 192.168.110.20  >>/ro/var/log/chk_links.log
    fastreboot
 fi
 exit 0
```

* To reboot WRAP2 when the adjacent networks are down, add this line to **/etc/crontab** but don't yet remove the # at the left of the line. Do that **LAST**, after all other steps and the networks are all up and running. Otherwise, the WRAPS will reboot themselves every few minutes. Cron runs the WRAP2 check every 8 minutes, (the sum of boot delays, plus a bit of time to actually connect to the box). Caution if this number falls below roughly 2*#WRAPs+2, the WRAPS can fall into a loop where a reboot on a WRAP brings down adjacent WRAPs. The endpoint WRAPs can reboot on a shorter interval. Station WPA re-association is the usual culprit (so far)

```
#*/8 *   * * *   root   test -x /usr/sbin/anacron || /usr/local/sbin/chk_links.sh
```

* To reset the system clock on WRAP2 to an NTP date server add this line to **/etc/crontab**

```
3  0  * * *      root     test -x /usr/sbin/anacron || ntpdate -b -s pool.ntp.org
```

NB: the second term above should be the same hour as the default boot time. It may vary by WRAP. It takes about 2 minutes to boot and associate, so getting the day's time fix a minute later is good.

WRAP3

* Copy this text to WRAP3's **/etc/wpa_0.conf** file:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=root
ap_scan=1
#eapol_version=2

network={
        ssid="Wrap2ToWrap3"
        psk=fee0fea8feedbadbeeff00ddeadbeafbadf0E
        scan_ssid=1
        key_mgmt=WPA-PSK
        proto=RSN
        pairwise=TKIP
        group=TKIP
}
```

* Copy this text to WRAP3's **/etc/wpa_1.conf** file:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=root
ap_scan=1
#eapol_version=2

network={
        ssid="Wrap3ToAP"
        psk=feedbadbeeff00ddeadbeafbadaaaaa111111eeeeee
        scan_ssid=1
        key_mgmt=WPA-PSK
        proto=RSN
        pairwise=TKIP
        group=TKIP
}
```

* Run wpa_passphrase and generate your own keys. Replace the SSIDs & keys in both files above. Use the SSID & key from **/etc/wpa_0.conf** in the WRAP2's **/etc/hostapd1.conf** file.

* Copy this text to WRAP3's **/etc/network/interfaces** file:

```
# Used by ifup(8) and ifdown(8). See the interfaces(5) manpage or
# /usr/share/doc/ifupdown/examples for more information.
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.111.10
        netmask 255.255.255.0
        network 192.168.111.0
        broadcast 192.168.111.255
        up ethtool -s eth0 wol d
# if ath1 happens it's 192.168.112.10       & needs to be firewalled from eth0

auto ath0
iface ath0 inet static
        address 192.168.110.20
        netmask 255.255.255.0
        network 192.168.110.0
        broadcast 192.168.110.255
        gateway 192.168.110.10
```

```
        pre-up sysctl -w dev.wifi0.diversity=0
        pre-up sysctl -w dev.wifi0.txantenna=1
        pre-up sysctl -w dev.wifi0.rxantenna=1
#       pre-up wlanconfig ath0 create wlandev wifi0 wlanmode adhoc
       pre-up wlanconfig ath0 create wlandev wifi0 wlanmode ahdemo
# turn of 2nd antenna
        pre-up iwpriv ath0 mode 1
        pre-up iwconfig ath0 channel 52
        pre-up iwpriv ath0 bgscan 0
##      pre-up iwconfig ath0 rate 54M auto

        pre-up iwconfig ath0 essid "Wrap2ToWrap3"
        up iwconfig ath0 txpower 5
#cwmin
        up iwpriv ath0 cwmin 0 1 1

        post-down wlanconfig ath0 destroy
# set the ack timeouts for a long range connection  (in meters) (mayking to courthouse 8km,
to e911 4 km)
#       up athctrl -i wifi0 -d 8000

auto ath1
iface ath1 inet static
       address 192.168.112.10
       netmask 255.255.255.0
       network 192.168.112.0
       broadcast 192.168.112.255
##       gateway 192.168.110.10
        pre-up sysctl -w dev.wifi1.diversity=0
        pre-up sysctl -w dev.wifi1.txantenna=1
        pre-up sysctl -w dev.wifi1.rxantenna=1
       pre-up wlanconfig ath1 create wlandev wifi1 wlanmode sta
## turn of 2nd antenna
        pre-up iwpriv ath1 mode 3
        pre-up iwconfig ath1 channel 1
        pre-up iwpriv ath1 bgscan 0
        pre-up iwconfig ath1 essid "YARD"
        up iwconfig ath1 txpower 16
##        up route add default gw 192.168.110.10
        post-down wlanconfig ath1 destroy
```

* Edit the interfaces file to set the channel, mode and txpower values for ATH0. Use the same channel, mode and essid as ATH1 above. Be sure that you have the WRAP3's ATH0 radio antenna correctly wired.

* Copy these files to WRAP3's /etc/shorewall files of the same name:

/etc/shorewall/init

```
/#############################################################
#############################
pkill wpa_supplicant
sleep 1
/usr/sbin/wpa_supplicant -B -D madwifi -i ath0 -c /etc/wpa_0.conf  -N -D
madwifi - i ath1 -c /etc/wpa_1.conf
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

* NB: remove the **-N -D madwifi - i ath1 -c /etc/wpa_1.conf from the** line above if

you are not implementing the WRAP3-ath1 Access Point and WPA.

/etc/shorewall/tunnels

```
#############################################################################
#TYPE                ZONE    GATEWAY         GATEWAY
openvpnclient:1194      a0          192.168.140.2
```

/etc/shorewall/zones

```
#############################################################################
#ZONE   TYPE          OPTIONS         IN                  OUT
#                                  OPTIONS             OPTIONS
# a0 is the ath0 lan, a1 is the ath1 lan, e0 is the etho lan
a0      ipv4
a1      ipv4
e0      ipv4
vpn     ipv4
fw      firewall
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

/etc/shorewall/interfaces

```
#############################################################################
#ZONE   INTERFACE       BROADCAST       OPTIONS
a0      ath0    detect
a1     ath1    detect
e0      eth0    detect
vpn     tun+     -      routeback
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Note that the wildcard ("+") on the **tun** interface: vpn zone applies to all **tun** interfaces - important if you want to support more than one openvpn client.

/etc/shorewall/policy

```
#############################################################################
#SOURCE         DEST          POLICY         LOG           LIMIT:BURST
#                                            LEVEL
e0      vpn     ACCEPT
e0      a0      ACCEPT
e0      a1      REJECT
e0      $FW     ACCEPT
e0      all     REJECT

a0      e0      REJECT
a0      a1      REJECT
a0      vpn     ACCEPT
a0      $FW     ACCEPT
a0      all     REJECT

a1      vpn     ACCEPT
a1      all     REJECT

#$FW    e0      ACCEPT
#$FW    a0      ACCEPT
#$FW    vpn     ACCEPT

$FW     all     ACCEPT
```

```
vpn     all     ACCEPT
all     all     REJECT
#LAST LINE -- DO NOT REMOVE
```

/etc/shorewall/rules

```
###############################################################################################
#ACTION SOURCE          DEST            PROTO   DEST    SOURCE          ORIGINAL
RATE            USER/
#                                       PORT    PORT(S)         DEST            LIMIT           GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW

# nail any IPP from LAN to FW or WLAN
DROP   e0       $FW     udp     631     -       -       -       -

ACCEPT a1   $FW   udp   137   -   -   -   -
#ACCEPT e0      a0      udp     1194    -       -       -       -
ACCEPT  e0      vpn     tcp     53      -       -       -       -
ACCEPT  e0      vpn     udp     53      -       -       -       -
ACCEPT  vpn     e0      tcp     53      -       -       -       -
ACCEPT  vpn     e0      tcp     53      -       -       -       -

ACCEPT  e0      vpn     icmp    8       -       -       -       -
ACCEPT  e0      vpn     icmp    8       -       -       -       -
ACCEPT  vpn     e0      icmp    8       -       -       -       -
ACCEPT  vpn     e0      icmp    8       -       -       -       -

ACCEPT  e0      vpn     tcp     ssh     -       -       -       -
ACCEPT  e0      vpn     udp     ssh     -       -       -       -
ACCEPT  vpn     e0      tcp     ssh     -       -       -       -
ACCEPT  vpn     e0      tcp     ssh     -       -       -       -

ACCEPT  e0      vpn     tcp     irc     -
ACCEPT  e0      vpn     udp     irc     -
ACCEPT  vpn     e0      tcp     irc     -
ACCEPT  vpn     e0      tcp     irc     -

ACCEPT  $FW     vpn     tcp     nntp    -       -       -       -
ACCEPT  $FW     vpn     tcp     imap    -       -       -       -
ACCEPT  $FW     a0      tcp     nntp    -       -       -       -
ACCEPT  $FW     a0      tcp     imap    -       -       -       -

ACCEPT  $FW     e0      tcp     ssh     -
ACCEPT  $FW     a0      tcp     ssh     -


#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

* Copy this text to WRAP3's **/usr/local/sbin/chk_links.sh** file:

```
#!/bin/sh
#############################################################################
###############
# Check for a ping reponse from any number of interfaces.
# Respond to 100% packet loss with a reboot
#
```

```
# Use cron to run this script- set the run interval to be at least 2x
# the reboot time/latency/delay of the slowest (to reboot) link.
#
#################################################################
###############
 ping -c 1 192.168.110.10 |grep "100% packet" >/tmp/test_
# if you want the WRAP to reboot when the eth0 connected firewall is down,
# uncomment the next line and set the correct IP.
  #ping -c 1 192.168.111.1 |grep "100% packet" >>/tmp/test_
 if [ -s /tmp/test_ ] ; then
   remountrw
   cp /tmp/test_ /ro/var/log/.
   echo " chk_links forced reboot. \n" > /ro/var/log/chk_links.log
   date >> /ro/var/log/chk_links.log
    ping -c 1 192.168.110.10  >>/ro/var/log/chk_links.log
    #ping -c 1 192.168.111.1 >>/ro/var/log/chk_links.log
    fastreboot
 fi
 exit 0
```

* To reboot WRAP3 when the adjacent networks are down, add this line to **/etc/crontab** but don't yet remove the # at the left of the line. Do that **LAST**, after all other steps and the networks are all up and running. Otherwise, the WRAPS will reboot themselves every few minutes. Cron runs the check every 5 minutes.
#*/5 * * * * root test -x /usr/sbin/anacron || /usr/local/sbin/chk_links.sh

* To reset the system clock on WRAP3 to an NTP date server add this line to **/etc/crontab**
3 1 * * * root test -x /usr/sbin/anacron || ntpdate -b -s pool.ntp.org

NB: the second term above should be the same hour as the default boot time. It may vary by WRAP. It takes about 2 minutes to boot and associate, so getting the day's time fix a minute later is good.

FORMAT AND PREP THE CF CARDS

* Create a mount point for the CF cards, **/mnt/cf** (mkdir /mnt/cf).

*Format the CF disks (assuming the Compact Flash device is on /dev/sda):
Key in **fdisk /dev/sda** and create a primary linux partition, 126 Megs or more, write and quit when done (the 126 is a litle shy of 128, which will make life easier if you choose to set up a 256 meg CF with two variants of Voyage).
Key in **mkfs.ext2 /dev/sda1**
Key in **tune2fs -c 0 /dev/sda1**
Repeat the above for the other two CF cards.

BURN A CF FOR EACH WRAP

* Start in the /usr/src/voyage/WRAP1 directory. Follow the **installation** instructions in the README file there. Hint: run **./voyage.update** Don't proceed past the installation section though. and select the current directory, the CF device (probably /dev/sda), the mount point you created above (/mnt/cf), the module configuration to install: 1 - WRAP , and the baud rate on the serial connection (9600).

* Change to the WRAP2 directory and repeat the above, and again from the WRAP3 directory. You'll end up with 3 CF cards, one for each WRAP.

* Now mount the Compact Flash cards in to the WRAPS

POWER UP & CUSTOMIZE WRAP1

* Lower the WRAP's baud rate to lighten up interrupt usage.
Connect a null-modem serial cable to the RS232 port. Attach the other end to a PC and use a telecom package, like minicom. Set the port parameters to 38400n81. Boot the WRAP, and while the WRAP is counting thru it's RAM, press "s". Once the RAM countdown is complete, you will see a small menu. Press "9" then "q" and say "Y"es to the save option. The WRAP will now boot with it's serial console set to 9600 baud.

* Connect WRAP1 Ethernet cable to the 192.168.4.0 network (have this online to the internet), and power up the WRAP.
* You can either connect a serial cable to the RS232 port, or **ssh** in to 192.168.4.10
* Log in as **root** with password **voyage**
* Key in **remountrw**
* Key in **passwd** and assign a new root password
* Key in **apt-get install openvpn** agree with all prompts and defaults.
* If you try to run OpenVPN & it fails because it cannot find openssh, key in **apt-get install openssl** (it may already be installed). Avoid this if you can, as it seems to stop the CF filesystem from remounting Read-Only

* Add the following lines to **/etc/init.d/openvpn** on the WRAP1, after the first line in the file. This enables a working certificate negotiation at startup and avoids buffer overruns:

 # force a date so openvpn can accept the certificates at startup
/bin/date 0101010105
 # force more free vm memory, to avoid "write UDPv4 No Buffer Space available"
echo 4096 >/proc/sys/vm/min_free_kbytes
#

* Copy **/usr/share/doc/packages/openvpn** to **/etc/openvpn**
* Edit the **/etc/openvpn/vars** file and set the KEY_COUNTRY, KEY_PROVINCE,

KEY_CITY, KEY_ORG, and KEY_EMAIL parameters. Don't leave any of these parameters blank. You'll have to rekey several of them, so make them simple.

* Now key in:

/bin/date 0101010100 (This sets the certificate date to Jan 01, 2000)
source ./vars
./clean-all
./build-ca
./build-dh
./build-key-server server_1
./build-key client_1

* If you anticipate needing more client certificates (running multiple clients), run build-key again as neccesary.
* You will have to (later) copy the key files to WRAP3 by hand or over a secure channel.
* To make the system most secure, after you generate the keys as above, remove the root key (**ca.key**) to a secure machine, preferably a standalone machine without a network connection. The root CA key (**ca.key**) need not be present on the OpenVPN server machine. It would be prudent to copy the entire /etc/openvpn directory, then destroy the original **ca.key** by overwriting it with a file of the same name.

This table (copied from the OpenVPN Howto v 2.0 [http://openvpn.net/howto.html]) describes the various generated keys and their attibutes

Filename	**Needed By**	**Purpose**	**Secret**
ca.crt	server + all clients	Root CA certificate	NO
ca.key	key signing machine only	Root CA key	YES
dh{n}.pem	server only	Diffie Hellman parameters	NO
server.crt	server only	Server Certificate	NO
server.key	server only	Server Key	YES
client1.crt	client1 only	Client1 Certificate	NO
client1.key	client1 only	Client1 Key	YES

client2.crt	client2 only	Client2 Certificate	NO
client2.key	client2 only	Client2 Key	YES
client3.crt	client3 only	Client3 Certificate	NO
client3.key	client3 only	Client3 Key	YES

* Use **scp** to copy the /etc/openvpn directory to an intermediate location (be sure to destroy or secure these files later). You will need to **scp** them back to WRAP3, and destroy the uneeded files (details below).

* Leave only these files in **/etc/openvpn/keys** on WRAP1:
ca.crt dh1924.pem index.txt.attr index.txt.old serial.old server_1.key dh1024.pem index.txt index.txt.attr.old serial server_1.crt
Erase all the rest (after you have made a secure backup of the entire dir on another machine- you will need to get the client certificates onto to WRAP3, so be sure to have them on hand)

* Copy the following to the file **/etc/openvpn/server.conf** on WRAP1

```
#log $server_log.txt

# Which local IP address should OpenVPN
# listen on? (optional)
# local a.b.c.d

port 1194
proto udp
dev tun

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).  Each client
# and the server must have their own cert and
# key file.  The server and all clients will
# use the same ca file.
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/server_1.crt
key /etc/openvpn/keys/server_1.key  # This file should be kept secret

dh /etc/openvpn/keys/dh1024.pem

server 192.168.140.0  255.255.255.0

ifconfig-pool-persist ipp.txt


# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
```

 # address pool (10.8.0.0/255.255.255.0)
 # back to the OpenVPN server.

push "route 192.168.4.0 255.255.255.0"
route 192.168.111.0 255.255.255.0
route 192.168.112.0 255.255.255.0

;push "route 192.168.20.0 255.255.255.0"

 # To assign specific IP addresses to specific
 # clients or if a connecting client has a private
 # subnet behind it that should also have VPN access,
 # use the subdirectory "ccd" for client-specific
 # configuration files (see man page for more info).

 # EXAMPLE: Suppose the client
 # having the certificate common name "client_1"
 # also has a net behind his connecting
 # machine, such as 192.168.111.0/255.255.255.0
 # First, uncomment out these lines:

client-config-dir ccd
route 192.168.111.0 255.255.255.0
route 192.168.112.0 255.255.255.0

 # Then create a file ccd/client_1 with this line:
 #   iroute 192.168.40.128 255.255.255.248
 # This will allow client_1's private subnet to
 # access the VPN. This example will only work
 # if you are routing, not bridging, i.e. you are
 # using "dev tun" and "server" directives.

 # EXAMPLE: Suppose you want to give
 # Thelonious a fixed VPN IP address of 10.9.0.1.
 # First uncomment out these lines:
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252
 # Then add this line to ccd/Thelonious:

 #   ifconfig-push 10.9.0.1 10.9.0.2

 # If enabled, this directive will configure
 # all clients to redirect their default
 # network gateway through the VPN
;push "redirect-gateway"

push "redirect-gateway def1"

 # Uncomment this directive to allow different
 # clients to be able to "see" each other.

##client-to-client
##push "route 192.168.111.0 255.255.255.0"

```
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120

# Select a cryptographic cipher.
cipher AES-128-CBC   # AES

# Enable compression on the VPN link.
comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
user nobody
group nogroup

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.  Use one
# or the other (but not both).
;log         openvpn.log
;log-append  openvpn.log

verb 3

# Silence repeating messages.  At most 5
# sequential messages of the same message
# category will be output to the log.
mute 5
```

* Now create the directory **/etc/openvpn/ccd**

* Create a text file named **/etc/openvpn/ccd/client_1** and insert the lines
iroute 192.168.111.0 255.255.255.0
iroute 192.168.112.0 255.255.255.0
into it and save the file.

* Key in **remountro**
* Power down WRAP1

POWER UP & CUSTOMIZE WRAP2

* Lower the WRAP's baud rate to lighten up interrupt usage.
Connect a null-modem serial cable to the RS232 port. Attach the other end to a PC and use a telecom package, like minicom. Set the port parameters to 38400n81. Boot the WRAP, and while the WRAP is counting thru it's RAM, press "s". Once the RAM countdown is complete, you will see a small menu. Press "9" then "q" and say "Y"es to the save option. The WRAP will now boot with it's serial console set to 9600 baud.

Power up WRAP2. It should require no additional configuration beyond changing the password. You can either connect via ethernet with **ssh** to 192.168.101.10
* Log in as **root** with password **voyage**
* Key in **remountrw**.
* Key in **passwd** and assign a new root password.
* Key in **remountro**.
* Power down WRAP2.

POWER UP & CUSTOMIZE WRAP3

* Lower the WRAP's baud rate to lighten up interrupt usage.
Connect a null-modem serial cable to the RS232 port. Attach the other end to a PC and use a telecom package, like minicom. Set the port parameters to 38400n81. Boot the WRAP, and while the WRAP is counting thru it's RAM, press "s". Once the RAM countdown is complete, you will see a small menu. Press "9" then "q" and say "Y"es to the save option. The WRAP will now boot with it's serial console set to 9600 baud.

* Temporarily connect WRAP3's Ethernet cable to the 192.168.4.0 network (have this online to the internet), and power up WRAP3.
* You can either connect a serial cable to the RS232 port, or **ssh** in to 192.168.111.10
* If you use ssh via the LAN: from an adjacent workstation (on the same hub as WRAP3), set that workstation's IP to 192.168.111.30/24 with the command: **ifconfig eth0 192.168.111.30 netmask 255.255.255.0**
* Log in as **root** with password **voyage**
* Key in **remountrw**
* Key in **passwd** and assign a new root password
* NB: in the next paragraph, you may need to change the IP addresses (.11 & .12) to not conflict with ones already on the 192.168.4.0 network.
* Key in **ifconfig eth0 192.168.4.11 netmask 255.255.255.0** to temporarily allow WRAP3 to the internet on the 192.168.4.0 network. If you are connected via ssh & the LAN, you will immediately lose your connection- in that case, reset the IP on the workstation with **ifconfig eth0 192.168.4.12 netmask 255.255.255.0** and re-ssh to WRAP3.

* You should be able to ping www.google.com now (for example).
* Key in **apt-get install openvpn** agree with all prompts and defaults.
* If you try to run OpenVPN & it fails because it cannot find openssh, key in **apt-get install openssl** (it may already be installed). Avoid this if you can, as it seems to stop the CF filesystem from remounting Read-Only

* Add the following lines to **/etc/init.d/openvpn** on WRAP3, after the first line in the file. This enables a working certificate negotiation at startup and avoids buffer overruns:

 # force a date so openvpn can accept the certificates at startup
/bin/date 0101010105
 # force more free vm memory, to avoid "write UDPv4 No Buffer Space available"
echo 4096 >/proc/sys/vm/min_free_kbytes
#

* Copy the following to the file **/etc/openvpn/client.conf** on WRAP3

```
# Specify that we are a client and that we
client
# Use the same setting as you are using on
# the server.
dev tun
proto udp

# The hostname/IP and port of the server.
remote 192.168.100.10 1194


# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind


# Downgrade privileges after initialization (non-Windows only)
user nobody
group nogroup

# Try to preserve some state across restarts.
persist-key
persist-tun

# Set this flag
# to silence duplicate packet warnings.
mute-replay-warnings

ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/client_1.crt
key /etc/openvpn/keys/client_1.key  # This file should be kept secret

# Verify server certificate by checking
# your server certificates have the nsCertType
```

```
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
;ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
cipher AES-128-CBC   # AES

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
 comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
mute 5
```

* Copy only these files from your secure key backup (made above) to **/etc/openvpn/keys** on WRAP3:
client_1.crt client_1.key index.txt.attr index.txt.old serial.old
ca.crt client_1.csr index.txt index.txt.attr.old serial server_1.csr

* Key in **remountro**
* Power down WRAP3

ROUTING

* On the internet gateway box (the firewall linking the dsl net to the system), aka 192.168.4.1, add the following lines to the **/etc/shorewall/init** file:

route add -net 192.168.110.0 netmask 255.255.255.0 gw 192.168.4.10
route add -net 192.168.101.0 netmask 255.255.255.0 gw 192.168.4.10
route add -net 192.168.111.0 netmask 255.255.255.0 gw 192.168.4.10
route add -net 192.168.112.0 netmask 255.255.255.0 gw 192.168.4.10
route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.4.10

NB: you may omit the second line if you want to defeat web access to WRAP3 (the routes beyond it will still be fine-this just locks out the WRAP3 iteself)

* On the internet gateway box (as above) append the following (no spaces between the comma separated fields) to the **/etc/shorewall/interfaces** file's line for the 192.168.4.0 ETHx (ie: eth0):

routeback,newnotsyn

* On the client network 192.168.111.0, set the gateway to 192.168.111.10

POWER UP ALL THE WRAPS

* Set all the WRAPS on a test bed, each at least 1m apart (2+ is better).
* Connect the LAN and power cables (usually POE- so only the POE's LAN cable connects to the WRAP, the PS and the LAN connects to the POE injector).
* Serial cable connections are handy about now, if there are any connectivity issues.

* On the WRAP1 box , key in **ip addr** and you should see something like the below:

```
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0d:b9:03:8a:f4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.4.10/24 brd 192.168.4.255 scope global eth0
    inet6 fe80::20d:b9ff:fe03:8af4/64 scope link
       valid_lft forever preferred_lft forever
3: wifi0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 199
    link/ieee802.11 00:0b:6b:4e:29:8c brd ff:ff:ff:ff:ff:ff
4: ath0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue
    link/ether 00:0b:6b:4e:29:8c brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.10/24 brd 192.168.100.255 scope global ath0
    inet6 fe80::20b:6bff:fe4e:298c/64 scope link
       valid_lft forever preferred_lft forever
```

* On the WRAP1 box , key in **route** and you should see something like the below:

```
Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

192.168.140.2 * 255.255.255.255 UH 0 0 0 tun0

192.168.100.0 * 255.255.255.0 U 0 0 0 ath0

192.168.4.0 * 255.255.255.0 U 0 0 0 eth0

192.168.111.0 192.168.140.2 255.255.255.0 UG 0 0 0 tun0

192.168.140.0 192.168.140.2 255.255.255.0 UG 0 0 0 tun0

default 192.168.4.1 0.0.0.0 UG 0 0 0 eth0
```

* On the WRAP1 box , key in **iwconfig ath0** and you should see something like the below:

```
ath0      IEEE 802.11a  ESSID:"Wrap1ToWrap2"
          Mode:Ad-Hoc  Frequency:5.805 GHz  Cell: 02:0B:6B:4E:29:8C
          Bit Rate:0 kb/s   Tx-Power=5 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

```
Link Quality=55/94  Signal level=-40 dBm  Noise level=-95 dBm
Rx invalid nwid:1  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

* On the WRAP1 box , key in **ifconfig** and you should see something like the below:

```
ath0      Link encap:Ethernet  HWaddr 00:0B:6B:4E:29:8C
          inet addr:192.168.100.10  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20b:6bff:fe4e:298c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10170 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9337 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1222308 (1.1 MiB)  TX bytes:917650 (896.1 KiB)

eth0      Link encap:Ethernet  HWaddr 00:0D:B9:03:8A:F4
          inet addr:192.168.4.10  Bcast:192.168.4.255  Mask:255.255.255.0
          inet6 addr: fe80::20d:b9ff:fe03:8af4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5387 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2728 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:573975 (560.5 KiB)  TX bytes:760120 (742.3 KiB)
          Interrupt:10 Base address:0x6000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.140.1  P-t-P:192.168.140.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:1601 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1947 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1160 (1.1 KiB)  TX bytes:0 (0.0 b)

wifi0     Link encap:UNSPEC  HWaddr 00-0B-6B-4E-29-8C-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:56530 errors:0 dropped:0 overruns:0 frame:6
          TX packets:9342 errors:2 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:199
          RX bytes:6220896 (5.9 MiB)  TX bytes:1123555 (1.0 MiB)
          Interrupt:12 Memory:c8940000-c8950000
```

* On the WRAP2 box , key in **ip addr** and you should see something like the below:

```
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
   inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
   link/ether 00:0d:b9:03:84:58 brd ff:ff:ff:ff:ff:ff
   inet 192.168.101.10/24 brd 192.168.101.255 scope global eth0
3: wifi0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 199
   link/ieee802.11 00:0b:6b:4e:29:94 brd ff:ff:ff:ff:ff:ff
```

```
4: wifi1: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 199
    link/ieee802.11 00:0b:6b:4e:29:f3 brd ff:ff:ff:ff:ff:ff
5: ath0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue
    link/ether 00:0b:6b:4e:29:94 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.20/24 brd 192.168.100.255 scope global ath0
    inet6 fe80::20b:6bff:fe4e:2994/64 scope link
       valid_lft forever preferred_lft forever
6: ath1: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue
    link/ether 00:0b:6b:4e:29:f3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.110.10/24 brd 192.168.110.255 scope global ath1
    inet6 fe80::20b:6bff:fe4e:29f3/64 scope link
       valid_lft forever preferred_lft forever
7: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
```

* On the WRAP2 box , key in **route** and you should see something like the below:

```
Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

192.168.100.0 * 255.255.255.0 U 0 0 0 ath0

192.168.101.0 * 255.255.255.0 U 0 0 0 eth0

192.168.110.0 * 255.255.255.0 U 0 0 0 ath1

default 192.168.100.10 0.0.0.0 UG 0 0 0 ath0
```

* On the WRAP2 box , key in **iwconfig** and you should see something like the below:

```
ath0      IEEE 802.11a  ESSID:"Wrap1ToWrap2"
          Mode:Ad-Hoc  Frequency:5.805 GHz  Cell: 02:0B:6B:4E:29:8C
          Bit Rate:0 kb/s   Tx-Power=5 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=41/94  Signal level=-54 dBm  Noise level=-95 dBm
          Rx invalid nwid:1  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

ath1      IEEE 802.11a  ESSID:"Wrap2ToWrap3"
          Mode:Ad-Hoc  Frequency:5.26 GHz  Cell: 02:0B:6B:4E:29:F3
          Bit Rate:0 kb/s   Tx-Power=5 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=51/94  Signal level=-44 dBm  Noise level=-95 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

* On the WRAP2 box , key in **ifconfig** and you should see something like the below:

```
ath0      Link encap:Ethernet  HWaddr 00:0B:6B:4E:29:94
          inet addr:192.168.100.20  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20b:6bff:fe4e:2994/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9543 errors:0 dropped:0 overruns:0 frame:0
```

```
          TX packets:10394 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:938351 (916.3 KiB)  TX bytes:1248508 (1.1 MiB)

ath1      Link encap:Ethernet  HWaddr 00:0B:6B:4E:29:F3
          inet addr:192.168.110.10  Bcast:192.168.110.255  Mask:255.255.255.0
          inet6 addr: fe80::20b:6bff:fe4e:29f3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9954 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8816 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1165069 (1.1 MiB)  TX bytes:872757 (852.3 KiB)

eth0      Link encap:Ethernet  HWaddr 00:0D:B9:03:84:58
          inet addr:192.168.101.10  Bcast:192.168.101.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:10 Base address:0x6000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:336 (336.0 b)  TX bytes:336 (336.0 b)

wifi0     Link encap:UNSPEC  HWaddr 00-0B-6B-4E-29-94-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:89736 errors:0 dropped:0 overruns:0 frame:66
          TX packets:10425 errors:3 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:199
          RX bytes:12774475 (12.1 MiB)  TX bytes:1478605 (1.4 MiB)
          Interrupt:12 Memory:c8940000-c8950000

wifi1     Link encap:UNSPEC  HWaddr 00-0B-6B-4E-29-F3-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:140904 errors:0 dropped:0 overruns:0 frame:22
          TX packets:8843 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:199
          RX bytes:19586194 (18.6 MiB)  TX bytes:1067879 (1.0 MiB)
          Interrupt:9 Memory:c8960000-c8970000
```

* On the WRAP3 box , key in **ip addr** and you should see something like the below:

```
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0d:b9:03:84:5c brd ff:ff:ff:ff:ff:ff
    inet 192.168.111.10/24 brd 192.168.111.255 scope global eth0
3: wifi0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 199
    link/ieee802.11 00:0b:6b:4d:77:47 brd ff:ff:ff:ff:ff:ff
4: wifi1: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 199
    link/ieee802.11 00:11:f5:7e:5d:96 brd ff:ff:ff:ff:ff:ff
5: ath0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue
```

```
    link/ether 00:0b:6b:4d:77:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.110.20/24 brd 192.168.110.255 scope global ath0
    inet6 fe80::20b:6bff:fe4d:7747/64 scope link
       valid_lft forever preferred_lft forever
6: ath1: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue
    link/ether 00:11:f5:7e:5d:96 brd ff:ff:ff:ff:ff:ff
    inet 192.168.112.10/24 brd 192.168.112.255 scope global ath1
    inet6 fe80::211:f5ff:fe7e:5d96/64 scope link
       valid_lft forever preferred_lft forever
7: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
8: tun0: <POINTOPOINT,MULTICAST,NOARP,UP> mtu 1500 qdisc pfifo_fast qlen 100
    link/[65534]
    inet 192.168.140.6 peer 192.168.140.5/32 scope global tun0
```

* On the WRAP3 box , key in **route** (once the tun0 device is up) and you should see something like the below:

```
Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

192.168.140.1 192.168.140.5 255.255.255.255 UGH 0 0 0 tun0

192.168.100.10 192.168.110.10 255.255.255.255 UGH 0 0 0 ath0

192.168.140.5 * 255.255.255.255 UH 0 0 0 tun0

192.168.4.0 192.168.140.5 255.255.255.0 UG 0 0 0 tun0

192.168.112.0 * 255.255.255.0 U 0 0 0 ath1

192.168.110.0 * 255.255.255.0 U 0 0 0 ath0

192.168.111.0 * 255.255.255.0 U 0 0 0 eth0

default 192.168.140.5 128.0.0.0 UG 0 0 0 tun0

128.0.0.0 192.168.140.5 128.0.0.0 UG 0 0 0 tun0

default 192.168.110.10 0.0.0.0 UG 0 0 0 ath0
```

* On the WRAP3 box , key in **iwconfig ath0** (once the tun0 device is up) and you should see something like the below:

```
ath0      IEEE 802.11a  ESSID:"Wrap2ToWrap3"
          Mode:Ad-Hoc  Frequency:5.26 GHz  Cell: Not-Associated
          Bit Rate:0 kb/s   Tx-Power=5 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=37/94  Signal level=-58 dBm  Noise level=-95 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

ath1      IEEE 802.11g  ESSID:"Wrap3ToAP"
```

```
Mode:Managed  Frequency:2.412 GHz  Access Point: 00:16:B6:DA:8D:1D
Bit Rate:54 Mb/s   Tx-Power=16 dBm   Sensitivity=0/3
Retry:off   RTS thr:off   Fragment thr:off
Encryption key:5721-A00E-1D77-05A3-3A08-59DB-AAE0-DB51   Security mode:restricted
Power Management:off
Link Quality=69/94  Signal level=-26 dBm  Noise level=-95 dBm
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

* On the WRAP3 box , key in **ifconfig** (once the tun0 device is up) and you should see something like the below:

```
ath0      Link encap:Ethernet  HWaddr 00:0B:6B:4D:77:47
          inet addr:192.168.110.20  Bcast:192.168.110.255  Mask:255.255.255.0
          inet6 addr: fe80::20b:6bff:fe4d:7747/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:294 errors:0 dropped:0 overruns:0 frame:0
          TX packets:249 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:147873 (144.4 KiB)  TX bytes:52109 (50.8 KiB)

ath1      Link encap:Ethernet  HWaddr 00:11:F5:7E:5D:96
          inet addr:192.168.112.10  Bcast:192.168.112.255  Mask:255.255.255.0
          inet6 addr: fe80::211:f5ff:fe7e:5d96/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:124 errors:0 dropped:0 overruns:0 frame:0
          TX packets:162 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24650 (24.0 KiB)  TX bytes:162260 (158.4 KiB)

eth0      Link encap:Ethernet  HWaddr 00:0D:B9:03:84:5C
          inet addr:192.168.111.10  Bcast:192.168.111.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:10 Base address:0x6000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.140.6  P-t-P:192.168.140.5  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:217 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:165602 (161.7 KiB)  TX bytes:29157 (28.4 KiB)

wifi0     Link encap:UNSPEC  HWaddr 00-0B-6B-4D-77-47-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:294 errors:0 dropped:0 overruns:0 frame:1
          TX packets:249 errors:1 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:199
```

```
          RX bytes:154341 (150.7 KiB)  TX bytes:57587 (56.2 KiB)
          Interrupt:12 Memory:c8940000-c8950000

wifi1     Link encap:UNSPEC  HWaddr 00-11-F5-7E-5D-96-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2059 errors:0 dropped:0 overruns:0 frame:239
          TX packets:476 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:199
          RX bytes:243199 (237.4 KiB)  TX bytes:184114 (179.7 KiB)
          Interrupt:9 Memory:c8960000-c8970000
```

* A client connected to WRAP3's eth0 on net 192.168.111.0 should be able to surf the internet. All traffic is encrypted and tunneled, with the attendant performance hit.

APPENDICES

Troubleshooting

  * If the WRAP2 drops out entirely, it may (but usually not) cause the WRAP3 tunnel to try to re-establish as TUN1 (not TUN0). Reboot (or restart the openvpn client) WRAP3 to fix.

 * If WRAP2 is down when WRAP3 boots, the VPN will fail & no net traffic will flow. Reboot WRAP3 after WRAP2 has come up.

 * Do not enable the **/etc/crontab** calls to **/usr/local/sbin/chk_links.sh** until you have Completely Finished the final installation. The chk_links.sh script will reboot the WRAPS unless the adjacent networks are up and ping-able.

Performance

 * Xfer rate with a direct eth0 link from Thinkpad T42 to WRAP1 (wired connection, not wireless):

```
 scp root@192.168.4.10:/test /dev/null
test                                                  100%   13MB 947.1KB/s   00:14
```

* Iperf rate thru entire repeater array with VPN tunnel link:

```
------------------------------------------------------------
Client connecting to 192.168.111.30, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.4.30 port 38900 connected with 192.168.111.30 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  7.05 MBytes  5.89 Mbits/sec
```

Sample Budgets, Hardware Vendors

Purchased Hardware: wifi

Vendor	Item		Total
http://www.fab-corp.com/product.php?productid=2874&cat=268&page=1$page&addedtocart=1$page&addedtocart=1	5GHz 0.6M 28/29dBi Dish Antenna + radomes (with an integrated N Female connector)	4	$642.30
http://www.fab-corp.com/product.php?productid=865&cat=261&page=1$page&addedtocart=1	Grounding Kit - Times Microwave LMR-400 Cables	4	96
http://www.wlanparts.com/product/SP6-230-BFM	Coaxial Surge Protectors DC to 6GHz Operation	4	134.39
http://www.fab-corp.com/product.php?productid=1484&cat=249&page=1$page&addedtocart=1	2 wall mounts and n-male to n-male lm400 cables	4	168.75
http://www.mini-box.com/s.nl;?categor	AC Adapter 18V-0.83A-15W /110/220V	4	54.73

y=19&it=A&id=383

www.netgate.com	wrap/case/poe/pigtails	3	1025.69	
pcmall.com	1000' cat5 plenum cable	1	125	
www.embeddedworks.com	RB4 & RB1	1	102.97	
www.embeddedworks.com	RB1	1	31.97	
www.wlanparts.com	CM9 radio, pigtails	1	77.39	
www.wlanparts.com	CM9 radio MPCI	2	102.33	
www.newegg.com	CF 128 MB	4	51.89	
				$2,733.41
		1	99.95	
		1	51.89	
		2	329.98	
		1	79.6	

FCC Regs

§15.407 General Technical Requirements. (a) Power limits: *** (2) For the 5.25-5.35 GHz and 5.47-5.725 GHz bands, the peak transmit power over the frequency bands of operation shall not exceed the lesser of 250 mW or 11 dBm + 10log B, where B is the 26 dB emission bandwidth in megahertz. In addition, the peak power spectral density shall not exceed 11 dBm in any 1 megahertz band. If transmitting antennas of directional gain greater than 6 dBi are used, both the peak transmit power and the peak power spectral density shall be reduced by the amount in dB that the directional gain of the antenna exceeds 6 dBi.

Proposed Changes to U-NII Rules 16. Technical requirements. Under the existing Part 15 U-NII rules, there are three different frequency sub-bands available to U-NII devices, each with its own set of technical requirements (e.g., transmit power and antenna gain), based on its sharing environment. 31 U-NII devices operating in the 5.150-5.250 GHz sub-band are restricted to indoor operations and a power limit of 200 mW e.i.r.p. in order to protect co-channel Mobile Satellite Service (MSS) feeder links. 32 Because of the relatively low power limit and indoor usage requirement, this sub-band is most suitable for U-NII devices providing communications links between devices separated by short distances indoors, such as between computing devices within a room or in adjoining rooms. **The 5.250-5.350 GHz sub-band may be used indoors and outdoors and is limited to 1 watt e.i.r.p.** This sub-band is shared with the Federal Government Radiolocation Service, Earth Exploration Satellite Service and Space Research Service. This U-NII sub-band is suitable for communications links both within and between buildings such as for campus-wide local area networks. **The 5.725-5.825 GHz sub-band may be used indoors and outdoors with power levels up to 4 watts e.i.r.p.** This U-NII sub-band is shared with Federal

Further, as noted below, we are proposing to permit a lower e.i.r.p. for U-NII devices operating in the 5.470-5.725 GHz band (i.e., 1 watt e.i.r.p.) than for the existing 5.725-5.825 GHz band (i.e., 4 watts e.i.r.p.). Therefore, we believe that U-NII devices can operate in 5.650-5.725 GHz band without causing interference. Finally, U-NII devices in this band would continue to operate under Part 15 of our rules and would be required to eliminate any harmful interference that may occur to the Amateur Radio service. We tentatively conclude that the proposals herein are adequate to protect the Amateur Radio service from interference. We seek comment on this tentative conclusion. 20. In addition to applying the existing technical requirements for the 5.250-5.350 GHz sub-band to the new 5.470-5.725 GHz band, to ensure protection to existing vital DoD radar operations, we are proposing that U-NII devices operating in both the existing 5.250-5.350 GHz sub-band and the new 5.470-5.725 GHz sub-band employ a listen-before-talk mechanism called dynamic frequency selection (DFS). DFS is an interference avoidance mechanism. Prior to the start of any transmissions, and through constant monitoring, the device (e.g., RLAN) equipped with such a mechanism monitors the radio environment for a radar’s presence. If the U-NII device determines that a radar is present, it either

Amateur, ISM, and other Part 15 devices and is suitable for communications links within and among buildings and over long distances through use of high-gain antennas.

enters a sleep mode if no channels are available. We propose that U-NII devices be required to continuously monitor their environment for the presence of radars both prior to and during operation.

[Title 47, Volume 1]
[Revised as of October 1, 2001]
From the U.S. Government Printing Office via GPO Access
[**CITE: 47CFR15.407**]
[Page 746-748]

TITLE 47--TELECOMMUNICATION

CHAPTER I--FEDERAL COMMUNICATIONS COMMISSION

PART 15--RADIO FREQUENCY DEVICES--Table of Contents

Subpart E--Unlicensed National Information Infrastructure Devices

Sec. 15.**407** General technical requirements.
(a) Power limits:
...
(2) For the band 5.25-5.35 GHz, the peak transmit power over the frequency band of operation shall not exceed the lesser of 250 mW or 11 dBm + 10logB, where B is the 26-dB emission bandwidth in MHz. In addition, the peak power spectral density shall not exceed 11 dBm in any 1-MHz band. If transmitting antennas of directional gain greater than 6 dBi are used, both the peak transmit power and the peak power spectral density shall be reduced by the amount in dB that the directional gain of the antenna exceeds 6 dBi.
(I think that means I can do 8-10dB on a 26-28 dB antenna)
(3) For the band 5.725-5.825 GHz...However, fixed point-to-point U-NII devices operating in this band may employ transmitting antennas with directional gain up to 23 dBi without any corresponding reduction in the transmitter peak output power or peak power spectral density. For fixed, point-to-point U-NII transmitters that employ a directional antenna gain greater than 23 dBi, a 1 dB reduction in peak transmitter power and peak power spectral density for each 1 dB of antenna gain in excess of 23 dBi would be required. Fixed, point-to-point operations exclude the use of point-to-multipoint systems, omni directional applications, and multiple collocated transmitters transmitting the same information. The operator of the U-NII device, or if the equipment is professionally installed, the installer, is responsible for ensuring that systems employing high gain directional antennas are used exclusively for fixed, point-to-point operations.

---

http://www.telexwireless.com/wireless/faq.nsf/cat!ReadForm&RestrictToCategory=FCC%20Part%2015

How much power can I legally transmit on a 23 dBi panel at **5.8 GHz**?

The **FCC** regulations for UNII-3 wideband digital fixed PtP transmitters allows a **maximum** 30 dBm (or 17 dBm + 10logB) output with directional antennas up to 23 dBi gain without any corresponding reduction in transmitter power. **Maximum EIRP** is 53 dBm (200 watts). Power is measured at the antenna connector, so subtract any cable loss between the amplifier and the antenna. Refer to the following table:

Power at antenna (dBm/Watts)	Antenna Gain (dBi)	**EIRP** (dBm)	**EIRP** (watts)
30 dBm (1 W)	6	36	4
30 dBm (1 W)	9	39	8
30 dBm (1 W)	12	42	16
30 dBm (1 W)	15	45	31
30 dBm (1 W)	18	48	62
30 dBm (1 W)	21	51	125
30 dBm (1 W)	23	53	200

---

http://www.connect802.com/tech_notes.htm

- **Maximum EIRP** for fixed, point-to-point (5.8GHz) links using an antenna with a minimum 6 dB gain:
  - **EIRP Maximum** = 4 watts (4000 mW, 36 dBm) where TPO Max = 30 dBm
- For antennas with greater than 6 dB of gain:
  - Reduce TPO from 1 watt by 1 dB for each 3 dB of additional antenna gain beyond 6 dB
- This allows E IRP to be greater than 36 dBm for antennas with greater than 6 dB gain.)

http://www.universitypark.org/hope/page10.html

A: **FCC** Part 15.407 for **5.3** GHz PtMP allows only 30 dBm (1 watt) **EIRP** in the **UNII-2** band. This is 24 dBm (250 mw) into a 6 dBi antenna. If you use a 10 dBi antenna, you must limit your transmitter (or amplifier) to 20 dBm (10 + 20 = 30 dBm). For a 15 dBi panel antenna, this allows a 15 dBm transmitter (or amplifier). Power is measured at the antenna connector, so subtract any cable loss between the amplifier

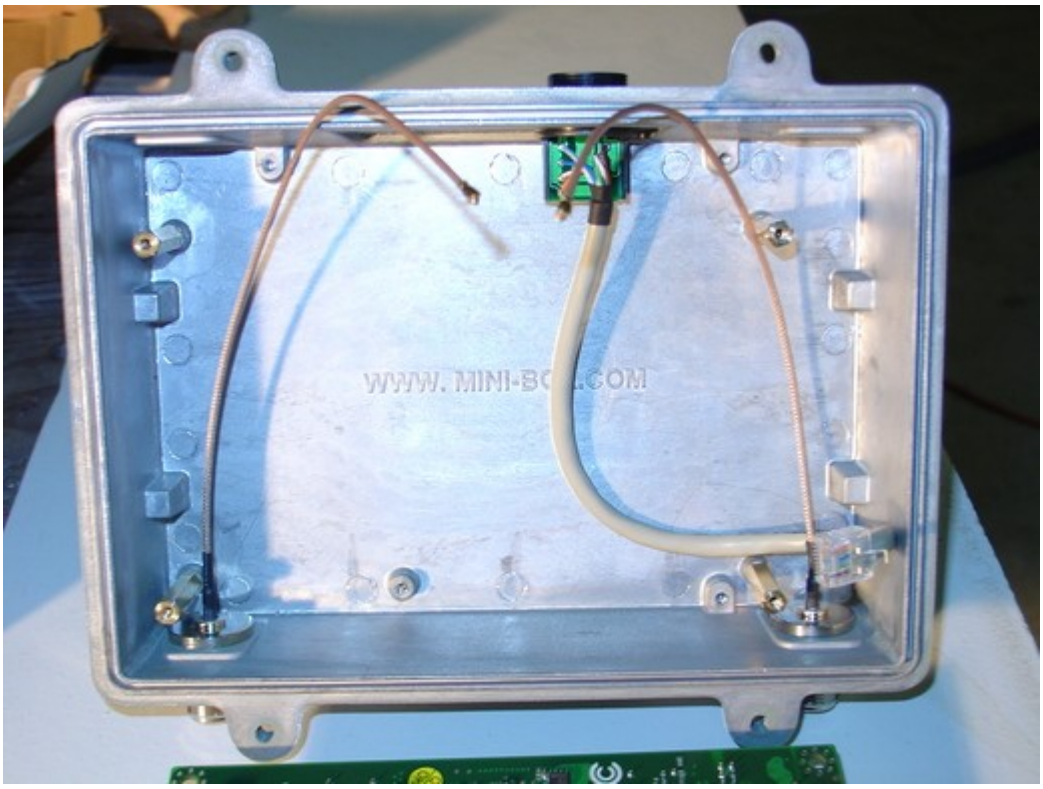
and the antenna. If you use a +17 dBm (50 mW) transmitter with an 18 dBi sector antenna, you must have 5 dB cable loss to be legal (17 + 18 - 5 = 30 dBm). Refer to the following table:

Power at antenna (dBm)	Antenna Gain (dBi)	**EIRP** (dBm)	**EIRP** (watts)
24	6	30	1
21	9	30	1
18	12	30	1
15	15	30	1
12	18	30	1
9	21	30	1
6	24	30	1

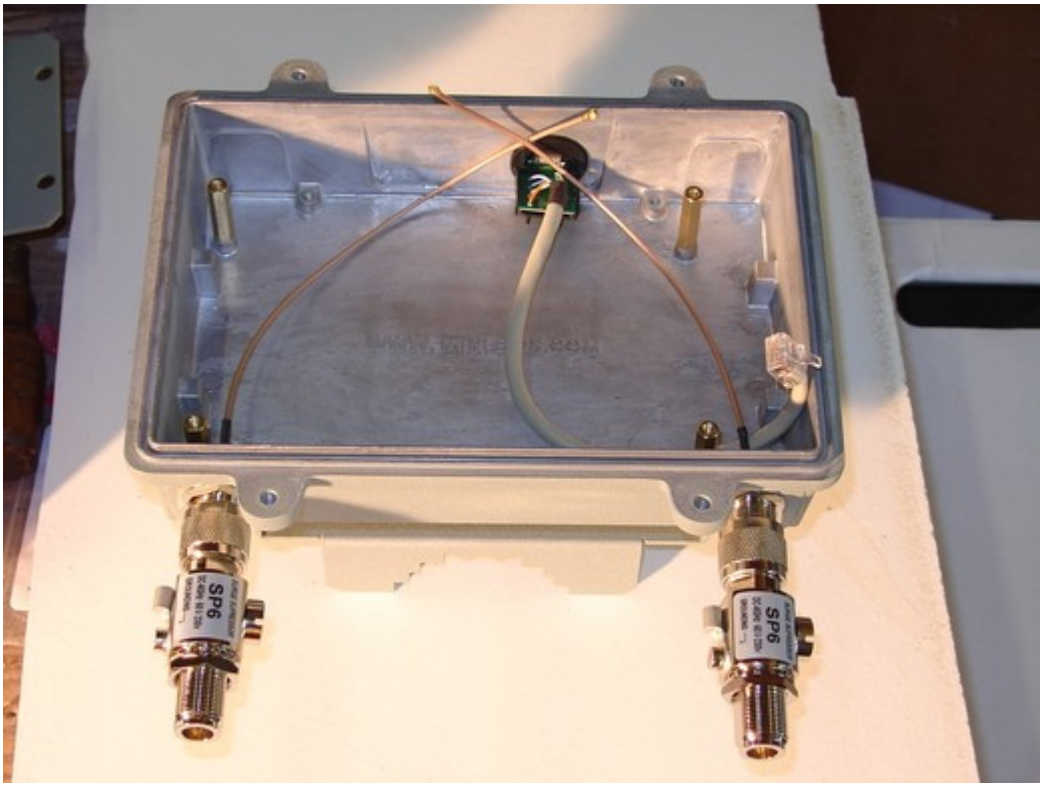
Photographs

The Two Sites (upper left & mid-center)

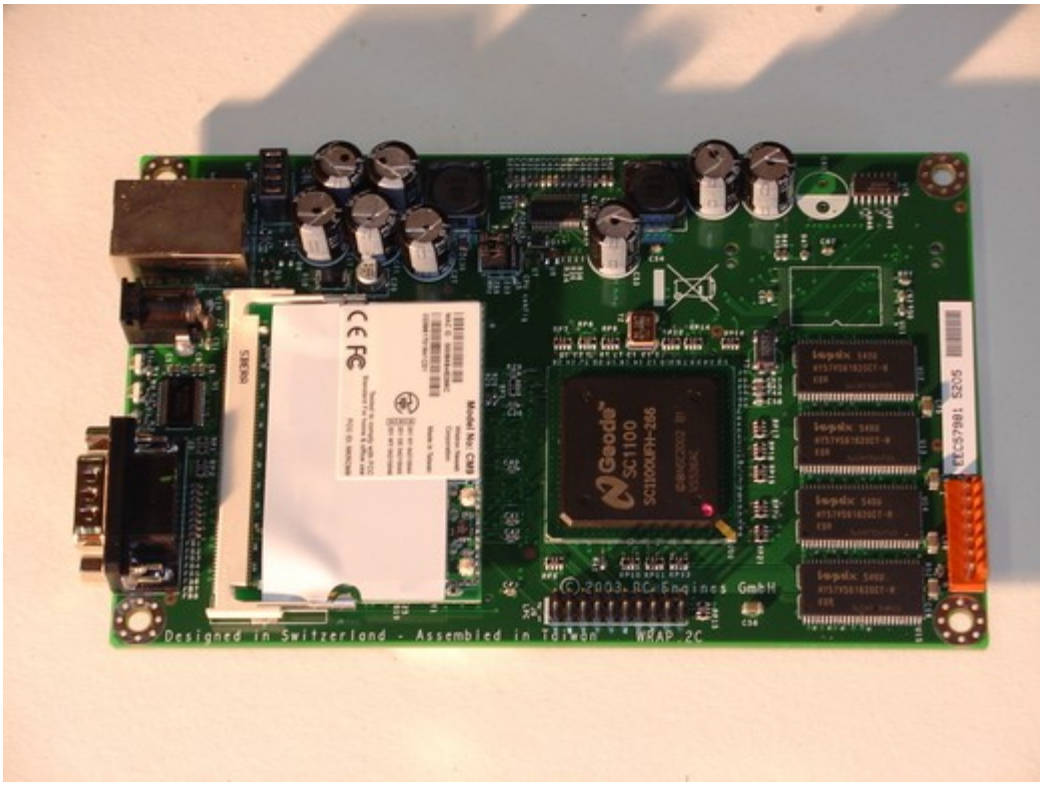
The WRAP Enclosure



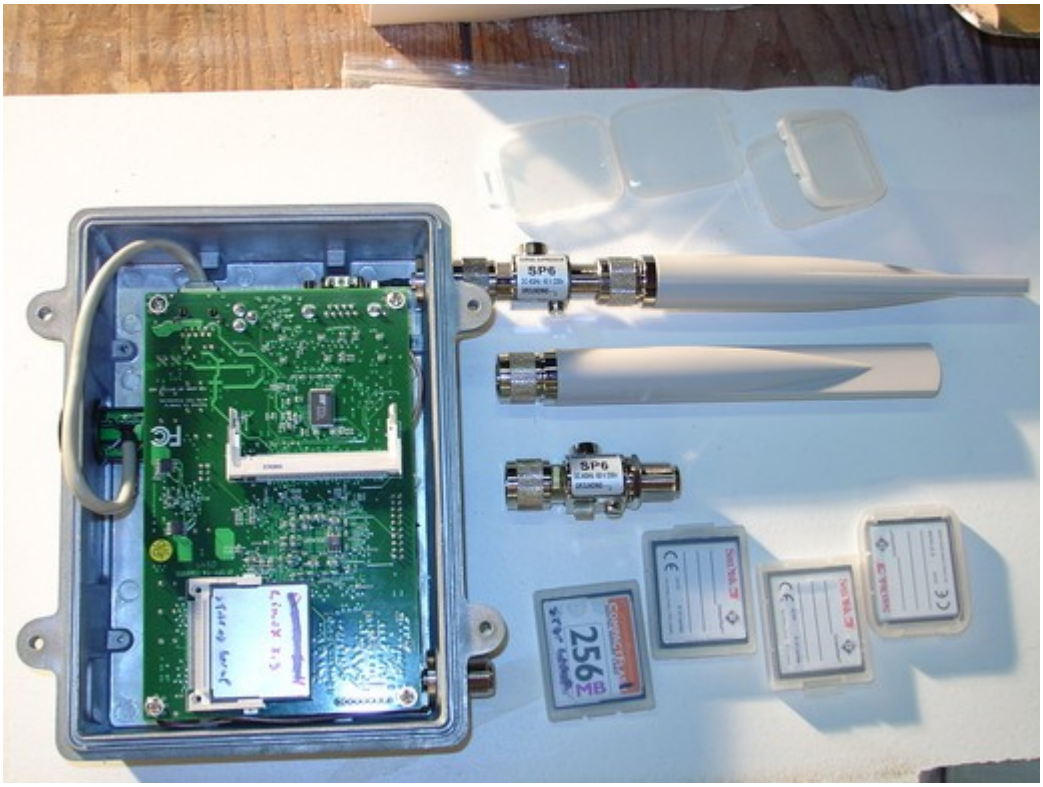
WRAP with Pigtails and Lightening Arrestors



A 266 MHz PC SBC with MPCI Radio Card

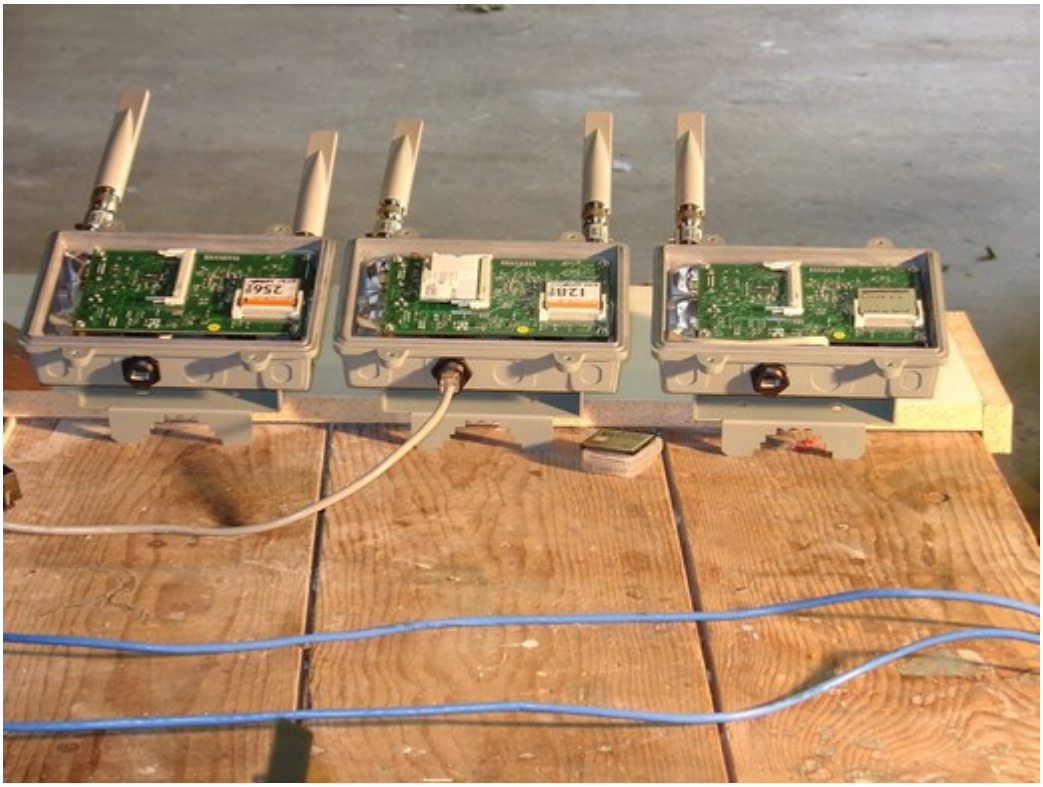


SBC in Enclosure, Example CF cards



POE Injector

Three WRAPS in Early Testing

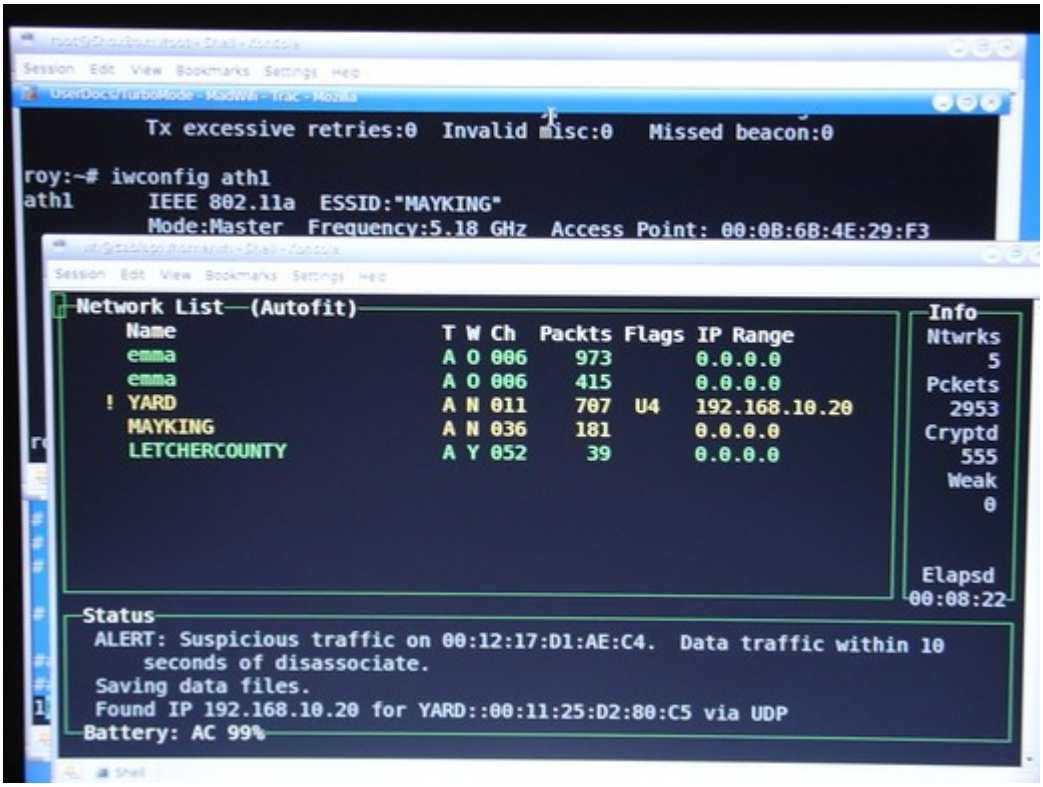


29 Db Antenna With Radome

Setting the Polarity on the Antenna

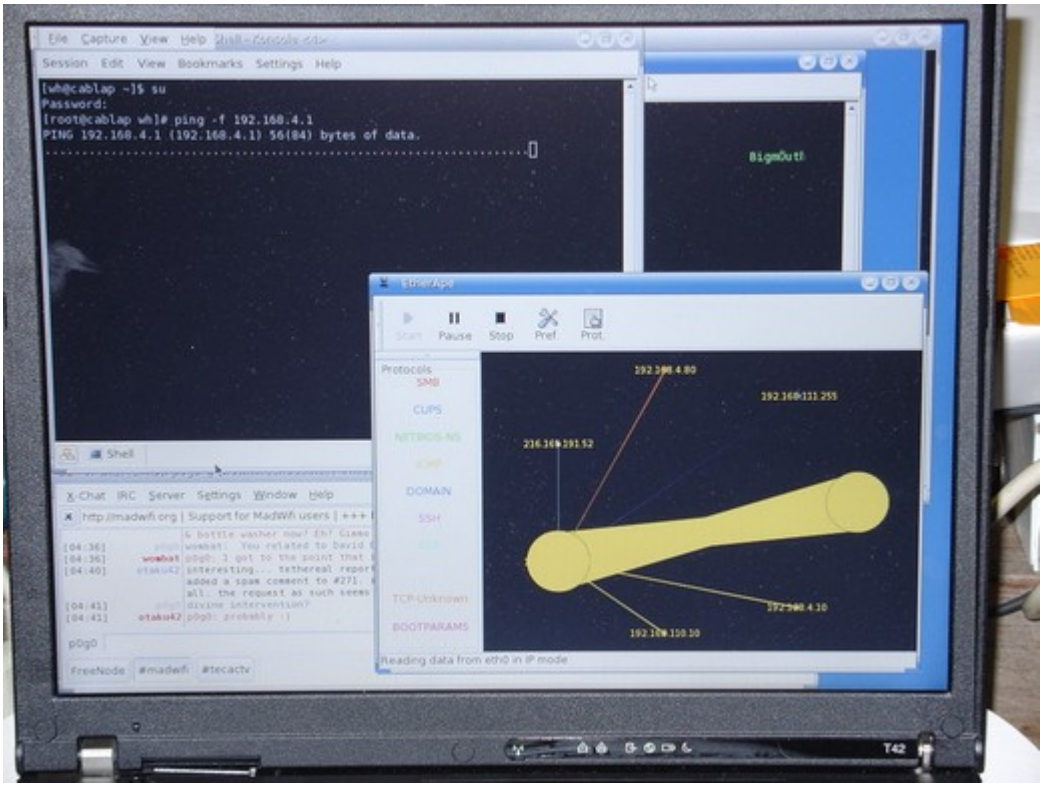
Rear View Showing Antenna Cable Connector (Remove the Black Cap)

Network Testing



The WRAPS in Testbed Mode

Success: Internet Access Across the WRAPs



The Repeater Tower

The Radio Shack

EIRP Budgets

5.8GHz

Wireless Network Link Analysis

http://my.athenet.net/~multiplx/cgi-bin/wireless.cgi

A service of Green Bay Professional Packet Radio - www.gbppr.org

---

Highest Transmitted Frequency : 5.805000 **GHz** (5805.000000 **MHz**)
Wavelength : 0.0516 **meters** (5.1644 **centimeters**)
: 0.1694 **feet** (2.0332 **inches**)
Transmitter RF Power Output : 14.000 **dBm** (25.119 **milliWatts**)
: -16.000 **dBW** (0.025 **Watts**)
: -46.000 **dBk** (0.00003 **kiloWatts**)
Transmitter Transmission Line Type : Times Microwave LMR-400

Transmitter Line Length	3.00 **meters** (9.84 **feet**)
Transmitter Line Loss Specification	35.52 **dB/100-meters** (10.83 **dB/100-feet**)
Calculated Transmitter Line Loss	1.07 **dB** (0.36 **dB/meter**) (0.11 **dB/foot**)
Transmitter Line Efficiency	78.24 % (acceptable line loss)
Total Transmitter Connector Loss	0.29 **dB through** 2 **connectors**
Transmitter Line Miscellaneous Loss	0.50 **dB**
Total Transmitter Line Loss	1.86 **dB**
Transmitter Path Miscellaneous Losses	0.00 **dB**
Transmitter Miscellaneous Gain	0.00 **dB**
Transmitter Antenna Peak Gain	28.00 **dBi** (25.85 **dBd**)
Transmitter Antenna Radome Loss	1.00 **dB**
Transmitter Antenna 3 dB Beamwidth	6.53 °
Total RF Input Power to the Antenna	12.14 **dBm** (16.38 **milliWatts**)
FCC Part 15.247 Allowed RF Input Power to Antenna	22.67 **dBm** (184.93 **milliWatts**)
Transmitter Antenna Height	14.00 **meters** (45.93 **feet**) **AGL**
Transmitter Antenna Site Elevation	1100.00 **meters** (3608.92 **feet**) **AMSL**
Overall Transmitter Antenna Height	1114.00 **meters** (3654.85 **feet**) **AMSL**
Transmitter Distance to the Radio Horizon	15.43 **kilometers** (9.59 **miles**)
Transmitter to Receiver Antenna Mechanical Tilt	-4.9267 ° (DOWNWARD)
Receiver Transmission Line Type	Times Microwave LMR-400
Receiver Line Length	3.00 **meters** (9.84 **feet**)
Receiver Line Loss Specification	35.52 **dB/100-meters** (10.83 **dB/100-feet**)
Calculated Receiver Line Loss	1.07 **dB** (0.36 **dB/meter**) (0.11 **dB/foot**)
Receiver Line Efficiency	78.24 % (acceptable line loss)
Total Receiver Connector Loss	0.29 **dB through** 2 **connectors**
Receiver Line Miscellaneous Loss	0.00 **dB**
Total Receiver Line Loss	1.36 **dB**
Receiver Miscellaneous Gain	0.00 **dB**
Receiver Antenna Peak Gain	28.00 **dBi** (25.85 **dBd**)
Receiver Antenna Radome Loss	1.00 **dB**
Receiver Antenna 3 dB Beamwidth	6.53 °
Receiver Antenna Height	30.00 **meters** (98.43 **feet**) **AGL**
Receiver Antenna Site Elevation	400.00 **meters** (1312.34 **feet**) **AMSL**
Overall Receiver Antenna Height	430.00 **meters** (1410.77 **feet**) **AMSL**
Receiver Distance to the Radio Horizon	22.58 **kilometers** (14.03 **miles**)
Receiver to Transmitter Antenna Mechanical Tilt	+4.8727 ° (UPWARD)
Vertical Space Diversity Antenna Height	0.00 **meters** (0.00 **feet**) **AGL**
Diversity Antenna Gain	0.00 **dBi** (-2.15 **dBd**)
Calculated Diversity Antenna Line Loss	0.00 **dB** (0.36 **dB/meter**) (0.11 **dB/foot**)
Diversity Line Miscellaneous Loss	0.00 **dB**
Overall Diversity Receiver Antenna Height	430.00 **meters** (1410.77 **feet**) **AMSL**
Transmitter Site Name	m
Transmitter Site Latitude	0.000000 (00° 00' 0.00")
Transmitter Site Longitude	0.000000 (000° 00' 0.00")
Receiver Site Name	c
Receiver Site Latitude	0.000000 (00° 00' 0.00")
Receiver Site Longitude	0.000000 (000° 00' 0.00")
Azimuth From Transmitter Site to Receiver Site	Not Applicable ° **East of true North**
Azimuth From Receiver Site to Transmitter Site	Not Applicable ° **East of true North**
Total Path Distance	8.00 **kilometers** (4.97 **miles**)
Free Space Path Loss	125.79 **dB**
Estimated Urban Area Path Loss	157.16 **dB**
Total Worst Case Precipitation Loss	0.000 **dB**
Total Water Vapor Loss	0.016 **dB**
Total Oxygen Loss	0.056 **dB**
Total System Free Space Path Loss	125.86 **dB**
Total System Urban Area Path loss	157.23 **dB**
Peak Effective Isotropic Radiated Power (EIRP)	39.144 **dBm** (8211.075 **milliWatts**)

: 9.144 dBW (8.211 Watts)
: -20.856 dBk (0.00821 kiloWatts)
Unfaded Free Space Received Carrier Power Level : -61.07 dBm (197.69 µV)
Unfaded Urban Area Received Carrier Power Level : -92.44 dBm (5.34 µV)
Receiver Threshold (sensitivity) : -90.00 dBm (7.07 µV)
Thermal Noise Free Space Fade Margin : 28.93 dB (Urban : -2.44 dB)
Diversity Thermal Noise Free Space Fade Margin : 28.93 dB (Urban : -2.44 dB)
Ideal Thermal Noise Fade Margin for This Climate : 2.51 dB
Dispersive Free Space Fade Margin : 0.00 dB (Urban : 0.00 dB)
External Interference Free Space Fade Margin : 0.00 dB (Urban : 0.00 dB)
Adj. Channel Interference Free Space Fade Margin : 0.00 dB (Urban : 0.00 dB)
Composite Free Space Fade Margin : 28.93 dB (Urban : -2.44 dB)
Dense, Dry, In-Leaf Temperate Climate Foliage Loss : 2.20 dB/meter (0.67 dB/foot) worst case
Estimated Attenuation Due to Precipitation : 0.000 dB/km (0.000 dB/mi) (0.0 mm/hour)
Estimated Attenuation Due to Water Vapor : 0.002 dB/km (0.001 dB/mi) 7.5 gm/m3
Estimated Attenuation Due to Oxygen Loss : 0.007 dB/kilometer (0.004 dB/mile)
Absolute Minimum Antenna Height for Either Antenna : 7.04 meters (23.09 feet)

One Way - No Spaced Vertical Antenna Diversity

Annual Free Space Multipath Reliability Estimate : 99.99994302 % (Urban : 99.92188195 %)
Annual Free Space Multipath Outage : 4.62 seconds (Urban : 1.76 hours)
Worst Month Free Space Multipath Outage : 1.48 seconds (Urban : 33.85 minutes)
Annual Free Space Severely Errored Seconds : 4.62 (Urban : 6336.94)
Worst Month Free Space Severely Errored Seconds : 1.48 (Urban : 2031.07)

One Way - With Spaced Vertical Antenna Diversity

Vertical Spacing for Diversity Antennas : 11.06 meters (36.29 feet) (calculated)
Free Space Diversity Improvement Factor : 84.16 (will improve link reliability)
Urban Area Diversity Improvement Factor : 0.06 (will not improve link reliability)
Annual Free Space Multipath Reliability Estimate : 99.99999932 % (Urban : 99.92188195 %)
Annual Free Space Multipath Outage : 0.05 seconds (Urban : 1.76 hours)
Worst Month Free Space Multipath Outage : 0.02 seconds (Urban : 33.85 minutes)
Annual Free Space Severely Errored Seconds : 0.05 (Urban : 6336.94)
Worst Month Free Space Severely Errored Seconds : 0.02 (Urban : 2031.07)
Effective Earth Radius (K Factor) : 4/3
Climate Factor : 0.25
Urban Environment Factor : Rural Country Side - Quasi Open
Terrain Roughness (std. dev. of elevations) : 15.00 meters (49.21 feet)
Average Annual Temperature : 11.11 ° C (52.00 ° F)
Sea Level Corrected Atmospheric Pressure : Not Applicable millibars
Saturation Vapor Pressure : Not Applicable millibars
Partial Vapor Pressure : Not Applicable millibars
Index of Refraction : Not Applicable N units
Maximum Free Space Wave Communications Distance : 38.01 kilometers (23.62 miles)
Receiver Site Grazing Angle : -0.11 °
Estimated RF Power Density Below the Radiating Antenna : 0.001 mW/cm2
FCC OET Bulletin #65 Maximum Permissible Exposure : 1.00 mW/cm2
Distance to RF Safety Compliance From Transmit Antenna : 0.47 meters (1.56 feet)

5.3 GHz

Wireless Network Link Analysis

A service of Green Bay Professional Packet Radio - www.gbppr.org

---

Highest Transmitted Frequency	5.250000 **GHz** (5250.000000 **MHz**)
Wavelength	0.0571 **meters** (5.7103 **centimeters**)
	0.1873 **feet** (2.2482 **inches**)
Transmitter RF Power Output	18.000 **dBm** (63.096 **milliWatts**)
	-12.000 **dBW** (0.063 **Watts**)
	-42.000 **dBk** (0.00006 **kiloWatts**)
Transmitter Transmission Line Type	Times Microwave LMR-400
Transmitter Line Length	3.00 **meters** (9.84 **feet**)
Transmitter Line Loss Specification	33.55 **dB/100-meters** (10.23 **dB/100-feet**)
Calculated Transmitter Line Loss	1.01 **dB** (0.34 **dB/meter**) (0.10 **dB/foot**)
Transmitter Line Efficiency	79.31 % (acceptable line loss)
Total Transmitter Connector Loss	0.26 **dB through** 2 **connectors**
Transmitter Line Miscellaneous Loss	0.50 **dB**
Total Transmitter Line Loss	1.77 **dB**
Transmitter Path Miscellaneous Losses	0.00 **dB**
Transmitter Miscellaneous Gain	0.00 **dB**
Transmitter Antenna Peak Gain	28.00 **dBi** (25.85 **dBd**)
Transmitter Antenna Radome Loss	1.00 **dB**
Transmitter Antenna 3 dB Beamwidth	6.53 °
Total RF Input Power to the Antenna	16.23 **dBm** (41.99 **milliWatts**)
FCC Part 15.247 Allowed RF Input Power to Antenna	22.67 **dBm** (184.93 **milliWatts**)
Transmitter Antenna Height	14.00 **meters** (45.93 **feet**) **AGL**
Transmitter Antenna Site Elevation	1100.00 **meters** (3608.92 **feet**) **AMSL**
Overall Transmitter Antenna Height	1114.00 **meters** (3654.85 **feet**) **AMSL**
Transmitter Distance to the Radio Horizon	15.43 **kilometers** (9.59 **miles**)
Transmitter to Receiver Antenna Mechanical Tilt	-4.9267 ° (DOWNWARD)
Receiver Transmission Line Type	Times Microwave LMR-400
Receiver Line Length	3.00 **meters** (9.84 **feet**)
Receiver Line Loss Specification	33.55 **dB/100-meters** (10.23 **dB/100-feet**)
Calculated Receiver Line Loss	1.01 **dB** (0.34 **dB/meter**) (0.10 **dB/foot**)
Receiver Line Efficiency	79.31 % (acceptable line loss)
Total Receiver Connector Loss	0.26 **dB through** 2 **connectors**
Receiver Line Miscellaneous Loss	0.00 **dB**
Total Receiver Line Loss	1.27 **dB**
Receiver Miscellaneous Gain	0.00 **dB**
Receiver Antenna Peak Gain	28.00 **dBi** (25.85 **dBd**)
Receiver Antenna Radome Loss	1.00 **dB**
Receiver Antenna 3 dB Beamwidth	6.53 °
Receiver Antenna Height	30.00 **meters** (98.43 **feet**) **AGL**
Receiver Antenna Site Elevation	400.00 **meters** (1312.34 **feet**) **AMSL**
Overall Receiver Antenna Height	430.00 **meters** (1410.77 **feet**) **AMSL**
Receiver Distance to the Radio Horizon	22.58 **kilometers** (14.03 **miles**)
Receiver to Transmitter Antenna Mechanical Tilt	+4.8727 ° (UPWARD)
Vertical Space Diversity Antenna Height	0.00 **meters** (0.00 **feet**) **AGL**
Diversity Antenna Gain	0.00 **dBi** (-2.15 **dBd**)
Calculated Diversity Antenna Line Loss	0.00 **dB** (0.34 **dB/meter**) (0.10

dB/foot)
Diversity Line Miscellaneous Loss : 0.00 dB
Overall Diversity Receiver Antenna Height : 430.00 meters (1410.77 feet) AMSL
Transmitter Site Name : m
Transmitter Site Latitude : 0.000000 (00° 00' 0.00")
Transmitter Site Longitude : 0.000000 (000° 00' 0.00")
Receiver Site Name : c
Receiver Site Latitude : 0.000000 (00° 00' 0.00")
Receiver Site Longitude : 0.000000 (000° 00' 0.00")
Azimuth From Transmitter Site to Receiver Site : Not Applicable ° East of true North
Azimuth From Receiver Site to Transmitter Site : Not Applicable ° East of true North
Total Path Distance : 8.00 kilometers (4.97 miles)
Free Space Path Loss : 124.91 dB
Estimated Urban Area Path Loss : 156.44 dB
Total Worst Case Precipitation Loss : 0.000 dB
Total Water Vapor Loss : 0.016 dB
Total Oxygen Loss : 0.056 dB
Total System Free Space Path Loss : 124.98 dB
Total System Urban Area Path loss : 156.51 dB
Peak Effective Isotropic Radiated Power (EIRP) : 43.231 dBm (21042.629 milliWatts)
: 13.231 dBW (21.043 Watts)
: -16.769 dBk (0.02104 kiloWatts)
Unfaded Free Space Received Carrier Power Level : -56.02 dBm (353.58 µV)
Unfaded Urban Area Received Carrier Power Level : -87.55 dBm (9.38 µV)
Receiver Threshold (sensitivity) : -90.00 dBm (7.07 µV)
Thermal Noise Free Space Fade Margin : 33.98 dB (Urban : 2.45 dB)
Diversity Thermal Noise Free Space Fade Margin : 33.98 dB (Urban : 2.45 dB)
Ideal Thermal Noise Fade Margin for This Climate : 2.07 dB
Dispersive Free Space Fade Margin : 0.00 dB (Urban : 0.00 dB)
External Interference Free Space Fade Margin : 0.00 dB (Urban : 0.00 dB)
Adj. Channel Interference Free Space Fade Margin : 0.00 dB (Urban : 0.00 dB)
Composite Free Space Fade Margin : 33.98 dB (Urban : 2.45 dB)
Dense, Dry, In-Leaf Temperate Climate Foliage Loss : 2.14 dB/meter (0.65 dB/foot) worst case
Estimated Attenuation Due to Precipitation : 0.000 dB/km (0.000 dB/mi) (0.0 mm/hour)
Estimated Attenuation Due to Water Vapor : 0.002 dB/km (0.001 dB/mi) 7.5 gm/m3
Estimated Attenuation Due to Oxygen Loss : 0.007 dB/kilometer (0.004 dB/mile)
Absolute Minimum Antenna Height for Either Antenna : 7.35 meters (24.12 feet)

One Way - No Spaced Vertical Antenna Diversity

Annual Free Space Multipath Reliability Estimate : 99.99998389 % (Urban : 99.97708560 %)
Annual Free Space Multipath Outage : 1.31 seconds (Urban : 30.98 minutes)
Worst Month Free Space Multipath Outage : 0.42 seconds (Urban : 9.93 minutes)
Annual Free Space Severely Errored Seconds : 1.31 (Urban : 1858.82)
Worst Month Free Space Severely Errored Seconds : 0.42 (Urban : 595.77)

One Way - With Spaced Vertical Antenna Diversity

Vertical Spacing for Diversity Antennas : 12.24 meters (40.16 feet) (calculated)
Free Space Diversity Improvement Factor : 298.19 (will improve link reliability)
Urban Area Diversity Improvement Factor : 0.21 (will not improve link reliability)
Annual Free Space Multipath Reliability Estimate : 99.99999995 % (Urban : 99.97708560 %)
Annual Free Space Multipath Outage : 0.00 seconds (Urban : 30.98 minutes)
Worst Month Free Space Multipath Outage : 0.00 seconds (Urban : 9.93 minutes)
Annual Free Space Severely Errored Seconds : 0.00 (Urban : 1858.82)
Worst Month Free Space Severely Errored Seconds : 0.00 (Urban : 595.77)
Effective Earth Radius (K Factor) : 4/3
Climate Factor : 0.25
Urban Environment Factor : Rural Country Side - Quasi Open

Terrain Roughness (std. dev. of elevations) : 15.00 **meters** (49.21 **feet**)
Average Annual Temperature : 11.11 **° C** (52.00 **° F**)
Sea Level Corrected Atmospheric Pressure : Not Applicable **millibars**
Saturation Vapor Pressure : Not Applicable **millibars**
Partial Vapor Pressure : Not Applicable **millibars**
Index of Refraction : Not Applicable **N units**
Maximum Free Space Wave Communications Distance : 38.01 **kilometers** (23.62 **miles**)
Receiver Site Grazing Angle : -0.11 **°**
Estimated RF Power Density Below the Radiating Antenna : 0.003 **mW/cm2**
FCC OET Bulletin #65 Maximum Permissible Exposure : 1.00 **mW/cm2**
Distance to RF Safety Compliance From Transmit Antenna : 0.75 **meters** (2.46 **feet**)

Safety

http://my.athenet.net/~multiplx/cgi-bin/rfsafety.main.cgi

Frequency of Operation : 5805.000 MHz
Average Power at Antenna : 0.050 Watts
Antenna Gain : 28.000 dBi
Distance from Antenna : 1.000 meters (3.281 feet)
Estimated Power Density : 0.644 mW/cm^2
Ground Reflections : Yes

Maximum Permissible Exposure (MPE)

Controlled Environment : 5.005 mW/cm^2
Uncontrolled Environment : 1.005 mW/cm^2

Distance to Compliance from Center of Antenna

Controlled Environment : 0.374 meters (1.228 feet)
Uncontrolled Environment : 0.818 meters (2.683 feet)
Is the Controlled Environment Area Compliant? :Yes
Is the Uncontrolled Environment Area Compliant? :Yes