

Tutorial 2 - P2P WiFi Groups w/ Automatic IP Address

Following tutorial was done with Raspbian 10 Buster and hostapd 2.7

Steps A2.1.x and A2.2.x are EXACT THE SAME AS THE TUTORIAL 1!

Step B2.3.x add the new instructions (Install DNSMASQ).

Recommendation:

DO NOT use your main system disk (sdCard), instead, use a fresh system or some "learn/lab/test" system to makes theses tutorials/experiments.

After completing all set of 3 tutorials you should be able to have a good basic understanding of the whole matter, and should be able to know the best way to use the knowledge...

Text Editor:

Use the text editor of your preference, like Geany (GUI based) or Nano (terminal based), etc.

A2.1.0 WiFi between 2 peers (or more) w/ automatic IP Address.

A2.1.1 Install hostapd software

```
sudo apt install hostapd
```

Temporarily shutdown hostapd service

```
sudo service hostapd stop
```

Unmask (unlock) hostapd service

```
sudo systemctl unmask hostapd.service  
sudo systemctl enable hostapd.service
```

A2.1.2 Create/Modify hostapd configuration file (/etc/hostapd/hostapd.conf)

```
sudo nano /etc/hostapd/hostapd.conf
```

Copy and Paste the following text

```
interface=wlan0  
driver=nl80211  
hw_mode=g  
channel=6  
wmm_enabled=0  
macaddr_acl=0  
auth_algs=1  
ignore_broadcast_ssid=0  
wpa=2  
wpa_key_mgmt=WPA-PSK  
wpa_pairwise=TKIP  
rsn_pairwise=CCMP  
ssid=YOUR-SSID  
wpa_passphrase=YOUR-PASSPHRASE-PASSWORD
```

A2.1.3 Edit the file /etc/hostapd, modify the variable "DAEMON_CONF".

Find the line with "#DAEMON_CONF=",

Remove any "#" sign at the beginning of the line, if it exist.

add the following value:

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

A2.1.4 Edit the file /etc/dhcpd.conf, give the WIFI an static IP Address

```
sudo nano /etc/dhcpd.conf
```

Add the following lines at the end of the file.

```
interface wlan0
static ip_address=192.168.50.1/24
nohook wpa_supplicant
```

A2.1.5 Start/Restart hostapd service

```
sudo service hostapd start
```

A2.1.6 Reboot the system

Reboot the system, so that you can use the installed software.

A2.2.0 Add Internet Routing to the peers.

A2.2.1 Edit /etc/sysctl.conf, allow IPv4 FORWARD

Find the line "`#net.ipv4.ip_forward=1`", then, remove the sharp (#) signal, at the start of the line. The sharp (#) signal means that this instruction is not active, the computer does not read lines starting with sharp (#)...

The line then becomes:

```
net.ipv4.ip_forward=1
```

This step will require a reboot.

This step will require a reboot.

The next time the system start it will be able to route traffic (forward) between peers and the Internet.

A2.2.2 Run the following iptables command line instructions

```
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo iptables -A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
```

Change the "eth0" and "wlan0" and use the names of your actual interfaces.

Use the command "ip a" to display the actual names of your interfaces.

Every time the computer REBOOT, you will need to run these lines!

B2.3.0 Install DNSMASQ (DNS Forwarder and DHCP Server)

B2.3.1 Install dnsmasq software

```
sudo apt install dnsmasq
```

Temporary stop dnsmasq service

```
sudo service dnsmasq stop
```

B2.3.2 Edit /etc/dnsmasq.conf

```
sudo nano /etc/dnsmasq.conf
```

Add following lines at top or end

```
interface=wlan0  
dhcp-range=192.168.50.50,192.168.50.100,255.255.255.0,24h
```

B2.3.3 Restart/start dnsmasq service

```
sudo service dnsmasq start
```

Congratulations,
now you can connect peer-guests without the
need of manual procedure to assign IP ADDRESS.

Just choose SSID and enter password/passphrase.

About DNSMASQ

The software dnsmasq provides 2 basic services: DHCP Server and DNS Forwarder.

The DHCP is the portion that gives a new IP ADDRESS for every
new peer-guest that connects to the network.

The DNS Forwarder provider a forward function to the your internet provider
dns server function (just a kind of linkage).