<table>
<thead>
<tr>
<th>NUMBER</th>
<th>DATE</th>
<th>DESCRIPTION</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2011-05-19</td>
<td></td>
<td>WB</td>
</tr>
</tbody>
</table>
# Contents

1. Introduction ................................................................. 1

2. Setup For Automatic Wireless Connection .......................... 1

3. Command Line Manual Method ........................................ 1

4. More Detail ........................................................................ 1

A. Things To Use Or Avoid .................................................. 2
1 Introduction

Setting up wireless networking on FreeBSD is not as complex as in the past. Here’s the short form. The examples that follow show a RealTek wireless device using the `urtw(4)` driver.

2 Setup For Automatic Wireless Connection

If needed, load driver modules in `/boot/loader.conf`.

```
if_urtw_load=YES
```

Create `/etc/wpa_supplicant.conf` with SSID and PSK.

```
network={
  ssid="myssid"
  psk="myultrasecretkey"
}
```

Modify `/etc/rc.conf` to create `wlan0` and connect:

```
wlangs_urtw0=wlan0
ifconfig_wlan0="WPA SYNCDHCP"
```

On startup, FreeBSD will automatically connect.

That’s it, pretty much all you need. Stop here unless you want to manually start a wireless connection.

3 Command Line Manual Method

```
# kldload if_urtw
# ifconfig wlan0 create wlandev urtw0
# wpa_supplicant -B -i wlan0 -c /etc/wpa_supplicant.conf
# dhclient wlan0
```

1. If your wireless card driver isn’t built into the `GENERIC` kernel, or you use a custom kernel without it, the driver module must be loaded first. Some devices also need firmware modules, usually provided by a port. See the man page for your device.

2. Create a generic wireless device for the wireless network code to use.

3. Run `wpa_supplicant(8)` to associate to an access point defined in `/etc/wpa_supplicant.conf`.

4. Get an IP address and DNS servers.

4 More Detail

The FreeBSD Handbook chapter on wireless networking.
A Things To Use Or Avoid

WEP is insecure, avoid it. WPA2 is much better, use it. If you have old equipment that doesn’t support WPA, smash it with a hammer or other convenient blunt instrument.

TKIP has some flaws. Use AES.

"Hidden" SSIDs are not really hidden. They make network setup more difficult and provide no real security benefits.