Connecting to a Wireless Network using WEP (Wired Equivalent Privacy) for Authentication and Encryption#

WEP can be used for both authentication and privacy with your wireless network. Authentication is a required pre-cursor to allowing a station to associate with an access point. The IEEE 802.11 standard defines two types of WEP authentication: Open System and Shared Key.

With an open system, the client will ALWAYS be authenticated with the WAP (i.e. be allowed to form an association). Keys that are passed into the client are not checked to see if they are valid. This can have the peculiar affect of having the client interface go "active" (become associated) BUT data won't be passed between the AP and station if the station key used to encrypt the data doesn't match that of the station. If you do end up with a situation in which your WEP station is active, but no traffic seems to be going through (e.g. dhcp.client doesn't work), please double check the key used for bringing up the connection.

The Shared Key authentication method involves a "challenge / response" handshake in which a "challenge" message is encrypted by the stations keys and returned to the access point for verification. If the encrypted challenge doesn't match that expected by the access point, then the station is prevented from forming an association. Unfortunately, this mechanism (in which the challenge and subsequent encrypted response) are available over the air exposes information that could leave the system more open to attacks so it is not recommended for use. While the stack does support this mode of operation, the code has not been added to ifconfig to allow it to be set.

Note that many access points offer the capability of entering a passphrase that can be used to generate the associated WEP keys. The key generation algorithm may vary from vendor to vendor. In these cases, the generated hexadecimal keys MUST be used for the network key (prefaced by 0x when used with ifconfig) and **not** the passphrase. This is in contrast to access points which allow you to enter keys in ASCII. The conversion to the hexadecimal key in that case is a simple conversion of the text into its corresponding ASCII hexadecimal representation. This form of conversion is supported by the stack.

Given the problems with WEP in general, we recommend using WPA / WPA2 for authentication and encryption where possible.

The network name can be up to 32 characters long. The WEP keymust be either 40 bits long or 104 bits long. This means you will have to give either 5 or 13 characters for the WEP key, or a 10 or 26 digit long hexadecimal value.

There are two ways to configure a WEP network. One is by use of the ifconfig utility, the other is through wpa_supplicant. You can use either of them.

When using ifconfig, the command is "ifconfig if_name ssid the_ssid nwkey the_key". For example: if your interface is ral0, you may run

- ifconfig ral0 ssid "corporate lan" nwkey corpseckey456 up (user chosen 128 bit WEP)

Once you have entered the network name and encryption method, the 802.11 network should be active. This can be verified with the ifconfig utility. In the case of ad-hoc networks, the status will only show active if there is at least one other peer on the (ssid) network.

```
ifconfig ral0
ral0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ssid "corporate lan" nwkey corpseckey456
    powersave off
    bssid 00:11:22:33:44:55 chan 11
    address: 11:44:88:44:88:44
    media: IEEE802.11 autoselect (OFDM36 mode 11g)
```

```
    status: active
```

Once the network status is active, you can send and receive packets on the wireless link.

When using wpa_supplicant, you need to edit a configuration file to tell the wpa_supplicant what you want to do. . For example, the file contains the following,

```
    network = {
    ssid = "corporate lan"          # the wifi network you want to associate to
    key_mgmt= NONE              # NONE is for WEP or none security
    wep_key0 = "corpseckey456"      # most of the cases you may specify a list from wep_key0 to wep_key3.
                    # and use key index to specify which one to be used.
}
```

Then you may run "wpa_supplicant -i ral0 -c your_config_file". By default, the configuration file is /etc/wpa_supplicant.conf. Alternatively you may use wpa_cli utility to tell the wpa_supplicant daemon what you want to do. Please refer to the TCP/IP Configuration in a Wireless Network (Client in Infrastructure Mode, or adhoc mode) section for TCP/IP interface configuration to complete your network configuration.