Scapy 802.11 Layers

```
>>> ls()

Dot11           : 802.11
Dot11ATIM       : 802.11 ATIM
Dot11AssoReq    : 802.11 Association Request
Dot11AssoResp   : 802.11 Association Response
Dot11Auth       : 802.11 Authentication
Dot11Beacon     : 802.11 Beacon
Dot11Deauth     : 802.11 Deauthentication
Dot11Disas      : 802.11 Disassociation
Dot11Elt        : 802.11 Information Element
Dot11ProbeReq   : 802.11 Probe Request
Dot11ProbeResp  : 802.11 Probe Response
Dot11QoS        : 802.11 QoS
Dot11ReassoReq  : 802.11 Reassociation Request
Dot11ReassoResp : 802.11 Reassociation Response
Dot11WEP        : 802.11 WEP packet
RadioTap        : RadioTap dummy
```

I/O Commands

```
# send layer 2 frame
sendp(pkt, iface='mon0', count=10, inter=0.2)

# read in pcap file
frame_list = rdpcap(filename)
frame_obj = frame_list[0]

# capture frames from interface in monitor mode
sniff(iface='mon0', count=10, prn=FrameHandler)

# write frames to pcap
wrpcap(filename, frames_list)
```

Useful Scripting Commands

```
# import scapy
from scapy.all import *

# check frame has specific layer
frame.haslayer(Dot11Beacon)

# get layer object
beacon_layer = frame_obj.getlayer(Dot11Beacon)

# get next layer in hierarchy
dot11_layer = radiotap_layer.payload

# show hierarchical print out of frame
print frame_obj.show()

# show one-line summary of frame
print frame_obj.summary()
```

RadioTap Layer Fields / Default Values

```
>>> ls(RadioTap)

Field        Type                    Default Value
-----------------------------------------------
version    : ByteField               = (0)
pad        : ByteField               = (0)
len        : FieldLenField           = (None)
present    : FlagsField              = (None)
notdecoded : StrLenField             = ('')
```

Dot11 Layer Fields / Default Values

```
>>> ls(Dot11)

Field        Type                    Default Value
-----------------------------------------------
subtype : BitField             = (0)
type    : BitEnumField         = (0)
proto   : BitField             = (0)
FCfield : FlagsField           = (0)
ID      : ShortField           = (0)
addr1   : MACField             = ('00:00:00:00:00:00')
addr2   : Dot11Addr2MACField   = ('00:00:00:00:00:00')
addr3   : Dot11Addr3MACField   = ('00:00:00:00:00:00')
SC      : Dot11SCField         = (0)
addr4   : Dot11Addr4MACField   = ('00:00:00:00:00:00')
```

Dot11Beacon Layer Fields / Default Values

```
>>> ls(Dot11Beacon)

Field        Type                    Default Value
-----------------------------------------------
timestamp      : LELongField         = (0)
beacon_interval: LEShortField        = (100)
cap            : FlagsField          = (0)
```

Dot11Elt Layer Fields / Default Values

```
>>> ls(Dot11Elt)

Field        Type                    Default Value
-----------------------------------------------
ID         : ByteEnumField           = (0)
len        : FieldLenField           = (None)
info       : StrLenField             = ('')
```

802.11 Scapy Cheat Sheet

Version 0.1

http://wifinigel.com

802.11 Layers Hierarchy

```
[RadioTap]
 -[Dot11]
 -- [Dot11<Frame Type>]
 --- [Dot11Elt]
 --- [Dot11Elt]
          …
 --- [Dot11Elt]
```

Interactive Mode Commands

```
Note: Scapy must be run with root level
privileges & capture iface in monintor mode

# list layers
>>> ls()

# list layer fields
>>> ls(Dot11)

# list scapy commands
>>> lsc()

# show scapy configuration
>>> conf

# show available methods for cmd/obj
dir(sniff)
dir(frame_obj)

# get help on cmd/obj
help(sniff)
help(frame_obk)

# sniff some frames & show summary
sniff(iface='mon0', count=10, prn=lambda x:
x.summary())

# exit scapy shell
exit()
```