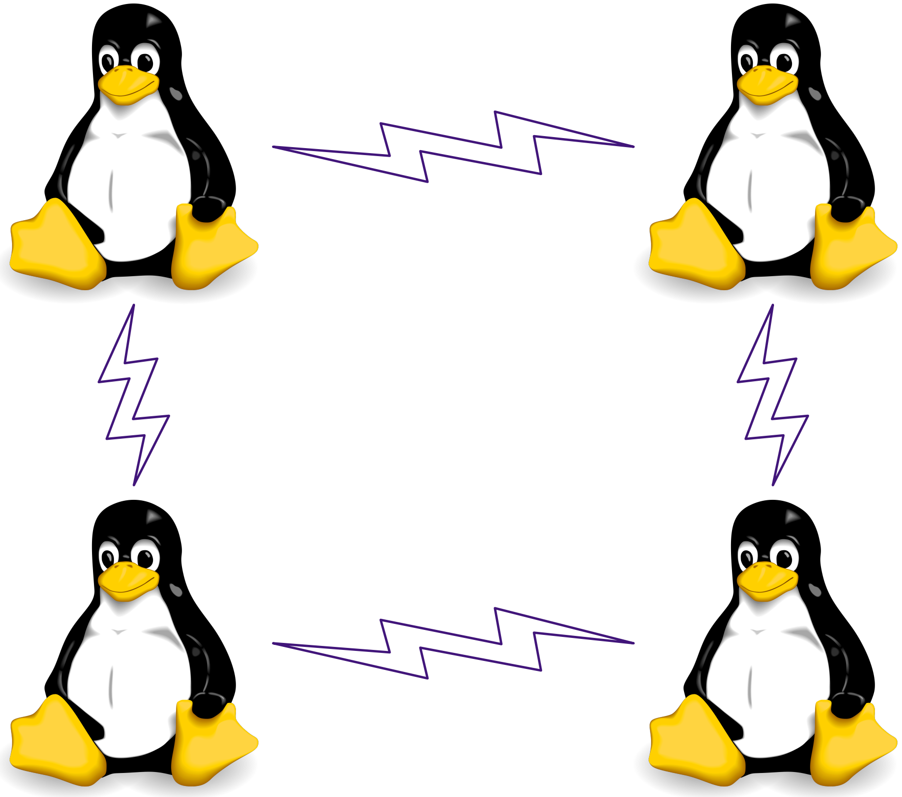
Wireless 802.11 Kernel Link Emulation



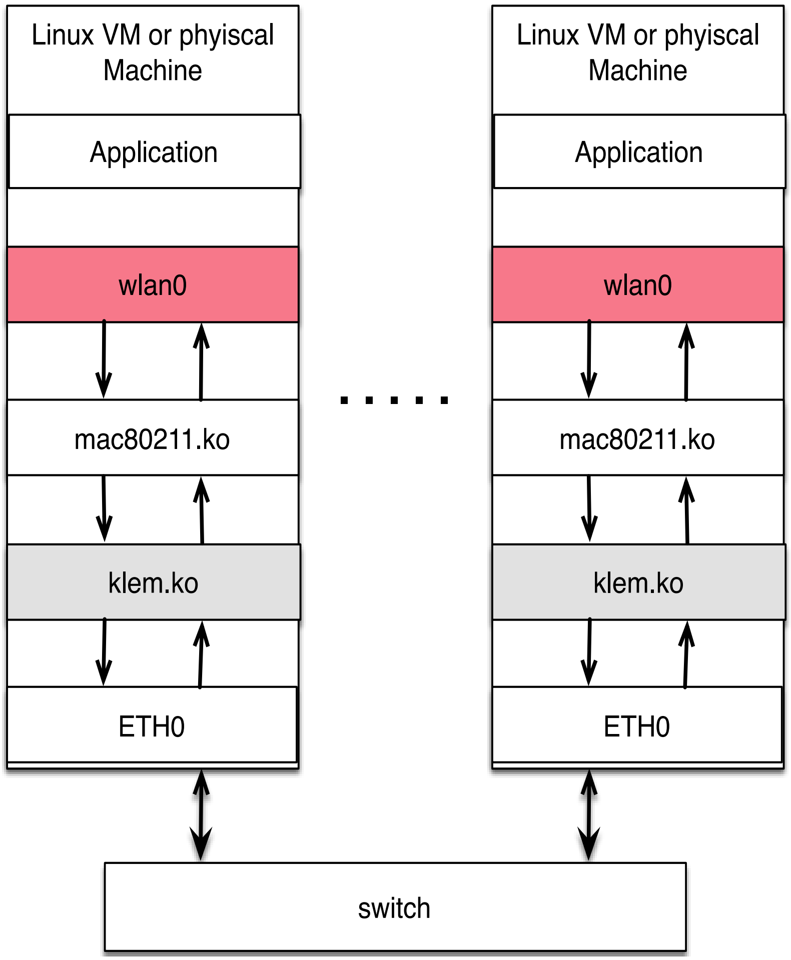
Stuart Wells

Wireless 802.11 Linux Kernel Link Emulation

A distributed Link Emulation driver that takes incoming wireless packets and determines which other connected virtual machine should receive that packet.

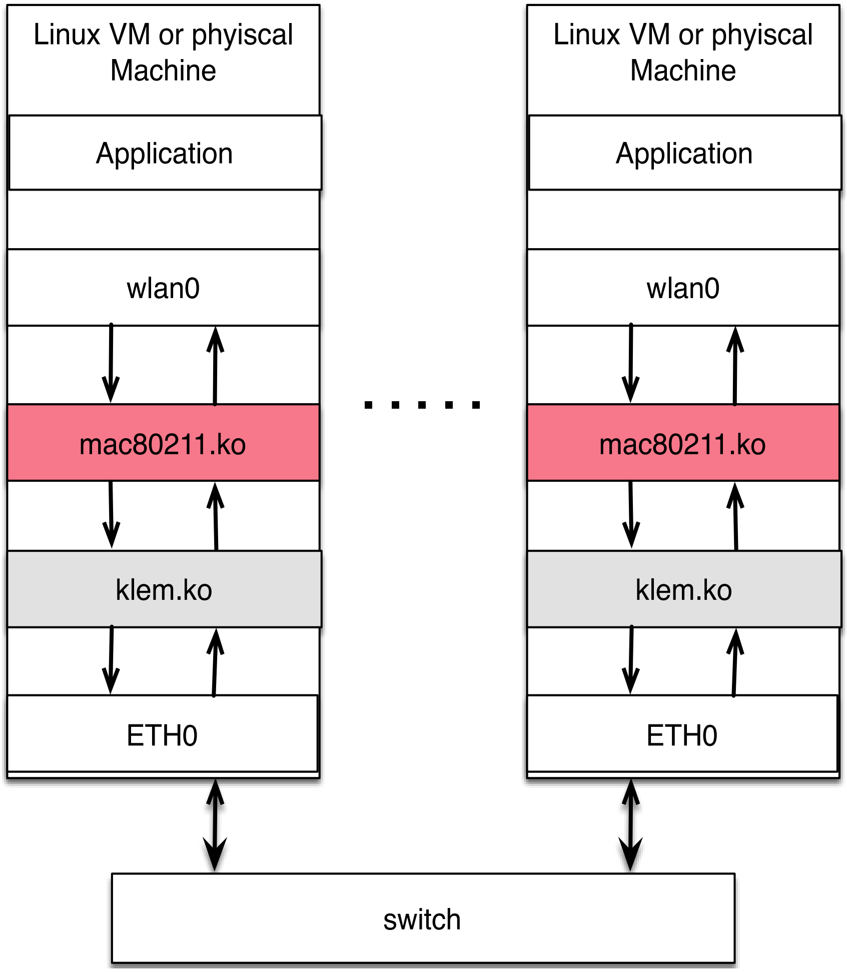
Allows specific network topologies to be simulated for applications without configuring physical hardware.

Standard Interface (wlan0)



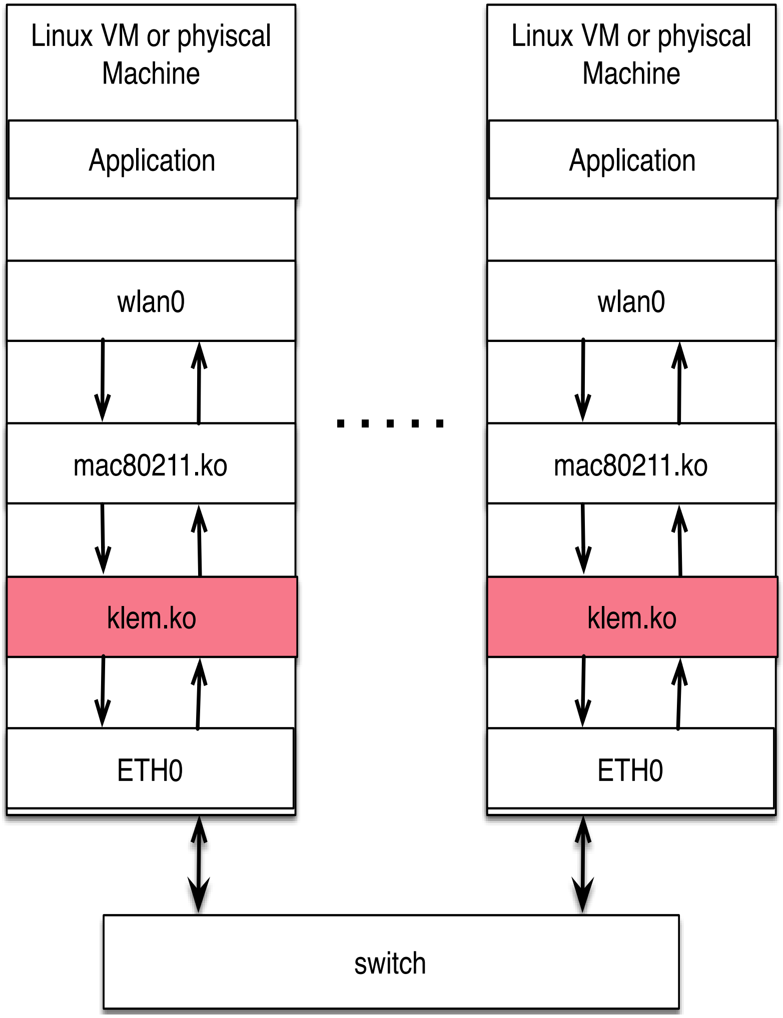
- Standard interface for wireless control
  - Controlled by iwconfig
  - Allows system to select mode, ssid, channel, address
  - Networks can be ad-hoc or configured by routers.

Soft MAC 802.11 Driver



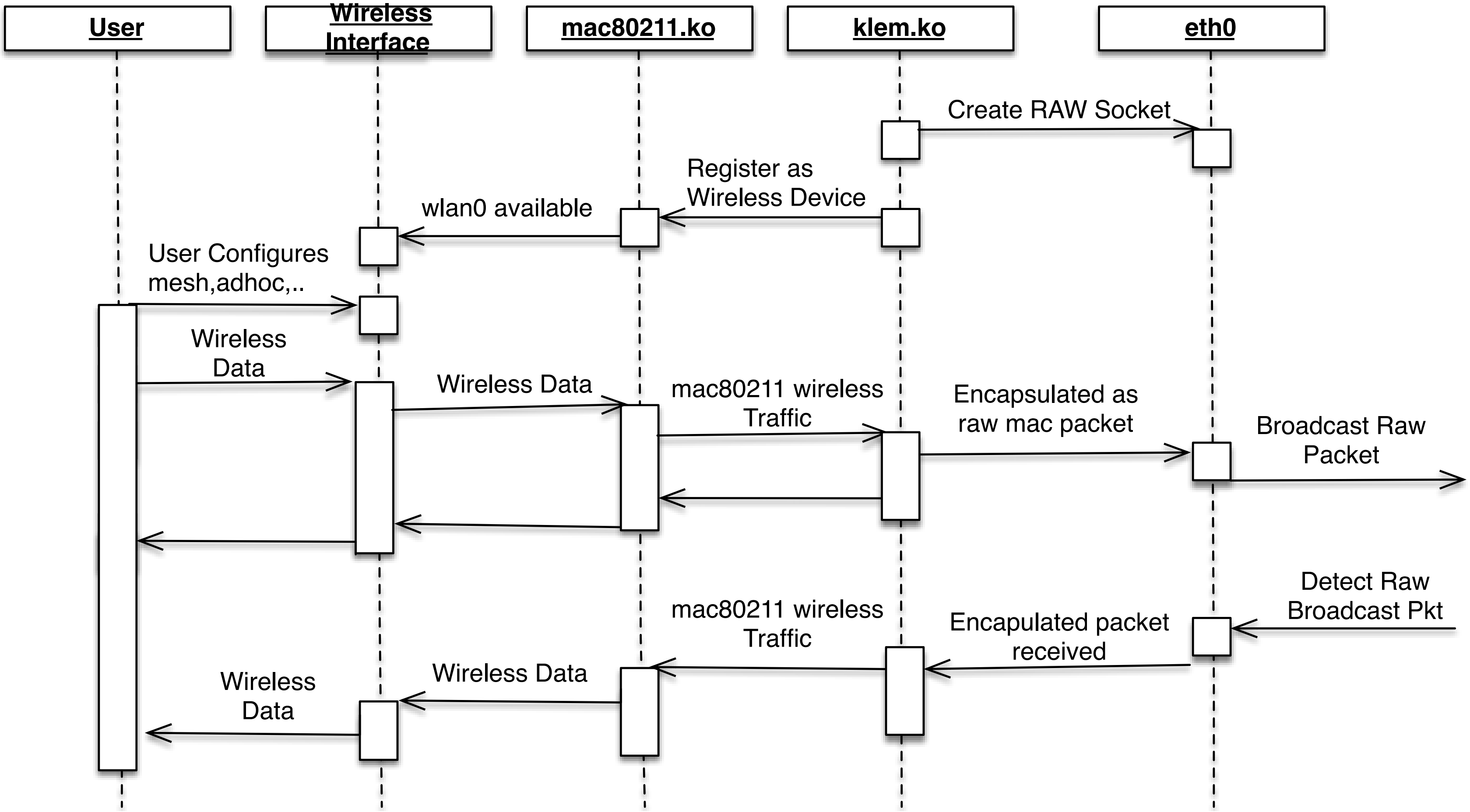
- SoftMAC 802.11
  - Framework that allows wireless frame management to be done completely in software.
  - Framework has been in Linux since 2.6.32 and is fairly stable.

KLEM Driver

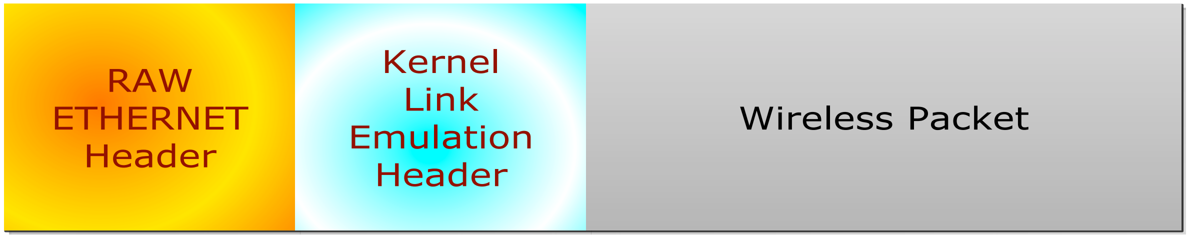


- Link Emulation Driver
  - Creates a virtual wireless connection between VMs.
  - Wraps all wireless traffic into a packet sent using eth0.
  - Can set which virtual machines are within “range” of each other.
- Packets sent using Raw

Kernel Link Emulation Sequence



Wrapping Wireless Packet



Length	**Description**	**Value**
6 bytes	Destination MAC	0xff ffffffffff (Broadcast)
6 bytes	Source MAC	MAC of virtual wireless device
2 bytes	Protocol	0xdead
4 bytes	Header	“klem”
4 bytes	Version	1
4 bytes	Band	Band used to “transmit” packet
4 bytes	Frequency	Frequency used to “transmit” packet
4 bytes	Power	Power level used to “transmit” packet.
4 bytes	KLEM ID	Value between 0-255

IEEE 802.11 Channel Mappings

Channel	**Band, Frequency**	**Channel**	**Band, Frequency**
1	2GHz, 2417 GHz	34	5GHz, 5170 GHz
2	2GHz, 2422 GHz	36	5GHz, 5180 GHz
3	2GHz, 2427 GHz	38	5Ghz, 5190 GHz
4	2GHz, 2432 GHz	40	5GHz, 5200 GHz
5	2GHz, 2437 GHz	42	5GHz, 5210 GHz
6	2GHz, 2442 GHz	44	5GHz, 5220 GHz
7	2GHz, 2447 GHz	46	5GHz, 5230 GHz
8	2GHz, 2452 GHz	48	5GHz, 5240 GHz
9	2GHz, 2457 GHz	52	5GHz, 5260 GHz
10	2GHz, 2462 GHz	56	5GHz, 5280 GHz
11	2GHz, 2473 GHz	60	5GHz, 5300 GHz
12	2GHz, 2467 GHz	64	5GHz, 5320 GHz
13	2GHz, 2472 GHz	100	5GHz, 5500 GHz
14	2GHz, 2484 GHz	104	5GHz, 5520 GHz

/proc Interface

/proc/klem interface to configure the link emulation driver

Example: ad-hoc

```
#modprobe mac80211
#modprobe cfg80211
#insmod klem.ko
#echo “device = eth0” > /proc/klem
#echo “command = start” > /proc/klem
#/sbin/iwconfig wlan0 mode ad-hoc
#/sbin/iwconfig wlan0 essid 2
#/sbin/ifconfig wlan0 x.x.x.x
```

/proc Interface

Example: Mesh

```
#modprobe mac80211
#modprobe cfg80211
#insmod klem.ko
#echo “device = eth0” > /proc/klem
#echo “id = 10” > /proc/klem
#echo “filter = 30” > /proc/klem
#echo “command = start” > /proc/klem
#iw dev wlan0 interface add mesh type mp mesh_id loki
#ifconfig mesh x.x.x.x/24
```

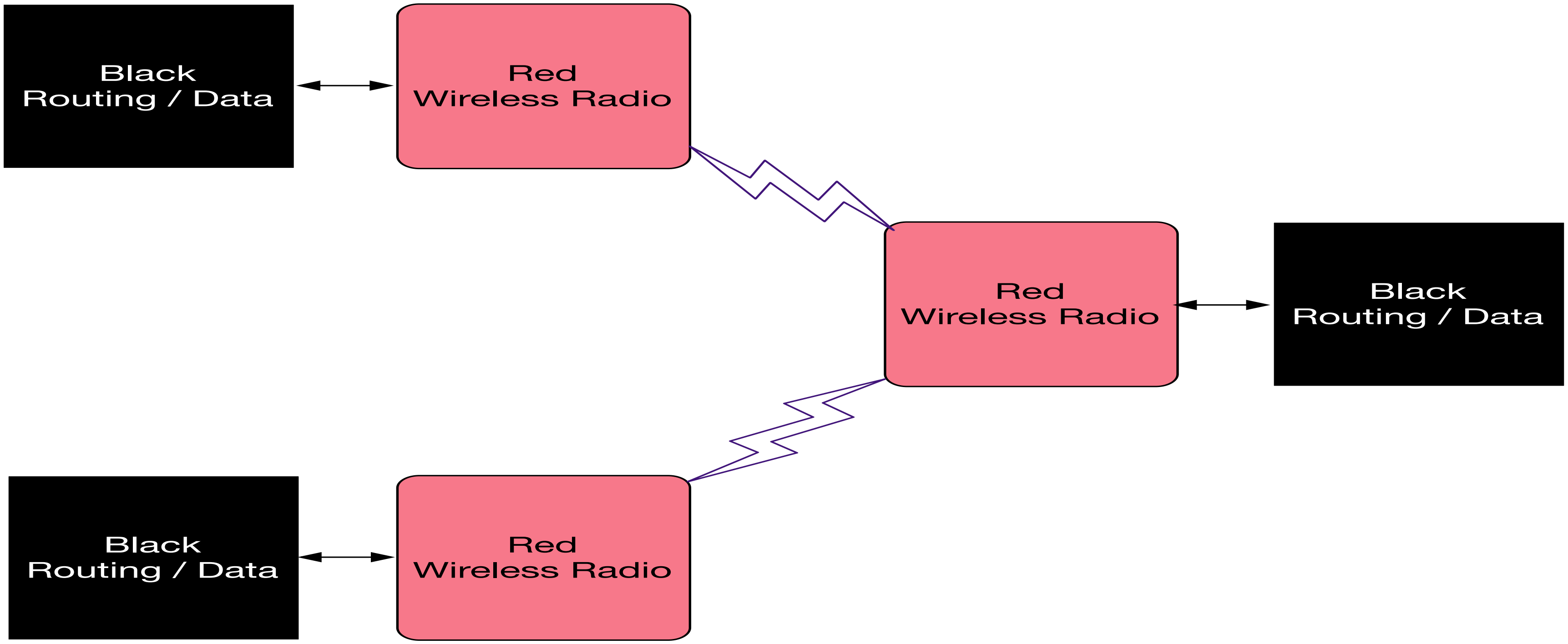
Distributed Link Emulation

- Useful for static network configurations
- Can simply add to network by activating virtual machines
- Allows for simulation of ad-hoc and mesh networks with minimal provisioning
- No central Link Emulation needed to coordinate specifics of each virtual machine

Red / Black Wireless Networks

Segregation in cryptographic systems

- Black:
  - Specifies classified processing, including routing done on secure devices
- Red
  - Work that can be done in on untrusted systems.



Target Uses

- Security
  - Examine security holes
  - Examine virus propagation
  - Network simulation
- Application Protocol Development
  - Audio
  - VoIP
  - Ad-hoc networking
- Automated System Testing