

# Mininet-WiFi

Redes de Ordenadores para Robots y Máquinas Inteligentes

GSyC

Departamento de Teoría de la Señal y Comunicaciones y  
Sistemas Telemáticos y Computación

Abril de 2024



©2024 Grupo de Sistemas y Comunicaciones.  
Algunos derechos reservados.  
Este trabajo se distribuye bajo la licencia  
Creative Commons Attribution Share-Alike  
disponible en <http://creativecommons.org/licenses/by-sa/4.0/deed.es>

- Mininet es un emulador de redes para Linux basado en SDN (**Software Defined Networking**). SDN es un nuevo paradigma en el campo de las redes de ordenadores donde se separa el plano de control (configuración de la red) del plano de datos (parte de reenvío de mensajes).
- El plano de control lo implementa un programa externo llamado **controlador** que se comunica con los dispositivos de la red a través del protocolo OpenFlow, consiguiendo la programación de los dispositivos de la red.

# Mininet-WiFi

- Mininet-WiFi está basado en Mininet y añade funcionalidad para dar soporte a enlaces inalámbricos.
- A partir de una topología determinada formada por APs y estaciones inalámbricas, Mininet-WiFi emula la comunicación de dichos dispositivos a través del protocolo 802.11.
- Existen topologías básicas predefinidas, pero lo habitual es arrancar una topología programada en python. En el siguiente ejemplo se arranca una topología predefinida un AP, ap1, y dos estaciones, sta1 y sta2.

```
sudo mn --wifi
*** Creating network
*** Adding controller
*** Adding stations:
sta1 sta2
*** Adding access points:
ap1
*** Configuring wifi nodes...

*** Adding link(s):
(sta1, ap1) (sta2, ap1)
*** Configuring nodes
*** Starting controller(s)
c0
*** Starting L2 nodes
ap1 ...
*** Starting CLI:
mininet-wifi>
```



sta1



ap1



sta2

- Mininet-WiFi ofrece una interfaz de comandos CLI que permite modificar la configuración y obtener información de la topología. Una vez arrancado mininet, la interfaz CLI se identifica con el prompt `mininet-wifi>`
- Para eliminar cualquier rastro de una ejecución previa de mininet: `sudo mn -c`

- La interfaz de comandos de Mininet-WiFi permite conocer el estado de la red:
  - `dump`: información de nodos, interfaces.
  - `net`: topología de la red
  - `links`: enlaces
  - `nodes`: nodos
  - `intfs`: interfaces
- Lanzar uno o varios terminales por cada estación:
  - `xterm <nombreEstación>`: lanza una ventana de terminal para ejecutar comandos en un estación.
- Monitorizar conectividad:
  - `pingall`: ejecuta la combinación de todos los pings posibles entre los dispositivos de esa topología, mostrando los detalles de cada ping.
  - `pingallfull`: ejecuta la combinación de todos los pings posibles entre los dispositivos de esa topología, mostrando solo los resultados finales.
- Ejecutar un comando en una estación determinada:  
`<nombreEstación> <cmd>`. Por ejemplo ejecutar en `sta1` la consulta de su tabla de encaminamiento: `sta1 route`.
- Salir `exit`

# Ejemplo de ejecución de comandos en CLI

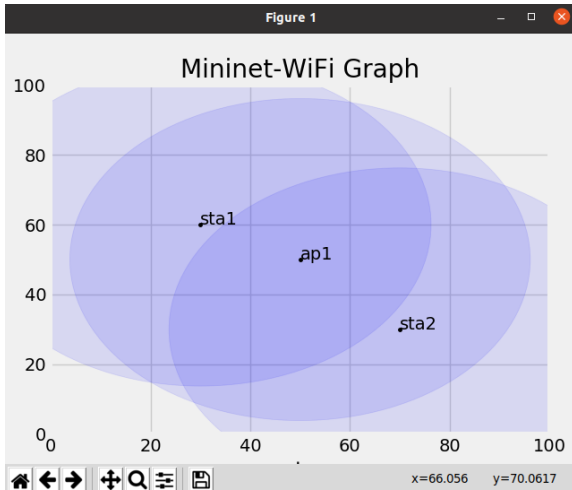
```
mininet-wifi> dump
<Controller c0: 127.0.0.1:6653 pid=9372>
<Station sta1: sta1-wlan0:10.0.0.1,sta1-wlan0:None pid=9379>
<Station sta2: sta2-wlan0:10.0.0.2,sta2-wlan0:None pid=9381>
<OVSAP ap1: lo:127.0.0.1,ap1-wlan1:None pid=9386>

mininet-wifi> pingall
*** Ping: testing ping reachability
sta1 -> *** sta1 : ('ping -c1 10.0.0.2',)
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.794 ms

--- 10.0.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.794/0.794/0.794/0.000 ms
sta2
sta2 -> *** sta2 : ('ping -c1 10.0.0.1',)
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.101 ms

--- 10.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.101/0.101/0.101/0.000 ms
sta1
*** Results: 0% dropped (2/2 received)
```

# Interfaz gráfica en 2 dimensiones



Posición(sta1)=(30,60)

Posición(sta2)=(70,30)

Posición(ap1)=(50,50)

# Información IP de las interfaces inalámbricas

- Las interfaces se nombran con el nombre de la máquina y wlan0, wlan1, etc. Por ejemplo para ver en sta1 la información IP de su primera interfaz sta1-wlan0:
- Desde la interfaz CLI:

```
mininet-wifi> sta1 ip addr show sta1-wlan0
29: sta1-wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc mq state DORMANT group default qlen 1000
    link/ether 00:00:00:00:00:11 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/8 brd 10.255.255.255 scope global sta1-wlan0
        valid_lft forever preferred_lft forever
    inet6 2001::1/64 scope global tentative
        valid_lft forever preferred_lft forever
```

- Lanzando un terminal para sta1 desde CLI: `mininet-wifi> xterm sta1` y ejecutando el comando desde ese terminal:

```
# ip addr show sta1-wlan0
29: sta1-wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc mq state DORMANT group default qlen 1000
    link/ether 00:00:00:00:00:11 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/8 brd 10.255.255.255 scope global sta1-wlan0
        valid_lft forever preferred_lft forever
    inet6 2001::1/64 scope global tentative
        valid_lft forever preferred_lft forever
```



# Información física de las interfaces inalámbricas

- Desde la interfaz CLI, con el comando `iw dev`:

```
mininet-wifi> sta1 iw dev
phy#11
  Interface sta1-wlan0
    ifindex 29
    wdev 0xb00000001
    addr 00:00:00:00:00:11
    ssid ssid1
    type managed
    channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412 MHz
    txpower 14.00 dBm
```

- O bien con el comando `iwconfig`:

```
mininet-wifi> sta1 iwconfig
lo          no wireless extensions.

sta1-wlan0  IEEE 802.11  ESSID:"ssid1"
    Mode:Managed  Frequency:2.412 GHz  Access Point: 00:00:00:00:00:01
    Bit Rate:12 Mb/s   Tx-Power=14 dBm
    Retry short limit:7   RTS thr:off   Fragment thr:off
    Encryption key:off
    Power Management:off
    Link Quality=34/70  Signal level=-76 dBm
    Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
    Tx excessive retries:0  Invalid misc:8  Missed beacon:0
```

# Realizar la asociación de una estación a un SSID

- Desde un terminal por ejemplo desde sta1 realizaremos la conexión al ssid ssid1:

```
iw dev sta1-wlan0 connect ssid1
```

- Si consultamos la información de la interfaz física, muestra que está asociado a un SSID y qué canal usa:

```
iw dev
phy#11
    Interface sta1-wlan0
        ifindex 29
        wdev 0xb00000001
        addr 00:00:00:00:00:11
        ssid ssid1
        type managed
        channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412 MHz
        txpower 14.00 dBm
```

```
iwconfig
lo          no wireless extensions.

sta1-wlan0  IEEE 802.11  ESSID:"ssid1"
            Mode:Managed  Frequency:2.412 GHz  Access Point: 00:00:00:00:00:01
            Bit Rate:12 Mb/s   Tx-Power=14 dBm
            Retry short limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:off
            Link Quality=34/70  Signal level=-76 dBm
            Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
            Tx excessive retries:0  Invalid misc:8  Missed beacon:0
```

# Eliminar la asociación de una estación a un SSID

- Desde un terminal por ejemplo desde sta1:

```
iw dev sta1-wlan0 disconnect
```

- Si consultamos la información de la interfaz física, ya no muestra que está asociado a un SSID ni el canal:

```
iw dev
phy#11
  Interface sta1-wlan0
    ifindex 29
    wdev 0xb00000001
    addr 00:00:00:00:00:11
    type managed
    txpower 30.00 dBm
```

```
iwconfig
lo          no wireless extensions.

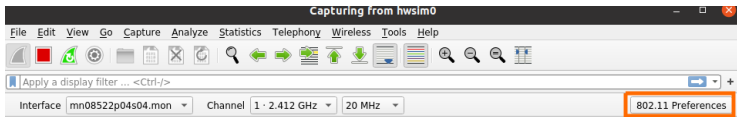
sta1-wlan0  IEEE 802.11  ESSID:off/any
            Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
            Retry short limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:off
```

# Interfaz para capturar 802.11

- Para poder capturar los paquetes con el protocolo 802.11 es necesario activar la interfaz que usa mininet-wifi para gestionar el tráfico inalámbrico.
- Desde la máquina real (fuera de mininet-wifi):

```
sudo ifconfig hwsim0 up
```

- Al lanzar Wireshark desde la máquina real (fuera de mininet-wifi) y seleccionar la interfaz hwsim0 podremos ver las tramas 802.11. Para capturar tráfico normalmente es necesario lanzar Wireshark con permiso de administrador (sudo). Wireshark tiene una barra de herramientas para tráfico wifi que se muestra desde el menú View → Wireless Toolbar y que permite acceder a la configuración rápida de este protocolo.



# Escaneo de redes inalámbricas visibles

- Para poder ver los SSIDs que una estación tiene disponibles desde su posición, se puede realizar un escaneo, buscando todos los posibles AP en todos los canales:

```
iw dev sta1-wlan0 scan
BSS 00:00:00:00:00:01(on sta1-wlan0) -- associated
    last seen: 42376.797s [boottime]
    TSF: 1615466590217747 usec (18697d, 12:43:10)
    freq: 2412
    beacon interval: 100 TUs
    capability: ESS ShortSlotTime (0x0401)
    signal: -76.00 dBm
    last seen: 0 ms ago
    Information elements from Probe Response frame:
    SSID: ssid1
    Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0
    DS Parameter set: channel 1
    ERP: Barker_Preamble_Mode
    Extended supported rates: 24.0 36.0 48.0 54.0
    Supported operating classes:
        * current operating class: 81
    Extended capabilities:
        * Extended Channel Switching
        * Multiple BSSID
        * SSID List
        * Operating Mode Notification
```

# Tráfico 802.11

- Además de la trama 802.11, Wireshark muestra metadatos asociados a información del driver de la tarjeta inalámbrica. Esta información no viaja por el canal sino que se extrae de las características de la señal recibida y se muestra en Wireshark debajo de las siguientes pestañas:

```
▼ Radiotap Header v0, Length 22
  Header revision: 0
  Header pad: 0
  Header length: 22
  ▶ Present flags
    MAC timestamp: 1615460191860784
  ▶ Flags: 0x00
    Data Rate: 1,0 Mb/s
    Channel frequency: 2457 [BG 10]
  ▶ Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
▼ 802.11 radio information
  PHY type: 802.11b (HR/DSSS) (4)
  Short preamble: False
  Data rate: 1,0 Mb/s
  Channel: 10
  Frequency: 2457MHz
  TSF timestamp: 1615460191860784
  ▶ [Duration: 872µs]
```

- Dependiendo del driver, podría dar información sobre la potencia de la señal recibida, los siguientes valores son una indicación de cómo es la señal:
  - 90 dBm: señal muy débil
  - 70 dBm: señal aceptable
  - 67 dBm: señal buena
  - 55 dBm: señal muy fuerte
  - 30 dBm: señal muy cerca del transmisor.