Redes IP y claves SSH

Configurar IP estática y generar claves

Equipo docente ClústerLab

6 de agosto de 2025

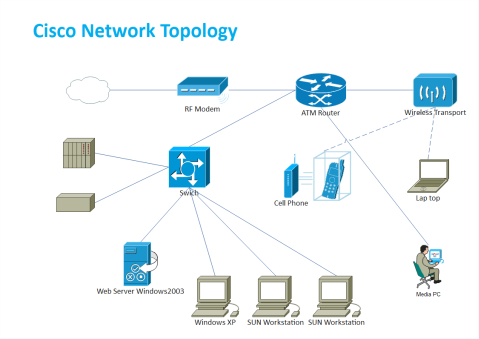
Los computadores y otros dispositivos, para comunicarse entre ellos, necesitan una especie de nombre, que sería la *ip address*, o dirección ip (ip: internet protocol).

La forma más común de ip es la IPv4 (ej: 192.168.0.155).

La ip se la da la entidad que esté por encima del dispositivo, entonces, un celular recibe su ip de el router o de la antena 4G/5G. El router y la antena reciben su ip de la ISP (internet service provider), como Claro o Movistar. Y estas ISP reciben sus ips de organismos mundiales (LACNIC <- ICANN/IANA)

Generalmente, se le asigna una IP única a cada dispositivo. Y, generalmente, esa IP se mantiene a lo largo del tiempo. Para ver la ip que uno tiene, en linux:

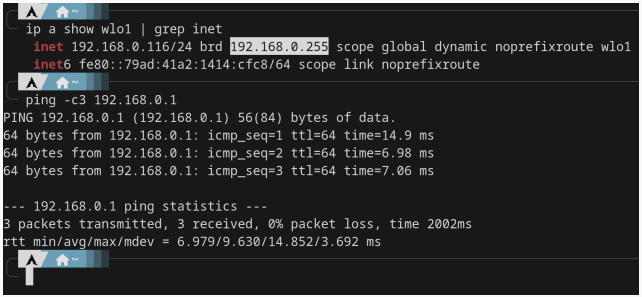
```
$ ip a
```



Verificar conectividad

```
$ ip addr show eth0 | grep 'inet '
$ ping -c3 10.0.0.1
```

- Confirma que la IP asignada se muestre en `inet`.
- Un par de `ping` verifica la ruta al gateway.



Nota

las ip que terminen en `.0`, `.1` o `.255` suelen ser reservadas. Intentar no molestar esas IPs

- red: `x.x.x.0`
- router: `x.x.x.1`
- todos: `x.x.x.255`

Nota

Intentar usar el comando `ping` siempre con `-c4` u otro número bajo. Sino, se quedará ejecutando hasta que sea interrumpido.

```
ping -c4
```

Probar acceso SSH

```
$ ssh pi@10.0.0.21 hostname
$ ssh pi@10.0.0.21 hostnamectl
```

Si la autenticación funciona, verás el nombre de tu Pi en la salida.

```
# Opcional en ~/.ssh/config
Host rpi21
  HostName 10.0.0.21
  User pi
```

Entonces basta con ejecutar:

```
$ ssh rpi21
```

Útil para conexiones frecuentes o contraseñas complejas. Sólo necesitas usar la contraseña una única vez.

1. Primero, generar claves, una pública y una privada.

```
$ ssh-keygen -t ed25519
```

2. Generará 2 archivos,
   - `~/.ssh/id_ed25519` clave **privada**. Nunca compartir.
   - `~/.ssh/id_ed25519.pub` clave **pública**. Esta se copiará al servidor.
3. Usar el commando `ssh-copy-id` para copiar la clave pública al servidor.

```
$ ssh-copy-id pi@10.0.0.21
```

4. Se te pedirá la contraseña una única vez, y la clave pública será añadida a `~/.ssh/authorized_keys` del servidor.

```
# Genera un par RSA de 4096 bits con comentario
$ ssh-keygen -t rsa -b 4096 -C "tu@correo"
# Copia la clave pública a la Raspberry Pi
$ ssh-copy-id pi@10.0.0.21
```

Nota

La autenticación sin contraseña simplifica el uso de `scp` y `rsync`. Protege tu clave privada (`~/.ssh/id_rsa`) con permisos 600.

Puertos Comúnes

- `21` es el puerto ftp (file transfer)
- `22` es el puerto ssh (conexión remota)
- `80` es el puerto http (página web)
- `443` es el puerto https (página web segura)

Descubrir vecinos con nmap

Instala la herramienta y explora quién está conectado:

```
$ sudo apt install -y nmap
$ nmap -sn 10.0.0.0/24          # escaneo rápido de hosts
$ nmap -p 22 --open 10.0.0.0/24 # encontrar servicios SSH activos
```

- La opción `-sn` (ping scan) lista IP y latencias.
- Usa `-p` para verificar puertos específicos como SSH.

Opciones útiles de nmap

```
$ nmap -A 10.0.0.0/24       # detección de servicios y SO
$ nmap --open -p 80 10.0.0.* # buscar servidores web
```

- `-A` entrega información detallada y requiere más tiempo.
- Limita el rango si la red está muy concurrida.