

Índice

Objetivo de la práctica

Los objetivos de la práctica son:

- Comprender los conceptos necesarios para implantar una VLAN
- Configurar un router con NAT para exponer un servicio
- Configurar una VPN con SSH
- Ayudarse de un acceso remoto auxiliar

La última versión de esta práctica está disponible en [este enlace](#).

Diagrama general

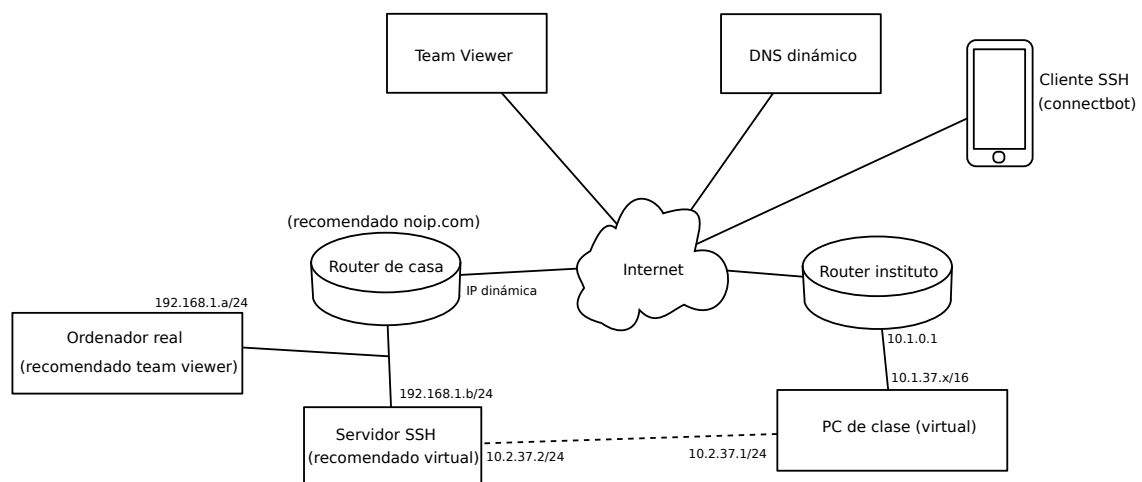


Figura 1: Diagrama general de la práctica

- Se creará una VPN entre un ordenador del aula y un ordenador en el domicilio del estudiante.
- Se supone que el ordenador real del domicilio es Windows
- Las máquinas virtuales serán Linux
- El ordenador en el domicilio será una máquina virtual (para mayor seguridad)
- La práctica se puede realizar fuera de clase, utilizando un móvil como punto de acceso desde un ordenador

(Opcional) Team Viewer en el ordenador real de casa

Durante el desarrollo de la práctica, puede ser necesario reconfigurar los ordenadores de casa o el propio router. Para ello hay varias opciones

1. El alumno configura su casa y luego acude a clase a configurar el resto. Si tiene que hacer algún cambio en casa vuelve allí.

2. La práctica se hace por parejas. Un alumno está en su casa y otro en el instituto.
3. Se configura solo el *Remote Desktop* al ordenador real, y se abre el puerto 3389 para poder acceder desde Internet.
4. **(Preferida)** Se instala Team Viewer en casa, que no necesita abrir ningún puerto, y se controla el PC real de casa en caso necesario.

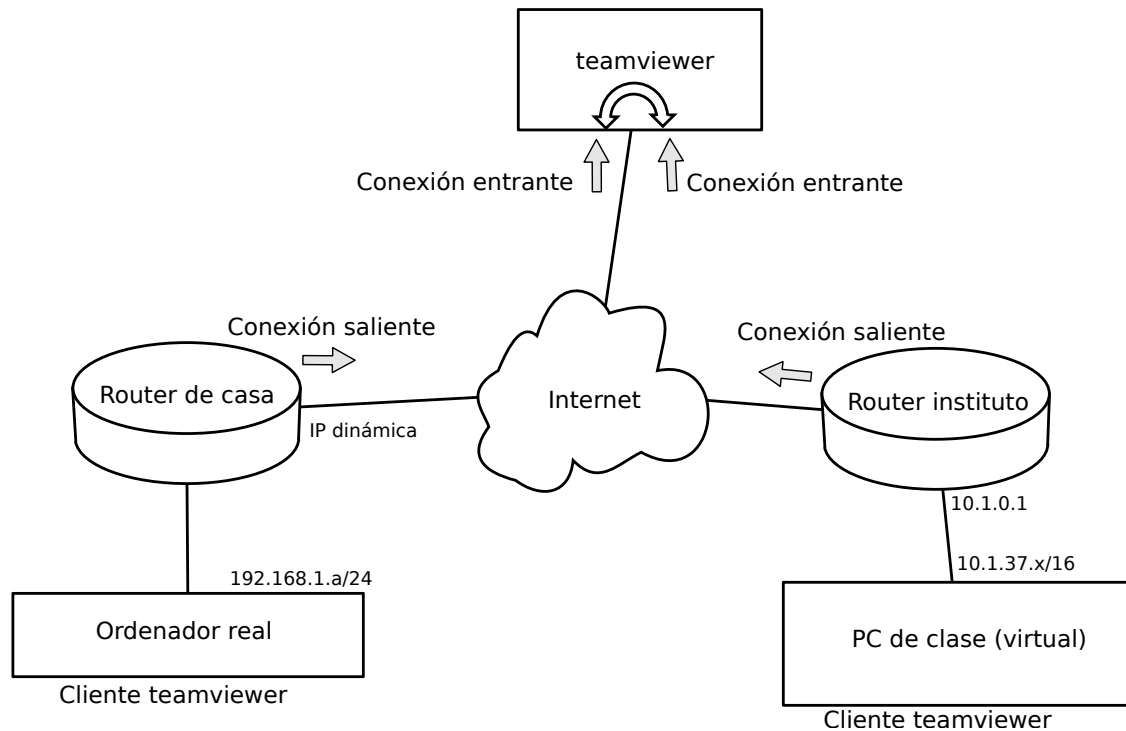


Figura 2: Diagrama general de la práctica

Aviso

- Si se opta por utilizar Remote Desktop, se debe utilizar una contraseña suficientemente segura.
- Se recomienda que el puerto externo de Remote Desktop no sea 3389, para evitar algunos ataques.

IP externa del router de casa

Hay varias opciones para conocer la IP externa del router de casa:

1. Desde un navegador de casa, visitar la página <http://www.cualesmiip.com/>. Dará la IP de ese momento, que puede cambiar en pocas horas.
2. **(Preferida)** Crear una cuenta de un [DNS dinámico](http://www.noip.com), como <http://www.noip.com>. Después, ejecutar un programa en la LAN que comunique automáticamente al DNS vuestra dirección IP
 - Algunos routers traen ya este programa instalado ([enlace a ejemplo](#))
 - También se puede instalar un [programa para actualizar la IP](#) en la máquina real Windows

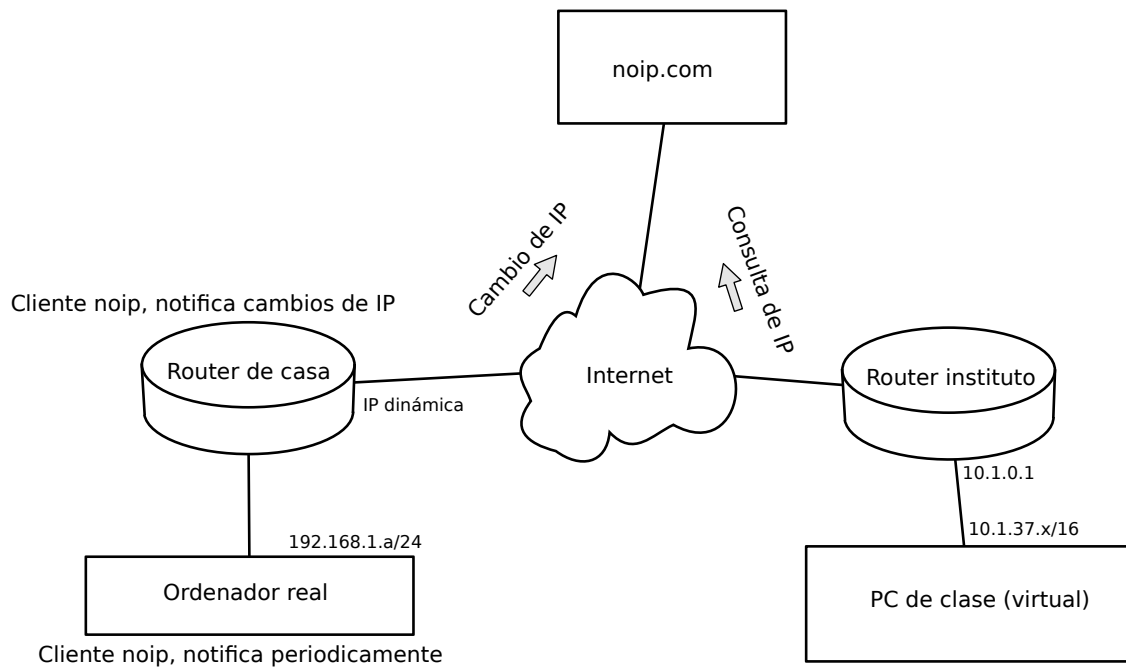


Figura 3: Funcionamiento DNS dinámico

Servidor SSH

- Se recomienda que sea una máquina virtual Linux
- Debe configurarse con IP fija dentro de la LAN de casa
- Se instalará openssh-server, con la configuración por defecto
- En el router, debe abrirse un puerto para el servidor SSH
 - Cada router de cada compañía telefónica es distinto
 - Los clientes de telefónica utilizan el [Portal Alejandra](#).
- Para comprobar que se ha abierto correctamente, puede utilizarse una [aplicación de cliente SSH](#) desde el móvil, accediendo por 3G (sin wifi)

Aviso

- Las contraseñas del servidor SSH deben ser **seguras**. Estará expuesto a Internet.
- Se recomienda que el puerto abierto para SSH no sea el 22, para evitar algunos ataques.
- Se debe contar con el **permiso de los padres** para modificar el router de casa.

VPN

El servidor SSH se debe configurar con las siguientes opciones en su fichero `/etc/ssh/sshd_config`:

```
PermitRootLogin yes
PermitTunnel yes
```

Listado 1: Opciones para el servidor SSH

1. Se creará una conexión VPN entre el ordenador del aula y el servidor SSH
2. Se asignarán las siguientes direcciones IP en las interfaces TUN
 - Aula: 10.2.37.1/24
 - Servidor SSH: 10.2.37.2/24

Tras esto, debe haber comunicación directa (1 salto IP) entre el servidor SSH y el PC del centro.

Acceso a la LAN desde el centro

1. El ordenador de clase añadirá una ruta para acceder a la red 192.168.0.0/16 a través de 10.2.37.1

```
route add -net 192.168.0.0/16 gw 10.2.37.2
```

Listado 2: Enrutamiento desde el aula a casa

2. El servidor SSH realizará NAT, de forma que el PC de clase sea enmascarado por el servidor SSH, y el resto de PCs de la LAN de casa puedan responderle

```
sudo iptables -t nat -A POSTROUTING -s 10.2.37.0/24 -o eth0 -j MASQUERADE
```

Listado 3: NAT para acceder a la LAN

Como resultado, el ordenador de clase debe acceder a todos los ordenadores de la LAN de casa.

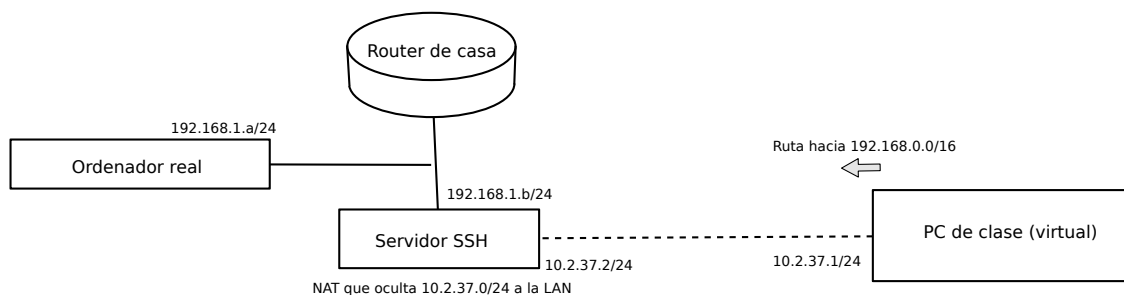


Figura 4: Enrutamiento y NAT para acceso a red de casa

Normas de entrega

- La entrega se realizará en el Aula Virtual
- Se entregará un fichero PKT que pueda abrirse con la versión 7.1 de Packet Tracer.
- Los equipos identificarán en su etiqueta su IP, y su pertenencia a algún departamento o función.

Qué se valorará

- Que se respeten los dominios de difusión (**3 puntos**)
 - Se entiende que dos equipos *no comparten dominio de difusión* si un broadcast de Ethernet (por ejemplo, ARP) no consigue viajar entre ellos en ninguno de los sentidos.

- Que se incluyan etiquetas identificativas en cada equipo (**1.5** puntos)
- Que los departamentos puedan comunicarse a través de la capa 3 (**2** puntos)
- Que se rellene correctamente la tabla de documentación de la red (**2** puntos)
- **No se valorará** el ejercicio si las direcciones IP no son de la subred 10.N.0.0/16.