DÍA 1 (Resetear, Perfiles, Actualizar/Downgradear, Crear usuarios,...)

RESETEAR ROUTER MIKROTIK

1. Quitar alimentación
2. Pulsa el botón reset (con la mina de un boli,...)
3. Dar alimentación
4. Esperar 10 segundos
5. Una luz empieza a parpadear, justo ahí deja de pulsar porque si no entra en otro modo que no es el reset

CONECTAMOS EL CABLE DEL ORDENADOR DE CLASE AL ether1 (INTERNET) DEL ROUTER Y EL LATIGUILLO DESDE EL ether2 DEL ROUTER AL ORDENADOR

AÑADIR PERFIL AL ORDENADOR

Clic arriba a la derecha -> Configuración de red cableada -> +

Le podemos poner IP fija, DHCP,... Y podemos cambiar de uno a otro fácilmente

PARA VER CONFIGURACIÓN DEL ADAPTADOR EN LINUX: ip a

CONTRASEÑA POR DEFECTO DE MI ROUTER (14): EKIVDHFW4I

ENTRAR AL ROUTER:

- Desde el acceso directo del Winbox: Ponemos IP o MAC del router, usuario (admin) contraseña y entramos
- Poner IP del puerto de enlace (el router) en el navegador: Y lo mismo.

ACTUALIZAR ROUTEROS:

System -> Packages -> Check for updates -> Download&Install

En el cuadro de abajo (changelog) está el registro de cambios que es importante leerlo antes de actualizar para saber qué cambios trae la actualización y si ésto afecta a la configuración que tenemos en algo.

Los channel:

- long term = versiones que van a salir cada mucho tiempo sin añadir una nueva funcionalidad.
- stable = ciclo de vida de meses. Si es la 7.14.2 por ejemplo, hasta que no cambie el 14 o el 7 no veremos nuevas funcionalidades.
- testing = para probar las nuevas versiones que van sacando (beta tester).
- development =

https://mikrotik.com/download/changelogs

ACTUALIZAR:

System -> RouterBOARD -> Upgrade
System -> Reboot

CONFIGURAR ACTUALIZACIÓN AUTOMÁTICA:
System -> RouterBOARD -> Settings

- factory firmware: el firmware de fabrica (si no va el que tenemos arrancar desde éste con reset).
- current firmware: el que tenemo.

ACTUALIZAR MANUALMENTE:
- https://mikrotik.com/download/archive
- Descargamos la versión (Comprobar que es x64, arm64, .npk,... y todo eso). Tanto la npk como la all packages .zip
- Arrastras al WinBox lo que quieres así a lo bruto (wifi-qcom, routeros,...) (si es en navegador *files->examinar*)
- Si el paquete es superior a la versión instalada hacer reboot y se instala
- Si el paquete es inferior a una versión instalada al hacer reboot no se instala, ¿como fuerzo el downgrade? *System -> Packages -> Downgrade*

Lo puedo subir con ftp, ssh,...

PROHIBIDO DECIR NO TENGO INTERNET:
Tener Internet hay que desglosarlo en:
- ¿Tengo conectividad e IP? Hacer *ping a una IP conocida* como la 8.8.8.8
- ¿Tengo resolución DNS? Hacer *ping a www.google.es* tal cual

NET INSTALL
- SOLO SE PUEDE HACER CON EL ether1.
- ¿Pero es el que usamos para tener Internet no? Pues cambia el puñetero cable.
- Vamos a https://mikrotik.com/download y descargamos el NetInstall para Linux (la de la izquierda la estable).
- Lo descomprimimos.
- En la carpeta de netinstall que acabamos de extraer metemos todos los ficheros que queremos usar para actualizar.
- Recuerda tener el perfil ip fija y tener conectado SOLO el ordenador al router por el ether1.
- Desconecta el router de la alimentación.
- Abrimos la terminal en la carpeta de netinstall y usamos el comando: *sudo ./netinstall-cli -i enp5s0 <Ficheros que queremos para actualizar>*
- Pulsamos el botón reset y ponemos la alimentación.
- Cuando ponga "Detected client architecture: arm64" ya puedes soltar el reset.

DESDE ether1 NO SE PUEDE CONFIGURAR EL ROUTER POR SEGURIDAD ESTÁ PUESTO ASÍ.

reset -> keep users

RESETEAR DESDE COMANDOS
system/reset-configuration no-default keep-users

EN RESUMEN, PODEMOS…
…Actualizar
- Desde el botón Check for updates.
- Manualmente.

- Con netinstall.

…Downgrade
- Manualmente.
- Con netinstall.

…Instalar paquetes
- Manualmente.

…Reset de la Configuración
- Por botón.
- Desde comando/menú winbox.
- Mantenimiento de usuarios.
- Reset Configuration - /Keep users /No Default configuration.

ABRIR TERMINAL: New Terminal

VER INTERFACES: Interfaces (deshabilita wifis para que no se nos estén conectando).

VER USUARIOS: System -> Users
- Vamos a crear un usuario: *System -> Users -> + -> Le ponemos nombre, contraseña y del grupo "read"*

Si entramos con este usuario no podemos hacer nada en **IP -> Addresses (por ejemplo) que es donde se ven las ips asignadas**, ni habilitar interfaces ni nada.

Los grupos que hay:
- read
- full
- write

Podemos gestionar los grupos

También podemos darle clic derecho a un usuario si somos de administración y darle a "expire password" para que deba cambiarla en el siguiente inicio de sesión.

Es habitual en empresas grandes que haya un usuario admin con una contraseña enorme y que cuando llegue yo ese me da un usuario. Cada uno su usuario para saber quien la caga.

DÍA 2 (Configuración por defecto, Cambiar nombre, Listas, “Tener Internet”, Neighbors, Poner IP 10.0.14.254/24, Copias de seguridad, import/export)

CONFIGURACIÓN POR DEFECTO QUE TIENEN LOS ROUTER
- Cliente DHCP en ether1.
- Bridge ether2-ether4.
- Loopback.
- IP 192.168.88.1/24 en bridge.

- Servidor DHCP en bridge.
- Reglas de FW que impiden configurar el router desde el ether1.
- NAT para que la red interna (192.168.88.0/24) salga a Internet usando la dirección IP pública adquirida por DHCP en ether1 (Es decir, la red 88.0/24 queda enmascarada detrás de la IP 192.168.27.x que el router coge en clase).

Configuración por defecto != Configuración en blanco

CAMBIAR NOMBRE AL ROUTER:
System -> Identity y le pongo 14-Lolo

PARA QUE NUESTRO ROUTER TENGA 'INTERNET':
1. Necesito una IP, un Gateway y un servidor DNS
2. Comprobar ping al gateway
3. Comprobar ping al servidor DNS
4. Comprobar ping a un dominio

Probar desde el ordenador y desde el router.

LISTAS
Puedo agrupar los interfaces en listas y así hacerle configuraciones simultáneas
Interfaces -> Interfaces List

PROTOCOLOS DE DESCUBRIMIENTO
- LLDP: Link Layer Discovery Protocol
- CDP: Cisco Discovery Protocol
- MNDP: MikroTik

Cada cierto tiempo mandan un mensajito y si un vecino lo recibe y lo entiende ya se conocen

VER A LOS PANAS:
IP -> Neighbors -> Discovery Settings -> Marcamos all -> Ok

==========

EJERCICIO: CAMBIO EN LA IP DE NUESTRA RED INTERNA
Antes: 192.168.88.1/24
Después: 10.0.nRouter.1/24

1. New Terminal y le **cambio la IP al bridge** con: *ip/address/set 0 address=10.0.14.1/24*

(Nos desconecta porque estábamos conectados por IP y la hemos cambiado, para evitar ésto conectarnos por MAC).

2. Creamos un perfil nuevo en conexión cableada (enps50) de nuestro ordenador con:
- IP = 10.0.14.2/24
- Gateway = 10.0.14.1

3. Borramos el pool, el dhcp server y el dhcp-server network:
   ip/pool/remove 0
   ip/dhcp-server/remove 0

ip/dhcp-server/network/remove 0

4. Y pongo un nuevo DHCP-server:
   [admin@14-Lolo] > ip/dhcp-server/setup
   Select interface to run DHCP server on

   dhcp server interface: bridge
   Select network for DHCP addresses

   dhcp address space: 10.0.14.0/24
   Select gateway for given network

   gateway for dhcp network: 10.0.14.1
   Select pool of ip addresses given out by DHCP server

   addresses to give out: 10.0.14.2-10.0.14.254
   Select DNS servers

   dns servers: 8.8.8.8
   Select lease time

   lease time: 1800

5. Ahora en Linux elijo un perfil con IP automática y le pone la 10.0.14.254

==========

COPIAS DE SEGURIDAD

Files -> Backup -> Bakcup
(Es aconsejable ponerle contraseña porque tiene información sensible)

Bakcup es un fichero binario que **solo sirve en el mismo mismísimo router**. NO SIRVE EN OTRO ROUTER AUNQUE SEA IGUAL.

Puede ser que suceda lo peor: que algo parezca que funcione pero en verdad no o no siempre. Por ejemplo:

- Que ambos routers restaurados con el mismo backup adquieran la misma MAC y que al funcionar juntos haya conflicto.
- Que el router confunda los interfaces, y se crea que ether2 es ether5 y así.

Creamos un backup "14-Lolo-ConfiguraciónInicial" y lo descargamos: *Clic derecho -> Download*

Si pasa algo restauro la copia con netinstall y listo.

"USAR" UNA COPIA DE SEGURIDAD EN OTRO ROUTER

Usamos el comando *export*, el cual nos muestra todos los comandos que nos llevan desde la configuración inicial hasta la final.

export por seguridad no importa usuarios, ni contraseñas, ni certificados digitales,...

==========

EJERCICIO: Exporta los datos del backup que hicimos incluyendo datos sensibles (usuarios, contraseñas,...)

export file=14-Lolo-ConfiguraciónInicial show-sensitive

==========

import es otra forma de llevar los comandos de un export a la línea de comandos en lugar de uno en uno.

Nota: Se pueden poner scripts que se ejecuten automáticamente tras un reset.
Nota2: Hay veces que se empieza a ejecutar el script antes de que se cargue parte del SO del router. Poner un delay de tiempo al principio del script.

DÍA 3 (Rutas, DHCP Server, DNS)

TODA LA INFO QUE VEMOS EN CLASE ESTÁ EN: help.mikrotik.com/docs

PARA CAMBIAR UN SERVIDOR DHCP HAY QUE:

- Borrar el servidor DHCP */ip/dhcp-server/remove* …
- Borrar la network */ip/dhcp-server/network/remove* …
- Borrar el pool */ip/pool/remove* …
- Borrar la IP 192.168.88.1/24 del bridge
- Asignar la nueva IP 10.0.X.1/24 al bridge
- Ejecutar */ip/dhcp-server/setup* sobre el bridge

CRITERIO DE SELECCIÓN DE RUTAS:
Una ruta es un destino con un gateway y una distancia.
Un router tiene configuradas muchas rutas.
Si un router tiene varias rutas al mismo destino, se elige la de menor distancia.
Si hay varias rutas a un mismo destino con igual distancia, ECMP.

NOTA: Si hay un bajo ancho de banda no se puede hacer interfaz remota, la única forma es llamar por teléfono.
NOTA: No confundir con Prioridad que se usa para colas, ni con Coste que es otra cosa.

ECMP = Cuando hay varios caminos unos van por un lado y otros por otros indistintamente (Elegidos a través de un Round-Robin,...). Corremos el riesgo de que los paquetes lleguen desordenados.

Jitter = Unidad de medida del desorden de los paquetes.

Añadir ruta: *IP -> Routes -> + -> ponemos dst-address y gateway -> Aceptar*

NOTA: Para saber si funciona el cable ir a Interfaces y ver si el ether tiene una R a la izquierda.

Cambiar distancia a la ruta: *DHCP-Client -> Doble click a la ruta -> Ponemos un valor en el Default Route Distance -> Ok*
En este momento se desactiva la ruta por defecto 192.168.27.1

Cambiar distancia a la ruta: *DHCP-Client -> Doble click a la ruta -> Check Gateway y elegimos PING*

Con esto el router hará ping al Gateway de esa ruta cada 10 segundos. Al segundo ping que falle la desactiva y coge otra de Distancia mayor si la hay.

Alomejor no queremos que se asigne una ruta por defecto cuando cae otra:
Cambiar distancia a la ruta: *DHCP-Client -> Doble click a la ruta -> DHCP -> Desmarcamos Add Default Route*

Puede ser que le cambie la tarjeta y por tanto la MAC, para poder seguir reconociendo el equipo le pongo un clientid que no cambia nunca.
DHCP-Client -> Doble click a la ruta -> Advanced -> Client id

DHCP-SERVER
Nos permite asignar configuración de red a los equipos que lo soliciten.

IP -> DHCP Server

Si hacemos doble click en un DHCP-Server concreto nos aparecen varias pestañitas:
- Script: Podemos poner un script que se ejecute automáticamente cuando se inicie, por ejemplo que me envíe un mensaje al Telegram cuando se conecta alguien.
- General: Vemos que tiene muchas cositas en General
- Queues: podemos ponerle Queues para limitar ancho de banda a los que se conecten por ejemplo

Cuando un DHCP-Server va a asignar una IP a un cliente se va a la pestañita networks y según la que le va a signar mira en una u otra

IP->DNS
Se encarga de, cuando le doy un nombre de dominio, buscar la IP correspondiente.

Por defecto usa el 8.8.8.8

Si le pongo en Servers el 1.1.1.1 usará este, ya que predomina lo manual sobre lo automático.

Nota: Las compañías proporcionan sus DNS para resolver nombres de dominio a sus clientes. Cada cierto tiempo reciben listas de nombres de dominio que no pueden visitar. Cuando el cliente intenta entrar en vez de resolver el nombre les deja colgados. Podemos sortear esto usando otro DNS.

DNS Resolver:
Si tenempos dominio1.dominio2.dominio3.es.com
Resuelve de forma recursiva desde el com hasta el dominio1.
Pregunta a un conjunto de DNS quien sabe resolver .com, estos preguntan quien sabe resolver .es ,... y así hasta dominio1.
Más costoso

DNS Relay:
Como el router, pasa la pelota a otro.
Más ligerito.

Si pongo en el ordenador el perfil automáticos con DNS automático coge tanto el router 10.0.14.1 como el 1.1.1.1

Si voy a *DNS -> Settings y desmarco "Allows Remote Requests"* **el router deja de ofrecerse a sí mismo como DNS** y ahora si pongo en el ordenador el perfil automáticos con DNS automático coge solo el 1.1.1.1

¿Que servidores DNS proporciona el servidor DHCP? En este orden:
0. ¿Esta marcado "no DNS" en la configuración Network del DHCP Server? Si es que si no va ninguno
1. ¿En la configuración de la red hay servidores DNS? Si es así: sólo se ofrecen esos.

En caso de que "No DNS" no esté marcado y que no haya DNS en la configuración de red:
2. ¿El router permite peticiones DNS? Si es así se ofrece
3. ¿El router tiene DNS dinámico?
   3a. Sí: Se ponen en orden
   3b. No: El router tiene servidores DNS estáticos configurados?
      3b1: Se ofrecen en el orden que llegan

El DNS depende de muchos "hilos" hay que saber entenderlos y jugar con ellos.

Quitar DNS: *IP -> DHCP Server -> Network -> Doble click en uno -> Marco "No DNS"*

En *IP->DNS* puedo añadir varios DNS ("Servers")

DÍA 4 (DHCP-Server, ARP, DNS)

ARP: Address Resolution Protocol
DHCP: Dynamic Host Configuration Protocol
DNS: Domain Name Server

DNS: Nos permite manejar 'nombres de dominio' en lugar de direcciones IP. Así cuando en el navegador escribimos www.google.es, pues el navegador va directamente a la IP de google. DNS es quien hace la búsqueda www.google.es <-> 142.250.184.3

Si yo sé que tengo que comunicar con www.google.es y no conozco su IP,
- Envío una consulta DNS a mi servidor DNS: ¿quien es www.google.es?
- El servidor DNS me responde: www.google.es es 142.250.184.3

ARP: Permite encontrar la dirección MAC de un equipo del que conocemos su IP.
NOTA: En la red local, los envíos se hacen en "CAPA 2", usando tramas ETHERNET que usan DIRECCIONES MAC de ORIGEN Y DESTINO y esas tramas, en su interior, llevan los PAQUETES IP con DIRECCIONES IP SRC y DST.

DHCP-SERVER
Pool: Conjunto de direcciones IP disponibles para asignar dinámicamente (en el caso actual, por DHCP... pero hay otros casos que ya veremos) y que además lleva el seguimiento de las direcciones asignadas (para no asignar varias veces la misma IP).

Si configuramos DHCP-SERVER con STATIC-ONLY (en lugar de un pool), sólo ofreceremos direcciones IP a los equipos que tengan una asignación estática en DHCP-SERVER - LEASES.
¡¡¡ Es una medida (simple) de protección de acceso a la red !!!

Pero... si el equipo que se conecta, que no tiene asignación de IP, se configura una dirección IP adecuada, con su GW y su DNS...
¡¡¡ La medida de seguridad es una m....a !!!

==========

EJERCICIO

1. **Asigna un STATIC-LEASE a tu equipo: 10.0.x.123.**
2. **Asegúrate de que sólo hay un LEASE (la de tu equipo).**
3. **Cambia el DHCP-SERVER y ponlo STATIC-ONLY.**
4. **Tu compañero/a se conecta a tu router: no obtiene IP.**
5. **Tu compañero/a asigna a su ordenador una IP adecuada a tu red: tiene acceso a internet.**
6. **Te sientes decepcionado: pensabas que proteguías tu red, pero no es así.**
7. **Piensa en dejar los estudios, los ordenadores, retirarte a un desierto lejano... :(**
8. **Pero te acuerdas del ARP.**
9. **En el DHCP-SERVER marcamos ADD ARP FOR LEASES.**
10. **En el interfaz BRIDGE configuraremos ARP: Reply-only.**
11. **Comprobamos que el/la listillo/a ya no tiene acceso a internet.**
12. **Ja ja ja ja jaja (risa malvada) (tengo mieo).**
13. **Tras las risas: volvemos a dejar todo casi como estaba:**

- **Nos aseguramos que el bridge tiene ARP: enable.**
- **En DHCP-SERVER desactivamos ADD ARP FOR LEASES y volvemos a poner el pool.**
- **Eso sí: Mantenemos el STATIC LEASE 10.0.X.123 a nuestro equipo.**

1. Nos vamos a IP-DHCPserver-leases y le damos a Make Static. Aquí quitamos el cliente-id y ponemos la 123 arriba, vemos que se cambie la IP.
2. Volvemos a dhcp-server y le damos doble click. Ponemos en address pool -> static-only (solo se conectan aquellos equipos que yo haya decidido) para poder conectarte a la red de tu compañero (coge ip)
3. Nos creamos un perfil nuevo con IP dentro del rango de la IP del compañero. En este caso la IP normal es 10.0.106.1 y pnemos la 123 que está dentro del rango

Aquí deberiamos tener internet

4. IP -> ARP (establece relación entre IP y MAC) manos mensaje a determinado IP,necesito la MAC y aqui en list aparecen,si no aparece para eso sirve la ARP para buscarla.
5. dhcp-server -> marcamos la casilla ADD ARP FOR LEASES
6. En interface bridge-> reply only
7. Cambiamos los cables de red por el del compañero,nos ponemos otra vez en su perfil y no nos dejará tener internet ya que esta vez lo ha prohibido

==========
==========

Ejercicio: Tu compi se conecta a tu router.

1. Haz ping a su dirección. Comprueba que OK.
2. En tu router, desactiva todas las reglas de Ip firewall-filter.
3. Crea una regla de FW: chain=forward protocol=icmp action=drop dst-address=10.0.x.123 (tu equipo).
4. Comprueba que tu compi puede hacerte ping aunque la regla de FW lo impida".
5. En bridge en el botón settings, activa la opción "use firewall".
6. Comprueba que ahora no puede hacerte ping.

IP -> Firewall y borramos todas (la primera no nos dejará).
==========

DÍA 5 (Bridge y Firewall)

SOC -> System On a Chip. En un solo circuito integrado se meten muchas cosas.

Nuestro router tiene en un chip: 1 CPU de 4 núcleos, 2 tarjetas de red y un switch
Esto se conecta a la RA, a los LEDs, a los amplificadores y a un PHY (que se interconecta los puertos ether y el switch del SOC).

Si creamos un bridge bien, la función del switch la realiza el switch del SoC => Mejor rendimiento

Bridge -> Pestaña "Ports" -> Doble click en un interfaz -> Pestaña "General" -> Opción Hardware Offload ("HW Offload"):

- Si desmarco HW Offload -> la función del bridge la hace la CPU siempre (software)
- Si marco HW Offload -> La función del bridge la hará el hardware siempre que se den las condiciones necesarias.

Estas condiciones son:

- El dispositivo tiene un switch-chip integrado con los puertos directamente conectados (ver diagrama de bloques del dispositivo).
- Solo puede haber creado un bridge por cada switch chip.

1. El switch coge la MAC de la traza que le llega y apunta por dónde le ha llegado en una tabla.
2. Coge la MAC de destino y busca si sabe por donde mandarla
3. a. Si conoce por dónde mandarla la transmite por ahí
   b. Si no conoce por dónde mandarla la transmite por todos los puertos menos por el que le ha llegado

¿Cuando falla esto? Cuando la tabla cambia
Se puede evitar poniéndole al switch algo de inteligencia

PRUEBAS EN EL ROUTER

1. ¿Tengo IP?
2. ¿Tengo Gateway?
3. ¿Llegó al Gateway?
4. ¿Tengo DNS?
5. ¿Llegó al DNS?

FIREWALL DEL BRIDGE

6. ¿Tengo IP?
7. ¿Tengo Gateway?
8. ¿Llegó al Gateway?
9. ¿Tengo DNS?
10. ¿Llegó al DNS?

FIREWALL de Bridge

El firewall se aplica a paquetes que pasan de una red a otra
Por defecto, las reglas de FW no se aplican a paquetes en la misma RED.

Podemos forzar a que el FW se aplique también a los paquetes que pasan por un bridge

IP -> Firewall

==========

Ejercicio

- Tu compañero/a se conecta a tu router. Haz ping a su dirección y comprueba que ok.
- En tu router, descativa todas las reglas de IP-Firewall-Filter.
- Crea una regla de FW: Chain=Forward Protocol=ICMP action=DROP dst-address=10.0.x.23 (tu equipo).
- Comprueba que tu compi puede hacerte PING aunque la regla de FW lo 'impida'.
- En bridge, en el botón SETTINGS, activa la opción "Use Firewall": Comprueba que ahora no puede hacerte ping.
- Cuando hayas terminado la comprobación, desactiva "use Firewall" en el bridge.

==========

DÍA 6 (FIREWALL)

Comprobaciones antes de empezar

- Nuestro ordenador tiene asignada la 10.0.xxxx.123 (static lease en DHCP Server)
- El primer servidor DNS que tiene nuestro ordenador es el router: 10.0.xxxx.1

FIREWALL (*IP -> Firewall*)

Chains:

- Input: Paquetes que llegan al router
- Output: Paquetes que salen del router
- Forward: Paquetes que atraviesan el router

Ejemplo: Hemos puesto una **regla que nos impide conectarnos al router**:

- EN PESTAÑA “GENERAL”: Chain "Input" ; Input Interface "bridge" ;
- EN PESTAÑA "ACTION": Action "Drop"

El router es nuestro único servidor DNS, podemos atravesarlo (forward) (porque la regla es input) y llegar a Internet (ping a 8.8.8.8) PERO no podemos hacer ping a www.google.es porque el router es el único que nos podría ayudar a resolver nombres de dominio.

==========

EJERCICIO: Haz que se puedan hacer peticiones DNS al router. (Pista UDP puerto 53)
Creo una regla => Chain: Input ; Protocol: UDP ; Port: 53 ; Input Interface: bridge

EJERCICIO: Haz que no se pueda usar el protocolo HTTP
Creo una regla => Chain: Forward ; Protocol: TCP ; Port: 80

==========

HTTP: puerto 80

HTTPS: puerto 443

Port Knocking: Hace que solo se pueda acceder al WINBOX del router (8291) los equipos que hagan la llamada mágica: 3500-1888-2450

==========

EJERCICIO: Port Knocking con Address Lists

Para implementar port knocking, configuras reglas de firewall que añaden direcciones IP a diferentes Address Lists según la secuencia de puertos. Aquí hay un ejemplo:

- port_knocking_stage1: Para las IPs que han tocado el primer puerto.
- port_knocking_stage2: Para las IPs que han tocado el segundo puerto después del primero.
- port_knocking_success: Para las IPs que han completado la secuencia de port knocking correctamente.

Primera secuencia de port knocking:

General:

- Chain: input
- Protocol: tcp
- Dst. Port: 1234

Action:

- Action: add-src-to-address-list
- Address List: port_knocking_stage1
- Timeout: 10

Segunda secuencia de port knocking:

General:

- Chain: input
- Protocol: tcp
- Dst. Port: 5678
- Src. Address List: port_knocking_stage1

Action:

- Action: add-src-to-address-list
- Address List: port_knocking_stage2
- Timeout: 10

Tercera secuencia de port knocking:

General:

- Chain: input
- Protocol: tcp
- Dst. Port: 9012
- Src. Address List: port_knocking_stage2

Action:

- Action: add-src-to-address-list
- Address List: port_knocking_success
- Timeout: 3600

Permitir acceso a Winbox:

General:

- Chain: input

- Src. Address List: port_knocking_success
- Protocol: tcp
- Dst. Port: 8291

  Action:
- Action: accept

Bloquear acceso no autorizado:

  General:
- Chain: input
- Protocol: tcp
- Dst. Port: 8291

  Action:
- Action: drop

Con estas configuraciones, solo los usuarios que completen la secuencia correcta de port knocking podrán acceder al puerto de Winbox. Las Address Lists manejan las IPs temporalmente, facilitando el proceso de autenticación por secuencias de puertos.

telnet 192.168.122.104 1234
telnet 192.168.122.104 5678
telnet 192.168.122.104 9012
==========

DÍA 7 (NAT)

NAT: Network Address Translation

Es un proceso de Firewall que permite modificar las direcciones de los paquetes. Se diseñó para paliar la escasez de direcciones IP.
Dos tipos de NAT según lo que se modifica:

- **Source NAT (Nat de Origen)**: Se modifica la dirección/puerto de origen del paquete.
- **Destination NAT (NAT de Destino)**: Se modifica la dirección/puerto destino del paquete.

Ejemplo de uso Source NAT: Cuando un paquete de mi ordenador de casa llega al router de casa y éste sustituye la IP origen (que es privada) de dicho paquete por la IP pública del router. Pasará a ser un paquete 'enmascarado'.

IP:puerto origen -> la privada de mi dispotivo
IP:puerto destino -> 8.8.8.8:53
IP:puerto nuevo origen -> la publica de mi router
IP:puerto nuevo destino -> 8.8.8.8:53

Ejemplo de uso Destination NAT: Como antes pero al revés, cuando llega el paquete de fuera al router de mi casa y éste le pone como IP destino la IP privada del dispositivo.

IP:puerto origen -> 8.8.8.8:53
IP:puerto destino -> la publica de mi router
IP:puerto nuevo origen -> 8.8.8.8:53

IP:puerto nuevo destino -> la privada de mi dispositivo

Para poder hacer NAT el router necesita llevar un seguimiento de las comunicaciones.

IP -> Firewall -> Pestaña NAT -> Doble click en la regla -> Pestaña General

Vemos que hay una chain "srcnat" que cuando llega un paquete por un puerto de la lista WAN (por defecto esta lista contiene solo ether1) hace la acción "masquerade".

Chains de NAT:

- **srcnat**: Permite cambiar la dirección IP y puerto de origen.
- **dstna**t: Permite cambiar la dirección IP y puerto de destino.

Actions de NAT:

- **accept**: Acepta el paquete y no se hacen cambios ni se sigue evaluando NAT.
- **src-nat**: Cambio la IP/puerto origen por los indicados. Debo indicar nueva IP/puerto.
- **dst-nat**: Cambio la IP/puerto destino por los indicados. Debo indicar nueva IP/puerto.
- **masquerade**: Similar a src-nat pero utiliza la dirección del interfaz de salida.
- **redirect**: Acción especial para dst-nat.

==========

<u>EJERCICIO</u> Redirect:

Nos aseguramos que:

- Nuestra IP es 10.0.x.123
- Nuestro PRIMER SERVIDOR DNS es 10.0.x.1

Una vez que lo hemos comprobado:

1. *IP -> DNS -> Static*
2. Doble click en la DNS Static (llamada router.lan) y ponemos de IP la 10.0.14.1
3. Si hacemos ping a router.lan lo traduce a 10.0.14.1

Ahora vamos a hacer **que nuestro router no haga respuestas DNS ni se ofrezca para ello:**
IP -> DNS -> Desmarco "Allow Remote Requests"
Ahora si cambiamos de perfil y volvemos al mismo vemos que ya no aparece como opción de Servidor DNS. Nuestro DNS es 8.8.8.8 y 8.8.8.8 no conoce router.lan (falla el ping).

Vamos a hacerle la jugarreta al router
Creamos una regla en firewall->NAT que cambie la dirección destino (dstnat) de los paquetes que:

- Usan protocolo UDP
- Puerto destino 53
- Está en la lista LAN

A éstos les hace redirect, y ya hay ping a router.lan

Vamos a *IP -> DNS -> Static* y creamos una nueva llamada "mibanco.com" y le ponemos como Address 10.0.14.1. A partir de aquí si entramos en "mibanco.com" vamos a la página del router.
==========

DNS es un servicio esencial en Internet

- Resuelve los nombres de dominio a direcciones IP
- No es un protocolo cifrado
- Tampoco es un protocolo autenticado
- Es muy fácil interceptar peticiones DNS y alterar las respuestas
- Podemos hacer que los incautos vayan a páginas peligrosas en lugar de las reales

Las redes van de: conectar redes, autenticar redes y asegurar redes ya que son la cosa más insegura por naturaleza.

DoH: DNS over HTTPS -> Se establece una comunicación segura y, en lugar de obtener una página web como siempre con HTTPS, obtengo la resolución DNS.

En los navegadores vamos a Ajustes, ponemos "DoH" y podemos establecer que siempre se use DoH para navegaciones más seguras.

Se puede poner DoH en el router pero requiere cargar servidores,... no es tan fácil como marcar y ya.

==========

EJERCICIO dstnat:

Abrimos la terminal y hacemos: *docker pull nginx:alpine*

nginx es un servidor de páginas web, vamos a ponerlo en marcha: *docker run -d -p 8000:80 nginx:alpine*

Esto nos devuelve un número.

Si vamos en el navegador a localhost:8000 nos sale la página de nginx.

Creamos una regla en Firewall-> NAT tal que:

GENERAL
- Chain: dstnat
- Protocol: 6 (tcp)
- Dst Port: 8000
- In. Interface List: WAN

ACTION
- Action: dst-nat
- To Addresses: 10.0.14.123
- To Ports: 8000

Ahora si alguien va en su navegador a 192.168.27.8:8000 (la IP pública de mi router) lo redirige a mi servidor nginx

==========

Ver procesos en docker: *docker ps -a*
Para proceso: *docker stop <name>*
Eliminar proceso: *docker rm <name>*

DÍA 8 (Túneles)

PPP: Point to Point Protocol
PPPoE: PPP over Ethernet
L2TP: Layer 2 Tunnel Protocol

HTML-TCP-IP-Trama Ethernet

Trama: 1500 bytes: MAC Origen - MAC Destino - Datos_trama
Paquete: 1480 bytes: IP Origen - IP Destino - Datos_paquete
TCP: 1460 bytes: Puerto origen - Puerto destino - Datos_tcp

Encapsulación: Como una muñeca rusa.

Tecnología de Túnel (VPN): Permite que dentro de un paquete los datos que se envían sean a su vez un paquete. Así el paquete-dato viaja hasta el destino como si fueran datos. Al llegar el receptor recibe el paquete-dato y lo enruta.

==========

Ejercicio: Crear un cliente PPP

1. Descativamos el cliente DHCP: *IP -> DHCP -> Click derecho y disabled*
2. *PPP -> + -> PPPoE Cliente -> En "General"*: Le ponemos nombre y como Interfaces lo ponemos sobre ether1; En Dial Out ponemos usuario, contraseña (la que nos diga el profesor que es el que va a montar el servidor PPP) y marcamos "User Peer DNS"
3. Vamos a *Interfaces -> Interfaces List -> + -> Añadimos una WAN que sea el interfaz que hemos creado* (¿PORQUÉ WAN? Porque tenemos una regla en IP->Firewall->NAT que enmascara todas las IPs que salen por una WAN. Como vamos a salir a Internet a través del ordenador del profesor la IP origen tiene que ser enmascarada con la IP del ordenador del profesor. Con esto se ahorra enrutarnos a todos uno a uno).
4. Vamos a *PPP -> Interface -> PPPoE Scan -> Elegimos la interfaz ether1 y le damos a Start* y ya debería salirnos el servidor del profesor.

Así nos conectaremos a Internet a través del servidor que lanza el maestro. Si el quiere nos quita Internet (si no pagamos).

==========

IP -> Addresses y vemos las IPs que tenemos.

Direcciones punto a punto: Caso especial de dirección. Como solo tengo dos extremos si envío algo llega al otro punto y ya. La máscara es /32. Nos permiten no desaprovechar las direcciones de broadcast y de red.

Killian crea un server y al hacer Scan lo vemos también. Un mismo interfaz soporta varias conexiones PPPoE. Intenta conectarse al primero que ve y si no prueba el siguiente y así...

==========

EJERCICIO: Uno hace de servidor y los demás se conectan sólo a este.
El que hace de servidor:

- **Desactiva el cliente PPPoE**
- **Activa el cliente DHCP y se asegura de 'tener Internet'**
- **Crea un POOL de direcciones para los clientes PPPoE**
- **Crea un PPP-Profile con remote-address=pool local-address=1.2.3.4**
- **Crea PPP-Secret para los usuarios, indicando el perfil creado.**

- **Crea un PPP-PPPoE Server en ether1 con un SERVICE NAME único.**

Los que hacen de Cliente:
- **Modifican en cliente PPPoE para conectarse al SERVICIO del compañero/a.**
- **Comprueban que se conectan al SERVIDOR y que ¡hay Internet!**

VERSIÓN MIGUEL

Paso 1: Configuración de la Topología en GNS3
- Abrir GNS3: Inicia GNS3 y abre un nuevo proyecto.
- Añadir dispositivos: Arrastra dos routers MikroTik (RouterOS 7.13.3) al área de trabajo. Añade también un switch y una máquina virtual con NAT.
- Conectar dispositivos: Conecta la interfaz ether1 de ambos routers al switch y conecta una interfaz del switch a la máquina virtual con NAT.

Paso 2: Configuración del Switch y NAT en GNS3
Asegúrate de que el switch en GNS3 no requiere configuración adicional y que todas las interfaces conectadas estén en la misma VLAN predeterminada. La máquina virtual NAT está preconfigurada para proporcionar acceso a Internet.

Paso 3: Configuración del Router A (PPPoE Server) a través de WinBox
Acceder al Router: Abre WinBox y conéctate al Router A usando su MAC address.

Configurar DHCP Client en ether1:
- Navega a IP > DHCP Client.
- Haz clic en + para añadir un nuevo cliente DHCP.
- Selecciona ether1 como la interfaz.
- Asegúrate de marcar "Use Peer DNS" y "Use Peer NTP" si deseas usar los servidores DNS y NTP proporcionados por el servidor DHCP.

Configurar PPPoE Server:
- Navega a PPP > Interfaces.
- Haz clic en + y selecciona PPPoE Server.
- Selecciona ether1 como la interfaz.
- Deja el Service Name por defecto o pon un nombre como pppoe-server.

Configura un rango de IP para los clientes PPPoE: Navega a PPP > Profiles, añade un nuevo perfil:
- Name: pppoe-profile
- Local Address: 10.0.0.1 (dirección del servidor PPPoE, diferente de la IP obtenida por DHCP)
- Remote Address: 10.0.0.2-10.0.0.254 (rango de direcciones para los clientes PPPoE).

Configurar Secrets:
- Navega a PPP > Secrets.
- Haz clic en + para añadir un nuevo secret:
    - Name: user1
    - Password: password1
    - Service: pppoe
    - Profile: pppoe-profile

Paso 4: Configuración del Router B (PPPoE Client) a través de WinBox
Acceder al Router: Abre WinBox y conéctate al Router B.

Configurar DHCP Client en ether1:
- Navega a IP > DHCP Client.
- Haz clic en + para añadir un nuevo cliente DHCP.
- Selecciona ether1 como la interfaz.
- Asegúrate de marcar "Use Peer DNS" y "Use Peer NTP".

Configurar PPPoE Client:
- Navega a PPP > Interfaces.
- Haz clic en + y selecciona PPPoE Client.
- Configura los siguientes parámetros:
    - Interface: ether1
    - User: user1 (el usuario que configuraste en el Router A)
    - Password: password1 (la contraseña que configuraste en el Router A)
    - Profile: default
    - Marca la opción Add Default Route.

Activar PPPoE Client: En la lista de interfaces, selecciona la interfaz pppoe-out1 que creaste y asegúrate de que esté habilitada.

Paso 5: Verificación de la Conexión
Verificar la Conexión en el Router B:
- Navega a PPP > Interfaces.
- Verifica que la interfaz pppoe-out1 esté running y que tenga una IP asignada por el Router A.

Ping de Prueba: Desde Router B, abre una terminal (New Terminal) y realiza un ping a la dirección IP del Router A para verificar la conectividad (ping 10.0.0.1)

Paso 6: Configuración de NAT (opcional) en Router A
Configurar NAT:
- Navega a IP > Firewall > NAT.
- Haz clic en + para añadir una nueva regla de NAT:
    - Chain: srcnat
    - Out Interface: ether1
    - Action: masquerade

Esto permitirá que las solicitudes de Router B accedan a Internet a través del Router A.

Siguiendo estos pasos, los ether1 de ambos routers MikroTik obtendrán sus direcciones IP automáticamente mediante DHCP desde la máquina virtual NAT y establecerán una conexión PPPoE entre ellos utilizando un rango de IP diferente para la conexión PPPoE. Además, tendrás acceso a Internet a través de la máquina virtual NAT.

Para comprobar que el cliente PPPoE se ha conectado al servidor PPPoE, puedes seguir estos pasos utilizando WinBox en los routers MikroTik:

En el Router A (PPPoE Server):

Verificar Conexiones Activas:

- Abre WinBox y conéctate al Router A.
- Navega a PPP > Active Connections.
- Deberías ver una entrada que muestra la conexión PPPoE del cliente. Verifica que el nombre de usuario (user1) esté en la lista y que la interfaz pppoe-out1 esté activa.

Verificar Registros:

- Navega a Log en el menú izquierdo.
- Busca entradas relacionadas con la autenticación PPPoE. Debe haber una entrada que confirme que el cliente user1 se ha conectado exitosamente.

En el Router B (PPPoE Client):

Verificar Estado de la Interfaz PPPoE:

- Abre WinBox y conéctate al Router B.
- Navega a PPP > Interfaces.
- Verifica que la interfaz pppoe-out1 esté en estado running. Esto indica que la interfaz está activa y ha establecido una conexión.

Verificar la Asignación de IP:

- Navega a IP > Addresses.
- Deberías ver una dirección IP asignada a la interfaz pppoe-out1. Esta dirección IP debería estar dentro del rango configurado en el perfil PPPoE del servidor.

Verificar la Ruta Predeterminada:

- Navega a IP > Routes.
- Asegúrate de que haya una ruta predeterminada (0.0.0.0/0) a través de la interfaz pppoe-out1. Esto confirma que el tráfico de Internet se enruta a través de la conexión PPPoE.

Pruebas de Conectividad:

- Realizar un Ping desde el Router B: Abre una terminal (New Terminal) en WinBox en el Router B. Realiza un ping a la dirección IP del servidor PPPoE (ping 10.0.0.1) (Router A):

Si los pings tienen éxito, esto confirma que la conexión PPPoE está establecida y funcionando.

Realizar un Ping a Internet

Desde la misma terminal en el Router B, realiza un ping a una dirección IP externa (como 8.8.8.8). Si los pings tienen éxito, esto confirma que el tráfico de Internet se está enrutando correctamente a través de la conexión PPPoE y el NAT.

VERSIÓN PAOLA

1. Vamos a dhcp-client y deshabilitamos el cliente que aparece.
2. Vamos a PPP y añadimos una interfaz PPPoE-cliente, poniendo en “Interfaces” ether1 (pestaña General). En la pestaña Dial Out si queremos conectarnos a un servicio en específico tenemos que poner el nombre del server en service
3. Vamos Interfaces List y añadimos la interfaz pppoe que hemos creado a la WAN
4. PPP→ Interface → Pulsa el botón de PPPoE scan → Start (aparecerá el servidor)

Esto lo hace el server

1. Activar el dhcp-client
2. Crear pool: ip → pool crear 10.200.200.1-10.200.200.255
3. Crear perfil: PPP→ profile → crear ; local address 10.200.200.1 ; remote address el pool creado
4. Crear secret: PPP→ secret crear ; meter usuarios y su contraseña ; profile meter servidor → aplicar

Ya saldria los clientes en interface como conectados

Resumen:
En el Router A (Servidor PPPoE):
- **Verifica conexiones activas en PPP > Active Connections.**
- **Revisa los registros en Log.**

En el Router B (Cliente PPPoE):
- **Verifica el estado de la interfaz PPPoE en PPP > Interfaces.**
- **Verifica la asignación de IP en IP > Addresses.**
- **Verifica la ruta predeterminada en IP > Routes.**

Pruebas de Conectividad:
- **Realiza pings desde el Router B para verificar la conectividad con el Router A y con Internet.**

Siguiendo estos pasos, podrás confirmar que el cliente PPPoE se ha conectado exitosamente al servidor PPPoE y que la configuración está funcionando correctamente.
==========

DÍA 9 (Túneles)

PPP: Point to Point Protocol
- Cifrado.
- Compresión de datos.

PPPoE: Pointo to Point Protocol Over Ethernet
- Funciona en L2 (la misma red… no atraviesa routers).
- Se utiliza como modo simple de autenticación en la red.

Paquete 'normal': Trama ethernet-Paquete IP-TCP-HTML
Paquete 'ppoe': Trama ethernet-Trama PPoE-Paquete IP-TCP-HTML

PPPoE solo vale dentro de una misma red. SSTP y L2TP actúan como VPN y valen para fuera de la red.

'Overhead'

L2TP: Layer 2 Tunnel Protocol

==========
EJERCICIO: L2DTP

[admin@R1] > interface/bridge/add
[admin@R1] > interface/bridge/port add bridge=bridge1 interface=ether2
[admin@R1] > interface/bridge/port add bridge=bridge1 interface=ether3
[admin@R1] > ip address/add interface=bridge1 address=192.168.88.1/24
[admin@R1] > ip dhcp-server/setup (interface=bridge1)
[admin@R1] > ip firewall/nat add chain=srcnat action=masquerade out-interface=ether1
[admin@R1] > ip dhcp-client/add interface=ether1
[admin@R1] > interface/l2tp-client/add connect-to=192.168.27.10 user=user114 password=user114 disabled=no
[admin@R1] > interface/l2tp-client/set 0 add-default-route=yes
[admin@R1] > ip dhcp-client/set 0 default-route-distance=2
==========

DÍA 10 (Túneles)

L2TP -> Obsoleto.
PPPoE -> Aún se usa pero en el caso de la fibra no es necesario.

Veamos otros ejemplos de tecnología VPN:

- **PPPTP ->** Se desaconseja por inseguro
- **SSTP ->** Secure Socket Tunnel Protocol

https: http sobre ssl

==========

EJERCICIO

En el proyecto de GNS3 "sstp" ponemos ips, rutas y dhcp-servers tal que así:

nucs <-> (192.168.1.1)R1(10.0.0.1) <-> (10.0.0.3)R3(10.1.0.3) <-> (10.1.0.2)R2(192.168.2.1) <-> nucs

Ahora vamos a crer un túnel: Pondremos en R1 un server y en R2 un cliente y creamos una interfaz tipo túnel que será lo mismo que tirar un cable de uno a otro. De forma que podremos decirle que para llegar coja por ahí.

R1
===

1. Con esto vemos como esta el servidor:

interface/sstp-server/server/print

2. Con esto lo activamos:

interface/sstp-server/server/set enabled=yes

Nota: Si fuéramos de mikrotik a no mikrotik necesitaríamos activar un certificado.

3. Creamos un usuario:

ppp/secret/add name=router2 password=secretodelrouter2 local-address=10.255.255.1 remote-address=10.255.255.2

local-address es la dirección del propio router en el túnel.

remote-address es la dirección de red.

Nota: Todo esto en modo gráfico se haría: *PPP -> + -> SSTP Server o Client*

R2
===

1. Creamos el inetrfaz:

interface/sstp-client/add connect-to=10.0.0.1 user=router2 password=secretodelrouter2

2. Habilitamos el interfaz:

interface/print e interface/enable <n> siendo n el número de la interfaz de túnel.

En ambos
========

Hago *interface/print* y tiene que salir DR en el del R1 (dinámico y running) y R en el del R2 (no es dinámico y running)

Diagnostica errores
================

En el server: *ppp/secret/export show-sensitive*
En el cliente: *interface/sstp-client/export show-sensitive*
Comprobamos que el user y el password coinciden
==========

En este caso solo hay un router entre R1 Y R2 pero el espacio entre ambos puede ser tan grandes como Internet. ESTO ES UNA VPN.

Las direcciones de los túneles son /32.

A partir de aquí, 10.255.255.1 es el servidor y 10.255.255.2 el cliente
Puedo hacer ping de uno a otro o incluso usar esas direcciones para hacer rutas y cosas:

- En R1: *ip/route/add dst-address=192.168.2.0/24 gateway=10.255.255.2*
- En R2: *ip/route/add dst-address=192.168.1.0/24 gateway=10.255.255.1*

Y ya habría ping de los nucs de un lado a los del otro.

<u>COMPROBACIONES SI NO DA ping</u>
EN EL ROUTER:
ip/address/print
ip/route/print

Vemos que tenemos la IP 10.255.255.1, la dirección de red 10.255.255.2 y el interfaz de túnel habilitado.
Vemos que está la ruta hasta R2 (10.255.255.2) por el gateway interfaz de túnel.

EN EL CLIENTE:
ip/address/print
ip/route/print

Vemos que tenemos la IP 10.255.255.2, la dir de red 10.255.255.1 y el interfaz de túnel habilitado.

Vemos que esta la ruta hasta R1 (10.255.255.1) por el gateway interfaz de túnel.

RESUMEN CONFIGURACIÓN SSTP MIKROTIK

Servidor:

- Activar servidor sstp
- Crear Pool (opcional)
- Crear secret y poner local-address y remote-address del túnel.
- Crear ruta estática usando la IP cliente del túnel

Cliente:

- Crear interfaz cliente
- Crear ruta estática usando la IP servidor del túnel

Check: Tiene que haber ping desde un ordenador a otro.

==========

EJERCICIO: LO HACEMOS CON UN COMPI

SIENDO YO CLIENTE CON JUAN DIEGO:

interface/sstp-client/add connect-to=192.168.27.9 user=JuanDiego1 password=JuanDiego1
interface/print
interface/enable 9

ping 10.255.255.1
ping 192.168.27.9
ping 10.0.9.123 <- No va, seguramente porque en connect-to tengo que poner la IP del bridge o bien crear la ruta a la red 10.0.9.0/24 a través del túnel manualmente.

SIENDO YO SERVER (TAMPOCO FUNCIONÓ):

Habilito el server:
interface/sstp-server/server/set enabled=yes

Creo el usuario y pongo las IPs de los extremos del túnel:
ppp/secret/add name=router password=router local-address=10.255.255.1 remote-address=10.255.255.2

A la red del compañero “y” se llega por el extremo cliente (10.255.255.2) del túnel:
ip/route/add dst-address=10.0.y.0/24 gateway=10.255.255.2

SIENDO YO CLIENTE CON MIGUEL (FUNCIONÓ PERFE!!!):

Creo la interfaz cliente al router de Miguel con las credenciales que ha puesto:
interface/sstp-client/add connect-to=192.168.27.8 user=router password=router

Habilito la interfaz sstp-out:
interface/print e *interface/enable y el número.*

Creo la ruta (a la red donde está el ordenador de Miguel llegó por el extremo server (10.255.255.1) del túnel:
ip/route/add dst-address=10.0.8.0/24 gateway=10.255.255.1
==========

DÍA 11 (ZeroTier)

Vamos a https://mikrotik.com/download/archive , descargamos el all packages arm64 7.14 .zip e instalamos wireless y zerotier (arrastra y reboot).

ZEROTIER

ZeroTier es un nuevo paradigma en la programación de redes:
SDN: Software Defined Networks ó Redes Definidas por Software.

Nos registramos en ZeroTier.com y creamos una red "Create A Network", la cual tiene un ID.

En WinBox:

- *ZeroTier -> Pestaña "Instances" y habilitas el que hay*
- *ZeroTier -> Pestaña "ZeroTier", creas uno nuevo y le pegas en "Network" el Network ID de la red de ZeroTier.*

Nos rechaza, en la web en la parte de configuración de nuestra red abajo del todo podemos autorizarla ("Auth?"). Vemos que ya se ha conectado y que nos da una IP.

Si queremos otra IP: en la parte de nuestra red en zerotier en el desplegable Members: la escribes -> + -> Borras la anterior.

Descargamos la aplicación ZeroTier One en el móvil, le damos a Add Net y escribimos el Network ID. Se crea una conexión de túnel (VPN) entre el móvil y el ordenador.

De esta forma vayamos donde vayamos mientras tengamos internet podremos hacer ping del móvil a nuestro ordenador.

Si en WinBox vamos a ZeroTier -> Pestaña ZeroTier y creas uno nuevo y le pegas en "Network" el Network ID de la red de ZeroTier del maestro ya podemos hacerle ping a su móvil.

Si en la pestaña Advanced ponemos en "Destination" 0.0.0.0 y en "Vía" la IP de nuestro router (la que le ha puesto ZeroTier) podremos salir a Internet desde nuestro router estemos desde donde estemos. Así nos vamos a Alemania pero Netflix creerá que seguimos en casa.

ZeroTier vale para Mikrotik, Linux, Windows, iOS y Android

Es una forma fácil de configurar una VPN.

¿COMO PRACTICAR PARA EL EXAMEN?

1. Abre GNS3
2. Pon: Nube NAT - Switch - Router / Router
3. Inicia los routers

4. Te vas a Winbox y te conectas a través de la MAC

DÍA 12 (Herramientas de rendimiento)

Tools -> BTest Server: Permite hacer test de ancho de banda. Quitamos la Authenticate
Tools -> Bandwith Test: Es un cliente para hacer test de ancho de banda.
Lo hago con un compañero con su dirección 192.168.27.x
Para el test de velocidad puedo usar protocolo UDP y TCP.

- UDP tira agua y luego se ve lo que ha caído. Los paquetes van en un autobús de mierda.
- TCP va abriendo y cerrando el grifo. Da un poco menos rendimiento. Los paquetes van cómodos.

El test se pone en el Servidor y en el Cliente para que los routers de en medio no hagan esfuerzo.

Tools -> SpeedTest: Otra herramienta para el rendimiento.

Tools -> Email: Configuras cual es el servidor (de correo electrónico), cuerpo, cifrado, dirección, usuario, form,... Se envía cuando pasa algo (cuando un usuario se conecte por VPN,...)

Tool -> Flood Ping: Manda una avalancha de pings sobre una dirección. No hacer sobre dirección externa porque te pueden banear.

Tools -> Graphing: Crea gráficos QUE NO SON EN TIEMPO REAL sobre todos o algunos de los interfaces, colas y recursos. La dirección IP indica desde donde se puede acceder a dicho gráfico
Para ver gráficos de los interfaces QUE SÍ SON EN TIEMPO REAL: *Interfaces -> Pestaña "Interface" -> Doble clic en uno -> Traffic*

Tools -> IP Scan: Manda ping a todas las IPS de un rango que le pongas (a toda la clase sería: 192.168.27.0/24)

Tools -> MAC Server -> MAC WinBox Server: y puedes habilitar, deshabilitar o modificar la conexión por MAC. Es una medida de seguridad.

Tools -> MAC Server -> MAC Telnet Server: y puedes habilitar, modificar o deshabilitar la capacidad para conectarse por Telnet a través de la MAC al router.
IP -> Neighbors -> Click derecho en uno de mis compañeros -> MAC Telnet -> Pones usuario y contraseña y entras si tiene habilitado la MAC Telnet

Tools -> Script: Script que se ejecute cuando algo, en que equipo y como lo compruebo, estado actual,...

Tools -> Packet Snifer: Almacena paquetes.
En la pestaña Filter pongo interfaces "ether1", le doy a Start y capturo todo lo que pase por ether1.
Si le doy al botón *Packets* veo los paquetes almacenados.
Si le pongo en la pestaña General nombre al File ("test" por ejemplo) al darle Start se genera un fichero en Files (donde están los backups). Puedo descargarlo y abrirlo con Wireshark y filtrar allí o inspeccionarlos o lo que sea.

Tools -> Ping: Hacer ping y más cosas

Tools -> Ping Speed: Mandar pings muy rápidamente, con intervalos. Para estadísticas de intercambio de paquetes,...

Tools -> RomON: Permite configurar los dispositivos para que nos podamos conectar a ellos sin necesidad de que tenga IP.
Funciona gracias a varios dispositivos de capa 2 con RomON activo que están conectados entre sí.

Tool -> Torch: Muestra en tiempo real los paquetes que están circulando por una interfaz.

Tool -> TraceRoute: Muestra el camino que hace desde el router hasta una IP.

Tool -> TrafficMonitor:

Tool -> WoL: Puedo hacer que un equipo se encienda desde lejos.