



# Tecnológico de Monterrey

Tec de Monterrey, Campus Guadalajara

**Clave:** TE2036.501

**Implementación de redes seguras (Gpo 501)**

**Examen argumentativo escrito**

Caso Práctico

**Profesor:**

Ramiro Alejandro Bermúdez Uribe

**Nombre:**

Elías Uriel Velázquez Rojas\_A01639716

**Fecha de entrega:**

29 de noviembre del 2022

## Examen ARG

---

### INDICACIONES DE LA ACTIVIDAD

#### Examen Final

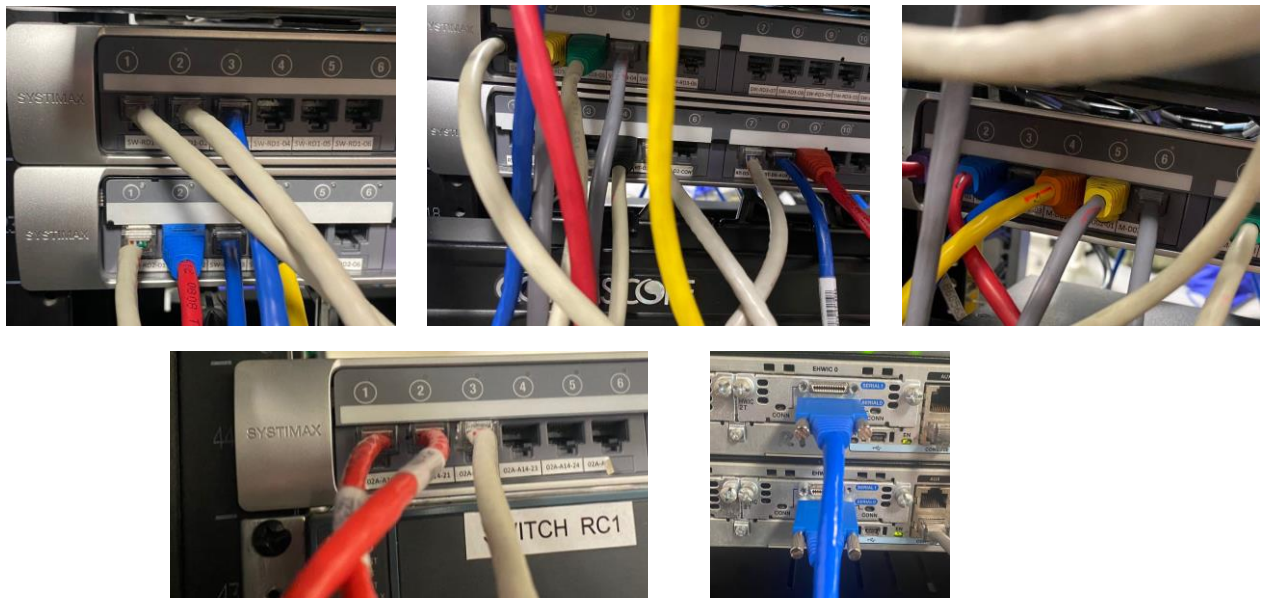
“Apegándose al Código de Ética de los Estudiantes del Tecnológico de Monterrey, me comprometo a que mi actuación en este examen esté regida por la honestidad académica.”

#### OBJETIVOS

- Con base al siguiente diagrama (figura1), configura los equipos y confirma conectividad en el laboratorio para salir a internet.
- Los equipos de minecraft NO pueden jugar este juego de 17:00 a 18:00 hrs. Fuera de este horario automáticamente pueden hacer conexión.
- Documenta con evidencias y explicaciones individuales: Sustentar prácticamente la teoría vista en estas 10 semanas con las capturas que realizó.
  1. Direccionamiento usado y capacidad en hosts diseñado.
  2. Explica tabla de ruteo.
  3. Explica tabla de arp.
  4. Vecinos de eigrp.
  5. Explica tabla de nat.
  6. Configuración de ACL para filtrar al equipo minecraft.
  7. Evidencia de conexión entre vlans, equipos remotos, salida a internet y wan.
- Entrega de archivos txt de todas las configuraciones.

## DESARROLLO DE LA PRÁCTICA

Lo primero que hicimos en la práctica fue hacer las conexiones de los switches, los seriales, routers y la conexión con consola, como se muestra en las siguientes imágenes:



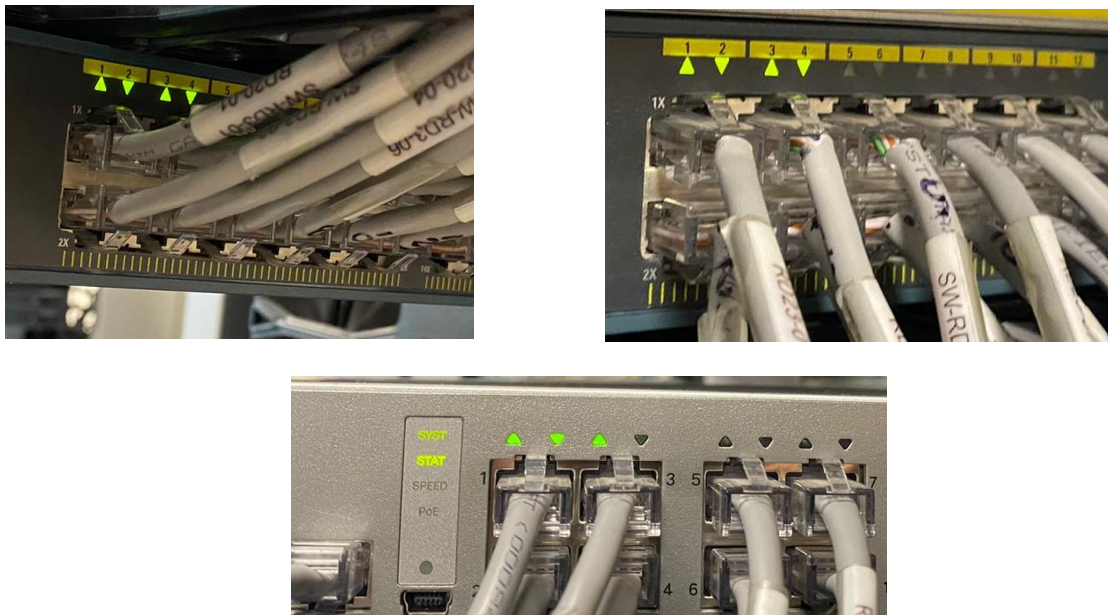
*Figura 1-5. Conexiones físicas realizadas entre switches, routers, seriales y otros dispositivos*

Para poder llegar a este apartado tuvimos problemas a la hora de conexión por varias cosas, al principio creíamos que los routers 2,3 no servían ya que cuando los conectábamos no encendían el foquito y después nos dimos cuenta al cambiar el cable de la computadora con el router 2 este si servía.

Pero la conexión del Access point era ahora la que nos estaba causando problemas porque no encendía el foco que verificaba que se estaba haciendo la conexión para después darnos cuenta que nos faltaba conectar el Access point a corriente y así se solucionó ese problema. Luego tuvimos otro contratiempo con los Gigabytes porque no

**Examen ARG**

teníamos el acceso a internet por lo que tuvimos que usar un switch como multiplexor para poder dar el acceso a internet al Gigabyte 0/1 del router 2 y el router 3 que son los que usamos.



*Figura 6-8. Conexiones correctas de routers, switches y otros dispositivos*



*Figura 9. Conexiones de consola, switch*

## Examen ARG

---

Después de verificar las conexiones y que todo estuviera funcionando bien empezamos a hacer nuestro diagrama a mano para entender un poco mejor que es lo que estamos haciendo y como se ven las conexiones físicas, podemos basar en esto a la hora de programar, para después asignar las ip con sus mascaras a los diferentes VLAN y poder representarlo digitalmente y así nos quedó nuestro diagrama de redes.

**Diagrama de la red realizado en Cisco:** Los gigabits 0/1 de los dos routers es el internet entonces la ip es de manera dinámica.

- Red de LAN de 24 host(R1)
  - Router Gigabit 0/0
  - Switch VLANZ: 172.15.0.16
  - Switch VLANX: 172.15.0.0
  - Switch VLANY: 172.15.0.8
  - Rango de DHCP:172.15.0.0 to 172.15.0.24
- Red de LAN de 24 host(R2)
  - Router Gigabit 0/0
  - Switch VLANZC: 172.15.1.16
  - Switch VLANXA: 172.15.1.0
  - Switch VLANYB: 172.15.1.8
  - Rango de DHCP:172.15.1.0 to 172.15.1.24
- Red WAN (R1 & R2)
  - Router1 Serial 0/0/0: 192.168.0.1
  - Rouer2 Serial 0/0/0: 192.168.0.2



## Examen ARG

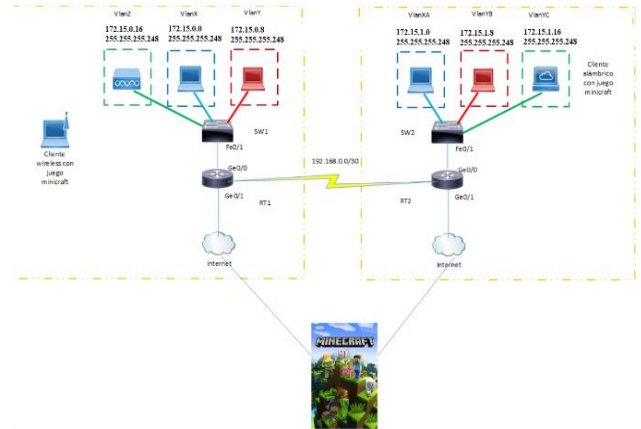
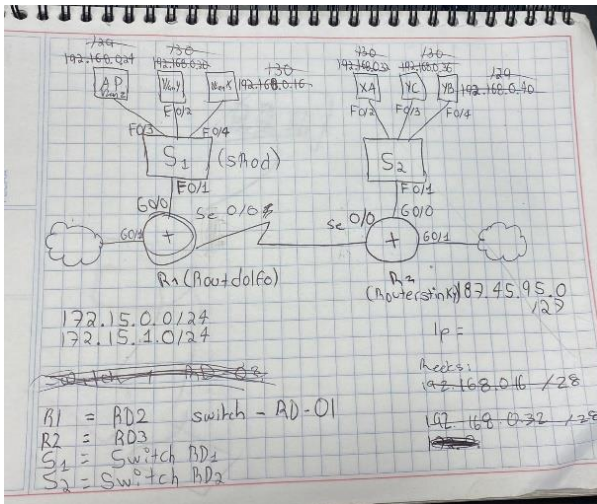


Figura 10-11. Bosquejo del diagrama y el diagrama de la red

Configuración de routers: [https://github.com/Shedew/Examen\\_Netes/tree/main/Routers](https://github.com/Shedew/Examen_Netes/tree/main/Routers)

Cuando terminamos nuestro diagrama el siguiente paso que hicimos fue comprobar que estuviera bien y esto lo hacemos programando los router y switches, lo primero que hicimos fue encenderlos y relacionar cada switch con su router para la programación del router 2 usamos la promoción de Routdolfo y router 3 usamos el de Routerstinky en las cuales definimos el interfaz de los gigabit y los seriales, para después excluir una dirección de address, poner un rango de ip para que tomen las Vlan definimos el ip route y el comando Access list 102 el cual nos sirve para denegar el acceso a minecraft prohibimos la conexión mediante la ayuda del tcp y el comando any any para después definir los vecinos EIGRP.

Configuración de switches: [https://github.com/Shedew/Examen\\_Netes/tree/main/Switches](https://github.com/Shedew/Examen_Netes/tree/main/Switches)

Y para los switches lo primero que hicimos fue definir el nombre para el router2 el switch era sRdo y para el router3 su switch era sRouper se definieron las vlan dentro de ellos y se les asignaron los nombres a cada una de ella además de vlan admin, después la interface fast con el modo de acceso del switchport además de definir el mode trunk.

```
Routerstinky#show access-list 102
Extended IP access list 102
 10 deny tcp any any eq 25565 time-range time-ssh (active) (5 matches)
 20 permit ip any any (17164 matches)
Routerstinky#show access-list 102
Extended IP access list 102
 10 deny tcp any any eq 25565 time-range time-ssh (active) (33 matches)
 20 permit ip any any (17338 matches)
Routerstinky#show access-list 102
Extended IP access list 102
 10 deny tcp any any eq 25565 time-range time-ssh (active) (33 matches)
 20 permit ip any any (32264 matches)
Routerstinky#show clock
17:58:19.071 UTC Mon Nov 28 2022
Routerstinky#show clock
17:58:41.109 UTC Mon Nov 28 2022
Routerstinky#show clock
17:59:05.903 UTC Mon Nov 28 2022
Routerstinky#show clock
17:59:14.471 UTC Mon Nov 28 2022
Routerstinky#show clock

Routerstinky#show access-list 102
Extended IP access list 102
 10 deny tcp any any eq 25565 time-range time-ssh (inactive) (52 matches)
 20 permit ip any any (33567 matches)
Routerstinky#show access-list 102
Extended IP access list 102
 10 deny tcp any any eq 25565 time-range time-ssh (inactive) (52 matches)
 20 permit ip any any (33766 matches)
Routerstinky#show clock
18:02:38.395 UTC Mon Nov 28 2022
Routerstinky#show clock
18:02:39.547 UTC Mon Nov 28 2022
Routerstinky#
```

Figura 12-13. Clok1 y clok2 del Router 2

```
Routdolfo#show clock
18:01:16.543 UTC Mon Nov 28 2022
Routdolfo#show access-list 102
Extended IP access list 102
 10 deny tcp any any eq 25565 time-range time-ssh (inactive) (3 matches)
 20 permit ip any any (254391 matches)
Routdolfo#clock set 17:59:00 28 NOV 2022
Routdolfo#
Nov 28 17:59:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 18:01:38 UTC Mon Nov 28 2022 to 17:59:00
UTC Mon Nov 28 2022, configured from console by cisco on console.
Routdolfo#show access-list 102
Extended IP access list 102
 10 deny tcp any any eq 25565 time-range time-ssh (active) (3 matches)
 20 permit ip any any (254450 matches)
Routdolfo#

Routdolfo#clock set 17:55:00 28 NOV 2022
Routdolfo#
Nov 28 17:55:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 23:33:16 UTC Mon Nov 28 2022 to 17:55:00
UTC Mon Nov 28 2022, configured from console by cisco on console.
Routdolfo#show access-list 102
Extended IP access list 102
 10 deny tcp any any eq 25565 time-range time-ssh (active)
 20 permit ip any any (221868 matches)
Routdolfo#
```

Figura 14-15. Clok1 y clok2 del Router 3

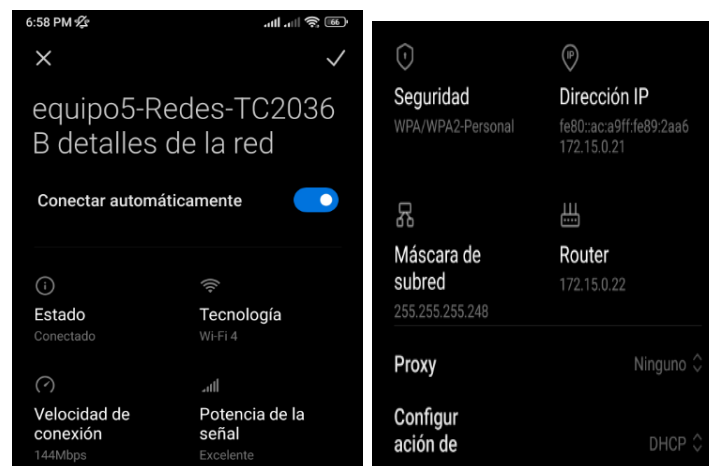


Figura 16-17-Conexión 7ccess point al teléfono

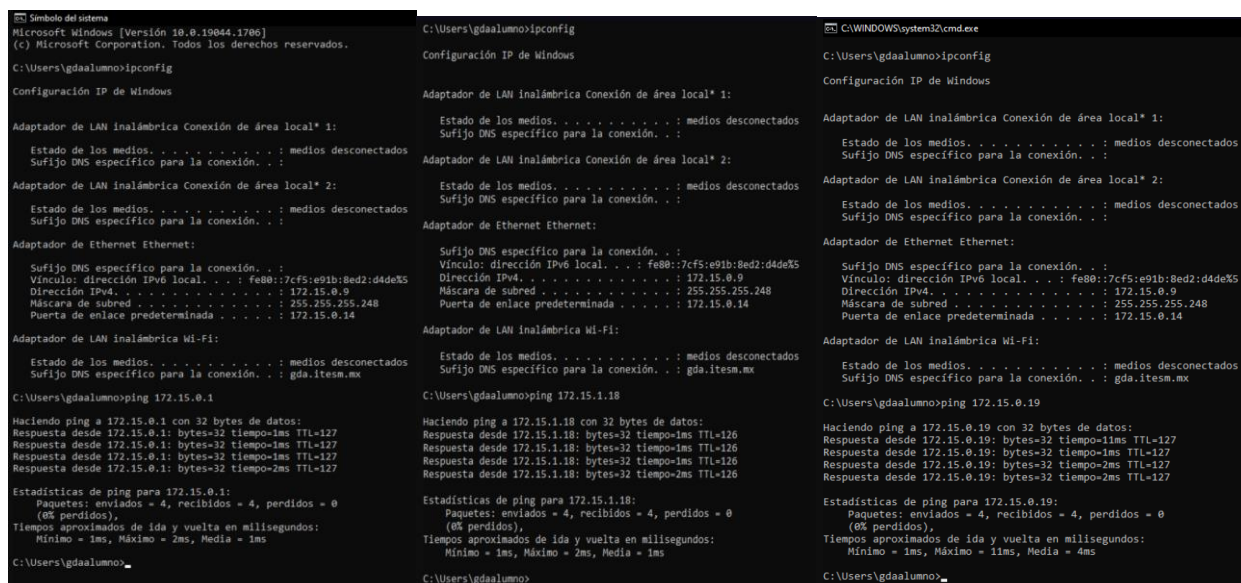
## Examen ARG

**EIGRP Neighbors:** En la imagen de aquí abajo mostramos el comando de show ip eigrp neighbors que nos muestra los vecinos, para que los routers puedan ejecutar EIGRP primero se deben convertir en vecino para después intercambiar la información de enrutamiento y esa información es la que nos muestra el comando, donde se puede ver la ip, el interdice, el tiempo de actividad, el SRTT, el RTO y demás información.

```
Routdolfo#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(2)
H   Address                Interface      Hold Uptime    SRTT   RTO  Q  Seq
                               (sec)          (ms)          Cnt  Num
0   192.168.0.2              Se0/0/0        11 01:48:59    3    200  0   3
Routdolfo#
```

*Figura 18-EIGRP Neighbors*

En las imágenes de abajo se puede ver las pruebas la primera imagen es de un ping a otra vlan en una misma red, la siguiente imagen ping a otra vlan pero en diferente red y por último un ping del Access point en una misma red.



The figure consists of three side-by-side screenshots of Windows command prompts, each showing network configuration and ping test results.

- Left Screenshot:** Shows the configuration of a Windows PC (C:\Users\gdaalumno>ipconfig). It displays the IP address 172.15.0.1, subnet mask 255.255.255.248, and gateway 172.15.0.14. Below this, it shows the results of a ping command to 172.15.0.1, indicating successful connectivity with 0% packet loss.
- Middle Screenshot:** Shows the configuration of a Windows PC (C:\Users\gdaalumno>ipconfig). It displays the IP address 172.15.1.18, subnet mask 255.255.255.248, and gateway 172.15.0.14. Below this, it shows the results of a ping command to 172.15.1.18, indicating successful connectivity with 0% packet loss.
- Right Screenshot:** Shows the configuration of a Windows PC (C:\Users\gdaalumno>ipconfig). It displays the IP address 172.15.0.19, subnet mask 255.255.255.248, and gateway 172.15.0.14. Below this, it shows the results of a ping command to 172.15.0.19, indicating successful connectivity with 0% packet loss.

*Figura 19 -Ping a otra vlan en misma red,Ping a otra vlan en otra red y Ping a vlan del access point en misma red*



## Examen ARG

**TABLA NAT:** La siguiente prueba que hicimos fue mostrar la tabla de nat con el comando `show ip nat translat` las cuales muestran las traducciones de las direcciones privadas que obtuvieron una dirección pública para poder navegar en internet, en la imagen se muestran las direcciones privadas y globales de las ips como se puede observar.

```
Router#show ip nat translations
Router#show ip nat translations
Outside local  Outside global
tcp 10.40.72.154:1025 172.15.0.1:1025 13.79.202.129:443 13.79.202.129:443
tcp 10.40.72.154:1026 172.15.0.1:1026 54.241.197.50:443 54.241.197.50:443
tcp 10.40.72.154:1027 172.15.0.1:1027 20.7.1.240:443 20.7.1.240:443
tcp 10.40.72.154:1028 172.15.0.1:1028 23.223.242.204:443 23.223.242.204:443
tcp 10.40.72.154:1029 172.15.0.1:1029 54.67.105.202:443 54.67.105.202:443
tcp 10.40.72.154:1030 172.15.0.1:1030 8.8.8.8:80 8.8.8.8:80
tcp 10.40.72.154:1031 172.15.0.1:1031 40.74.177.140:80 40.74.177.140:80
tcp 10.40.72.154:1032 172.15.0.1:1032 200.33.42.250:80 200.33.42.250:80
tcp 10.40.72.154:1033 172.15.0.1:1033 8.8.8.8:80 8.8.8.8:80
tcp 10.40.72.154:1034 172.15.0.1:1034 74.125.135.140:443 74.125.135.140:443
tcp 10.40.72.154:1035 172.15.0.1:1035 23.215.40.23:443 23.215.40.23:443
tcp 10.40.72.154:1036 172.15.0.1:1036 54.225.12.200:443 54.225.12.200:443
tcp 10.40.72.154:1037 172.15.0.1:1037 44.211.1.234:443 44.211.1.234:443
tcp 10.40.72.154:1038 172.15.0.1:1038 140.82.113.3:443 140.82.113.3:443
tcp 10.40.72.154:1039 172.15.0.1:1039 184.50.41.236:443 184.50.41.236:443
tcp 10.40.72.154:1040 172.15.0.1:1040 52.46.155.104:443 52.46.155.104:443
tcp 10.40.72.154:1041 172.15.0.1:1041 185.199.110.135:443 185.199.110.135:443
tcp 10.40.72.154:1042 172.15.0.1:1042 140.82.113.4:443 140.82.113.4:443
tcp 10.40.72.154:1043 172.15.0.1:1043 69.175.41.79:443 69.175.41.79:443
tcp 10.40.72.154:1044 172.15.0.1:1044 140.82.113.4:443 140.82.113.4:443
tcp 10.40.72.154:1045 172.15.0.1:1045 184.50.41.236:443 184.50.41.236:443
tcp 10.40.72.154:1046 172.15.0.1:1046 23.182.184.203:443 23.182.184.203:443
tcp 10.40.72.154:1047 172.15.0.1:1047 54.67.54.116:443 54.67.54.116:443
tcp 10.40.72.154:1048 172.15.0.1:1048 54.187.172.230:443 54.187.172.230:443
tcp 10.40.72.154:1049 172.15.0.1:1049 54.152.232.204:443 54.152.232.204:443
tcp 10.40.72.154:1050 172.15.0.1:1050 179.239.59.72:443 179.239.59.72:443
tcp 10.40.72.154:1051 172.15.0.1:1051 169.197.150.8:443 169.197.150.8:443
tcp 10.40.72.154:1052 172.15.0.1:1052 72.34.202.75:443 72.34.202.75:443
tcp 10.40.72.154:1053 172.15.0.1:1053 35.184.159.173:443 35.184.159.173:443
tcp 10.40.72.154:1054 172.15.0.1:1054 35.214.223.133:443 35.214.223.133:443
tcp 10.40.72.154:1055 172.15.0.1:1055 34.70.223.2:443 34.70.223.2:443
tcp 10.40.72.154:1056 172.15.0.1:1056 184.140.27.140:443 184.140.27.140:443
tcp 10.40.72.154:1057 172.15.0.1:1057 23.182.184.22:443 23.182.184.22:443
tcp 10.40.72.154:1058 172.15.0.1:1058 35.190.40.146:443 35.190.40.146:443
tcp 10.40.72.154:1059 172.15.0.1:1059 189.127.204.171:443 189.127.204.171:443
tcp 10.40.72.154:1060 172.15.0.1:1060 189.127.204.171:443 189.127.204.171:443
tcp 10.40.72.154:1061 172.15.0.1:1061 8.43.72.90:443 8.43.72.90:443
tcp 10.40.72.154:1062 172.15.0.1:1062 189.127.204.171:443 189.127.204.171:443
tcp 10.40.72.154:1063 172.15.0.1:1063 189.127.204.171:443 189.127.204.171:443
tcp 10.40.72.154:1064 172.15.0.1:1064 72.34.202.75:443 72.34.202.75:443
tcp 10.40.72.154:1065 172.15.0.1:1065 23.215.41.250:443 23.215.41.250:443
tcp 10.40.72.154:1066 172.15.0.1:1066 23.182.184.22:443 23.182.184.22:443
tcp 10.40.72.154:1067 172.15.0.1:1067 179.239.59.72:443 179.239.59.72:443
tcp 10.40.72.154:1068 172.15.0.1:1068 8.43.72.90:443 8.43.72.90:443
tcp 10.40.72.154:1069 172.15.0.1:1069 8.43.72.90:443 8.43.72.90:443
tcp 10.40.72.154:1070 172.15.0.1:1070 184.50.41.236:443 184.50.41.236:443
tcp 10.40.72.154:1071 172.15.0.1:1071 54.187.172.230:443 54.187.172.230:443
tcp 10.40.72.154:1072 172.15.0.1:1072 84.175.47.128:443 84.175.47.128:443
tcp 10.40.72.154:1073 172.15.0.1:1073 179.239.59.72:443 179.239.59.72:443
tcp 10.40.72.154:1074 172.15.0.1:1074 155.203.145.121:443 155.203.145.121:443
tcp 10.40.72.154:1075 172.15.0.1:1075 20.127.251.7:443 20.127.251.7:443
tcp 10.40.72.154:1076 172.15.0.1:1076 5.17.243.71:443 5.17.243.71:443
```

Figura 20-Tabla del nat

**TABLA ARP:** Después de las tablas Nat, usamos el comando `arp -a` para que nos muestro la tabla arp en las cuales se puede observar las direcciones físicas vinculadas con las direcciones ip dentro de una Red, las direcciones físicas estáticas son porque no pertenecen a un dispositivo y las dinámicas si pertenecen a un dispositivo porque estas pueden variar.

```
C:\Users\gdaalumno>arp -a

Interfaz: 172.15.0.9 --- 0x5
Dirección de Internet      Dirección física      Tipo
169.254.169.254            50-57-a8-e0-d0-60    dinámico
172.15.0.14                 50-57-a8-e0-d0-60    dinámico
172.15.0.15                 ff-ff-ff-ff-ff-ff     estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb     estático
224.0.0.252                01-00-5e-00-00-fc     estático
239.255.255.250            01-00-5e-7f-ff-fa     estático
255.255.255.255            ff-ff-ff-ff-ff-ff     estático

Interfaz: 172.15.1.18 --- 0xe
Dirección de Internet      Dirección física      Tipo
172.15.1.22                50-57-a8-3e-9e-c8    dinámico
172.15.1.23                ff-ff-ff-ff-ff-ff     estático
224.0.0.22                01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb     estático
224.0.0.252                01-00-5e-00-00-fc     estático
239.255.255.250            01-00-5e-7f-ff-fa     estático
255.255.255.255            ff-ff-ff-ff-ff-ff     estático
```

Figura 21-arp

## Examen ARG

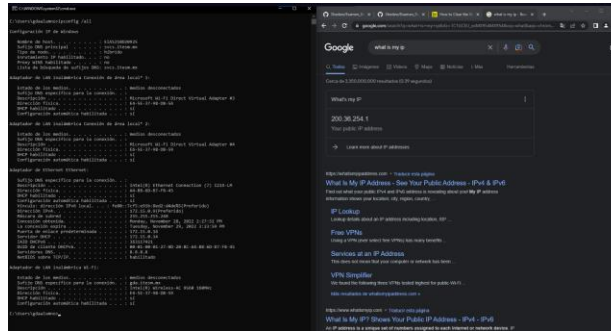


Figura 22- Ip pública

**TABLAS DE RUTEO:** Los enrutadores lo usan para enviar paquetes de datos a la red de destino. Los enrutadores se basan en la dirección IP de destino del paquete para enrutar el paquete a su destino y en la imagen se puede ver que dos de ellas necesitan dos saltos y eso es porque un salto es para la Gateway y el otro salto a la dirección destino y eso sucede por que están dentro de la misma red, el que ocupa tres saltos no está dentro de la misma red está en una red vecina por lo que hace un salto extra al otro router vecino para después redirigir la dirección destino.

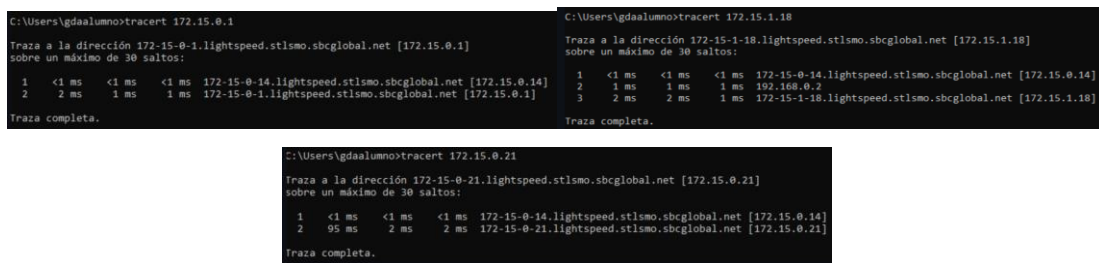
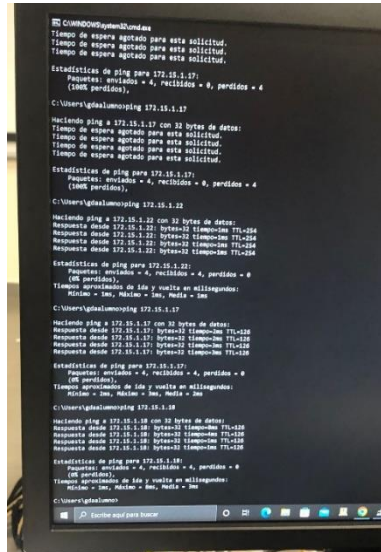


Figura 23-Tracert a otra red, tracert en misma red por access point y tracert en una misma red

## Examen ARG



*Figura 24. Pings a diferentes ip.*

### Configuración de ACL para filtrar al equipo minecraft:

Los 3 comandos para su declaración son los siguientes:

- access-list 102 remark Minecraft deny-ssh
- access-list 102 deny tcp any any eq 25565 time-range time-ssh
- access-list 102 permit ip any any

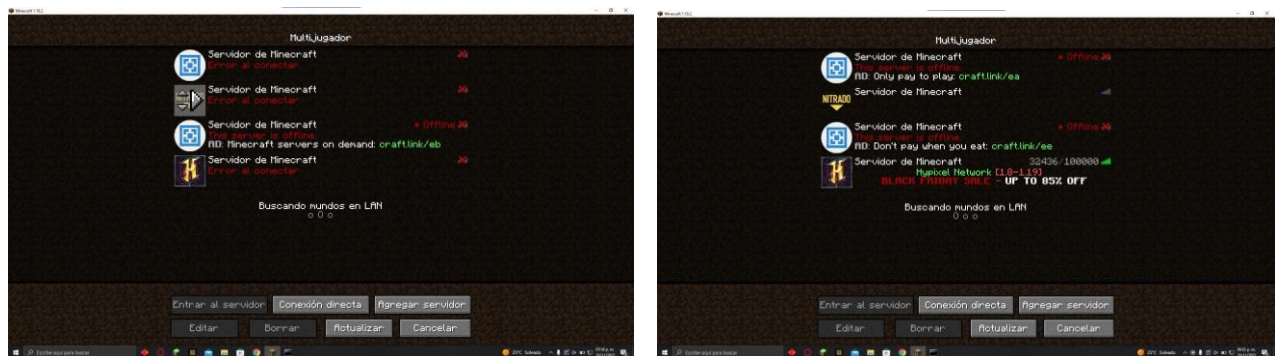
El primero de estos comandos solo nos sirve como comentario para saber que hacer, el segundo comando nos sirve para negar el acceso a puerto 25565 default de minecraft para negarnos el acceso, y el time range nos sirve para negar dentro del tiempo que queremos y el último comando nos permite todo porque antes teníamos un negar todo implícito.

Después de realizar todas las configuraciones creíamos que teníamos todo bien, pero a la hora de probar si negaba el acceso a Minecraft nos dimos cuenta que aún teníamos acceso por lo que empezamos a buscar los errores. Al principio nos dimos cuenta que teníamos el error porque estaba negando todo, ya que teníamos un negar todo implícito y ese error lo corregimos con el ultimo comando del ACL que básicamente lo que hace es permitir todo,

## Examen ARG

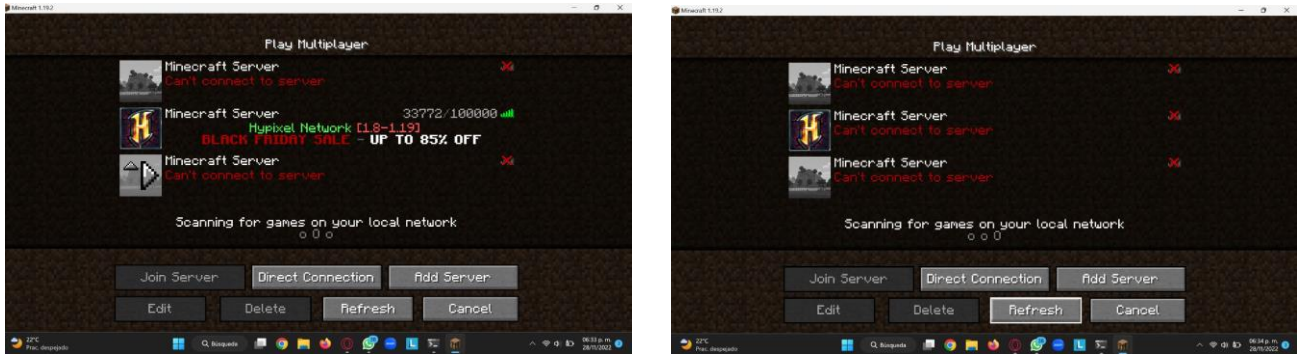
después de corregir ese error volvimos a intentar la conexión y otra vez nos dejó entrar entonces después nos dimos cuenta que la hora a la que estaban los routers era diferente a nuestra hora diaria y la configuración se basó en nuestra hora por lo que nos daba error, entonces para solucionarlo le tuvimos que cambiar la hora a nuestro router mediante el comando `!clock set 17:55:00 28 NOV 2022` para que entrara en vigor la hora en la que denegamos el acceso a minecraft y ya con eso empezó a funcionar.

Como se puede observar en las siguientes 4 figuras en las cuales se ve que nos denegaba el accesos antes de las 6 y después ya nos dejaba entrar, las primeras figuras son con conexión alámbrica por medio de ethernet y las figuras 27-28 es mediante la conexión inalámbrica.



*Figura 25-26. Conexión fallida y exitosa Minecraft con ethernet*

## Examen ARG



*Figura 27-28. Conexión exitosa y fallida Minecraft con conexión inalámbrica*