

## Laboratorio No. 6 – Parte 2

### Capa de red

#### MARCO TEÓRICO

---

##### **Routers:**

Los routers guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web. Los paquetes de datos tienen varias capas o secciones; una de ellas transporta la información de identificación, como emisor, tipo de datos, tamaño y, aún más importante, la dirección IP (protocolo de Internet) de destino. El router lee esta capa, prioriza los datos y elige la mejor ruta para cada transmisión.

De igual manera, son una herramienta común para la computación en red moderna, los routers conectan a los empleados a las redes locales y a Internet, donde se realizan casi todas las actividades empresariales esenciales. Sin routers, no podríamos usar Internet para colaborar, comunicarnos o recopilar información y aprender.

Los routers también pueden proporcionar seguridad. El software de firewall y filtrado de contenido integrado proporciona una protección adicional contra el contenido no deseado y los sitios web maliciosos, sin que esto afecte la experiencia en línea.

No obstante, un router no solo sirve para la transmisión de datos o las conexiones a Internet. La mayoría de los routers permiten conectar discos duros y usarlos como servidores de uso compartido de archivos, o impresoras a las que pueden acceder todos los usuarios de la red.

##### **Protocolo ICMP**

*Internet Control Message Protocol* (ICMP) es responsable de reportar errores a través de la generación y envío de mensajes a la dirección IP de origen cuando hay problemas de red que son encontrados por el sistema.

Los mensajes que genera la ICMP indican que no se puede acceder a un determinado gateway, router, servicio o incluso host que deba conectarse a Internet. Básicamente, el destinatario no puede recibir paquetes durante la transmisión. Cualquier dispositivo de red IP puede enviar, generar, recibir y procesar mensajes de error ICMP.

Como función principal, la ICMP no es necesariamente usada regularmente por individuos en aplicaciones de usuario final, sino que es utilizada por

numerosos administradores de red con el fin de solucionar cualquier error presente en las conexiones de Internet a través de un diagnóstico de utilidad como:

- *Ping*

**Packet Internet Gopher**, es una herramienta de diagnóstico que prueba la conectividad entre dos nodos o dispositivos a través de una red. PING verifica si un paquete de datos de red es capaz de ser distribuido a una dirección sin tener errores. También determina la accesibilidad a la red de una dirección IP específica y se utiliza para determinar y asegurar que una computadora host a la que un usuario está tratando de llegar esté realmente operando. Principalmente, PING se utiliza para solucionar problemas de conexión a Internet. En pocas palabras, PING se utiliza comúnmente para comprobar los errores que tiene la red y también significa simplemente "llamar la atención de" o "comprobar la presencia de".

- *Traceroute*

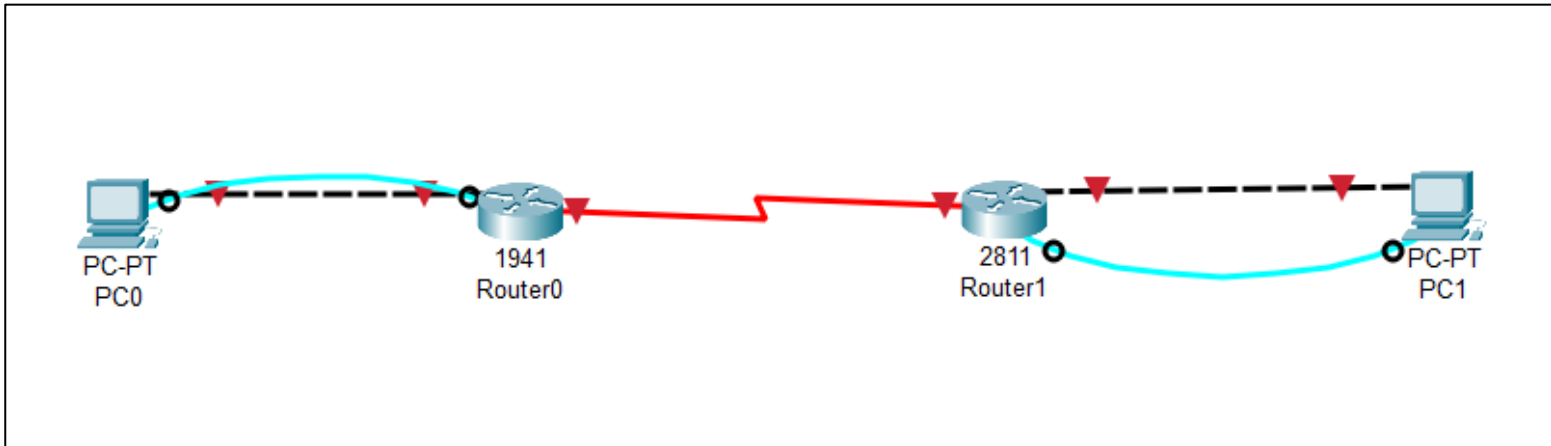
Es una herramienta de diagnóstico de red que se utiliza para registrar la ruta o los ordenadores específicos de la pasarela en cada salto a través de Internet entre el ordenador y otro ordenador de destino especificado en el proceso de transmisión de datos. Calcula y muestra el tiempo que tardó cada salto. También se utiliza para rastrear la ruta tomada por un paquete en una red de Protocolo de Internet (IP) desde la fuente hasta el destino. Este procedimiento permite al usuario averiguar con precisión cómo sería la transmisión de datos, como una búsqueda en Google, de un dispositivo informático a otro. Además, traceroute es una herramienta muy útil que se utiliza tanto para entender dónde están los problemas en la red como para obtener una visión detallada de la propia Internet.

## **Protocolo ARP**

El ARP (protocolo Protocolo de resolución de la dirección (ARP)) se utiliza para no perder de vista todos los dispositivos que estén conectados directamente con el Switch. El Switch mantiene una tabla ARP que tenga la dirección IP y la dirección MAC de cada dispositivo conectado con el Switch. Cuando un paquete necesita ser ruteado a cierto dispositivo, el Switch mira para arriba la dirección IP del dispositivo en su tabla ARP para obtener la dirección MAC del dispositivo de destino. La tabla ARP da la información útil sobre los diversos dispositivos conectados. En caso de que el Switch no pueda decir si un dispositivo está conectado o no, la tabla ARP puede ayudar a determinar este problema. También, usted puede agregar manualmente los dispositivos a la tabla ARP, que da más Seguridad a la red mientras que usted no pierde de vista qué dispositivos son parte de la tabla ARP.

## 1. ACCESO Y CONFIGURACIÓN BÁSICA A LOS ROUTERS

- Montaje.



Contorno de color azul → PC0 - ROUTER 0  
Contorno de color amarillo → PC1 - ROUTER 1

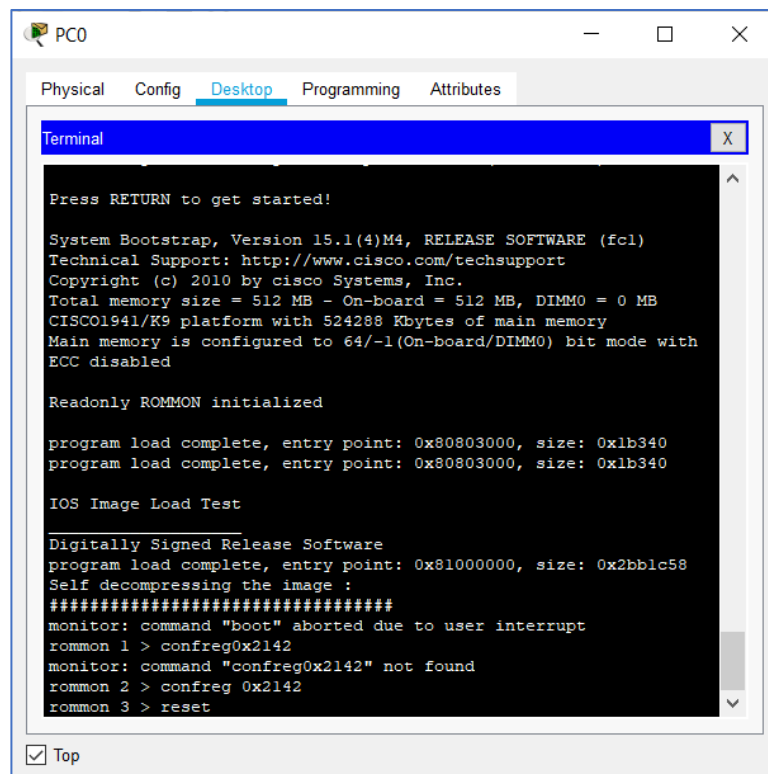
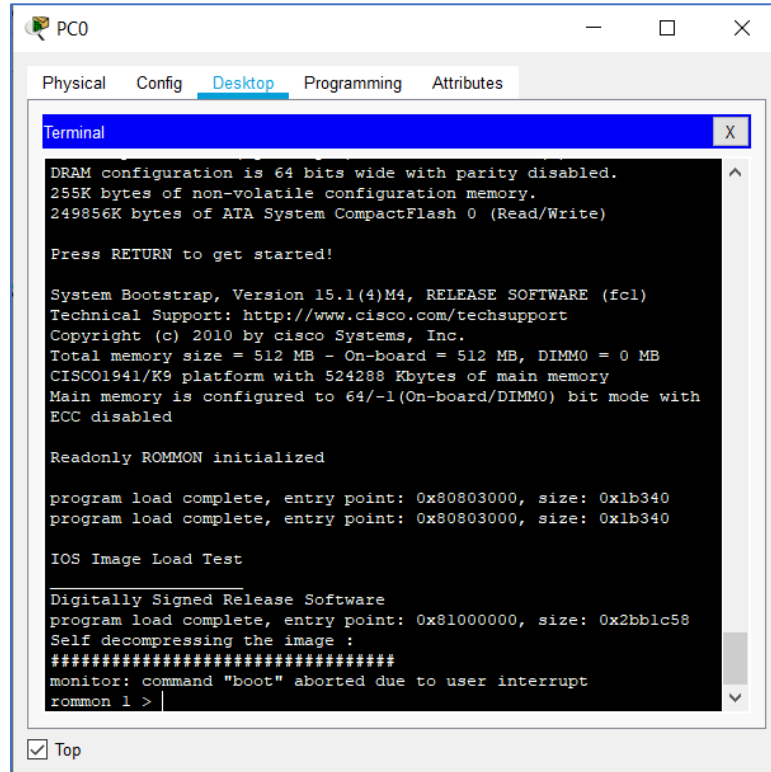
- Cambio de configuración para acceder al modo privilegiado.

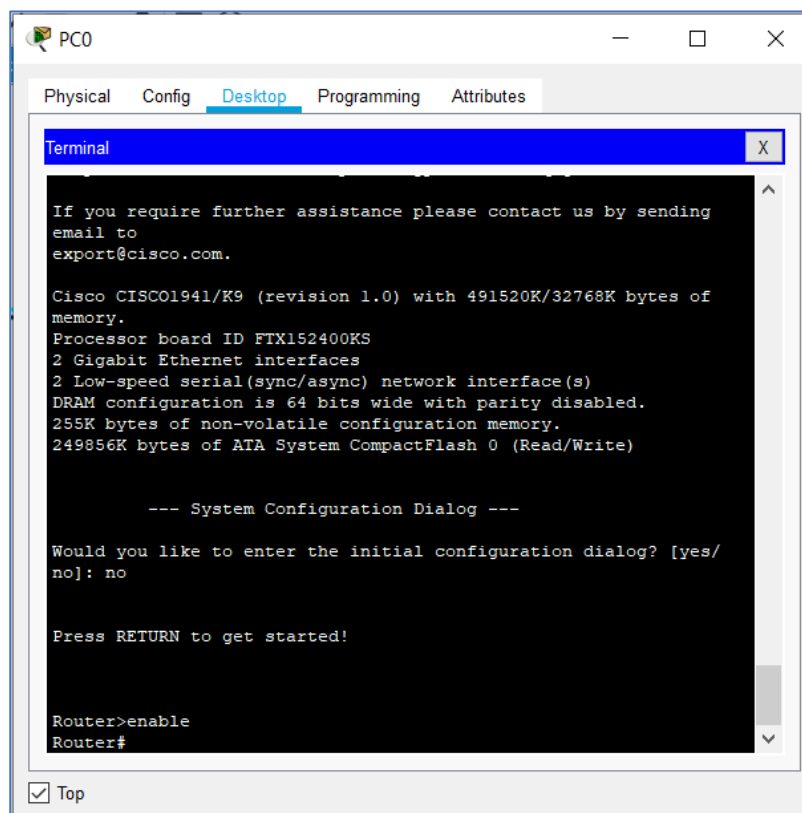
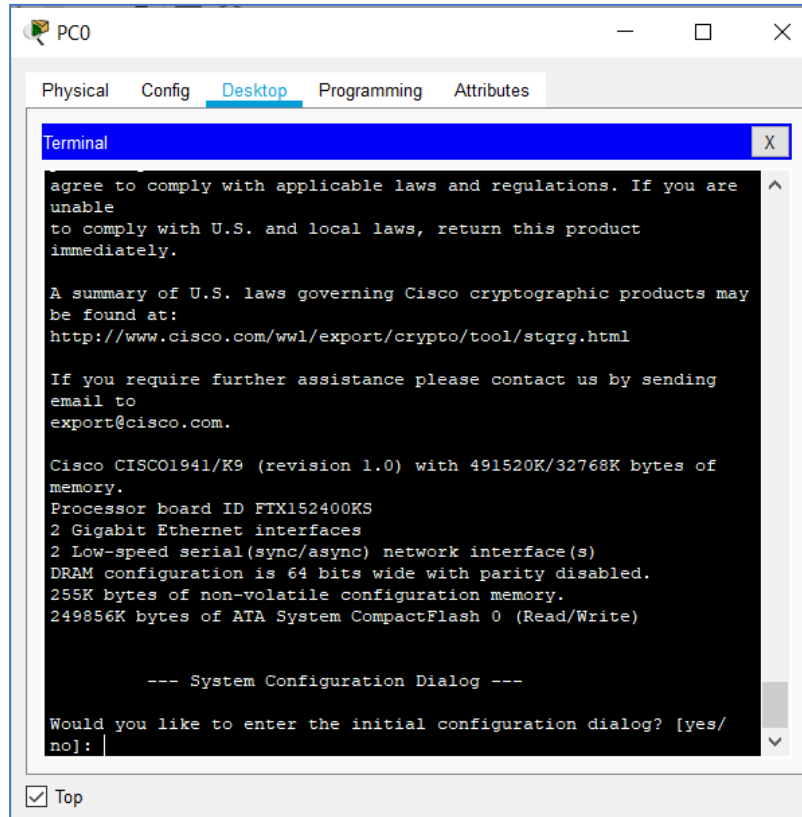
Al momento de empezar la configuración básica de los router nos dimos cuenta de que los router ya estaban configurados y por lo tanto no podíamos acceder ya que no conocíamos clave ni la información configurada.

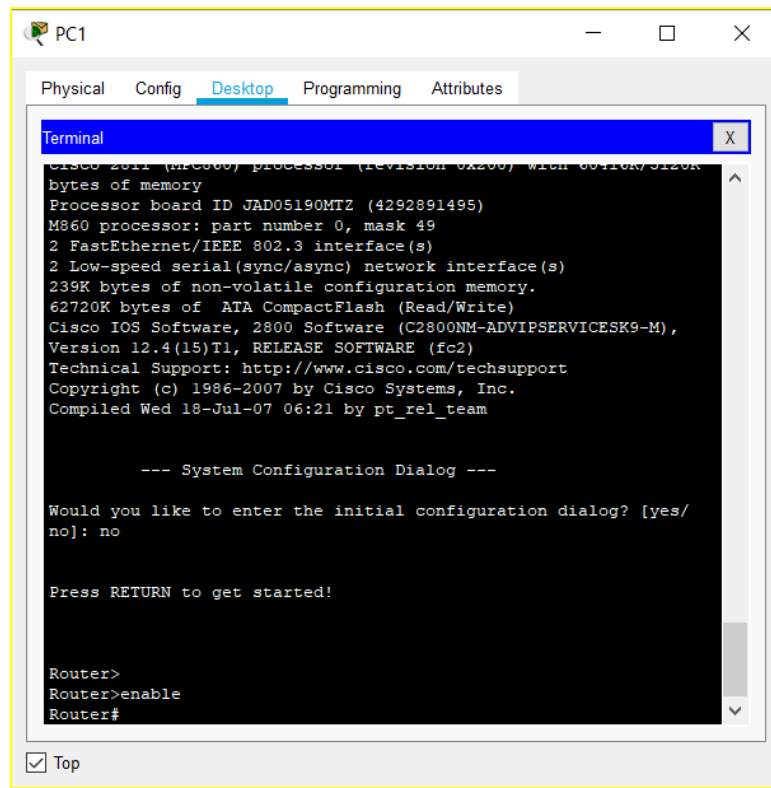
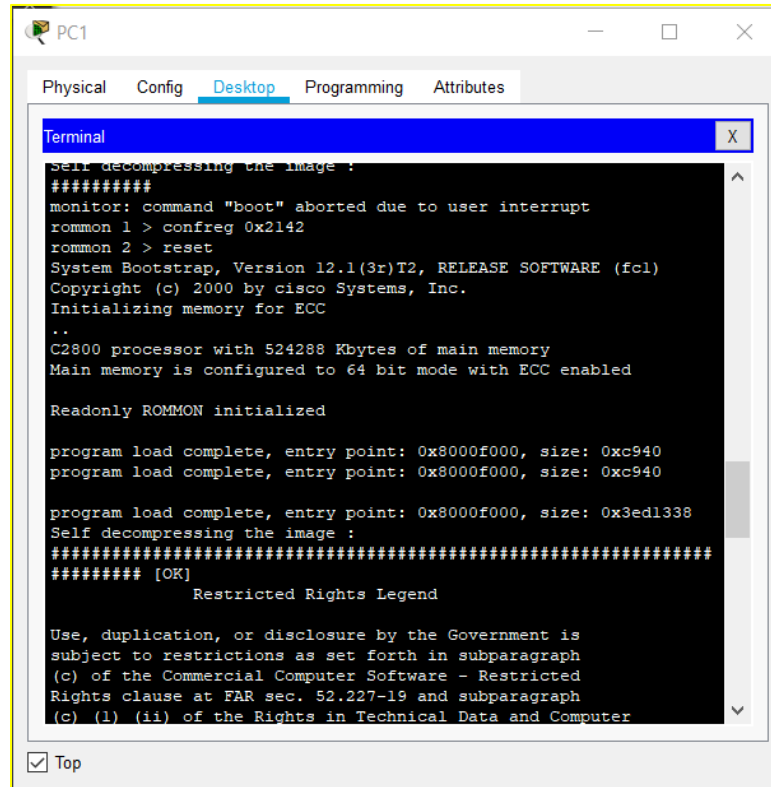
Entonces, el paso a seguir era eliminar cuanto información tuvieran para poder empezar a configurarlos como nosotros queríamos para esto debemos:

- Apagar el router y prenderlo, para que inicie la carga del IOS, una vez inicie la carga debemos interrumpir el arranque presionando **Ctrl + c** y así iniciar en el modo ROM.
- Allí escribimos el comando **confreg 0x2142**.
- Luego damos reset para reiniciar el router.
- Luego de esto preguntará si deseamos crear una configuración básica automática y le pondremos **no**.

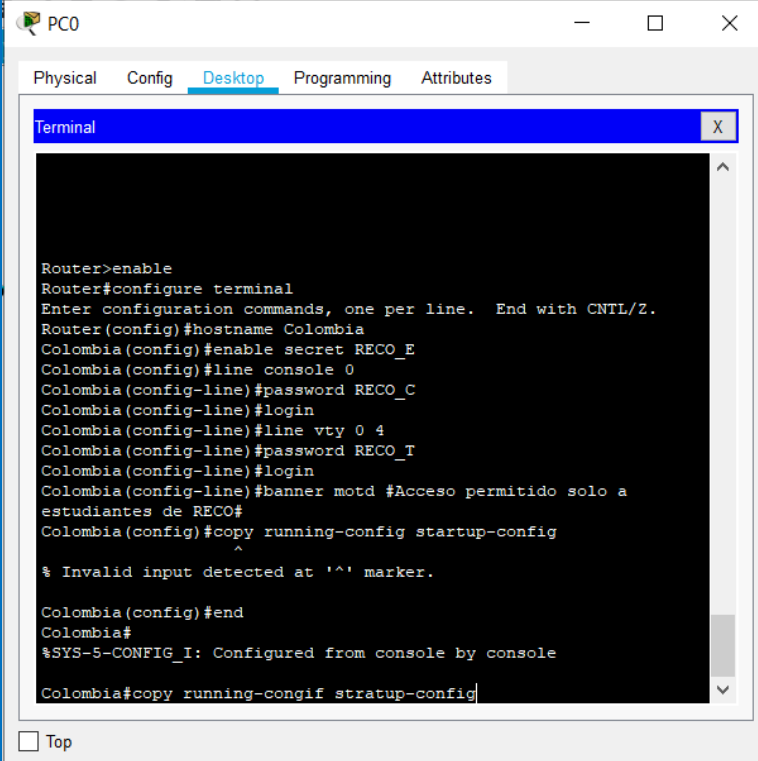
Una vez realizados estos pasos podremos ver como ya tenemos acceso al modo privilegiado para empezar nuestra propia configuración.







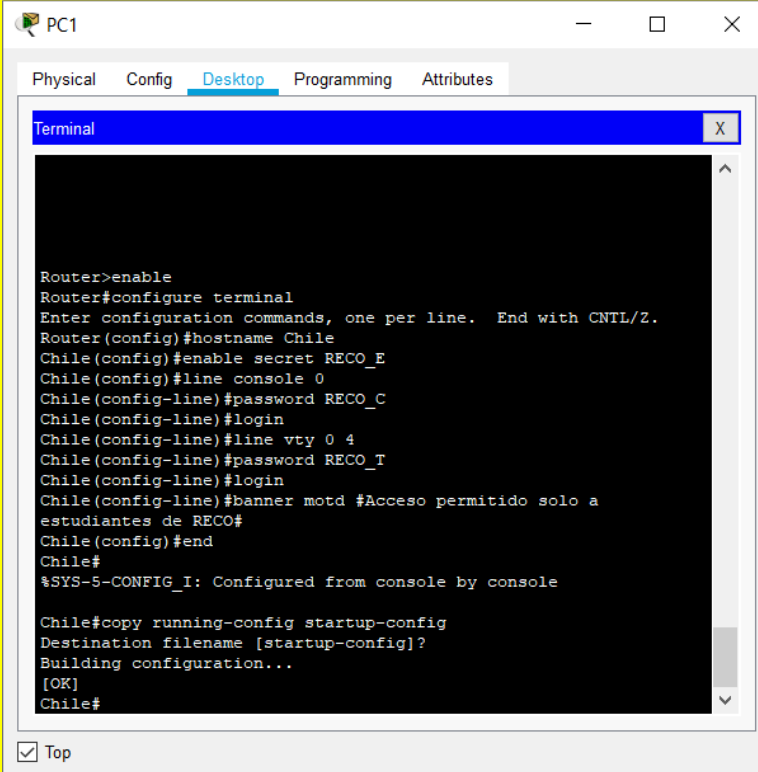
- Configuración nombre y claves:



The screenshot shows a terminal window titled 'PC0' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a terminal session. The user enters 'enable' to enter privileged mode, then 'configure terminal' to enter configuration mode. The configuration includes setting the hostname to 'Colombia', enabling secret passwords, configuring console and vty lines with passwords 'RECO\_C' and 'RECO\_T' respectively, and setting a MOTD banner. Finally, the running configuration is copied to the startup configuration. The terminal shows the following commands and output:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Colombia
Colombia(config)#enable secret RECO_E
Colombia(config)#line console 0
Colombia(config-line)#password RECO_C
Colombia(config-line)#login
Colombia(config-line)#line vty 0 4
Colombia(config-line)#password RECO_T
Colombia(config-line)#login
Colombia(config-line)#banner motd #Acceso permitido solo a
estudiantes de RECO#
Colombia(config)#copy running-config startup-config
^
% Invalid input detected at '^' marker.
Colombia(config)#end
Colombia#
%SYS-5-CONFIG_I: Configured from console by console
Colombia#copy running-congif stratup-config
```

*ROUTER 0*



The screenshot shows a terminal window titled 'PC1' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a terminal session. The user enters 'enable' to enter privileged mode, then 'configure terminal' to enter configuration mode. The configuration includes setting the hostname to 'Chile', enabling secret passwords, configuring console and vty lines with passwords 'RECO\_C' and 'RECO\_T' respectively, and setting a MOTD banner. Finally, the running configuration is copied to the startup configuration. The terminal shows the following commands and output:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Chile
Chile(config)#enable secret RECO_E
Chile(config)#line console 0
Chile(config-line)#password RECO_C
Chile(config-line)#login
Chile(config-line)#line vty 0 4
Chile(config-line)#password RECO_T
Chile(config-line)#login
Chile(config-line)#banner motd #Acceso permitido solo a
estudiantes de RECO#
Chile(config)#end
Chile#
%SYS-5-CONFIG_I: Configured from console by console
Chile#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Chile#
```

*ROUTER 1*

- Sincronización de pantallas de consola y acceso remoto.

```
Colombia#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Colombia(config)#line console 0
Colombia(config-line)#login synchronous
Colombia(config-line)#no ip domain-lookup
Colombia(config)#
```

☐ Top

*ROUTER COLOMBIA*

PC1

Physical Config Desktop Programming Attributes

Terminal X

```
Chile>enable
Password:
Chile#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Chile(config)#line conole 0
      ^
% Invalid input detected at '^' marker.

Chile(config)#line console 0
Chile(config-line)#login synchronous
Chile(config-line)#end
Chile#
%SYS-5-CONFIG_I: Configured from console by console

Chile#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Chile(config)#no ip domain-lookup
Chile(config)#end
Chile#
%SYS-5-CONFIG_I: Configured from console by console

Chile#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Chile#
```

☐ Top

*ROUTER CHILE*



- Configuración interfaces.

Para la configuración de las interfaces, en la conexión entre el computador y el router se tomo la primera dirección ip de la red dada en el laboratorio. Esta sería el mismo Gateway para el PC. En la conexión entre los routers se utilizaron las siguientes dos redes de la red dada en el laboratorio.

```
Colombia#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Colombia(config)#interface GigabitEthernet0/0
Colombia(config-if)#description Conexion a la LAN - Equipo PC0"
Colombia(config-if)#ip address 80.123.128.1 255.255.192.0
Colombia(config-if)#
```

☐ Top

```
Colombia(config)#interface Serial0/1/0
Colombia(config-if)#description Conexion WAN entre routers
Colombia(config-if)#ip address 100.56.120.4 255.255.255.252
Bad mask /30 for address 100.56.120.4
Colombia(config-if)#ip address 100.56.120.5 255.255.255.252
Colombia(config-if)#end
Colombia#
%SYS-5-CONFIG_I: Configured from console by console

Colombia#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Colombia#
```

☐ Top

```
Chile#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Chile(config)#interface FastEthernet0/0
Chile(config-if)#descriptionConexion a la LAN - Equipo PC1
^
% Invalid input detected at '^' marker.

Chile(config-if)#description Conexion a la LAN - Equipo PC1
Chile(config-if)#ip address 90.250.64.1 255.255.240.0
Chile(config-if)#
```

☐ Top

```
Chile(config)#interface Serial0/3/0
Chile(config-if)#description Conexion WAN entre routers
Chile(config-if)#ip address 100.56.120.6 255.255.255.252
Chile(config-if)#
Chile(config-if)#end
Chile#
%SYS-5-CONFIG_I: Configured from console by console

Chile#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Chile#
```

☐ Top

- Configuración ip - equipos.

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 80.123.128.2

Subnet Mask 255.255.192.0

Default Gateway 80.123.128.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::202:4AFF:FEEC:9621

Default Gateway

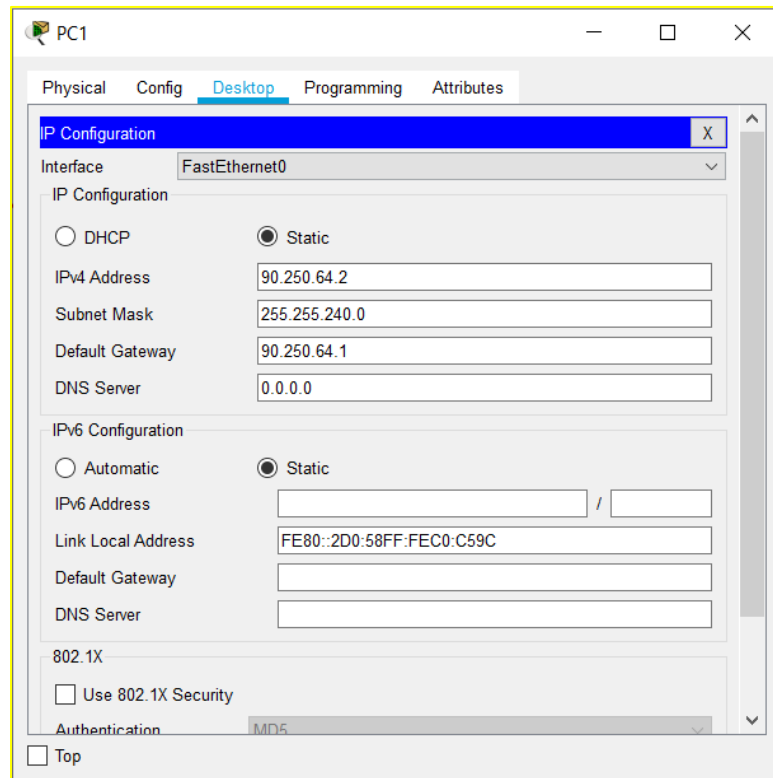
DNS Server

802.1X

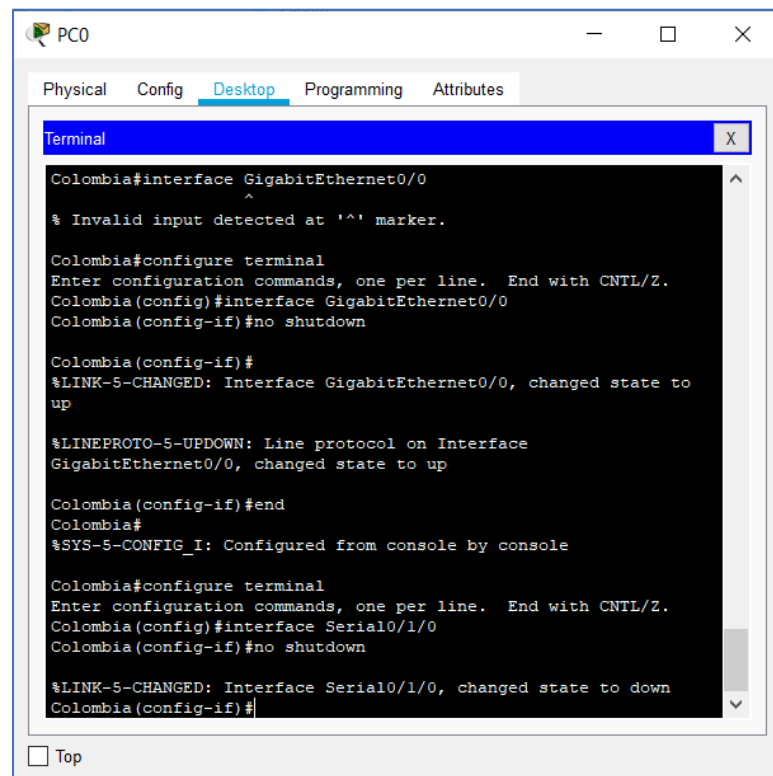
☐ Use 802.1X Security

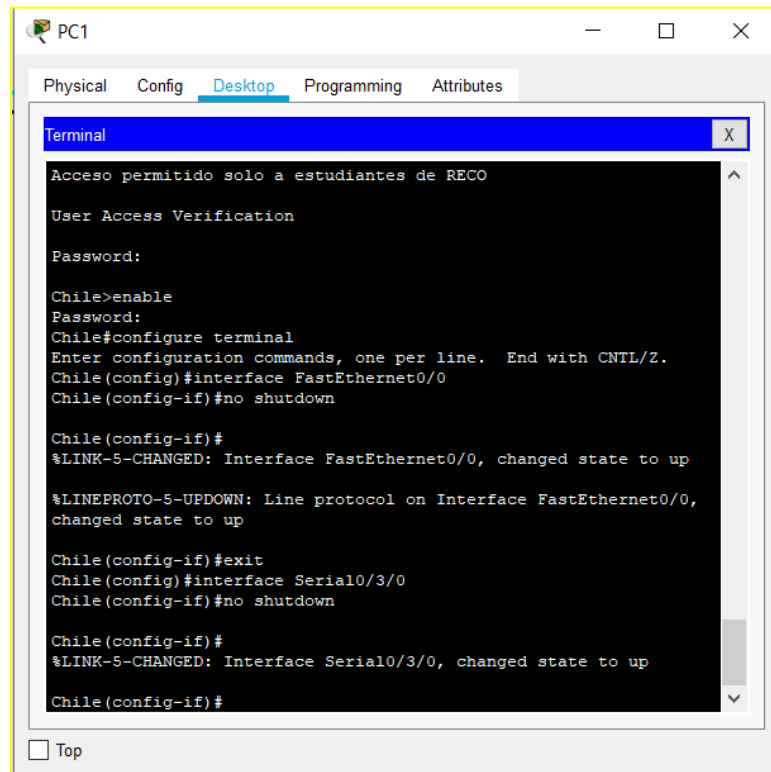
Authentication MD5

☐ Top



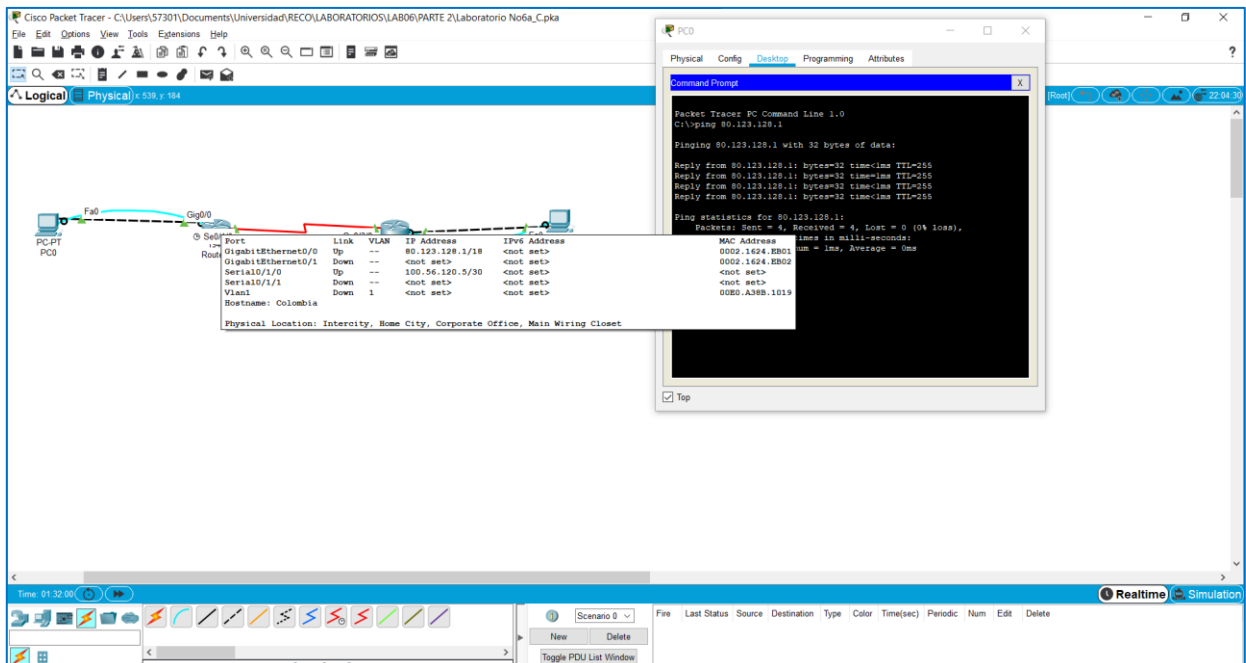
- Activar puertos

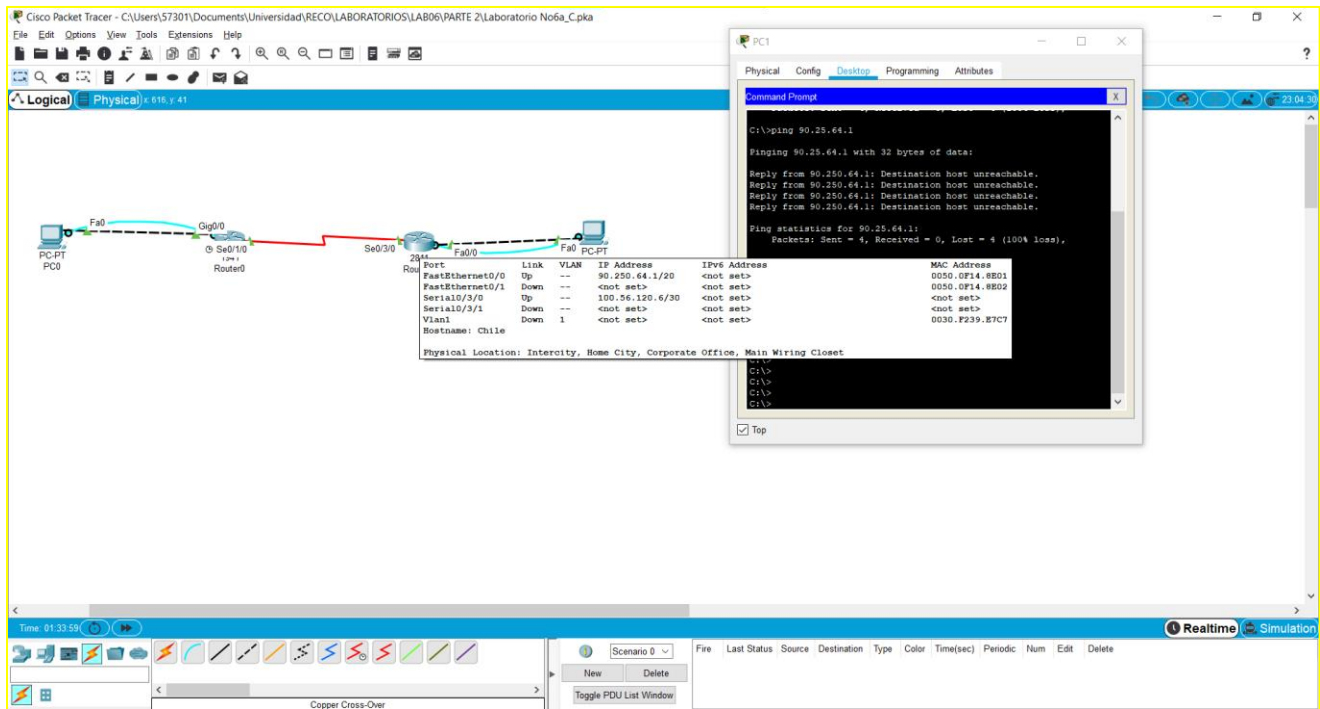




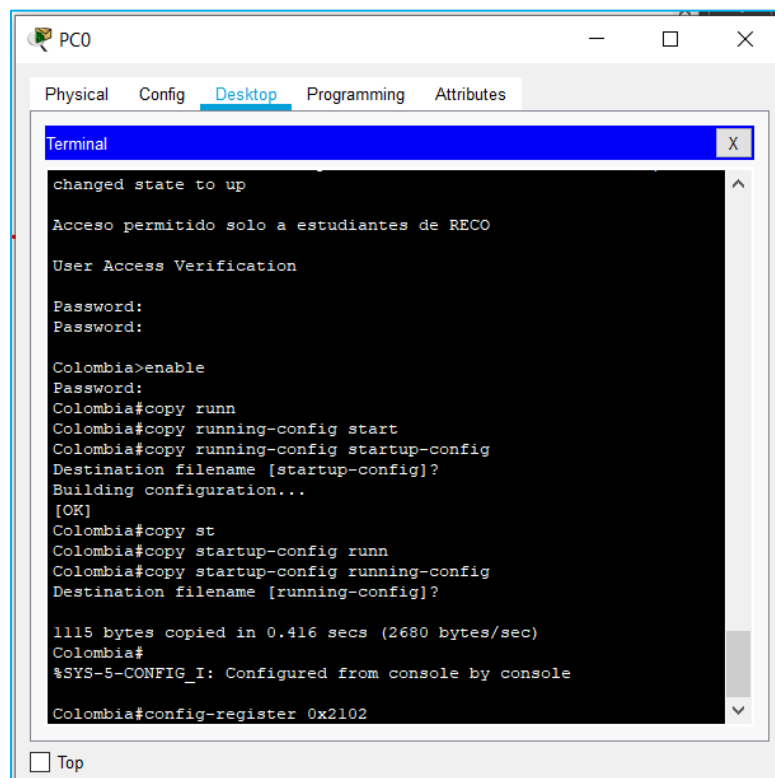
- Conectividad.

La conectividad entre cada computador y su router fue válida, en cambio al momento de hacer ping entre los dos computadores no fue posible





- Cambiar modo de arranque.



- ARCHIVOS 100%

PT Activity: 05:42:12

## Laboratorio No 6 parte 2

### Trabajo con Routers

Siga las instrucciones dadas en el documento del Laboratorio. En el botón [Check Results](#), pestaña [Assessment Items](#) puede revisar lo que falta para

... quiere reestablecer la ... de lo contrario, se

Completion: 100%

1/1 >

**Activity Results**

**Congratulations Ana Gabriela ! You completed the activity.**

[Overall Feedback](#) [Assessment Items](#) [Connectivity Tests](#)

**Congratulations on completing this activity!**

PT Activity: 01:15:26

## Laboratorio No 6 parte 2

### Trabajo con Routers

Siga las instrucciones dadas en el documento del Laboratorio. En el botón [Check Results](#), pestaña [Assessment Items](#) puede revisar lo que falta para

... CLI del router si requiere reestablecer la ... privilegiado del equipo, de lo contrario, se

Completion: 100%

activity < 1/1 >

**Activity Results**

**Congratulations Sebastián Mina! You completed the activity.**

[Overall Feedback](#) [Assessment Items](#) [Connectivity Tests](#)

**Congratulations on completing this activity!**

## 2. SEGUIMIENTO PROTOCOLO ARP

Para revisar la tabla arp en el computador, ejecutaremos el comando **arp -a**. Nos muestra tres columnas, la primera muestra las direcciones IP, las segundas las direcciones MAC y la tercera el tipo (Dinámico o estático).

Las direcciones estáticas son un IP asignada a un dispositivo y nunca se modifica. En cambio, una dirección IP dinámica es la que cambia cada cierto tiempo.

```
C:\Users\57301>arp -a

Interfaz: 192.168.188.1 --- 0x8
Dirección de Internet      Dirección física      Tipo
192.168.188.255           ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    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
224.0.1.187                01-00-5e-00-01-bb    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático

Interfaz: 192.168.0.18 --- 0xa
Dirección de Internet      Dirección física      Tipo
192.168.0.1                b0-c2-87-28-25-19    dinámico
192.168.0.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    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
239.255.255.253            01-00-5e-7f-ff-fd    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

Interfaz: 192.168.79.1 --- 0x14
Dirección de Internet      Dirección física      Tipo
192.168.79.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    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
224.0.1.187                01-00-5e-00-01-bb    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
```

```
C:\> Símbolo del sistema
Microsoft Windows [Versión 10.0.18363.1500]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ARP -a

Interfaz: 192.168.1.14 --- 0xa
Dirección de Internet      Dirección física      Tipo
192.168.1.1                4c-6e-6e-28-5a-63    dinámico
192.168.1.13              f8-77-b8-9f-b1-49    dinámico
192.168.1.255             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
```

Tabla ARP – Sebastián

- Borrar tabla arp: se utiliza el comando ***netsh interface ip delete arpcache***, se vuelve a ejecutar el comando arp -a para verificar que sí se halla eliminado.

```
C:\WINDOWS\system32>netsh interface ip delete arpcache
Aceptar

C:\WINDOWS\system32>arp -a

Interfaz: 192.168.188.1 --- 0x8
Dirección de Internet      Dirección física      Tipo
224.0.0.22                 01-00-5e-00-00-16    estático

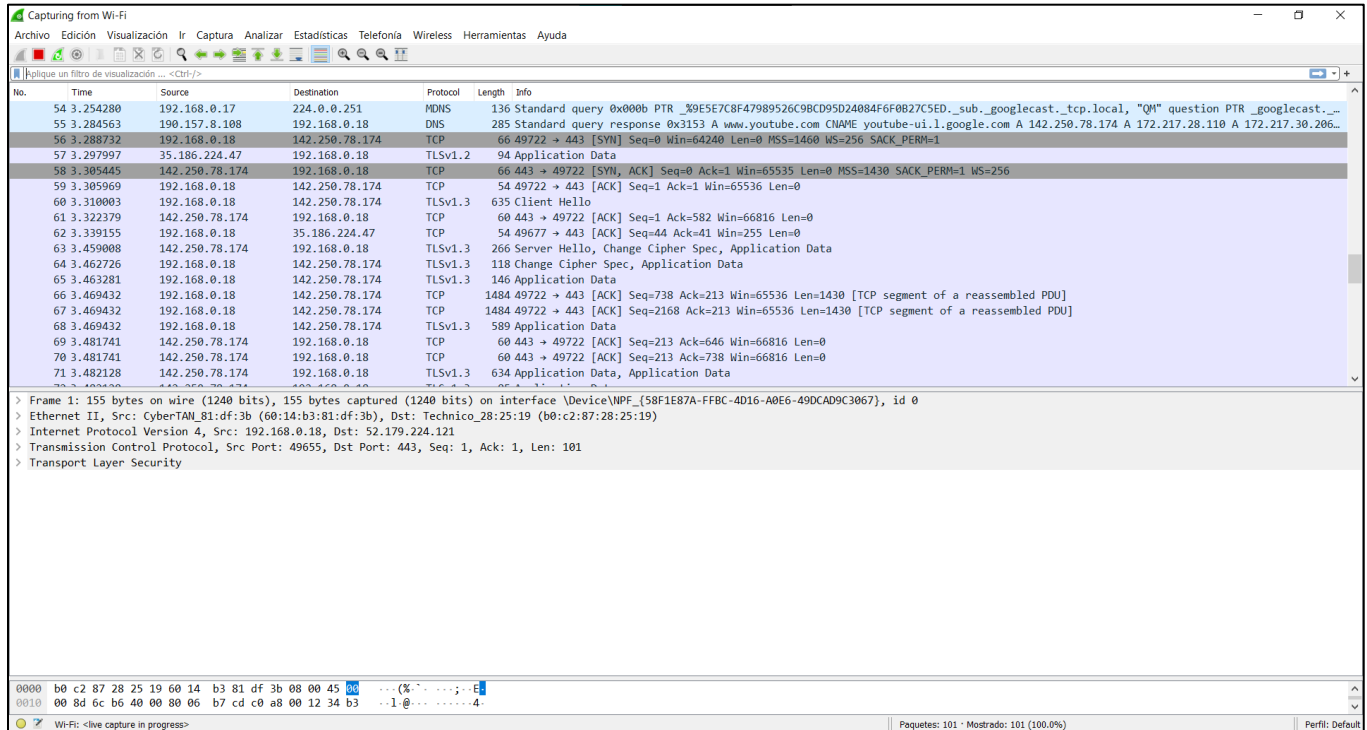
Interfaz: 192.168.0.18 --- 0xa
Dirección de Internet      Dirección física      Tipo
192.168.0.1                b0-c2-87-28-25-19    dinámico
224.0.0.2                  01-00-5e-00-00-02    estático

Interfaz: 192.168.79.1 --- 0x14
Dirección de Internet      Dirección física      Tipo
224.0.0.22                 01-00-5e-00-00-16    estático

C:\WINDOWS\system32>
```



- Sniffer corriendo.



- Ping a [www.google.com](http://www.google.com)

```
C:\Users\57301>ping www.google.com

Haciendo ping a www.google.com [142.250.78.100] con 32 bytes de datos:
Respuesta desde 142.250.78.100: bytes=32 tiempo=17ms TTL=118
Respuesta desde 142.250.78.100: bytes=32 tiempo=24ms TTL=118
Respuesta desde 142.250.78.100: bytes=32 tiempo=14ms TTL=118
Respuesta desde 142.250.78.100: bytes=32 tiempo=24ms TTL=118

Estadísticas de ping para 142.250.78.100:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 14ms, Máximo = 24ms, Media = 19ms
```

Después de realizar el ping, vemos cuantas veces se hizo uso del protocolo ARP, haciendo el request del destino, como se muestra en la siguiente imagen.

\*Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

arp

No.	Time	Source	Destination	Protocol	Length	Info
19393	531.439362	Technico_28:25:19	Broadcast	ARP	60	Who has 192.168.0.17? Tell 192.168.0.1
19394	531.540920	Technico_28:25:19	Broadcast	ARP	60	Who has 192.168.0.18? Tell 192.168.0.1
19395	531.541039	CyberTAN_81:df:3b	Technico_28:25:19	ARP	42	192.168.0.18 is at 60:14:b3:81:df:3b
19558	550.271380	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
19569	553.277379	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
19570	554.288959	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
19574	555.283529	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
19575	557.287587	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
19576	558.279179	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
19586	559.275136	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
19588	565.295101	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
19589	566.281827	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
19590	567.270373	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
19689	614.282579	2a:01:85:af:9a:33	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.11
19695	615.304776	2a:01:85:af:9a:33	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.11
19696	617.351183	2a:01:85:af:9a:33	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.11
19700	618.274328	2a:01:85:af:9a:33	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.11
19854	667.937347	Apple_42:5f:5b	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.12
19860	668.962506	Apple_42:5f:5b	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.12
19864	669.985024	Apple_42:5f:5b	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.12
19873	671.013353	Apple_42:5f:5b	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.12
19880	671.930583	Apple_42:5f:5b	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.12
33415	805.983483	2a:01:85:af:9a:33	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.11
33430	806.999326	2a:01:85:af:9a:33	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.11
33598	808.024060	2a:01:85:af:9a:33	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.11
34073	809.044963	2a:01:85:af:9a:33	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.11
34085	810.069512	2a:01:85:af:9a:33	Broadcast	ARP	42	Who has 192.168.0.2? Tell 192.168.0.11
40839	872.774830	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
40869	875.308258	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
42917	876.285013	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
42919	877.283760	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
42921	879.309437	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
43512	880.281063	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
43513	881.278299	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
43613	887.317408	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
43627	888.278221	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18
43634	889.279501	CyberTAN_81:df:3b	Broadcast	ARP	42	Who has 192.168.0.28? Tell 192.168.0.18

Frame 15884: A2 bytes on wire (336 bits) A2 bytes captured (336 bits) on interface \Device\NPF\_{58E1E874-FFC8-AD16-80F6-A9DCAD9C3067}\_id 0

Address Resolution Protocol: Protocol Paquetes: 43950 - Mostrado: 105 (0.2%) Perfil: Default

Después de esto, se ve que la tabla arp se vuelve a construir por la realización del ping.

```
C:\Users\57301>arp -a

Interfaz: 192.168.188.1 --- 0x8
Dirección de Internet      Dirección física      Tipo
192.168.188.255            ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    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
224.0.1.187                01-00-5e-00-01-bb    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático

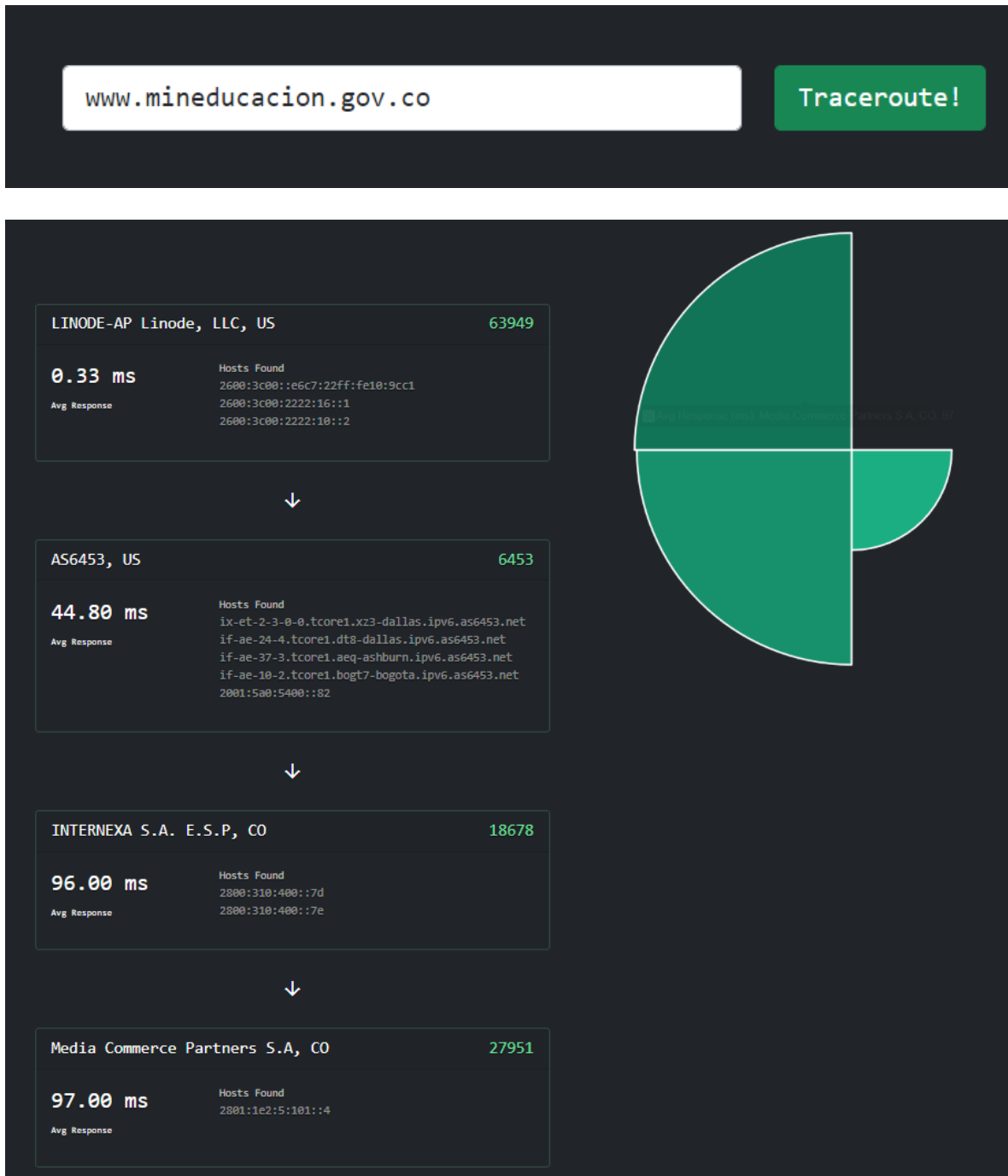
Interfaz: 192.168.0.18 --- 0xa
Dirección de Internet      Dirección física      Tipo
192.168.0.1                b0-c2-87-28-25-19    dinámico
192.168.0.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
224.0.1.187                01-00-5e-00-01-bb    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
239.255.255.253            01-00-5e-7f-ff-fd    estático












Interfaz: 192.168.79.1 --- 0x14
Dirección de Internet      Dirección física      Tipo
192.168.79.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    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
224.0.1.187                01-00-5e-00-01-bb    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
```

### 3. USO DE MENSAJES ICMP

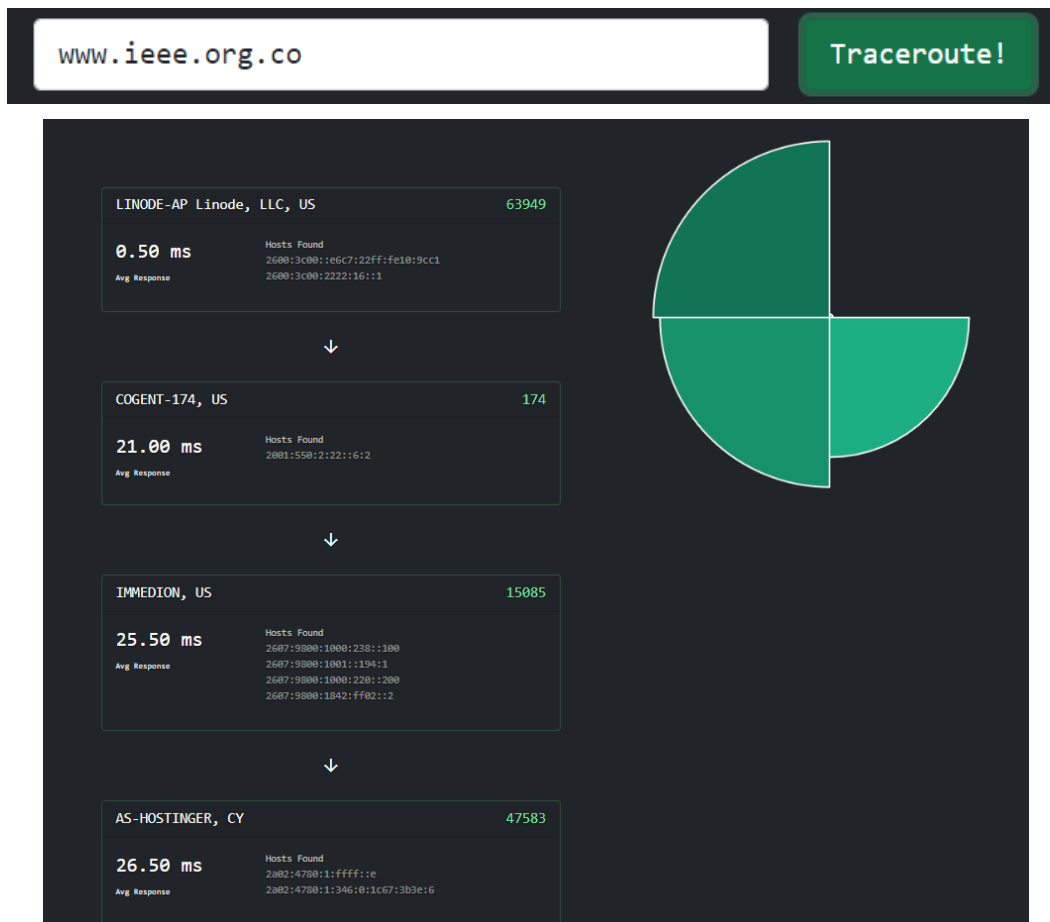
Resultados *traceroute-online.com*










1. [www.mineducacion.gov.co](http://www.mineducacion.gov.co)



Hop	IP / Host Name	ISP	Netblock	Country	Loss	Response
1	2600:3c00::e6c7:22ff:fe10:9cc1	LINODE-AP Linode, LLC, US	2600:3c00::/32		0.0%	1.22ms
2	2600:3c00:2222:16::1	LINODE-AP Linode, LLC, US	2600:3c00::/32		0.0%	0.66ms
3	2600:3c00:2222:10::2	LINODE-AP Linode, LLC, US	2600:3c00::/32		0.0%	0.65ms
4	ix-et-2-3-0-0.tcore1.xz3-dallas.ipv6.as6453.net 2001:5a0:4b00::11	AS6453, US	2001:5a0::/32		0.0%	1.12ms
5	if-ae-24-4.tcore1.dt8-dallas.ipv6.as6453.net 2001:5a0:200:500::9d	AS6453, US	2001:5a0::/32		0.0%	1.20ms
6	if-ae-37-3.tcore1.aeq-ashburn.ipv6.as6453.net 2001:5a0:600:400::98	AS6453, US	2001:5a0::/32		0.0%	30.49ms
7	if-ae-10-2.tcore1.bogt7-bogota.ipv6.as6453.net 2001:5a0:5400::1	AS6453, US	2001:5a0::/32		0.0%	97.12ms
8	2001:5a0:5400::82	AS6453, US	2001:5a0::/32		0.0%	95.36ms
9	2800:310:400::7d	INTERNEXA S.A. E.S.P, CO	2800:310::/32		0.0%	96.17ms
10	2800:310:400::7e	INTERNEXA S.A. E.S.P, CO	2800:310::/32		0.0%	96.88ms
11	???					
12	2801:1e2:5:101::4	Media Commerce Partners S.A, CO	2801:1e2::/44		0.0%	97.40ms
13	???					

## 2. [www.ieee.org.co](http://www.ieee.org.co)



Hop	IP / Host Name	ISP	Netblock	Country	Loss	Response
1	2600:3c00::e6c7:22ff:fe10:9cc1	LINODE-AP Linode, LLC, US	2600:3c00::/32		0.0%	1.38ms
2	2600:3c00:2222:16::1	LINODE-AP Linode, LLC, US	2600:3c00::/32		0.0%	0.63ms
3	???					
4	???					
5	???					
6	???					
7	???					
8	2001:550:2:22::6:2	COGENT-174, US	2001:550::/32		0.0%	21.36ms
9	2607:9800:1000:238::100	IMMEDION, US	2607:9800::/32		0.0%	21.44ms
10	2607:9800:1001::194:1	IMMEDION, US	2607:9800::/32		0.0%	28.71ms
11	2607:9800:1000:220::200	IMMEDION, US	2607:9800::/32		0.0%	27.64ms
12	2607:9800:1842:ff02::2	IMMEDION, US	2607:9800::/32		0.0%	26.95ms
13	2a02:4780:1:ffff::e	AS-HOSTINGER, CY	2a02:4780:1::/48		0.0%	27.07ms
14	2a02:4780:1:346:0:1c67:3b3e:6	AS-HOSTINGER, CY	2a02:4780:1::/48		0.0%	26.93ms

- Utilizando el comando ***tracert***

```

C:\Users\57301>tracert mastersonlineempresa.uc3m.es

Traza a la dirección mastersonlineempresa.uc3m.es [31.200.242.108]
sobre un máximo de 30 saltos:

 1  15 ms    3 ms    4 ms    192.168.0.1
 2  11 ms    11 ms   16 ms   static-ip-cr1901471061.cable.net.co [190.147.106.1]
 3  19 ms    20 ms   16 ms   172.21.16.10
 4  45 ms    44 ms   47 ms   telmex-ic321792-mai-b2.ip.twelve99-cust.net [213.248.70.69]
 5  64 ms    69 ms   70 ms   ix-et-10-0-5-0.tcore1.mln-miami.as6453.net [66.110.9.197]
 6  192 ms   193 ms  183 ms   if-ae-7-2.tcore1.aeq-ashburn.as6453.net [66.198.154.177]
 7  189 ms   195 ms  191 ms   63.243.137.133
 8  187 ms   190 ms  195 ms   if-ae-12-2.tcore4.njy-newark.as6453.net [216.6.87.43]
 9  186 ms   185 ms  191 ms   if-ae-1-3.tcore3.njy-newark.as6453.net [216.6.57.5]
10  190 ms   190 ms  195 ms   if-ae-15-2.tcore1.l78-london.as6453.net [80.231.130.25]
11  188 ms   184 ms  190 ms   if-ae-11-2.tcore2.sv8-highbridge.as6453.net [80.231.139.41]
12  191 ms   186 ms  188 ms   if-ae-14-2.tcore1.dvs-bilbao.as6453.net [80.231.139.66]
13  224 ms   233 ms  228 ms   if-ae-10-4.tcore1.wv6-madrid.as6453.net [80.231.91.105]
14  188 ms   191 ms  201 ms   if-ae-11-2.tcore2.wv6-madrid.as6453.net [80.231.91.66]
15  198 ms   196 ms  195 ms   if-et-2-2.hcore1.mx2-madrid.as6453.net [195.219.124.54]
16  179 ms   171 ms  174 ms   94.76.144.57
17  *        *        *        Tiempo de espera agotado para esta solicitud.
18  *        *        *        Tiempo de espera agotado para esta solicitud.
19  *        *        *        Tiempo de espera agotado para esta solicitud.
20  *        *        *        Tiempo de espera agotado para esta solicitud.
21  *        *        *        Tiempo de espera agotado para esta solicitud.
22  182 ms   184 ms  177 ms   server24.gestiondns.eu [31.200.242.108]

Traza completa.

```

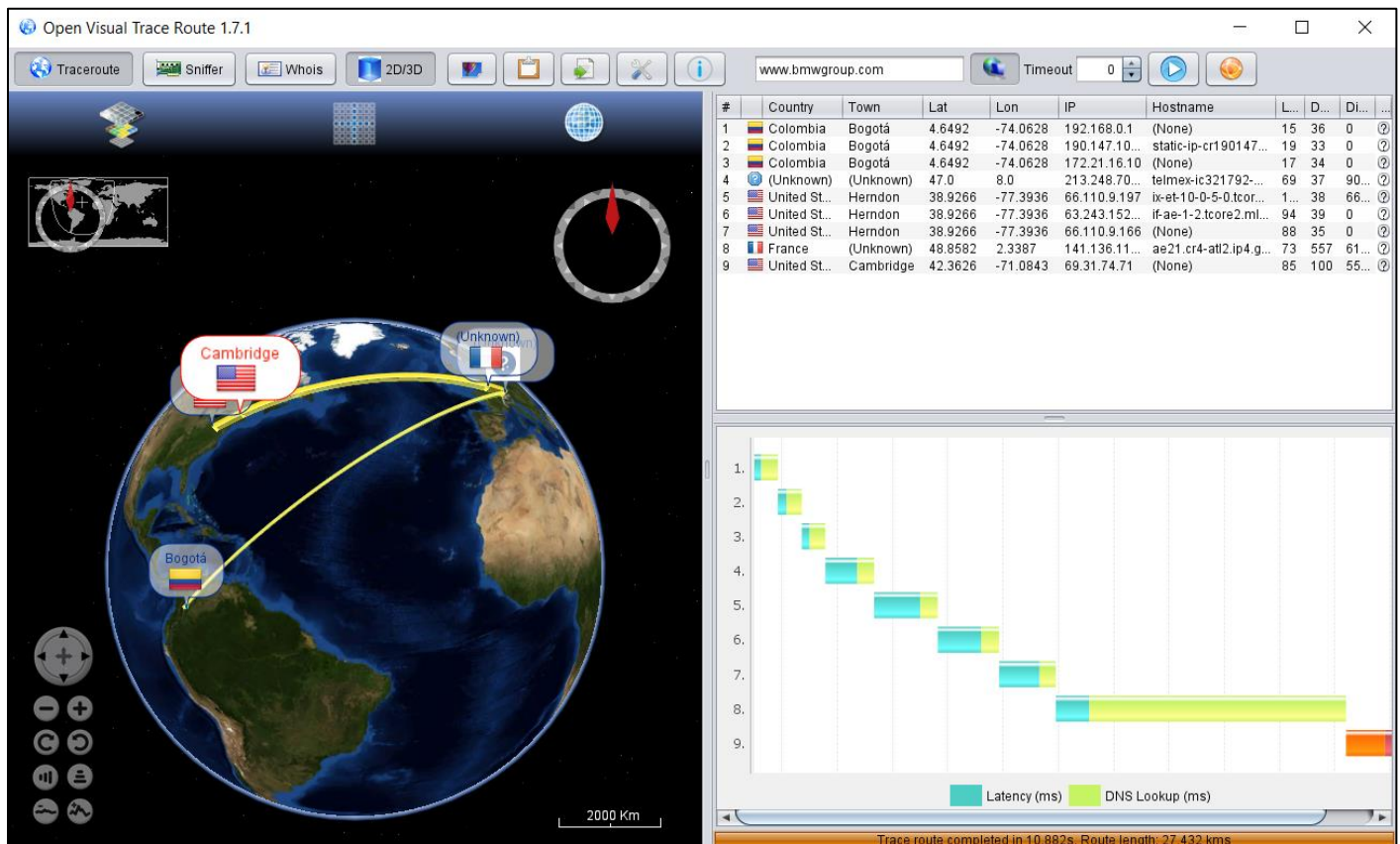
Se realizó el tracert a la página web de la universidad Carlos III de Madrid, ejecutando el comando ***tracert mastersonlineempresa.uc3m.es***. La ruta empieza desde la dirección del proveedor de internet desde allí llegar a la dirección de destino pedida.

- Utilizando **OPEN VISUAL TRACE**

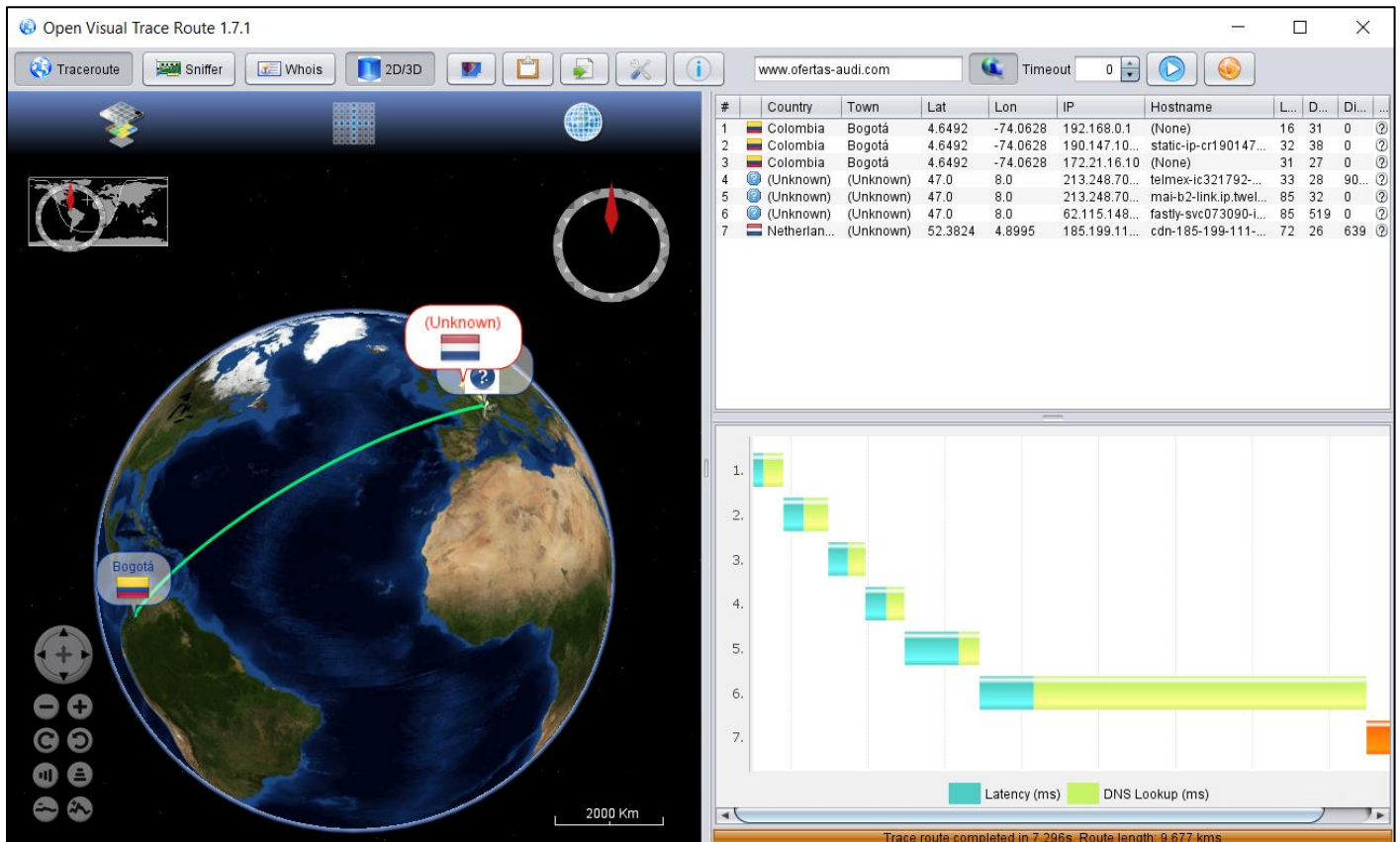
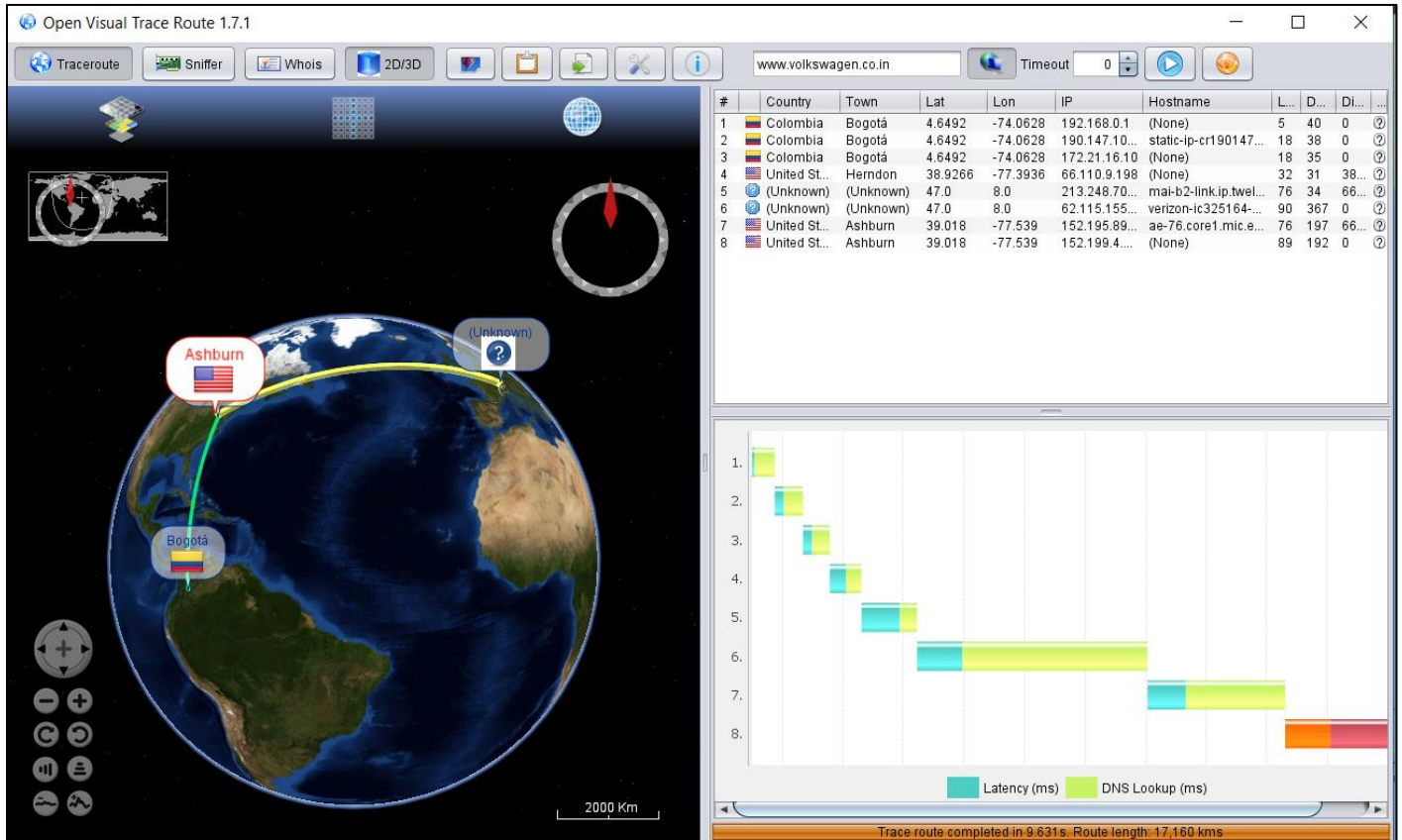
A continuación se mostrarán las rutas de diferentes páginas de proveedores de carros:

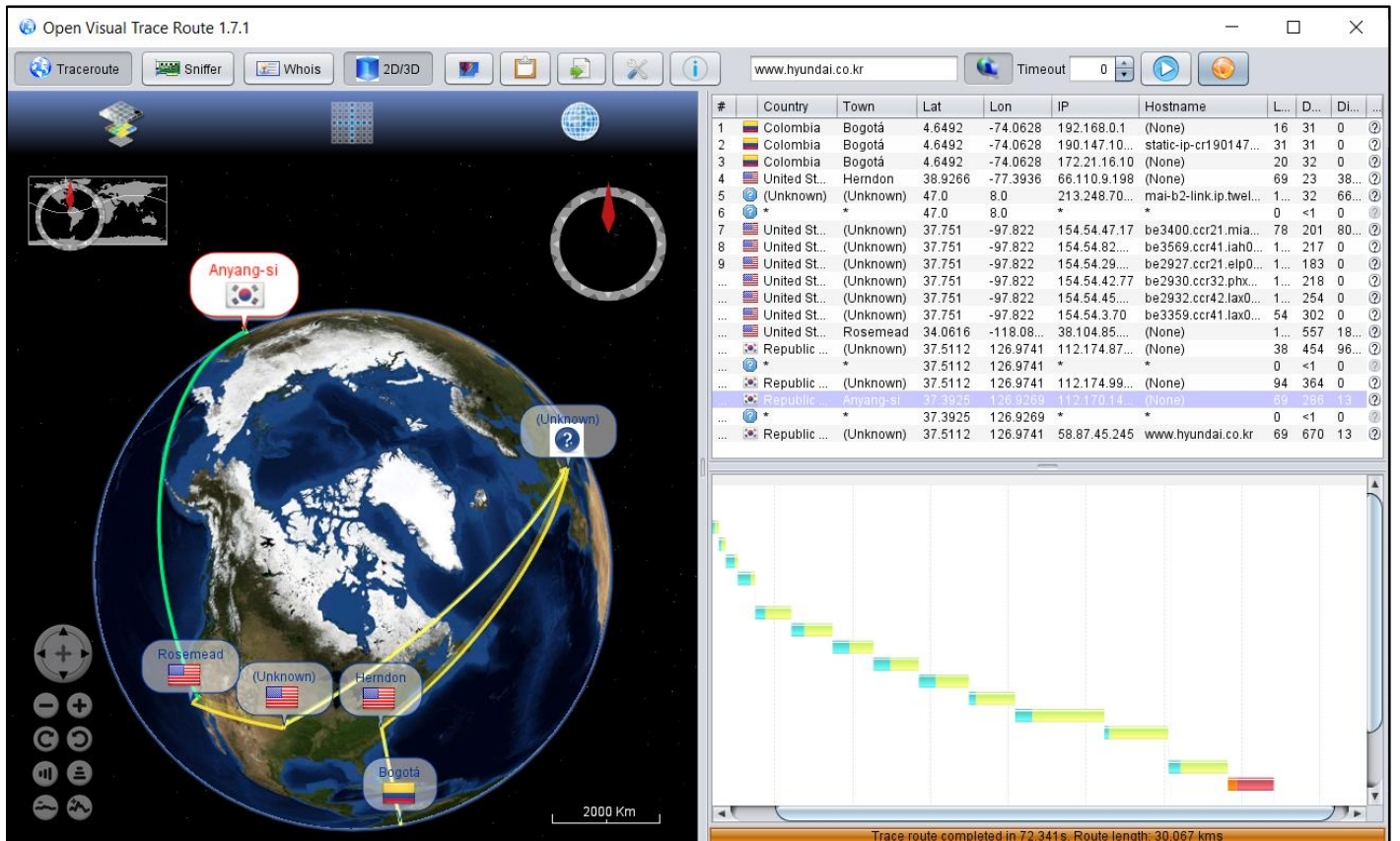
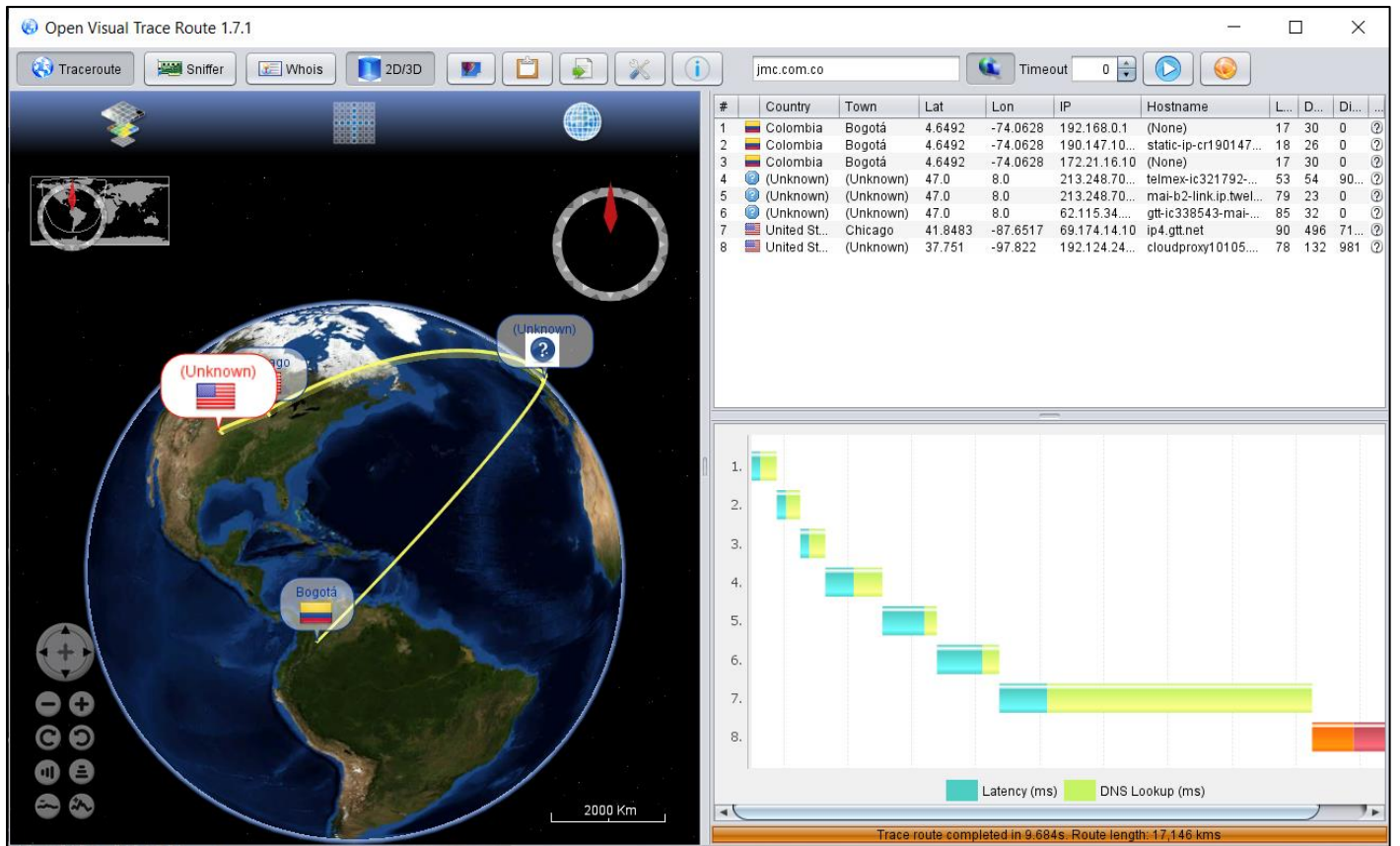
1. Se consultó la página oficial de la empresa BMW - [www.bmwgroup.com](http://www.bmwgroup.com)
2. Se consultó la página oficial de Volkswagen - [www.volkswagen.co.in](http://www.volkswagen.co.in)
3. Se consultó la página oficial de la empresa Audi - [www.ofertas-audi.com](http://www.ofertas-audi.com)
4. Se consultó la página oficial de la empresa JMC - [www.jmc.com.co](http://www.jmc.com.co)
5. Se consultó la página oficial de la empresa Hyundai - [www.hyundai.co.kr](http://www.hyundai.co.kr)

Todas las rutas empezaron desde Colombia y desde aquí se empezó a conocer la ruta que hacía en los diferentes países y/o ciudades.











## CONCLUSIONES

---

1. La configuración de los router es similar a la de un Switch, así que no fue complicado realizar la configuración de estos gracias a la base y el conocimiento que ya teníamos previamente.
2. El tipo de arranque 0x2142 examina los comandos existentes que tenga el sistema y los agrega en el caso de que no los tenga y olvida todo lo almacenado (contraseñas) y devuelve el router al modo de fábrica. En cambio el arranque 0x2102 analiza los comandos sobre la configuración ya realiza y no borra lo que tiene previamente configurado.
3. El Sniffer se encarga de observar el flujo de datos por una red y obtener información de estos, este nos ayudó a identificar los protocolos durante la captura.

## REFERENCIAS

---

[¿Qué es un router? - Definición y usos - Cisco](#)

[¿Qué es la ICMP? \(speedcheck.org\)](#)

[¿Qué es un Traceroute? \(speedcheck.org\)](#)

[¿Qué es Ping? \(speedcheck.org\)](#)

[Quitar o modificar contraseña de un Router Cisco | Alejandro Ramírez \(ingalejandroramirez.blogspot.com\)](#)

[Borrar la Caché ARP en Windows - XARCOM BLOG](#)

[Sniffer de Windows 10: Qué es y cómo usar pktmon.exe \(adslzone.net\)](#)

[¿Qué es un Sniffer? \(infotecs.mx\)](#)