

Escuela Colombiana de Ingeniería Julio Garavito

Laboratorio # 5: Capa de red

**Juan Sebastián Frásica Galeano
Juan Sebastián Gómez López**

Redes de Computadores

Profesora: Ing. Claudia Patricia Santiago Cely

Introducción:

En este laboratorio se analizará en detalle y de forma práctica algunas de las funciones que realiza la capa de red, principalmente la función de los routers en una red. Se aprenderá a configurar un router, y las funciones de los protocolos ICMP y ARP. Se utilizarán algunas herramientas como Wireshark, Packet Tracer, y VisualRoute. Y finalmente implementar un servidor web en las maquinas virtuales de Linux y Windows.

Marco teórico:

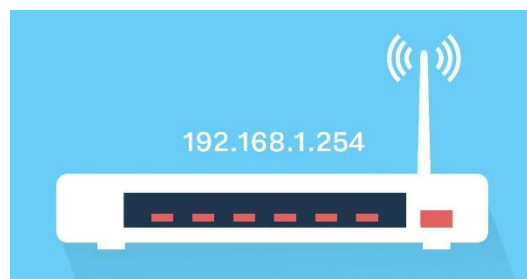
Capa de red:

Se ocupa de controlar el funcionamiento de la subred, del manejo de rutas, determinar el comportamiento de equipos de la red según el tipo de conexión entre la Fuente y el destino, control de congestión, facturación de usuarios, solución de problemas entre redes diferentes y direccionamiento.

Se encarga de llevar los paquetes desde el origen hasta el destino, esto puede requerir de muchos saltos por enrutadores intermedios, para lograrlo debe conocer la topología de la subred y escoger las trayectorias adecuadas a través de ellas.

Esta capa utiliza el protocolo IP. IP Es la base fundamental del Internet. Porta datagramas de la fuente al destino. El nivel de transporte parte el flujo de datos en datagramas. Durante su transmisión se puede partir un datagrama en fragmentos que se montan de nuevo en el destino. El Protocolo IP proporciona un servicio de distribución de paquetes de información orientado a no conexión de manera no fiable. La orientación a no conexión significa que los paquetes de información, que será emitido a la red, son tratados independientemente, pudiendo viajar por diferentes trayectorias para llegar a su destino.

Dirección IP: Para que en una red dos computadoras puedan comunicarse entre sí ellas deben estar identificadas con precisión Este identificador puede estar definido en niveles bajos (identificador físico) o en niveles altos (identificador lógico) dependiendo del protocolo utilizado. TCP/IP utiliza un identificador denominado dirección internet o dirección IP, cuya longitud es de 32 bites. La dirección IP identifica tanto a la red a la que pertenece una computadora como a ella misma dentro de dicha red.



Mascara de Red: Es una combinación de bits que sirve para delimitar el ámbito de una

red de ordenadores. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

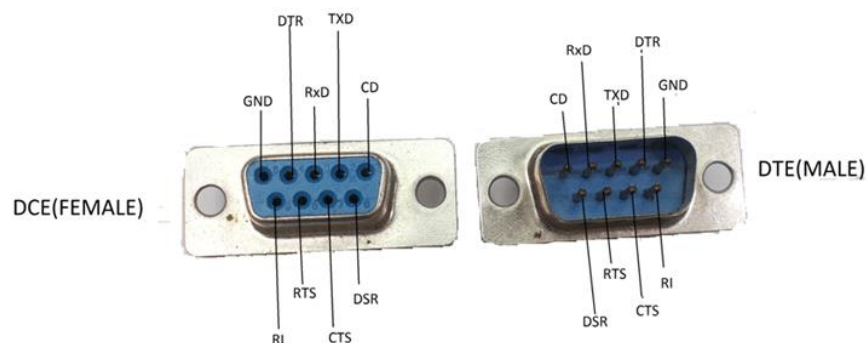
Gateway: Es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más computadoras.

Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

Router: Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red o un switch), y que por tanto tienen prefijos de red distintos.



RS232: También conocido como EIA/TIA RS-232C, es una interfaz que designa una norma para el intercambio de datos binarios serie entre un DTE (Data Terminal Equipment, "Equipo Terminal de Datos"), como por ejemplo una computadora, y un DCE (Data Communication Equipment, "Equipo de Comunicación de Datos"), por ejemplo, un módem.



Desarrollo del tema:

Experimentos

Realice las siguientes pruebas en grupos de dos estudiantes y documente la experiencia.

1. Solución de problemas

- Haga ping entre los dos computadores y a un computador de otro grupo del Laboratorio de Redes de computadores. ¿Funcionó?

No, no funcionó.

Al PC de mi compañero:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.441]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Redes>ping 10.2.67.105

Pinging 10.2.67.105 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 10.2.67.105:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Redes>
```

A otro equipo del laboratorio:

```
C:\Users\Redes>ping 10.2.67.108

Pinging 10.2.67.108 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 10.2.67.108:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Redes>
```

- Haga ping a www.google.com y www.facebook.com. ¿Funcionó?

Tampoco funcionó.

A www.google.com:

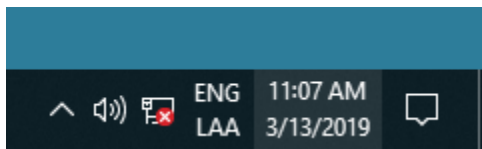
```
C:\Users\Redes>ping www.google.com
Ping request could not find host www.google.com. Please check the name and try again.
```

A www.facebook.com:

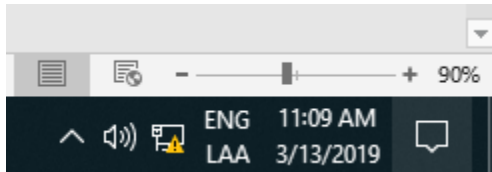
```
C:\Users\Redes>ping www.facebook.com
Ping request could not find host www.facebook.com. Please check the name and try again.
```

- Si no puede hacer alguno de los dos pasos anteriores, encuentre el problema, explique por qué se presentó y soluciónelo. El direccionamiento debe ser el que siempre se encuentra en los equipos del laboratorio de redes

Primero se revisa la capa física, es decir, las conexiones físicas, y el cable de Ethernet estaba desconectado, luego se procedió a conectarlo.



Despues de conectarlo:



Luego se revisa la capa de enlace, se revisa que el PC tenga una dirección MAC:

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . : 
Description . . . . . : Intel(R) Ethernet Connection I217-LM
Physical Address. . . . . : 50-65-F3-25-7A-BE
```

Luego la capa de red, y se revisa la configuracion IPv4:

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 172 . 16 . 0 . 106

Subnet mask: 255 . 255 . 0 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

Como se puede ver, estaba mal configurada. Se procede a corregirla:

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 2 . 67 . 106

Subnet mask: 255 . 255 . 0 . 0

Default gateway: 10 . 2 . 65 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 10 . 2 . 65 . 60

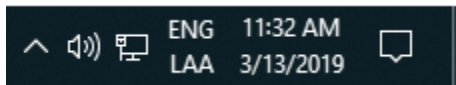
Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

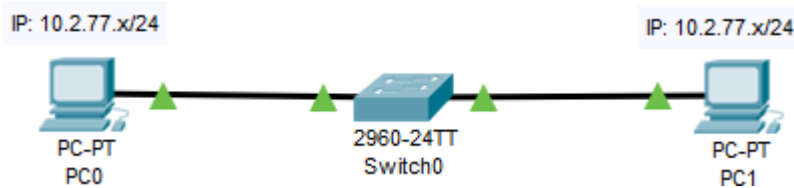
OK Cancel

Y ahora, sí hay conexión a internet.



1. Montaje - Seguimiento protocolo ARP

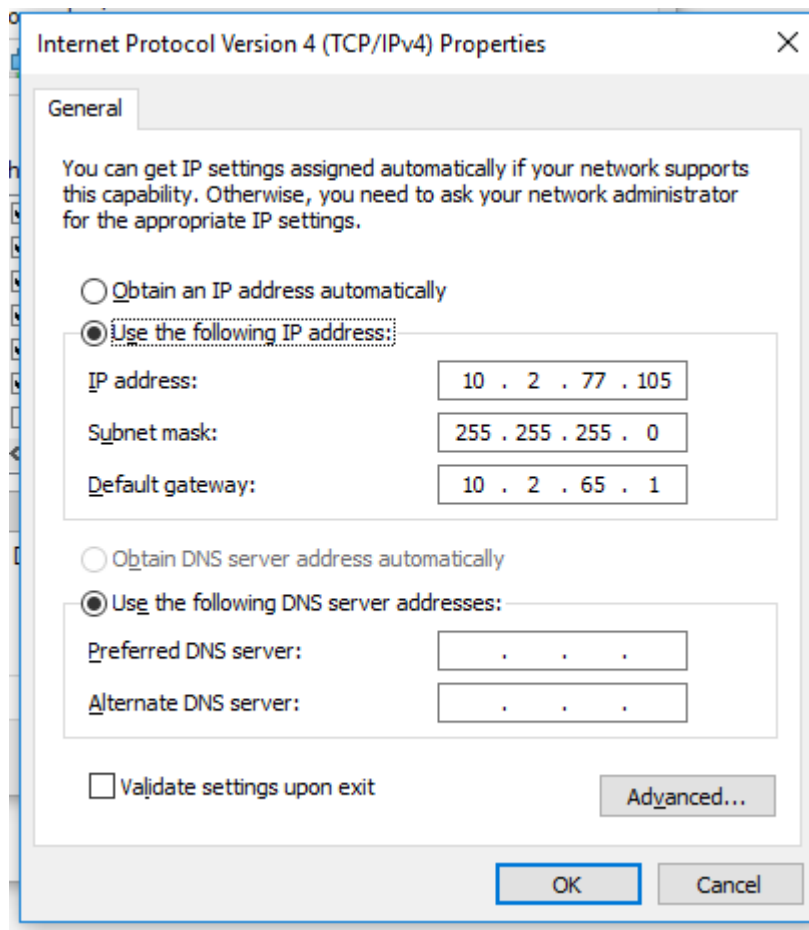
Realice el montaje presentado en la figura



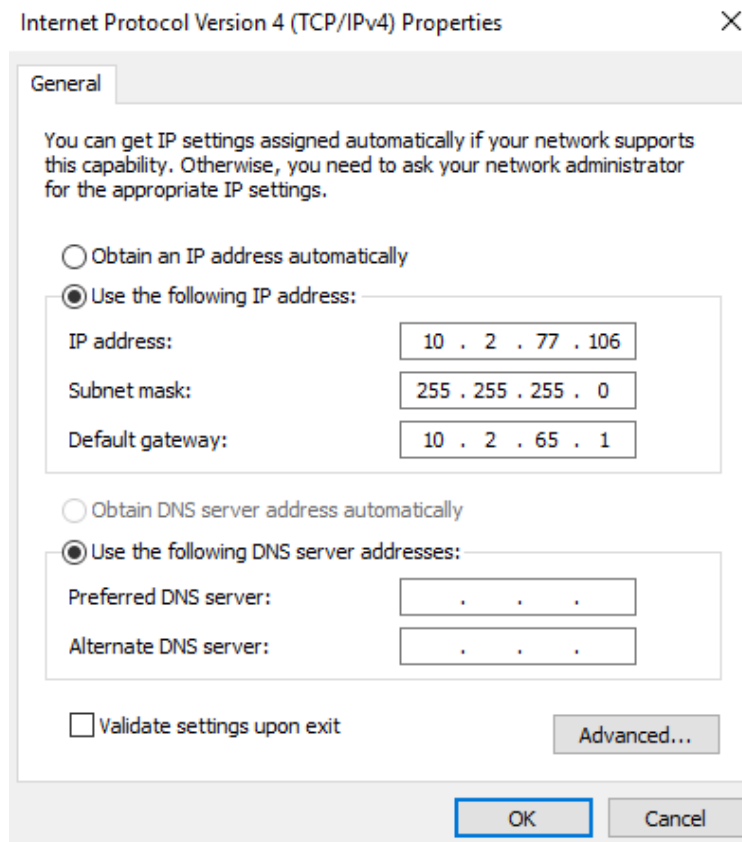
Siga los siguientes pasos, procure seguir los pasos según la indicación para obtener los resultados correctos:

- Configure redes LAN con el rango de direcciones indicado en el dibujo. (NOTA: PONGA A CADA COMPUTADOR, COMO ÚLTIMO BYTE, EL NÚMERO DEL EQUIPO DADO POR EL LABORATORIO DE INFORMÁTICA)

Configuración IPv4 del equipo del laboratorio #105:



Configuración IPv4 del equipo del laboratorio #106:



- Ponga a correr el Sniffer, realice un ping entre los computadores de la LAN y documente la captura en lo relacionado al protocolo ARP y la construcción de tablas de ARP en los equipos.

Primero se hizo un ping desde 10.2.77.105 a 10.2.77.106

Y el Sniffer mostró lo siguiente:

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
11	3.568882	HewlettP_25:77:e4	HewlettP_25:7a:be	ARP	60	Who has 10.2.77.106? Tell 10.2.77.105
12	3.568932	HewlettP_25:7a:be	HewlettP_25:77:e4	ARP	42	10.2.77.106 is at 50:65:f3:25:7a:be
13	3.620204	HewlettP_25:7a:be	HewlettP_25:77:e4			
14	3.621449	HewlettP_25:77:e4	HewlettP_25:7a:be			
21	5.177444	HewlettP_25:77:e4	Broadcast			
24	6.068971	HewlettP_25:77:e4	Broadcast			
28	7.069265	HewlettP_25:77:e4	Broadcast			
29	8.183502	HewlettP_25:77:e4	Broadcast			
31	9.068480	HewlettP_25:77:e4	Broadcast			
33	10.068906	HewlettP_25:77:e4	Broadcast			

Command Prompt

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description : Intel(R) Ethernet Connection I217-LM
Physical Address. : 50-65-F3-25-7A-BE

En el primer paquete, 10.2.77.105 pregunta quien tiene la dirección IPv4 10.2.77.106

Y 10.2.77.106 responde que está en 50:65:f3:25:7a:be

Y se puede observar que ésta coincide con su dirección MAC.

- Ve a la tabla ARP de los computadores utilizados y documento los hallazgos.

Para ver las tablas ARP, toca ejecutar el siguiente comando:

arp -a

Tablas ARP del host 10.2.77.106

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

Internet Address	Physical Address	Type
Interface: 192.168.35.1 --- 0x7		
192.168.35.254	00-50-56-ef-da-c5	dynamic
192.168.35.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static
Interface: 10.2.77.106 --- 0xb		
10.2.77.105	50-65-f3-25-77-e4	dynamic
10.2.77.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Tablas ARP del host 10.2.77.105

```

C:\Users\Redes>arp -a

Interface: 192.168.35.1 --- 0x7
Internet Address      Physical Address      Type
192.168.35.254        00-50-56-f2-4a-5e     dynamic
192.168.35.255        ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
224.0.0.252          01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.2.77.105 --- 0xb
Internet Address      Physical Address      Type
10.2.77.106          50-65-f3-25-7a-be     dynamic
10.2.77.255          ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
224.0.0.252          01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0xd
Internet Address      Physical Address      Type
192.168.56.255        ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
224.0.0.252          01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static

```

- Haga ping entre los equipos y revise el frame Ethernet e indique los campos que lo componen.

The image shows a Wireshark packet capture interface. The top pane displays a list of captured packets. Packet 2 is selected, which is an Ethernet II frame. The bottom pane shows the detailed structure of this frame, with fields like Destination, Source, and Type expanded. A red box highlights the Ethernet II details pane.

Wireshark - Packet 2 - Ethernet

> Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

▼ Ethernet II, Src: HewlettP_25:77:e4 (50:65:f3:25:77:e4), Dst: HewlettP_25:7a:be (50:65:f3:25:7a:be)

▼ Destination: HewlettP_25:7a:be (50:65:f3:25:7a:be)

Address: HewlettP_25:7a:be (50:65:f3:25:7a:be)

.....0..... = LG bit: Globally unique address (factory default)

.....0..... = IG bit: Individual address (unicast)

▼ Source: HewlettP_25:77:e4 (50:65:f3:25:77:e4)

Address: HewlettP_25:77:e4 (50:65:f3:25:77:e4)

.....0..... = LG bit: Globally unique address (factory default)

.....0..... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 10.2.77.105, Dst: 10.2.77.106

> Internet Control Message Protocol

The packet bytes pane at the bottom shows the raw data of the frame, with the destination MAC address (50:65:f3:25:7a:be) highlighted in blue.

Se puede observar que el frame Ethernet está compuesto por dirección MAC destino, dirección MAC origen y el tipo de direccionamiento, el cual es IPv4.

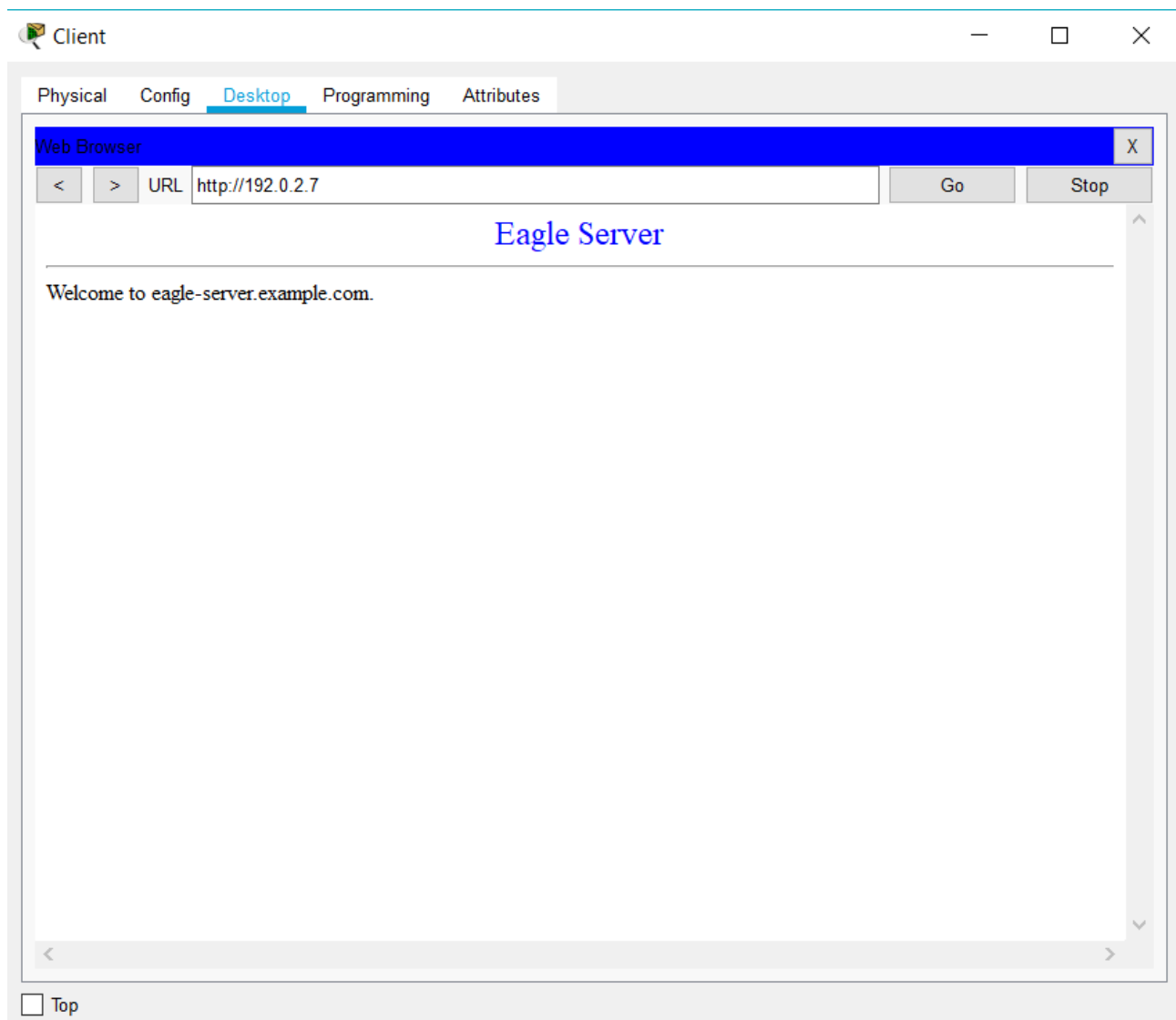
2. ARP

Usando PacketTracer, realice la simulación enunciada en el archivo ProtocoloARP.pka, la cual hace referencia al funcionamiento del protocolo ARP. Dicho archivo se encuentra publicado en el aula virtual del curso.

Task 1: Trace HTTP-initiated Packets.

Step 1. Initialize the Network.

While in Realtime mode, open the Web Browser from the Desktop of the PC Client. Type 192.0.2.7 into the URL and press the Enter key. The web page should be retrieved. This process helps populate tables so you can focus on just the HTTP-related packets.



Step 2. Set Event List Filters.

Switch to Simulation mode. We only want to capture HTTP events. In the Event List Filters section, click the Edit Filters button. Select only HTTP events. By viewing HTTP events only, DNS, ARP, TCP, and RIP processes are still occurring, but are not displayed. Sometimes, if an HTTP packet is buffered it causes a distinct packet event in the event list that looks like a duplicate but is just a pause before transmitting. This happens because the other protocol events are still occurring, just not visibly.

The screenshot shows the PacketTracer7 interface. On the left, the 'Misc' tab is selected in the 'PacketTracer7' window, and the 'HTTP' checkbox is checked. On the right, the 'Simulation Panel' is open, showing the 'Event List' section. The 'Event List' table has columns: Vis., Time(sec), Last Device, At Device, and Type. Below the table, the 'Event List Filters - Visible Events' section shows 'HTTP' selected. The 'Edit Filters' button is visible. The bottom status bar shows 'Event List', 'Realtime', and 'Simulation' modes.

PacketTracer7

IPv4 IPv6 Misc

☐ Bluetooth ☐ CAPWAP ☐ CDP

☐ DTP ☐ EAPOL ☐ FTP

☐ H.323 ☒ HTTP ☐ HTTPS

☐ IPsec ☐ ISAKMP ☐ IoT

☐ IoT TCP ☐ LACP ☐ LLDP

☐ Meraki ☐ NETFLOW ☐ NTP

☐ PAgP ☐ POP3 ☐ PPP

☐ PPPoED ☐ PTP ☐ RADIUS

☐ REP ☐ RTP ☐ SCCP

☐ SMTP ☐ SNMP ☐ SSH

☐ STP ☐ SYSLOG ☐ TACACS

☐ TCP ☐ TFTP ☐ Telnet

☐ UDP ☐ USB ☐ VTP

Edit ACL Filters

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
------	-----------	-------------	-----------	------

Reset Simulation ☒ Constant Delay Captured to: (no captures)

Play Controls

Event List Filters - Visible Events

HTTP

Edit Filters Show All/None

Event List Realtime Simulation

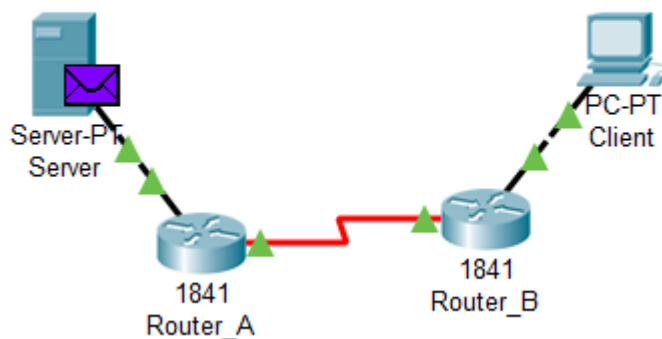
Step 3. Step through the simulation.

From the PC client's browser, click the Go button to request the web page again. Click the Capture / Forward button once and examine the packet. Then click Capture / Forward again and again, opening the packet for examination at each step in the process. When you are done analyzing the packets, switch to Realtime mode, and click on the Power Cycle Devices button to reboot the devices. When the link lights turn from red to green, return to Simulation mode.

The screenshot shows the 'Simulation Panel' window. At the top, there's a status bar with '[Root]' and a clock showing '09:39:30'. Below it, the 'Event List' table is visible:

Vis.	Time(sec)	Last Device	At Device	Type
	474.801	--	Client	HTTP
	474.802	--	Client	HTTP
	474.803	Client	Router_B	HTTP
	474.804	Router_B	Router_A	HTTP
	474.805	Router_A	Server	HTTP

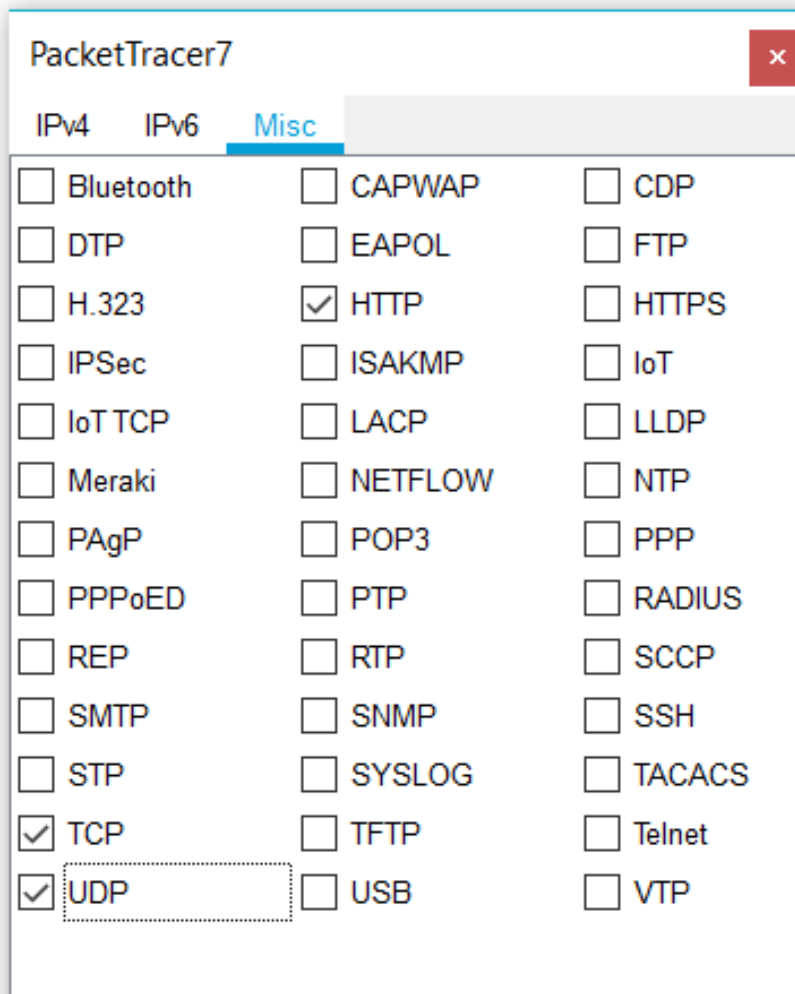
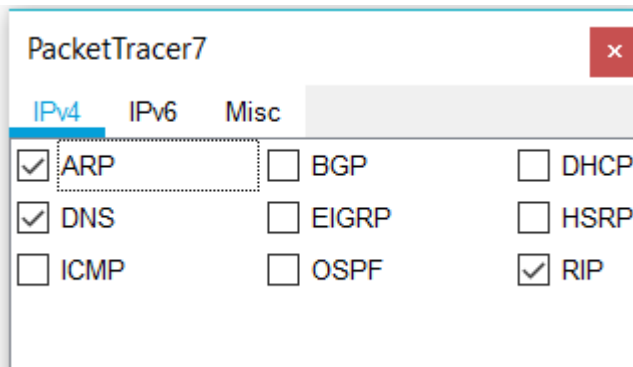
Below the table, there are controls: 'Reset Simulation', a checked 'Constant Delay' checkbox, and 'Captured to: 474.805 s'. Under 'Play Controls', there are buttons for previous, play, and next, with a progress bar below them. The 'Event List Filters - Visible Events' section shows 'HTTP' selected, with 'Edit Filters' and 'Show All/None' buttons. At the bottom, there are tabs for 'Event List', 'Realtime', and 'Simulation', with 'Simulation' being the active tab.



Task 2: Observe the same situation, viewing more than just HTTP-initiated packets.

Step 1. View more protocols.

In the Event List Filters section, click the Edit Filters button. Select HTTP, DNS, TCP, UDP, ARP, and RIP. This will provide a more realistic view of the network. It is similar to what is observed in a Wireshark capture.



Step 2. Step through the simulation.

Open the Web Browser of the PC client and type eagle-server.example.com into the URL and press the Enter key. Click the Go button. Click the Capture / Forward button repeatedly and view the complexities of this seemingly simple interaction of protocols. After the exchange the routers begin exchanging RIPv2 packets. This exchange will continue indefinitely. Stop after a couple of exchanges. At this point in the course you should start to be able to explain this sequence of packets.

The screenshot shows a 'Simulation Panel' window with an 'Event List' table. The table has five columns: 'Vis.', 'Time(sec)', 'Last Device', 'At Device', and 'Type'. The events are as follows:

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Client	DNS
	0.001	Client	Router_B	DNS
	0.002	Router_B	Router_A	DNS
	0.003	Router_A	Server	DNS
	0.004	Server	Router_A	DNS
	0.005	Router_A	Router_B	DNS
	0.006	Router_B	Client	DNS
	7.102	--	Router_B	RIPv2
	7.102	--	Router_B	RIPv2
	7.103	Router_B	Client	RIPv2
	7.103	Router_B	Router_A	RIPv2
	24.923	--	Router_A	RIPv2
	24.923	--	Router_A	RIPv2
	24.924	Router_A	Server	RIPv2
	24.924	Router_A	Router_B	RIPv2
	35.251	--	Router_B	RIPv2
	35.251	--	Router_B	RIPv2
	35.252	Router_B	Client	RIPv2
	35.252	Router_B	Router_A	RIPv2
	53.482	--	Router_A	RIPv2
	53.482	--	Router_A	RIPv2

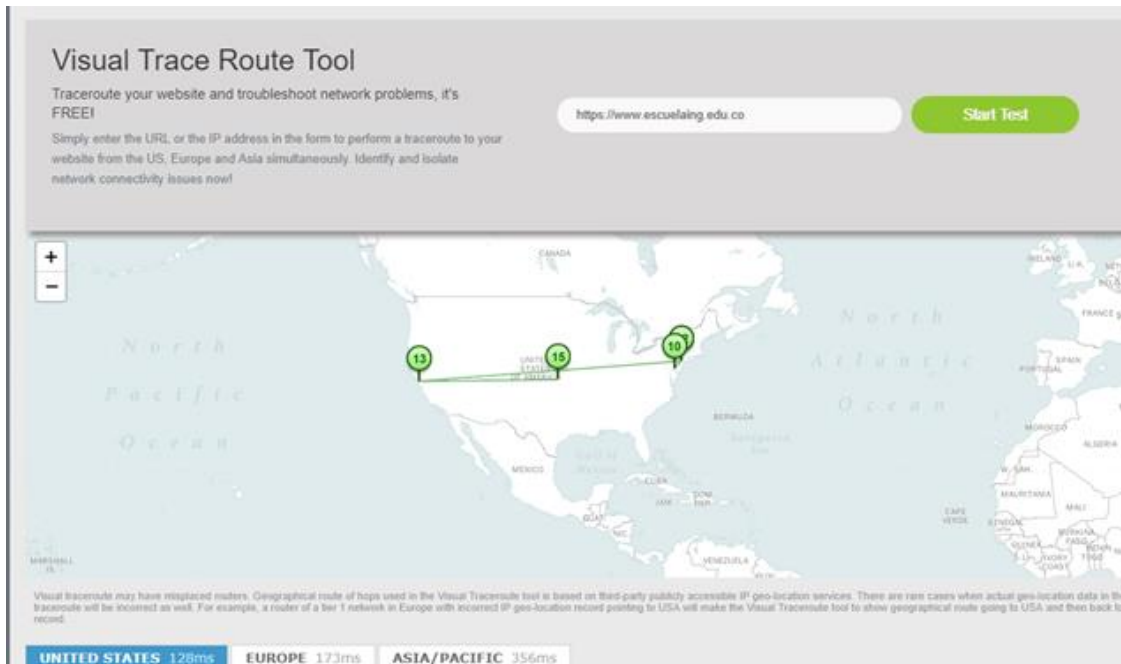
Below the table, there is a 'Reset Simulation' button, a checked 'Constant Delay' checkbox, and a 'Captured to: 53.482 s' label. Below that is a 'Play Controls' section with three buttons: a left arrow, a right arrow, and a double right arrow. A progress bar is also visible. At the bottom, there is an 'Event List Filters - Visible Events' section showing 'ARP, DNS, HTTP, RIP, TCP, UDP'. Below this are 'Edit Filters' and 'Show All/None' buttons. The bottom of the window has a blue bar with three tabs: 'Event List' (selected), 'Realtime', and 'Simulation'.

3. Uso de mensajes

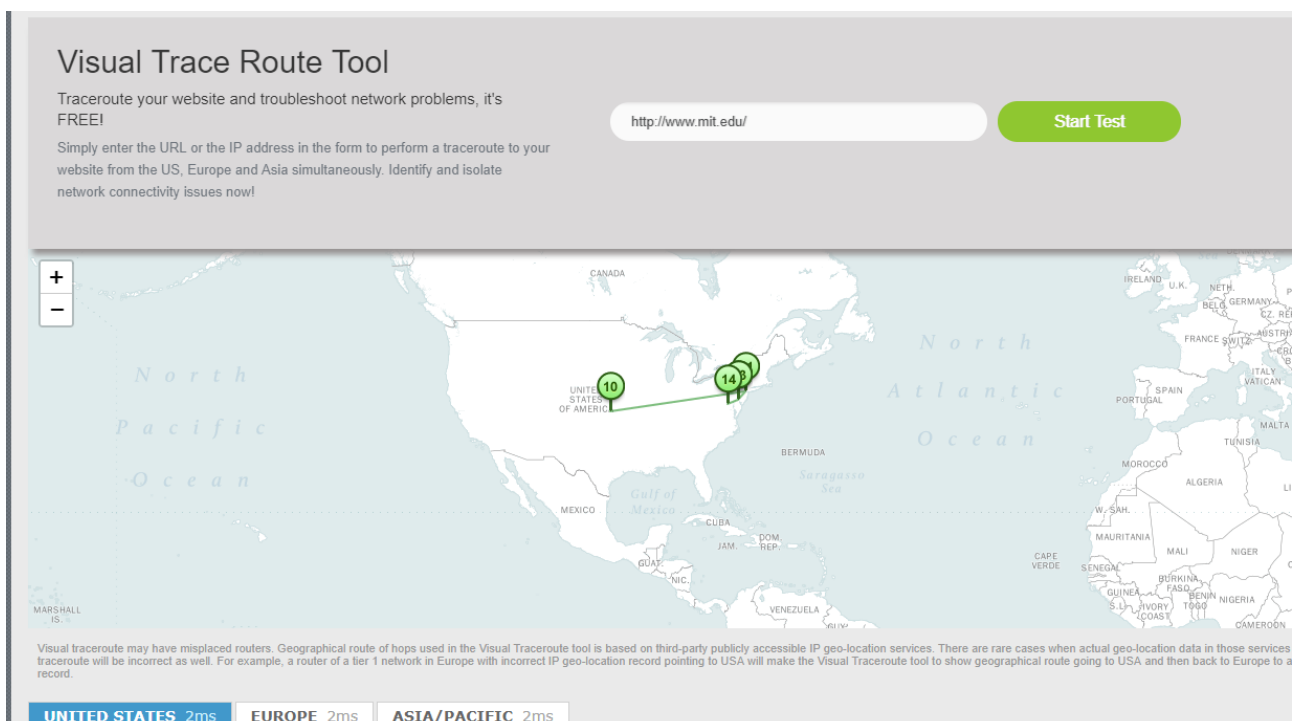
ICMP Rutas

- Vaya a <http://traceroute.monitis.com/> y busque la página de la Escuela y la página de MIT. Muestre los resultados.

Página de la Escuela:



Página de MIT:



- Usando el comando tracert o traceroute, busque una página en Alemania y revise la ruta.

Tracert a la Universidad de Berlín:

```
C:\Users\Redes>tracert www.hu-berlin.de

Tracing route to webmania.cms.hu-berlin.de [141.20.5.188]
over a maximum of 30 hops:

  1    1 ms    <1 ms    1 ms    10.2.65.1
  2    1 ms    1 ms    1 ms    10.250.0.1
  3    1 ms    1 ms    1 ms    static-190-24-150-66.static.etb.net.co [190.24.150.66]
  4    2 ms    2 ms    2 ms    dynamic-186-154-222-125.dynamic.etb.net.co [186.154.222.125]
  5    3 ms    6 ms    6 ms    10.5.2.10
  6    *        *        *        Request timed out.
  7   166 ms    *       167 ms    ae-1-5.bar1.Hamburg1.Level3.net [4.69.142.209]
  8   169 ms   173 ms   169 ms    195.122.181.62
  9   175 ms   172 ms   173 ms    cr-tub2-be13.x-win.dfn.de [188.1.144.58]
 10   172 ms   172 ms   172 ms    kr-adh41-0.x-win.dfn.de [188.1.236.70]
 11   172 ms   173 ms   173 ms    mlxe-fortiback.mgmt.hu-berlin.de [141.20.0.210]
 12   173 ms   174 ms   180 ms    webmania.cms.hu-berlin.de [141.20.5.188]

Trace complete.
```

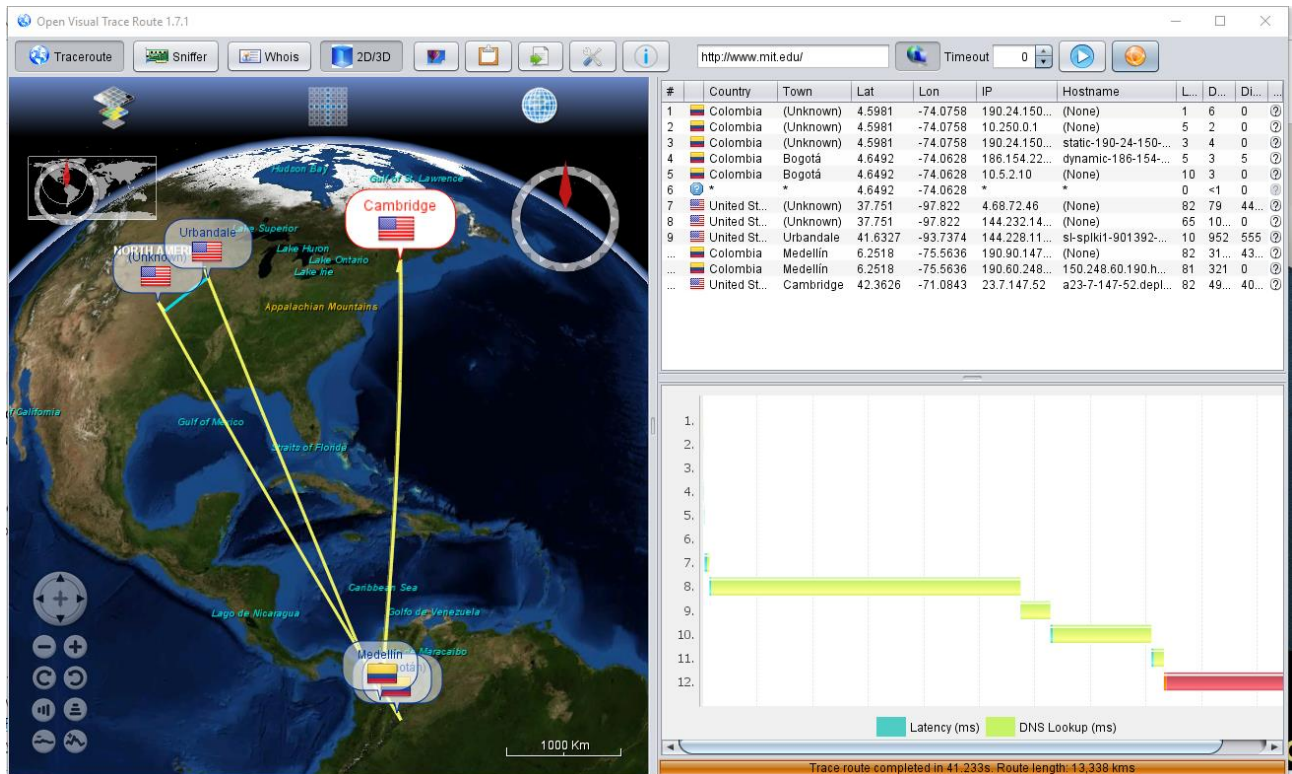
- Descargue e instale un software tipo VisualRoute, Open Visual Traceroute o similar. Pueden ser herramientas libres o demos.

Nota: sólo instale este tipo de software, no incluya otros utilitarios o barras de herramientas que se sugieran en la instalación, para esto, durante la instalación use el modo avanzado para verificar lo que se está instalando. Pruebe la herramienta, conozca un poco las facilidades que incluye.

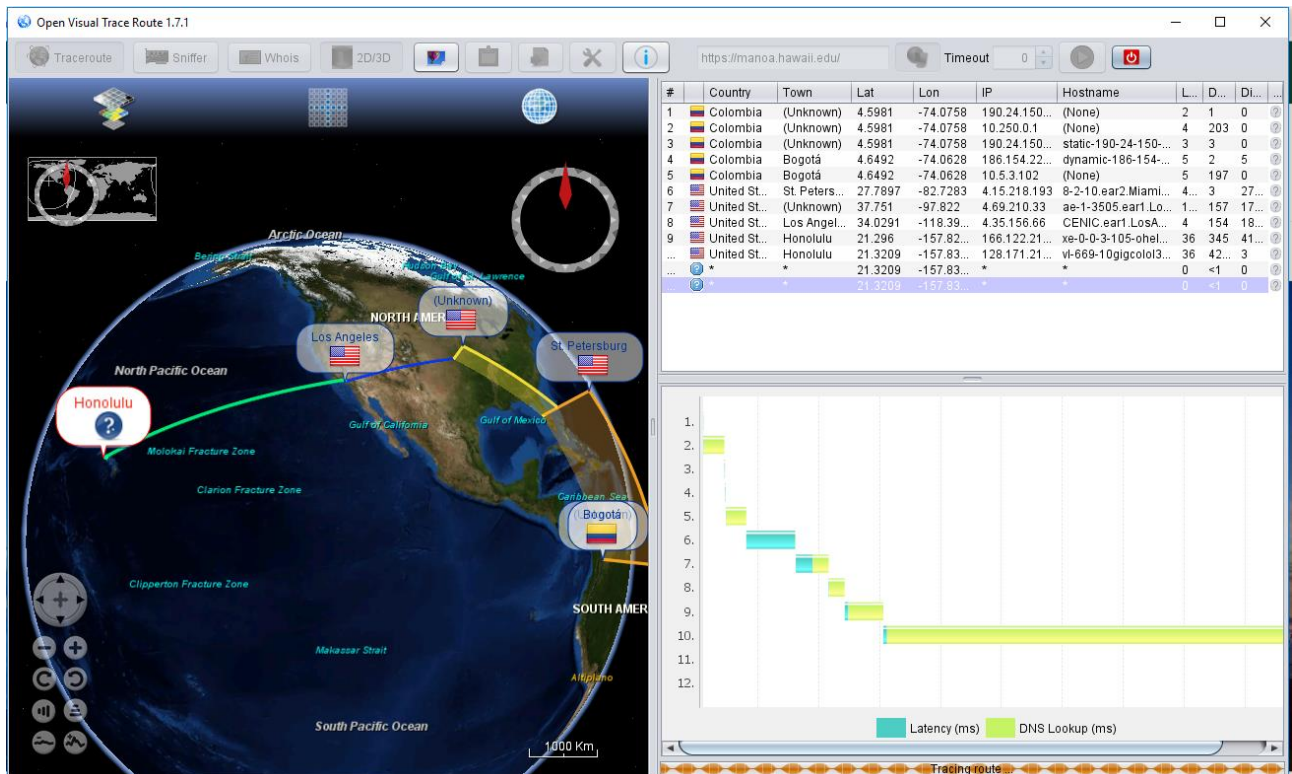
- Documente el funcionamiento de la herramienta buscando 5 páginas web de universidades alrededor del mundo con la herramienta.

Nota: Las páginas deben estar ubicadas en diferentes países, preferiblemente en diferentes continentes.

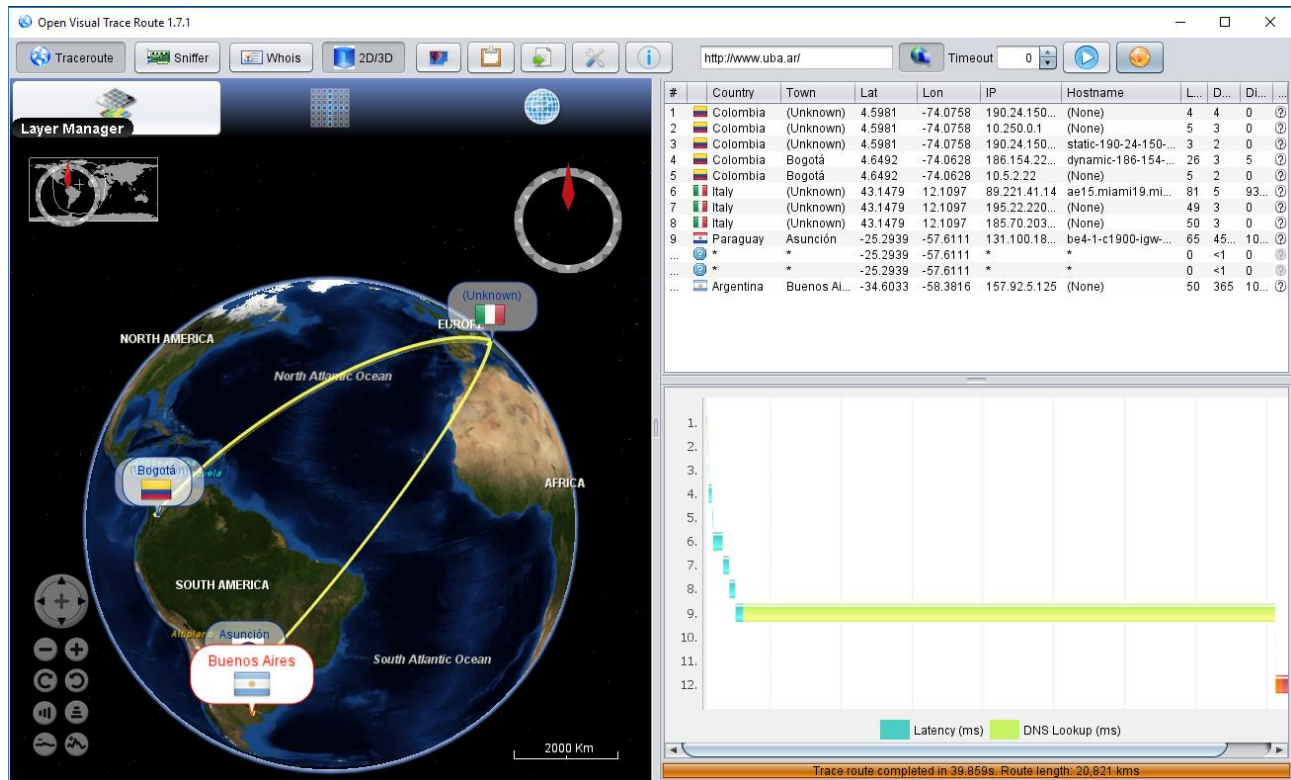
USA:



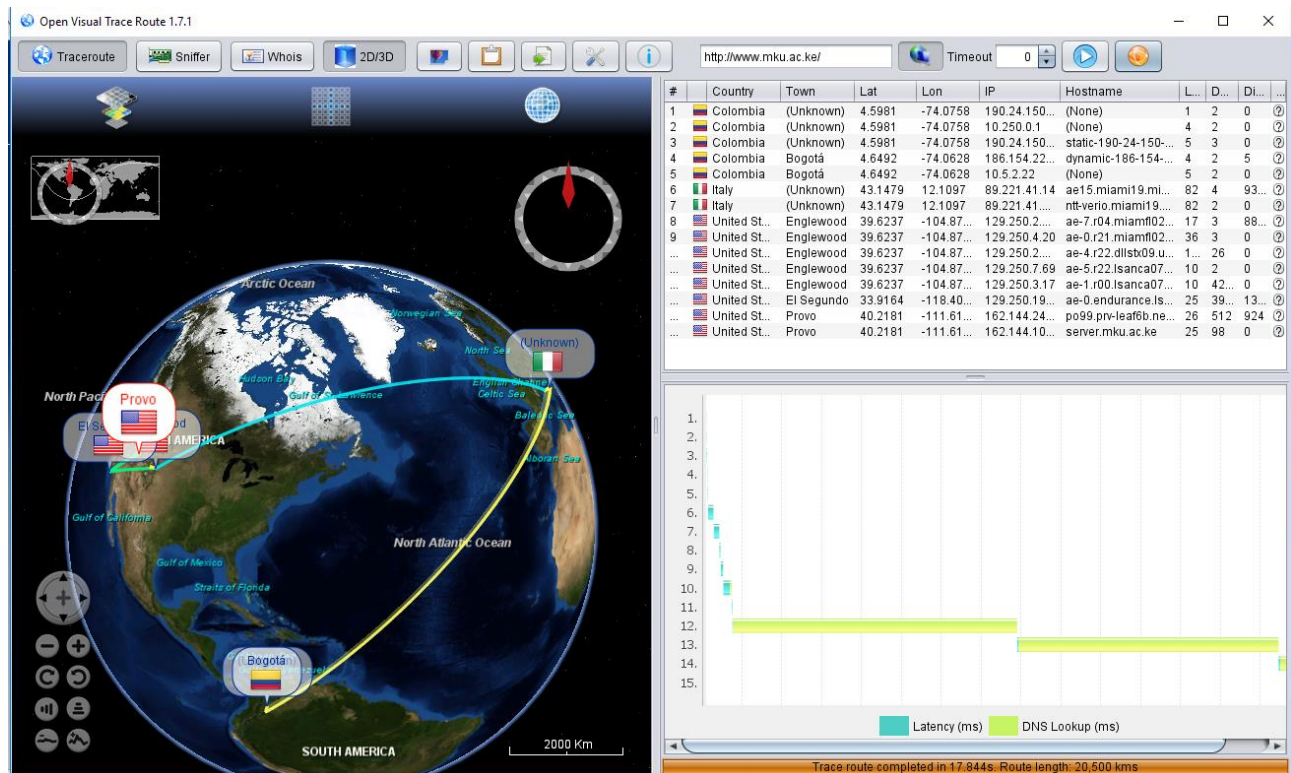
En Honolulu:



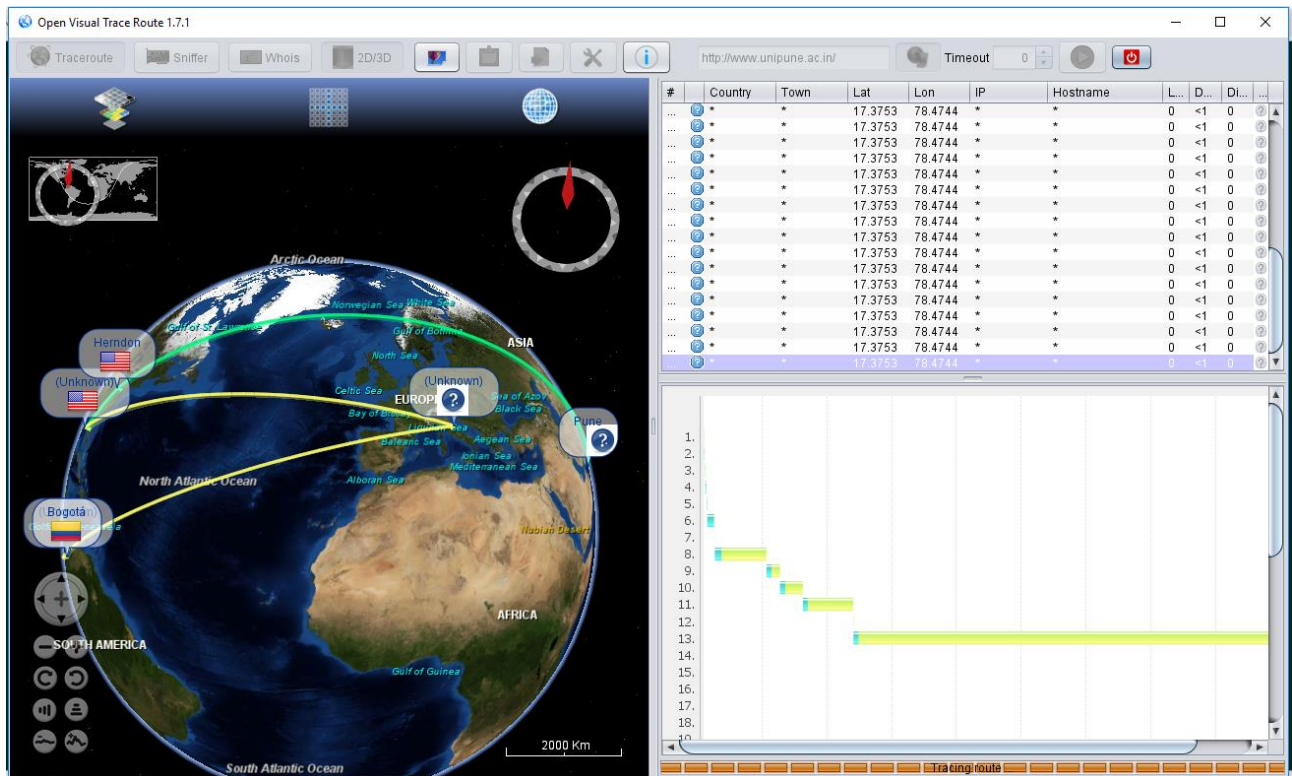
En Buenos Aires:



Kenia:



India:



4. Montaje: Acceso y configuración básica a los routers

- Revisen y documenten los diferentes routers que se tienen en el Laboratorio y las interfaces de red con que cuentan.

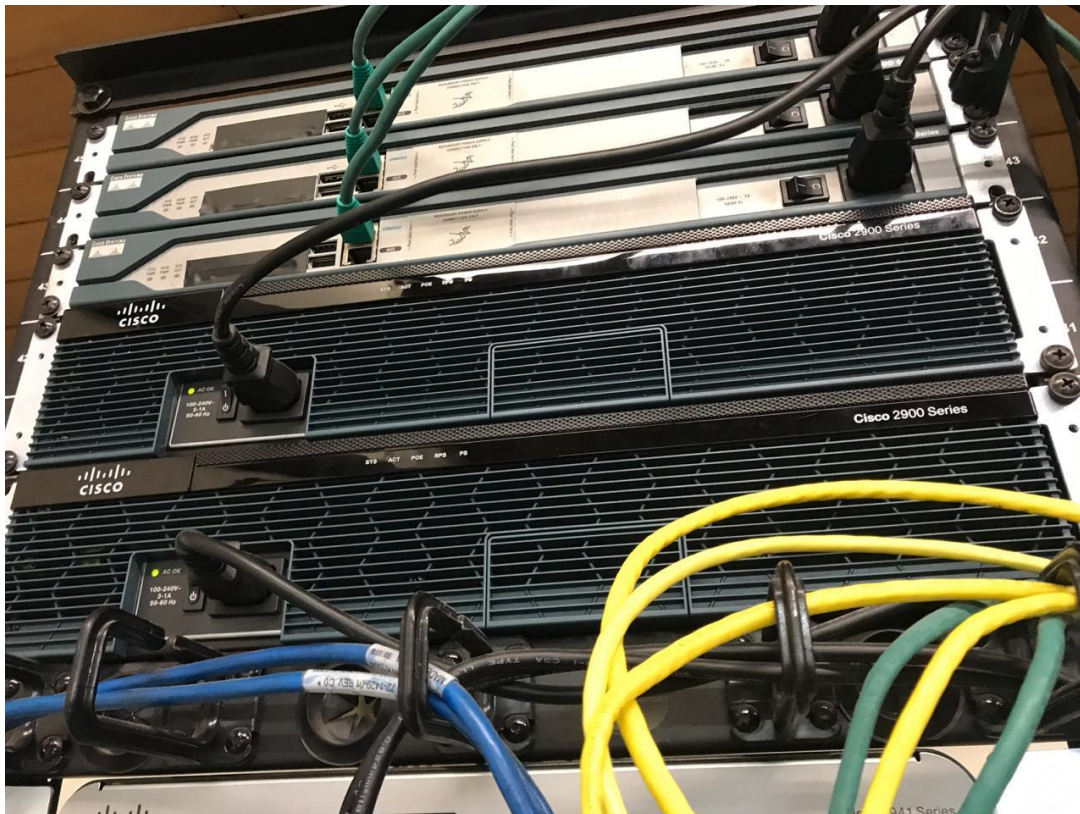
Los routers del laboratorio cuentan con interfaces para Ethernet y consola. Algunos tienen interfaces para USB, conexiones seriales o Aux.

Router Cisco 2800: Son los router 1,2 y 3 del laboratorio.



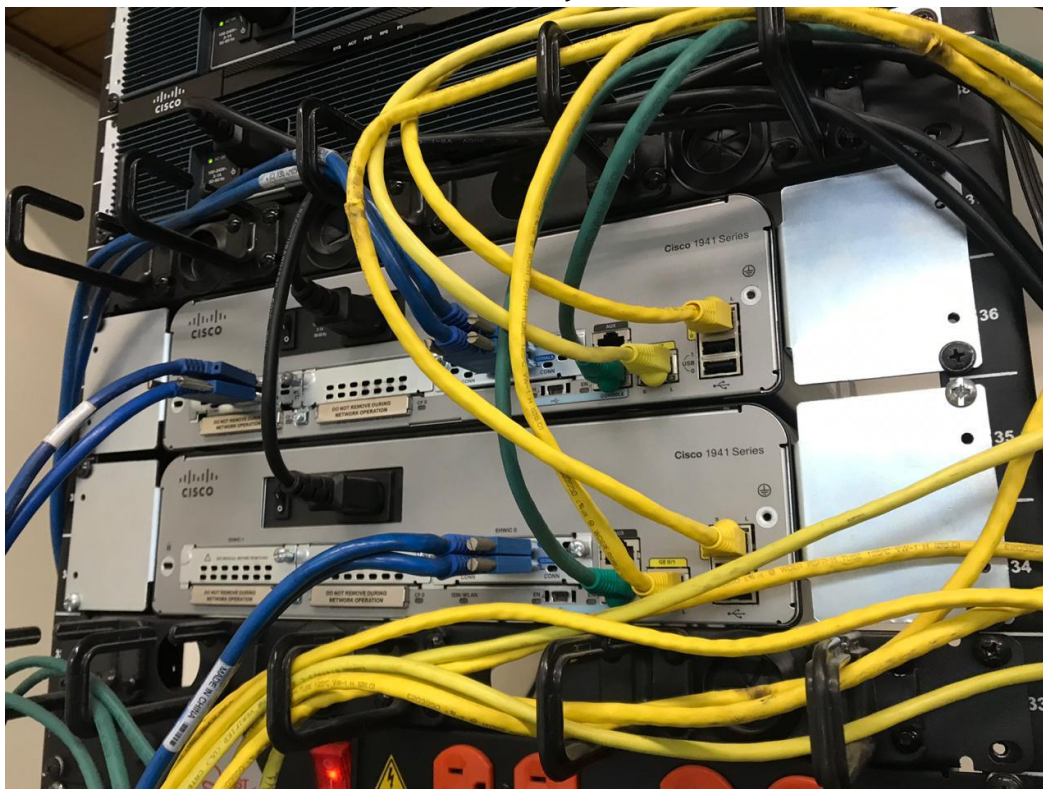


Router Cisco 2900: Son los router #4 y #5 del laboratorio.

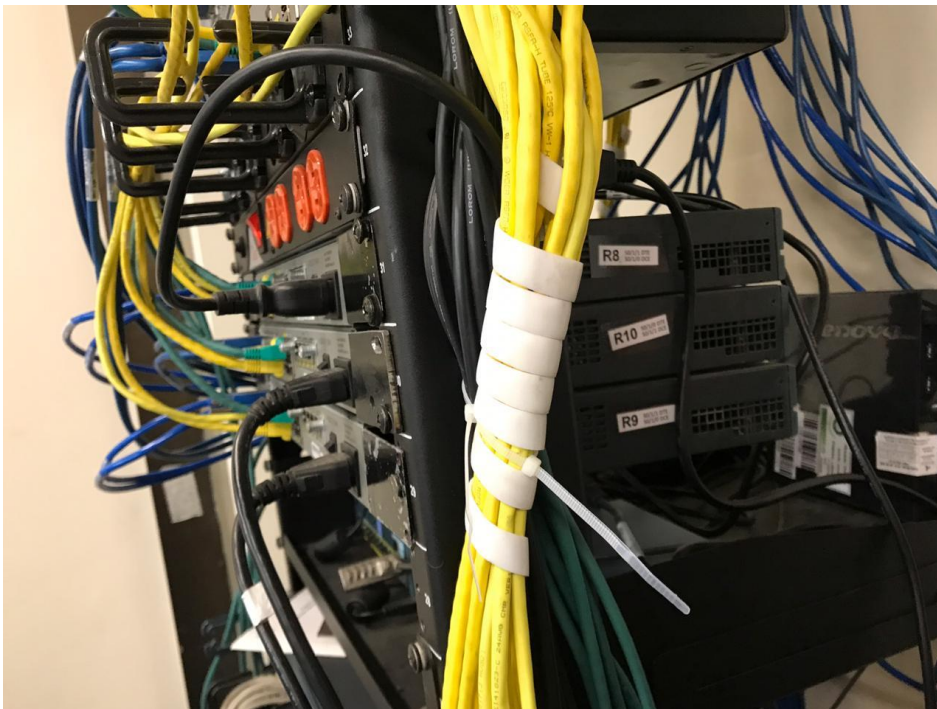
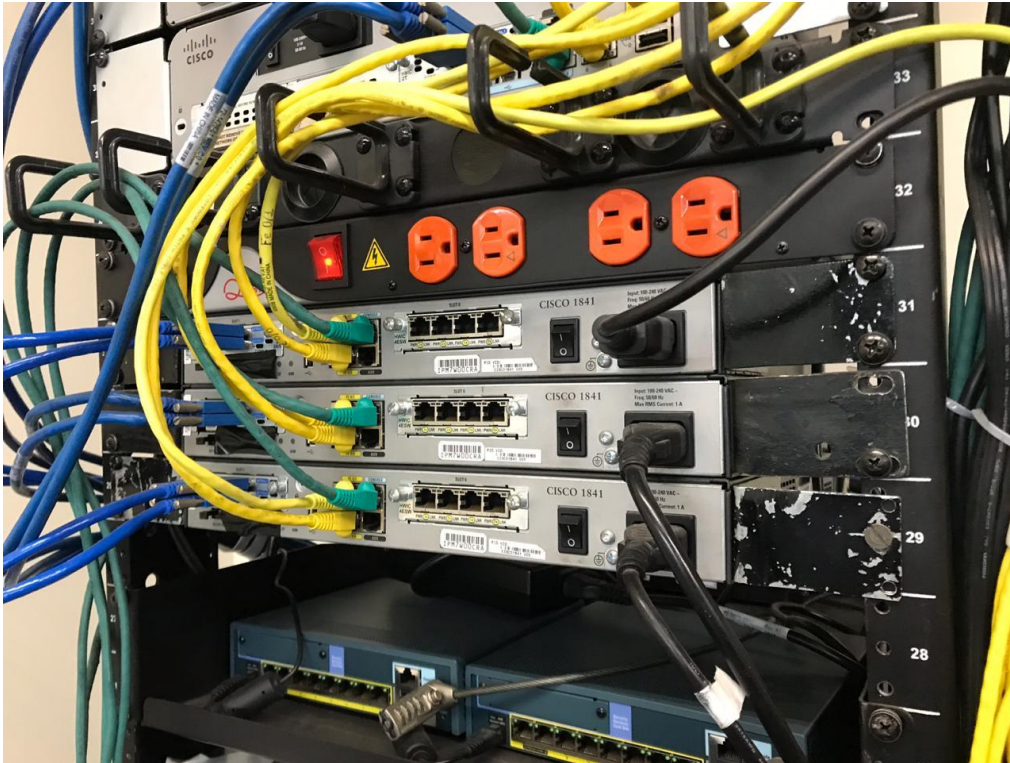




Router Cisco 1941: Son los routers #6 y #7



Router Cisco 1841: Son los routers #8, #9, #10



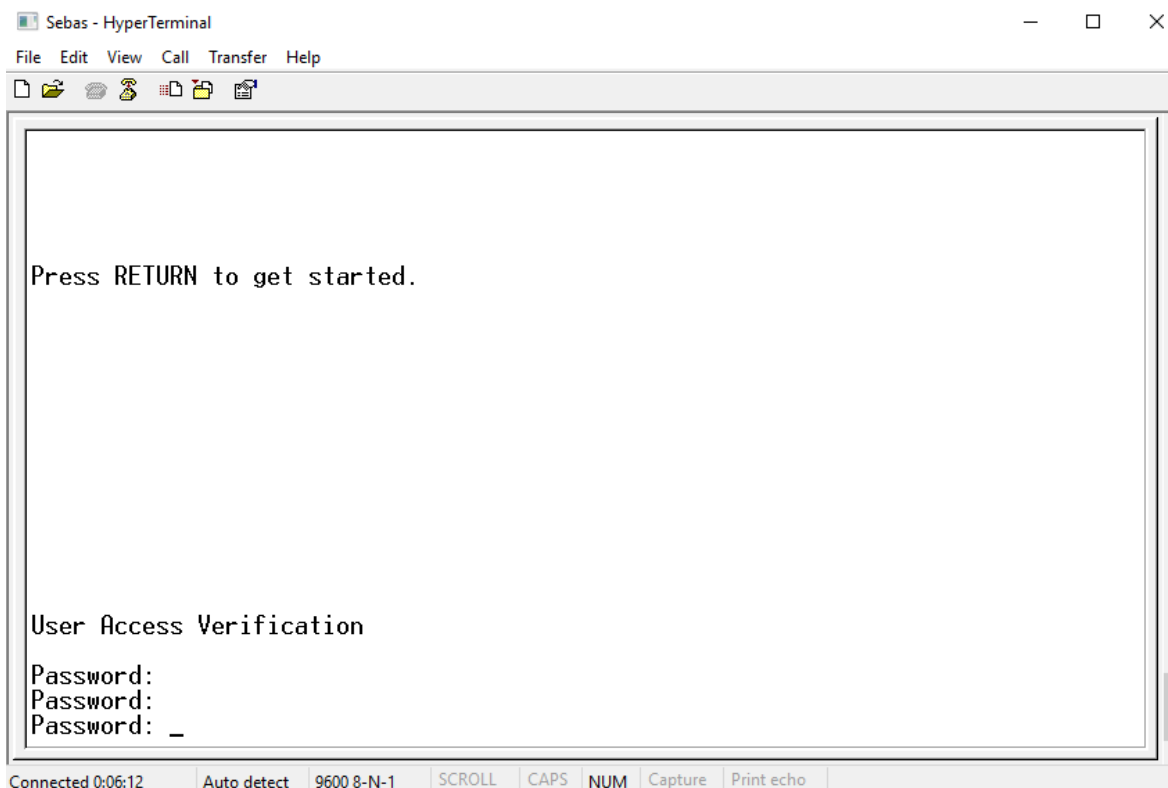
- Para conectarse a los router a través de la consola es necesario conectarse por el cable de consola y usar la aplicación hyperterminal o putty de manera similar a como se conectaron a los switches.



Vamos a trabajar con el Router #1, que es de serie 2800.
Lo primero que toca hacer es encender el router.

- Al iniciar el router aparecen el mismo estilo de mensajes que aparecen en el switches o en el simulador (Packet tracer), intente ingresar al router y entrar al modo privilegiado. Si todo sale bien, podrá ingresar y podrá comenzar a configurar la red que se indica más adelante, pero si el acceso al router o al modo privilegiado del mismo está protegido mediante passwords, deberá quitarle dicha configuración para comenzar a trabajar con el equipo.

Como se puede observar en la siguiente imagen, al ingresar al router pide contraseñas.



Para desconfigurarlas, tenemos que realizar lo siguiente:
Al encender el router presionar las teclas Control + Pausa

```
Sebas - HyperTerminal
File Edit View Call Transfer Help

PC = 0xbfc10908, Cause = 0x2000, Status Reg = 0x3040a803
PC = 0xbfc10d54, Cause = 0x2000, Status Reg = 0x3040a803

rommon 1 > PC = 0xbfc10d54, Cause = 0x2000, Status Reg = 0x3040a803
rommon 1 > PC = 0xbfc10d54, Cause = 0x2000, Status Reg = 0x3040a803
rommon 1 > PC = 0xbfc10908, Cause = 0x2000, Status Reg = 0x3040a803
PC = 0xbfc10d54, Cause = 0x2000, Status Reg = 0x3040a803
rommon 1 > PC = 0xbfc10d54, Cause = 0x2000, Status Reg = 0x3040a803
rommon 1 > PC = 0xbfc10908, Cause = 0x2000, Status Reg = 0x3040a803
PC = 0xbfc10d54, Cause = 0x2000, Status Reg = 0x3040a803
rommon 1 > PC = 0xbfc10d54, Cause = 0x2000, Status Reg = 0x3040a803
rommon 1 > PC = 0xbfc10d54, Cause = 0x2000, Status Reg = 0x3040a803
rommon 1 > PC = 0xbfc10d54, Cause = 0x2000, Status Reg = 0x3040a803
rommon 1 > PC = 0xbfc10d54, Cause = 0x2000, Status Reg = 0x3040a803
rommon 1 > _

Connected 0:05:26 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Luego, en rommon 1 escribir el siguiente comando:

confreg 0x2142

```
rommon 1 > confreg 0x2142
```

```
You must reset or power cycle for new config to take effect
rommon 2 > _
```

Luego, el comando:

Reset

Luego, el comando:

Enable

```
Sebas - HyperTerminal
File Edit View Call Transfer Help

Router>on Interface Serial0/3/0, changed state to down
*Jan 1 00:31:50.355: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/
1, changed state to down
*Jan 1 00:31:58.347: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.4(3i), RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 28-Nov-07 21:09 by stshen
*Jan 1 00:31:58.351: %SNMP-5-COLDSTART: SNMP agent on host Router is undergoing
a cold start
*Jan 1 00:32:00.079: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Jan 1 00:32:00.079: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
*Jan 1 00:32:00.079: %LINK-5-CHANGED: Interface Serial0/2/0, changed state to a
dministratively down
*Jan 1 00:32:00.079: %LINK-5-CHANGED: Interface Serial0/2/1, changed state to a
dministratively down
*Jan 1 00:32:00.079: %LINK-5-CHANGED: Interface Serial0/3/0, changed state to a
dministratively down
*Jan 1 00:32:00.079: %LINK-5-CHANGED: Interface Serial0/3/1, changed state to a
dministratively down
Router>enable_

Connected 0:09:10 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Luego, configure memory:

```
Router#configure memory

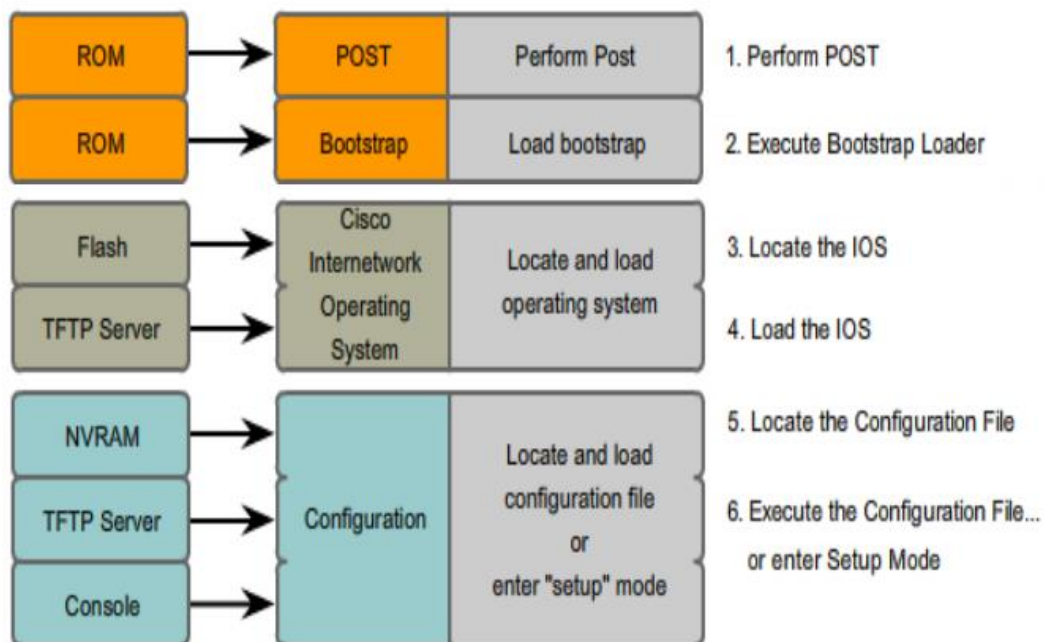
Router#
*Jan 1 00:33:24.603: %SYS-5-CONFIG_I: Configured from memory by console
Router#_

Connected 0:10:23 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

La password que venía en el router estaba cifrada:

```
!
enable secret 5 $1$Ba43$Qno098byAJq01/ntgsLC50uration is 64 bits wide with parit
!
```

- Para los routers Cisco, ¿Qué significan los modos de arranque 0x2142 y 0x2102?



El modo de arranque 0x2142 omite el start-up config, es decir, omite la parte de arranque del router de: Locate the IOS y Load the IOS

Mientras que el modo de arranque 0x2102 sí realiza todos los pasos del arranque del router.

0x2142

- Ignora interrupción
- Inicia desde la memoria ROM si falla el arranque inicial
- Velocidad de consola en baudios: 9600
- Ignora el contenido de la Memoria RAM No Volátil (el NVRAM) (ignora la configuración)

0x2102

- Ignora interrupción
- Inicia desde la memoria ROM si falla el arranque inicial
- Valor predeterminado de velocidad de consola 9600 en baudios para la mayoría de las plataformas

- Realice la siguiente configuración usando los equipos físicos y documente el proceso. La configuración básica de un router debe tener:
 - Claves de acceso al modo privilegiado, consola y acceso remoto. la clave de acceso a modo privilegiado debe ser lab5priv, el de consola, lab5con y el de acceso remoto (telnet), lab5rem.

Se le coloca la siguiente contraseña en el modo de configuración para entrar al modo privilegiado: lab5priv

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret lab5priv
```

La contraseña de consola: lab5con

```
Router(config)#line console 0
Router(config-line)#pass
Router(config-line)#password lab5con_
```

La contraseña de acceso remoto: lab5rem

```
Router(config)#line vty 0 15
Router(config-line)#password lab5rem_
```

- Nombre del router. Coloque el apellido de uno de los estudiantes del grupo al router.

```
Router(config)#hostname Frasica
Frasica(config)#_
```

- Sincronización de pantallas de consola y acceso remoto

De consola:

```
Frasica(config)#line console 0
Frasica(config-line)#logg
Frasica(config-line)#logging s
Frasica(config-line)#logging synchronous
```

De acceso remoto:

```
Frasica(config)#enable secret lab5priv
Frasica(config)#line con
Frasica(config)#line console 0
Frasica(config-line)#password lab5con
Frasica(config-line)#logg
Frasica(config-line)#logging sy
Frasica(config-line)#logging synchronous
Frasica(config-line)#login
Frasica(config-line)#exit
Frasica(config)#line v
Frasica(config)#line vty 0 4
Frasica(config-line)#password lab5rem
Frasica(config-line)#logg
Frasica(config-line)#logging s
Frasica(config-line)#logging synchronous
Frasica(config-line)#_
```

- Descripción de las interfaces que usen

```

Frasica(config)#int fa0/0
Frasica(config-if)#description "Esta es la conexion para SISTEMAS106"
Frasica(config-if)#exit
Frasica(config)#int fa0/1
Frasica(config-if)#description "Esta es la conexion para SISTEMAS105"
Frasica(config-if)#exit
Frasica(config)#_

```

- No consultar servidor remoto de comandos

```

Frasica(config)#no ip
Frasica(config)#no ip do
Frasica(config)#no ip domain-
Frasica(config)#no ip domain-look
Frasica(config)#no ip domain-lookup

```

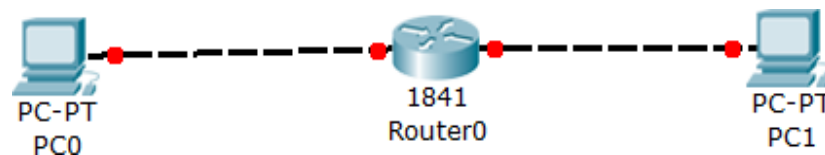
- Mensaje del día

```

Frasica(config)#banner motd "Este router solo puede ser utilizado en el Lab5 d$

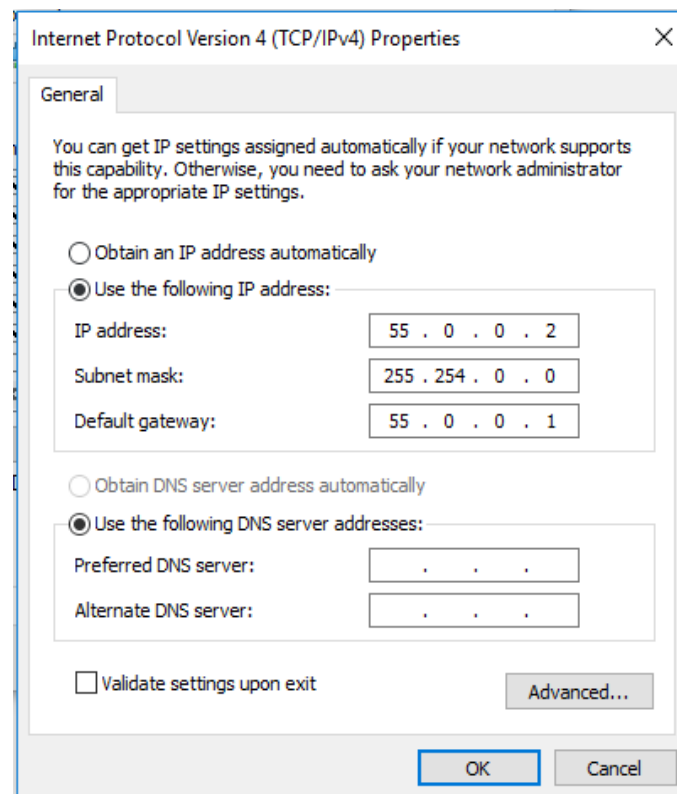
```

- Para la red de la izquierda use el rango 55.0.0.0/15 y para la red de la derecha, el rango 134.43.0.0/20.

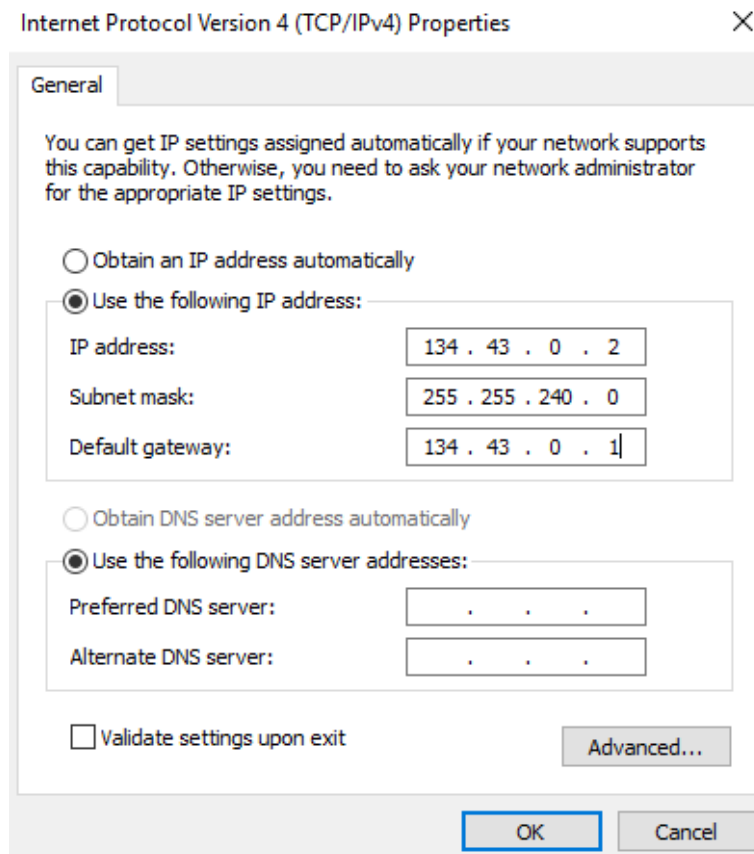


Recomendación: Primero configure el router a través del cable de consola y luego haga la configuración y conexión a los PCs.

Configuración IPv4 del PC 0:



Configuración IPv4 del PC 1:



Configuración IPv4 del router:

```
Frasica(config)#interface FastEthernet 0/0
Frasica(config-if)#ip add
Frasica(config-if)#ip address 134.43.0.1 255.255.240.0
Frasica(config-if)#_
```

```
-----
Frasica(config)#int fa0/0
Frasica(config-if)#no shut
Frasica(config-if)#no shutdown _
```

```
Frasica(config)#int fa 0/1
Frasica(config-if)#ip add
Frasica(config-if)#ip address 55.0.0.1 255.254.0.0
Frasica(config-if)#no shutdown_
```

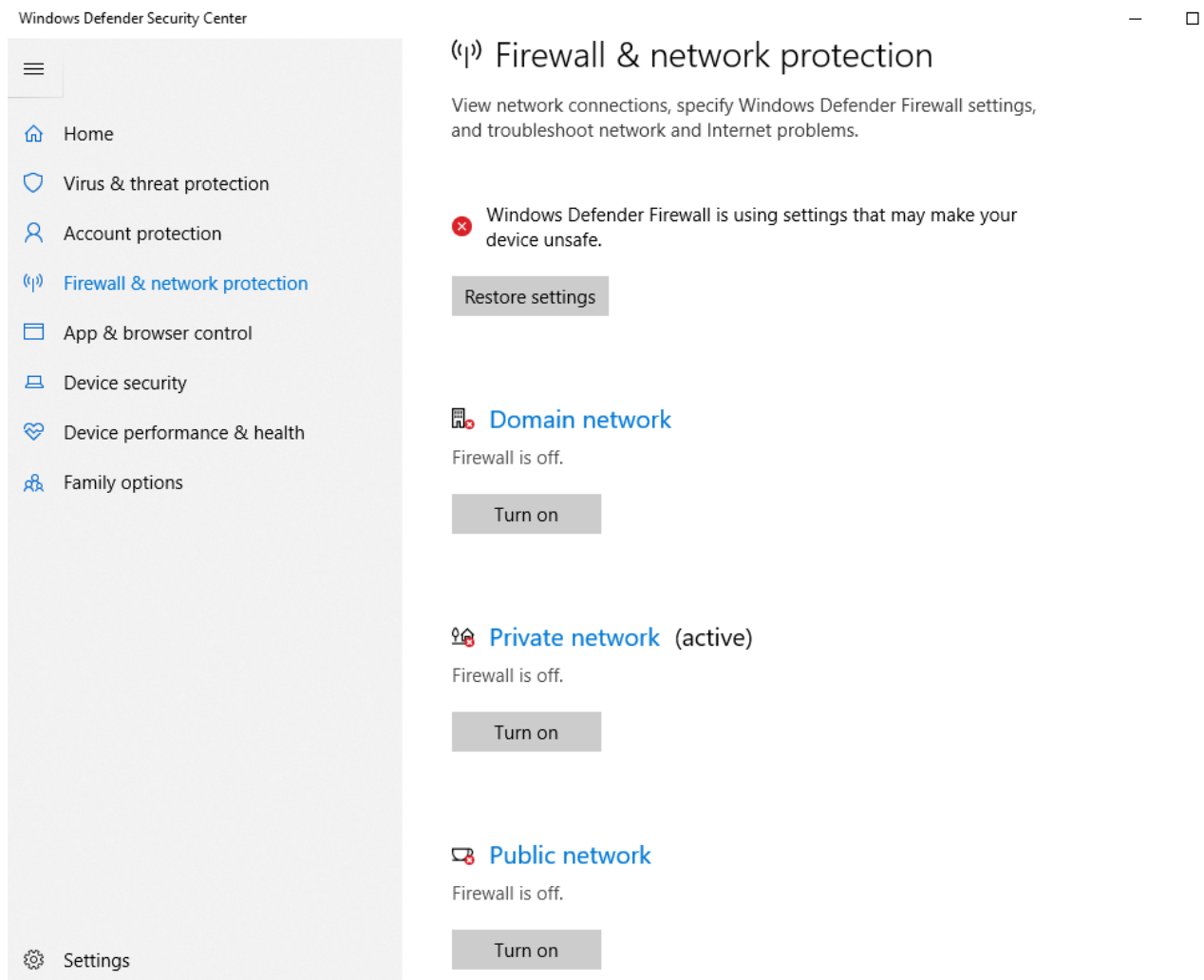
Luego, al ejecutar el comando show run:

```

interface FastEthernet0/0
description "Esta es la conexion para SISTEMAS106"
ip address 134.43.0.1 255.255.240.0
duplex auto
speed auto
!
interface FastEthernet0/1
description "Esta es la conexion para SISTEMAS105"
ip address 55.0.0.1 255.254.0.0
duplex auto
speed auto

```

Para poder realizar el ping, toca desactivar el Firewall de Windows:



Ping al router desde PC0:


```
C:\Users\Redes>ping 55.0.0.1

Pinging 55.0.0.1 with 32 bytes of data:
Reply from 55.0.0.1: bytes=32 time=1ms TTL=255
Reply from 55.0.0.1: bytes=32 time=1ms TTL=255
Reply from 55.0.0.1: bytes=32 time=1ms TTL=255
Reply from 55.0.0.1: bytes=32 time=1ms TTL=255

Ping statistics for 55.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Ping a PC1 desde PC0:

```
C:\Users\Redes>ping 134.43.0.2

Pinging 134.43.0.2 with 32 bytes of data:
Reply from 134.43.0.2: bytes=32 time=1ms TTL=127
Reply from 134.43.0.2: bytes=32 time=1ms TTL=127
Reply from 134.43.0.2: bytes=32 time=1ms TTL=127
Reply from 134.43.0.2: bytes=32 time=2ms TTL=127

Ping statistics for 134.43.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Ping al router desde PC1:

```
C:\Users\Redes>ping 134.43.0.1

Pinging 134.43.0.1 with 32 bytes of data:
Reply from 134.43.0.1: bytes=32 time=1ms TTL=255
Reply from 134.43.0.1: bytes=32 time=1ms TTL=255
Reply from 134.43.0.1: bytes=32 time=1ms TTL=255
Reply from 134.43.0.1: bytes=32 time=1ms TTL=255

Ping statistics for 134.43.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Ping a PC0 desde PC1:

```

C:\Users\Redes>ping 55.0.0.2

Pinging 55.0.0.2 with 32 bytes of data:
Reply from 55.0.0.2: bytes=32 time=1ms TTL=127
Reply from 55.0.0.2: bytes=32 time=2ms TTL=127
Reply from 55.0.0.2: bytes=32 time=2ms TTL=127
Reply from 55.0.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 55.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

```

5. Montaje - Interconexión serial

Únase con otro grupo de estudiantes e interconecte los router que utilizaron en el punto anterior. Para la interconexión de los mismos use las tarjetas seriales de los equipos. Use la red 200.24.25.16/30



Los router utilizados son:

- R1s0/3/0 DTE
- R6s0/0/1 DCE

```

Frasica(config)#int s
Frasica(config)#int serial 0/3/0
Frasica(config-if)#ip add 200.24.25.17 255.255.255.252
Frasica(config-if)#no shut
Frasica(config-if)#no shutdown _

```

- Usando el comando ping, verifique la comunicación desde el router 0 y router1.

Nota: ¡la interconexión de computador a computador no funcionará todavía!

- ¿Qué es un null modem?

Es una forma de enlazar dos terminales por ejemplo (computador, terminal, impresora,

etc) usando un cable RS-232 (serie ó paralelo). El cableado Null-Modem tiene cruzadas las líneas de transmisión y recepción.



La conexión Null-Modem no está definida por algún estándar y es por eso que existen muchas formas de realizar este tipo de conexión.

Es un cable especialmente diseñado que permite una conexión head to head entre dos dispositivos seriales cercanos a través de sus puertos RS232, se usa comúnmente para conectar equipos dentro de la misma sala con el fin de enviar y recibir archivos. También se conoce como un cable cruzado.

- **¿Para qué se usa el comando clock rate en los routers?, ¿por qué se necesita?**

El clockrate (que se configura solo para DCE) se usa para el sincronismo de la conexión en serie. Sin el clockrate, la conexión no funciona porque no hay ningún entendimiento de la velocidad de los datos enviados entre los dos extremos de la conexión.

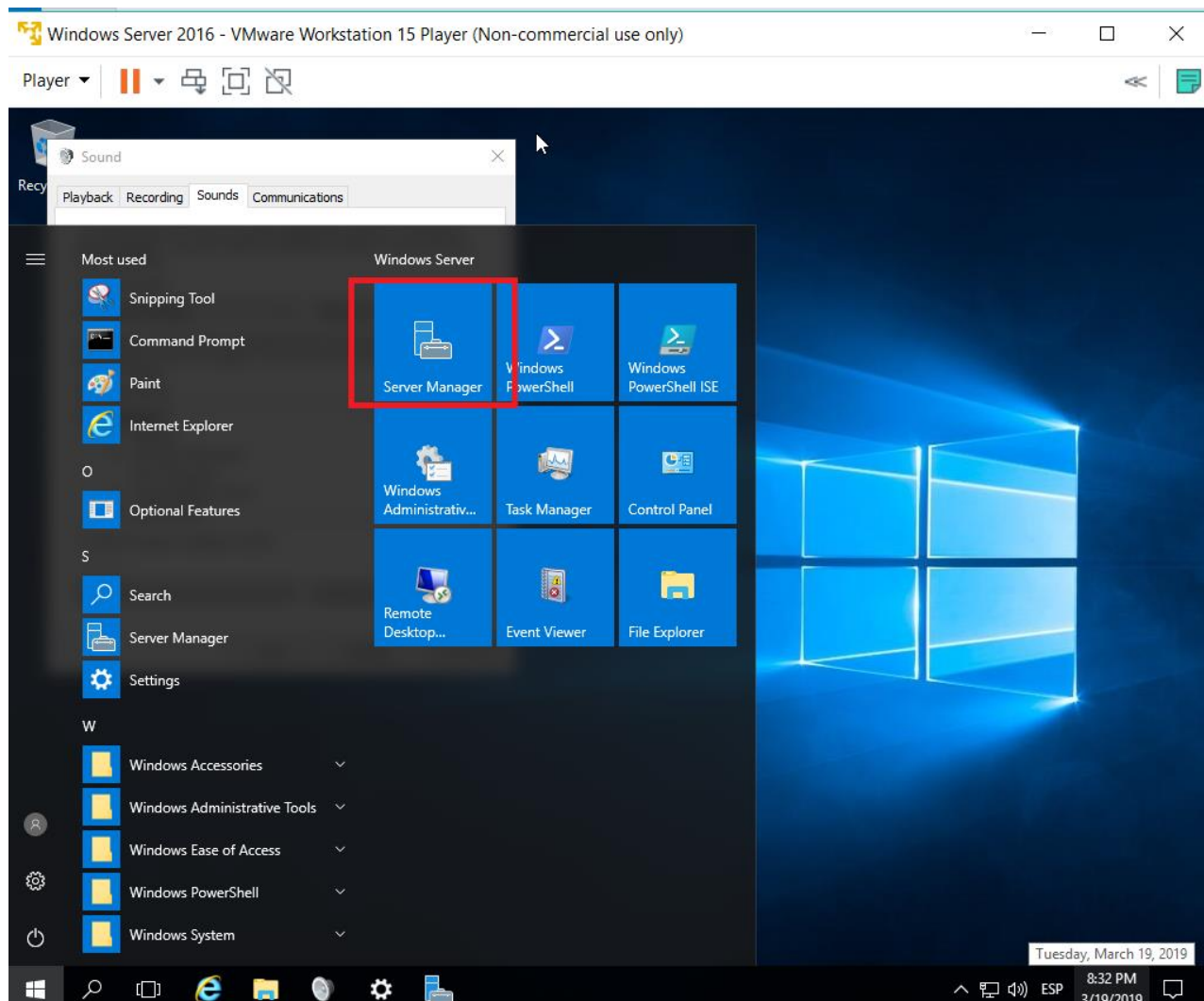
Instalación de software base

Parte de la plataforma base de una infraestructura computacional de una organización es el servidor Web. A través de él se acceden a aplicaciones y datos de la organización.

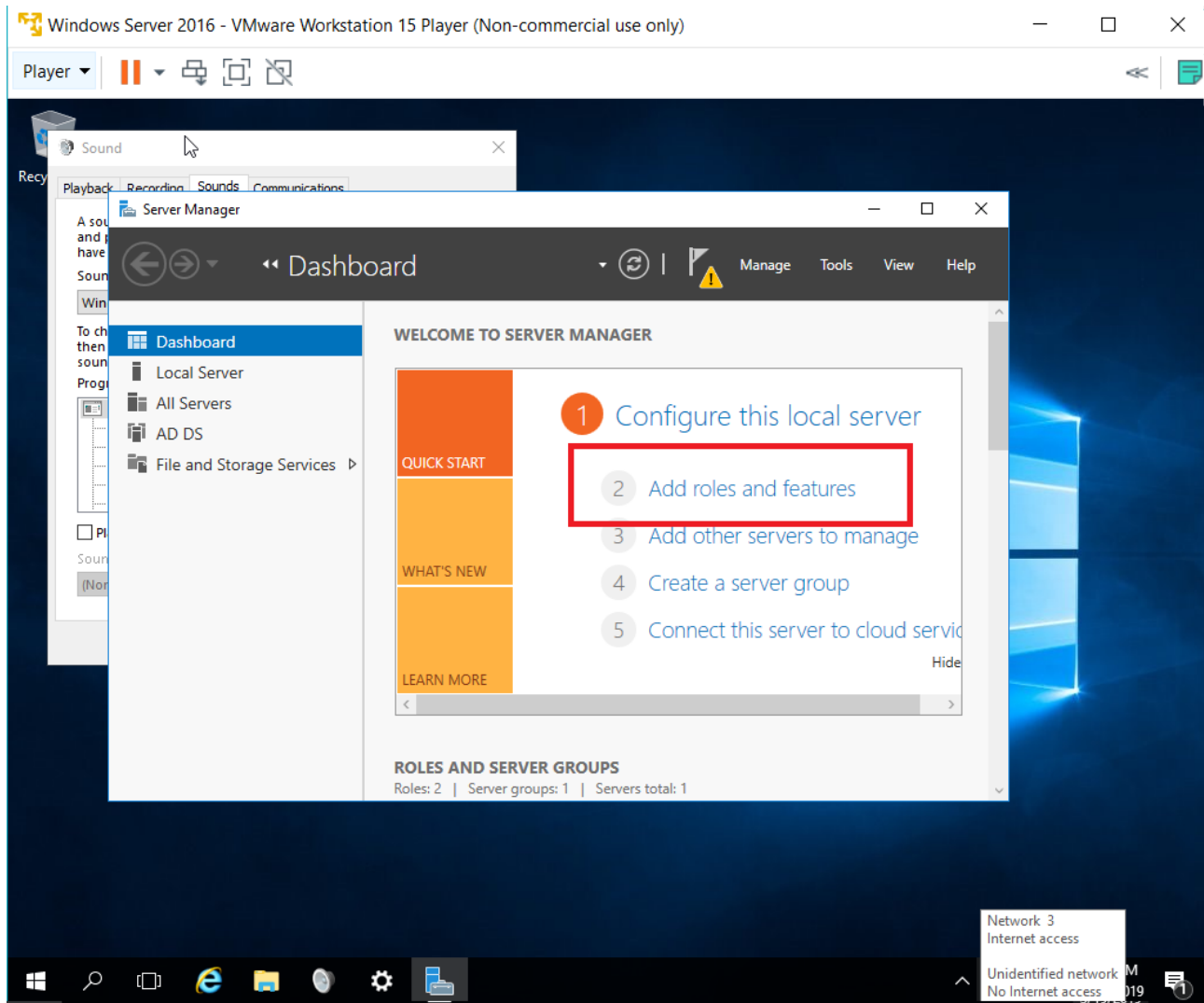
En los mismos grupos en los que se realizó todo este laboratorio, realice las siguientes actividades:

1. Configure el servidor web con que viene Windows Server

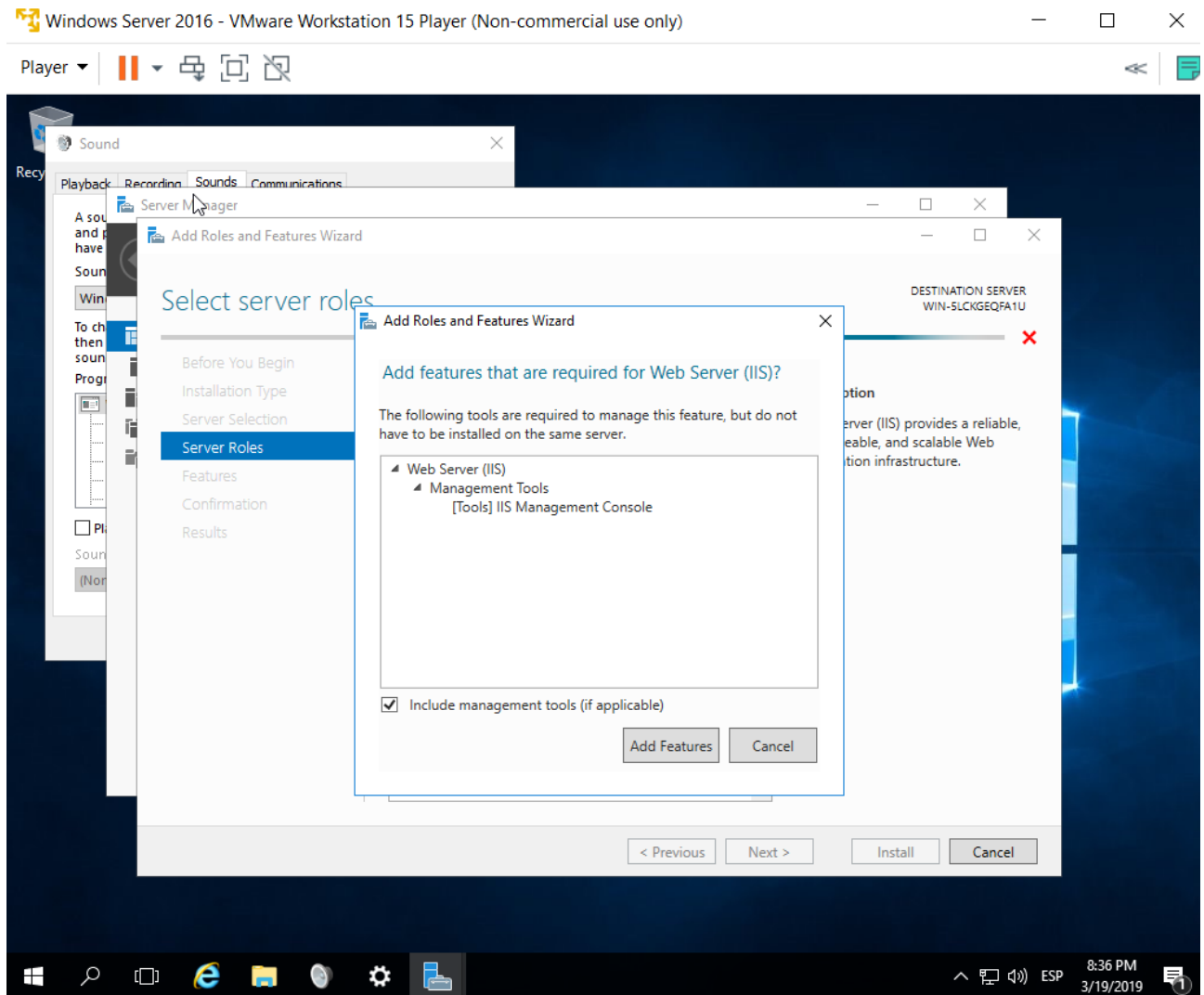
Primero, accedemos a la maquina virtual de Windows Server 2016 creada y configurada en el primer laboratorio. Y nos vamos a la parte de Server Manager.



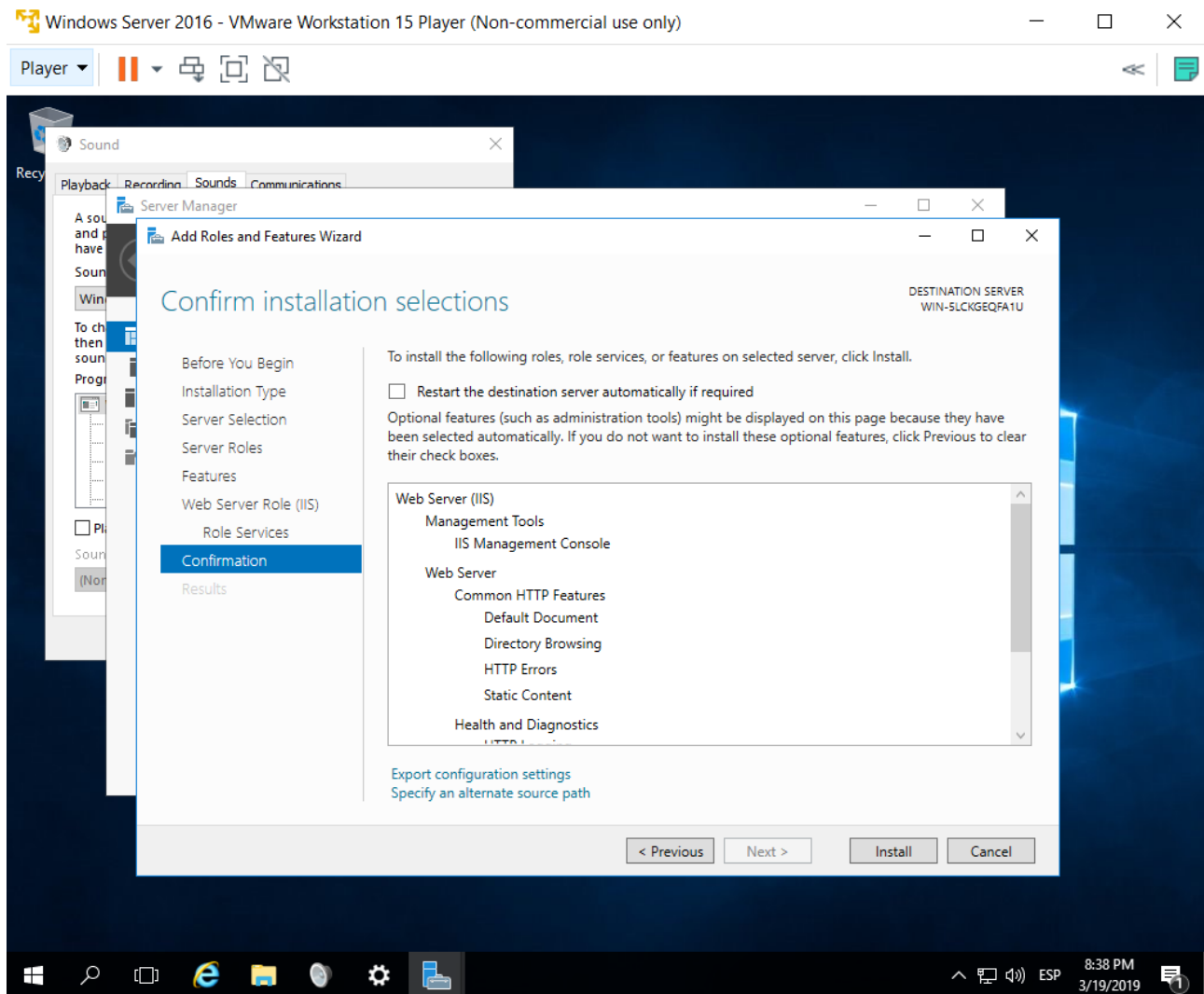
Luego a la parte que dice “Add roles and features”



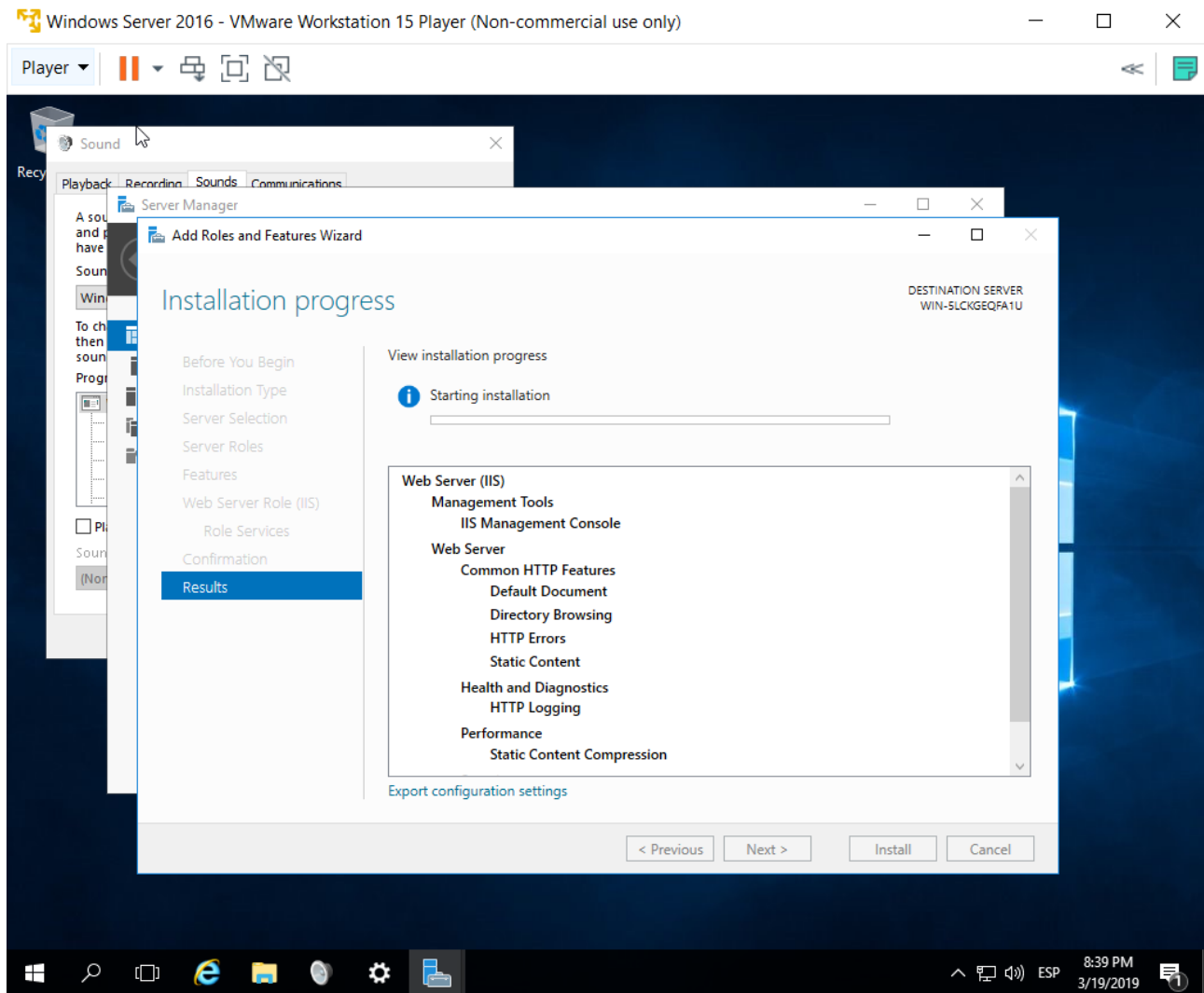
Luego, en la parte de Server Roles, agregamos el feature de Web Server (ISS)



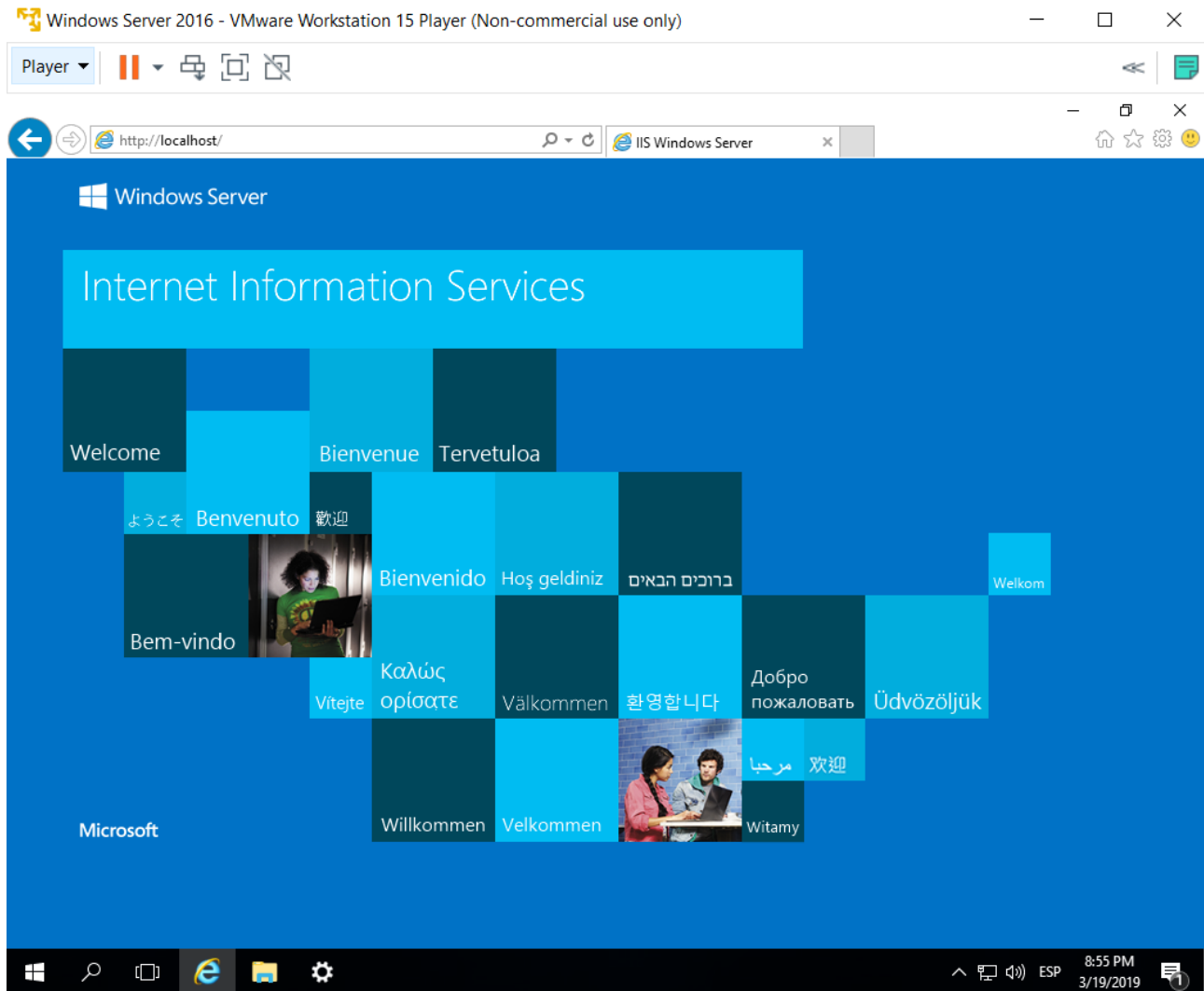
Se procede a instalar el servidor web:



Esperamos que termine de instalar...



Para confirmar la instalación del servidor web ingresamos la siguiente dirección en el navegador: <http://localhost/>



Y se puede observar que el servidor web fue instalado correctamente.

2. Cree 2 páginas web así

a. Torneo.

- Se deberá configurar en el servidor Windows Server.
- Haga una aplicación sencilla que muestre el contenido de la base de datos del torneo.

b. Maratones.

- Se deberá configurar en el servidor Linux Slackware.
- Haga una aplicación sencilla que muestre el contenido de la base de datos de competencias de maratones y entrenamientos.

Conclusiones:

- Mediante este laboratorio se aprendió a configurar un router Cisco serie 2800.
- Se aprendió a solucionar problemas de red de manera manual.
- Se conoció la operación del protocolo ARP en una red.

- Se realizó seguimiento de redes con el protocolo ICMP.
- Se entendió que los paquetes que se envían a través de la red pueden llegar a viajar por muchas partes del mundo.
- Se aprendió a configurar un servidor web en Windows Server.
- Se entendieron y se vio en práctica algunas de las funcionalidades que realiza la capa de red siguiendo la arquitectura TCP/IP.

Bibliografía:

- Anónimo. Procedimiento para recuperación de contraseña para los Cisco 2600 y 2800 Series Router [consulta: 15 de marzo de 2019] Disponible en:
https://www.cisco.com/c/es_mx/support/docs/routers/2600-series-multiservice-platforms/22188-pswdrec-2600.pdf
- Claudia Santiago. *Capa de Red* [online]. [consulta: 16 de marzo de 2019].
Disponible en:
http://campusvirtual.escuelaing.edu.co/moodle/pluginfile.php/152626/mod_resource/content/2/04-capaRed_2019-1%20P1.pdf
- Georg Pauwen. ¿Para qué sirve el ClockRate? [consulta: 15 de marzo de 2019]
Disponible en:
<https://community.cisco.com/t5/other-network-architecture/para-que-sirve-el-clockrate/td-p/282854>