--

**MATERIAL NECESARIO**

1. PC con acceso a la LAN/WLAN basada en switch / WiFi con acceso a Internet, con

Analizador de Tramas  **Wireshark, última versión**.

**DESCRIPCION**

Este trabajo será desarrollado por cada alumno en una PC con acceso a LAN/WLAN Ethernet y **evaluado individualmente**.

***1. Caso de Estudio***

Tráfico real circulante en la red y / o generado por el alumno.

***2. Requerimientos para el alumno (Objetivos Técnicos)***

**a. Examinar y utilizar las funciones de análisis del software de análisis de protocolos.**

***b.* Comprender el funcionamiento de los siguientes protocolos mediante la verificación experimental del modelo y proceso descripto en la teoría y en las RFCs respectivas*.***

**c. Resguardar los archivos de capturas, para futuras actividades de laboratorio.**

**d. Responder el cuestionario escrito al finalizar las tareas.**

***3. Tareas***

Realice las siguientes tareas en el intérprete de comandos (ejecute *cmd* en

Texto

Descripción generada automáticamenteWindows):

**a. Análisis de la LAN / WLAN donde está su estación de trabajo**

**1)** Obtenga los datos de su Host en su entorno de LAN/WLAN con el comando

***ipconfig /all*** y registre los datos obtenidos en la siguiente tabla:

Tabla

Descripción generada automáticamente

|  |  |
| --- | --- |
|  | |
| Nombre de host | DESKTOP-E21ALTV |
| Dirección IP de Host | 192.168.0.47 (Adaptador Ethernet) |
| Mascara de subred de host | 255.255.255.0 |
| Puerta de enlace predeterminada | 192.168.0.1  fe80::ae3b:77ff:fe9e:5376%15 |
| Dirección IP de Broadcast de la red | 192.168.0.255 |
| Servidor DHCP de la Red Wifi | 192.168.0.1 |
| Dirección MAC de la Placa de Red Wifi | D8-5E-D3-D5-E5-9A |
| Servidor/es DNS reconocidos | 2800:810:100:1:200:115:192:29  2800:810:100:3:200:115:192:89  2800:810:100:1:200:115:192:30  2800:810:100:1:200:115:192:28  100.72.3.105  100.72.3.1  2800:810:100:1:200:115:192:29  2800:810:100:3:200:115:192:89  2800:810:100:1:200:115:192:30 |

PS C:\Users\Daniel> ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . . . . . : DESKTOP-E21ALTV

Sufijo DNS principal . . . . . :

Tipo de nodo. . . . . . . . . . : híbrido

Enrutamiento IP habilitado. . . : no

Proxy WINS habilitado . . . . . : no

Lista de búsqueda de sufijos DNS: home

192.168.50.60

Adaptador desconocido OpenVPN Wintun:

Estado de los medios. . . . . . . . . . . : medios desconectados

Sufijo DNS específico para la conexión. . :

Descripción . . . . . . . . . . . . . . . : Wintun Userspace Tunnel

Dirección física. . . . . . . . . . . . . :

DHCP habilitado . . . . . . . . . . . . . : no

Configuración automática habilitada . . . : sí

Adaptador desconocido Conexión de área local:

Estado de los medios. . . . . . . . . . . : medios desconectados

Sufijo DNS específico para la conexión. . :

Descripción . . . . . . . . . . . . . . . : Wintun Userspace Tunnel #2

Dirección física. . . . . . . . . . . . . :

DHCP habilitado . . . . . . . . . . . . . : no

Configuración automática habilitada . . . : sí

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . : home

Descripción . . . . . . . . . . . . . . . : Realtek Gaming GbE Family Controller

Dirección física. . . . . . . . . . . . . : D8-5E-D3-D5-E5-9A

DHCP habilitado . . . . . . . . . . . . . : sí

Configuración automática habilitada . . . : sí

Dirección IPv6 . . . . . . . . . . : 2800:810:536:2d14:168:f321:8501:4b2c(Preferido)

Concesión obtenida. . . . . . . . . . . . : martes, 17 de mayo de 1887 5:25:13

La concesión expira . . . . . . . . . . . : viernes, 23 de junio de 2023 10:52:54

Dirección IPv6 . . . . . . . . . . : 2800:810:536:2d14:48f3:5a7a:ea0b:f6e7(Preferido)

Dirección IPv6 . . . . . . . . . . : fdaa:bbcc:ddee:0:ccc6:3c1f:417f:8216(Preferido)

Dirección IPv6 temporal. . . . . . : 2800:810:536:2d14:294b:a012:5ce2:702b(Preferido)

Dirección IPv6 temporal. . . . . . : fdaa:bbcc:ddee:0:294b:a012:5ce2:702b(Preferido)

Vínculo: dirección IPv6 local. . . : fe80::a110:8f6b:a356:4868%15(Preferido)

Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.47(Preferido)

Máscara de subred . . . . . . . . . . . . : 255.255.255.0

Concesión obtenida. . . . . . . . . . . . : martes, 17 de mayo de 1887 5:25:12

La concesión expira . . . . . . . . . . . : viernes, 23 de junio de 2023 10:53:27

Puerta de enlace predeterminada . . . . . : fe80::ae3b:77ff:fe9e:5376%15

192.168.0.1

Servidor DHCP . . . . . . . . . . . . . . : 192.168.0.1

IAID DHCPv6 . . . . . . . . . . . . . . . : 265838291

DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-2C-0E-66-09-D8-5E-D3-D5-E5-9A

Servidores DNS. . . . . . . . . . . . . . : 2800:810:100:1:200:115:192:29

2800:810:100:3:200:115:192:89

2800:810:100:1:200:115:192:30

2800:810:100:1:200:115:192:28

100.72.3.105

100.72.3.1

2800:810:100:1:200:115:192:29

2800:810:100:3:200:115:192:89

2800:810:100:1:200:115:192:30

NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado

Lista de búsqueda de sufijos DNS específicos de conexión:

home

Adaptador de Ethernet Ethernet 2:

Sufijo DNS específico para la conexión. . :

Descripción . . . . . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter

Dirección física. . . . . . . . . . . . . : 0A-00-27-00-00-11

DHCP habilitado . . . . . . . . . . . . . : no

Configuración automática habilitada . . . : sí

Vínculo: dirección IPv6 local. . . : fe80::1495:8f12:2946:b377%17(Preferido)

Dirección IPv4. . . . . . . . . . . . . . : 192.168.56.1(Preferido)

Máscara de subred . . . . . . . . . . . . : 255.255.255.0

Puerta de enlace predeterminada . . . . . :

IAID DHCPv6 . . . . . . . . . . . . . . . : 671744039

DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-2C-0E-66-09-D8-5E-D3-D5-E5-9A

Servidores DNS. . . . . . . . . . . . . . : fec0:0:0:ffff::1%1

fec0:0:0:ffff::2%1

fec0:0:0:ffff::3%1

NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado

**2)** Obtenga las direcciones IP conocidas por su Host en el entorno de la misma red

IP para utilizarlas en el laboratorio, mediante el comando ***arp – a***:

***C:\>WINDOWS>arp –a***

PS C:\Users\Daniel> arp -a

Interfaz: 10.10.102.22 --- 0x3

Dirección de Internet Dirección física Tipo

10.10.102.21 00-ff-11-3f-4a-fa dinámico

10.10.102.23 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

239.255.255.250 01-00-5e-7f-ff-fa estático

255.255.255.255 ff-ff-ff-ff-ff-ff estático

Interfaz: 192.168.0.47 --- 0xf

Dirección de Internet Dirección física Tipo

192.168.0.1 ac-3b-77-9e-53-76 dinámico

192.168.0.255 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

Interfaz: 192.168.56.1 --- 0x11

Dirección de Internet Dirección física Tipo

192.168.56.255 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

**3)** Si tiene el celular, tablet, notebook o PC conectados en la misma LAN / WLAN

identifique cuáles direcciones IP y MAC corresponden a cada uno.

|  |  |  |
| --- | --- | --- |
| **HOST** | **IP** | **MAC** |
| PC |  |  |
| Celular |  |  |
| Notebook |  |  |
| Access Point (Gateway) |  |  |

**4)** Confirme los datos con los que fueron obtenidos mediante el comando ***ipconfig /all***

**5)** ¿De qué clase es la dirección IP del Host utilizado?

Si es A, B o C

Viendo la mascara

Generalmente en la casa es clase C o /24 que es 255.255.255.0

**6)** ¿Cuál es su máscara de red? ¿Es una máscara por defecto?

**7)** ¿La red tiene subredes?

En base a la mascara

**8)** ¿La dirección de red es pública o privada? ¿Qué otras direcciones de red de esta misma clase están reservadas?

**9)** ¿Cuántos hosts puede haber en la red como máximo?

**10)** ¿Cuál es el estándar IEEE que se emplea en esta red? ¿Qué método de

Control de Acceso utiliza, CSMA/CD o CSMA/CA?

Se vio en la teoría, que es CD, colisión-detection

**11)** ¿Es una red que detecta colisiones? En caso afirmativo, ¿Cuántos dominios de colisión tiene?

**12)** ¿Es una red que previene colisiones? En caso afirmativo, ¿Qué problemas resuelve

CSMA/CA que no resuelve CSMA/CD?

**13)** ¿Es una red que utiliza broadcast de direcciones MAC? En caso afirmativo,

¿Cuántos dominios de broadcast tiene? ¿Qué protocolos en entorno

LAN/WLAN utilizan broadcast de capa 2 para funcionar)

A los dominios de broadcast, donde hay dominio de router hay dominio de broadcast

**14)** En una LAN ¿cómo se puede segmentar un dominio de colisión?

Se puede con vlan segmentarlo

**15)** En una LAN ¿cómo se puede segmentar un dominio de broadcast?

Poniendo un router en el medio

**16)** ¿Esta red emplea direccionamiento IP estático o dinámico? ¿Qué protocolo se utiliza para asignación dinámica de direcciones IP y cuántas PDU se intercambian entre el cliente y el servidor?

Depende de la configuración

Generalmente en wifi ya viene configurado el DHCP

**17)** Identifique direcciones IP públicas conocidas por su Host.

**b. Análisis de una trama Ethernet**

Inicie una captura con el Analizador y haga PING al Gateway (puerta de enlace) o a otro host de su misma LAN/WLAN (puede ser su móvil u otro dispositivo conectado a su LAN/W[LAN).](https://wiki.wireshark.org/STP) Detenga la captura. Responda las siguientes preguntas, analizando una trama en particular:

**1)** ¿Cuáles son los camp[os de la](https://wiki.wireshark.org/VLAN) trama? ¿Qué valores tiene cada campo y cuál es su significado?

**2)** ¿Qué tamaño tiene el encabezado de la trama y cuáles son sus campos?

**3)** ¿Qué tamaño tiene la cola de su trama? ¿Qué campo sirve para detectar errores y cuál es su valor?

**4)** ¿Cuántos bytes corresponden a los datos? ¿Este campo es de tamaño fijo o variable? En este nivel ¿el campo de datos tiene una longitud mínima, máxima o no está especificado por su estándar?

**5)** Revisando nuevamente la trama Ethernet ¿qué campos se corresponden con los especificados en IEEE 802.2 y cuáles a IEEE 802.3?

**En 802.3 es el len**

**Ethernet es el letter type**

**6)** ¿Qué protocolos de nivel 3 (TCP/IP) se encapsularon en las tramas?

**7)** ¿Qué protocolos de nivel 4 y 5 (TCP/IP) se encapsularon en la trama?

**c. Estudio comparativo de tramas típicas de LAN Ethernet**

Agregue a la captura de tramas Ethernet: IEEE 802.3 ó 802.11, las capturas en su red o ejemplos del sitio https://wiki.wireshark.org/ que se correspondan con:

• IEEE\_802.11: IEEE 802.11 wireless LANs

• STP: IEEE 802.1D Spanning Tree Protocol

• VLAN: IEEE 802.1Q Virtual Bridged Local Area Networks

Realice un estudio comparativo de los 4 tipos de tramas, identificando las funciones particulares de la capa de enlace, qué campos intervienen en cada caso, los procesos que intervienen en el Tx y en el Rx, señalando similitudes y diferencias.

**d. Análisis del tráfico ARP**

Realice las siguientes tareas en el intérprete de comandos (cuando sea necesario ejecute el comando con permisos de *Administrador*) y capture una o más tramas auxiliándose con el analizador de protocolos:

**1)** Observe el estado de la memoria caché de ARP en su PC.

***C:\>WINDOWS>arp –a***

**2)** Borre la memoria caché de ARP en su PC.

***C:\>WINDOWS>arp -d <dirección IP>***

**3)** Inicie una captura con el Analizador y haga PING a otra PC, host o dispositivo de la misma LAN/WLAN o al Gateway de su red. Detenga la captura.

Responda:

a) ¿En nivel del modelo OSI funciona el protocolo ARP?

b) ¿Cuántas PDU intervienen en la resolución ARP?

c) Describa la secuencia de tramas involucradas, justificando todas las direcciones MAC e IP que aparecen

d) ¿Cuál es el estado actual de la memoria caché de ARP?

e) Volver a ejecutar el comando Ping a la misma máquina y observar la secuencia de tramas ARP. ¿Aparecen las mismas tramas ARP? ¿Por qué?

f) ¿Qué formato tiene una PDU ARP?

**4)** Abra una página en Internet no haya abierto desde que encendió la PC.

Capture el tráfico involucrado y responda las mismas preguntas que en el ejercicio anterior. ¿Los Hosts que intervienen en esta captura son los mismos que en el caso anterior?

**e. Análisis del tráfico IP e ICMP**

Realice las siguientes tareas en el intérprete de comandos y registre lo obtenido, auxiliándose con el analizador de protocolos:

Responda las siguientes preguntas para cada caso:

**1)** Al hacer Ping a la dirección IP de su PC.

**2)** Al hacer Ping a otra PC, host o Gateway de la LAN o WLAN.

**3)** Al hacer Ping a la dirección IP de un sitio de Internet no disponible en caché (por ej: a una web de otro país no visitada habitualmente).

|  |  |  |  |
| --- | --- | --- | --- |
| **Preguntas** | **Caso 1)** | **Caso 2)** | **Caso 3)** |
| a) ¿Se ejecutó la  aplicación Ping? |  |  |  |
| b) ¿Salen paquetes hacia la red?  ¿Cuántos? |  |  |  |
| c) ¿Qué tamaño tiene  cada paquete? |  |  |  |
| d) ¿Cuántos bytes corresponden a  cada protocolo? |  |  |  |
| e) ¿Cuántos bytes corresponden a los datos transmitidos? |  |  |  |

**4)** Al hacer Ping ¿cuántas capas del Modelo OSI y qué protocolos intervienen?

¿Qué tipos y códigos de mensaje ICMP se observaron en los casos analizados?

**f. Análisis del MTU de la red**

Ejecute la aplicación COMMAND o en Programas el icono MS-DOS e inicie una nueva captura con el analizador de protocolos. Utilice para el tamaño de paquetes el parámetro **– l** de la aplicación Ping.

Realice las siguientes tareas en el intérprete de comandos y registre lo obtenido:

**1) Ping a una PC o terminal con tamaño de paquete de 200 bytes.**

(***C:\>WINDOWS>ping -l 200 <dirección IP>)***

**2) Ídem con 1499 bytes.**

**3) Ídem con 2000 bytes**

Responda las siguientes preguntas para cada ítem:

a) ¿En qué caso se fragmentaron los paquetes? ¿A cuántos bytes se produjo la fragmentación?

b) ¿Qué campos de que protocolos intervienen en la fragmentación?

c) ¿Qué tamaño tiene cada paquete?

d) ¿Cuántos bytes corresponden a cada protocolo?

e) ¿Cuántos bytes corresponden a los datos transmitidos?

f) ¿Qué valor de tamaño de paquete tiene el umbral de fragmentación?

¿es constante o variable?

**4) Calcule un valor umbral de Bytes, que deben ser configurados como parámetro en la aplicación Ping, para que el datagrama IP se fragmente en 15 paquetes. Verifíquelo en la PC.**

**TIEMPO ASIGNADO**: 120 minutos