*27 de Mayo de 2024*

Redes de Teleinformática I - Práctico IX

*Nombres y foto de los integrantes:*

* Lucero Ruiz, Maximo
* Borgogno, Francisco
* Quesada, Santiago
* Cañas, Felipe



**Tema:**

* Capa 2 de modelo OSI, Ethernet, LAN, Bridges, Switches

**Objetivo de la clase:**

Comprender el protocolo Ethernet

Definir las funciones que cumplen los dispositivos con Bridges y switches en las funciones de capa II.

**Redes de Área Local. Protocolo Ethernet / IEEE 802.3**

Ahora veamos EL protocolo que mas usado en las redes de Area Local, Ethernet / 802.3

1. **¿Qué características tiene una red LAN? ¿Qué diferencias tiene con una red WAN?**

* Realice un cuadro comparativo con al menos 4 diferencias entre ambas

| **Características** | **LAN (Local Area Network)** | **WAN (Wide Area Network)** |
| --- | --- | --- |
| **Alcance Geográfico** | Limitada a un área pequeña (edificio, oficina, campus) | Amplia, abarca grandes áreas geográficas (ciudades, países, continentes) |
| **Velocidad** | 100 Mbps a 400 Gbps | Terabps |
| **Tecnología** | eth, wifi, fo | fo, sat, radioenlaces |
| **Conexión** | com, print, serv | router, switch, modem, LANs |
| **Latencia** | Baja debido a la proximidad de los dispositivos | Alta debido a la larga distancia entre los dispositivos |
| **Costo** | Relativamente bajo | Relativamente alto |
| **Latencia** | 2-10 mseg | 15-200 mseg |

**¿Cuál es el formato de una trama ethernet?**

* Explique la función que cumple cada uno de los campos que posee una Trama Ethernet 802.3

| **Campo** | **Longitud (bytes)** | **Descripción** |
| --- | --- | --- |
| **Preamble (Preámbulo)** | 7 | Serie de bits alternantes que permite a los dispositivos de red sincronizarse. |
| **Start Frame Delimiter (SFD)** | 1 | Indica el comienzo de la trama de datos. El valor es 10101011. |
| **Destination MAC Address** | 6 | Dirección MAC del dispositivo de destino. |
| **Source MAC Address** | 6 | Dirección MAC del dispositivo de origen. |
| **EtherType / Length** | 2 | Tipo de protocolo o longitud de datos |
| **Payload (Datos)** | 46 a 1518 | Datos a ser transmitidos |
| **Frame Check Sequence (FCS)** | 4 | Secuencia de verificación para detección de errores (CRC) |

1. **¿Qué velocidades tenemos en una red LAN?**

En una red LAN (Local Area Network), las velocidades pueden variar ampliamente dependiendo del tipo de tecnología y equipo utilizado. A continuación se enumeran las velocidades más comunes en las redes LAN:

* Ethernet (10 Mbps): Una de las primeras formas de Ethernet, ahora casi obsoleta, ofrece velocidades de hasta 10 megabits por segundo (Mbps).
* Fast Ethernet (100 Mbps): Una versión más rápida de Ethernet que ofrece velocidades de hasta 100 Mbps. Fue muy popular en los años 90 y principios de los 2000.
* Gigabit Ethernet (1 Gbps): Este es actualmente el estándar más común en muchas redes LAN modernas, ofreciendo velocidades de hasta 1 gigabit por segundo (Gbps).
* 10 Gigabit Ethernet (10 Gbps): Utilizada principalmente en entornos empresariales y centros de datos, esta tecnología ofrece velocidades de hasta 10 Gbps.
* 25 Gigabit Ethernet (25 Gbps): Más reciente que 10 Gbps, es utilizada en centros de datos y aplicaciones de alta demanda.
* 40 Gigabit Ethernet (40 Gbps): Utilizada en entornos donde se necesita una gran capacidad de transferencia de datos, como centros de datos y redes backbone.
* 100 Gigabit Ethernet (100 Gbps): Empleada en infraestructuras de red de alta capacidad y centros de datos, proporciona velocidades de hasta 100 Gbps.
* 2.5 Gigabit Ethernet (2.5 Gbps) y 5 Gigabit Ethernet (5 Gbps): Estas velocidades intermedias han sido introducidas más recientemente para ofrecer mejoras sobre Gigabit Ethernet sin necesidad de actualizar todo el cableado de la red a los estándares requeridos para 10 Gbps.

1. **¿Tiene control de flujo Ethernet?**

Sí, Ethernet tiene mecanismos de control de flujo diseñados para gestionar el tráfico y prevenir la congestión en la red. Los mecanismos más comunes de control de flujo en Ethernet son:

* Control de flujo 802.3x
* Control de Flujo en Full-Duplex
* Prioridades de Paquetes (QoS)
* Control de Flujo en Redes Inalámbricas

1. **Hay tres métodos de control de flujo en un medio compartido**
2. **Round Robin**

* Round Robin es un método de control de flujo que asigna el uso del canal a cada dispositivo en turnos fijos.
* Funciona en un orden cíclico, donde cada dispositivo tiene una cantidad de tiempo predefinida para transmitir datos antes de pasar el control al siguiente dispositivo en la cola.
* Este método es justo, ya que cada dispositivo tiene igual oportunidad de acceso al canal.
* Simple y fácil de implementar.
* Garantiza un acceso equitativo al canal para todos los dispositivos.
* Puede ser ineficiente si algunos dispositivos no tienen datos para enviar durante su turno.
* El tiempo de espera puede ser alto si hay muchos dispositivos en la red.

1. **Reservation**

* En el método de Reservation, los dispositivos reservan el canal antes de transmitir datos.
* Esto puede hacerse mediante una señal previa o una fase de reserva en la que los dispositivos indican su intención de usar el canal.
* Una vez que un dispositivo ha reservado el canal, tiene el derecho exclusivo de transmitir durante el tiempo reservado.
* Reduce las colisiones y asegura que los dispositivos con datos para transmitir puedan hacerlo de manera ordenada.
* Puede ser eficiente en redes con alta carga de tráfico y dispositivos que necesitan transmitir grandes cantidades de datos.
* Puede requerir una fase de reserva adicional, lo que añade un pequeño overhead.
* Los dispositivos deben esperar su turno de reserva, lo que puede introducir latencia.

1. **Contention**

* En el método de Contention, los dispositivos compiten por el uso del canal.
* Los dispositivos intentan transmitir cuando el canal está libre, pero pueden ocurrir colisiones si dos o más dispositivos transmiten simultáneamente.
* Protocolos como CSMA/CD (Carrier Sense Multiple Access with Collision Detection) son ejemplos de métodos de contention.
* No requiere una fase de reserva previa, permitiendo un acceso más dinámico.
* Puede ser más eficiente en redes con baja carga de tráfico y pocos dispositivos.
* Las colisiones pueden llevar a retransmisiones, reduciendo la eficiencia del canal.
* El rendimiento puede degradarse significativamente a medida que aumenta el número de dispositivos o la carga de tráfico.

1. Ethernet, ¿Usa control de errores? ¿En qué caso retransmite la trama?

Ethernet utiliza mecanismos de detección de errores pero no incluye control de errores en el sentido de retransmisión de tramas a nivel de enlace de datos. La detección de errores en Ethernet se realiza mediante el uso de un campo llamado FCS (Frame Check Sequence).

Detección de Errores en Ethernet

Frame Check Sequence (FCS): Cada trama Ethernet incluye un campo FCS, que contiene un valor de CRC (Cyclic Redundancy Check) calculado a partir del contenido de la trama. Cuando una trama llega a su destino, el dispositivo receptor recalcula el CRC y lo compara con el valor recibido en el FCS. Si los valores no coinciden, se detecta un error en la trama.

Retransmisión de Tramas

Aunque Ethernet no retransmite tramas a nivel de enlace de datos, existen mecanismos a niveles superiores que se encargan de la retransmisión cuando se detectan errores:

* Nivel de Enlace (MAC Layer): En redes Ethernet, si una trama está dañada (detectada por una discrepancia en el FCS), simplemente se descarta y no se retransmite automáticamente en esta capa. La corrección de errores y la retransmisión se delegan a niveles superiores del modelo OSI.
* Nivel de Red y Transporte (IP y TCP):
  + IP (Internet Protocol): El protocolo IP también puede detectar errores mediante un checksum en el encabezado, pero no realiza retransmisiones.
  + TCP (Transmission Control Protocol): TCP, que opera en el nivel de transporte, es responsable de la retransmisión de datos perdidos o dañados. Si TCP no recibe un acuse de recibo (ACK) para un segmento de datos dentro de un tiempo específico, asume que el segmento se ha perdido y lo retransmite. TCP también usa números de secuencia y verificaciones de integridad para asegurar que los datos se entregan correctamente.

1. ¿A qué se llama Colisión?

Se refiere a un evento en el que dos o más dispositivos intentan transmitir datos simultáneamente en el mismo segmento de red. Esto ocurre porque ambos dispositivos están compartiendo el mismo medio de transmisión y no tienen conocimiento de que otro dispositivo está enviando datos al mismo tiempo.

1. ¿Qué tipo de direcciones tiene la trama Ethernet y quien las asigna?

Las tramas Ethernet utilizan direcciones MAC (Media Access Control) para identificar de manera única los dispositivos en la red. Existen distintos tipos de direcciones:

**Dirección MAC Unicast:**

* **Descripción:** Identifica de manera única a una sola interfaz de red o dispositivo en la red. Es la dirección utilizada en la mayoría de las comunicaciones de red, donde los datos se envían de un dispositivo específico a otro.
* **Formato:** Compuesto por 48 bits (6 bytes) escritos en formato hexadecimal, como 00:1A:2B:3C:4D:5E.
* **Ejemplo:** Una impresora o un ordenador tiene una dirección MAC unicast única.

**Dirección MAC Multicast:**

* **Descripción: I**dentifica a un grupo de dispositivos en la red. Los datos enviados a una dirección MAC multicast son recibidos por todos los dispositivos que forman parte del grupo multicast.
* **Formato:** También compuesto por 48 bits, pero el primer octeto tiene su bit más significativo (el bit de más a la izquierda) establecido en 1, indicando que es una dirección multicast. Por ejemplo, 01:00:5E:xx:xx:xx.
* **Ejemplo:** Envío de video streaming a múltiples dispositivos en una red.

**Dirección MAC Broadcast:**

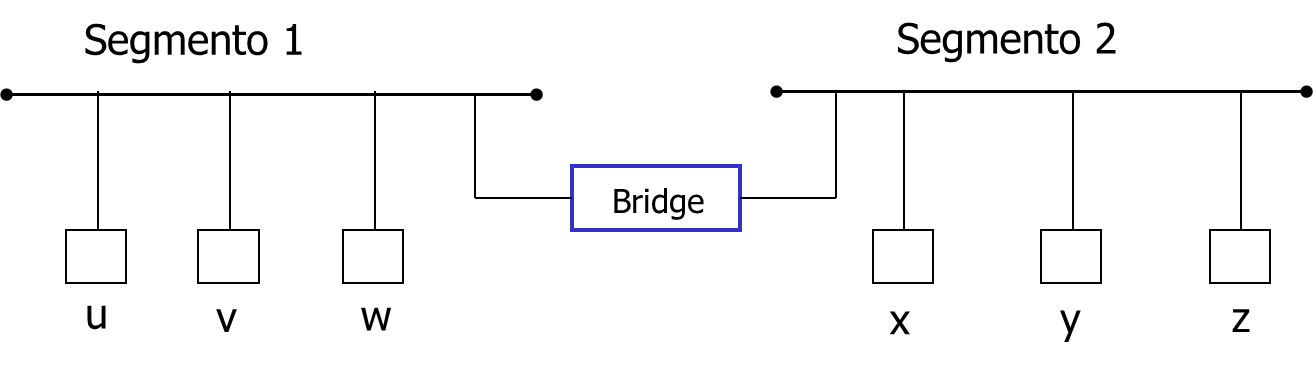
* **Descripción:** Una dirección especial que representa a todos los dispositivos en la red. Los datos enviados a la dirección broadcast son recibidos por todos los dispositivos en la misma red de área local (LAN).
* **Formato:** Es una dirección de 48 bits donde todos los bits están en 1, es decir, FF:FF:FF:FF:FF:FF.
* **Ejemplo:** Un mensaje ARP (Address Resolution Protocol) para descubrir la dirección MAC de un dispositivo en la red.

Las direcciones MAC pueden ser asignadas por el fabricante del hardware de red o de manera dinámica mediante software.

1. ¿Qué es un Repetidor? ¿A que nivel del OSI Trabaja?

Un repetidor es un dispositivo de red que se utiliza para regenerar y retransmitir señales a lo largo de un medio de comunicación. Su función principal es amplificar la señal para extender la distancia que puede recorrer sin degradarse. Trabaja en el nivel 1 (Capa Física) del modelo OSI.

1. ¿Qué es un Bridge?¿A que nivel trabaja del modelo OSI?



Es un dispositivo que vincula dos segmentos de red LAN y habla a nivel 2 del modelo OSI es decir reconociendo el MAC address de la trama. Evito con esto que se reproduzca el dominio de colisión, por segmentación a nivel físico.

Arma una tabla como sigue:

Si u transmite a v el bridge sabe que v está a la izquierda y no la envía al Segmento 2.

“Forwardean” tramas multicast y broadcast.

**¿Cómo aprenden?**

Examina la dirección origen de las tramas que recibe.

Incorpora esa dirección en su tabla según la interfaz de dónde provino.

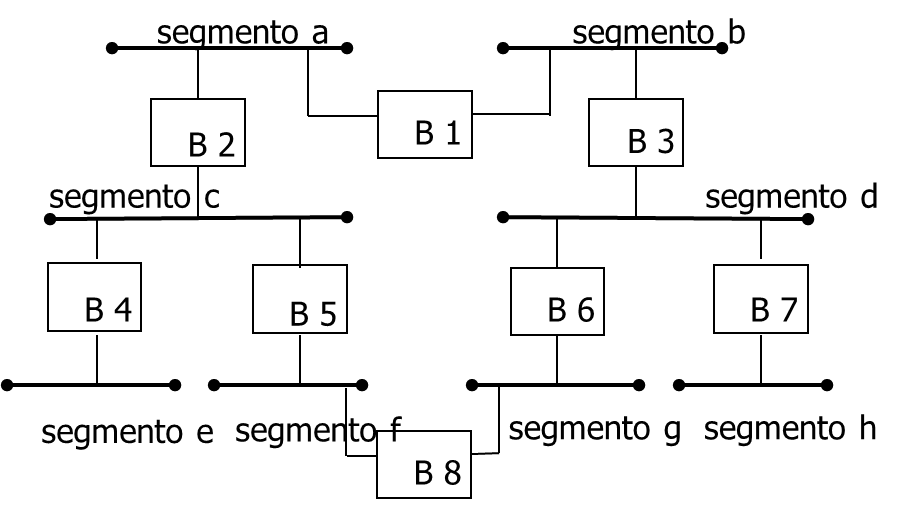
Veamos un ejemplo:

| Evento | Lado izquierdo (segmento 1) | Lado derecho (segmento 2) |
| --- | --- | --- |
| Inicio del Bridge | -- | -- |
| u transmite a v | u | -- |
| v transmite a u | u, v | -- |
| z transmite un broadcast | u, v | z |
| y transmite a v | u, v | z, y |
| y transmite a x | u, v | z, y |
| x transmite a w | u, v | z, y, x |
| w transmite a z | u, v, w | z, y, x |

¿Qué protocolo se utiliza para resolver los bucles que se pueden generar al unir varios bridges o switches que permiten tener más de un camino para vincular dos equipos?

El protocolo utilizado para resolver los bucles que se pueden generar al unir varios bridges o switches, permitiendo tener más de un camino para vincular dos equipos, es el **Spanning Tree Protocol (STP)**.

Veamos un ejemplo:



* En este caso cuando una estación del segmento c quiera enviarle una trama a una del segmento g habrá múltiples caminos, B2, B1, B3 y B6 por un lado y B5, B8 por el otro.
* La estación destino recibirá dos tramas idénticas y por la estructura de la trama sabemos que no puede distinguirlas como tales.
* El problema se resuelve eliminando los caminos múltiples. Típicamente se reduce el grafo de la red a un árbol.
* Justamente el algoritmo más utilizado y que es adoptado para los bridges estándares es el de “spanning tree”.
* Si bien en la actualidad los bridges son poco utilizados es importante notar que los switches de LAN presentan características similares, inclusive la interconexión de switches se resuelve con “spanning tree”.

1. ¿Qué es un Switch y para que sirve?

Un switch es un dispositivo de red que conecta múltiples dispositivos en una red local (LAN) y utiliza la dirección MAC para enviar y recibir datos de manera eficiente.

1. Busque en páginas de fabricantes de Switches algún modelo que posea al menos 24 puertos Giga Ethernet.

Tp-Link TL-SG1024 V1.1



**Redes Wireless LAN**

Para investigar:

Complete estas respuestas, como guía de temas puede acceder al link que se encuentra debajo, el cual permite el acceso al libro Servicios en Red, capítulo 9

<https://elibro.net/es/ereader/bibliotecas-ucc/43261?page=235>

Servicios en red

Información Bibliográfica

AUTOR:

Román Carceller Cheza

PRINT ISBN:

9788415656630

E - ISBN:

9788415991427

EDITORIAL:

Macmillan Iberia, S.A.

* [Unidad 9. Despliegue de redes inalámbricas](https://elibro.net/es/ereader/bibliotecas-ucc/43261?page=235)
  + [1 >> Redes inalámbricas WLAN](https://elibro.net/es/ereader/bibliotecas-ucc/43261?page=236)
  + [2 >> Acceso a redes inalámbricas en sistemas GNU/Linux](https://elibro.net/es/ereader/bibliotecas-ucc/43261?page=245)
  + [3 >> Acceso a redes inalámbricas en sistemas Windows](https://elibro.net/es/ereader/bibliotecas-ucc/43261?page=246)

1. ¿Que son las redes Wireless LAN?

Las redes Wireless LAN son redes que permiten la comunicación y el intercambio de datos entre dispositivos utilizando ondas de radio en lugar de cables físicos.

1. ¿Quién creo la Certificación WiFi, basada en el estándar 802.11?

La Wi-Fi Alliance es la organización responsable de la creación y gestión de la certificación Wi-Fi, basada en el estándar IEEE 802.11. La Wi-Fi Alliance es una organización mundial de la industria sin fines de lucro que promueve la adopción y evolución de las tecnologías Wi-Fi.

1. ¿Cuáles son los estándares WLAN más usados?

| **Estándar** | **Año** | **Frecuencia** | **Velocidad máxima** | **Alcance en interior** | **Alcance en exterior** |
| --- | --- | --- | --- | --- | --- |
| 802.11 legacy | 1997 | 2.4 GHz | 2 Mbps | 20 mts | 100 mts |
| 802.11a | 1999 | 5.7 GHz | 54 Mbps | 35 mts | 120 mts |
| 802.11b | 1999 | 2.4 GHz | 11 Mbps | 38 mts | 140 mts |
| 802.11g | 2003 | 2.4 GHz | 54 Mbps | 38 mts | 140 mts |
| 802.11n | 2009 | 2.4 y 5.7 GHz | > 300 Mbps | 70 mts | 250 mts |

1. ¿Cuáles son los componentes WLAN?

Los componentes WLAN se pueden dividir en tres grupos:

* Distribución: puntos de acceso y equipos mixtos
* Adaptadores de red inalámbrica o tarjetas de red: WNIC
* Antenas

1. ¿Describa los AP y los WNIC?

* **Access Points (AP):** Un punto de acceso (AP) es un dispositivo que puede actuar como punto central de una red inalámbrica independiente (figura 9.1). Tiene una dirección IP que permite configurarlo y su función principal es proveer a los clientes de acceso a la red inalámbrica. Las funciones de enrutamiento y direccionamiento las suele delegar en servidores (routers).
* **Wireless Network Interface Cards (WNIC):** Estos adaptadores, dependiendo de su punto de interconexión con el dispositivo, pueden dividirse en los siguiente:
  + Adaptadores integrados: van incluidos en la placa del dispositivo. Los ordenadores portátiles, las tablets, las consolas y los smartphones suelen ir equipados con un adaptador integrado.
  + Tarjetas PCMCIA: permiten a los ordenadores portátiles que no posean un adaptador integrado disponer de una interfaz Wi-Fi mediante la conexión de una tarjeta externa a una puerto PCMCIA libre del ordenador.
  + Tarjetas PCI: se conectan a un puerto PCI libre de un ordenador personal. Poseen una antena externa que puede ser sustituida por una de mayor potencia.
  + Adaptadores USB: son dispositivos inalámbricos externos al ordenador que se conecta a un puerto USB libre. Su instalación es muy sencilla ya que el puerto USB es Plug&Play y, por lo tanto, el ordenador normalmente lo detecta de manera automática. También pueden cam- biarse de equipo de forma rápida para adecuar las necesidades inalám- bricas de la red.

1. ¿Las antenas se pueden clasificar según sus tipos de radiación, cuáles son?

* **Isotrópica:** es una antena teórica que emite la misma potencia de radiación en todas las direcciones. Su diagrama de radiación es una esfera perfecta.
* **Omnidireccional:** es una antena que radia la misma cantidad de potencia en todas las direcciones de un plano de emisión. Su diagrama de radiación sería un toroide. Son las más utilizadas en las redes WLAN, ya que cubren de manera uniforme toda la superficie en la que se debe dar servicio inalámbrico.
* **Direccional:** es una antena que emite la máxima potencia en una dirección determinada. Suelen utilizarse para crear uniones punto a punto o conectar zonas muy alejadas. Se subdividen en: – Unidireccionales: emiten la potencia en un solo sentido. – Bidireccionales: reparten la potencia en los dos sentidos de la dirección.
* **Sectorial:** es una antena que emite su máxima potencia en un sector determinado. Suelen utilizarse en redes urbanas. Pueden cubrir sectores de 120°, 60°, etc..

1. ¿Qué otras características poseen las antenas?

* **Ganancia:** es el incremento de potencia de una antena en la dirección de máxima radiación en relación con una antena modelo. Puede medirse en dBi (decibelios respecto a una antena isotrópica) o dBd (decibelios respecto a un dipolo), dependiendo de la antena usada como referencia. Un dipolo posee un diagrama de radiación omnidireccional. Si el resultado es positivo, indica mayor potencia de radiación que el modelo; si, por el contrario, el resultado es negativo, indica menor potencia de radiación.
* **Ancho de banda:** son las bandas de frecuencia en las cuales trabaja la antena de manera óptima.
* **Eficiencia:** es la relación entre la potencia emitida por la antena y la que le es suministrada por el equipo transmisor. Cuanto mayor sea la eficiencia menor será la cantidad de potencia que se perderá en forma de calor.

1. ¿Qué modos de operación poseen los WLAN?

* **Redes ad hoc:** es una red inalámbrica descentralizada. En ella todos los equipos están conectados sin necesidad de un nodo central que realice las funciones de router. Este tipo de redes no necesita ni puntos de acceso ni dispositivos mixtos; cada equipo actúa como punto de acceso y cliente inalámbrico.
* **Redes en infraestructura:** estas redes son aquellas en las cuales los dispositivos se conectan a la red mediante puntos de acceso. Añadiendo AP adicionales se aumentará el alcance de la red y el número de usuarios. Frente a las redes ad hoc, ofrecen una mejor escalabilidad, así como un sistema de seguridad centralizado.

1. Sobre la seguridad de WLAN, defina tipos de autenticación y tipos de cifrado.

* **Tipos de autenticación:**
  + Sistema abierto u Open System: permite el acceso de todos los usuarios a la red inalámbrica, ya que no se comprueba su identidad.
  + Clave compartida o PSK (Preshared Key): en este sistema solo los usuarios que conozcan una clave previamente introducida en el punto de acceso podrán ser autorizados.
  + EAP (Extensible Authentication Protocol) o protocolo ampliable de autentificación: permite la autenticación en los sistemas basados en el estándar IEEE 802.1X. Este último posibilita que todos los usuarios tengan claves de autenticación diferentes. IEEE 802.1X utiliza una estructura cliente-servidor y dispone de tres dispositivos básicos:
    - Suplicantes: dispositivos que desean acceder a la red.
    - Servidores de autenticación: dispositivos que guardarán las credenciales de los equipos que desean acceder a la red.
    - Autenticadores: equipos a los que se conectan los clientes para autenticarse; normalmente se trata de un AP. Actúan como puente entre el servidor y el cliente.
  + Filtros MAC: los puntos de acceso permiten crear una lista de direcciones MAC para permitir o denegar el acceso a determinados dispositivos. Una vez que se ha realizado una primera autenticación, el AP busca la dirección MAC del dispositivo y confirma o deniega el acceso dependiendo del resultado.
* **Tipos de cifrado**:
  + Claves estáticas: las claves simétricas y estáticas son aquellas que no cambian de manera automática, lo que les hace más vulnerables a posibles ataques.
  + Claves dinámicas: las claves simétricas y dinámicas son aquellas que van cambiando automáticamente. Así, el tiempo que la clave permanece activa es menor que el tiempo necesario para descifrarla:
    - TKIP (Temporal Key Integrity Protocol) o protocolo de integridad temporal de clave: es un sistema de claves dinámico. Utiliza una clave temporal de 128 bits, la dirección MAC del cliente y un vector de 16 octetos para generar la clave de autenticación.
    - AES (Advanced Encryption Standard) o estándar avanzado de encriptación: es un sistema de claves dinámico basado en el cifrado por bloques. Adaptado por el gobierno de los Estados Unidos, presenta una mayor resistencia a los ataques.

1. Sobre los ataques a la redes de WLAN, describa cada tipo de ataque.

* **Ataque de diccionario:** consiste en intentar averiguar una contraseña probando todas las palabras de una lista, como puede ser un diccionario. Conociendo alguno de los parámetros que intervienen en la generación de la clave se reduce el tiempo de proceso. Por ejemplo, en el sistema de cifrado AES sobre redes inalámbricas, se incorpora la SSID para generar la contraseña. Si se hace visible el nombre del punto de acceso se estarán facilitando los ataques por diccionario. Si se oculta el nombre del AP, sólo podrán acceder a la red aquellos usuarios que lo conozcan por adelantado, aunque existen programas que permiten averiguarlo.
* **Ataque de fuerza bruta:** consiste en probar todas las combinaciones posibles hasta encontrar la que permite el acceso. Es menos eficiente que el ataque por diccionario. Para provocar que sea tan costoso en tiempo que no merezca la pena intentarlo, se deberá aumentar la fortaleza de la contraseña. Utilizaremos para ello el máximo número de caracteres permitidos por el sistema de acceso para la contraseña, así como los diferentes tipos de caracteres posibles: mayúsculas, minúsculas, números y símbolos. También es recomendable que los caracteres se dispongan aleatoriamente sin formar palabras reales.

**Práctico:**

**Objetivo**: Identificar la estructura que tienen los paquetes en una red de datos.

Inicialmente vamos a instalar el programa Wireshark en nuestras computadoras.

<https://www.wireshark.org/>

Luego vamos a buscar tutoriales para comprender su funcionamiento básico.

Wireshark es un programa que permite observar todo el tráfico que circula por una red a la que se encuentre conectada la pc que lo está ejecutando.

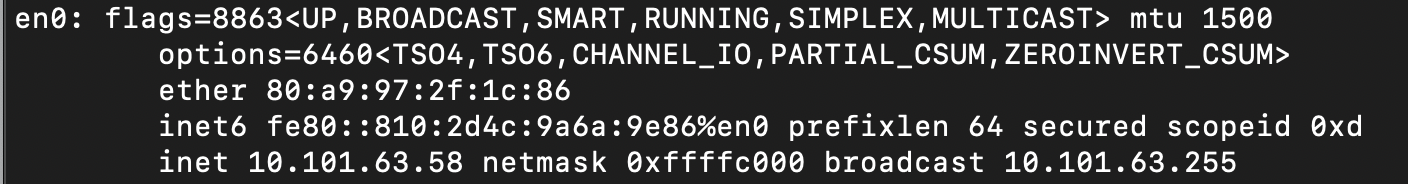
Aprovechando esta herramienta vamos a realizar dos actividades:

**Actividad 1:**

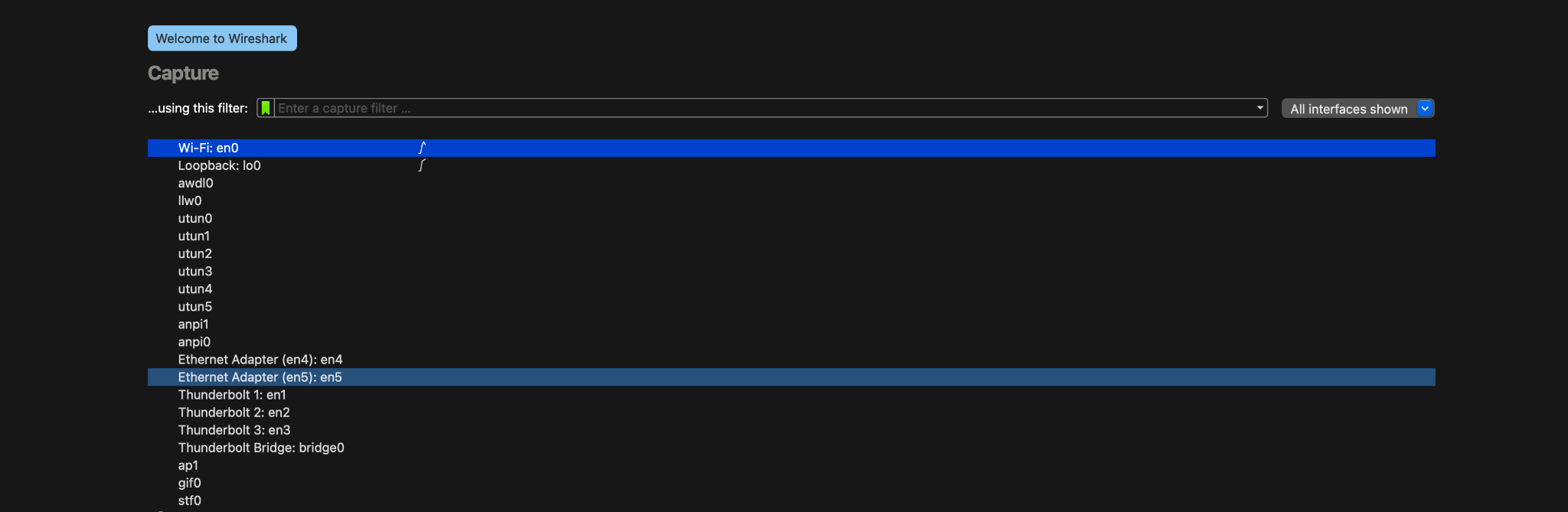
* Identificar la dirección de IP de su PC. Puede usar el comando ipconfig/all que se puede ejecutar desde el programa cmd que viene en Windows.



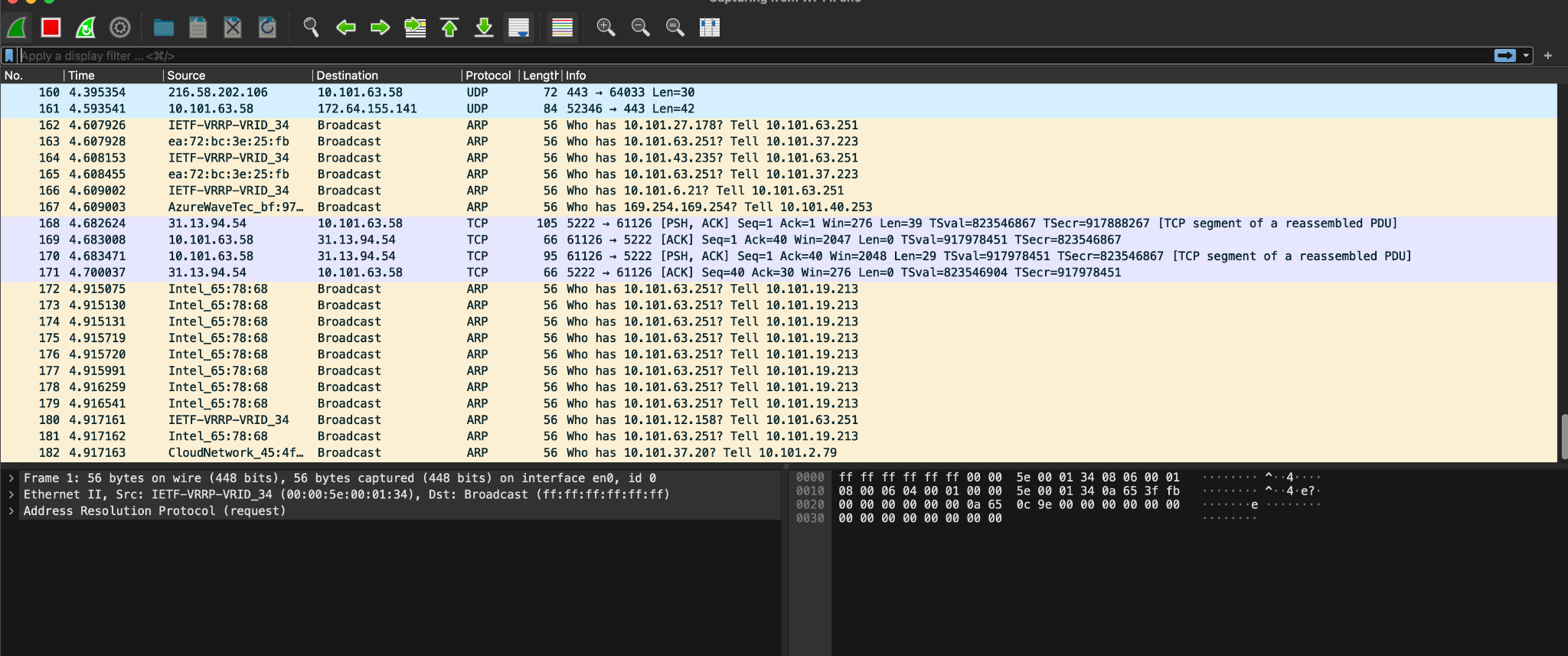
* Conectar otra PC mas a la red y chequear que IP posee usando el comando IPconfig /all desde la misma pc.



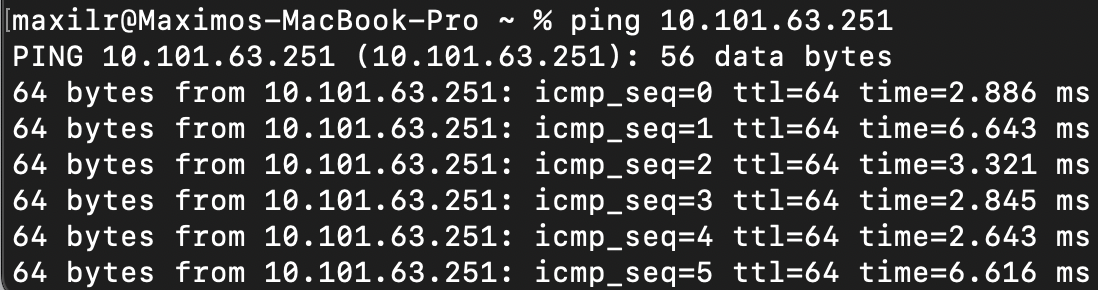
* Ejecutar en programa Wireshark en nuestra PC



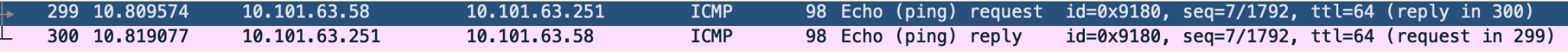
* Elegir una interfaz que se encuentre conectada a nuestro modem/Router que nos provee la conexión de Internet (generalmente es la interfaz de WiFi salvo que usted tenga un cable UTP entre su PC y el modem/router)



* Activar el monitoreo del tráfico
* Realizar el comando PING entre su PC y la otra.

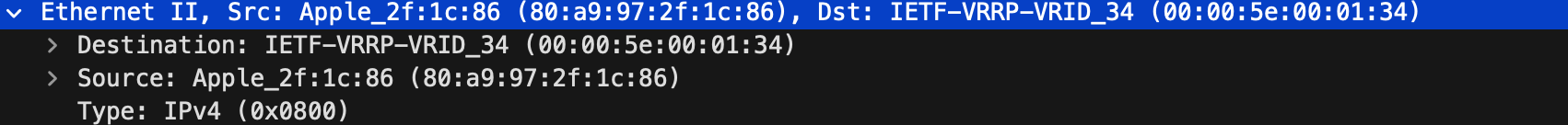


* Detener el monitoreo del WShark.
* Buscar en los paquetes capturados cual es el protocolo que utiliza el comando PING.

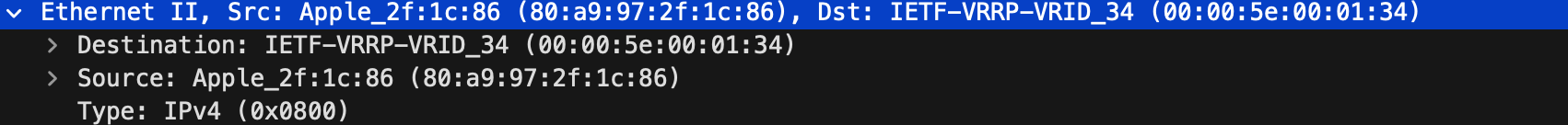


Protocolo: *ICMP*

* Identificar cual es la MAC address de origen que lleva la trama Ethernet que contiene a este paquete.



* Identificar también la MAC address de destino de la trama Ethernet



* ¿A qué computadores pertenecen estas MAC address?

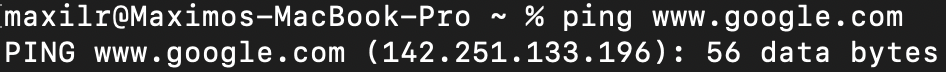
*A la mía y al Gateway.*

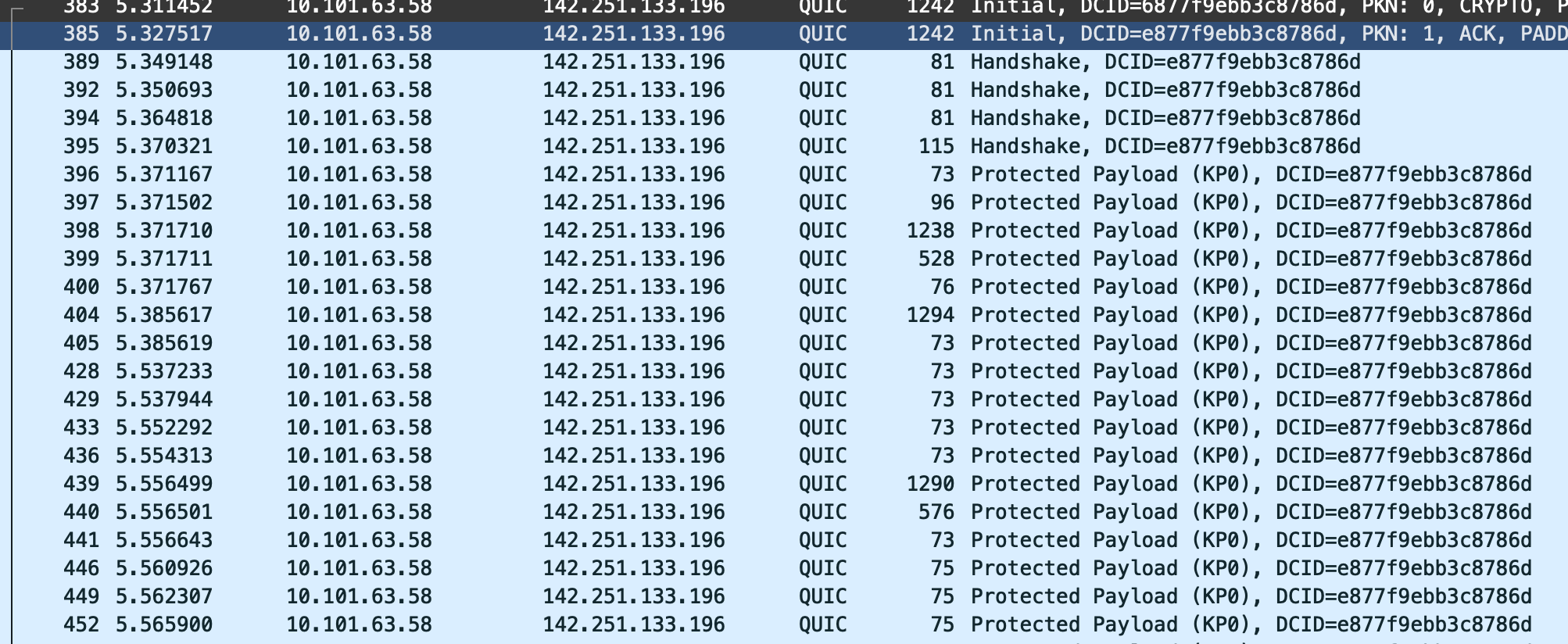
* ¿Por qué cree que la trama posee esas direcciones MAC?

*Porque el dispositivo siempre tiene que salir al gateway antes de vincularse con cualquier otro dispositivo, ya sea dentro de la misma red local o de la red pública.*

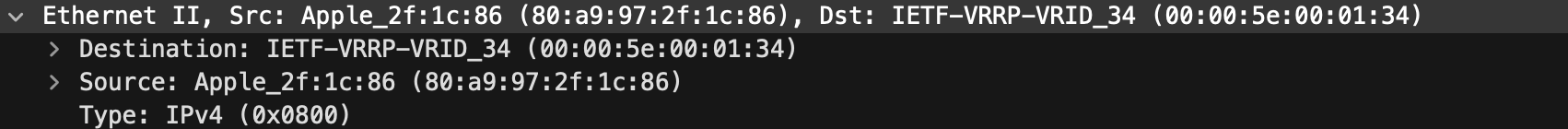
**Actividad 2:**

* Reiniciar nuevamente el monitoreo del WShrak.
* Realizar una búsqueda en el browser de internet de su máquina a cualquier sitio de Internet, por ejemplo [www.google.com](http://www.google.com).
* Detener el monitoreo.
* Identificar el protocolo de IP que se utiliza para encontrar la IP address que pertenece al nombre del dominio de [www.google.com](http://www.google.com).





* Encontrar la MAC address de origen y la MAC address de destino que contienen los paquetes que viajar a Internet con destino a [www.google.com](http://www.google.com)



* ¿A que dispositivo pertenece la MAC address de Origen y la Mac address de destino de esa trama Ethernet?

*Una es la computadora o dispositivo que busca o navega utilizando ese dominio y la otra es la MAC Address del Gateway de la red local.*

* ¿Por qué cree que esa trama tiene esas direcciones MAC?

*Porque llega por saltos al destino, no es directo, y lo más inmediato a mi computadora para salir a la red externa es el Gateway de la red local.*