Material del profesor - Teoría introductoria

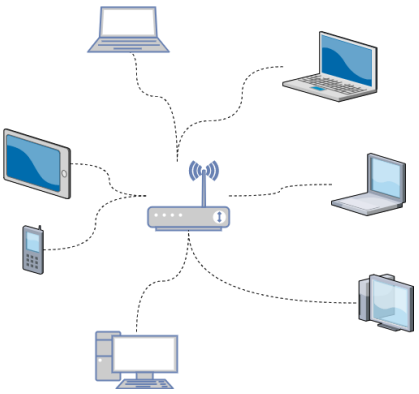
Palabras clave

Wireless, Wi-fi, protocolo 802.11, TCP, HTTP, WebSocket, Wireshark, modelo OSI, modelo TCP/IP.

Redes Wireless

Las redes wireless no necesitan estar cableadas para poder comunicarse entre ellas, la información se transmite de forma inalámbrica como ondas electromagnéticas a través del espacio. Para esto, se utilizan diversos dispositivos que utilizan tecnologías de radiación electromagnética, tales como infrarrojos o radiofrecuencias, basadas en estándares definidos en distintos protocolos.
Dentro de las más reconocidas y que utilizamos todos los días se encuentran el Bluetooth, Wi-Fi, 3G, 4G, Li-Fi, entre otros.

Wi-Fi (protocolo IEEE 802.11)



Lo que conocemos como Wi-Fi es un tipo de red inalámbrica que se basa en el protocolo IEEE 802.11.
La estructura que cumple es uno o varios dispositivos conectados de manera inalámbrica a un router.
Generalmente se ven como en el diagrama, aunque también se puede tener otros dispositivos que intervengan, como, por ejemplo, repetidores.
La comunicación se realiza a través de diferentes canales de radiofrecuencias, los definidos por el estándar usan las frecuencias que rondan entre los 2.4GHz y 5.0GHz.
Entre aquellos en la banda de 2.4GHz se separan en canales conocidos con números del 1 al 11 (aunque los más utilizados son el 1, 6 y 11 debido a interferencias entre los mismos[1]) mientras que en la banda de los 5GHz se separan en 28 canales, también numerados, que van del 34 al 165 como se muestra en los siguientes gráficos.

Canales en espectro/banda 2.4GHz											
Número	1	2	3	4	5	6	7	8	9	10	11
GHz	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462

[1] Sitio de Xataka:
https://www.xataka.com/servicios/que-existen-distintos-canales-wifi-como-podemos-configurarlos-para-evitar-interferencias

Canales en espectro/banda 5GHz												
Número	34	36	38	40	42	44	46	48	52	56	60	60
GHz	5.170	5.180	5.190	5.200	5.210	5.220	5.230	5.240	5.260	5.280	5.300	5.300
Número	100	104	108	112	116	120	124	128	132	136	140	
GHz	5.500	5.520	5.540	5.560	5.580	5.600	5.620	5.640	5.660	5.680	5.700	
Número	149	153	157	161	165							
GHz	5.745	5.765	5.785	5.805	5.825							

Modelo TCP/IP y Modelo OSI

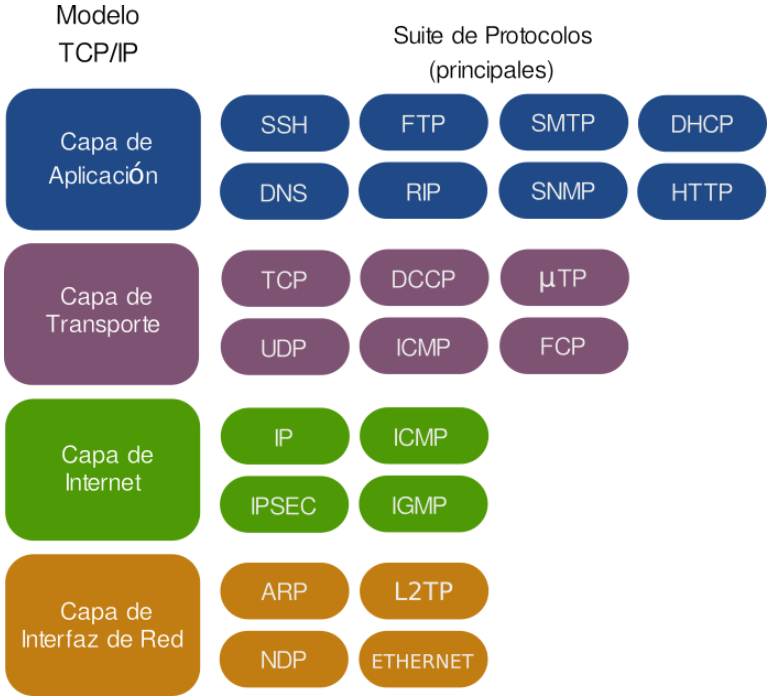


Imagen modelo OSI[2] ***Imagen modelo TCP/IP***[3]

El modelo OSI es un modelo de referencia para los protocolos de la red, más teórico, aunque hay implementaciones del mismo. Está conformado por 7 (siete) capas o niveles de abstracción. Cada capa define uno o diversos protocolos que deben implementarse en cada extremo de la conexión de red.
De nuestra parte nos centraremos en el modelo TCP/IP dado que simplifica las capas OSI, y que es el que se convirtió en estándar.

---

[2] Fuente: https://es.wikipedia.org/wiki/Archivo:Pila-osi-es.svg
[3] Fuente: https://es.wikipedia.org/wiki/Familia_de_protocolos_de_internet#/media/Archivo:Suite_de_Protocolos_TCPIP.png

Descripción de las capas del modelo TCP/IP.

Capa de Interfaz de Red

También conocida como capa de enlace o capa de acceso, o capa de acceso a la red, se encarga de las conexiones de la computadora a la red, las principales funciones son transmitir el flujo de bits, manejar señales eléctricas y garantizar la conexión (no la fiabilidad). Ejemplos de algunos protocolos son: Ethernet, Wi-Fi y ARP.

Capa de Internet

Se encarga de seleccionar la mejor ruta para enviar paquetes a través de la red; es responsable de proporcionar el paquete de datos. Y se comunica a través de direcciones IP: Una dirección ip es una etiqueta numérica, por ejemplo "192.0.10.1" que identifica, de manera lógica y jerárquica, a una interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el Protocolo de Internet o que corresponde al nivel de red del modelo TCP/IP.

Las direcciones ip se dividen en clases:

Descripción	Rango
Rango de clase A:	1.0.0.0 – 126.255.255.255
Rango de clase B:	128.0.0.0 – 191.255.255.255
Rango de clase C:	192.0.0.0 – 223.255.255.255

Y se diferencian entre públicas y privadas de la siguiente manera.

Privadas

Son las direcciones IP que se utilizan para interconectar dispositivos en una red y necesitan de un proceso de traducción a ip pública para poder conectarse a Internet.

Descripción	Rango
Privadas de clase A:	10.0.0.0 – 10.255.255.255
Privadas de clase B:	172.16.0.0 – 172.31.255.255
Privadas de clase C:	192.168.0.0 – 192.168.255.255

Públicas

Las direcciones IP públicas se utilizan para interactuar con Internet y de esta forma un dispositivo se identifique de forma unívoca en la red.

Capa de Transporte

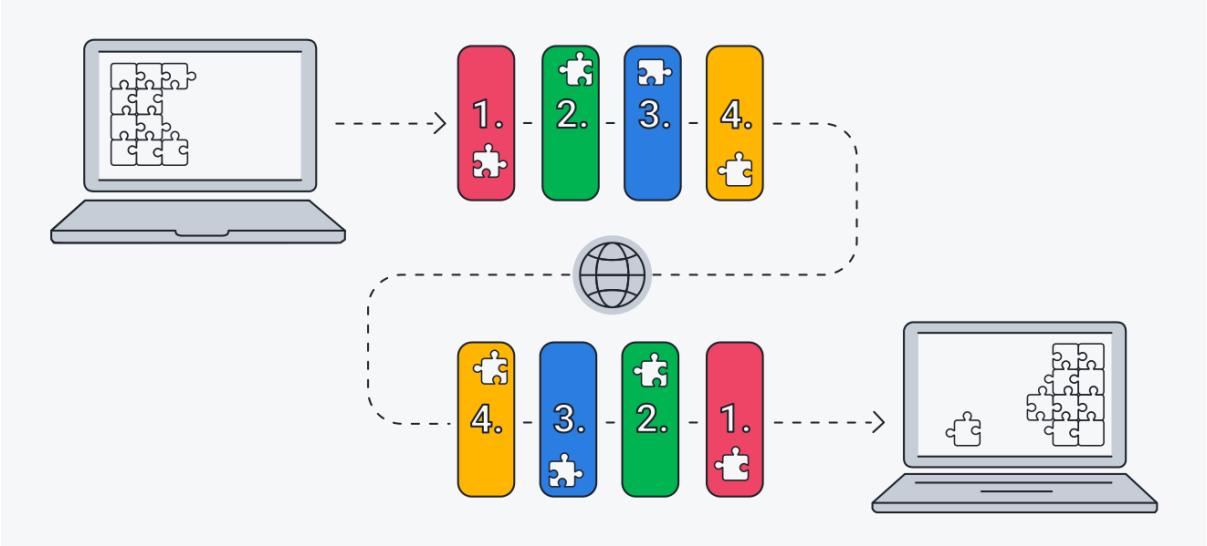
Proporciona fundamentalmente una conexión lógica entre el emisor y el receptor, segmentando y reensamblando los datos, junto con mecanismos que permiten conocer el estado de la transmisión. Ejemplos de algunos protocolos son: TCP y UDP.

Capa de aplicación

La función depende de la aplicación que se use, pero se podría resumir en proporcionar servicios para que el usuario pueda interactuar acorde con la máquina ya sea enviando correos y datos, visitando páginas web o descargando información. Ejemplos de algunos protocolos son: HTTP, DNS, SMTP y SSH.

TCP

TCP (Protocolo de Control de Transmisión, por sus siglas en inglés Transmission Control Protocol), es un protocolo de la capa de **transporte** que garantiza la entrega de datos en el mismo orden que se enviaron, haciendo del mismo un protocolo **confiable**.



Un diagrama de cómo el modelo TCP/IP divide los datos en paquetes y los envía a través de cuatro capas distintas.[4]

Lo que interesa saber sobre TCP en este escenario es que todas las comunicaciones se llevan a cabo con los protocolos WebSocket y HTTP, y dichos protocolos funcionan sobre TCP.
Por lo que siempre que trabajemos con capturas de tráfico para analizar esas comunicaciones (por ejemplo con Wireshark) nos va a aparecer TCP en algún lado, pueden encontrar más información en el sitio de Mozilla.[5]

---

[4] Fuente: https://www.avg.com/es/signal/what-is-tcp-ip
[5]Sitio de Mozilla sobre TCP: https://developer.mozilla.org/es/docs/Glossary/TCP

DNS

DNS (Domain Name Service) es un protocolo de la capa de aplicación que tiene la funcionalidad de recibir un nombre de dominio (como podría ser unlp.edu.ar) y devolver las direcciones IP asociadas al mismo para que el navegador pueda acceder y sea transparente al usuario final.
Existen diferentes servidores DNS y el más conocido es el servicio 8.8.8.8 de Google.

HTTP

HTTP (Protocolo de Transferencia de Hypertexto o Hypertext Transfer Protocol en inglés) es un protocolo de la capa de **aplicación** que es mayormente utilizado para el acceso a páginas web, el puerto utilizado para este protocolo es el 80.
La transferencia de información a través del protocolo se realiza sin ningún tipo de **encriptación** por lo que al capturar los paquetes correspondientes a este protocolo revela toda la información contenida.
Sigue el modelo cliente-servidor, es decir, un cliente establece una conexión y luego se comunican a través de la misma. Utiliza el protocolo TCP en la capa de **transporte** para generar esta conexión y realizar toda la comunicación.
Existe un protocolo llamado HTTPS (HTTP Secure o HTTP Seguro) que realiza distintas encriptaciones a los paquetes para que la comunicación sea segura, el puerto utilizado para este protocolo es el 443.
HTTPS utiliza TLS (Transport Layer Security) en alguna de sus versiones para manejar la encriptación y el envío de los paquetes. Pueden encontrar más información en el sitio de Mozilla[6].

WebSocket

WebSocket (WS) es, al igual que HTTP, un protocolo de la capa de aplicación que utiliza el protocolo TCP en la capa de **enlace** y no encripta su información. Es generalmente utilizado en dispositivos **IOT** dado que sirve para conectar el navegador de un usuario a un dispositivo, también existe un WebSocket Secure (WSS) pero dado que los dispositivos que implementan WS suelen tener memoria o capacidad de cómputo limitada no puede siempre implementarse. Pueden encontrar más información en el sitio de Mozilla[7].

Wireshark

Wireshark[8] es una herramienta que nos permite tanto realizar como visualizar capturas de paquetes de red en una interfaz gráfica.
Para realizar una captura de tráfico utilizando wireshark basta con ejecutarlo con derechos de administrador y elegir una interfaz.

---

[6]Sitio de Mozilla sobre HTTP: https://developer.mozilla.org/es/docs/Web/HTTP
[7]Sitio de Mozilla sobre WebSocket: https://developer.mozilla.org/es/docs/Web/API/WebSockets_API
[8]Sitio de descarga de Wireshark: https://www.wireshark.org/#download

Una interfaz puede ser tanto física (e.g. una placa de red cableada o una placa Wi-Fi) como virtual (como generada por la herramienta Aircrack-ng o el mismo sistema operativo).
Existen varias maneras de capturar tráfico pero la que nos interesa es la que nos permite capturar, además del tráfico dirigido a nuestra interfaz, aquel tráfico que nuestra interfaz lee pero no está dirigido a la misma, a éste modo se lo conoce como “Modo Promiscuo” y la acción de capturar el tráfico en modo promiscuo se la llama “Sniffing”. En los próximos capítulos aprenderemos cómo realizar sniffing a través de Wi-Fi utilizando Wireshark y Aircrack-ng.
El análisis de una captura de tráfico también puede realizarse con Wireshark que nos facilita algunas herramientas, como filtros y desencriptación automática en ciertos protocolos.
En este video[9] se hace una explicación un poco más detallada de la herramienta y como usarla.

[9] Introducción al análisis de tráfico de red con Wireshark: https://www.youtube.com/watch?v=shp42M7gbDE

Glosario

Router: Es un dispositivo que permite interconectar redes con distinto prefijo en su dirección IP. Su función es la de establecer la mejor ruta que destinará a cada paquete de datos para llegar a la red y al dispositivo de destino. Es bastante utilizado para conectarse a Internet ya que conecta la red de nuestro hogar, oficina o cualquier red a la red de nuestro proveedor de este servicio.

Bit: Corresponde a un dígito del sistema de numeración binario y representa la unidad mínima de información.

Ethernet: Es un estándar de redes de área local para computadoras que define las características de cableado y señalización; de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

ARP: El protocolo de resolución de direcciones (ARP, del inglés Address Resolution Protocol) es un protocolo de comunicaciones de la capa de enlace de datos responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

ICMP: El protocolo de mensajes de control de Internet (en inglés: Internet Control Message Protocol y conocido por sus siglas ICMP) es parte del conjunto de protocolos IP. Es utilizado para enviar mensajes de error e información operativa indicando, por ejemplo, que un host no puede ser localizado o que un servicio que se ha solicitado no está disponible. Estos mensajes del protocolo ICMP se envían a la dirección IP de origen del paquete.

UDP: El protocolo de datagramas de usuario (en inglés: User Datagram Protocol o UDP) es un protocolo del nivel de transporte basado en la transmisión sin conexión de datagramas y representa una alternativa al protocolo TCP. Permite el envío de datagramas de forma rápida en redes IP sin establecer previamente una conexión, dado que el propio datagrama incorpora suficiente información sobre el destinatario en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción.

SMTP: Es el protocolo para transferencia simple de correo (en inglés: Simple Mail Transfer Protocol o SMTP) es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, impresoras, etc.).

SSH: Es el nombre de un protocolo cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.