**PARTE 1**

¿Qué es un protocolo **standard**?

Un protocolo estándar, en el contexto de las telecomunicaciones y la teleinformática, es un conjunto de reglas y convenciones establecidas que gobiernan la comunicación y el intercambio de datos entre dispositivos o sistemas en una red. Estos protocolos son ampliamente aceptados y adoptados por la industria y la comunidad técnica para garantizar la interoperabilidad y la comunicación eficiente entre diferentes equipos y aplicaciones.

Un protocolo estándar define cómo se deben iniciar, mantener y finalizar las comunicaciones, así como la estructura y el formato de los mensajes o datos que se intercambian. Ejemplos de protocolos estándar ampliamente utilizados incluyen el Protocolo de Transferencia de Hipertexto (HTTP) para la web, el Protocolo de Correo Electrónico (SMTP y IMAP) para el correo electrónico, el Protocolo de Control de Transmisión (TCP) para la transmisión confiable de datos en redes IP, y muchos otros.

Estos protocolos estándar son esenciales para garantizar que los dispositivos y sistemas de diferentes fabricantes puedan comunicarse de manera efectiva y que las aplicaciones desarrolladas por diferentes empresas puedan interactuar entre sí de manera coherente en una red. Además, los estándares promueven la seguridad, la calidad y la fiabilidad de las comunicaciones en un entorno tecnológico cada vez más interconectado.

¿Cuál es la diferencia entre protocolo **estándar** Vs **implementación de protocolo**?

La diferencia principal entre un protocolo estándar y la implementación de un protocolo radica en su naturaleza y función:

**Protocolo Estándar:**

\* Un protocolo estándar es una especificación general que define las reglas, el formato y los procedimientos para llevar a cabo una comunicación o intercambio de datos en una red o sistema de manera amplia y genérica.

\* Los protocolos estándar son documentos que describen cómo deben comportarse los dispositivos o sistemas para garantizar la interoperabilidad y la comunicación exitosa.

\* Estos estándares suelen ser desarrollados y mantenidos por organizaciones de normalización, como el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), la Corporación de Internet para la Asignación de Nombres y Números (ICANN), la Organización Internacional de Normalización (ISO) y otros.

\* Ejemplos de protocolos estándar incluyen TCP/IP, HTTP, SMTP y otros mencionados en la respuesta anterior.

**Implementación de Protocolo:**

\* La implementación de un protocolo se refiere a la creación de software o hardware específico que sigue las reglas y las especificaciones de un protocolo estándar particular.

\* Es la materialización práctica de un protocolo estándar en un dispositivo, una aplicación o un sistema informático específico.

\* Las implementaciones de protocolo pueden variar en calidad, eficiencia y nivel de cumplimiento con respecto a las especificaciones del estándar.

\* Los desarrolladores crean implementaciones de protocolo para que los dispositivos y sistemas puedan comunicarse y funcionar en una red de acuerdo con las normas establecidas.

**En resumen,** un protocolo estándar es una especificación generalizada que establece cómo deben funcionar las comunicaciones en una red, mientras que la implementación de un protocolo se refiere a la creación de software o hardware específico que sigue esas reglas para lograr la comunicación en la práctica. Las implementaciones pueden variar en calidad y conformidad con el estándar, pero el estándar mismo define las reglas fundamentales que todos deben seguir para garantizar la interoperabilidad.

¿Qué es una **RFC**?

RFC son las siglas de "Request for Comments" (Solicitud de Comentarios) en inglés. En el contexto de las telecomunicaciones y la informática, una RFC es un documento publicado por la Internet Engineering Task Force (IETF) y otras organizaciones relacionadas que describe estándares, protocolos, procedimientos y otros aspectos relacionados con la operación de Internet y las redes de computadoras.

Las RFC son documentos técnicos que sirven como una forma abierta y colaborativa de desarrollar, revisar y definir estándares en la comunidad de Internet. Aunque el nombre "Request for Comments" sugiere que se trata de una solicitud de comentarios, muchas RFC son en realidad estándares establecidos que han pasado por un proceso de revisión y aprobación.

Las RFC abordan una amplia variedad de temas, desde la especificación de protocolos de red, como el Protocolo de Control de Transmisión (TCP) e Internet Protocol (IP), hasta aspectos relacionados con la administración de nombres de dominio, la seguridad en Internet, la gestión de direcciones IP, entre otros.

Cada RFC se identifica con un número único y se publica de manera abierta y accesible en línea. La comunidad técnica y la industria suelen hacer referencia a las RFC como documentos de referencia autoritarios para implementar y comprender los estándares y protocolos utilizados en Internet y otras redes de computadoras.

¿Qué es un puerto **TCP**?

Un puerto TCP (Transmission Control Protocol) es un número de 16 bits que se utiliza para identificar de manera única un servicio o aplicación específica en un dispositivo o servidor en una red de computadoras. El TCP es uno de los protocolos principales de la capa de transporte en el modelo OSI (Open Systems Interconnection) y se utiliza para proporcionar una comunicación confiable y orientada a la conexión entre dos dispositivos en una red.

Cada dispositivo o servidor que utiliza TCP para ofrecer servicios, como servidores web, servidores de correo electrónico, servidores FTP (File Transfer Protocol), entre otros, tiene asignados uno o varios puertos TCP para gestionar diferentes tipos de solicitudes de comunicación. Los puertos TCP van desde el número 0 hasta el 65535.

La asignación de un puerto TCP permite que múltiples servicios y aplicaciones se ejecuten en el mismo dispositivo o servidor sin conflictos, ya que cada solicitud entrante a través de la red incluye información sobre el número de puerto de destino. Cuando un dispositivo recibe una solicitud entrante, consulta el número de puerto para determinar a qué servicio o aplicación debe dirigirse. Esto facilita la segmentación y la gestión de la comunicación en una red, ya que permite que múltiples servicios se ejecuten simultáneamente en una misma máquina sin interferir entre sí.

Por ejemplo, el puerto 80 se reserva comúnmente para los servicios web HTTP, mientras que el puerto 25 se utiliza para el correo electrónico SMTP. Cuando un cliente solicita una página web, su solicitud se envía al puerto 80 del servidor web correspondiente. Los puertos TCP son esenciales para el funcionamiento de Internet y las redes de computadoras, ya que permiten que los servicios y aplicaciones se comuniquen de manera eficiente y organizada.

¿Cuál es la misión de **ICANN**?

La misión de ICANN, la Corporación de Internet para la Asignación de Nombres y Números, es coordinar y supervisar de manera global los aspectos técnicos y operativos clave de Internet. En términos generales, ICANN desempeña un papel fundamental en la gestión de los recursos críticos de Internet y en la promoción de la seguridad, la estabilidad y la interoperabilidad de la red global.

Las principales áreas de misión y responsabilidad de ICANN incluyen:

\* **Asignación de Nombres de Dominio:** ICANN administra y coordina el sistema de nombres de dominio (DNS) de nivel superior, lo que significa que es responsable de la asignación de nombres de dominio de nivel superior (como .com, .org, .net) y de mantener la base de datos centralizada que asocia los nombres de dominio con direcciones IP.

\* **Asignación de Números IP:** ICANN también supervisa la asignación y administración de direcciones IP (Protocolo de Internet) y bloques de direcciones IP a nivel global. Esto es esencial para garantizar que cada dispositivo conectado a Internet tenga una dirección IP única y que las redes puedan enrutar los paquetes de datos de manera efectiva.

\* **Coordinación de Parámetros de Internet:** ICANN administra y coordina parámetros técnicos críticos de Internet, como los números de puerto utilizados en protocolos de comunicación, para garantizar la interoperabilidad de los sistemas y aplicaciones en la red.

\* **Mantenimiento de la Seguridad y Estabilidad de Internet:** ICANN trabaja para mantener la seguridad y estabilidad del DNS y otros aspectos técnicos de Internet, colaborando con diversas partes interesadas de la comunidad de Internet para abordar amenazas y vulnerabilidades.

\* **Promoción de la Participación y la Diversidad:** ICANN fomenta la participación de múltiples partes interesadas en sus procesos de toma de decisiones y se esfuerza por ser inclusivo y transparente en sus operaciones.

**En resumen,** la misión de ICANN es esencialmente garantizar que los recursos técnicos y operativos fundamentales de Internet se gestionen de manera eficaz y que Internet siga siendo una red global segura y estable que sea accesible para usuarios de todo el mundo. ICANN trabaja en colaboración con la comunidad global de Internet para cumplir con esta misión.

¿Qué función tiene un **ruteador**?

Un ruteador, también conocido como router en inglés, desempeña varias funciones clave en una red de computadoras, y su papel es fundamental para permitir la comunicación efectiva entre dispositivos en una red. Algunas de las principales funciones de un ruteador son las siguientes:

\* **Enrutamiento de Datos:** La función principal de un ruteador es enrutar o dirigir paquetes de datos entre diferentes redes o subredes. Esto implica tomar decisiones sobre la mejor ruta para que los datos lleguen desde la fuente hasta el destino a través de la red.

\* **Conexión entre Redes:** Un ruteador actúa como un dispositivo intermediario que conecta diferentes redes entre sí. Esto puede incluir la conexión entre una red local (LAN) y la red de Internet, lo que permite que los dispositivos de la LAN accedan a recursos en Internet y viceversa.

\* **NAT (Network Address Translation):** Los ruteadores suelen realizar NAT, que permite que varios dispositivos en una red local compartan una única dirección IP pública para acceder a Internet. Esto ayuda a conservar direcciones IP públicas y mejora la seguridad al ocultar las direcciones IP internas de la red local.

\* **Firewall:** Muchos ruteadores incluyen capacidades de firewall que ayudan a proteger la red local al filtrar el tráfico no deseado o potencialmente malicioso. El firewall puede bloquear ciertos tipos de conexiones entrantes y salientes según las reglas de seguridad configuradas.

\* **Gestión de Ancho de Banda:** Algunos ruteadores ofrecen herramientas para gestionar y controlar el ancho de banda de la red. Esto permite priorizar ciertos tipos de tráfico, como el tráfico de voz o video, para garantizar un rendimiento óptimo.

\* **DHCP (Dynamic Host Configuration Protocol):** Los ruteadores a menudo actúan como servidores DHCP, asignando automáticamente direcciones IP a los dispositivos de la red local cuando se conectan, lo que simplifica la configuración de los dispositivos.

\* **Seguridad Inalámbrica:** En el caso de ruteadores inalámbricos (WiFi), proporcionan conectividad inalámbrica a dispositivos como computadoras portátiles y teléfonos inteligentes y permiten configurar medidas de seguridad, como cifrado de datos (por ejemplo, WPA2 o WPA3) y autenticación.

\* **Registro y Gestión de Tráfico:** Los ruteadores a menudo registran datos sobre el tráfico de red, lo que permite a los administradores de red supervisar y analizar la actividad de la red para detectar problemas o identificar patrones de uso.

**En resumen,** un ruteador es un componente esencial en la infraestructura de redes, ya que facilita la comunicación entre dispositivos en diferentes redes, protege la red local y permite el acceso a Internet. Su capacidad para enrutar datos y realizar funciones de seguridad lo convierte en una pieza clave en la construcción y administración de redes de computadoras.

¿Cuál es la ventaja del diseño modular del modelo **TCP IP**?

El diseño modular del modelo TCP/IP, también conocido como el modelo de Internet, ofrece varias ventajas significativas en la gestión y el funcionamiento de las redes de computadoras. Estas ventajas son las siguientes:

\* **Flexibilidad y Escalabilidad:** El modelo TCP/IP está compuesto por capas independientes, cada una con una función específica. Esto facilita la expansión y la adaptación de la red a medida que cambian los requisitos y las tecnologías. Puedes actualizar o reemplazar componentes de una capa sin afectar las demás.

\* **Interoperabilidad:** El diseño modular permite que diferentes dispositivos y sistemas, incluso de fabricantes diferentes, se comuniquen entre sí de manera efectiva, siempre y cuando sigan el estándar TCP/IP. Esto fomenta la interoperabilidad en la Internet y las redes empresariales.

\* **Facilita el Desarrollo y la Mantenibilidad:** La separación de funciones en capas hace que sea más fácil desarrollar, mantener y solucionar problemas en sistemas de red. Los equipos de desarrollo pueden centrarse en una capa sin preocuparse por las demás.

\* **Evolución Tecnológica:** A lo largo del tiempo, las tecnologías de red han evolucionado y diversificado. El diseño modular del modelo TCP/IP permite la incorporación de nuevas tecnologías y protocolos sin alterar las capas existentes.

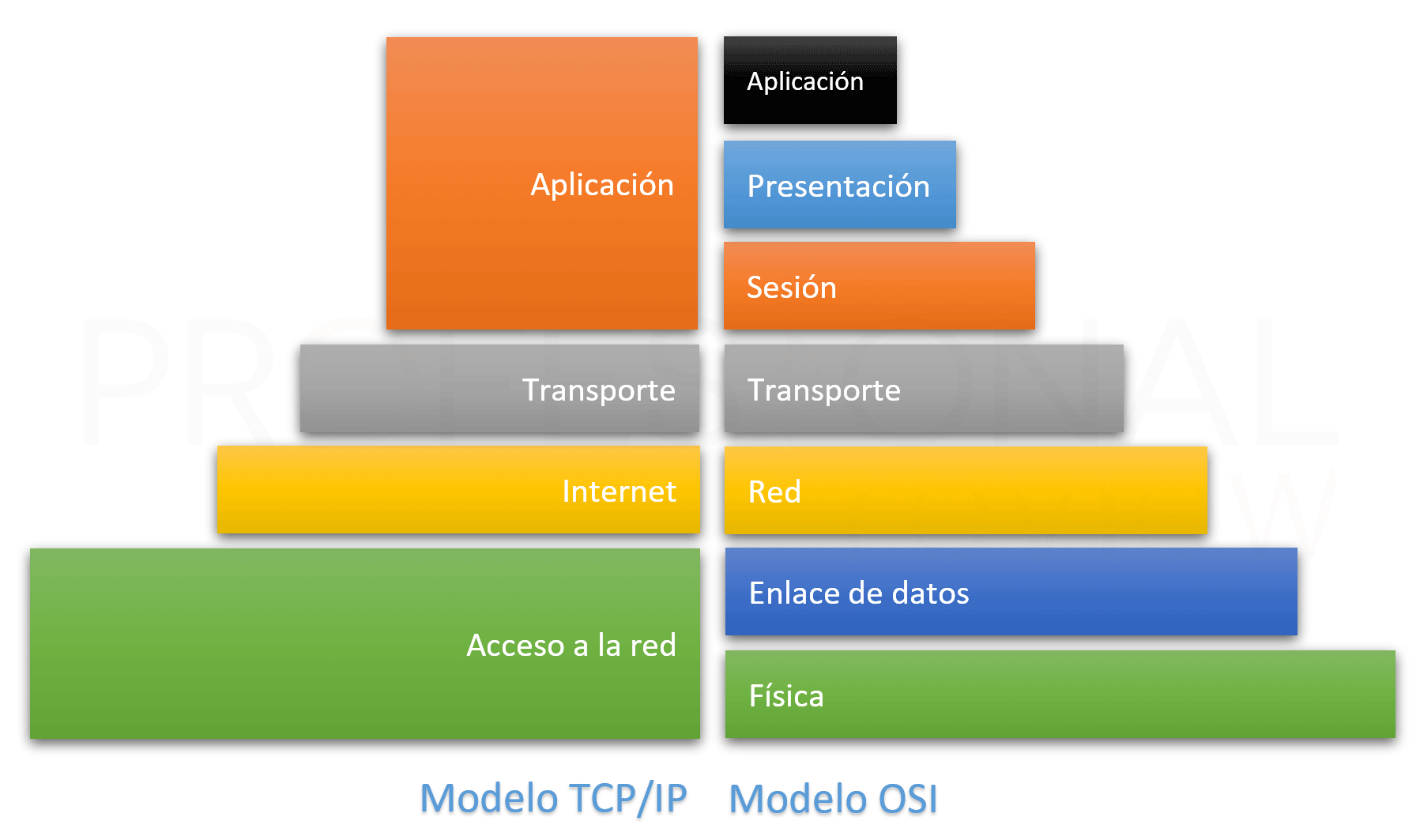
\* **Independencia de la Capa Física:** El modelo TCP/IP se enfoca en las capas superiores de la red, lo que significa que es independiente de la tecnología subyacente en la capa física. Esto permite que funcione en una amplia variedad de medios de transmisión, como cables de cobre, fibra óptica o conexiones inalámbricas.

\* **Enfoque en Funcionalidad Específica:** Cada capa se centra en una función específica, lo que simplifica la comprensión y la resolución de problemas. Por ejemplo, la Capa de Aplicación se ocupa de la comunicación de aplicaciones, mientras que la Capa de Red se encarga del enrutamiento de datos.

\* **Estándar Global:** El modelo TCP/IP es un estándar global ampliamente adoptado, lo que significa que es utilizado en todo el mundo. Esto ayuda a garantizar la coherencia y la compatibilidad en la comunicación en Internet y otras redes globales.

**En resumen,** el diseño modular del modelo TCP/IP brinda flexibilidad, interoperabilidad, facilidad de desarrollo y mantenimiento, y la capacidad de evolucionar con las cambiantes tecnologías de red. Estas ventajas son esenciales para el funcionamiento eficiente y la gestión efectiva de redes en la era de la conectividad global.

¿Cuál es la función de la **capa de acceso a la red**?



La capa de acceso a la red, también conocida como capa de acceso, es una de las capas del modelo OSI (Open Systems Interconnection) y del modelo TCP/IP. Su función principal es facilitar la conexión de dispositivos finales (como computadoras, impresoras, cámaras IP, teléfonos, etc.) a la red local o al segmento de red al que están conectados. Esta capa se encuentra en la parte inferior del modelo de capas y es fundamental para la comunicación de datos en una red local.

Las principales funciones de la capa de acceso a la red son las siguientes:

\* **Control de Acceso al Medio:** La capa de acceso controla cómo los dispositivos comparten el medio de transmisión en una red local. Esto incluye determinar cuándo un dispositivo puede transmitir datos, evitar colisiones de datos en redes Ethernet (mediante el protocolo CSMA/CD), y coordinar el acceso al medio en redes inalámbricas.

\* **Encapsulación y Desencapsulación:** Esta capa es responsable de agregar una cabecera específica de acceso a la red a los datos que se envían o recibirán en la red local. Cuando los datos llegan a su destino, la capa de acceso elimina esta cabecera para que los datos puedan ser entregados al dispositivo correcto en la red.

\* **Direccionamiento Físico:** En esta capa se utilizan direcciones físicas, como las direcciones MAC (Media Access Control), para identificar de manera única cada dispositivo en la red local. Estas direcciones son utilizadas por los conmutadores (switches) y otros dispositivos de la capa de acceso para determinar a qué dispositivo se debe enviar un paquete de datos.

\* **Segmentación de Dominios de Colisión:** En redes Ethernet, la capa de acceso divide la red en segmentos más pequeños llamados dominios de colisión. Esto ayuda a limitar el alcance de las colisiones de datos, lo que mejora la eficiencia de la red.

\* **Traducción de Protocolos:** En algunos casos, la capa de acceso puede realizar la traducción de protocolos cuando se conectan dispositivos con diferentes protocolos de acceso a la red, como Ethernet y Wi-Fi.

**En resumen,** la capa de acceso a la red juega un papel fundamental en la conexión de dispositivos finales a la red local y en la administración de la comunicación en ese entorno. Sus funciones incluyen el control de acceso al medio, la encapsulación de datos, el direccionamiento físico y la segmentación de dominios de colisión, entre otros, lo que contribuye a la eficiencia y la confiabilidad de las redes locales.

¿Cuál es la función del **heade**r que agrega cada capa?

En el modelo TCP/IP, cada capa agrega una cabecera (header) específica a los datos a medida que pasan a través de esa capa. Estas cabeceras contienen información importante que se utiliza en el proceso de comunicación de datos a lo largo de la red. A continuación, se describen las funciones de las cabeceras agregadas por cada capa en el modelo TCP/IP:

\* **Capa de Aplicación (Capa 7):** La cabecera en esta capa no se agrega específicamente, pero los datos de la aplicación pueden incluir información de control o metadatos que son necesarios para la aplicación en sí. Por ejemplo, en una solicitud HTTP, la cabecera podría incluir información como la dirección IP del servidor web al que se dirige la solicitud y el tipo de contenido que se espera en la respuesta.

\* **Capa de Transporte (Capa 4):** La capa de transporte agrega una cabecera que contiene información sobre el control de flujo, la identificación de puertos de origen y destino, y números de secuencia y de reconocimiento. En el caso de TCP, también se incluye información para establecer y mantener una conexión confiable y orientada a la conexión, como las banderas SYN, ACK y FIN.

\* **Capa de Red (Capa 3):** La cabecera en la capa de red contiene información de direccionamiento IP, como las direcciones IP de origen y destino, la versión del protocolo IP, el número de TTL (Time-to-Live) para controlar la vida útil del paquete, y otras informaciones de enrutamiento como la máscara de subred.

\* **Capa de Acceso a la Red (Capa 2):** La cabecera de la capa de acceso a la red agrega información específica del medio de transmisión utilizado en la red local. Por ejemplo, en Ethernet, esta cabecera incluye direcciones MAC (Media Access Control) de origen y destino, el tipo de trama, y detalles de control, como las secuencias de bits para detectar errores.

\* **Capa Física (Capa 1):** La capa física se encarga de la transmisión física de los bits a través del medio de transmisión, como cables de cobre, fibra óptica o señales inalámbricas. No agrega una cabecera específica, pero se encarga de convertir los datos y las cabeceras en señales eléctricas, ópticas o de radio para la transmisión a través del medio físico.

Cada capa agrega su cabecera para proporcionar información necesaria para el proceso de comunicación y el enrutamiento de datos a través de la red. A medida que los datos viajan de la capa de aplicación a la capa física en el remitente y de la capa física a la capa de aplicación en el receptor, estas cabeceras se utilizan para dirigir y controlar la transmisión de datos de manera eficiente y precisa.

1. Indique las ventajas y desventajas comparativas de **TCP** Vs **UDP**.
2. ¿Qué significa que los datos se “**encapsulan**”?
3. ¿Qué significa que **TCP** es un **protocolo confiable**?
4. ¿Cuál es la tecnología **LAN** mas común?
5. ¿Qué es **CSMA/CD**?
6. ¿Que función tiene **CRC**?
7. ¿Qué formato tiene una dirección **IPv4**?
8. ¿Qué información devuelve **ARP**?
9. ¿Cuál es el propósito del **TTL**?
10. ¿Cuál es la diferencia entre **ARP** y **RARP**?
11. Suponga una máscara **255.255.0.0**. ¿Cuántos host permite? ¿Cuantas subredes permite?
12. ¿Qué es lo que hace que a **TCP** confiable?
13. ¿Qué es el “**triple handshake**”?
14. ¿Qué servicio corre en el **puerto TCP 25**?
15. ¿Qué servicio corre en **puerto UDP 53**?

Responda **negrita azul**

**PARTE 2**

1. Dadas las siguientes direcciones MAC de tarjetas de red:

Indique por que empresa fueron fabricadas y de la dirección de su sitio Web

|  |  |
| --- | --- |
| 00:05:5D:7F:8E:83 |  |
| 00:04:98:00:78:FD |  |
| 00:89:56:CD:EF:AB |  |
| 00:05:5D:7F:8A:83 |  |

1. Supongamos que en una trama que envía un PC, el campo MAC origen está rellenado con la siguiente combinación de ceros y unos: **0011**0000**0001**0101**0101**0111**1100**1111**1110**1110**0011**0100

¿Cómo sería la expresión de “dirección física” cuando empleamos el comando ipconfig/all?

1. Dada la siguiente dirección física: 00:05:5D:AB:CD:FA ¿A qué expresión binaria sería equivalente?
2. Escribe la IP origen, IP destino, MAC origen y MAC destino de los dos paquetes que se intercambian dos equipos cuando

**PC1 de IP 192.168.1.1 y MAC00:00:b4:c3:c8:f4**

quiere comunicarse por primera vez con

**PC2 de IP 192.168.1.2 y MAC 00:a0:b5:89:d5:67**.

1. Cuando en Windows empleamos el comando **ipconfig/all**
   1. ¿A qué nos referimos con “nombre del host”?
   2. ¿Qué expresión indica que la dirección MAC del equipo buscado es desconocida?
2. Lo primero que hace un PC de una red local que quiere comunicarse con otro de la misma red local es consultar su tabla arp
   1. ¿por qué?
   2. ¿cómo podemos averiguar el contenido de la tabla arp del PC?
   3. ¿Qué pasaría si en la tabla arp no se encuentran los datos del equipo con quien queremos comunicar?
3. ¿Es suficiente en una LAN saber la dirección IP de un equipo para comunicarte con él ¿Por qué?
4. Cuando un PC utiliza el protocolo ARP en una LAN
   1. ¿A cuántos PCs llegará su ARP request (primer mensaje ARP) ?
   2. ¿Cuántos le contestarán (ARP reply o segundo mensaje ARP) ?
5. ¿Cuántos bits expresan una dirección IP cuando se usa el protocolo IPv4?
6. Dada la siguiente dirección IP, 192.168.120.1, exprésala en binario.
7. La siguiente combinación de bits expresa una dirección IP: 11000000111111100111111101111110
   1. ¿Cuál sería su expresión en decimal?
   2. ¿Es una IP pública o privada?
8. Dada la dirección IP especial: 11111111111111111111111111111111

¿Qué significado tiene?

¿se le puede poner a un PC esta IP ?

1. Una red local se conecta a Internet por medio de un router
   1. ¿Cuántas direcciones IP tiene como mínimo el router?
   2. ¿son públicas o privadas?
2. Clasifica estas direcciones IP en direcciones IP públicas, privadas o inexistentes

|  |  |
| --- | --- |
| 192.170.23.3 |  |
| 80.35.45.67 |  |
| 10.224.120.5 |  |
| 172.16.78.4 |  |
| 172.32.24.5 |  |
| 192.168.5.3 |  |
| 45.46.36.34 |  |
| 195.45.56.3 |  |

1. Dado un mensaje RARP
   1. ¿Para qué se usa el protocolo RARP?
   2. ¿Cuáles serán los campos
      1. IP origen,
      2. IP destino
      3. MAC Origen
      4. MAC destino

del primer mensaje que envíe un cliente RARP?

1. Lea la tabla **arp** de su máquina y pegue su contenido.