

# Sistemas Operativos y Distribuidos

Iren Lorenzo Fonseca  
iren.fonseca@ua.es



TEMA 2. Fundamentos de Redes de Computadores.  
Ejercicios

# Pregunta 1

## Dispositivos

---

Referente a los dispositivos:

- a) **¿Qué son los dispositivos intermedios y finales?**
- b) Ponga 3 ejemplos de dispositivos intermedios de diferentes capas del modelo OSI. Identifique la capa de cada uno de los dispositivos.
- c)¿Cuál es la diferencia entre un hub y un switch?
- d)¿Qué relación hay entre un router y un gateway?

# Respuesta Pregunta 1

a

---

**Dispositivos finales:** Son los dispositivos que los usuarios utilizan para comunicarse en la red y acceden a la información y los servicios ofrecidos a través de la red. Ejemplos incluyen computadoras, teléfonos inteligentes, tablets, impresoras, etc.

**Dispositivos intermedios:** Son los dispositivos que facilitan la comunicación y el flujo de datos a través de la red, actuando como intermediarios entre los dispositivos finales. Ejemplos incluyen routers, switches, hubs, firewalls, etc.

# Pregunta 1

## Dispositivos

---

Referente a los dispositivos:

- a) ¿Qué son los dispositivos intermedios y finales?
- b) Ponga 3 ejemplos de dispositivos intermedios de diferentes capas del modelo OSI. Identifique la capa de cada uno de los dispositivos.**
- c)¿Cuál es la diferencia entre un hub y un switch?
- d)¿Qué relación hay entre un router y un gateway?

# Respuesta Pregunta 1

b

---



**Repetidores:** dispositivos que amplifican y retransmiten señales de red para extender su alcance. Capa 1



**Hubs:** es un dispositivo de red básico que se utiliza para conectar varios dispositivos en una red local (LAN). Capa 1



**switch:** Un switch es un dispositivo de red que se utiliza para conectar múltiples dispositivos en una misma red local (LAN) y gestionar el tráfico de datos entre ellos. El switch recibe los datos (en forma de paquetes) de un dispositivo de origen y los envía únicamente al dispositivo de destino, utilizando direcciones MAC (Media Access Control). Esto reduce el tráfico innecesario en la red. Capa 2



**router:** El router (o enrutador) dirige el tráfico de datos entre redes diferentes, adaptando protocolos, y determinando la mejor ruta. Capa 3

# Pregunta 1

## Dispositivos

---

Referente a los dispositivos:

- a) ¿Qué son los dispositivos intermedios y finales?
- b) Ponga 3 ejemplos de dispositivos intermedios de diferentes capas del modelo OSI. Identifique la capa de cada uno de los dispositivos.
- c) **¿Cuál es la diferencia entre un hub y un switch?**
- d) ¿Qué relación hay entre un router y un gateway?

# Respuesta Pregunta 1

c

---

•**Hub:** Un hub es un dispositivo de red que permite conectar múltiples dispositivos en una red local. Opera en la capa física (Capa 1) del modelo OSI y simplemente repite las señales de datos que recibe a todos los puertos, sin discriminar entre los destinatarios. Esto puede generar colisiones y congestión en la red.

•**Switch:** Un switch, en cambio, opera en la capa de enlace de datos (Capa 2) y es más eficiente que un hub. Utiliza direcciones MAC para enviar los datos solo al puerto específico al que está conectado el dispositivo de destino. Esto reduce las colisiones y mejora el rendimiento de la red.

# Respuesta Pregunta 1

C

Característica	Hub	Switch
Tipo de dispositivo	Pasivo, simple	Inteligente, gestionado
Redirección de tráfico	Envía datos a todos los puertos	Envía datos solo al puerto de destino
Colisiones	Más propenso a colisiones	Elimina las colisiones en cada puerto
Eficiencia	Baja eficiencia, ancho de banda compartido	Alta eficiencia, ancho de banda dedicado por puerto
Dirección de los datos	No tiene capacidad para dirigir los datos	Utiliza direcciones MAC para direccionar los datos
Costo	Más barato	Más caro
Tecnología	Capa 1 (física)	Capa 2 (enlace de datos), puede ser Capa 3
Seguridad	Menor seguridad, todos los dispositivos ven el tráfico	Mayor seguridad, tráfico solo entre el origen y el destino



# Pregunta 1

## Dispositivos

---

Referente a los dispositivos:

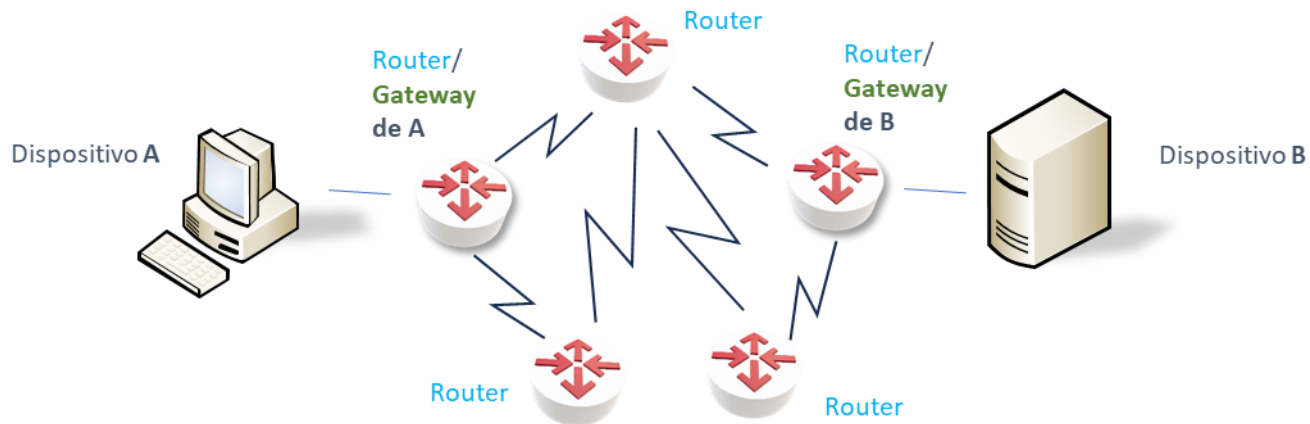
- a) ¿Qué son los dispositivos intermedios y finales?
- b) Ponga 3 ejemplos de dispositivos intermedios de diferentes capas del modelo OSI. Identifique la capa de cada uno de los dispositivos.
- c)¿Cuál es la diferencia entre un hub y un switch?
- d)¿Qué relación hay entre un router y un gateway?**

# Respuesta Pregunta 1

d

- **Routers:** dispositivos que dirigen el tráfico de datos entre redes diferentes, adaptando protocolos y señales, y determinando la mejor ruta para el envío de los datos.
- **Gateways:** generalmente se trata de routers que actúan como puntos de entrada y salida en una red, permitiendo la comunicación entre redes diferentes. Los **gateways** pueden incluir funciones de traducción de protocolos.

Los **routers** que actúan como punto de entrada y salida en una red se denominan **gateways** (o **pasarelas**).



# Pregunta 2

## Dispositivos

---

Qué dispositivo capa 7 debo utilizar en el diseño de mi red si necesito:

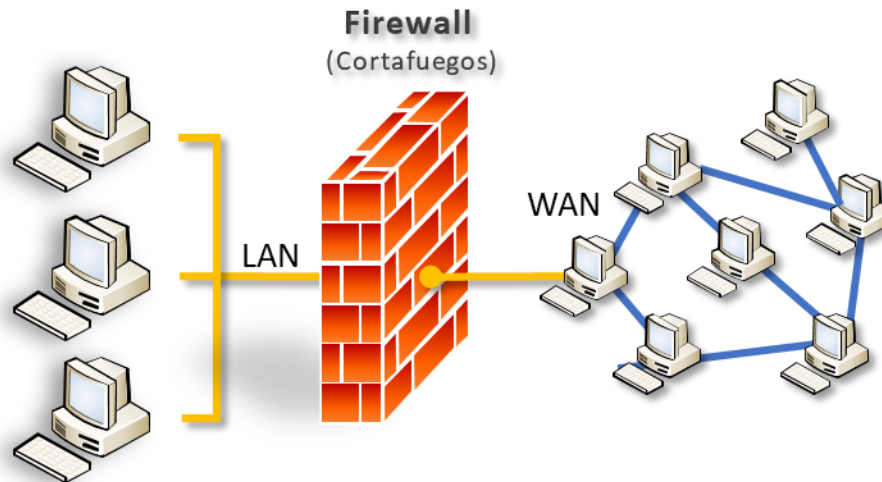
- a) Filtrar el tráfico con reglas para evitar ataques. Explique el dispositivo seleccionado
- b) No exponer las IPs de los ordenadores de mi red cuando quieran conectarse a algún servicio http. Explique el dispositivo seleccionado y comente si haría alguna variación teniendo en cuenta que se quiere aumentar la velocidad de respuesta y disminuir el tráfico de red saliente
- c) Tengo servidores web para los cuales quiero hacer un balanceo de carga
- d) ¿Cuál es la diferencia entre un proxy y un proxy inverso?

# Respuesta Pregunta 2

a

El dispositivo adecuado para esta tarea es un **firewall**

- sistemas (basado en dispositivo especializado o en software) de seguridad que controlan el tráfico de red basado en reglas de seguridad predeterminadas, protegiendo las redes internas de accesos no autorizados. Capa 7
- Un **firewall** (cortafuegos en español) es un dispositivo de seguridad de red o un software que se utiliza para **monitorear y controlar el tráfico de red** entre diferentes redes, como la red interna de una organización e Internet, según reglas de seguridad predefinidas. Su propósito principal es **proteger la red** de accesos no autorizados y de amenazas externas, como ataques cibernéticos, virus o malware.



# Pregunta 2

## Dispositivos

---

Qué dispositivo capa 7 debo utilizar en el diseño de mi red si necesito:

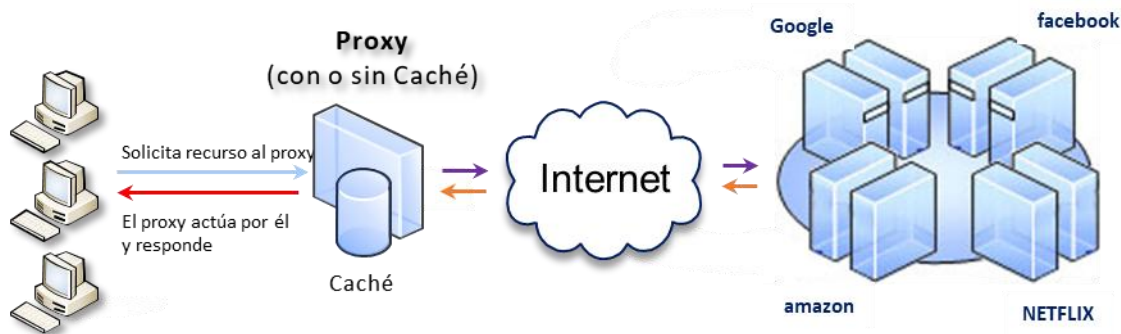
- a) Filtrar el tráfico con reglas para evitar ataques. Explique el dispositivo seleccionado
- b) No exponer las IPs de los ordenadores de mi red cuando quieran conectarse a algún servicio http. Explique el dispositivo seleccionado y comente si haría alguna variación teniendo en cuenta que se quiere aumentar la velocidad de respuesta y disminuir el tráfico de red saliente.**
- c) Tengo servidores web para los cuales quiero hacer un balanceo de carga
- d) ¿Cuál es la diferencia entre un proxy un un proxy inverso?

# Respuesta Pregunta 2

b

El dispositivo adecuado para esta tarea es un proxy

- Un **proxy HTTP** actúa como intermediario entre los clientes (los ordenadores de tu red) y los servidores HTTP en Internet. Cuando los clientes hacen solicitudes HTTP, el proxy las envía al servidor en su nombre, lo que oculta las IPs internas de los clientes. Este enfoque también permite implementar medidas de seguridad, controlar el acceso y optimizar el rendimiento.
- Si se desea mejorar la velocidad de respuesta y reducir el tráfico saliente, una opción adicional sería usar un **proxy caché**. El proxy caché guarda una copia de las respuestas HTTP de los servidores, por lo que cuando un cliente hace una solicitud para el mismo contenido, el proxy puede responder directamente desde su caché, reduciendo la carga en la red y el servidor, lo que mejora la eficiencia y velocidad de la red.



# Pregunta 2

## Dispositivos

---

Qué dispositivo capa 7 debo utilizar en el diseño de mi red si necesito:

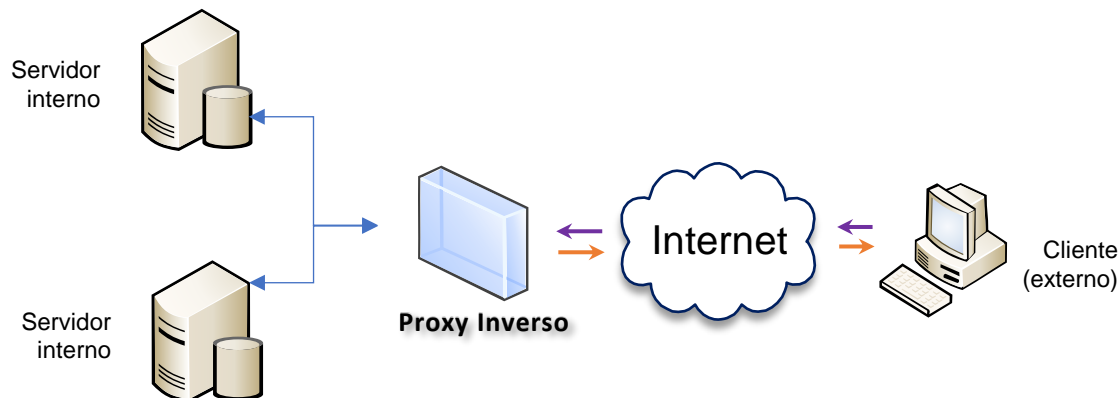
- a) Filtrar el tráfico con reglas para evitar ataques. Explique el dispositivo seleccionado
- b) No exponer las IPs de los ordenadores de mi red cuando quieran conectarse a algún servicio http. Explique el dispositivo seleccionado y comente si haría alguna variación teniendo en cuenta que se quiere aumentar la velocidad de respuesta y disminuir el tráfico de red saliente.
- c) **Tengo servidores web para los cuales quiero hacer un balanceo de carga**
- d) ¿Cuál es la diferencia entre un proxy un un proxy inverso?

# Respuesta Pregunta 2



El dispositivo adecuado para esta tarea es un proxy inverso.

Un proxy inverso actúa como intermediario entre los clientes y los servidores web. El proxy inverso recibe todas las solicitudes entrantes de los clientes y las distribuye entre los diferentes servidores web disponibles, según el algoritmo de balanceo de carga configurado (por ejemplo, Round Robin, Least Connections, etc.). Esto permite distribuir la carga de trabajo de manera equitativa entre los servidores y mejora la disponibilidad y escalabilidad del servicio web.





# Pregunta 2

## Dispositivos

---

Qué dispositivo capa 7 debo utilizar en el diseño de mi red si necesito:

- a) Filtrar el tráfico con reglas para evitar ataques. Explique el dispositivo seleccionado
- b) No exponer las IPs de los ordenadores de mi red cuando quieran conectarse a algún servicio http. Explique el dispositivo seleccionado y comente si haría alguna variación teniendo en cuenta que se quiere aumentar la velocidad de respuesta y disminuir el tráfico de red saliente.
- c) Tengo servidores web para los cuales quiero hacer un balanceo de carga
- d) **¿Cuál es la diferencia entre un proxy un un proxy inverso?**

# Respuesta Pregunta 2

d

---

Un proxy es un dispositivo o software que actúa como intermediario entre los clientes (usuarios o dispositivos) y los servidores a los que estos quieren acceder. El proxy recibe las solicitudes de los clientes, las reenvía al servidor de destino y luego devuelve la respuesta del servidor al cliente. Esto se utiliza para ocultar las IPs de los clientes, implementar políticas de seguridad, caching, control de acceso, entre otras funciones.

**Uso típico:** Los proxies son utilizados por los clientes para ocultar su identidad, acceder a contenido bloqueado, o mejorar el rendimiento mediante caching.

# Respuesta Pregunta 2

d

---

Un proxy inverso es un dispositivo o software que se coloca entre los clientes y uno o varios servidores web. A diferencia del proxy tradicional, que actúa en nombre de los clientes, el proxy inverso actúa en nombre de los servidores. Los clientes no interactúan directamente con los servidores web, sino con el proxy inverso, que luego se encarga de redirigir las solicitudes a los servidores adecuados.

**Uso típico:** El proxy inverso se usa principalmente para mejorar el rendimiento mediante caching de contenido, balanceo de carga, y seguridad (ocultar la infraestructura interna, proteger los servidores detrás del proxy, etc.).

# Pregunta 3

Red física

---

Referente a los conceptos de Ancho de banda, Rendimiento real y Capacidad de transferencia útil:

- a) **¿Cuál de las tres es la mayor y cuál es la menor?**
- b) ¿Cuáles podrían ser las causas de que el rendimiento real sea menor que el ancho de banda?
- c) ¿Por qué la capacidad de transferencia útil siempre será menor que el rendimiento real?
- c) Mi proveedor de servicios me ofrece una conexión a Internet de 1 Gbps. En casa tengo un switch con una velocidad máxima de 300 Mbps, conectado al router, y a ese switch conecto mi ordenador. Al realizar una prueba, veo que un archivo de 200 Megabits tarda 2 segundos en enviarse. En esta situación, ¿cuál es el ancho de banda, ¿cuál sería el rendimiento real máximo que podría tener mi ordenador y cuál es la velocidad de transferencia útil? Justifique su respuesta.

# Respuesta Pregunta 3

a

---

**Ancho de banda** es generalmente la mayor de las tres. Representa la capacidad máxima teórica de transmisión de datos de una red, normalmente medida en bits por segundo (bps), y se refiere al límite superior de la velocidad de transmisión.

**Capacidad de transferencia útil** es la menor de las tres. Representa la cantidad de datos útiles que pueden ser transferidos efectivamente, teniendo en cuenta que se pierde rendimiento con las sobrecargas de protocolo y las pérdidas por retransmisión o errores.

**Rendimiento real** suele ser la intermedia. Este es el valor de la velocidad a la que realmente se transmiten los datos, teniendo en cuenta factores como la congestión de la red, los errores de transmisión y los protocolos involucrados, entre otros.

# Pregunta 3

Red física

---

Referente a los conceptos de Ancho de banda, Rendimiento real y Capacidad de transferencia útil:

- a) ¿Cuál de las tres es la mayor y cuál es la menor?
- b) ¿Cuáles podrían ser las causas de que el rendimiento real sea menor que el ancho de banda?**
- c) ¿Por qué la capacidad de transferencia útil siempre será menor que el rendimiento real?
- c) Mi proveedor de servicios me ofrece una conexión a Internet de 1 Gbps. En casa tengo un switch con una velocidad máxima de 300 Mbps, conectado al router, y a ese switch conecto mi ordenador. Al realizar una prueba, veo que un archivo de 200 Megabits tarda 2 segundos en enviarse. En esta situación, ¿cuál es el ancho de banda, ¿cuál sería el rendimiento real máximo que podría tener mi ordenador y cuál es la velocidad de transferencia útil? Justifique su respuesta.

# Respuesta Pregunta 3

b

---

El rendimiento real suele ser menor que el ancho de banda por varias razones:

- **Limitaciones de hardware:** Si alguno de los componentes de la red (como el router, switch o tarjeta de red) tiene una capacidad inferior, el rendimiento real se verá afectado, incluso si el ancho de banda teórico es más alto.
- **Protocolos de red:** Los protocolos de red, como TCP, implican un overhead (sobrepeso) que reduce la cantidad de datos útiles que se pueden transmitir, ya que parte del ancho de banda se usa para la gestión de la conexión (control de flujo, verificación de errores, etc.).
- **SO:** Los sistemas operativos gestionan las conexiones de red a través de sus controladores y pilas TCP/IP. Si los controladores de red o el sistema operativo no están optimizados, esto puede afectar negativamente el rendimiento real, incluso si la red tiene un alto ancho de banda.

# Respuesta Pregunta 3

b

---

El rendimiento real suele ser menor que el ancho de banda por varias razones:

- **Software de seguridad:** firewalls y antivirus puede introducir una sobrecarga adicional en el procesamiento de los paquetes de datos. Estos sistemas inspeccionan y filtran el tráfico, lo que consume recursos de CPU y puede ralentizar la transmisión de datos
- **Congestión de red:** Cuando hay muchos dispositivos utilizando la misma red, puede haber competencia por el ancho de banda disponible, lo que reduce el rendimiento real.
- **Pérdida de paquetes:** Si se pierden paquetes de datos, el protocolo de transporte (como TCP) necesita retransmitir esos paquetes, lo que disminuye la eficiencia de la transmisión.
- **Interferencia y ruido:** Factores físicos o interferencias en la red pueden degradar la calidad de la señal, lo que afecta la velocidad real de transmisión.



# Pregunta 3

Red física

---

Referente a los conceptos de Ancho de banda, Rendimiento real y Capacidad de transferencia útil:

- a) ¿Cuál de las tres es la mayor y cuál es la menor?
- b) ¿Cuáles podrían ser las causas de que el rendimiento real sea menor que el ancho de banda?
- c) **¿Por qué la capacidad de transferencia útil siempre será menor que el rendimiento real?**
- c) Mi proveedor de servicios me ofrece una conexión a Internet de 1 Gbps. En casa tengo un switch con una velocidad máxima de 300 Mbps, conectado al router, y a ese switch conecto mi ordenador. Al realizar una prueba, veo que un archivo de 200 Megabits tarda 2 segundos en enviarse. En esta situación, ¿cuál es el ancho de banda, ¿cuál sería el rendimiento real máximo que podría tener mi ordenador y cuál es la velocidad de transferencia útil? Justifique su respuesta.

# Respuesta Pregunta 3

C

---

**Capacidad de transferencia útil** mide solo los datos **útiles** que se transmiten de forma efectiva, excluyendo aquellos factores que no contribuyen directamente al envío de datos útiles, tales como:

- **Sobrecargas de protocolo:** Los protocolos de red como TCP/IP añaden encabezados y otros datos de control a los paquetes que se envían a través de la red. Estos encabezados y datos adicionales no son datos útiles para el usuario, sino que sirven para controlar y asegurar la transmisión. Esto reduce la cantidad de datos útiles que realmente se pueden transferir en un determinado período de tiempo.
- **Pérdidas por retransmisión:** Si durante la transmisión de los datos se pierden paquetes debido a errores en la red o congestión, esos paquetes deben ser retransmitidos. El proceso de retransmisión consume más ancho de banda, pero no contribuye directamente a la transferencia de datos útiles, ya que son paquetes que no llegaron correctamente en el primer intento.
- **Errores:** Errores de transmisión, como interferencias en la señal o corrupción de datos, también pueden reducir la cantidad de datos que se pueden transferir efectivamente, ya que los paquetes erróneos necesitan ser detectados y reenviados, lo que consume más tiempo y recursos.

# Pregunta 3

Red física

---

Referente a los conceptos de Ancho de banda, Rendimiento real y Capacidad de transferencia útil:

- a) ¿Cuál de las tres es la mayor y cuál es la menor?
  - b) ¿Cuáles podrían ser las causas de que el rendimiento real sea menor que el ancho de banda?
  - c) ¿Por qué la capacidad de transferencia útil siempre será menor que el rendimiento real?
- c) Mi proveedor de servicios me ofrece una conexión a Internet de 1 Gbps. En casa tengo un switch con una velocidad máxima de 300 Mbps conectado al router, y a ese switch conecto mi ordenador. Al realizar una prueba, veo que un archivo de 200 Megabits tarda 2 segundos en enviarse. En esta situación, ¿cuál es el ancho de banda, ¿cuál sería el rendimiento real máximo que podría tener mi ordenador y cuál es la velocidad de transferencia útil? Justifique su respuesta.**

# Respuesta Pregunta 3

---

## **Ancho de banda:**

El ancho de banda es la capacidad máxima teórica de transmisión de datos de tu conexión a Internet o de tu red local. En este caso, el proveedor de Internet te ofrece 1 Gbps (1000 Mbps), lo que significa que la red podría, en condiciones ideales, soportar hasta 1 Gbps de transmisión de datos entre tu router y tu dispositivo final.

**Ancho de banda** = 1 Gbps (proporcionado por el proveedor de Internet).

# Respuesta Pregunta 3

d

---

## **Rendimiento real máximo:**

El **rendimiento real máximo** se refiere a la velocidad a la que realmente puedes transferir datos a través de la red. Esto depende de varios factores, pero en este caso, el **hardware del switch** es el factor limitante, ya que su velocidad máxima es **300 Mbps**. A pesar de que el proveedor de servicios de Internet ofrezca una conexión de **1 Gbps**, la velocidad máxima de transferencia a través del switch es de **300 Mbps**.

**Rendimiento real máximo = 300 Mbps** (limitado por el switch).

# Respuesta Pregunta 3

---

Para calcular la **velocidad de transferencia útil**, primero tenemos que asegurarnos de que estamos utilizando las unidades correctas. En este caso, el archivo tiene un tamaño de **200 Mb** (megabits) y tarda **2 segundos** en enviarse.

$$\text{Velocidad de transferencia útil} = \frac{200 \text{ Mb}}{2 \text{ segundos}} = 100 \text{ Mbps}$$

# Pregunta 4

Protocolos

---

Referente al modelo OSI y la pila TCP/IP:

- a) Cuáles son las capas de cada uno y la equivalencia entre ellas**
- b) Menciona al menos un protocolo de cada una de las capas de la pila TCP/IP, su funcionalidad principal y los datos principales de control que contiene su cabecera
- c) Que son las VLAN y que capas del modelo OSI están implicadas

# Respuesta Pregunta 4

a

## Modelo OSI:

- **Capa de Aplicación:** Proporciona servicios de red a las aplicaciones
- **Capa de Presentación:** Traduce los datos entre el formato de la red y el formato que las aplicaciones pueden procesar, incluyendo la encriptación y la compresión
- **Capa de Sesión:** Establece, administra y finaliza sesiones entre aplicaciones
- **Capa de Transporte:** Asegura la transferencia de datos fiable y ordenada entre extremos
- **Capa de Red:** Encargada del encaminamiento de paquetes a través de múltiples redes
- **Capa de Enlace de Datos:** Proporciona métodos para transferir datos entre nodos en la misma red
- **Capa Física:** Maneja la transmisión y recepción de bits brutos a través de un medio físico



# Respuesta Pregunta 4

a

---

## Pila TCP/IP:

- **Capa de Aplicación:** Combina las funciones de las capas de sesión, presentación y aplicación del modelo OSI.
- **Capa de Transporte:** Asegura la transferencia de datos fiable y ordenada, similar a la capa de transporte del modelo OSI.
- **Capa de Internet:** Equivale a la capa de red del modelo OSI, encargada del encaminamiento de paquetes.
- **Capa de Acceso a Red:** Es la capa que hace de interfaz entre las capas superiores y la red física siendo la responsable de la transmisión y recepción de datos a través de una red física

# Respuesta Pregunta 4

a

## Equivalencia:

- Capa de Sesión (OSI),  
• Capa de Presentación (OSI),  
• Capa de Aplicación (OSI) ↔ Capa de Aplicación (TCP/IP)

---

- Capa de Transporte (OSI) ↔ Capa de Transporte (TCP/IP)

---

- Capa de Red (OSI) ↔ Capa de Internet (TCP/IP)

---

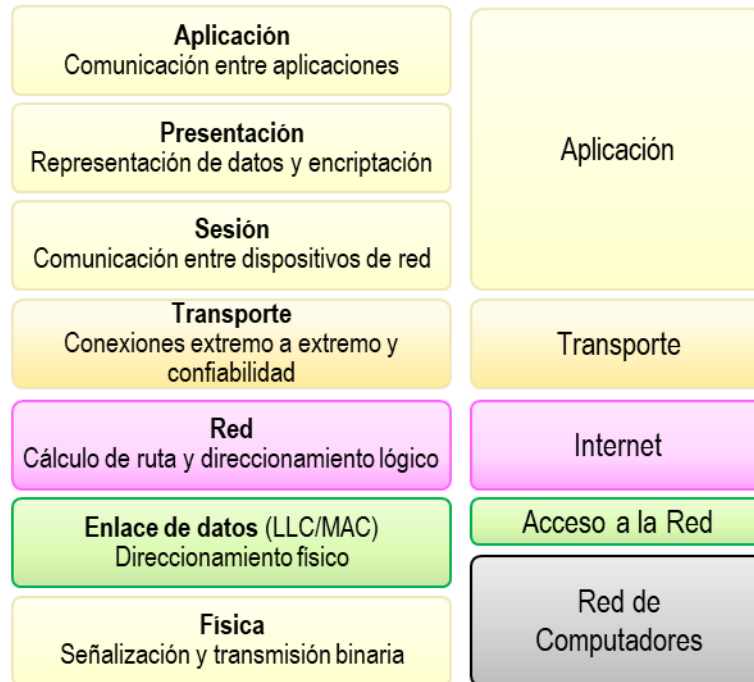
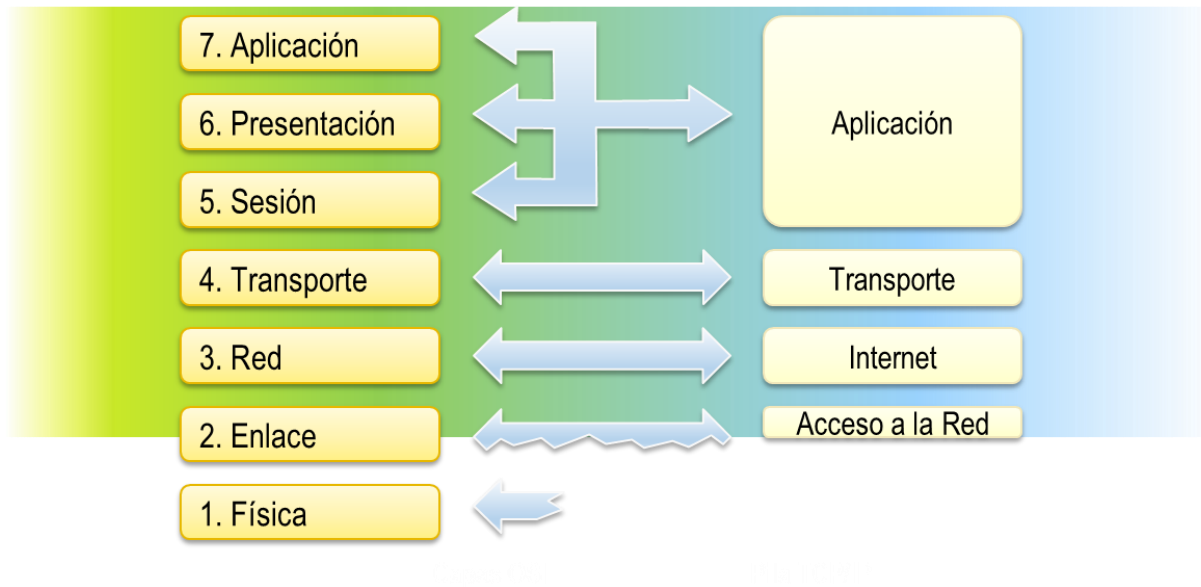
- Capa de Enlace de Datos (MAC y LLC) (OSI) ↔ MAC no se recoge en TCP/IP LLC  
está en la Capa de Acceso a Red (TCP/IP)

---

- Capa Física (OSI) ↔ No se recoge en TCP/IP

## Capas del Modelo OSI

## Capas de la pila Pila TCP/IP



# Respuesta a Pregunta 4

# Pregunta 4

## OSI y TCP/IP

---

Referente al modelo OSI y la pila TCP/IP:

- a) Cuáles son las capas de cada uno y la equivalencia entre ellas
- b) Menciona al menos un protocolo de cada una de las capas de la pila TCP/IP, su funcionalidad principal y los datos principales de control que contiene su cabecera**
- c) Que son las VLAN y que capas del modelo OSI están implicadas

# Respuesta Pregunta 4

b

## **Capa de Aplicación:**

Protocolo: HTTP (Hypertext Transfer Protocol)

Permite la transferencia de documentos HTML y otros recursos en la web.

## **Datos principales de control en la cabecera:**

Métodos (GET, POST, PUT, DELETE), códigos de estado (200 OK, 404 Not Found), encabezados HTTP (Host, User-Agent, Content-Type).

# Respuesta Pregunta 4

b

---

## **Capa de Transporte:**

Protocolo: TCP (Transmission Control Protocol)

Proporciona un servicio de transmisión de datos fiable y orientado a la conexión. Esto significa que los datos se envían estableciendo una conexión previa entre el emisor y el receptor, y hay garantía de entrega, orden, y protección contra duplicados.

## **Datos principales de control en la cabecera:**

Números de puerto de origen y destino, numero de segmento

# Respuesta Pregunta 4

b

---

## **Capa de Transporte:**

Protocolo: UDP (User Datagram Protocol)

Proporciona un servicio de transmisión de datos no fiable y sin conexión. Esto significa que los datos se envían sin establecer una conexión previa entre el emisor y el receptor, y no hay garantía de entrega, orden, ni protección contra duplicados.

## **Datos principales de control en la cabecera:**

Números de puerto de origen y destino

# Respuesta Pregunta 4

---

## **Capa de Internet:**

Protocolo: IP (Internet Protocol)

Encaminamiento de paquetes a través de diferentes redes.

## **Datos principales de control en la cabecera:**

Dirección IP de origen y destino, protocolo de nivel superior (TCP, UDP), longitud total del paquete.



# Respuesta Pregunta 4

b

---

## **Capa de Acceso a Red:**

Protocolo: ARP

ARP permite a un dispositivo en una red local determinar la dirección MAC correspondiente a una dirección IP. Esto es crucial porque, aunque los dispositivos en una red pueden comunicarse a nivel de capa 3 (IP), la entrega real de los paquetes se realiza a través de las direcciones MAC en la capa 2.

## **Datos principales de control en la cabecera:**

Dirección MAC de origen, Dirección MAC de destino

# Pregunta 4

Protocolos

---

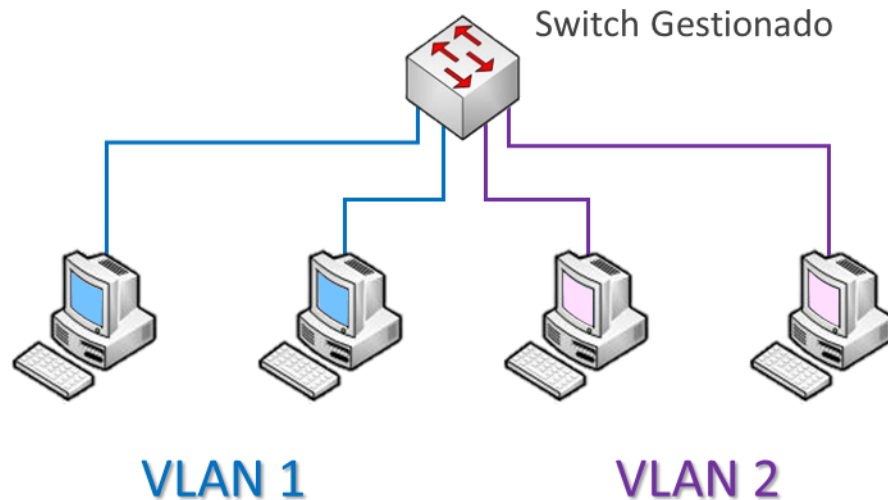
Referente al modelo OSI y la pila TCP/IP:

- a) Cuáles son las capas de cada uno y la equivalencia entre ellas
- b) Menciona al menos un protocolo de cada una de las capas de la pila TCP/IP, su funcionalidad principal y los datos principales de control que contiene su cabecera
- c) **Que son las VLAN y que capas del modelo OSI están implicadas**

# Respuesta Pregunta 4

C

VLAN (Virtual Local Area Network): Es una tecnología que permite crear redes lógicas independientes dentro de una misma red física. Las VLANs segmentan una red en distintas subredes virtuales, mejorando la gestión y la seguridad del tráfico de red.



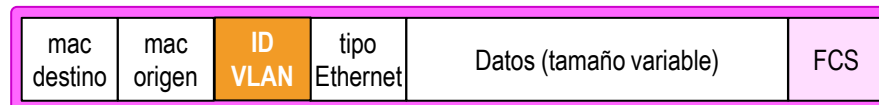
# Respuesta Pregunta 4

C

Las VLANs, permiten la segmentación lógica de una red física en varias subredes virtuales. Aunque operan principalmente en la Capa 2 (Capa de Enlace de Datos), su implementación y gestión afectan también a la Capa 3 (Capa de Red):

Capa 2: Las VLANs segmentan la red en el nivel de enlace de datos utilizando etiquetas (tags) VLAN en las tramas (subcapa MAC). Esto permite que diferentes segmentos de red (VLANs) compartan la misma infraestructura física de red (switches y cables) mientras permanecen lógicamente separados.

Trama de red



# Respuesta Pregunta 4

c

---

Capa 3: Para que los dispositivos en diferentes VLANs se comuniquen entre sí, es necesario un enrutador (o un dispositivo con capacidad de enrutamiento, como un switch de capa 3). Este enrutador opera en la capa de red, manejando la comunicación entre subredes VLAN diferentes mediante el uso de direcciones IP.

La comunicación entre dispositivos en la misma VLAN se realiza en la capa 2. Sin embargo, cuando se necesita comunicar dispositivos en diferentes VLANs, se involucra la capa 3. Esto se hace mediante un enrutador o un switch de capa 3 que realiza el enrutamiento entre las subredes asociadas a cada VLAN

# Pregunta 5

Capas TCP e identificación

---

Referente al protocolo TCP/IP

**a) Explique cómo se lleva a cabo la identificación de:**

- La aplicación a la que va dirigido el paquete
- El nodo de red al que va dirigido el paquete
- La tarjeta de red

b) ¿Qué tipo de paquete generaría la llamada ping 8.8.8.8?

c) ¿Qué diferencia tendría si hago un ping google.com?

d) Que llamadas genera mi navegador cuando pongo en la barra de direcciones <https://google.com> y doy enter.

# Respuesta Pregunta 5

a

---

## **La aplicación a la que va dirigido el paquete:**

A través del número de **puerto** en la cabecera del segmento TCP o datagrama UDP. Cada aplicación en un dispositivo utiliza un puerto específico para comunicarse. Por ejemplo, HTTP típicamente utiliza el puerto 80 y HTTPS el puerto 443.

## **El nodo de red al que va dirigido el paquete:**

A través de la **dirección IP** de destino en la cabecera del paquete IP. La dirección IP identifica de manera única a cada dispositivo en una red IP, permitiendo el enrutamiento de los paquetes desde el origen hasta el destino.

La tarjeta de red:

A través de la **dirección MAC** en la cabecera de la trama.

La dirección MAC es una dirección física única asignada a la tarjeta de red de un dispositivo.

# Pregunta 5

Capas TCP e identificación

---

Referente al protocolo TCP/IP

a) Explique cómo se lleva a cabo la identificación de:

- La aplicación a la que va dirigido el paquete
- El nodo de red al que va dirigido el paquete
- La tarjeta de red

**b) ¿Qué tipo de paquete generaría la llamada ping 8.8.8.8?**

c) ¿Qué diferencia tendría si hago un ping google.com?

d) Que llamadas genera mi navegador cuando pongo en la barra de direcciones <https://google.com> y doy enter.



# Respuesta Pregunta 5

b

---

Tipo de Paquete: ICMP (Internet Control Message Protocol).

El comando ping envía mensajes ICMP Echo Request a la dirección IP 8.8.8.8 y espera recibir mensajes ICMP Echo Reply para medir la accesibilidad y el tiempo de respuesta.

# Pregunta 5

Capas TCP e identificación

---

Referente al protocolo TCP/IP

a) Explique cómo se lleva a cabo la identificación de:

- La aplicación a la que va dirigido el paquete
- El nodo de red al que va dirigido el paquete
- La tarjeta de red

b) ¿Qué tipo de paquete generaría la llamada ping 8.8.8.8?

**c) ¿Qué diferencia tendría si hago un ping google.com?**

d) Que llamadas genera mi navegador cuando pongo en la barra de direcciones <https://google.com> y doy enter.

# Respuesta Pregunta 5

b

La principal diferencia es la resolución de nombres.

Al hacer ping google.com, el sistema primero realiza una consulta DNS para resolver el nombre de dominio google.com en una dirección IP (por ejemplo, 8.8.8.8).

Luego, se envía el paquete ICMP Echo Request a la dirección IP resultante. En cambio, al hacer ping 8.8.8.8, se omite la resolución DNS porque se utiliza directamente una dirección IP.

# Pregunta 5

Capas TCP e identificación

---

Referente al protocolo TCP/IP

a) Explique cómo se lleva a cabo la identificación de:

- La aplicación a la que va dirigido el paquete
- El nodo de red al que va dirigido el paquete
- La tarjeta de red

b) ¿Qué tipo de paquete generaría la llamada ping 8.8.8.8?

c) ¿Qué diferencia tendría si hago un ping google.com?

d) **Que llamadas genera mi navegador cuando pongo en la barra de direcciones <https://google.com> y doy enter.**

# Respuesta Pregunta 5

d

---

## Llamadas Generadas:

- **Resolución DNS:** El navegador realiza una consulta DNS para convertir el nombre de dominio google.com en una dirección IP.
- **Establecimiento de Conexión TCP:** El navegador establece una conexión TCP con el servidor web de Google en el puerto 443 (HTTPS).
- **Negociación TLS/SSL:** Se realiza un handshake TLS/SSL para establecer una conexión segura y cifrada.
- **Solicitud HTTP:** El navegador envía una solicitud HTTP GET al servidor para obtener la página web.
- **Recepción de la Respuesta:** El servidor web de Google envía la respuesta HTTP, que contiene el contenido de la página solicitada.

Al ser https el http request viaja encriptado por el protocolo TLS.

Estos pasos permiten al navegador acceder y mostrar el contenido de la página web de forma segura.

# Pregunta 6

DNS

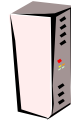
Teniendo el siguiente escenario:

Cache local:  
Google.com 142.250.184.174



Servidor DNS: 80.58.61.250

80.58.61.250



## Registro DNS

Google.com IN A 142.250.184.174  
example.com. IN A 192.0.2.1  
www.example.com. IN A 192.0.2.1  
mailserver.example.com. IN A 192.0.2.2



## Registro DNS

...  
iei.ua.es IN A 193.145.235.30  
...

- Si desde un navegador del cliente se solicita la página <https://iei.ua.es>, ¿qué pasos y llamadas haría el servicio DNS?
- Define los siguientes conceptos: espacio de nombres, dominio, dominio raíz, dominio de primer y segundo nivel, zonas y subdominios.
- ¿Qué protocolo de transporte utiliza DNS y por qué?

# Respuesta Pregunta 6

a

Se introduce **https://iei.ua.es** en el navegador:

Cache local:

Google.com 142.250.184.174

**Registro DNS**

Google.com IN A 142.250.184.174

example.com. IN A 192.0.2.1

www.example.com. IN A 192.0.2.1

mailserver.example.com. IN A 192.0.2.2

**Registro DNS**

...

iei.ua.es IN A 193.145.235.30

...

1. El navegador primero busca en su caché local.
2. Como no lo encuentra envía una consulta al servidor DNS configurado en el sistema (80.58.61.250 -Movistar).
3. No lo encuentra, por lo que pasa la consulta al servidor raíz (198.41.0.4).
4. El servidor raíz detecta que es **.es** y lo envía al servidor de la zona **.es** (194.69.254.1)
5. El servidor **.es** detecta que es **.ua** y lo envía al servidor de la zona **.ua** (193.145.233.6) donde sí que se encuentra la IP del dominio solicitada
6. Finalmente, se devuelve la dirección IP correspondiente al cliente, que utiliza esa IP (193.145.235.30) para conectarse al servidor web del departamento.

# Pregunta 6

DNS

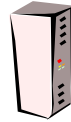
Teniendo el siguiente escenario:

Cache local:  
Google.com 142.250.184.174



Servidor DNS: 80.58.61.250

80.58.61.250



## Registro DNS

Google.com IN A 142.250.184.174  
example.com. IN A 192.0.2.1  
www.example.com. IN A 192.0.2.1  
mailserver.example.com. IN A 192.0.2.2

## Registro DNS

...  
iei.ua.es IN A 193.145.235.30  
...

- Si desde un navegador del cliente se solicita la página <https://iei.ua.es>, ¿qué pasos y llamadas haría el servicio DNS?
- Define los siguientes conceptos: espacio de nombres, dominio, dominio raíz, dominio de primer y segundo nivel, zonas y subdominios.**
- ¿Qué protocolo de transporte utiliza DNS y por qué?



# Respuesta Pregunta 6

b

---

**Espacio de nombres:** Es una estructura jerárquica que organiza y asigna identificadores (nombres) en un sistema. En el contexto de DNS, el espacio de nombres está organizado en un árbol de dominios que representa la relación entre diferentes nombres de dominio y subdominios.

**Dominio (Domain):** Un dominio es una unidad dentro del espacio de nombres. Es una cadena de caracteres que se utiliza para identificar un conjunto de direcciones IP asociadas a un recurso de la red, como un sitio web. Los dominios están jerárquicamente organizados en el sistema DNS. (ej. iei.ua.es)

**Dominio raíz (Root Domain):** Es el nivel más alto del espacio de nombres DNS y es representado por el símbolo . (punto). El dominio raíz no tiene nombre y actúa como punto de inicio para la resolución de nombres en el sistema DNS. Desde este nivel, se derivan todos los demás dominios.

# Respuesta Pregunta 6

b

**Dominio de primer nivel** (Top-Level Domain - TLD): Son los dominios que se encuentran justo debajo del dominio raíz. Están representados por la última parte del nombre de dominio (por ejemplo, .com, .org, .net, o códigos de país como .es, .mx). Los TLD pueden ser genéricos (gTLD) o de código de país (ccTLD).

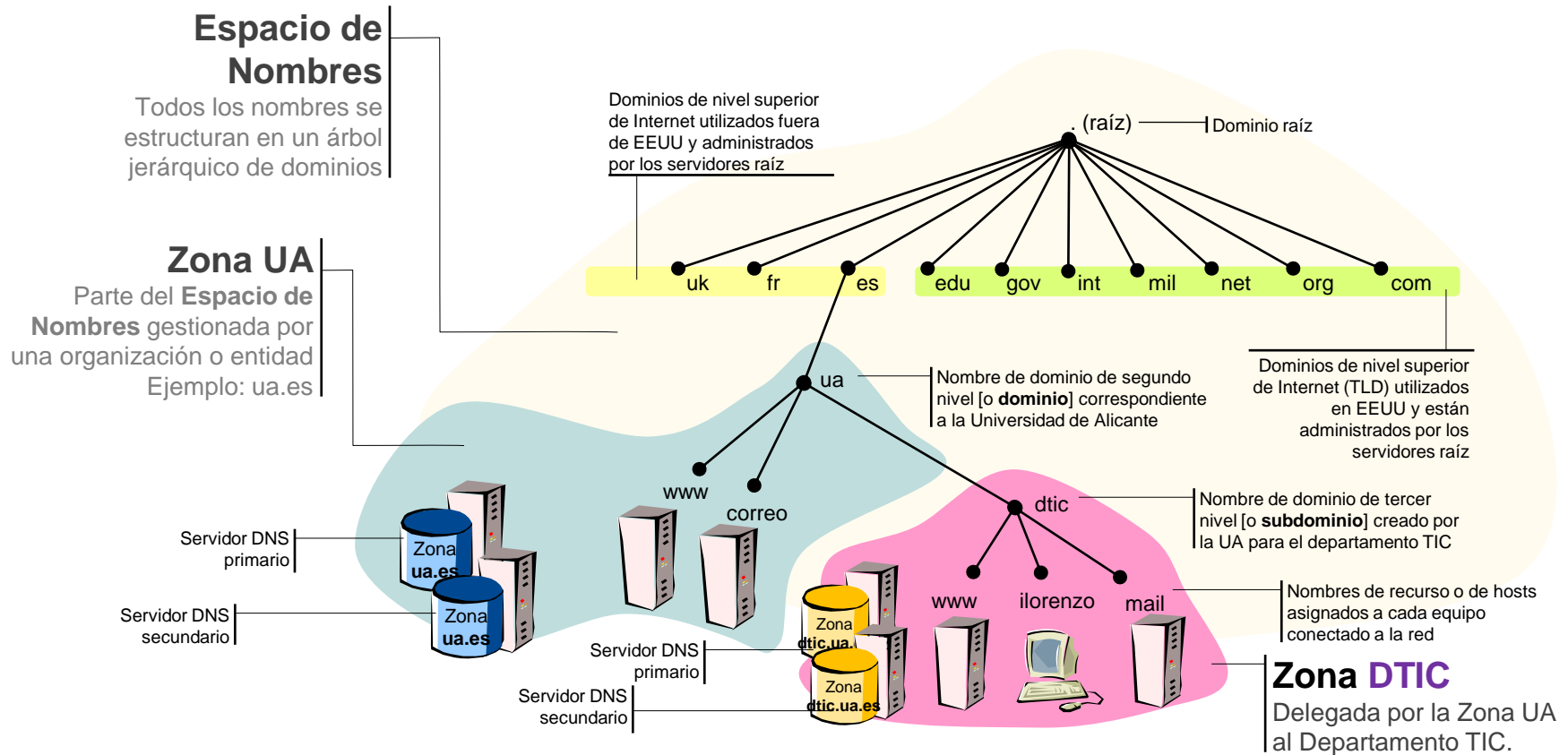
**Dominio de segundo nivel** (Second-Level Domain - SLD): Es el nivel de dominio que está justo debajo del TLD. Por ejemplo, en el nombre de dominio ua.es, “ua” sería el dominio de segundo nivel. Generalmente, es donde se registran los nombres de dominio específicos de una organización o entidad.

**Zonas** (Zones): Una zona DNS es una parte del espacio de nombres que está bajo la administración de un servidor de nombres. Una zona contiene información sobre un dominio y sus subdominios. Una zona puede ser delegada a servidores de nombres autoritativos para esa porción del espacio de nombres.

**Subdominios** (Subdomains): Un subdominio es un dominio que está dentro de otro dominio. Por ejemplo, en iei.ua.es, “iei” es un subdominio de ua.es. Los subdominios pueden ser creados para organizar y administrar diferentes servicios o secciones de un sitio web.

# Respuesta Pregunta 6

b



# Pregunta 6

DNS

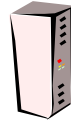
Teniendo el siguiente escenario:

Cache local:  
Google.com 142.250.184.174



Servidor DNS: 80.58.61.250

80.58.61.250



## Registro DNS

Google.com IN A 142.250.184.174  
example.com. IN A 192.0.2.1  
www.example.com. IN A 192.0.2.1  
mailserver.example.com. IN A 192.0.2.2



## Registro DNS

...  
iei.ua.es IN A 193.145.235.30  
...

- Si desde un navegador del cliente se solicita la página <https://iei.ua.es>, ¿qué pasos y llamadas haría el servicio DNS?
- Define los siguientes conceptos: espacio de nombres, dominio, dominio raíz, dominio de primer y segundo nivel, zonas y subdominios.
- ¿Qué protocolo de transporte utiliza DNS y por qué?

# Respuesta Pregunta 6

c

---

El protocolo de transporte utilizado por DNS es **UDP (User Datagram Protocol)**.

La razón principal de su uso es la rapidez, ya que UDP es un protocolo sin conexión que permite enviar consultas y respuestas con un mínimo de sobrecarga. DNS generalmente maneja consultas pequeñas (como la resolución de un nombre de dominio) y puede permitir el uso de UDP debido a su baja latencia y el pequeño tamaño de los paquetes.

# Pregunta 7

Diseño de Redes

---

Si queremos montar una red en nuestra empresa y nos dan el rango de redes 172.16.1.0 con mascara 255.255.255.0:

**a) Dado este rango y máscara de subred 255.255.255.0:**

- ¿Cuántos bits están destinados a la identificación de la red y cuántos a la de los hosts?
- ¿Cuál sería la representación comprimida de la máscara de subred?
- ¿Cuántos nodos (hosts) puede soportar esta red?

**b) Si necesitas dividir esta red en dos redes independientes para dos departamentos, ¿cómo modificarías la máscara de subred para lograrlo?**

- ¿Cuántos nodos podrá tener cada una de las nuevas redes?
- Muestra cómo quedaría el direccionamiento para ambas redes, indicando las direcciones de red, las direcciones de broadcast y los rangos de direcciones IP disponibles para los hosts en cada red

# Respuesta Pregunta 7

a

**Cuántos bits están destinados a identificar la red y cuántos a los hosts:**

La máscara de subred 255.255.255.0 indica que los primeros 24 bits (los tres primeros octetos) se destinan a identificar la red y los últimos 8 bits (el último octeto) a los hosts.

Bits para la red: 24

Bits para los hosts: 8

**Representación comprimida de la máscara:**

La representación comprimida de la máscara de subred 255.255.255.0 es /24, ya que se utilizan 24 bits para la parte de la red.

**Cuántos nodos puede tener la red:**

En una red con máscara /24, hay 8 bits para los hosts. El número máximo de nodos es  $2^8 - 2 = 254$  nodos. Se resta 2 porque uno se reserva para la dirección de red (172.16.1.0) y otro para la dirección de broadcast (172.16.1.255).

# Pregunta 7

Diseño de Redes

---

Si queremos montar una red en nuestra empresa y nos dan el rango de redes 172.16.1.0 con mascara 255.255.255.0:

a) Dado este rango y máscara de subred 255.255.255.0:

- ¿Cuántos bits están destinados a la identificación de la red y cuántos a la de los hosts?
- ¿Cuál sería la representación comprimida de la máscara de subred?
- ¿Cuántos nodos (hosts) puede soportar esta red?

**b) Si necesitas dividir esta red en dos redes independientes para dos departamentos, ¿cómo modificarías la máscara de subred para lograrlo?**

- ¿Cuántos nodos podrá tener cada una de las nuevas redes?
- Muestra cómo quedaría el direccionamiento para ambas redes, indicando las direcciones de red, las direcciones de broadcast y los rangos de direcciones IP disponibles para los hosts en cada red



# Respuesta Pregunta 7

b

Para dividir la red 172.16.1.0/24 en dos subredes, necesitamos "tomar prestados" bits de los 8 bits de hosts. Utilizando 1 bit adicional, podemos crear dos subredes.

La nueva máscara sería 255.255.255.128, que se representa como /25. Esto deja **7 bits** para los hosts en cada subred.

Máscara en binario: **11111111. 11111111. 11111111. 10000000**

Cuántos nodos puede tener cada red:

Con una máscara de /25, quedan 7 bits para los hosts, lo que da como resultado  $2^7 - 2$  = 126 nodos por subred.

# Respuesta Pregunta 7

b

---

Direccionamiento de las dos redes:

## **Primera subred (172.16.1.0/25):**

- Rango de direcciones de hosts: 172.16.1.1 a 172.16.1.126
- Dirección de red: 172.16.1.0
- Dirección de broadcast: 172.16.1.127

## **Segunda subred (172.16.1.128/25):**

- Rango de direcciones de hosts: 172.16.1.129 a 172.16.1.254
- Dirección de red: 172.16.1.128
- Dirección de broadcast: 172.16.1.255

De esta forma, hemos dividido la red 172.16.1.0/24 en dos subredes con máscara /25, y cada subred tiene hasta 126 hosts disponibles.

# Respuesta Pregunta 7

b

172.16.1.0/25

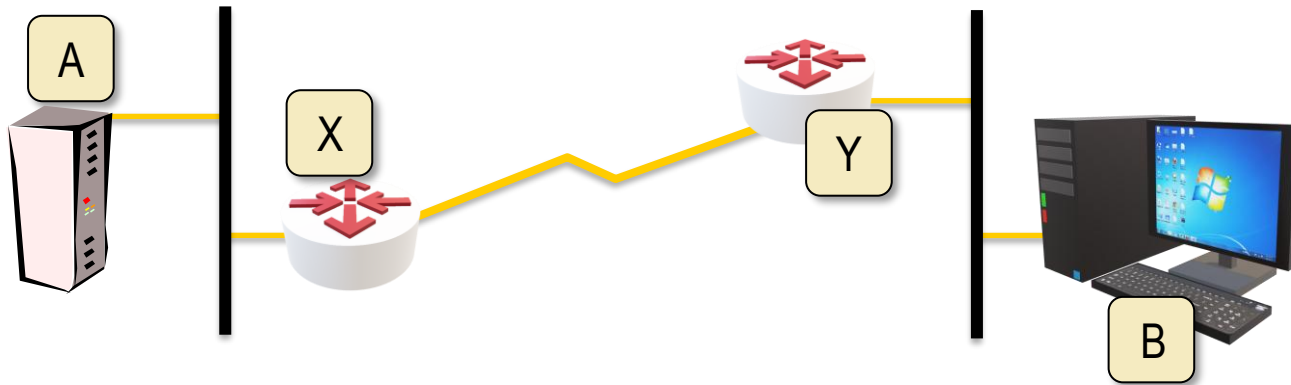
Red	Host			
255.255.255.1	00000000	128		
172.16.1.0	00000000	0	<b>Dir. de Red</b>	<b>Red 0</b>
172.16.1.1	00000001	1	Dir. de Host 1	
172.16.1.2	00000010	2	Dir. de Host 2	
. . .				
172.16.1.61	00111101	61	Dir. de Host 61	
172.16.1.62	00111110	62	Dir. de Host 62	
172.16.1.63	00111111	63	Dir. de Host 63	
172.16.1.64	01000000	64	Dir. de Host 64	
172.16.1.65	01000001	65	Dir. de Host 65	
172.16.1.66	01000010	66	Dir. de Host 66	
. . .				
172.16.1.125	01111101	125	Dir. de Host 125	
172.16.1.126	01111110	126	Dir. de Host 126	
172.16.1.127	01111111	127	<b>Dir. de Broadcast</b>	
172.16.1.128	10000000	128	<b>Dir. de Red</b>	<b>Red 1</b>
172.16.1.129	10000001	129	Dir. de Host 1	
172.16.1.130	10000010	130	Dir. de Host 2	
. . .				
172.16.1.189	10111101	189	Dir. de Host 61	
172.16.1.190	10111110	190	Dir. de Host 62	
172.16.1.191	10111111	191	Dir. de Host 63	
172.16.1.192	11000000	192	Dir. de Host 64	
172.16.1.193	11000001	193	Dir. de Host 65	
172.16.1.194	11000010	194	Dir. de Host 66	
. . .				
172.16.1.253	11111101	253	Dir. de Host 125	
172.16.1.254	11111110	254	Dir. de Host 126	
172.16.1.255	11111111	255	<b>Dir. de Broadcast</b>	

# Pregunta 8

## enrutamientos

---

Teniendo en cuenta el siguiente escenario:



Desde el ordenador B un navegador web con un socket en el puerto 12678 quiere enviar un mensaje http en su versión segura, al servidor A.

Muestre los distintos datagramas que llegan y salen de los dispositivos B, Y, X y A.

Identifique las tramas que representa entregas directas e indirectas

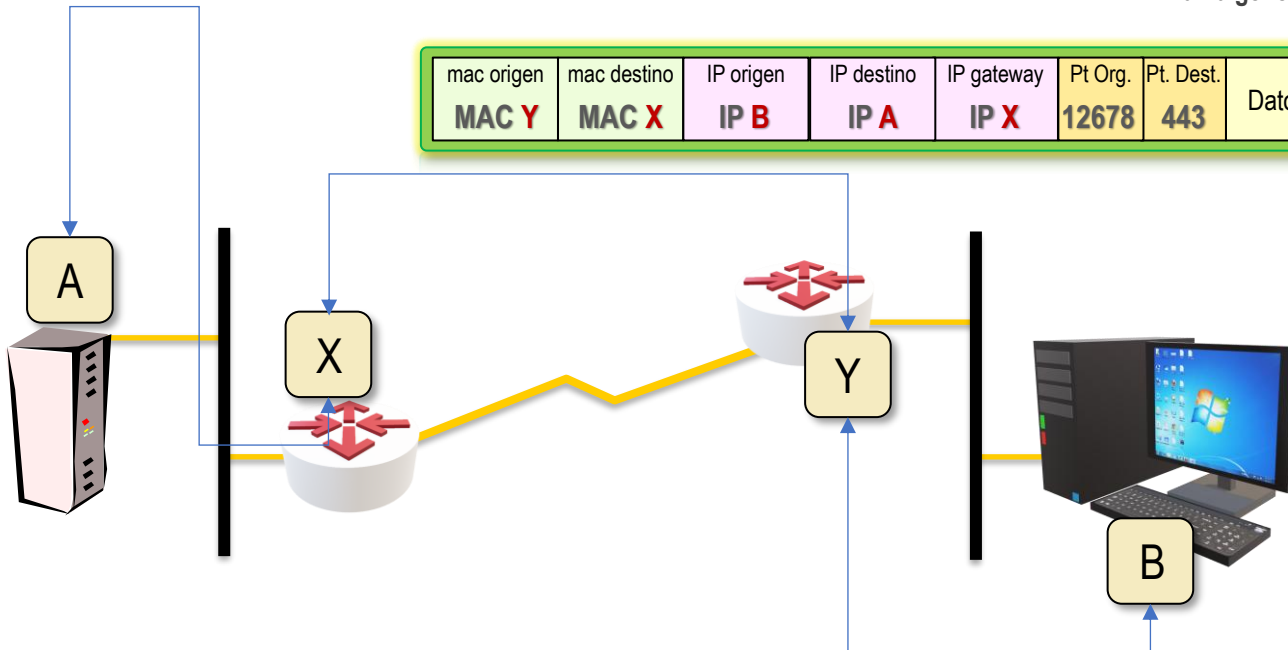
# Respuesta Pregunta 8

Trama generada por X

mac origen	mac destino	IP origen	IP destino	IP gateway	Pt. Org.	Pt. Dest.	Datos Aplicación	CRC
MAC X	MAC A	IP B	IP A	---	12678	443		

Trama generada por Y

mac origen	mac destino	IP origen	IP destino	IP gateway	Pt. Org.	Pt. Dest.	Datos Aplicación	CRC
MAC Y	MAC X	IP B	IP A	IP X	12678	443		



mac origen	mac destino	IP origen	IP destino	IP gateway	Pt. Org.	Pt. Dest.	Datos Aplicación	CRC
MAC B	MAC Y	IP B	IP A	IP Y	12678	443		

Trama generada por B

# Respuesta Pregunta 8

---

mac origen	mac destino	IP origen	IP destino	IP gateway	Pt Org.	Pt. Dest.	Datos Aplicación	CRC
MAC B	MAC Y	IP B	IP A	IP Y	12678	443		

Trama de salida de B y entrada a Y  
Indirecta

mac origen	mac destino	IP origen	IP destino	IP gateway	Pt Org.	Pt. Dest.	Datos Aplicación	CRC
MAC Y	MAC X	IP B	IP A	IP X	12678	443		

Trama de salida de Y y entrada a X  
Indirecta

mac origen	mac destino	IP origen	IP destino	IP gateway	Pt Org.	Pt. Dest.	Datos Aplicación	CRC
MAC X	MAC A	IP B	IP A		12678	443		

Trama de salida de X y entrada a A  
Directa, no necesita gateway

# Sistemas Operativos y Distribuidos

Iren Lorenzo Fonseca  
iren.fonseca@ua.es



TEMA 2. Fundamentos de Redes de Computadores.  
Ejercicios