1)

a.

En resumen, la MTU determina el tamaño máximo de transmisión de una PDU.

El mecanismo de fragmentación consiste en dividir una PDU en fragmentos más pequeños para que pueda ser transmitida. Esto se realiza en el sistema de origen. Cada PDU fraccionada utilizará los siguientes campos de la cabecera IP: ID (identificador compuesto por las direcciones de origen y destino), Longitud, Offset (desplazamiento, representa la longitud de un fragmento en múltiplos de 64 bits y se utiliza para ordenar los datos de forma correcta en el sistema destino) y el indicador de más datos. El procedimiento para fragmentar una PDU es el siguiente:

* Se crean dos nuevas PDU y se copia la cabecera de la PDU original en ambas.
* Se dividen los datos en dos partes aproximadamente iguales, con límites de 64 bits, y se sitúa una en cada PDU nueva.
* En la primer PDU nueva se establece la longitud de los datos insertados en ella y se establece el indicador de más datos en 1 (indicando que hay fragmentación y se debe esperar otra PDU). El campo desplazamiento queda en 0.
* En la segunda PDU se repite el paso previo para la longitud de los datos y se actualiza el campo desplazamiento. A este se le suma la primera porción de los datos dividida por 8.
* Si los datos siguen superando la MTU, se repite el proceso para la PDU que corresponda.

En contraparte, la PDU deberá reconstruirse en el sistema de destino para poder recibir la información adecuada. Este proceso se conoce como reensamblado. Se requiere de suficiente espacio en memoria temporal, ya que se almacenarán los datos recibidos en ella hasta que se logre armar una secuencia de datos ordenados.

b.

Si bien puede realizarse este mecanismo en varias capas del modelo OSI, al hablar de entrega no confiable podría mencionarse específicamente en el protocolo IP. Esto quiere decir que se ubicaría en la capa 3 (red) del modelo OSI.

Una forma de resolver este problema es asignar un tiempo de vida a la primer PDU que se reciba y, si este tiempo expira antes de poder reensamblar la PDU completa, se descartan todas las PDU fragmentadas almacenadas en memoria temporal. Otra técnica es hacer esto mismo, pero utilizando el tiempo de vida de la PDU, propio de la cabecera de cada fragmento entrante. Esta responsabilidad recae generalmente en la capa de Transporte, que cuenta con múltiples mecanismos de control de flujo y detección de errores.

2)

Es correcta, pero no está completa.

En IEEE 802.11 se reemplaza el mecanismo de control CSMA/CD por MACA (Multiple Access with Collision Avoidance) o CSMA/CA. Una de sus técnicas para resolver este problema es el uso de las tramas cortas RTS/CTS.

* Request to Send: una estación envía una trama pequeña informando que desea transmitir.
* Clear to Send: si la estación destino está libre, responde con una pequeña trama informando que está lista para recibir información.

Ambas tramas se retransmiten a todas las estaciones dentro de los rangos de las estaciones origen y destino, por lo que se van a abstener de transmitir durante ese período de tiempo. Este período de tiempo se denomina IFS (Interframe Space) y se calcula a partir de 3 valores posibles:

* SIFS (short IFS): el más pequeño, para acciones de respuesta inmediatas.
* PIFS (point cordination function IFS): tamaño medio, utilizado en por el controlador central en PCF al emitir un sondeo.
* DIFS (distributed coordination function IFS): el más grande, utilizado como retardo mínimo para tramas asíncronas que compiten por el acceso al medio.

También se utiliza una trama de datos ACK para confirmar que se recibieron los datos correctamente.

3)

a.

El mecanismo de encapsulamiento consiste en que cada capa agregue información de control pertinente para establecer una comunicación con el sistema de destino. Además, abstrae a las capas superiores de recibir información que no necesitan.

**Capa de aplicación**

El usuario interactúa con un sitio web dentro del navegador. Para poder acceder a ese sitio web hará uso de la caché de este o, en caso de no encontrarse la dirección IP del sitio en la caché, deberá realizar la consulta necesaria a un servidor DNS.

Una vez obtenida la dirección, el navegador formula una solicitud HTTPS, especificando la acción a realizar (en este caso, un GET) y el recurso al que desea acceder (<https://www.gov.ph/>).

Estos datos HTTP son los que pasan a la capa de Transporte. Incluyen también datos de sesión y de cifrado, ya que TCP/IP abarca las capas Aplicación, Presentación y Sesión en la capa de Aplicación.

|  |
| --- |
| Datos HTTPS |

**Capa de Transporte**

Puede utilizar dos protocolos, dependiendo del tipo de conexión:

* TCP
  + Comunicación fiable (servicio orientado a la conexión).
  + Se establece una conexión, se transmite y luego se libera la misma.
  + Se añade una cabecera TCP (denominada segmento) a la información:

|  |  |
| --- | --- |
| Segmento TCP | Datos HTTPS |

* + El segmento TCP contiene la siguiente información:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Puerto origen | | Puerto destino | | | | | | | |
| Nro. de secuencia | | | | | | | | |
| Nro. de confirmación | | | | | | | | |
| Desplazamiento de los datos | Reservado | U  R  G | A  C  K | P  S  H | R  S  T | S  Y  N | F  I  N | Ventana | |
| Suma de comprobación | | Puntero urgente | | | | | | | |
| Opciones + Relleno | | | | | | | | |

* UDP
  + Comunicación no fiable (servicio no orientado a la conexión).
  + Se envía un datagrama de datos y no se garantiza la entrega.
  + Se delega la fiabilidad de los datos a las capas superiores.
  + Se añade una cabecera de control UDP:

|  |  |
| --- | --- |
| Cabecera UDP | Datos HTTPS |

* + La cabecera UDP contiene la siguiente información:

|  |  |
| --- | --- |
| Puerto origen | Puerto destino |
| Longitud | Suma de comprobación |

**Capa de red/internet**

Se utiliza el protocolo IP. Se encarga de encaminar la PDU a través de un sistema de redes hacia su destino. Añade una cabecera de control propia:

|  |  |  |
| --- | --- | --- |
| Cabecera IP | Cabecera UDP | Datos HTTPS |

La cabecera IP contiene la siguiente información (asumiendo el uso de IPV4):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Versión | IHL | Servicios diferenciados | Longitud total | |
| Identificación |  | D  F | M  F | Desplazamiento del fragmento |
| Tiempo de vida | Protocolo | Suma de verificación del encabezado | | |
| Dirección de origen | | | | |
| Dirección de destino | | | | |
| Opciones | | | | |

**Capa de enlace de datos/acceso a la red**

En esta capa se añade una cabecera y una cola a la PDU, formando una Trama.

Se divide en dos subcapas:

* Control de enlace lógico (LLC): relacionada con la transmisión de una PDU entre dos estaciones.
  + Formato de la PDU LLC:

|  |  |  |  |
| --- | --- | --- | --- |
| DSAP | SSAP | Control LLC | Información |

* + El campo DSAP a su vez está compuesto por:

|  |  |
| --- | --- |
| I/G | Valor DSAP |

* + El campo SSAP a su vez está compuesto por:

|  |  |
| --- | --- |
| C/R | Valor SSAP |

* Control de acceso al medio (MAC): método de control de acceso al medio.
  + Formato de la trama MAC:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control MAC | Dirección MAC destino | Dirección MAC origen | PDU LLC | CRC |

El formato de la Trama de Enlace de Datos finalmente queda de la siguiente forma:

|  |  |  |
| --- | --- | --- |
| Cabecera Enlace de Datos | Datos | Cola Enlace de Datos |

El campo datos incluye todas las cabeceras añadidas en capas superiores.

**Capa física**

Se convierten los datos en señales eléctricas y se transmiten por el medio físico.

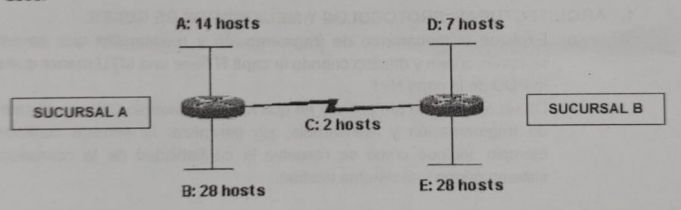
b.

Si, es posible utilizar el mecanismo ARQ con ventanas deslizantes en el caso de utilizar el protocolo TCP. Por ende, se utilizaría en la capa 4.

Se utiliza para la entrega confiable de paquetes.

4.

**Red: 172.16.32.0 /24 [255.255.255.0]**



Utilizo 8 subredes. Esto me permitiría tener 32 hosts por cada subred y utilizaría 3 bits de subred. De esta forma cumplo con todos los requerimientos para las subredes propuestas. La primera queda reservada, se utilizan 5, y sobran 2 para futuros usos. La máscara de red es /27 [255.255.255.224].

* 172.16.32.0 **[Reservada]**
* 172.16.32.32 [A]
* 172.16.32.64 [B]
* 172.16.32.96 [C]
* 172.16.32.128 [D]
* 172.16.32.160 [E]
* 172.16.32.192 [Libre]
* 172.16.32.224 [Libre]

5.

Texto

El contenido generado por IA puede ser incorrecto.

Suponiendo la asignación de redes de la siguiente forma:

* A: 172.16.32.64/28
* B: 172.16.32.0/27
* C: 172.16.32.96/30
* D: 172.16.32.80/28
* E: 172.16.32.32/27

Los /27 son correctos, siguen siendo dos subredes sin la aplicación de VLSM.

La red C es incorrecta. Al tomar un /30 solo podría tener 4 hosts dado que se necesitarían 3 bits extra para determinar la subred. Como puede verse en el ejemplo, utilizaría un rango de direcciones de host de 81 a 94.

La red A es correcta y aprovecha el uso completo de la subred VLSM, ya que se queda sin hosts disponibles.

La red D es incorrecta. Al tomar un /28 con VLSM de la red 172.16.32.80 su rango de direcciones válido es [172.16.32.81 - 172.16.32.94].