# **Alsina**

## **Finales**:

### **2022 09 06**

1. Ventajas y desventajas de segmentar una LAN. ¿Como se hace?

**RTA**:

* **Ventajas**:
  + Aislar el tráfico entre los distintos segmentos.
  + Aumentar el ancho de banda al crear dominios de colisión más pequeños
  + Mejora la seguridad.
* **Desventajas**:
  + Performance ya que se estan agregando más equipos a la red.
* **Formas**:
  + Utilizando un Router.
  + Utilizando un Bridge
  + Utilizando un Switch

1. Ventajas y desventajas de utilizar firma digital.

**RTA**:

* Ventajas:
  + Autenticidad
  + No repudio
  + Integridad
  + Confidencialidad: Solamente si el mensaje que se firma está encriptado
* Desventajas:
  + Una firma se vincula a un único documento.
  + Requiere de una autoridad certificante

1. IP 200.10.10.0. Utilizar 3 bits para la subred. Cantidad máxima de subredes que se pueden tener y cuantos hosts por cada una.

**RTA**:

* Clase C: 8 bits para host.
* Mascara / 27 → 3 bits para subred y 5 para host.
* Cantidad subredes: 6
* Cantidad hosts x subred: 30

1. IP VLSM: 172.21.10.0. Se requieren 3 subredes. Direccionar de la forma más eficiente.
   1. 129 hosts + 12 hosts + 58 hosts

**RTA**:

* Para 129 hosts necesito 8 bits
* Para 58 hosts necesito 6 bits
* Para 12 hosts necesito 4 bits
* Clase B: 16 bits para host.

| **Red** | **ID Red** | **Broadcast** | **Rango direccionable** |
| --- | --- | --- | --- |
| 172.21.10.0 / 24 | 172.21.10.0 | 172.21.10.255 | 1 - 254 |
| 172.21.11.0 / 26 | 172.21.11.0 | 172.21.11.63 | 1 - 62 |
| 172.21.11.64 / 28 | 172.21.11.64 | 172.21.11.79 | 65 - 78 |

1. Como se realiza el direccionamiento IP dinámico. ¿Por que tiene un tiempo limitado y cual es?

**RTA**:

* El direccionamiento dinámico intenta buscar la mejor ruta de entre todas las posibles.
* El protocolo OSPF calcula la ruta a través de las redes que menor costo tenga según la necesidad que declare el usuario.
  + Cada Router debe tener el grafo completo de la red.
* El TTL (Time To Live) es el tiempo (en segundos) que tiene un datagrama para estar en tránsito al destino antes de que se lo descarte.
  + Se utiliza para que una trama que no llega a destino no quede de forma indefinida en la red, ya sea dando vueltas o parado.

1. Se tiene un paquete IP de 5 MB, una red que transmite a 1000 Mbps y un tiempo de acceso a tramas de 9,5 \* (10 ^ -6) segundos. ¿Cuanto tiempo tarda en enviar el paquete?

### **2023 02 22**

1. Consola monitorea red con SNMP. 50 Routers en red Frame Relay. Se envían mensajes con una PDU de 44 Bytes. AR = 256 Kbps, CIR = 128 Kbps, EIR = 64 Kbps. SNMP usa UDP.
2. Frecuencia máxima para sondear dispositivos para que todos los mensajes se manden garantizados
3. Dispositivos máximos que puede sondear (por segundo) sin que rechace.
4. 3 Alternativas para monitorear con la misma estación a 2000 Routers.

**RTA**:

* AR = 256 Kbps.
* CIR = 128 Kbps.
* EIR = 64 Kbps
* Trama = PDU

2) VLSM: IP 10.16.0.0 /22 De la forma más eficiente para:

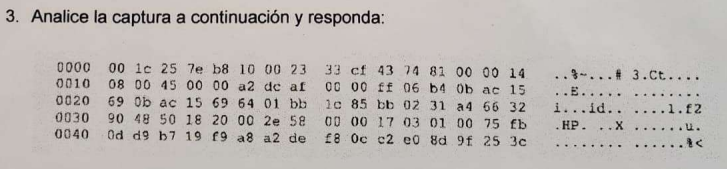
1. 256 Host, 70 Host y 58 Host.

**RTA**:

* Para 256 host direccionables, necesito 9 bits (512)
* Para 70 host, necesito 7 bits (128)
* Para 58 host, necesito 6 bits (64)
* Analizo el 3er y 4to octeto:
  + 0000000|0 . 00000000
  + 00000010 . 0|0000000
  + 00000010 . 10|000000

| Dirección Subred | Máscara | Broadcast Red | Rango Direccionable |
| --- | --- | --- | --- |
| 10.16.0.0 | / 23 | 10.16.1.255 | 10.16.0.1 - 10.16.1.254 |
| 10.16.2.0 | / 25 | 10.16.2.127 | 10.16.2.1 - 10.16.2.126 |
| 10.16.2.128 | / 26 | 10.16.2.191 | 10.16.2.129 - 10.16.2.190 |

3)



1. ¿A que VLAN está dirigida la trama?
2. ¿Que entrada existirá en la cache ARP del remitente? Indicar MAC e IP
3. ¿A que clase pertenecen la dirección IP origen y destino?

**RTA**:

Ethernet:

* Mac Destino: 00 1C 25 7E B8 10
* Mac Origen: 00 23 33 CF 43 74
* VLAN Tag:
  + Ethertype: 81 00
  + Prioridad + CFI: 00
  + VLAN ID: 14 → 20
* Type: 08 → IPv4
* Len: 00

IPv4:

* Versión: 4
* Hlen: 5
* ToS: 00
* Long. Total: 00 A2 → 162
* ID: DC AF
* Flags + Offset: 00 00
* TTL: FF → 255
* Protocolo: 06 → TCP
* Checksum: B4 0B
* IP Origen: AC 15 69 0B → 172.21.105.11
* IP Destino: AC 15 69 64 → 172.21.105.100

TCP:

* Puerto Origen: 01 BB → 443
* Puerto Destino: 1C 85 → 7301
* Nro Seq: BB 02 31 A4
* Nro ACK: 66 32 90 48
* Hlen: 5
* Reservado + Flags: 018
* Window: 20 00 → 8192
* Checksum: 2E 58
* Puntero Urgente: 00 00

1. VLAN ID: 20
2. Al ser una VLAN, no existirá una entrada en la tabla ARP.
3. Ambas pertenece a clase B

4) MTU de 1000 Bytes. Se transmite un segmento TCP de 1460 Bytes.

1. Cuantos fragmentos se crearán si la cabecera IP tiene el bit DF = 1
2. Cuantos fragmentos si tiene DF = 0
3. ¿Quien realiza la fragmentación en caso de ser necesaria y posible?
4. ¿Quien se encarga de reensamblar?

**RTA**:

1. Si el bit DF = 1 y se necesita fragmentar, entonces no se va a crear ningún fragmento, ya que el Router de origen va a cancelar el envío del paquete y enviar un mensaje por ICMP “Destino inalcanzable” con motivo “Fragmentation needed”
2. La cabecera de TCP (Sin opciones) tiene un peso de 20 Bytes. Esta se debe enviar en un fragmento por separado al inicio de la conexión.
   1. Datos: 1460 - 20 = 1440 Bytes.
   2. 1440 / 1000 = 1,44 = 2 Fragmentos.
   3. Se enviarán 3 fragmentos en total.
3. La fragmentación la realiza, en caso de ser necesaria, el router de origen.
4. El reensamblado se realiza en el dispositivo destino ya que debe reunir todos los fragmentos que le fueron enviado y reconstruir el mensaje.

5) ¿Que indica la recepción de un mensaje de “Destino inalcanzable”? Indicar 3 situaciones.

**RTA**:

* Destino inalcanzable es un mensaje del protocolo ICMP que se notifica cuando el datagrama no se puede conmutar o entregar por lo que Router dispara la notificación antes de descartarlo.
* Fragmentation needed: El paquete está marcado como Dont Fragment pero requiere de fragmentación debido a la MTU.
* Network unreachable: No se sabe como conectar a la red.
* Host unreachable: Se conecta a la red pero el host destino no contesta.

6) Delimitación de tramas en HDLC. En que consiste inserción de ceros.

**RTA**:

* HDLC utiliza la secuencia ‘111111’ para indicar el fin de la trama. Para evitar truncar el campo datos y perder información, HDLC tiene el mecanismo de inserción de ceros, el cual, cada vez que detecta la secuencia ‘11111’ inserta inmediatamente un cero después.
  + El receptor del mensaje es el encargado de remover estos ceros insertados para una correcta lectura del mensaje.

## **Parciales**:

### **1er**:

#### **2018 1C**

1. Que pasa cuando se detecta una colisión y que algoritmo lo soluciona.

**RTA**:

* CSMA / CD: Algoritmo que detecta y soluciona colisiones.
  + Cuando detecta, aborta la transmisión y espera un tiempo aleatorio para volver a transmitir.
  + Realiza un sensado permanente del canal.

1. Diferencias y similitudes entre TCP y UDP.

**RTA**:

* **UDP** es un protocolo de capa de transporte, el cual se encapsula sobre IP. Está orientado a la no conexión (no guarda estado), es no confiable (no notifica en caso de descarte), no mantiene el orden y no realiza control de flujo (no tiene un campo ventana).
  + Es más veloz que TCP
  + Su PDU es el User Datagram Protocolo
  + Todos sus problemas deben ser resuelto por las aplicaciones.
* **TCP** es un protocolo de la capa de transporte que se encapsula sobre IP.
  + Orientado a la conexión.
    - Ambos extremos de la conexión mantienen el estado y progreso de la misma.
  + Garantiza entrega en orden.
  + Full duplex.
  + Utiliza confirmación ACK
  + Conmutación de paquetes modo circuito virtual.
  + Su PDU se denomina Segmento.
    - MSS: Tamaño máximo del campo datos en el segmento.
      * Se calcula a partir de la MTU de la interfaz.
      * Se declara al inicio de la conexión.
      * No se permite cambiarlo a lo largo de la conexión.
    - Opciones: Campo que permite realizar optimizaciones en la conexión.
    - Puntero urgente: Campo que indica donde finaliza la secuencia de datos que deben ser entregados con urgencia.
  + Control de flujo: Utiliza ARQ Sliding windows.
    - Separa la confirmación de un mensaje de los datos de otro para poder enviar con mayor capacidad.
    - Se utiliza un sistema de otorgamiento de créditos:
      * Se comienza con un valor inicial y con cada confirmación se va incrementando.
  + Congestión: Puede ocurrir por exceso de la capacidad o por encolar muchos mensajes en el buffer y producir descartes.
    - Utiliza 3 mecanismo para controlarla:
      * Slow Start: Comenzar enviando poca cantidad de mensajes sin confirmación e ir aumentando conforme la red lo permita.
      * Fast retransmit: Si recibe un 3er ACK duplicado, entonces interpreta que se perdió el paquete y retransmite.
      * Fast recovery: Intenta evitar el slow start por pérdida.
  + Control de errores: TCP no utiliza confirmación de rechazo.
    - Se retransmite si no se obtiene un ACK en un tiempo RTO:
      * RTO: Retransmisión Timeout: Tiempo que debe pasar antes de considerar un paquete como perdido y que necesite retransmisión.
      * Si es muy pequeño, se van a producir muchas retransmisiones si hay delay.
      * Si es muy grande, va a tardar mucho en retransmitir cuando haya pérdida.
  + Establecimiento de conexión: Triple handshake:
    - El cliente envía al servidor un msg vacío con el bit SYN (Synchronization) activo.
    - El servidor responde con un msg vacío con el bit SYN (Synchronization) y ACK.
      * Puede incluir Nro secuencia y nro acuse recibo.
    - El cliente envía un segmento ACK.
      * Puede contener o no información.
      * La conexión ya está establecida.

1. En que capa se realiza la multiplexación. Como funciona?

**RTA**:

* La multiplexación se define como el mecanismo que te permite que la información proveniente de diversas fuentes puedan compartir el mismo canal de forma simultanea.
* Se realiza en la capa de transporte.
* Tanto UDP como TCP tienen 2 campos (Puerto origen y destino) de 16 bits cada uno que posibilita esto.

1. Explicar el modo orientado a la conexión y a la no conexión.

**RTA**:

* No conexión: El orden de envío puede o no mantenerse.
  + El encaminamiento es independiente
  + Se utiliza como analogía el correo postal.
* Conexión: Se garantiza entrega ordenada.
  + Se establece, mantiene y libera la conexión una vez finalizado.
  + Se utiliza como analogía un tubo.

### **2do**:

#### **2018 1C**

1. Explicar capas ATM y sus funciones.

RTA:

* El modelo ATM implementa Capa 1 y parcialmente capa 2 del modelo OSI.
* **Capa física**:
  + **Subcapa física**:
    - Medio físico: Define funciones de control para el medio físico.
      * Formato de cables, conectores, etc.
    - Convergencia de Tx:
      * Independiza la velocidad del flujo de las celda de la interfaz física.
      * Sincronización de celdas.
      * Conversión de flujo de celdas a flujo de bits.
  + **ATM**:
    - Multiplexación.
    - Armado de celdas
    - Agregar / sacar encabezado.
    - Control de congestión.
    - Ruteo en UNI.
* **Capa AAL**:
  + **Segmentación / Ensamblado:**
    - De la información de las capas superiores.
    - Manejar frames con un tamaño mayor a la longitud de una celda.
    - Adaptar la información a 48 B
  + **Convergencia**:
    - Independizarse de los protocolos superiores.
    - Identificar los mensajes
    - Recuperar la señal de reloj.

1. Definición de FRAD

**RTA**:

* Es un dispositivo de acceso a la red Frame Relay
  + Es un CPE: Equipo de terminal del abonado.

1. En Frame Relay, que protocolos de usuario y de control se usan?

**RTA**:

* Tanto para el usuario como para el control se utilizan:
  + LAPF Core: Provee mecanismo de control de errores y flujo.
  + LAPD: Controla el enlace datos para el canal que transporta información de control y señalización.

1. Que es ICMP.
   1. ¿Cuando se produce destino inalcanzable?
   2. ¿Quien es emisor y quien es receptor?

**RTA**:

* ICMP (Internet Control Message Protocol) es un protocolo que se encapsula sobre IP que provee mecanismo para salvar los problemas del protocolo IP (Errores de red o eventos inesperados)
  + Solamente notifica del evento o error.
    - No provee una solución
  + Destino inalcanzable es uno de los mensajes que provee el protocolo e indica cuando no se puede conmutar o entregar un datagrama.
    - El router es quien notifica antes de descartarlo.
    - El cliente es quien recibe el error.

1. Explicar 3 características de ATM:

**RTA**:

* PDU: Celda. Tiene un tamaño fijo de 53 Bytes.
  + Su pequeño tamaño hace más rápido el procesamiento y requiere un menor buffer.
  + Su cabecera tiene 5 Bytes.
    - HEC: Campo que realiza un control de errores sobre la cabecera.
      * Si hay error en 1 bit, lo soluciona.
  + MTU: 48 Bytes.
* Asincronismo:
  + Las celdas se procesan en modo sincrónico.
  + No se realiza sincronismo respecto de ningún usuario.
  + Tráfico en rafagas: La asignación de la posición en el flujo es bajo demanda.
* Transparente: Permite transportar cualquier secuencia de bits.

1. ¿Que es IP SEC? En que capa funciona y cuales son los modos.

RTA:

* IP SEC (IP Security) es un conjunto de protocolos de seguridad que permiten agregar encriptación y autenticación en la comunicación.
  + Funciona en capa Red (3)
  + **Modos**:
    - Transporte: No protege la información de IP.
    - Túnel: Protege toda la información.
      * Es más costoso.

1. Definir BE, BC, TC, CIR, EIR, NNI, UNI:

RTA:

* TC: Intervalo de medición. En segundos.
* BC: Tamaño comprometido de rafaga. En bits.
* BE: Tamaño en exceso de rafaga. En bits
* CIR: Velocidad de información comprometida. En bps.
* EIR: Velocidad de información en exceso. En bps
* NNI: Network 2 Network interface.
  + Es interno.
* UNI: User 2 Network interface.
  + Es el punto de ingreso a la red.

# **Echazú**

## **Finales**:

### **2022 07 20**

1. X25, FR y ATM
   1. En cual de ellas está reducido al mínimo la capacidad de control de errores.
   2. Como se denomina la PDU en esta tecnología y que características tiene
   3. En que consiste el control de errores en esta tecnología y como se lleva a cabo.

**RTA**:

1. ATM Tiene la menor capacidad de control de errores, ya que el único control es el campo HEC en la cabecera de la PDU
2. La PDU de ATM se denomina Celda y tiene un tamaño fijo pequeño (53 Bytes) de los cuales 5 se usan para cabecera y 48 para datos.
3. Se tiene un campo HEC de longitud 1 Byte que realiza control de errores unicamente en la cabecera de la celda.
4. X25, FR y ATM
   1. Que bits están previstos en FR para el control de congestión

**RTA**:

* Se utilizan 2 bits unicamente para notificar congestión, FECN y BECN. El primero indica que hay congestión hacia adelante (Forward) y el último indica que hay congestión hacia atrás (Backwards)

1. LAN
   1. Definir NEXT, en que unidades se mide y que expresión se emplea para su cálculo.
   2. Mencionar las funciones de la capa MAC y LLC

**RTA**:

1. NEXT (Paradiafonía) es un fenómeno que ocurre cuando la señal de un par de cables es tomada por otro par adyacente.
   1. Se mide en DB
   2. Se busca que sea lo más cercana al infinito negativo
   3. NEXT = 10 \* Log (P2 / P1)
2. Capas:
   1. LLC 802.2: Interfaz con capas superiores.
      1. Control de flujo y corrección de errores con ARQ.
      2. Tipos de conexión: Datagrama / Datagrama Confirmado / Modo conexión (lógica)
   2. MAC 802.3: Armado y desarmado de tramas.
      1. Detección de errores.
      2. Control de acceso al medio.

4) FR: AR 2048 kbps, CIR 1024 Kbps, EIR 512 kbps, Tc = 1 seg. Velocidad promedio 768 Kbps. Velocidad pico 1900 Kbps. Trama 6000 Bytes (48 kb)

1. ¿Sirven las condiciones actuales de contratación?
2. Calcular tramas garantizadas, marcadas y descartadas.
3. Especificar nuevas condiciones de contratación.

**RTA**:

* BC = 1024 Kb
* BE = 512 Kb

1. Se necesita que cumpla la condición (Vtx <= CIR + EIR).
   1. 768 lo cumple
   2. 1900 no lo cumple.
2. Garantizadas: 1024 / 48 = 21,33 = 22
   1. Marcadas: 512 / 48 = 10,66 = 11
   2. Rechazadas: (1900 - 1024 - 512) / 48 = 7,58 = 8
3. Las nuevas condiciones de contratación deben ser tal que, al menos, se cumpla la condición (Vtx <= CIR + EIR)
   1. Con un EIR de, al menos, 876 Kbps, se logra que EIR + CIR = 1900

5) Forward Tramas: Red 100BaseT con trama Ethernet (1526B)

**RTA**:

* Vel. Forward = Vtx / Trama
* Vtx = 100 Mbps = 100.000.000 bps
* Trama = 1526 B = 12208b
* VF = 100000000 / 12208 = 8191,34 = 8192 Tramas / seg

6) Segmento TCP de 5000B. MTU 500 B. Datagrama IP sin opciones. Calcular cantidad fragmentos.

**RTA**:

* La cabecera del segmento se envía en un fragmento al principio y tiene un tamaño de 20B
* Los 4800 Bytes restantes de datos se deben dividir según la MTU.
* Se debe redondear para arriba, ya que la información, por más de que no ocupe la totalidad del fragmento, se debe enviar igual.
* Fragmentos Datos = 4800 / 500 = 9,6 = 10 Fragmentos
* Total Fragmentos = 10 (Datos) + 1 (Cabecera) = 11

7) IP: 192.168.1.142 / 26

1. Cantidad subredes
2. A que subred pertenece el host del dato
3. Dirección IP para subred 4 → Host 10
4. Máxima cantidad de hosts x subred
5. Dirección broadcast de la subred 2

RTA:

* Clase C: usa 8 bits para host. De los 8, dos se usan para mascara.

1. Cant. Subredes = 2^2 -2 = 2 subredes
2. 4to Octeto:
   1. 10|001110
   2. Pertenece a la subred 3
3. 4to Octeto:
   1. 11|001010
   2. 192.168.1.202
4. Cant hosts x subred: 2^6 - 2 = 62 hosts.
5. 4to Octeto:
   1. 01|111111
   2. 192.168.1.127

## **Parciales**

### **1er**:

#### **2013 1C 1R**

1. En ARQ, no es necesario operar en Full Duplex en:

**RTA**:

* RQ Inactiva

1. Que mecanismo implementa TCP y UDP para realizar control de flujo.

**RTA**:

* UDP no implementa control de flujo.
* TCP utiliza ARQ Sliding Windows de tamaño variable.
  + Sliding Windows opera en full duplex.
  + Ventana: Cantidad de mensajes que se pueden enviar sin recibir una confirmación.
  + Tamaño variable: El tamaño de la ventana puede cambiar a lo largo de la transmisión dependiendo de varios factores y necesidades.

1. Explicar CSMA / CD.

**RTA**:

* Es un mecanismo de Detección y solución de colisiones (Collision detection).
* Realiza un sensado permanente del canal.
* Puede abortar la transmisión.
* Cuando detecta una colisión, espera un tiempo aleatorio para retransmitir.

1. Contestar breve:
2. Para que se usa el campo de 16 bits de ID en un datagrama.
3. Protocolos de Capa 3 y 4 de TCP/IP orientados a la conexión.
4. Control de errores en un datagrama IP
5. ¿Cual equipo se ocupa de la fragmentación de datagramas IP? ¿Que es la MTU?

**RTA**:

1. Debido a la fragmentación que se realiza en el Router a la hora de enviar un datagrama IP y dado que cada parte puede tener un camino independiente, se requiere un identificador para reensamblarlo cuando llegue a destino.
2. Capa 3: TCP / Capa 4: SCTP.
3. Se realiza detección de errores mediante un Checksum a la cabecera del datagrama IP (Se utilizan 16 bits).
   1. No es CRC
4. El Router es el encargado de la fragmentación.
   1. MTU es el tamaño máximo del campo Datos en el datagrama IP (Maximum Transfer Unit)

#### **2014 1C**

1. En que caso es necesario operar en full duplex en ARQ.

**RTA**:

* RQ Continua, retroceder N
* Cuando la RQ es inactiva, opera en half duplex.

1. Especificar el formato de una trama Ethernet. Explicar el control de errores que hace y sobre que campos aplica.

**RTA**:

* Tiene un tamaño mínimo de 64 Bytes y uno máximo de 1518 Bytes
* El control de errores no se aplica al preámbulo.
* **Trama**:
  + Preámbulo: 2 Bytes.
  + Dirección destino: 6 Bytes.
  + Dirección origen: 6 Bytes.
  + Datos: 46 a 1500 Bytes.
  + FCS: 4 Bytes. Método CRC.

1. Para una LAN de 10 Mbps se indica que el RTT máximo es de 51,2 microsegundos.
   1. ¿Como se obtiene este valor?
   2. ¿Cual es el valor para una red Fast Ethernet?

**RTA**:

* RTT Máximo: Tiempo máximo de ida y vuelta de un mensaje que contempla la ventana de colisión.
* En LAN (Ethernet) la trama mínima tiene un tamaño de 64 Bytes (512 bits)
* Vel. Trans = 10 Mbps
* Vel Trans Fast Ethernet = 100 Mbps.

1. Vel Trans (10 Mbps) = bits / RTT → 10 Mbps = 512 / (51,2 \* 10 ^-6) = 10 Mbps.
2. RTT (Fast Ethernet) → bits / 100 Mbps = 512 / 10 \* 10^7 = 5,12 micro segundos

4) Contestar breve:

1. Para que se usa el campo de 16 bits de ID datagrama
2. Mencionar protocolos de Capa 3 y 4 de TCP/IP son orientados a la conexión
3. Control de errores en un datagrama IP
4. Dominio de colisión
5. Dominio de Broadcast.

**RTA**:

1. Debido a que el encaminamiento de los datagramas es independiente y se fragmenta en el Router, se necesita un identificador para poder volver a reunirlos una vez que todos sean recibidos.
2. Capa 3: TCP.
   1. Capa 4: SCTP: Stream Control Transmission Protocol
3. Se utilizan 16 bits para hacer Checksum y DETECTAR errores en la cabecera del datagrama.
   1. No es CRC
4. Área de la red donde se propagan las colisiones por ocupar el canal de forma simultánea.
   1. Los repetidores y hubs propagan colisiones.
5. Área de la red donde se propagan las tramas de difusiones.
   1. El Router no propaga difusiones.

#### **2014 2C**

1. Cual CRC se utiliza en el protocolo MAC de Ethernet o 802.3

**RTA**:

* Se utiliza CRC 32. No contempla el preámbulo a la hora de hacer la validación

1. Valor de la impedancia característica del coaxil que se usa en LAN 10B5.

**RTA**:

* 50 Ohms. Es un coaxil de tipo grueso

1. IP 153.50.6.27 con máscara /25. Determinar ID subred y dirección broadcast de subred.

**RTA**:

* Clase B: Se usan 16 bits para host y 16 para subred
* De los 16 de host, se van a usar 9 para subred y 7 para host
* ID subred: 153.50.6.0
* Dir broadcast: 153.50.6.127

1. Formas de difusión para IP:

**RTA**:

* Dirigida a una red local.
* Limitada en una red.
* Multidifusión.

1. Que significa que un protocolo orientado al bit tenga “Transparencia en los datos”

**RTA**:

* Permite que el campo datos contenga cualquier secuencia arbitraria de bits.

1. Cual, de los siguientes protocolos, está orientado a la no conexión.

**RTA**:

* UDP. Es un protocolo que no tiene control de errores, no tiene validaciones y no garantiza orden, duplicados, etc. pero es más veloz que TCP.

1. Dada la IP 130.180.20.30. ¿Cual mascara no genera subredes?

**RTA**:

* Clase B: 16 bits para host
* Mascara: 255.255.0.0 /16

1. Cual combinación es correcta para la suite TCP/IP

**RTA**:

* FTP, TCP , IP
* FTP: Capa de aplicación. Protocolo de transferencia de archivos simple con autenticación.
* TCP: Protocolo que reside en capa de transporte.
* IP: Protocolo de capa de red.

#### **2017 1C**

1. Especificar el formato de la trama Ethernet. Indicar el control de errores que hace y sobre que campos.

**RTA**:

* Tamaño mínimo de 64 Bytes para la trama entera.
* Utiliza CRC de 32 bits para realizar control de errores sobre todos los campos menos el preámbulo.
* **Trama**:
  + Preámbulo: 7 Bytes.
  + SFD: Delimitador inicio: 1 Byte.
  + Dirección Origen: 6 Bytes.
  + Dirección Destino: 6 Bytes.
  + Len / Type: 2 Bytes.
  + Datos: 0 - 1500 Bytes.
  + Relleno: Opcional.
  + CRC: 4 Bytes. CRC 32

1. Cual de los siguientes no pertenece a la misma subred con la mascara proporcionada.

* Mascara: /19
* 172.16.66.24
* 172.16.65.33
* 172.16.64.42
* 172.162.63.51

**RTA**:

* Son Clase B: Utilizan 16 bits para host y 16 para red.
* Con la mascara, implica que 3 bits se usan para subred y 13 para host.
* 172.66 permanece igual para todos.
* 3 Octeto:
  + 010|00010
  + 010|00001
  + 010|00000
  + 001|11111
* Los primeros 3 pertenecen a la subred “2” mientras que el ultimo pertenece a subred “1”

1. Se tiene una red (10.1.1.0) con 4 subredes y se prevee un crecimiento de 1 subred por año durante 4 años. ¿Cual es la mascara que más cantidad de host provee con esta configuración?

**RTA**:

* Clase A: Utiliza 8 bits para red y 24 para host.
* Si se tienen 4 subredes y se necesitan 4 más, necesito al menos 4 bits para poder direccionarlas.
* Mascara: 8 bits Clase A + 4 bits para direccionar subredes.
* 255.240.0.0 / 12

1. Una red Clase B se divide en 20 subredes y esperan sumarse 30 más en los próximos años. ¿Que mascara te permite tener, al menos, 800 host por subred?

**RTA**:

* Clase B: 16 bits para red y 16 para host.
* Si se tienen 50 subredes, se necesitan al menos 6 bits (64) para poder direccionarlas
* Si se necesitan al menos 800 hosts, se necesitan al menos 10 bits (1024) para poder direccionarlas.
* Mascara: 16 bits Clase B + 6 bits subred
* 255.255.240.0 / 22

1. IP 192.168.85.129 / 26. Dirección subred y broadcast a la que pertenece al host.

**RTA**:

* Clase C: Usa 8 bits para el host.
* Mascara: /26 → 2 bits para subred y 6 para host.
* 4 Octeto:
  + 10|00001
* Dir Subred: 192.168.85.128
  + 10|000000
* Dir Broadcast Subred: 192.168.85.192
  + 10|111111

1. Contestar breve.
2. Para que se usa el campo 16 bits de ID datagrama.
3. Que protocolo de la suite TCP/IP se debería usar para trabajar en tiempo real
4. Control de errores en un datagrama IP
5. En que consiste Espectro expandido y que variantes tiene.

**RTA**:

1. Debido a la fragmentación que es realizada en los Routers a la hora de encaminar un datagrama IP, se requiere un campo que permita identificar a la hora de ensamblarlo en el destino.
2. Dependiendo lo que se intente priorizar se puede utilizar:
   1. UDP: No tiene validaciones ni controles, por lo que no garantiza que no haya duplicaciones, perdidas, etc. pero provee una mayor velocidad.
   2. TCP: Posee control de errores, ordenamiento, por lo que garantiza mayor confiabilidad en la transmisión pero tiene menor velocidad que UDP.
3. Se realiza control de errores utilizando CRC 32 a todos los campos del encabezado menos al preámbulo y al SFD.
   1. Se valida que la longitud del encabezado esté entre 20 y 64 Bytes.
4. Sirve para que dos personas se puedan comunicar, utilizando un código pseudoaleatorio muy seguro.
   1. Se ensancha el AB en el canal y cuando llega al receptor se expande el ruido.
   2. Resistente a interferencias
   3. Baja detectabilidad
   4. Encriptación
   5. Dos variantes: Secuencia directa y salto de frecuencia.

#### **2018 2C T1**

1. En que consiste MIMO y en que red local se aplica. Explicar ventajas.

**RTA**:

* MIMO permite la conexión de múltiples usuario de entrada y múltiples de salida. Se utiliza en redes WiFi
  + Optimiza la relación entre la señal y el ruido
  + Aumenta la capacidad de transmisión de datos.

1. Especificar trama Ethernet 802.3. Explicar el control de errores que hace y sobre que campos aplica.

**RTA**:

* La trama tiene una longitud mínima de 64 Bytes y una máxima de 1526 Bytes.
* El control de errores CRC 32 no se realiza sobre el preámbulo ni el SFD.
* Trama:
  + Preámbulo: 7 Bytes.
  + SFD: Delimitador de trama: 1 Byte.
  + Dirección origen: 6 Bytes.
  + Dirección destino: 6 Bytes.
  + Longitud datos: 2 Bytes.
  + Datos: 0 - 1500 Bytes.
  + Relleno: Opcional.
  + CRC - 32: 4 Bytes.

1. Contestar brevemente:
   1. Para que se usa el campo de 16 bits de ID Datagrama
   2. En una aplicación en tiempo real, que conviene usar de TCP/IP
   3. Que es Espectro expandido. Cuales variantes tiene. Que tecnología LAN la usa.

**RTA**:

1. Debido a la fragmentación que puede sufrir un datagrama (de ser necesario según la MTU) en el Router, se debe poder identificar el origen de las partes del datagrama para poder ensamblarlo una vez que llega a destino.
2. Dependiendo lo que se priorice:
   1. UDP: Si se prioriza la velocidad, ya que no tiene control de errores, duplicado, retransmisión, pérdidas por lo que convierte en una alternativa veloz pero poco confiable.
   2. TCP: Provee mecanismos de control de errores, flujo, congestión por lo que es más confiable pero tiene menor velocidad.
3. Es una tecnología que permite la comunicación entre dos usuarios utilizando un código pseudoaleatorio.
   1. Tiene dos variantes: Salto de frecuencia y secuencia directa.
   2. Se utiliza en WLAN.

#### **2018 2C T2**

1. Afirmaciones incorrectas de ARQ.

**RTA**:

* Stop And Wait opera en full duplex.
  + Opera en half duplex.
* Sliding Windows opera en half duplex.
  + Opera en full duplex.

1. Especificar formato trama UDP. Detalle nombre de PDU, control de errores y el tipo de servicio de comunicación que establece.

**RTA**:

* No realiza control de errores.
* Está orientado a la no conexión.
* No es confiable.
* PDU: User Datagram: Datagrama de usuario.
* **Trama**:
  + Puerto origen: 2 Bytes
  + Puerto destino: 2 Bytes. Opcional
  + Longitud total: 2 Bytes.
  + Checksum: 2 Bytes.
  + Datos.

1. Dir IP: 192.168.1.142 / 27
   1. Cantidad total de subredes (Sin las prohibidas) y cantidad total de host por subred.
   2. ID subred del dato individualizado y el nro de host.
   3. Dirección broadcast de la subred y de la red.
   4. Dirección a asignar para el Host 12 de la subred 2.

**RTA**:

* Clase C: 8 bits para host.
* Mascara / 27
* bits Host = 8 - 3 = 5
* bits Subred = 3
* 4to Octeto:
  + 100|01110
* Cantidad subredes = 8 - 2 = 6
* Cantidad hosts = 32 - 2 = 30
* Dato individualizado: Subred 4 → Host 14
* Dir broadcast subred: 192.168.1.159
  + 100|11111
* Dir broadcast red: 192.168.1.255
  + 111|11111
  + Todos los bits del host (ya sean subred o host) en 1
* Host 12 de la subred 2: 192.168.1.76
  + 010|01100

1. Contestar brevemente:
   1. Para que sirve el protocolo ARP. Que pasa si se ejecuta el comando arp.
   2. Que mecanismo utiliza 802.11 para la entrega fiable de datos.
   3. Explicar el uso de DNS, sobre que protocolo de transporte trabaja y por que.

**RTA**:

1. El protocolo ARP se utiliza para obtener, a partir de una dirección MAC, la dirección IP de destino.
   1. Si se ejecuta el comando ARP se puede visualizar la tabla ARP actualmente existente en el sistema y permite crear nuevas o editar las que ya esten cargadas.
2. Tiene 2 mecanismos para garantizarlos:
   1. 2 Tramas: ACK + Timeout.
      1. Retransmite de ser necesario.
   2. 4 Tramas: ACK + RTS / CTS
      1. Evita colisiones
3. DNS es un espacio de nombres de dominio. Permite la traducción de dominios a direcciones IP. Trabaja sobre el protocolo de UDP debido a:
   1. El paquete DNS que se envía es sencillo y también lo es la respuesta.
   2. La velocidad del protocolo.

#### **2019 2C T1 y T2**

1. IP 192.100.100.128 / 31. Cantidad de subredes válidas y hosts válidos por subred.

**RTA**:

* Clase C: 8 bits para host.
* Al ser / 31, deja 7 bits para subred y 1 para host.
* Cantidad subredes = 128 - 2 = 126
* Cantidad de hosts: 2 - 2 = 0.
  + No existen hosts válidos ya que uno se utiliza para identificar subred y otro para broadcast.

1. Relacionar conceptos:

**RTA**:

* IEEE 802.11 → WiFi
* IEEE 802.16 → Wi Max
* FH → DS
* WRAN → IEEE 802.22
* IEEE 802.2 → LLC

#### **2020 1C**

1. Segmento TCP de 5000 bytes a través de una LAN con una MTU de 500 bytes. Si el datagrama IP no tiene opciones, ¿Cuantos fragmentos se envían?

**RTA**:

* 11
* 20 Bytes para el encabezado, por lo que necesita un fragmento individual
* Bytes datos = 5000 - 20 → 4980 Bytes
* Fragmentos datos = 4980 / 500 → 9,96 → Se redondea hacia arriba porque se necesita enviar todo → Fragmentos datos = 10
* Total = Fragmento Header + Fragmentos Datos = 1 + 10 = 11

1. ¿Cual combinación de LAN tiene, todas, acceso al medio de forma aleatoria?

**RTA**:

* WiFi + 10B5 + 100BFX

1. Direccionamiento IP:

Dirección: 192.168.1.120

Mascara: 255.255.255.224 / 27

1. Cantidad de subredes que se pueden asociar (sin considerar las prohibidas)
2. Número de la subred que pertenece el host del dato de dirección
3. Máxima cantidad de hosts a direccionar por subred
4. Nro de host individualizado por la IP dato
5. Dirección broadcast de la subred dato
6. ¿Que dirección se debe asignar al host 18 de la subred 5?

**RTA**:

Clase c: Se utilizan 8 bits para el host

Mascara /27 → De los 8 bits, 3 para la subred y 5 para el host

1. Cant subredes = 2^ (bits subred) - 2 = 6
   1. La subred 0 (ID red) y la 7 (broadcast) se sacan
2. 001 → Subred host = 3
3. Cant hosts por subred = 2 ^ (bits hosts) - 2 = 30
4. 11000 → Nro host = 24
5. 011|11000 → Todos los bits del host en 1 → 011|11111 → 192.168.1.127
6. Subred 5 → 101 / Host 18 → 10010 → 10110010 → 192.168.1.178

4) Conexionado que se utiliza en LAN 10B5 es el:

**RTA**:

* Tiene separada la parte controladora de la transceptora.

5) En IEEE 802.11, fiabilidad de tramas se aplica con CSMA / CA

**RTA**:

* Verdadero
* El mecanismo de 4 tramas utiliza Datos + ACK + RTS / CTS y evita colisiones.

6) Secuencia de protocolos TCP/IP correcta

**RTA**:

* TELNET / TCP / IP
* Telnet es un aplicación (capa 7) con autenticación de la suite de TCP (reside en capa 4), la cual se encapsula sobre IP.

7) Afirmación correcta respecto de ARQ Sliding Windows.

**RTA**:

* Tamaño de la ventana puede ser fijo o variable.
* Respecto de la necesidad de la red.

#### **2021 1C**

1. Afirmación correcta de ARQ Stop and Wait

**RTA**:

* Tiene tamaño de ventana 1.
  + Debe esperar confirmación de cada envío.

1. Grupos de tecnologías con acceso al medio de forma aleatoria.

**RTA**:

* Wi Fi + 10B5 + 100 BFX.

### **2do**:

#### **2021 1C**

1. Red Conmutación paquetes Wan: Afirmaciones incorrectas

**RTA**:

* ATM tiene un modelo de 2 capas.

1. Pares de términos que no corresponden a Frame Relay.

**RTA**:

* DE, PAD: PAD (Packet Assembler Disassembler) es un componente de WAN X 25.
* LC y VC, Nivel 3: Frame Relay es un protocolo de capa de enlace (2)
* Celda, FECN: Celda se utiliza en el protocolo ATM
* Multiplexión, VPI: VPI (Virtual Path ID) se utiliza para la conmutación en ATM

1. Asociaciones incorrectas.

**RTA**:

* AAL1 - MPLS: AAL1 es un subcapa dentro del protocolo ATM.

1. Afirmación correcta.

**RTA**:

* ATM opera en conmutación de paquetes modo VC.

1. Afirmaciones correctas sobre MPLS.

**RTA**:

* Realiza agrupación de bloques con los mismos atributos constituyendo un FEC.
  + Forward Equivalent Class.
* Las etiquetas las aplican los LSR externos.
  + Al ingresar a la red. Durante el viaje interno solo se analiza la misma y al salir de la red se remueve dicha etiqueta.

1. Ejercicio Frame Relay. AR E1, CIR = 50% AR, EIR = 50% CIR, Tramas de 9600 bits, Velocidad de 1600 kbps, TC = 0,1seg. Hallar BC,BE y tramas garantizadas, rechazadas y con descarte.

**RTA**:

* AR E1 = 2048 Kbps
* CIR = 1024 Kbps
* EIR = 512 Kbps
* Trama = 9600 bits = 1200 B
* V puerto = 1600 Kbps \* 0,1 seg = 160 Kb
* BC = CIR \* TC = 1024 \* 0,1 = 102,4 Kb
* BE = EIR \* TC = 512 \* 0,1 = 51,2 Kb
* Tramas garantizadas = BC / Long trama = 102,4 / 1,2 = 85.33 = 86
* Tramas descarte = BE / Long trama = 51,2 / 1,2 = 42,33 = 43
* Tramas rechazadas = (V puerto - BC - BE) / Long trama = (160 - 102,4 - 51,2) / 1,2 = 5,33 = 6

1. La firma digital provee:

**RTA**:

* No repudio.
* Autenticidad.
* Integridad.
* Encriptación (Solo si el mensaje que firma lo tiene)

1. HDLC: Que método utiliza para que la bandera no sea interpretada como delimitador dentro del campo datos.

**RTA**:

* Inserción de ceros: Cuando se detecta la combinación “11111” se inserta un cero posterior a la secuencia para evitar que se trunque. Remover este cero es responsabilidad del receptor cuando recibe el mensaje.

1. Una comunicación entre redes LAN requiere el nivel de servicio:

**RTA**:

* ABR: Available Bit Rate.
  + Reserva con el conocimiento del AB necesario.
  + Se transmite por ráfagas.

# **Cicerchia / Mansilla**

## **Finales**:

### **2023 02 15**

<https://www.utnianos.com.ar/foro/tema-redes-final-febrero-2023-15-2-2023>

1. Red 192.168.1.0 / 24. Usar VLSM para definir una subred de 67 hosts y una de 12 hosts de la forma más eficiente.

**RTA**:

* Para direccionar 67 hosts necesito 7 bits (128)
* Para direccionar 12 hosts necesito 4 bits (16)
* Subred 67:
  + ID Subred: 192.168.1.0
  + Mascara: 255.255.255.128 (/25)
  + Broadcast: 192.168.1.127
  + Rango direccionable: 1 - 126
* Subred 12:
  + ID Subred: 192.168.1.128
  + Mascara: 255.255.255.240 (/28)
  + Broadcast: 192.168.1.143
  + Rango direccionable: 129 - 142

1. Obtener las superredes para implementar CIDR que sumarize:
   1. 192.168.4.0 / 22
   2. 192.168.2.0 / 23
   3. 192.168.0.0 / 23
   4. 192.168.8.0 / 21

**RTA**:

* Los primeros 16 bits son iguales para todos.
* 3er octeto:
  + 000001|00
  + 0000001|0
  + 0000000|0
  + 00001|000
* Los primeros 4 bits del 3er octeto coinciden, por lo que la mascara es /20
* Se hace un AND entre la mascara (/20) y cualquier dirección. Los primeros 16 bits quedan iguales y los 4 del 3er octeto son todo 0.
* Dirección Sumarizada: 192.168.0.0 / 20

1. Trama.
2. LAN / WLAN: Indicar arquitectura de Ethernet, capas, subcapas y protocolos que se usan para direccionar y control de flujo.

**RTA**:

* Capa física: Codificación y decodificación.
  + Generación y eliminación del preámbulo.
  + Transmisión y recepción de bits.
* Capa de enlace:
  + LLC 802.2: Interfaz con capas superiores.
    - Control de flujo y corrección de errores con ARQ.
    - Tipos de conexión: Datagrama / Datagrama Confirmado / Modo conexión (lógica)
  + MAC 802.3: Armado y desarmado de tramas.
    - Detección de errores.
    - Control de acceso al medio.
* Capa de Red: Asignación del preámbulo.
* Control de flujo: ARQ Sliding Windows.
  + Posee un tamaño de ventana (fijo o variable) que indica la cantidad de mensajes que se pueden enviar sin recibir confirmaciones.
  + Opera en full duplex.
* Acceso al medio: CSMA / CD.
  + Detecta y resuelve colisiones.
  + Realiza un sensado permanente del canal.
  + Frente a una colisión puede abortar.
  + Espera un tiempo aleatorio para retransmitir.

1. Mecanismo que utiliza IEEE 802.11 (Wi Fi) para el acceso distribuido al medio.

**RTA**:

* Utiliza CSMA / CA
  + Utiliza técnicas de evasión de colisiones.
  + No sensa de forma permanente
  + Cuando evade una colisión espera un RTT max para intentar transmitir

1. Que utiliza TCP para lograr multiplexación.

**RTA**:

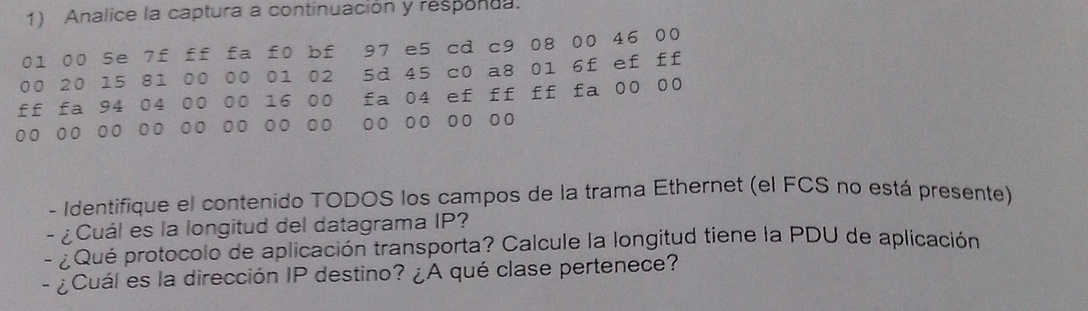
* Multiplexación es un mecanismo que permite que información proveniente de diversos fuentes pueda circular por el mismo canal en simultaneo.
* En TCP se tiene 2 campos en la cabecera para el Puerto origen y destino (16b c/u)

# **Koval**:

## **Finales**:

### **2014 07 30**

1. Trama



**RTA**:

Ethernet:

* Mac Destino: 01 00 5E 7F FF FA
* Mac Origen: F0 BF 97 E5 CD C9
* Protocolo: 08 → IPv4
* Len: 00

IPv4:

* Versión 4
* HLEN: 6
* ToS: 00
* Long Total: 00 20
* ID: 15 81
* Flags + offset: 00 00
* TTL: 01
* Protocolo: 02
* Checksum: 5D 45
* IP Origen: C0 A8 01 6F → 192.168.1.111
* IP Destino: EF FF FF FA → 239.255.255.250

1. El campo Long Total es 20 en Hexa = 32 Bytes
2. Tiene el código 02 que es IGMP. PDU
3. IP Destino: EF FF FF FA → 239.255.255.250 → Clase D

2) IP Clase A. Se usan 11 bits para subredes.

1. Mascara resultante.
2. Cuantas subredes se pueden armar como máximo
3. Dirección para subred 160, host 261
4. Dirección de broadcast de la subred 170
5. Dirección más baja dentro de la subred 170.

**RTA**:

* Utilizo 1.0.0.0
* 11 bits para subred y 13 bits para host (/19)

1. Mascara: 255.255.224.0 (/19)
2. 2^11 - 2 = 2046 Subredes.
3. Analizo 2do, 3er y 4to octeto
   1. 00010100.000|00001.00000101
   2. 1.20.1.5
4. Analizo 2do, 3er y 4to octeto:
   1. 00010101.010|11111.11111111
   2. 1.21.95.255
5. Analizo 2do, 3er y 4to octeto:
   1. 00010101.010|00000.00000000
   2. Si es la mínima de la red es 1.21.64.0
   3. Si es la mínima direccionable es 1.21.64.1

3) FR. AR 768 Kbps. CIR 384 Kbps. EIR 192 Kbps. Trama 9,6 Kb. Velocidad 800 Kbps. TC

1 Seg.

**RTA**:

* CIR = BC / TC → BC = 384 Kb.
* EIR = BE / TC → BE = 192 Kb.
* Garantizadas = BC / Trama → Garantizadas = 40
* Descarte = BE / Trama → Descarte = 20
* Rechazo = (Vtx \* TC - BC - BE) / Trama = 23,33 = 24

4) Definición de control de flujo. Explicar el mecanismo en TCP y que campos de la cabecera intervienen.

**RTA**:

* El control de flujo es un mecanismo de gestión de tráfico entre transmisor y receptor de una comunicación.
* TCP implementa ARQ (Requerimiento automático de repetición) en su versión Sliding Windows. Esta versión se utiliza en conexiones full duplex y tiene el concepto de Ventana (Cantidad de mensajes que se pueden enviar sin recibir una confirmación).
  + Dicha ventana puede ser fija o variable a lo largo de la transmisión.
* TCP utiliza el Otorgamiento de créditos, que implica que, al establecerse la conexión, se asigna una cantidad de bytes que se está dispuesto a recibir de dicha conexión y, conforme avance la misma y lleguen las confirmaciones, el mismo se puede ir actualizando.
  + En la cabecera TCP está el campo Window (16 bits) que indica la cantidad de Bytes que está dispuesto a recibir.

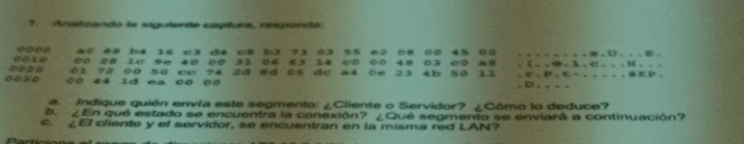
5) Formato de celda ATM. Explicar HEC.

**RTA**:

* La PDU del protocolo ATM se denomina Celda. La misma tiene un tamaño fijo de 53 bytes, lo que garantiza un procesamiento mas simple y un buffer necesario mas pequeño.
* La cabecera de ATM ocupa 5 Bytes, por lo que la MTU es de 48 Bytes.
* La cabecera varía dependiendo si es una interfaz NNI (Network to Network - Interna) o UNI (User to Network Interface - Puerta de acceso de los usuarios)
  + UNI:
    - GFI: 4 bits
    - VPI: 8 bits
    - VCI: 16 bits
    - Payload Type: 3 bits
    - Prioridad: 1 bit
    - HEC: 8 bits.
  + NNI:
    - VPI: 12 bits
    - VCI: 16 bits
    - Payload Type: 3 bits
    - Prioridad: 1 bit
    - HEC: 8 bits.
* El campo HEC (Header Error Check) se encarga de verificar que la cabecera no tenga errores. En el caso de que haya UNICAMENTE 1 bit de error, lo puede corregir. Si hay mas de 1 bit erroneo, se descarta la celda

### **2015 02 11**

1. Trama



**RTA**:

Ethernet:

* MAC Destino: A0 6B B4 16 C3 D4
* MAC Origen: C8 B3 73 03 55 E2
* Type: 08 → IPv4
* Len: 00

IPv4:

* Versión: 4
* Hlen: 5
* ToS: 00
* Longitud total: 00 2B
* ID: 1C 9E
* Flags + offset: 40 00
* TTL: 31
* Protocolo: 06 → TCP
* Checksum: 63 14
* IP Origen: C0 00 48 03 → 192.0.72.3
* IP Destino: C0 A8 01 72 → 192.168.1.114

TCP:

* Puerto Origen: 00 50 → 80
* Puerto Destino: CC 74 → 52340
* Nro Secuencia: 2D 8D 05 DC
* Nro ACK: A4 0E 23 4B
* Hlen: 5
* Reservado + Flags: 0 11
  + 0000 00|010001
  + FIN y ACK
* Window: 00 44
* Checksum: 1D EA
* Puntero Urgente: 00 00

1. Lo envía el servidor con IP 192.0.72.3 ya que tiene el puerto 80, el cual está reservado para HTTP.
2. El segmento tiene el bit FIN activo, lo que indica que el servidor indicó que la conexión debe terminar.
   1. El próximo segmento a recibir será un ACK por parte del cliente.
3. 192.0.72.3 y 192.168.1.114
   1. 11000000.00000000.01001000.00000011
   2. 11000000.10101000.00000001.01110010
   3. Ambos son de clase C y no comparten la Red.

2) VLSM: 172.16.0.0 /23 para tener una red de 129, una de 10 y una de 58.

**RTA**:

* Para una red de 129 host necesito 8 bits (256)
* Para una de 58 necesito 6 bits (64)
* Para una de 10 necesito 4 bits (16)
* Analizo el 3er y 4to octeto:
  + 00000000|.00000000
  + 00000001.00|000000
  + 00000001.0100|0000

| ID Red | Mascara | Broadcast | Rango direccionable |
| --- | --- | --- | --- |
| 172.16.0.0 | 24 | 172.16.0.255 | 172.16.0.1 - 172.16.0.254 |
| 172.16.1.0 | 26 | 172.16.1.63 | 172.16.1.1 - 172.16.1.62 |
| 172.16.1.64 | 28 | 172.16.1.79 | 172.16.1.65 - 172.16.1.78 |

3) SNMP. 50 Routers. PDU capa 7 (44 Bytes). AR 256 Kbps. CIR 128 Kbps. EIR 64 Kbps.

**RTA**:

* Total Trama: Capa 7 + Capa 4 + Capa 3 + Capa 2.
  + 44B + 8B + 20B + 6B = 78B
* Total dispositivos = 50 \* 78 B = 50 \* 624 bits = 31,2 Kb

1. Para sondear sin marcar se debe usar el valor de BC con TC = 1 segundo.
   1. CIR = BC / TC → CIR \* TC = BC → BC = 128 Kb
   2. Frecuencia de Sondeo = 128 Kb / 32,1 Kb = 4,1 = 4 sondeos por segundo.
2. Para que no se descarten, el valor debe ser menor o igual a BC + BE.
   1. BC + BE = 192 Kb
   2. No se que formula usar
3. Se puede aumentar el AR, disminuir el tamaño de trama o monitorear en intervalos de grupos.

4) Explicar DCF para 802.11 y en que se diferencia con PCF.

**RTA**:

* DCF es el acceso al medio de forma distribuida, en el cual todos deben realizar un control.
  + Existe la competencia para poder transmitir.
  + NAV: Indica si el medio está libre para transmitir.
  + Utiliza RTS / CTS.
* PCF es el acceso al medio de forma puntual, en donde se intenta que no sea 100% aleatorio.
  + El AP es el encargado de asignar turnos a los equipos que intentan transmitir.
  + Mientras el AP esté en modo PCF, los equipos no escuchan para transmitir sino para suscribirse a la lista de dispositivos que quieren transmitir.
  + El AP va preguntando a cada uno si quiere transmitir.
  + Al finalizar este modo regresa a DFC.

5) Que función cumple un protocolo de ruteo. En que se diferencia Link State de Vector distancia.

RTA:

* El protocolo de ruteo es un conjunto de reglas para poder enviar un paquete a través de una o más redes.
* Vector distancia es un algoritmo que solo toma en cuenta la menor cantidad de saltos que deben realizarse mientras que Estado de enlace (Link state) toma en cuenta el delay, la confiabilidad del enlace, la distancia y la capacidad.

6) TCP

1. Que mecanismo implementa Window en la cabecera y que longitud tiene el campo.
2. Cual es el credito máximo
3. Existe algún mecanismo para alargarlo
4. Explicar significado de RTO y su uso. Como se calcula y que pasa si se sobreestima o se subestima..

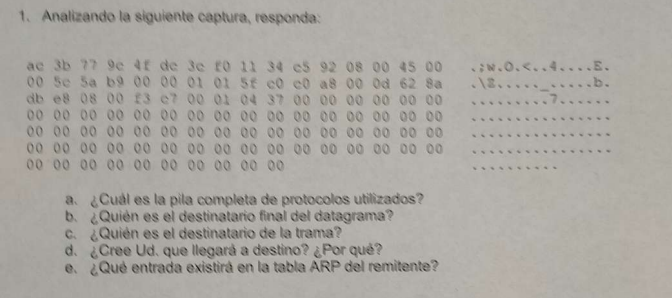
RTA:

1. El campo Window tiene una longitud de 16 bits e indica la cantidad de bytes que está dispuesto a recibir.
2. El crédito máximo es 2^16 - 1 = 65535
3. TCP utiliza el mecanismo de “otorgamiento de créditos” en el cual por cada confirmación ACK este valor puede incrementar.
4. RTO (Retransmission timeout) es el valor que se está dispuesto a esperar sin una confirmación ACK. Una vez cumplido el tiempo, se toma como que el paquete se perdió y se retransmite.
   1. Su valor suele ser similar al RTT (Tiempo entre estaciones) el cual implica el tiempo que tarda un mensaje en ir a destino y volver al origen.
   2. También se puede utilizar el RTT Max que indica el tiempo de un mensaje entre las estaciones más alejadas de una red.
   3. Si se utiliza un valor muy pequeño de RTO, frente a un delay, van a existir muchas retransmisiones.
   4. Si hay un valor muy grande RTO, frente a una pérdida, el receptor va a tardar mucho en retransmitir.

### **2022 04 28**

<https://www.utnianos.com.ar/foro/tema-final-redes-28-04-2022-koval-con-resolucion>

1. Tramas



RTA:

* Siempre arranca con una trama Ethernet, así que se analizan los primeros 14B
* Cuando se analiza IPv4, hay que analizar el campo HLEN: Si es 5, entonces no tiene opciones.

Ethernet:

* Dir MAC Destino: AC 3B 77 9C 4F DC
* Dir Mac Origen: 3C F0 11 34 C5 92
* Type: 08 → IPv4
* Len: 0

IPv4:

* Versión: 4
* Hlen: 5
* ToS: 00
* Long Total: 00 5C → 92
* ID: 5A B9 → 23225
* Flags + Offset: 00 00
* TTL: 01 → 1
* Protocolo: 01 → ICMP
* Checksum: 5F C0
* IP Origen: C0 A8 00 0D → 192.168.0.13
* IP Destino: 62 8A DB E8 → 98.138.219.232

ICMP:

* Tipo: 08 → Echo
* Code: 00
* Checksum: F3 C7
* ID: 00 01
* Nro. Secuencia: 04 37

1. Ethernet | IPv4 | ICMP
2. Destinatario Datagrama: 98.138.219.232
3. Destinatario Trama: AC 3B 77 9C 4F DC
4. Es un mensaje de tipo ECHO y le queda 1 salto de vida (TTL = 1)
5. Se va a crear una entrada en la tabla ARP con la dirección MAC AC 3B 77 9C 4F DC - IP 98.138.219.232
6. Frame Relay: AR 768 Kbps. CIR 50 % AR. EIR 50% CIR. Trama 9600 bits. Velocidad 800 Kbps. TC = 1 seg. Hallar Bc, Be y tramas garantizadas y descartadas.

**RTA**:

* CIR = 384 Kbps
* EIR = 192 Kbps
* Vpue = 800 Kb
* T.Trama = 9600 b
* BC = CIR \* TC = 384 Kb
* BE = EIR \* TC = 192 Kb
* Tramas:
  + Garantizada: BC / T.Trama = 384000 / 9600 = 40
  + Descarte: BE / T. Trama = 192000 / 9600 = 20
  + Rechazadas: (Vpue - Bc - Be) / T.Trama = 224000 / 9600 = 23,33 = 24

1. IP: 162.19.249.114 / 21
   1. A que subred está conectado
   2. Que máscara tiene configurada
   3. Cual es el default gateway
   4. Cuantos hosts vecinos posee como máximo
   5. ¿Se puede hacer subneteo para asignar una red de 1024 y otra de 780 respectivamente?

**RTA**:

* Clase B: Utiliza 16 bits para host.
* De los 16 bits de host, 5 los usa para la máscara de subred.

1. 3er y 4to octeto:
   1. 11111|001.01110010
   2. Dirección subred: 192.19.248.0 / 21
2. Mascara: 255.255.248.0 (/21)
3. El default gateway es el primer host direccionable dentro de la red. En este caso se puede utilizar el 162.19.248.1 / 21
4. Se dejan 11 bits restantes para la asignación de hosts dentro de la subred.
   1. 2 ^ 11 - 2 = 2046 hosts por subred.
   2. Se debe restar uno más ya que no se puede ser vecino de uno mismo
   3. Hosts máximos vecinos = 2045
5. No es posible, ya que para direccionar 1024 hosts se necesita, al menos, 11 bits, que es la mascara completa. Al hacer esto no quedaría espacio para direccionar las 2 redes necesarias.

4) IPV6:

1. Longitud de la dirección.
2. Como se conforma una dirección IPv6
3. Como se identifica el broadcast.

**RTA**:

1. 128 bits.
2. Son ocho campos de 16 bits cada uno separados por “:”. Se dividen en 3 grupos:
   1. ID Ruteo: 48 bits.
   2. ID Subred: 16 bits.
   3. ID interfaz: 64 bits.
3. IPv6 no implementa broadcast pero si implementa multicast, el permite enviar un paquete a todas las interfaces de un grupo.

5) IPSEC:

1. Servicios de protocolos AH y ESP
2. Diferencias entre modo túnel y modo transporte.
3. Variantes de encriptación y hash.

**RTA**:

1. Protocolos:
   1. AH: Authentication Header: Garantiza autenticidad e integridad.
      1. No realiza encriptación del mensaje.
   2. ESP: Encrypted Security Payload: Garantiza autenticidad, integridad y privacidad
2. El modo transporte no encripta la información de IP mientras que túnel encripta todo (pero tiene un mayor costo)

6) Ruteo IP:

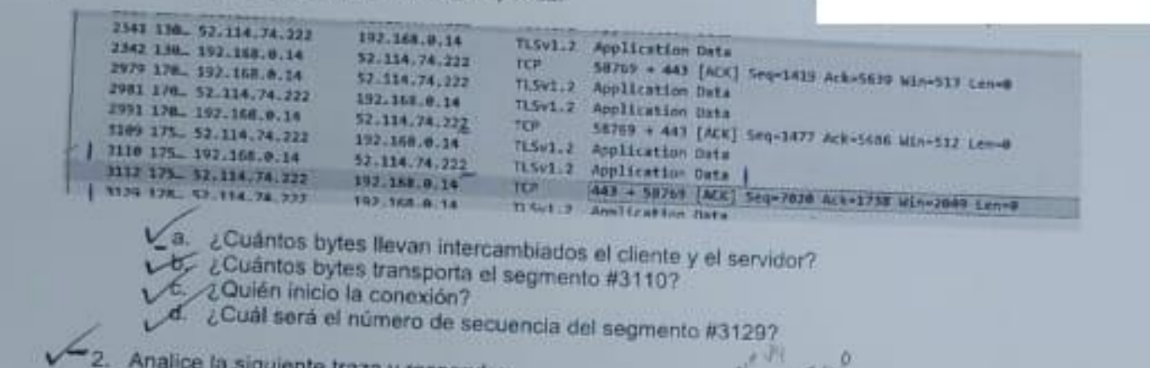
1. ¿Que elementos de información tiene una tabla de ruteo?
2. Diferencias entre Vector-Distancia y Link-state (Estado del enlace)
3. Indicar a que grupo pertenecen los que se utilizaron en el laboratorio.

**RTA**:

1. Se puede visualizar:
   1. Red destino
   2. Máscara
   3. Gateway: Indica el próximo salto a realizar.
   4. Interfaz: Indica el camino por donde va a realizarlo.
   5. Métrica: Cuanto menor sea este número, más recomendable es tomar esa opción si hay más de 1.
2. Son dos formas de obtener el mejor camino:
   1. Vector distancia: Busca en base a la menor cantidad de saltos.
   2. Estado del enlace: Contempla la distancia, el delay, la capacidad y la confiabilidad del enlace.
3. Los del laboratorio utilizan Vector Distancia.

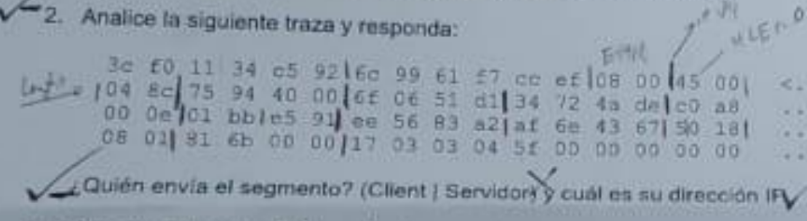
### **2022 08 03:**

1. Tramas.



* Cliente inicia con SEQ = 1419 ACK = 5639 WIN = 517

1. Trama:



RTA:

* Arranca con trama Ethernet y se analiza lo después.
* Como HLEN = 5 en IPv4, no tiene opciones.

Ethernet:

* Mac Destino: 3C F0 11 34 C5 92
* Mac Origen: 6C 99 61 F7 CC EF
* Type: 08 → IPv4
* Len: 00

IPv4:

* Versión: 4
* HLEN: 5
* ToS: 00
* Long Total: 04 8C
* ID: 75 94
* Flags + Offset: 40 00
* TTL: 6F
* Protocolo: 06 → TCP
* Checksum: 51 D1
* IP Origen: 34 72 4A DE → 52.114.74.222
* IP Destino: C0 A8 00 0E → 192.168.0.14

TCP:

* Puerto Origen: 01 BB → 443
* Puerto Destino: E5 91 → ??

1. El origen de la transmisión es la IP 52.114.74.222 con el puerto 443.
   1. 443 es un WKP de HTTPS
   2. Es un servidor
2. Dirección IP Clase A. Se utilizan 11 bits para subred.
   1. Cual es la mascara resultante para las subredes.
   2. Cuantas subredes se pueden armar, como máximo
   3. Cual es la dirección del host 261 de la subred 160
   4. Cual es la dirección de broadcast de la subred 170 y la dirección más baja del host dentro de esa subred.

**RTA**:

* Clase A: Utiliza 24 bits para host.
* De los 24 bits, 11 son para subred y 13 para host.

1. Mascara: 255.255.224.0 (/19)
2. Cantidad de subredes = 2 ^ 11 - 2 = 2046 subredes.
3. Se deben analizar el 2do, 3er y 4to octeto:
   1. 00000000.000|00000.00000000
   2. Se arma el nro 160 en los primeros 11 bits y se arma el nro 261 en los últimos 13.
   3. 00010100.000|00001.00000101
   4. 1.20.1.5
4. Mismo que el anterior:
   1. Se arma el nro 170 en los primeros 11 bits y se pone todos los bits de host en “1” para encontrar el broadcast.
   2. 00010101.01011111.11111111
   3. Broadcast #170: 1.21.95.255
   4. Mínimo Host #170: 1.21.64.1

4) IP:

1. Función del protocolo ICMP. 3 Mensajes del protocolo.
2. Definición de dirección Clase D y para que servicio se utiliza.
3. Que función cumple el campo Offset en la cabecera IP.

**RTA**:

1. Internet Control Message Protocol:
   1. Provee mecanismos para comunicar problemas del protocolo IP tales como errores de red o eventos inesperados.
   2. Solo informa errores pero no provee una solución
   3. Mensajes:
      1. Echo Request / Reply.
      2. Destino inalcanzable
      3. Tiempo de espera agotado.
2. Son direcciones que se reservan para multidifusión.
   1. No tiene máscara ya que no se utiliza para conectar hosts.
   2. Comienza en el 224.0.0.0
3. Ayuda a reordenar los datagramas que fueron enviados gracias a la fragmentación realizada en el Router origen.

5) MPLS:

1. Dispositivos encargados de retirar e insertar etiquetas.
2. En que capa del modelo OSI opera
3. Como se distribuye la información de etiquetas dentro de una red MPLS.

**RTA**:

1. Los LSR de tipo EDGE son los puntos de ingreso y egreso de una red MPLS.
   1. Los mismos se encargan de, cuando intenta ingresar, asignar una etiqueta.
   2. Al salir de la red, se remueve la etiqueta dejando intacto el paquete original.
2. Opera entre la capa 2 y 3 (Enlace y red respectivamente)
3. Debido a que la asociación de información tiene un significado local unicamente, dicha asociación se intercambia entre los LSR internos a través del Label Distribution protocol.

6) TCP:

1. Que son las opciones. Ejemplos.
2. Función del campo Puntero Urgente
3. Que es el RTO. Que pasa si sucede muy rápido.

**RTA**:

1. Es un campo opcional y variable que permite realizar optimizaciones en las conexiones y/o transmisiones.
   1. Uno de los más usados es el MSS, que indica el tamaño máximo del campo datos del segmento TCP
2. Apunta al último byte de la secuencia de datos urgentes.
   1. Indica donde terminan
3. RTO es Retransmission Timeout. Es el tiempo que se espera una respuesta para darle como perdida y retransmitir.
   1. En el caso de que el RTO sea muy chico, se va a retransmitir muchas veces antes de que regrese la confirmación.
   2. Si es muy grande, frente a una pérdida, se tarda mucho en retransmitir.

## **Parciales**:

### **1er**:

#### **2019 1C**

1. Redes LAN:
   1. En que se diferen las tramas Ethernet y 802.3. Como determina el receptor de 802.3 a que capa superior entregar el PDU.
   2. Como se compone una dirección MAC y como es el broadcast.
   3. Como realiza ethernet el control de errores.
   4. Que utilidad tiene el protocolo Spanning Tree y que dispositivos lo ejecutan.

**RTA**:

1. IEEE 802.3 tiene 7 Preámbulo 1 SFD y 2 Longitud de trama. Admite direcciones de 2 o 6 Bytes
   1. Ethernet tiene 8 Preámbulo y 2 Type / Len. Admite solo direcciones de 6 Bytes.
2. Una dirección MAC se compone de 12 números hexadecimales (48 bits) separados en grupos de 2 números por “:”
   1. La dirección Broadcast Mac es FF:FF:FF:FF:FF:FF
3. Ethernet tiene un campo FCS de 4 Bytes en la cabecera que se encarga de hacer detección de errores utilizando CRC - 32 solo a la cabecera, sin contar el preámbulo y el SFD.
4. El protocolo Spanning Tree se encarga de validar que no existan vínculos redundantes en una topología.
   1. Transforma una red física de tipo malla en una red lógica de tipo árbol sin bucles.
   2. Los Switches lo ejecutan.

2) WLAN:

1. ¿En que bandas operan las distintas normas? ¿Que diferencias tienen?
2. ¿Como opera un AP en modo PCF?
3. Cuantas direcciones MAC contiene la cabecera 802.11?

**RTA**:

1. 802.11a opera en 5Ghz mientras que 802.11ac opera en 2,4 y 5 Ghz
2. Un Access Point en modo Centralizado (Puntual - PCF) se encarga de que el acceso al medio no sea 100% aleatorio.
   1. Para esto designa al que tiene el poder de transmitir.
      1. Periódicamente va preguntando a los equipos de la lista si tienen algo para transmitir.
   2. Cada vez que un nuevo equipo se intenta conectar, se le pregunta si se quiere suscribir a la lista de equipos para transmitir.
   3. Luego se vuelve a DFC.
3. Se tienen 4 direcciones MAC:
   1. Dirección 1: Identifica al dispositivo destino.
   2. Dirección 2: Identifica al dispositivo de origen.
   3. Dirección 3: Dirección para que el AP o el sistema de distribución haga filtrado.
   4. Dirección 4: Opcional.

3) IP

1. Que es default gateway, default route y como se relacionan.
2. Que campos de la cabecera intervienen en el mecanismo de fragmentación.
3. Mensajes de la operación ARP y a quien van dirigidos.

RTA:

1. Default gateway es el próximo salto que se le asigna por defecto a un paquete.
   1. Default route se utiliza para paquetes en donde no tienen información para el próximo salto.
2. El campo ID (16b) permite identificar el datagrama.
   1. El flag More Fragments (1b) indica que todavía hay más fragmentos del paquete original.
      1. Cuando sea cero, implica que no hay más que ese.
   2. El campo Offset (13b) permite identificar el desplazamiento relativo a partir del primer fragmento enviado.
3. El protocolo ARP envía un mensaje Broadcast MAC con la dirección IP destino para que el destino responda con su MAC y se cree una entrada en el cache ARP.

#### **2020 1C**

1. VLSM: IP 172.16.21.128 / 25. Asignar red de 22 host, 6 host y 5 host.

**RTA**:

* Para 22 host → 5 bit (32)
* Para 5 host → 3 bit (8)
* Para 6 host → 3 bit (8)
* Se analiza solamente el último octeto.
  + 100|00000 → De 128 a 159
  + 10100|000 → De 160 a 167
  + 10101|000 → De 168 a 175

| ID Red | Mascara | Broadcast | Rango direccionable |
| --- | --- | --- | --- |
| 172.16.21.128 | / 27 | 172.16.21.159 | 129 - 158 |
| 172.16.21.160 | / 29 | 172.16.21.167 | 161 - 166 |
| 172.16.21.168 | / 29 | 172.16.21.175 | 169 - 174 |

1. IP: 172.16.31.255. Seleccionar afirmaciones correctas

**RTA**:

* Es broadcast de 172.16.31.0 / 24
  + Último octeto todo en 1 transforma el 0 en 255.
* Es broadcast de 172.16.28.0 / 22
  + 000111|00.00000000
* Es broadcast de 172.16.30.0 / 23
  + 0001111|0.00000000

1. El protocolo IP es no orientado a la conexión. No garantiza entrega en orden. Corrige errores en su cabecera pero no el campo datos.

**RTA**:

* Falso. Solo detecta errores en su cabecera con un campo Checksum de 16b.

1. La imposibilidad de conmutar un datagrama provoca en el router la generación de un mensaje ICMP “Destino inalcanzable” para informar el error al remitente del datagrama.

**RTA**:

* Verdadero.

1. ARP usa mensajes de broadcast para consultar quien posee una dirección IP determinada. El host indicado responderá a quien consulta mediante un mensaje unicast.

**RTA**:

* Verdadero

1. OSI: Los protocolos de capa par implementados en el transmisor y receptor deben coincidir en todas las capas.

**RTA**:

* Verdadero:

1. IP 192.168.122.3 / 25. La afirmación es correcta?
   1. IP es clase C. Se crearon 2 subredes considerando la 0 y la 1 como válida. La dirección pertenece a la primera subred y corresponde al 3er host.

**RTA**:

* Verdadero.
* Es clase C porque es mayor a 192.0.0.0
* Se analiza el 4to octeto:
  + 0|0000011
  + Subred 0
  + Host 3

1. Protocolo ICMP cumple las siguientes funciones:

**RTA**:

* Informa cuando el TTL llegó a cero. Es el caso del mensaje de tipo “Tiempo de espera agotado”
* Informar acerca de eventos inesperados en la red.

1. OSI: Afirmaciones correctas.

**RTA**:

* El modelo OSI posee más capas que TCP/IP.
  + Osi tiene 7 capas mientras que TCP IP solo tiene 4.
* El modelo OSI permite la implementación parcial.
  + La mayoría de protocolos no implementan todas las capas.
* Se denomina “Trama” a la PDU de capa 2 y “Paquete” a la PDU de capa 3.

1. Asociar capa OSI para cada protocolo

**RTA**:

* Ethernet: Capa 2.
* 802.11: Capa 2.
* Manchester diferencial: Capa 1.
* DHCP: Capa 7.
* TCP: Capa 4.
* IP: Capa 3.

1. ARP: Afirmaciones correctas.

**RTA**:

* Se utiliza para obtener la dirección MAC del default gateway.
* Se usa para mapear una dirección IP de 32 bits a una MAC de 48 bits.

### **2do**:

#### **2018 1C:**

1. IPSEC contempla 2 protocolos y 2 modos de operación. ¿Cuales son?

**RTA**:

* IPSEC es un conjunto de protocolos que permite agregar autenticidad e integridad a la comunicación.
* Modos:
  + Transporte: Solo protege la información de transporte.
    - No protege la información IP.
  + Túnel: Protege toda la información.
    - Es más costoso.
* Protocolos:
  + AH: Authentication Header: Garantiza autenticidad e integridad.
    - No encripta la información.
  + ESP: Encrypted Security Payload: Garantiza autenticidad, integridad y privacidad.
    - Encripta la información.

1. Explicar DE y FECN en Frame Relay.

**RTA**:

* Son mecanismos para el control de la congestión.
* DE es un bit que indica que la trama puede ser descartada, de ser requerido, frente a una congestión en el tráfico.
* FECN indica que el sentido de la congestión coincide con el del frame.

1. Indicar para que sirven las capas AAL1 y AAL2 en ATM. Diferencias.

**RTA**:

* Ambas son capas de adaptación del protocolo ATM.
* AAL1 está pensada para tratar flujos de bits constantes.
* AAL2 para voz y video comprimidos.

1. Como se realiza el cierre de conexión en TCP y en UDP.

**RTA**:

* En UDP no hay conexión.
* En TCP se utiliza un mecanismo de 4 pasos:
  + El cliente envía un mensaje FIN.
  + El servidor envía un mensaje ACK y el cliente queda a la espera.
  + El servidor le envía un mensaje FIN al cliente.
  + El cliente responde con un ACK.

1. ¿Que provoca la retransmisión de un segmento TCP? ¿Como se detecta la necesidad de retransmitir?

**RTA**:

* TCP no cuenta con confirmación de rechazo. Frente a la falta de confirmación ACK de un segmento en un tiempo RTO, interpreta que se perdió e intenta retransmitir.
  + RTO significa retransmission timeout e implica el tiempo que tiene un segmento para no entregar confirmación antes de ser considerado como perdido.
    - Un valor muy pequeño va a implicar muchas retransmisiones si hay delay.
    - Un valor muy grande va a hacer que se tarde mucho en retransmitir en caso de perdida.

1. Características que debe cumplir una función de Hash.

**RTA**:

* Aleatoriedad: No se debe poder predecir el mensaje original.
* Consistencia: Frente a la misma entrada siempre debe ser la misma salida.
* One Way: No poder, a partir de la salida, obtener el valor de entrada
* Unicidad: Debe ser casi imposible encontrar 2 mensajes con la misma salida.

#### **2020 2C**

1. UDP: Afirmaciones verdaderas.

**RTA**:

* No realiza control de flujo.
* Utiliza los campos puerto origen y destino como TCP.
* Es el protocolo de transporte utilizado para el envío de trafico multicast y broadcast.
* La cabecera ocupa 8 bytes.
  + Puerto origen y destino (32b) + Long. mensaje y Checksum (32b)

1. IPv6: Afirmaciones correctas.

**RTA**:

* IPv6 resuelve la escasez de dirección extendiendo a 128 bits.
* La cabecera IPv6 ocupa el doble de bytes que la de IPv4.
  + 320 la de IPv6 vs 160 de IPv4.

1. MPLS: Se basa en la conmutación de etiquetas asignadas por LSRs a partir de identificar un FEC.

**RTA**:

* Verdadero.
  + Los LER (Label Edge Router) colocados en el ingreso y egreso de la red, son los encargados de genera y asignar la etiqueta al paquete para luego ser removidos cuando salen de la red mpls.
    - Estos router conocen protocolo IP y MPLS.
  + Los LSR (Label Switch Router) colocados dentro de la red mpls son los encargados de conmutar los paquetes solo utilizando la etiqueta MPLS, logrando mayor performance.
    - Estos router solo conocen MPLS.

1. MPLS: Afirmaciones verdaderas

**RTA**:

* Los LSR Edge solo interpretan etiquetas. Falso.
  + Los LSR Core son los que interpretan.
* Un paquete en la red MPLS solo puede tener una única etiqueta. Falso.
  + Se pueden apilar etiquetas.
* El campo dirección en la cabecera MPLS identifica el tipo de servicio. Falso.
  + No hay tal campo.
* La etiqueta se inserta entre la cabecera de red y transporte. Falso.
  + Se inserta entre las cabeceras de Enlace y Red.

1. ATM: Clase de servicio B.

**RTA**:

* Tasa de bits variable.
* Requiere sincronización entre origen y destino.
* Se implementa con AAL2.

1. Frame Relay permite multiplexar conexiones sobre un único acceso mientras que HDLC no lo contempla.

**RTA**:

* Verdadero.

1. ATM: Afirmaciones correctas.

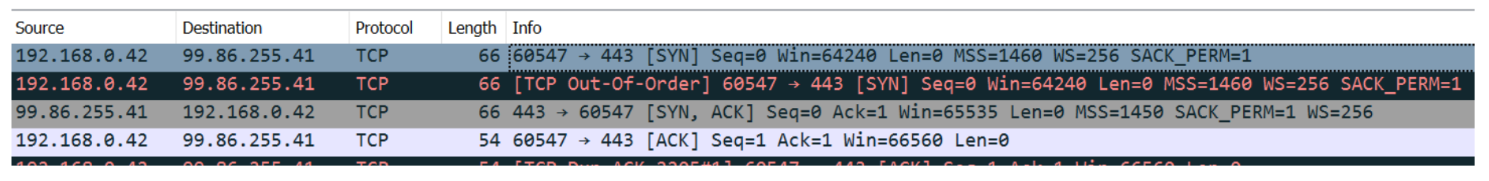
**RTA**:

* El protocolo permite la multiplexación de conexiones en capa 2 usando VPI/VCI como identificador. Verdadero.
  + VPI: Virtual Path Indicator.
  + VCI: Virtual Channel Indicator.
* Utiliza celdas pequeñas con una capacidad de datos de 48 Bytes. Verdadero.
  + El total de la celda es de 53 bytes.
  + Al ser pequeña y tamaño fijo es más sencillo el procesamiento y menor el buffer requerido.
  + La cabecera está conformada por:
    - GFI: 0 o 4 bits dependiendo si es UNI o NNI.
    - VPI: 8 o 12 bits dependiendo si es UNI o NNI.
    - VCI: 16 bits.
    - Payload Type: 3 bits.
    - CLP: 1 bit: Prioridad.
    - HEC: 8 bits: Control de errores en la cabecera.
      * Solo corrige 1 bit de error, si hay más se descarta.
* El protocolo implementa una subcapa “Capa de adaptación ATM”.
  + Es la subcapa perteneciente a la capa de enlace y se divide en:
    - Segmentación / Ensamblado: De la información de capas superiores.
    - Convergencia: Independizar de protocolos superiores.
      * Recuperar la señal de clock

1. TCP: El campo Hlen permite determinar la presencia de opciones.

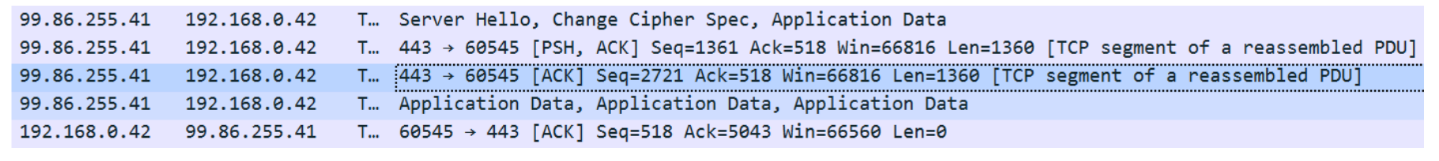
**RTA**:

* Verdadero. Si el campo HLEN = 5, indica que solamente hay 5 palabras de 32 bits en la cabecera por lo tanto no hay opciones.



**RTA**:

* El servidor otorga al cliente un crédito de 65535 bytes. Verdadero.
  + La window del servidor indica que puede recibir hasta 65535 bytes.
* El servidor rechaza la conexión del cliente. Falso.
  + Out of order solo indica que los fragmentos se entregaron en un orden distinto al que fueron enviados.
* El cliente tiene 256 segundos para completar la conexión. Falso.
  + WS no indica la cantidad de segundos restantes de conexión.
* El cliente 192.168.0.42 inicia la comunicación. Verdadero.
  + El cliente envía SYN, servidor responde SYN,ACK y luego el cliente establece la conexión enviando un ACK.



**RTA**:

* El cliente indica haber transmitido al servidor 5043 bytes. Falso.
  + ACK indica el nro del próximo byte que espera recibir el cliente.
* El cliente confirma haber recibido del servidor 5042 bytes. Verdadero.
  + Al esperar el 5043, indica que recibió satisfactoriamente hasta el 5042 inclusive.
* El protocolo de aplicación usado es HTTPS. Verdadero.
  + El puerto 443 del servidor es el utilizado para HTTPS.
* La conexión se realiza sobre TLS. Verdadero.
  + HTTPS utiliza TLS para encriptar la comunicación.

1. TCP: Utiliza un intercambio de tres pasos para establecer la conexión. El proceso lo inicia el cliente enviando un SYN al servidor.

**RTA**:

* Cliente envía un segmento con SYN activo, Nro Seq = X y Nro ACK = vacío
* Servidor responde con un segmento SYN, ACK con Nro Seq = Y y nro ACK = X + 1
* Cliente responde con un segmento ACK con nro Seq = X + 1 y nro ACK = Y + 1
  + Puede o no enviar datos en este segmento
  + La conexión ya está establecida

1. IPSEC contempla la operación en modo túnel y transporte.

**RTA**:

* Verdadero
  + Modo transporte solo provee seguridad a la información de transporte.
    - No a la información de IP.
  + Modo túnel encapsula todo en un datagrama IP incluida la información IP.
    - Es más costoso.

1. IPSEC: Afirmaciones correctas.

**RTA**:

* El modo túnel garantiza la protección del mensaje encriptandolo y encapsulandolo dentro de otro datagrama IP.
  + Es más costoso.
* El modo transporte protege la comunicación entre dos host exclusivamente.
* El algoritmo de encriptación debe acordarse entre los extremos.

1. HDLC: El protocolo utiliza 3 tramas: Información, supervisión y no numeradas.

**RTA**:

* Verdadero.
  + Información: Encargadas del transporte de información y el control de flujo y errores si se utiliza piggyback.
  + Supervisión: Encargadas del control de flujo y errores si no se requiere piggyback.
  + No numeradas: Funciones para el control del enlace.

1. UDP: Es un protocolo orientando a la no conexión. Cualquiera de los extremos pueden finalizar la conexión aunque queden mensajes sin confirmar.

**RTA**:

* Falso. No hay conexión en UDP.

1. Frame Relay: Afirmaciones correctas.

**RTA**:

* DE identifica tramas elegibles para descarte.
  + Las tramas que viajen con DE = 1 podrán ser descartadas en caso de congestión.
* FECN y BECN se usan para notificar la congestión, no para controlarla.
  + FECN indica congestión en el mismo sentido que el frame.
  + BECN indica congestión en el sentido contrario al frame.
* CIR es la tasa de transmisión, en bps, que la red garantiza transmitir en condiciones normales.

1. La encriptación asimétrica usa algoritmos y claves diferentes para la encriptación del tráfico.

**RTA**:

* Verdadera.
  + Se utilizan claves públicas y privadas.
  + Cada uno puede o no utilizar el mismo algoritmo.

1. HDLC implementa control de flujo por Sliding Windows. Los campos N(s) y N(r) tienen una longitud de 3 bits y permiten ventana de 8 tramas.

**RTA**:

* Verdadero.

1. IPv6 tiene un prefijo de red de longitud fija de 64 bits.

**RTA**:

* Verdadero.

1. Una función de hash debe cumplir:

**RTA**:

* Consistencia: Frente a la misma entrada siempre dar la misma salida.
* One way: Debe ser casi imposible obtener la entrada a partir de la salida.
* Unicidad: Debe ser casi imposible encontrar 2 entradas que den la misma salida.
* Aleatoriedad: Impedir adivinar el mensaje original.

#### **2021 2C**

1. El protocolo HDLC usa tramas no numeradas para realizar el control de flujo.

**RTA**:

* Falso

1. UDP: Afirmaciones correctas.

**RTA**:

* No realiza control de flujo.
* Es el protocolo de transporte utilizado para el envío de multicast y broadcast.
* La cabecera tan solo ocupa 8 Bytes.
  + Puerto Origen + Puerto Destino: 4 Bytes.
  + Long mensaje + Checksum: 4 Bytes.
* Utiliza los campos puerto Origen y Destino como TCP para identificar aplicaciones de usuario.

1. Un datagrama IPv6 puede dar el doble de saltos que un IPv4.

**RTA**:

* Falso. Tanto el campo TTL en IPv4 como Hop Limit en IPv6 tienen 8 bits.

1. UDP: Afirmaciones correctas.

**RTA**:

* Utiliza una cabecera de solo 8 Bytes.
  + Puerto origen y destino: 32 bits
  + Longitud mensaje y checksum: 32 bits.
* La detección de errores es opcional.
  + El campo checksum de la cabecera es opcional.
* Es el protocolo de transporte usado en Google Meet.
  + Es eficiente en la transmisión de voz y video.
* Utiliza los campos puerto origen y destino como TCP.

1. La encriptación asimétrica usa algoritmos y claves diferentes para encriptar y desencriptar el tráfico.

**RTA**:

* Verdadero. Utiliza clave pública y privada y los algoritmos pueden o no ser los mismos entre las partes.

1. TCP utiliza un intercambio de 3 pasos para establecer una conexión. El servidor puede rechazar la petición de conexión respondiendo con un segmento NACK..

**RTA**:

* Falso. El mecanismo que utiliza TCP consiste.
  + El cliente envía un segmento SYN con Nro de secuencia X y Nro ACK vacío.
  + El servidor responde con un segmento con SYN y ACK activo, con nro de secuencia Y y nro ACK X + 1
  + El cliente responde con un segmento ACK activo, con nro de secuencia X+1 y nro ACK Y +1
    - Puede o no enviar datos pero la conexión ya está establecida.

1. Los datos “urgentes” no están contemplados en la secuencia de TCP.

**RTA**:

* Verdadero. Los datos en sí no son parte del segmento TCP sino que es el payload que viaja dentro del paquete.
  + Lo que si especifica TCP es un bit URG (para indicar que hay datos urgentes) y un campo de 16 bits que indica donde finaliza la secuencia de datos urgentes.
  + Dichos datos son enviados por un canal especial y, frente a una posible congestión, tienen prioridad.

1. Frame Relay: Afirmaciones verdaderas.

**RTA**:

* FECN y BECN notifican congestión, no la controlan.
  + FECN es un bit que indica que la congestión va en el mismo sentido que el frame mientras que BECN indica que la congestión va en sentido contrario.
* El bit DE identifica a las tramas elegibles para descarte.
  + Frente a congestión, estas tramas se pueden descartar.
* CIR es la tasa de transmisión, en bps, que la red garantiza transmitir bajo condiciones normales.

1. IPSec: Afirmaciones verdaderas:

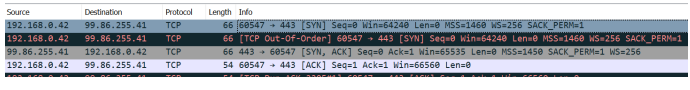
**RTA**:

* El modo transporte protege la comunicación entre dos hosts exclusivamente.
  + No protege la información de IP.
* El modo túnel garantiza la protección del mensaje encriptandolo y encapsulandolo dentro de otro datagrama IP.
  + Es más costoso.
* El algoritmo de encriptación utilizado debe acordarse entre ambos extremos de la comunicación.
  + Sino no sería posible que los extremos puedan leer su contenido.

1. Frame Relay permite multiplexar conexiones sobre un único acceso mientras que HDLC no lo contempla.

**RTA**:

* Verdadero.



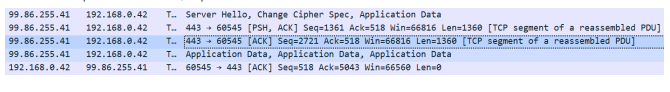
**RTA**:

* El servidor otorga al cliente un crédito de 65535 Bytes. Verdadero.
  + La window que envía el servidor (línea 3) es de 65535
* El cliente 192.168.0.42 inicia la comunicación. Verdadero.
  + Se observa que envía un mensaje SYN, el servidor responde SYN,ACK y luego el cliente envía SYN.
* El cliente tiene 256 segundos para completar la conexión. Falso.
  + El campo WS no indica segundos restantes.
* EL servidor rechaza la conexión del cliente. Falso.
  + TCP Out of order solamente indica que los paquetes llegaron en un orden distinto al que fueron enviados.

1. Una función de hash debe cumplir:

**RTA**:

* One Way: No se puede realizar el proceso inverso y obtener una entrada a partir de una salida.
* Unicidad: Para una entrada solo debe existir una sola salida.
* Consistencia: Para la misma entrada siempre debe ser la misma salida.



**RTA**:

* El cliente indica haber transmitido al servidor 5043 Bytes. Falso
  + ACK indica que el próximo que espera es el 5043.
* El cliente confirma haber recibido del servidor 5042 Bytes. Verdadero.
  + Si espera recibir el 5043 es porque ya recibió hasta el inmediato anterior.
* El protocolo utilizado es HTTPS. Verdadero.
  + El puerto 443 es el designado para HTTPS.
* La conexión se realiza sobre TLS. Verdadero. HTTPS implementa TLS para el cifrado

1. El protocolo HDLC utiliza 3 tipos de tramas: Información, supervisión y no numeradas.

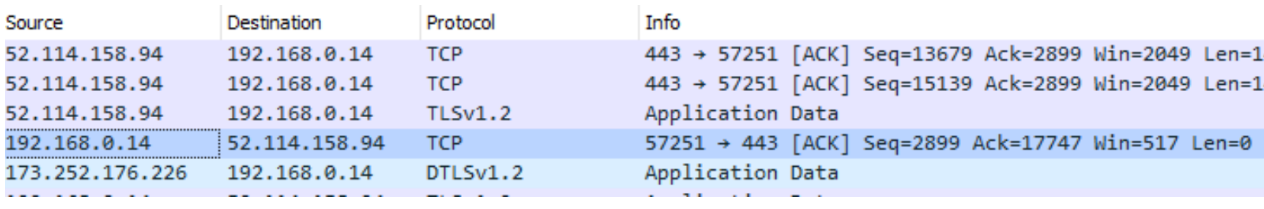
**RTA**:

* Verdadero.
  + Las de información transportan información y realizan control de flujo y errores cuando se utiliza piggyback.
  + Las de supervisión se encargan del control y flujo de errores cuando no se requiere piggyback.
  + Las no numeradas se encargan del control del enlace.

1. IPv6: Afirmaciones correctas.

**RTA**:

* La cabecera IPv6 ocupa el doble de bytes que la cabecera IPv4
  + Verdadero, la de IPv6 ocupa 320 bits mientras que la de IPv4 ocupa 160
* IPv6 resuelve la escasez de direcciones al extender su longitud a 128 bits.
  + Utiliza 48 bits para el prefijo de ruteo.
  + Utiliza 16 bits para identificar la subred.
  + Utiliza 64 bits para identificar la interfaz dentro de la subred.



**RTA**:

* El servidor puede transmitir hasta 2049 bytes sin recibir confirmación. Falso.
  + El campo window indica cuanto está dispuesto a recibir en total.
* El cliente transmitió 57251 bytes. Falso.
  + 57251 indica el puerto del cliente.
* El cliente espera recibir el octeto numero 17747. Verdadero
  + ACK indica el próximo byte que espera recibir.
* El servidor ha enviado 17746 bytes, que fueron correctamente recibidos por el cliente. Verdadero.
  + ACK indica el próximo a recibir y también que hasta el anterior inmediato incluido fueron recibidos correctamente.

1. UDP es un protocolo no orientado a la conexión. Cualquiera de los dos extremos puede finalizar la conexión en cualquier momento, aun cuando queden mensajes sin confirmar.

**RTA**:

* Falso. Al ser no orientado a la conexión, nunca se establece conexión.

1. TCP utiliza un intercambio de 3 pasos para establecer conexión. El proceso lo envía el cliente enviando un segmento SYN al servidor.

**RTA**:

* Verdadero.
  + El cliente envía un segmento SYN con Nro Seq = X y Nro ACK = Vacio.
  + El servidor responde con un fragmento SYN, ACK con Nro Seq = Y y Nro ACK = X + 1}
  + El cliente responde con un fragmento ACK con Nro Seq = X + 1 y Nro ACK = Y + 1.
    - La conexión ya queda establecida.

1. IPSEC operando en modo túnel encripta el datagrama IP completo adicionando una nueva cabecera IP.

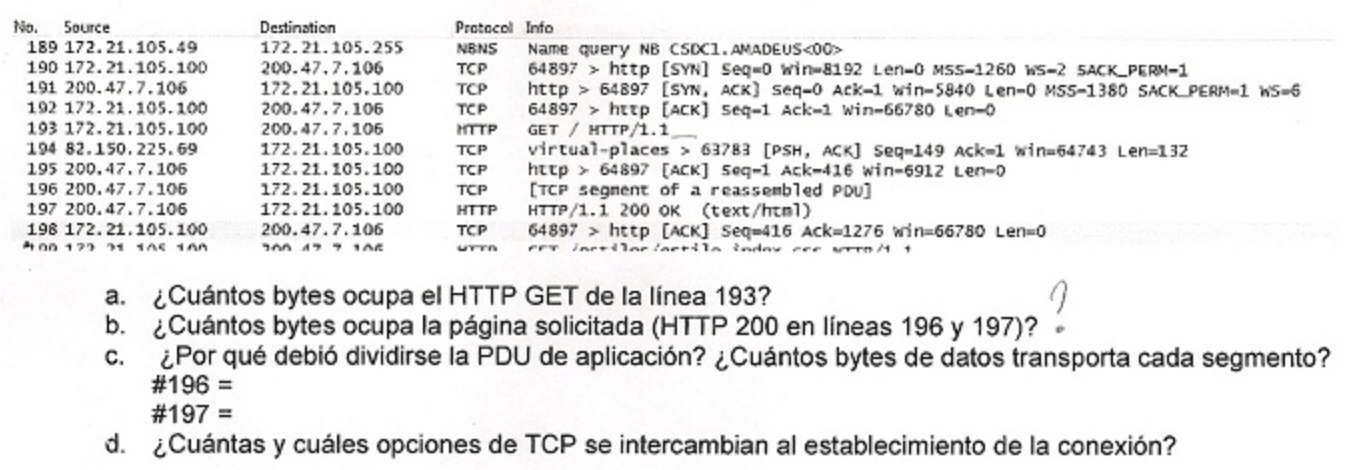
**RTA**:

* Verdadero.
  + Da más seguridad que Modo Transporte pero es más costoso.

# **Sin Dueño:**

## **Finales:**

### **2010 12 22**



**RTA**:

1. En la línea 192, 172.21.105.100 tiene SEQ = ACK = 1
   1. Luego de la consulta, en la línea 198, se observa que, luego de las recepciones del servidor, el ACK = 416.
   2. La diferencia entre el SEQ inicial y el ACK final luego de la recepción, indica la cantidad de bytes que ocupó la instrucción.
   3. El ACK es el próximo Byte que espera recibir.
   4. Cantidad Bytes = 415
2. En la línea 195, se puede ver que 200.47.7.106 tiene SEQ = 1 y ACK = 416
   1. Luego de la consulta http, sus valores quedan en SEQ = 416 y ACK = 1276
   2. Cantidad Bytes = 1276 - 1 = 1275 Bytes
3. La PDU tuvo que dividirse ya que 172.21.105.100 declaró que tiene un MSS máximo de 1260 y el total de get HTTP era 1275
   1. El 196 ocupa un fragmento entero = 1260 Bytes
   2. El 197 ocupa lo restante del total = 15 Bytes
4. Las opciones se intercambian al inicio de la conexión. En este caso en la fila 190 y 191
   1. MSS, SACK\_PERM\_ WS

2) Enunciar las capas del modelo OSI y en cual se realiza el control de errores.

**RTA**:

* Física, enlace, red, transporte, sesión, presentación y aplicación.
* La capa de enlace y de transporte proveen mecanismos de control de errores.

3) Detallar el formato de celda ATM e indicar como interviene el HEC en:

1. Detección de errores.
2. Obtención y mantenimiento del sincronismo.

**RTA**:

1. La celda ATM tiene un tamaño fijo de 53 Bytes, de los cuales 48 son para Datos y 5 para encabezado.
   1. HEC: Header Error Check: 8 bits
   2. GFC: Control de flujo: 4 bits. Solo se usa en UNI.
   3. VPI: Virtual Path Indicator: 8 (UNI) o 12 (NNI) bits.
   4. VCI: Virtual Channel Indicator: 16 bits
   5. Tipo de carga: 3 bits.
   6. CLP: 1 bit.
2. HEC analiza por errores la cabecera y solo puede corregir 1 bit de error. Cualquier caso que tenga más bits erróneos será descartado.

4) IP 192.168.0.223 es la broadcast de una red.

1. Dirección de red.
2. Mascara
3. Cantidad de subredes creadas.

**RTA**:

1. Analizo el 4to octeto:
   1. 110|11111
   2. Red: 192.168.0.192
2. Mascara: Utiliza 3 bits para subred
   1. 255.255.255.224 (/27(
3. Se pueden un máximo de 2^3 - 2 subredes.
   1. Máximo de 6 subredes (Descontando las prohibidas)