**Modelo OSI**

1. ***Responda de forma concisa.***
   1. ***¿En qué capas del modelo OSI se realiza el control de errores?***

La detección y corrección de errores se realiza en la capa de enlace de datos (MAC).

* 1. ***¿Porque habría de realizarse este control más de una vez?***

Para asegurar que los datos transmitidos y luego enviados a niveles superiores estén libres de errores. Sin alteraciones en las secuencias de los bits. En el orden correcto de las tramas. Sin duplicidades.

* 1. ***¿Qué capa se encargará de la encriptación de los datos?***

De encriptar y desencriptar datos se encarga la capa de presentación.

1. ***Enumere las ventajas y desventajas del diseño en capas para un protocolo.***

***Ventajas:***

* Facilita la comprensión al dividir un problema complejo en partes más simples.
* Normaliza los componentes de red y permite el desarrollo por parte de diferentes fabricantes.
* Evita los problemas de incompatibilidad.
* Los cambios de una capa no afectan las demás capas y estas pueden evolucionar más rápido.
* Simplifica el aprendizaje.

***Desventajas:***

* Mala sincronización
* Mala tecnología
* Malas instrumentaciones
* Mala política.

1. ***Justifique si es necesaria o no una capa de red (capa 3 del Modelo OSI) en una red***

***de difusión (Broadcast).***

Los dispositivos de la capa 3 OSI (como los routers) son necesarios para segmentar los dominios de colisión y difusión(broadcast).

1. ***Considerando el modelo de capas OSI, ubique a los siguientes dispositivos en la***

***capa que mejor describe las funciones que realiza:***

* 1. Repetidor → Capa 1
  2. HUB→ Capa 1
  3. Bridge→ Capa 2
  4. Modem→ Capa 1
  5. LAN switch→ Capa 2
  6. Router→ Capa 3
  7. Firewall→ Capa 7

1. ***Clasificación de Redes:***

De acuerdo con su extensión:

* LAN (Local Area Network)
* WAN (Wide Area Network)
* GAN (Global Area Network)

***Diferencias***

* Públicas / Privadas
* Diferentes Anchos de banda, Velocidades de transferencia y Tasa de error (BER)
* Gestión del enlace
* Redes de conmutación de circuitos/paquetes
* Protocolos diferentes

***Topologías***

* Bus o Barra / Arbol
* Anillo
* Estrella
* Híbrida

***Características Capa OSI***

* Capas separadas para funciones diferentes
* Funciones similares dentro de la misma capa
* Interacción mínima entre capas
* Permite la implementación parcial

***Filosofía de TCP/IP***

* Servicios de Aplicación
* Servicio de Transporte Confiable
* Servicio de Entrega de Paquetes ConnectionLess

***Servicio Connection-less***

* No confiable - significa que los paquetes pueden ser:
* Perdidos
* Duplicados
* Desordenados
* Demorados
* Connectionless – paquetes tratados independientemente
* No existe un “estado” en los routers acerca de cómo fueron tratados los paquetes anteriores, ni qué contenían.
* Entrega Best-Effort – el software realiza un serio intento por entregar el paquete

**Redes LAN**

1. ***Mencione 3 ventajas de implementar una red conmutada (con switch) frente a una***

***red compartida (con hubs).***

* 1. Divide los dominios de colisión
  2. Todos los dispositivos de la red tienen una capacidad dedicada igual a la de

la LAN completa. Permite Full Duplex.

* 1. Permite el escalado de forma sencilla.

1. ***¿Qué función cumple el campo PAD (relleno) en la trama Ethernet/802.3?***

El Campo PAD se utiliza porque nuestra trama tiene que tener un mínimo de 64 Bytes, y en el caso en que el encabezado sumado a los datos no llegue a los 64 Bytes mínimos necesarios, se utiliza el campo PAD para rellenar la trama.

1. ***¿Cómo realiza Ethernet el control de errores?***

CRC-32 y funciona de la siguiente manera:

A cada bloque de datos le corresponde una secuencia fija de números binarios conocida como código CRC (esto se calcula con una misma función para cada bloque). Ambos se envían o almacenan juntos. Cuando un bloque de datos es leído o recibido, dicha función es aplicada nuevamente al bloque, si el código CRC generado no coincide con el código CRC original, entonces significa que el bloque contiene un error. Eso hará que el dispositivo intente solucionar el error releyendo el bloque o requiriendo que sea enviado nuevamente.

Si coinciden ambos códigos CRC, entonces se asume que el bloque no contiene errores (existe una remota posibilidad de que haya un error sin detectar). El nombre "control/comprobación de redundancia cíclica" se debe a que se "controla" (verificación de datos) un código redundante (no agrega nueva información, el código CRC representa el mismo bloque de datos) y el algoritmo está basado en códigos cíclicos. Es importante destacar que el número de caracteres de entrada a la función CRC puede tener cualquier longitud, pero siempre producirá un código CRC de igual longitud.

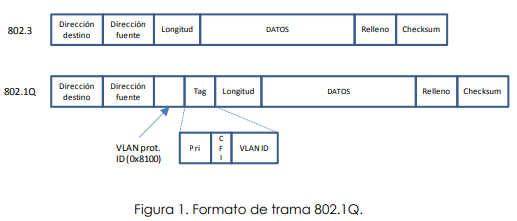
1. ***¿Qué utilidad tiene el protocolo Spanning Tree? ¿Qué dispositivos lo ejecutan?***

Permite evitar un loop de red en caso de múltiples switches con **vínculos redundantes**. Estos se producen por el desconocimiento de la existencia deotros bridges/switches en la red. Lo ejecutan los switches, ya que es unprotocolo de capa 2 (enlace de datos).

1. ***Explique qué es una colisión en Ethernet y como se resuelve esta condición. ¿Cómo cambia esta situación la incorporación de un bridge/switch?***

Una colisión se da cuando dos estaciones quieren transmitir a la vez por un mismo medio y sus paquetes colisionan, para resolver este problema se utilizan mecanismos de control de acceso al medio. Entre ellos esta CSMD/CD, CSMD-1, etc. Los Switchs particionan los dominios de colisión, con lo cual las colisiones no pueden pasar el dominio del conmutador.

1. ***¿Dónde se introduce la etiqueta 802.1Q? y ¿qué campos contiene?***



Como se puede apreciar en la Figura 1, la VLAN tag se inserta en la trama Ethernet entre el campo “Dirección fuente” y “Longitud. Los primeros 2 bytes del VLAN tag consisten en el “Tag Type" (tipo de tag) de 802.1Q y siempre está puesto a 0x8100. Los últimos 2 bytes contienen la siguiente información:

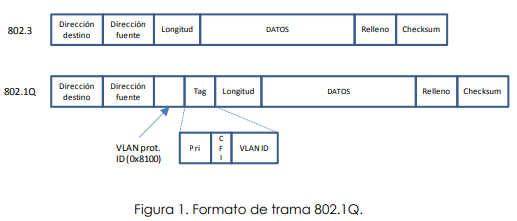
* 1. Los primeros 3 bits son el campo User Priority Field que pueden ser usados para asignar un nivel de prioridad.
  2. El próximo bit es el campo Canonical Format Indicator (CFI) usado para indicar la presencia de un campo Routing Information Field (RIF).
  3. Los restantes 12 bits son el VLAN Identifier (VID) que identifica de forma única a la VLAN a la cual pertenece la trama Ethernet.

1. ***¿Cómo realiza el protocolo Spanning Tree la elección del root?***
2. Todo switch tiene un bridge Identifier (BID) compuesto de: BID = Bridge Priority (BP) + MAC.
3. El de menor BID menor se designa como root.
4. En caso de 2 switch con igual BID, se define la prioridad en base a su MAC (se selecciona la MENOR). Una vez que los switches son inicializados intercambian BPDU y cada switch reemplaza su “switch raíz” por el de BID menor.
5. ***Enuncie al menos 3 diferencias entre el mecanismo CSMA (acceso múltiple con escucha de portadora y detección de colisiones) utilizado en redes LAN 10baseT (802.3) y el utilizado por 802.11(Wireless).***

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Funcionamiento** | **Ventajas** | **Desventajas** |
| **CSMA/CD** | Utilizado en redes IEEE 802.3.  Los dispositivos de red que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de red están ocupados o no.  En caso de que haya dos dispositivos que no detectan ningún otro tráfico, ambos tratarán de transmitir al mismo tiempo, dando como resultado una colisión. A partir de esta colisión se genera un algoritmo de espera con el que las estaciones retransmitirán aleatoriamente. | - Transmisión en colisión es cancelada reduce el mal uso del canal. - Fácil detección de colisiones en LAN cableadas. - Colisiones detectadas en corto tiempo. | - Con inalámbrica difícil detección. |
| **CSMA/CA** | Utilizado en IEEE 802.11.  Permite que múltiples estaciones utilicen un mismo medio de transmisión y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. | - Si el canal está libre transmite trama entera. - Si en canal está ocupado posterga la información. | - Colisiones por tiempo de retardo. - El tiempo completo de envió y de espera es desperdiciado. - El rol de la distancia y el retardo de propagación determinan la probabilidad de colisión. |

1. ***¿Para qué sirve el protocolo 802.1Q? ¿Cómo modifica la trama? De un ejemplo de aplicación.***

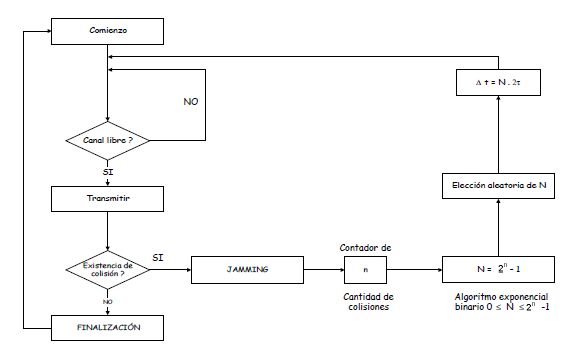
El protocolo 802.1Q permite la asociación lógica de estaciones que constituyen una VLAN, creadas dentro de un mismo switch.



Por ejemplo, generar un VLAN correspondiente a ALUMNOS, otra VLAN correspondiente a DOCENTES y otra correspondiente a ADMINISTRACION, de esa manera cada VLAN transmitirá la información que le corresponda.

1. ***Detalle el funcionamiento del algoritmo exponencial binario utilizado en 802.3 para resolver las colisiones.***

Luego de 16 colisiones consecutivas, la subcapa MAC aborta la transmisión. Cuando logra transmitir, se resetea el contador de intentos.

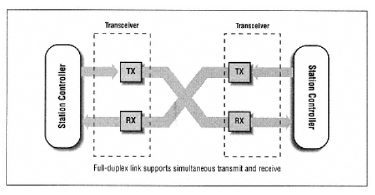


1. ***Indique 3 diferencias con el mecanismo utilizado en 802.11***

El envío de tramas en 802.11 utiliza un mecanismo de transferencia básico. La fuente emite una solicitud para enviar (RQT) y el destino responde con el permiso para recibir (CTS). De esta forma, inician la conexión y recibe tramas de datos confirmando con un ACK. El resto de las estaciones se abstienen de enviar datos ya que le fue notificado el CTS.

1. ***Interfaz Full-Duplex***

* Caminos de transmisión y recepción independientes que operan en simultaneo
* Dos estaciones conectadas punto a punto con un vínculo full dúplex
* No hay contención 🡪 se elimina el CSMA/CD



***Bridging***

* Transparent Bridge
  + Operan en el nivel 2 y utilizan las direcciones MAC para encaminar las tramas.
  + Aprenden automáticamente la ubicación de los hosts.
  + Las tramas soportan dos procesos. “Filtering y Forwarding”
* Translating Bridge
  + Realiza además conversión de protocolo y velocidad

**Otros Profesores:**

1. ***Sin considerar el campo sincronismo, indicar el tamaño de una trama corta en 10Mbps.***

Trama Mínima = 64 bytes

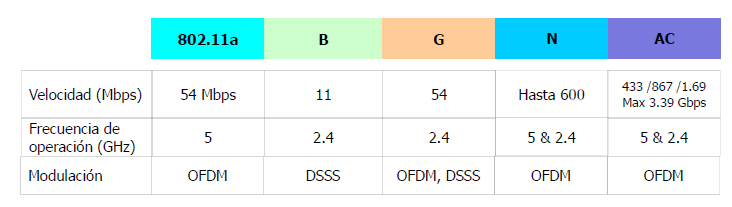
**Wireless LAN**

1. ***¿Cuáles son las diferentes tecnologías de redes LAN inalámbricas?***

* Infrarrojo (IR)
  + Haz dirigido
  + Omnidireccional
  + Difusión (Uso de Reflector)
* Radio por Espectro Expandido
  + Dos técnicas: Salto de Frecuencia y Secuencia Directa. Banda 900 MHz, 2.4 GHz y 5,8 GHz.
  + Topología con concentrador o peer to peer
  + No necesita licencia de la CNC
* Radio (microondas) de banda estrecha
  + Se conoce también como radioenlaces
  + Con licencia de la CNC (coordinación, sin interferencias, configuración en celdas). Banda 18 GHz.
  + Sin licencia de la CNC (configuración entre pares, baja potencia). Banda *5.8 GHz.*

1. ***¿Cuáles son las bandas en que operan las diferentes normas? ¿Qué diferencia hay***

***entre ellas?***



1. ***¿Para qué se creó el mecanismo RTS/CTS (Ready To Send/Clear To Send) en 802.11? ¿Como funciona?***

El mecanismo RTS/CTS se creó para evitar colisiones.

Funciona así: Si una estación quiere transmitir, escucha el medio durante un intervalo DIFS. Si está libre, envía un RTS (Ready to Send). Cuando recibe un CTS (Clear To Send), transmite. Si recibe un Acknowledge quiere decir que la transmisión fue exitosa (sino lo recibe vuelve a intentar después de un tiempo random).

1. ***¿Cuántas direcciones MAC contiene la cabecera 802.11? ¿Qué dispositivos***

***identifica?***

Contiene 4 campos de 6 Bytes para direcciones MAC. Y están destinados a

las direcciones de la fuente, el destino, la estación transmisora y la estación

receptora.

1. ***¿Cómo opera el modo DCF (Función de Control Distribuida)?***

El modo DCF opera así: para transmitir lo primero que tiene que hacer es escuchar el medio durante un intervalo DIFS (Distributed Inter Frame Spacing), y para que pueda proseguir, en ese intervalo no tendría que haber transmitido nadie.

1. ***¿Qué indican los flags “ToDS” y “FromDS” de la cabecera?***

ToDS significa hacía distribution system, o sea, que el paquete iría hacía el Access point. Y FromDS al revés, desde distribution system, desde el Access point al terminal.

1. ***Explique el mecanismo de control de acceso utilizado en redes Wireless (802.11) y detalle 3 diferencias con el CSMA/CD utilizado por 802.3.***

DCF (Función de coordinación distributiva) utiliza CSMA/CA con intercambio RTS/CTS opcional y ACK.

No se puede utilizar CSMA/CD en inalámbricas, por eso usa CSMA/CA

PCF (Point Cordination Function) es una técnica de control de acceso a medios utilizado en redes 802.11, que reside en el Access Point, entonces está restringido a redes de infraestructura. No es implementado normalmente y utiliza un tiempo de ranura menor para poder ganar prioridad en un intervalo más corto.

1. ***Que es el mecanismo de control de acceso al medio DCF utilizado por 802.11? ¿En que difiere de PCF?***

DCF utiliza un algoritmo que consiste en que la estación que desea transmitir (A), en primera instancia debe escuchar al canal un determinado tiempo denotado como DIFS para verificar que el canal esté libre. Si el canal está libre durante el periodo de tiempo DIFS, la estación A procede a enviar una solicitud para transmisión o RTS (Request To Send). La estación de destino (B) que recibe la RTS espera durante un intervalo de tiempo llamado SIFS; si el canal está libre, procede a responder con un CTS (Clear To Send) o con un RxBusy si está recibiendo datos de otra estación oculta (C) para la estación A. Una vez que la estación A recibe la CTS, también debe esperar el tiempo SIFS antes de proceder a transmitir los datos hacia la estación B. La estación B, una vez que recibe los datos vuelve a esperar el intervalo de tiempo SIFS hasta poder transmitir el acuse de recibo ACK o de no haber recibido nada NAK hacia la estación A.

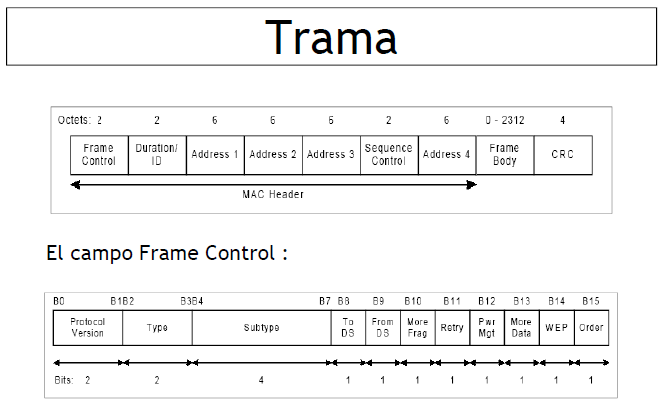
Cabe destacar que, durante este proceso, las estaciones de origen y destino sólo esperan el tiempo SIFS para continuar con el proceso; mientras que las otras estaciones deben esperar un tiempo DIFS para comenzar a hacer sus solicitudes de transmisión.

PCF tiene al AP como orquestador. Este sensa el medio durante un tiempo PIFS (tiempo previo a la autorización para transmitir), y se asegura de acceder al medio. Una vez que accede, empieza el periodo de libre contención y pollea a cada estación para ver si hay algo que transmitir. Después de un poll se espera un ACK y datos (si no tiene nada, manda nulo). Y después de cada mensaje enviado hay un tiempo SIFS que es un espacio inter-trama corto (siempre previo a datos). Para que las otras estaciones sepan cuando volver a intentar, el AP envía beacons a todas las estaciones constantemente para que seteen su tiempo de libre contención (NAV).  
  
La diferencia con DFC es que DFC utiliza DIFS como espacio de tiempo entre cada transmisión. Como DIFS es más grande que PIFS, siempre PCF tendrá prioridad de acceso al medio. Además, DFC utiliza los mensajes RTS y CTS.

1. ***Wireless LAN***

Posee una estructura celular, donde cada celda (llamada BSS) contiene:

* Distribution System (DS): generalmente la red LAN cableada
* Access Point (AP): estación base a la cual se conectan los terminales remotos
* Terminales



1. ***Frame Control***

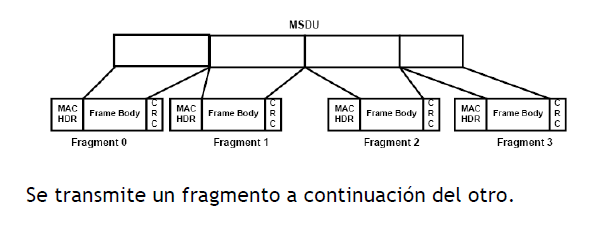
Las tramas pueden ser:

* Management: Petición/confirmación de asociación, autenticación, Beacon.
* Control: RTS, CTS, ACK
* Datos
  + ToDS: vale 1 cuando la trama se envía al AP con destino a una estación en DS.
  + FromDS: vale 1 cuando la trama viene del DS.
  + MF: indica que hay más fragmentos pertenecientes a la misma trama.
  + Retry: Indica que esta trama ya ha sido transmitida. Sirve para descartar duplicados en caso que se pierda el ACK.
  + Power Mgmt: indica en que modo estará la estación luego de transmitir esta trama.
  + More Data: idem, el AP indica a la estación que tiene más fragmentos para ella.
  + WEP: indica que el campo de datos está encriptado.

1. ***Diferencias con Eth.***

* Fragmentación y reensamblado

Debido a alto BER de la capa 1, conviene dividir los 1500 bytes en fragmentos menores



Se transmite un fragmento a continuación del otro.

1. ***Wireless LAN***

Para incorporase a una celda, una estación debe completar los siguientes pasos:

* Sincronización: por medio de los “beacon frames” transmitidos por el AP.
* Autenticación: intercambio de información (clave) entre el AP y el terminal
* Asociación: Se vincula la terminal al AP. A partir de este momento puede comenzar a transmitir.

1. ***Protección***

Se utiliza el protocolo WEP (Wired Equivalent Privacy) para evitar la intercepción de la información. Y para limitar el acceso de los terminales a un determinado AP.

**Otros Profesores:**

1. ***Indicar cuál es problema del nodo oculto y como se resuelve.***

Una condición conocida como el problema del nodo o terminal oculto ha sido identificada en sistemas inalámbricos y es causado por problemas en la detección de la transmisión. El terminal oculto es una situación encontrada en WLANs en la cual al menos un nodo es incapaz de escuchar o detectar uno o más del resto de los nodos conectados a la WLAN. En esta situación, un nodo puede oír al AP pero no puede detectar que existen otros terminales conectados al mismo AP debido a algún obstáculo o a la larga distancia entre ellos. Esta situación causa un problema en el acceso del medio, causando colisiones entre las transmisiones de los nodos. Estas colisiones pueden resultar en un considerable degrado del rendimiento en la WLAN.

**IP**

1. ***¿Qué es la interfaz loopback y para que se utiliza?***

La interfaz loopback es la 127.0.0.0 y es una interfaz que siempre está arriba. Le mandas un PING a cualquier dirección que empiece con 127 y siempre te responde. Generalmente se usa para conectar procesos en una misma computadora y para hacer tests.

1. ***¿Cuáles son las direcciones D, cuántas son, y para qué se utilizan?***

|  |  |
| --- | --- |
| 1 1 1 0 | 28 bits |

Las direcciones Clase D van de la 224.0.0.0 a la 239.255.255.255. Son 2^28 y se utilizan para multicast.

1. ***¿Qué campos de la cabecera intervienen en el mecanismo de fragmentación?***

Los campos de la cabecera que intervienen en el mecanismo de fragmentación son el offset y los flags don’t fragment y more fragment.

1. ***¿En qué casos no es necesario ejecutar el ARP para obtener la dirección MAC a***

***partir de una dirección IP?***

Cuando se envía un Broadcast o un Multicast.

1. ***¿Cuántas direcciones clase A existen? ¿Cuántos host permite direccionar una clase B?***

Clases A:

|  |  |  |
| --- | --- | --- |
| **0** | **Network ID (7 bits)** | **Host ID (24 bits)** |

Las direcciones Clase A van de 1.0.0.0 a 126.0.0.0. Son 2^7.

Clase B: Permite direccionar 2^16 host.

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **0** | **Network ID (14 bits)** | **Host ID (16 bits)** |

1. ***¿Qué mecanismo implementa el campo checksum en la cabecera? Indique su alcance.***

Solo controla errores en la cabecera, respetando un protocolo CRC-16 (16 x ser 16bit el campo). No hace corrección de errores (ya que la corrección de errores la delega potencialmente a la capa superior), ya que ip es un protocolo no orientado a la conexión.

Fácil implementación por software.

El receptor calcula el mismo checksum y si encuentra errores, descarta el datagrama. No se generan mensajes de error.

1. ***TOS (Type of Service) – 4 bits***

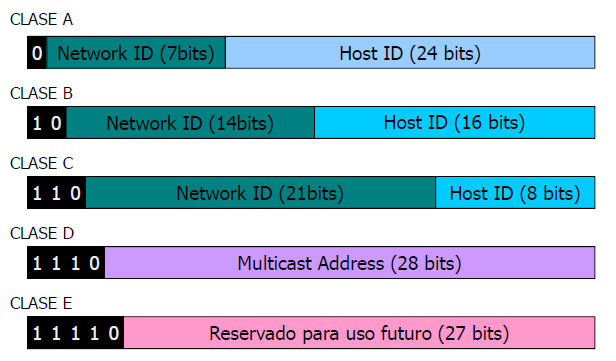
Solo uno puede estar encendido

* “Minimize delay” bit 🡪 Minimizar el Retraso
* “Maximize throughput” bit 🡪 Maximizar el Rendimiento
* “Maximize reliabilty” bit 🡪 Maximiza la Confiabilidad
* “Minimize cost” bit 🡪 Minimiza el Costo

1. ***Fragmentación y Reensamblado***

* MTU: Maximum Transfer Unit: Cada tecnología de conmutación de paquetes, fija un límite máximo para la cantidad de datos que pueden transmitirse en una única trama
* Desventajas de la Fragmentación
  + Duplica la probabilidad de pérdida de un datagrama
  + Genera mayor carga de procesamiento en los routers

1. ***Clases de Direcciones***



CLASE A 🡪 0 7 24

CLASE B 🡪 10 14 16

CLASE C 🡪 110 21 8

CLASE D 🡪 1110 28

CLASE E 🡪 11110 27

1. ***Direccionamiento***



D 🡪 224.0.0.0 a 239.255.255.255

**ARP**

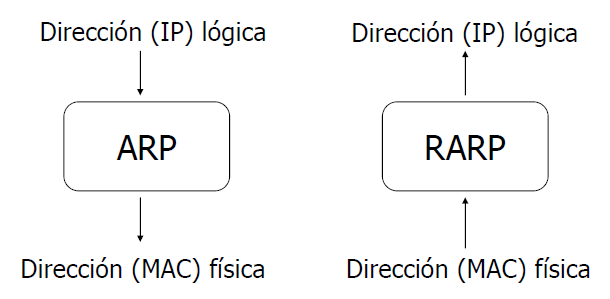
1. ***¿Cómo funciona el protocolo ARP? Explique muy brevemente. ¿Para qué sirve el “Gratuitous ARP”?***

El protopocolo ARP permite conocer la dirección MAC a través de su dirección IP. Funciona así: Transmite una difusión con la IP destino al servidor ARP y este le responde con la MAC destino.

Gratuitous ARP sirve para:

* Permiten detectar conflictos en IP
* Actualizan el contenido del cache ARP
* Informan a los switches el MAC del cliente conectado
* Sucede a cada cambio de estado de la interfaz 🡪 indicador de problemas

1. ***ARP vs RARP***



**Routeo en IP (Capa 3)**

1. ***¿Qué elementos fundamentales se almacenan en una tabla de routeo?***

Los elementos fundamentales que se almacenan en una tabla de routeo son: Dirección IP de red, máscara, default Gateway, métrica, interfaz.

1. ***¿Qué sucede si el router no encuentra información en la tabla de routeo para conmutar un datagrama?***

Se dispara el protocolo ICMP que le manda un mensaje de error al origen.

1. ***¿Qué es el tiempo de convergencia?***

El tiempo de convergencia de un protocolo de ruteo dinámico es el tiempo en que tardan en ser consistentes todas las tablas de routeo de los routers después de un cambio en la topología.

1. ***¿En qué elemento de información se basa la métrica utilizada por RIP?***

La métrica utilizada por RIP se basa en la cantidad de saltos.

1. ***¿Qué indica la recepción de un mensaje “destino inalcanzable”?***

***Indique 3 situaciones***

Ante la imposibilidad de conmutar/entregar un datagrama el router envia un mensaje ICMP antes de descartarlo.

***Motivos:***

* + Red No Disponible
  + Host Inalcanzable
  + Protocolo (TCP/UDP) no habillitado
  + Puerto no vinculado a un servicio
  + Fragmentación Necesaria, pero DF flag set
  + Fallo de la Ruta de Origen

1. ***Objetivo de un protocolo de routeo:***

* ***Flexible:*** Rápida adaptación a los cambios en la topología de la red
* ***Optimo:*** La optimalidad de un protocolo consiste en la habilidad para elegir la mejor ruta.
* ***Rápida Convergencia:*** La Convergencia ocurre cuando todos los routers dentro de una red poseen tablas de ruteo consistentes
* ***Robusto:*** Un protocolo robusto es aquel que mantiene su correcto funcionamiento aun en condiciones inusuales o impredecibles:
  + Alta utilización de los vínculos
  + Falla de Hardware
  + Configuraciones incorrectas
* ***Simple:*** La simplicidad de un protocolo se refiere a la habilidad de operar eficientemente.

1. ***Clasificación de un Protocolo de Ruteo:***

* Estáticos / Dinámicos
* Single-Path / Multi-Path
* Flat / Hierarchical
* Interior / Exterior
* Distance Vector / Link State

**Protocolos de Enrutamiento**

1. ***¿Qué función cumple un protocolo de ruteo? Indique 5 diferencias entre RIP y OSPF.***

La función de un protocolo de routeo es la de informar a todos sus routers el estado de cada uno de ellos a través de su tabla de routeo, como así también el mejor camino que se debe usar y el objetivo principal de transmitir datos entre todos los que conforman la red.

Los elementos fundamentales que se almacenan en una tabla de routeo son: Dirección IP de red, máscara, default Gateway, métrica, interfaz.

***Indique 5 diferencias entre RIP y OSPF.***

OSPF:

* Converge más rápido
* Sus rutas nunca presentan bucles
* Sobre IP
* Contiene menos información

***¿Qué es una métrica?***

La métrica es una medida que utiliza cada protocolo para definir qué camino tomar.

En RIP la métrica que se utiliza es cantidad de saltos.

En OSPF la métrica que se utiliza es el de mayor costo.

1. ***¿Qué función cumple un protocolo de ruteo? ¿En qué se diferencia un protocolo “Link State” de uno “Distance Vector”?***

La función de un protocolo de routeo es la de informar a todos sus routers el estado de cada uno de ellos a través de su tabla de routeo, como así también el mejor camino que se debe usar y el objetivo principal de transmitir datos entre todos los que conforman la red.

Link State (estado de enlace): Define el camino con mayor peso (mayor velocidad). Ej: OSPF.

Distance Vector (Vector distancia): Intercambio de info con los vecinos. Es decir, el menor camino entre los routers. ej: RIP

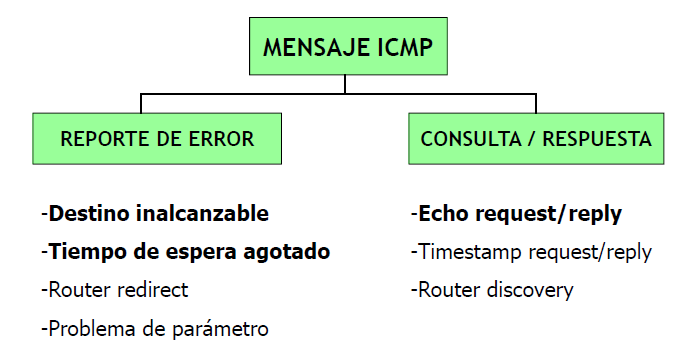
* OSPF funciona igual que EIGRP.

**ICMP**

***Función del Protocolo ICMP***

1. Comunica Errores a nivel de red
2. Informa acerca de eventos inesperados
3. Informa acerca de la red, en respuesta a consultas
4. Solo informa el error, no especifica qué acción correctiva tomar

***Tipos de Mensaje ICMP:***



* ***Destino Inalcanzable:***

Ante la imposibilidad de conmutar/entregar un datagrama el router envia un mensaje ICMP antes de descartarlo.

**Motivos:**

* + Red No Disponible
  + Host Inalcanzable
  + Protocolo (TCP/UDP) no habillitado
  + Puerto no vinculado a un servicio
  + Fragmentación Necesaria, pero DF flag set
  + Fallo de la Ruta de Origen

***PING/TracerRoute – Que mensajes utilizan?***

1. ***TracerRoute 🡪 Tiempo de Espera Agotado***

Motivos:

* El router detecta que el campo TTL debe decrementarse a 0
* El host destino ha desistido a la espera de un fragmento

1. **PING 🡪 Echo Request / Reply**

Utilizado para conocer si la interfaz destino es alcanzable y está funcionando

* + Echo request: Envia un identificador y un número de secuencia para contrastar requests y replies.
  + Echo reply: La respuesta no es obligatoria. Debe responder incluyendo los datos recibidos en el request.

1. ***¿Como descubre TracerRoute los routers a lo largo del camino?***

Envia mensajes con ttl creciente (1,2,3...), lo que genera un mensaje de icmp en cada salto.

**DHCP**

* Derivado del BOOTP, protocolo que permite la inicialización de computadoras sin disco rígido
* Centraliza y administra la asignación de direcciones IP
* Mantiene un registro de la IP asignada a cada cliente
* Asignación de Direcciones IP
  + Estática
  + Dinámica

Todo Host debe poseer:

* Dirección IP única
* Máscara de subred
* Default Gateway
* Servidor DNS
* Ventajas de la Asignación Dinámica
* Elimina la necesidad de llevar un registro de direcciones asignadas (facilita la administración)
* Facilita la modificación del espacio de direcciones de una red
* Permite la utilización eficiente de un espacio de direcciones reducido (más hosts que direcciones IP disponibles - ISP)
* Elimina la existencia de errores en la configuración
* Permite asignar a cada host todos los parámetros de configuración junto con la dirección IP

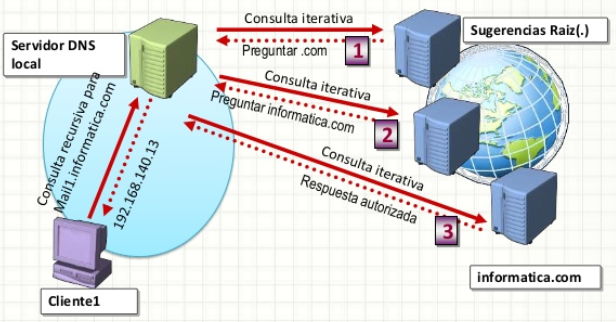
**DNS**

1. ***DNS. ¿Qué es una consulta DNS? ¿En qué se diferencia una consulta recursiva de una iterativa?***

Una consulta es una solicitud de resolución de nombres que se envía a un servidor DNS. Hay dos tipos de consultas:

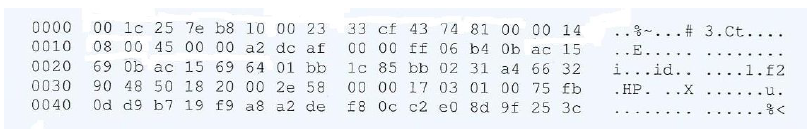
* Recursivas: Consulta Recursiva es aquella realizada a un servidor DNS, en la que el cliente DNS solicita al servidor DNS que proporcione una respuesta completa a la consulta.



* Iterativas: Una consulta iterativa es aquella efectuada a un servidor DNS en la que el cliente DNS solicita la mejor respuesta que el servidor DNS puede proporcionar sin buscar ayuda adicional de otros servidores DNS. 

**Práctica**

1. ***Analice la captura a continuación y responda:***



Ethernet:

MAC Destino: 00 1c 25 7e b8 10

MAC Origen: 00 23 33 cf 43 74

Protocolo: VLAN (81 00)

VLAN:

Prioridad|CFI|ID: 0014 (000|0|**0000 0001 0100**) 🡪 2^4+2^2 = 16+4 = 20

1. **¿A qué VLAN va dirigida la trama?**

VLAN 8100 🡪 VLAN 802.1Q

Va dirigida a la VLAN 20.

1. **¿Qué entrada existirá en el caché ARP del remitente? Indique MAC e IP.**

No existirá entrada en la Cache ARP debido a que tiene encapsulado protocolo 0800 y no protocolo 0806 que es el número de protocolo correspondiente para ARP.

1. **¿A qué clase pertenecen la dirección IP origen y destino?**

IP Origen: ac 15 69 0b = 172.21.105.11

IP Destino: ac 15 69 64 = 172.21.105. 100

Ambas son de Clase B que van de 128.0.0.0 a 191.255.255.255

1. ***El protocolo de nivel 2 de un vínculo que interconecta 2 redes LAN tiene un MTU de 1000 bytes. Si un host transmite un segmento TCP de 1460 bytes:***
2. **¿Cuántos fragmentos se crearán, si la cabecera IP tiene el bit DF = 1?**

Si DF=1 es que no admite fragmentación, por lo tanto, no es posible realizar la transmisión ya que no se podrían transmitir los 1460 bytes todos juntos, considerando que podés mandar máximo de a 1000 bytes.

1. **¿Cuántos, si el bit DF = 0?**

Con DF=0 se habilita la fragmentación, entonces:  
  
Cant. fragmentos = 1460/980 = 1,48 = 2 fragmentos (redondeo para arriba)  
  
980 porque le resté el tamaño de la cabecera TCP al MTU (1000-20=980). De los 1000 que podés mandar como máximo, 20 son de cabecera y 980 son de datos.

1. **¿Quién realizará la fragmentación, en caso de ser necesaria y posible?**

La capa de transporte del emisor, en este caso TCP, Router.

1. **¿Quién se encarga del reensamblado?**

La capa de transporte del receptor, en este caso TCP. Host Destino.

1. ***A partir de la dirección de broadcast 193.233.42.63, responda:***
2. ***¿Cuál es la dirección de red?***

Paso decimal a binario:

193 = 10000001

233 = 11101001

42 = 00101010

63 = 00111111

**10000001. 11101001. 00101010. 00**|111111

La dirección de red es: 193.233.42.0/26

1. ***¿Cuántas subredes existen, a su criterio?***

2^2= 4 subredes

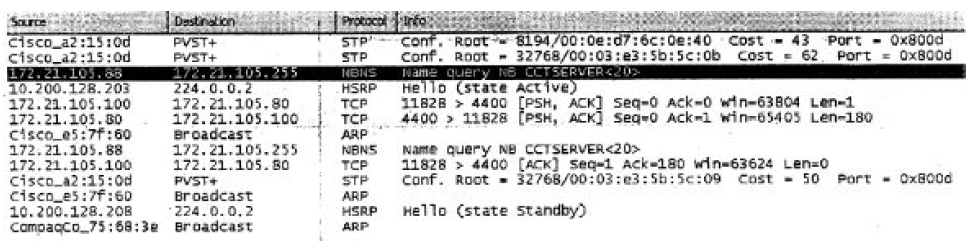
1. ¿Cuántas subredes se crearán a partir de aplica una máscara: 255.255.254.0 a la

red 172.21.0.0/16? ¿Cuál será la dirección de broadcast de la octava subred?

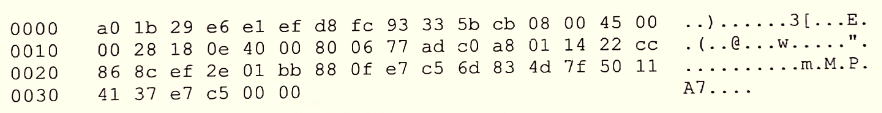
1. Aplicando la máscara 255.255.240.0 a la red 172.16.0.0/16, indique:
2. ¿Cuántas subredes se crearán?
3. ¿Cuál será la dirección de broadcast de la tercera subred?
4. ¿Cuántos dispositivos como máximo podrán conectarse a cada subred?
5. Dada la dirección de red 200.10.13.0 se desean armar 6 subredes. Indicar qué rango

de direcciones IP tendrá cada subred y la cantidad de hosts.

1. ***Analice la captura a continuación y responda***



1. ¿Cuántas direcciones IP identifica y a que clase pertenece cada una?
2. ¿Cuál es a su criterio la red a la cual estamos conectados? ¿Cuál es la máscara?
3. ¿A quién está dirigido entonces el datagrama resaltado?
4. Indique cuál es entonces la dirección MAC destino de esa trama Ethernet.
5. ¿Las tramas indicadas como ARP, son peticiones (requests) o respuestas (replies)? ¿Porqué?
6. Una red WAN compuesta por sitios debe modificar el direccionamiento IP de sus redes para adecuarse a las normativas de su casa matriz corporativa. Para esto debe utilizar el rango 171.17.10.0/23 y asignar un bloque a cada red. Las redes tienen 115, 68, 5, 10 y 12 dispositivos respectivamente.
7. ¿Cuántas subredes se crearán a partir de aplicar una máscara 255.255.224.0 a la red 172.21.0.0/16? ¿Cuál será la dirección de broadcast de la segunda subred?
8. ***Analizando la siguiente captura, responda:***



1. ***A partir de las direcciones IP origen y destino, determine si el datagrama ingresa o egresa del dispositivo donde se realizó la captura. ¿Cómo lo deduce?***

IP origen = c0 a8 01 14 = 192.168.1.20 (Clase C) 🡪 Publica

IP destino = 22 cc 86 8c = 34.204.134.140 (Clase A) 🡪 Privada

Ingresa a un host, debido a que va de una IP publica a una IP privada.

1. ***¿A qué dispositivo corresponde la dirección MAC destino?***

MAC Destino = a0 1b 29 e6 e1 ef

Corresponde a un host o un switch

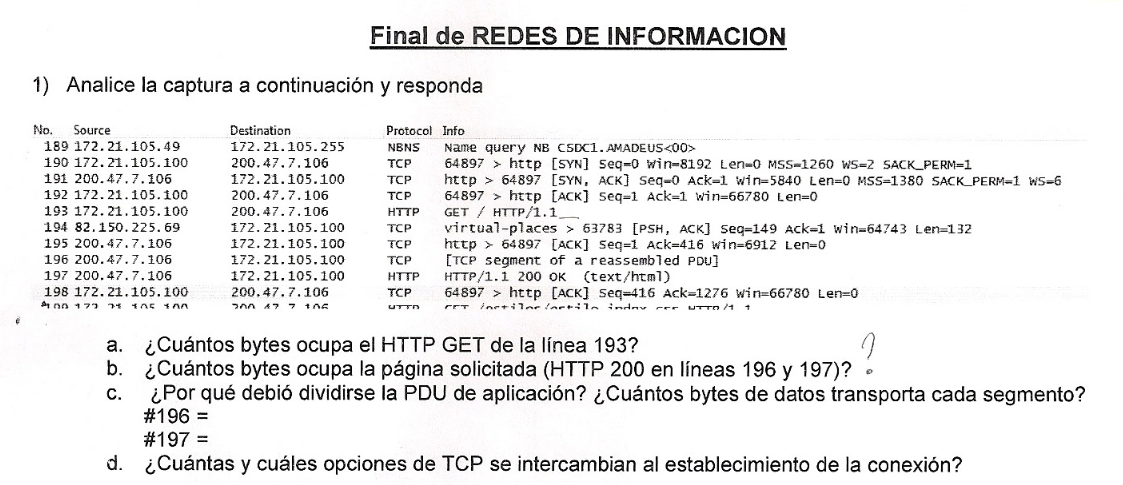
1. ***¿Cuántos “saltos” lleva dados el datagrama y por qué?***

TTL = 80 = 128

Todavía no salió del router, eso lo defino porque 128 es el máximo.

Puerto Origen = ef 2e = 61230

Puerto Destino = 01 bb = 443 = HTTPS

****

1. Como es un paquete HTTP, tenemos que fijarnos en el envío anterior.  
   Seq(#192) = 1 El paquete de 193 volverá a enviar el byte 1.  
   La línea #194 no se la tiene en cuenta por tener un source distinto.  
   En la línea #195 el ACK= 416, con lo cual se está pidiendo el B = 416, como anteriormente partimos del 1, tamaño de #193 = 415 B
2. También es un paquete HTTP, entonces miramos #195 y SEQ=1.  
   Al ver la respuesta en #198 ACK=1276, luego #196 + #197 = 1276 B -1B = 1275 B.
3. Debió dividirse por que el tamaño de datos a enviar era mayor al MSS utilizado en la sesión. Es el menor de los dos intercambiados al iniciar la misma, así que es 1260 (1275 es, efectivamente, mayor a 1260). El MSS es una de las opciones que se envían en los segmentos de inicio de sesión([SYN] (#190) y [SYN + ACK] (#191)). En este caso se intercambian MSS = 1260 y MSS = 1380.  
     
   #196 = 1260 B  
   #197 = 15 B
4. Opciones intercambiadas: MSS, WS, Sack\_Perm

***Con lo que debe obtener 6 respuestas:  
Ejemplo: red 192.168.1.0 máscara 255.255.255.224***

**1.** La cantidad de subredes utilizables se calcula tomando como base la cantidad de bits de la porción del nodo que se toman para generar subredes, y aplicando la fórmula siguiente:

2[bits de subred] – 2 = subredes utilizables

ejemplo:

23 – 2 = 6

**2.** La cantidad de direcciones de nodo útiles que soporta cada subred, surge de la aplicación se la siguiente fórmula que toma como base la cantidad de bits que quedan para identificar los nodos:

2[bits de nodo] – 2 = nodos

ejemplo:

25 – 2 = 30

**3.** La dirección reservada de la primera subred útil surge de restar a 256 el valor decimal de la porción de la máscara de subred en la que se define el límite entre subred y nodo:

256 – [máscara] = [primera subred útil y rango de nodos]

Las direcciones de las subredes siguientes surgen de seguir sumando la misma cifra.

ejemplo:

256 – 224 = 32

                             192.168.1.0         subred 0  
                             192.168.1.32       subred 1  - primer subred útil  
                 + 32     192.168.1.64       subred 2  
                 + 32     192.168.1.96       subred 3  
                 + 32     192.168.1.128      subred 4  
                 + 32      …  …  …

**4.**Las direcciones reservadas de broadcast se obtienen restando 1 a la dirección reservada de subred de la subred siguiente:

ejemplo:

32 – 1 = 31        192.168.1.31        subred 0  
64 – 1 = 63        192.168.1.63        subred 1  
96 – 1 = 95        192.168.1.95        subred 2  
128 – 1 = 127    192.168.1.127      subred 3  
… … …

5. La dirección IP del primer nodo útil de cada subred se obtiene sumando uno a la dirección reservada de subred:

reservada de subred + 1 = primer nodo utilizable

ejemplo:

32 + 1 = 33        192.168.1.33      primer nodo subred 1  
64 + 1 = 65        192.168.1.65      primer nodo subred 2  
96 + 1 = 97        192.168.1.97      primer nodo subred 3  
128 + 1 = 129    192.168.1.129    primer nodo subred 4  
… … …

6.  La dirección IP del último nodo útil de cada subred se obtiene restando 1 a la dirección reservada de broadcast:

63 – 1= 62          192.168.1.62     último nodo subred 1  
95 – 1 = 94         192.168.1.94     último nodo subred 2  
127 – 1 = 126     192.168.1.126   último nodo subred 3  
… … …

Sintetizando:

Con esa máscara de subred se obtienen 6 subredes útiles, cada una de ellas con una capacidad máxima de 30 nodos (32 direcciones IP):

#    Subred             Primer nodo útil        Último nodo útil           Broadcast  
0   192.168.1.0     
1   192.168.1.32     192.168.1.33            192.168.1.62              192.168.1.63  
2   192.168.1.64     192.168.1.65            192.168.1.94              192.168.1.95  
3   192.168.1.96     192.168.1.97            192.168.1.126            192.168.1.127  
4   192.168.1.128   192.168.1.129          … … ...                     … … …



a) Digo que la dirección 91.0.0.0 es de Clase A pq en binario empieza con 01 y no me dicen q la dirección que me dieron es sin clase.

Por eso tengo una máscara /8 para la red. Luego como la dirección que me dan tiene una máscara /20 puedo saber que los bits destinados para subred son 20-8 = 12. Ordenando me que quedaría 8bits para red + 12 para subred + 12 para hosts.

Sabiendo eso y que me piden la subred nro 3419(en binario 1101 0101 1011):

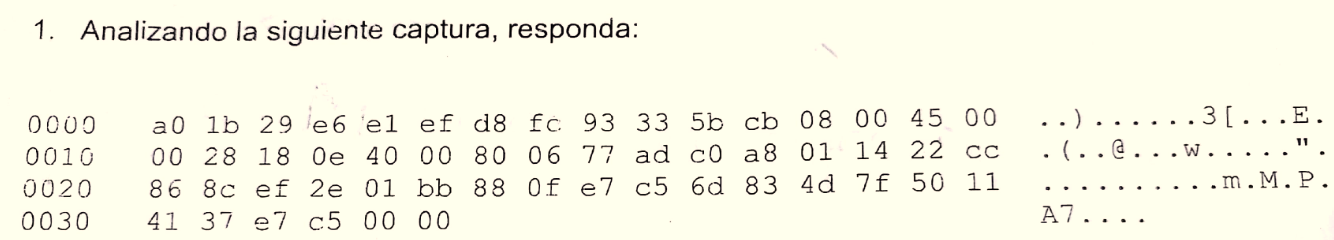
en binario los últimos octetos 91.00000000.00000000.00000000 + 1101 0101 1011 = 91.11010101.10110000.00000000 en decimal 91.213.176.0/20 es la subred 3419.

b) primer host: 91.213.176.1/20

c) ultimo host: 91.213.176.254/20

d)dir de broadcast: 91.213.176.255/20

e) Nro de dir para host = 2^n -2(n: nro de bits utilizados para hosts) 🡪 Nro de dir para host =2^12 - 2 = 4094



1. ***A partir de las direcciones IP origen y destino, determine si el datagrama ingresa o egresa del dispositivo donde se realizó la captura. ¿Cómo lo deduce?***

MAC Destino = a0 1b 29 e6 e1 ef

MAC Origen = d8 fc 92 33 5b cb

Tipo de Trama = 0800

Versión = IPv4

Longitud de Cabecera = 5

Tipo de Servicio = 00

Longitud Total = 00 28

Datagrama ID = 18 0e

Flags + Offset = 40 00 |0100|0000|0000|0000

TTL = 80

Tipo de Protocolo = 06 (TCP)

CheckSum = 77 ad

**IP Origen = c0 a8 01 14 = 192.168.1.20 🡪 Clase C 🡪 IP Publica**

**IP Destino = 22 cc 86 8c = 34.204.134.140 🡪 Clase A 🡪 IP Privada**

Puerto Origen = ef 2e = 61230

Puerto Destino = 01 bb = 443 (HTTPS)

Sequence Number = 88 0f e7 c5

ACK Number = 6d 83 4d 7f

Data Offset + Reserved + Flags = 50 11 🡪 0101|0000|0001|0001 ACK+FIN

A partir de las direcciones IP origen y destino, puedo deducir que Ingresa a un host, debido a que va de una IP publica a una IP privada.

1. ***¿A qué dispositivo corresponde la dirección MAC Destino?***

MAC Destino = a0 1b 29 e6 e1 ef

Corresponde a un host o un switch

1. ***¿Cuántos “saltos” lleva dado el datagrama y por qué?***

TTL = 80 = 128

Todavía no salió del router, eso lo defino porque 128 es el máximo.

1. ***¿De qué aplicación se trata?***

Está utilizando la aplicación HTTPS debido a que el puerto destino es 443

Puerto Destino = 01 bb = 443 (HTTPS)

1. ***¿En qué estado se encuentra la conexión?***

Data Offset + Reserved + Flags = 50 11 🡪 0101|0000|0001|0001 ACK+FIN

**CLOSE\_WAIT** – La conexión remota ha terminado, y está a la espera que se cierre el socket.

1. ***Una consola de monitoreo sondea dispositivos en la red utilizando SNMP (Protocolo Simple de Administración de Red). Para monitorear 50 routers de una red Frame Relay, envía mensajes GetRequest-PDU (44 bytes\*) sobre el siguiente acceso:***

***Access Rate: 256 kbps***

***CIR: 50%***

***EIR: 64 Kbps***

***SNMP trabaja sobre UDP***

***Indique:***

1. ***¿Con qué frecuencia máxima [Poll/Sec] puede sondear a los dispositivos, asegurando que TODOS los mensajes se transporten garantizados (sin marcar)?***

CIR/(Trama\* cantidad de routers)

128000/(624\*50) = 128000/31200 = 4.10 -> La frecuencia maxima es 4 Poll/Seg

1. ***¿Cuántos dispositivos podrá sondear [por segundo] como máximo, sin ningún mensaje debe ser rechazado por la red (descartado)?***

128000/ 624 = 205.12 -> La cantidad máxima es 205

1. ***¿Qué se debe hacer para monitorear con esta estación a 2000 routers? Indique 3 alternativas.***

* Aumentar el Access Rate
* Disminuir el tamaño de la trama
* Monitorear en intervalos por grupo

[Flag(1 B)+DireccionFR (2 B)+[Caberecera IP (18 B)+[Cabecera UDP (8 B)+[SNMP 44 B] ] ] + FCS (2 B) + Flag (1 B)] = 78 Bytes (Total Trama)

Cabecera IP: 18B

* MAC Destino: 6 B
* Mac Origen: 6B
* CRC: 4 B
* EtherType: 2 B  
  Flag FR: 1 byte

Dirección FR: 2 bytes

Cabecera IP: 20 bytes

Cabecera UDP: 8 bytes

Mensaje SNMP: 44 bytes  
FCS FR: 2 bytes

Flag FR: 1 byte

Trama: 78 Bytes 🡪 78 \* 8 = 624 Bits.

Access Rate: 256000 bps

CIR: 128000 Porque que es 256000/2 = 1280000

EIR: 64000 bps

1. ***Particione el rango de direcciones 10.16.0.0/22 de la manera más eficiente posible para cubrir las necesidades de direccionamiento de las siguientes redes: a) 256 hosts, b) 70 hosts y c) 58 hosts. Indique en cada caso, la dirección de sub-red y la máscara o prefijo asignados.***

10.16.0.0/22

IP 00010000.00010110.00000000.00000000

Mascara 11111111.11111111.11111100.00000000

Piden host no direcciones-> hay que restar 2 a la cantidad de direcciones por estar reservadas para dirección de la subred y del broadcast

256 host 🡪 9 bit de direccionamiento 🡪 32-9 = 23

70 host 🡪 7 bit de direccionamiento 🡪 32-7 = 25

58 host 🡪 6 bit de direccionamiento 🡪 32-6 = 26

00010000.00010110.0000000/23

.00000010.0/25

.10/26

a) IP 10.16.0.0/23

b) IP 10.16.2.0/25

c) IP 10.16.2.128/26