

19/12/2012

1) Explique cómo realizan los distintos protocolos para eliminar y solucionar los problemas de congestión. Grafico que muestre la congestión y el retardo en las tramas.

TCP – orientado a la conexión. 3-way-handshake. RTS/CTS. **Mecanismo de ventana deslizante.**

X.25 / LAPB / HDLC – Ventana deslizante y Piggyback (WikiPérez)

Frame Relay (LAPF) – campos FECN, BECN, DE.

ATM. Utiliza celdas fijas. Se negocia el tipo de tráfico y servicio entre las terminales. La red ATM supervisa que los paquetes cumplan con el acuerdo establecido, si no lo hacen, los descarta o los marca para potencial descarte. Además adaptar y suavizar el tráfico almacenando celdas en buffer??

El header ATM tiene un campo de 1 bit ->CLP: Prioridad de pérdida de celda. (0=alta, 1=puede descartar)

2) Explique que el uso de temporizadores IFS en wireless y diga los valores de DISF y SISF para las redes 802.11 a b g

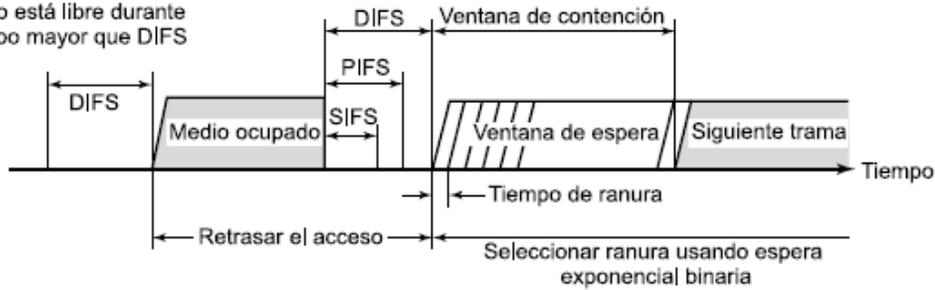
SIFS (IFS corto, *short IFS*): es el IFS más pequeño y se utiliza para todas las acciones de respuesta inmediatas, tal y como se explica más adelante.

PIFS (IFS de la función de coordinación puntual, *Point coordination function IFS*): se trata de un IFS de tamaño medio, utilizado por el controlador central en el esquema PCF cuando emite un sondeo.

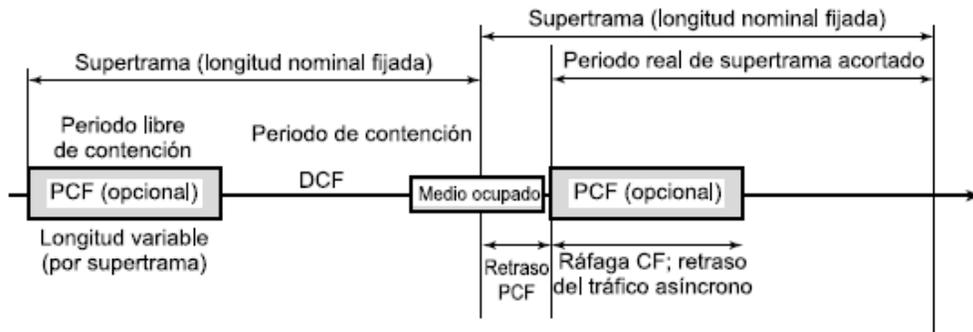
DIFS (IFS de la función de coordinación distribuida, *Distributed coordination function IFS*): constituye el IFS más grande y se usa como un retardo mínimo para las tramas asíncronas que compiten por el acceso al medio.

STA: 575

Acceso inmediato cuando el medio está libre durante un tiempo mayor que DIFS



(a) Método básico de acceso



(b) Uso de las supertramas por la PCF

Figura 17.7. Ordenación temporal de los eventos MAC en IEEE 802.11.

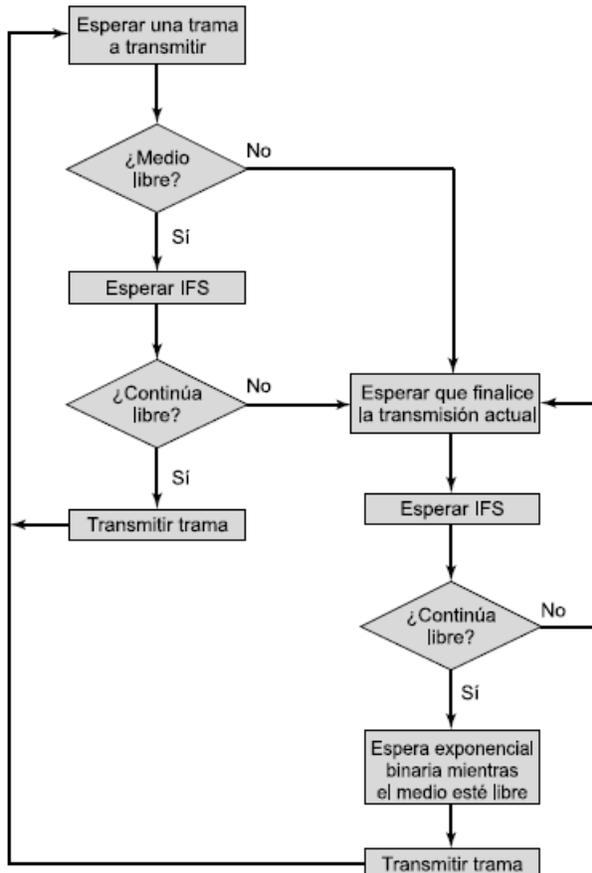


Figura 17.6. Lógica de control de acceso al medio en IEEE 802.11.

DIFS: Tiempo que debe censar el medio como libre antes de transmitir.
 SIFS: Tiempo que debe esperar la terminal antes de responder un mensaje.
 SIFS < DIFS

802.11 Wireless LAN Standards			
	802.11a	802.11b	802.11g
Velocidad (Mbps)	54	11	54
Frecuencia de operación (GHz)	5	2.4	2.4
Compatibilidad	No compatible con 802.11b o 802.11g	No compatible con 802.11a o 802.11g	Compatible con 802.11b
Rango	150feet	150feet	150feet
Riesgo de interferencia	Bajo	Alto	Alto
Precio	Caro	Barato	Moderado

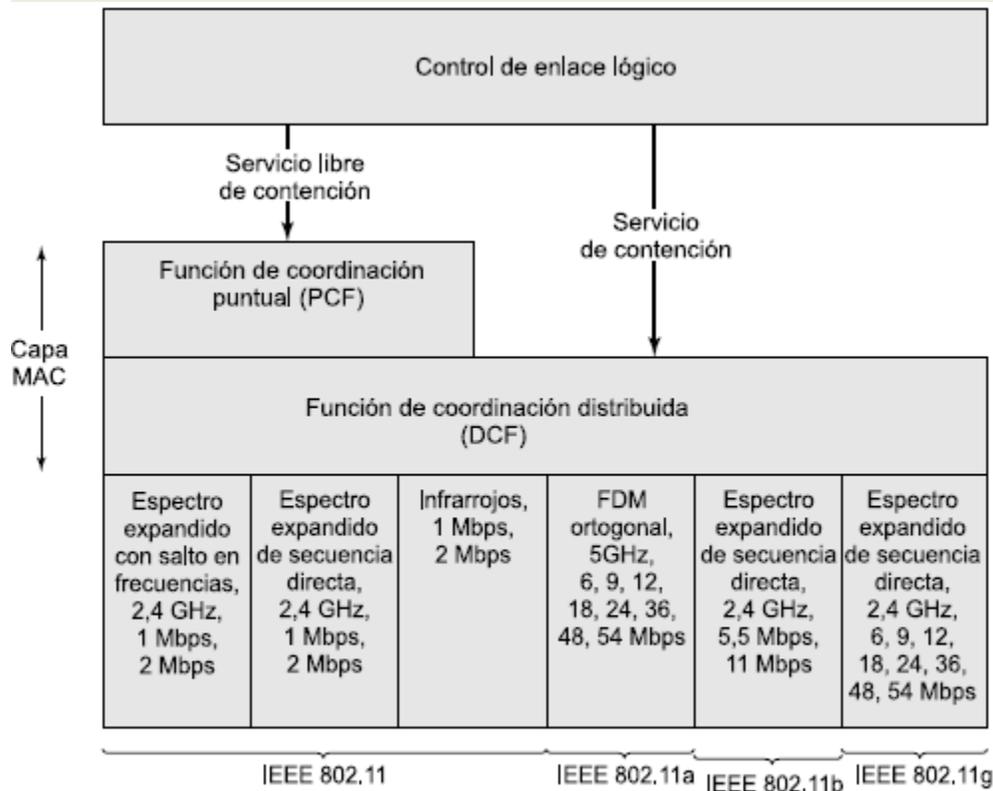


Figura 17.5. Arquitectura de protocolos IEEE 802.11.

13/02/2013

3) WiFi. 802.11. Cuáles son los tres principales tipos de tramas, para qué se utilizan y qué campo de la trama las identifica

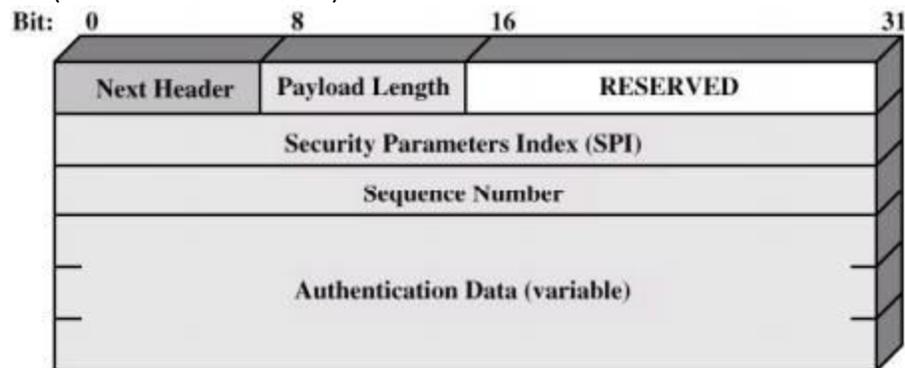
- Datos (00): los datos del usuario, null, otros (sin datos)
- Control (01): Power Save-Poll (PS-Poll), RTS, CTS, ACK
- Gestión o Supervisión o Management (10): para gestionar las comunicaciones entre las estaciones y los AP. Funciones que cubren incluyen la gestión de las asociaciones (solicitud, respuesta, reasociación, disociación y autenticación).

Las identifica el primer campo de la trama. "Tipo de trama" o "Frame Control" (FC). Son 2 bytes.

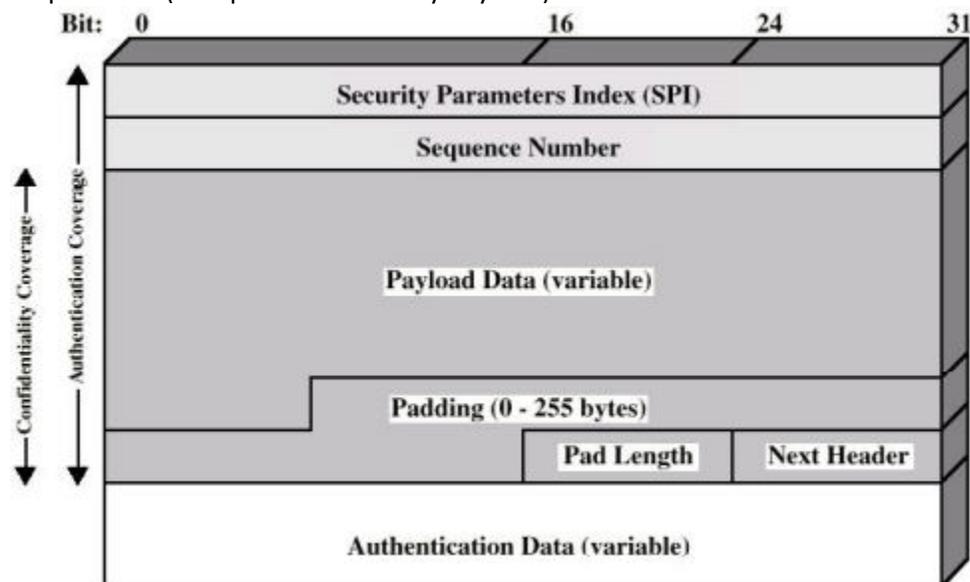
[Stallings página 578]

4) IPsec. Protocolos ESP y AH. Explique las acciones que llevan a cabo los mismos en los modos TRANSPORTE Y TUNEL

AH (Authentication Header)



Paquete ESP (Encapsulation Security Payload)



25/02/2015 – Perez.

[Protocolos de IPsec](#)

*Internet Key Exchange (IKE).

Negociación de parámetros e intercambio seguro de claves.

***Authentication Header (AH).**

Proporciona **autenticación e integridad**.

***Encapsulating Security Payload (ESP).**

Proporciona **confidencialidad**. (Encriptación)

- AH ()
 - Agregado después del encabezamiento IP
 - No es un campo opcional del IP
 - En el encabezamiento IP se cambia el campo "Protocol"
 - Usa el formato IP versión 6
 - No se envía toda la información de seguridad, sólo pequeños índices preasignados a los parámetros
- ESP ()
 - Encripta el contenido de los paquetes
 - Agrega un encabezamiento de 8 octetos y una cola con autenticación

Modos de uso:

***Transporte:** protege los datos de la capa de transporte, extremo a extremo. Típicamente, entre hosts.

***Túnel:** protege el datagrama IP completo, encapsulándolo dentro de otro. Obligatorio cuando uno o ambos extremos se comportan como Gateway (red).

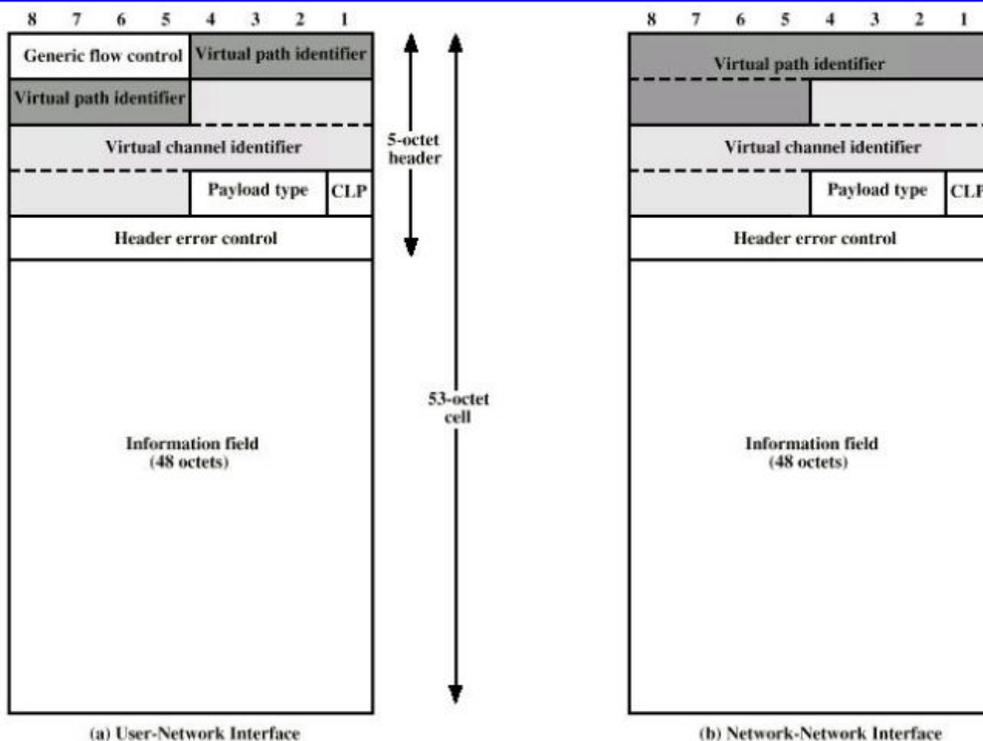
<https://es.wikipedia.org/wiki/IPsec>

5) ATM. Campo TIPO DE CARGA UTIL. Indique el significado de cada uno de los bits.

Repasar **CELDA completa de ATM**.

- PTI (Payload Type Identifier) o TCU (Tipo de Carga Útil):
 - o Primer bit: 0=Datos Usuario; 1=Info
 - o **Segundo bit: 0=No Congestión; 1=Congestión**
 - o Tercer bit: 0=Intermedio; 1=fin.

Formato de Celdas ATM



6) Frame Relay. DLCI completo, garantía de que la trama llegue a destino/cómo se corrigen errores. Detallar la trama FR general y el significado de cada campo.

- DLCI: identificador de conexión del enlace de datos
- Representa el número del CV (Circuito Virtual) de FR correspondiente a una conexión en particular
- En el caso de interconexión LAN / WAN, el DLCI define el puerto virtual al cual la LAN de destino está conectada
- Los DLCIs tienen **validez local**: entre el FRAD y la red
- Hay una tabla en cada conmutador asociando un DLCI en uno de sus puertos a otro DLCI en otro de sus puertos

Trama Frame Relay



DLCI normal y extendido

El encabezado de FR puede ser extendido a 3 ó 4 bytes para aumentar el direccionamiento



7) Para qué se usa la firma digital y citar ejemplos de protocolos que la usan.

Firma digital

- El trasmisor encripta el mensaje con su clave privada
- El receptor puede desencriptar usando clave pública conocida

- Sirve para autenticar al trasmisor, quien es el único que tiene la clave correcta
- No da privacidad a los datos porque la clave es pública
- Garantiza la integridad del documento

Los protocolos que usan Firma Digital son ... ¿?

27/02/2013

8) Indicar las direcciones ESPECIALES de IPv4 y citar la RFC correspondiente.

Las DIR que comienzan con 127, con 255 o que están entre 224 y 247 son reservadas (Tipo D y E)

IP Privadas

10.0.0.0 al 10.255.255.255 (clase A)

172.16.0.0 al 172.31.255.255 (clase B)

192.168.0.0 al 192.168.255.255 (clase C)

169.254.0.0 al 169.254.255.255 (clase B)

- Valores especiales

—Dirección de red: bits de host en 0

—Dirección de broadcast local: bits de network y host en 1

—Dirección de broadcast remoto: bits de host en 1

*Multicast: Consiste en utilizar una dirección clase D, la cual especifica el grupo de dispositivos que recibirán el paquete

*0.0.0.0

*127.0.0.0

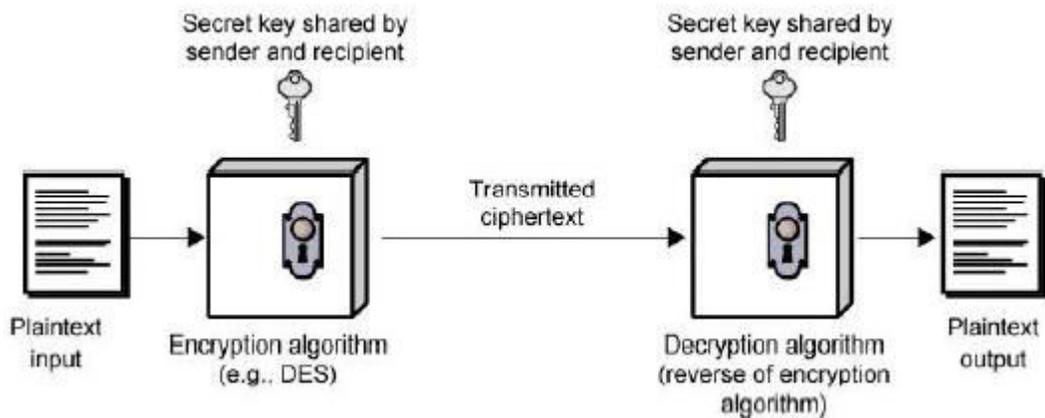
*Direcciones privadas

<http://www.sobrepc.com/internet/direcciones/direcciones2a.html>

RFC: 791

9) Ventajas y desventajas de usar cifrado Simétrico o Asimétrico.

Encriptación Simétrica



Ingredientes

- Texto plano
- Algoritmo de Encriptación
- Una sola clave secreta
- Texto cifrado
- Algoritmo de desencriptación

VENTAJAS:

- Muy **fácil de usar**.
- Es muy útil para el cifrado de archivos de datos personales, **ya que sólo se requiere de una clave**
- **Es rápida y utiliza menos recursos** informáticos que otras formas de cifrado
- Si utilizas diferentes claves compartidas con diferentes personas, cuando una de las claves está en peligro, sólo una persona se ve afectada en lugar de todos.

http://www.ehowenespanol.com/ventajas-desventajas-criptografia-clave-simetrica-info_276624/

Algoritmos simétricos

• Inconvenientes:

—**Cómo garantizar el intercambio seguro de claves sin un canal seguro?**

—Además, el **manejo de claves es complejo** (usuarios = $x(x-1)/2$ claves) $n(n-1)/2$ ¿No debería ser una clave por receptor?

—Los mensajes **no son irrepudiables**.

—Es necesario ponderar claramente los riesgos antes de implementar.

Encriptación asimétrica

- Conocida como encriptación de “Encriptación de Clave Pública”
- Los extremos pueden utilizar el mismo algoritmo o uno diferente pero complementario para encriptar y desencriptar la información
- Dos valores de clave diferentes, pero complementarios una clave pública y una clave privada

Requisitos para Seguridad

- Fuerte algoritmo de encriptación
- Aunque sea conocido no se puede desencriptar sin la clave
- Las claves secretas se deben distribuir de manera segura
- Conocida la clave toda la comunicación es clara

Algoritmos asimétricos

• Ventajas:

—**Muy fuertes**, dadas las implementaciones correctas.

—**Proporcionan servicios de confidencialidad, integridad, autenticidad (sin restricciones)**

—Los mensajes con firma digital son **irrepudiables**

—El **manejo de claves es más sencillo** (usuarios = pares pública/privada) y **no requiere un canal seguro para comunicar la clave pública**.

• Inconvenientes:

—Son **más lentos** en términos de ejecución

—Son **más difíciles de implementar**.

—Es necesario ponderar los riesgos antes de implementar.

https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica#Ventajas_y_desventajas_del_cifrado_asim.C3.A9trico

04/12/2013 – Echazú?

10) Cuando se implementa una red compleja con switches de core y de borde para que se utiliza el Spanning Tree Protocol (STP)? Construya un ejemplo.

Se utiliza para garantizar que no existan bucles en la topología. Arma una topología lógica de red en forma de árbol sin bucles. Los bucles físicamente existen para garantizar la disponibilidad de conexiones.

https://es.wikipedia.org/wiki/Spanning_tree

11) Que entiende por sistema autónomo, como se conectan los sistemas autónomos? Describa un protocolo de enrutamiento que opere con el vector de distancia y otro que utilice el estado del enlace, cuando emplearía cada uno?

Es un grupo de redes que posee una política de rutas propia e independiente, realiza su propia gestión del tráfico. Los SA se comunican entre sí mediante routers, intercambiando información para tener actualizadas sus tablas de ruteo mediante el protocolo BGP. [Sacado del Word]

- Un Sistema Autónomo (AS) es el que maneja un administrador, tiene sus propios algoritmos internos y se conecta con otros AS
- Un AS tiene routers
 - Interiores
 - De frontera ()

Algoritmo vector distancia

- Utiliza una tabla inicial
 - Periódicamente los routers vecinos intercambian información
 - Si un router recibe información con menor cantidad de saltos para una red, actualiza su tabla con esa dirección
- Lo emplearía para una red pequeña/básica. No funciona si se necesitan más de 15 saltos.
- Ej.: RIP (Router Information Protocol)

Ventaja: Muy fácil de configurar.

Desventajas: Se intercambian paquetes cada 10 segundos, aunque no haya cambios en la topología. No tiene en cuenta otras métricas, sólo los saltos. No funciona con más de 15 saltos.

Algoritmo estado de enlaces

- Por medio de mensajes de broadcast cada router mide la menor distancia a cada red
- La distancia se mide por varios criterios
 - retardo (delays)
 - ancho de banda (AB)
 - saltos
 - confiabilidad
 - jitter
 - costo

Lo emplearía para una red grande/compleja.

Ej.: OSPF (Open Shortest Path First)

Ventajas: Es mejor, tiene en cuenta más métricas, no se envían paquetes si no hay cambios en la topología.

Desventaja: Requiere mayor procesamiento.

11/12/2013

12) ¿Qué campos utiliza el protocolo TCP para MULTIPLEXAR la información que envía?

Los campos que utiliza son: Puerto Origen, Puerto Destino. [Yo]

Permite multiplexar los datos, es decir, que la información que viene de diferentes fuentes (por ejemplo, aplicaciones) en la misma línea pueda circular simultáneamente. [Wiki]

13) Explique los campos que conforman la trama MPDU (Mac PDU) de una red IEEE 802.11 e indique cuantos tipos de tramas existen

SEMI-REPETIDO: 13/02/2013



Figura 17.8. Formato de la trama MAC en IEEE 802.11.

14) IPsec. Indique las diferencias entre los protocolos AH y ESP.

REPETIDO: 13/02/2013

18/12/2013 – Echazú?

15) En qué unidades se mide el ruido en un cable.

Potencia del ruido presente en el canal, (mW, microW, etc.) que trata de enmascarar a la señal útil.

16) Tipos de transmisión inalámbricas. Gráfico de frecuencias.

RESPONDIDA: 26/02/2014

17) Indicar tres diferencias entre ATM y FR

	X.25	FRAME RELAY	ATM
Niveles de protocolos	1,2,3 Osi	1,2 Osi	Medio físico, atm, aal
Vel bin max	64 kbps	2 mbps	622 mbps y más (2,4 gbps)
Control de errores	Salto por salto Lap-b (hdlc)	Nodos interme-dios rtx. Extremos detectan, no recuperan. Lap-f y lap-d (hdlc)	Solo de extremo a extremo Control de header de celda
Soporte com	Red analógica y digital Baja calidad	Isdn Mejor calidad	B-isdn Alta calidad
PDU	Trama y paquete	Cuadro	Celda o celula
Longitud de la PDU	Grande y variable (16/1024 b paq)	Grande y variable (1600/4096 b)	Pequeña y fija (53 b)
Tipo de tráfico más adecuado	File transfer, batch, correo electrónico	Ráfagas (lan), voz	Info en tiempo real, voz, video, video-conferencia
Tipo de servicio	O. Conexión	O. Conexión	O. Conexión
Conmutación	Por software (mayor procesamiento)	Por software (menor procesamiento)	Por hardware (menor retardo)
Multiplexión e identificadores	Lc (canal lógico) Vc (circuito virtual) Lci	Vc (circuito virtual) Dlci	Vp (camino virtual) Vc (canal virtual) Vpi y vci

Eficiencia	Asignación fija	Asignación por demanda	Asignación por demanda
-------------------	-----------------	------------------------	------------------------

Comparación entre sistemas

	TDM	X.25	FRAME RELAY	ATM
Facilidades	Muy pocas	Muchas	Pocas	Pocas
Velocidad	Alta	Media	Alta	Muy Alta
Retardo	Muy bajo	Alto	Bajo	Muy bajo
Throughput	Alto	Bajo	Alto	Muy alto
Coste CPE	Bajo	Bajo	Bajo	Alto
Overhead	Bajo	Bajo	Bajo	Alto
Puerto Comp.	No	Sí	Si	Si
Tipo tráfico	Cualquiera	Datos	Datos/voz	Multimedia

12/02/2014

18) Detallar los campos del paquete X 25 de datos.

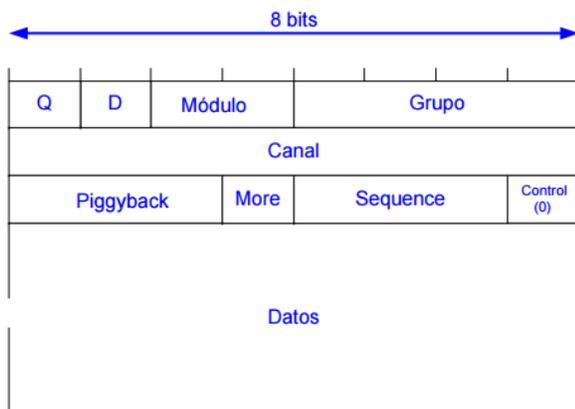
Repasar Paquete X.25

Nivel 2 – LAPB - (HDLC)



NIVEL 3 (RED)

FORMATO DEL PAQUETE



- Bit **Q** no está definido (lo usa la capa 4)
- Bit **D** cambia significado de PIGGYBACK indicando quién recibió el paquete (DTE=1 o DCE=0)
- Campo **CONTROL** en 0
- Campos **SECUENCIA** y **PIGGYBACK** hacen control de flujo con ventanas deslizantes
- Campo **MODULO**
 - 01: hay 7 ventanas (3bits) enlaces terrestres
 - 10: hay 127 ventanas (7 bits) enlaces satelitales
- **Datos** de usuario: generalmente 128 octetos

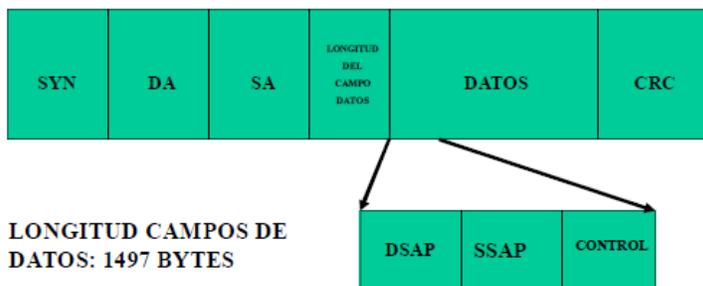
- El bit **Q** indica datos cualificados. Esto no está definido en X.25 pero la idea es que el protocolo de transporte lo use para separar sus paquetes de control y datos.
- El campo **CONTROL** está siempre a 0.
- Los campos **SECUENCIA** y **PIGGYBACK** se usan para control del flujo por un mecanismo de ventana deslizante. Los números de secuencia son Mod-8 si el campo **MODULO** es 01 y Mod-128 si es 10 (00 y 11 son ilegales). Si se usan números de secuencia Mod-128 la cabecera se extiende con un byte extra para acomodar los campos más largos de secuencia y piggyback (4 bits adicionales para cada uno).
- El significado del campo de piggyback lo determina el bit **D**:
 - ✓ **D=0** → la siguiente confirmación indica que el DCE local recibió el paquete, y no que el DTE remoto lo recibió.
 - ✓ **D=1** → la confirmación es realmente indicio de una recepción correcta del paquete en el DTE remoto al otro extremo.
- Aunque D valga 0 el campo de piggyback es útil pues le indica al DTE que su DCE está listo para el próximo paquete (controlando así el flujo DTE→DCE).

Más: <http://www.lcc.uma.es/~eat/courses/cdd-contents/tema5.pdf>

<http://www.utnianos.com.ar/foro/tema-final-de-redes-12-02-2014?pid=369873#pid369873>

19) Detallar la estructura de la trama Ethernet IEEE 802.3 con cabecera 802.2 LLC.

TRAMA ETHERNET IEEE 802.3 CON CABECERA 802.2 LLC



DSAP Y SSAP se emplean para identificar el protocolo

DA: Destination Address. SA: Source Address

DSAP: Destination Service Access Point. SSAP: Source Service Access Point. 1 byte cada uno.

El campo de Control es igual al del protocolo HDLC. Usa versión 8 o 16 bits según el servicio.

https://es.wikipedia.org/wiki/Control_de_enlace_l%C3%B3gico

https://es.wikipedia.org/wiki/IEEE_802.2

19/02/2014 – Echazú?

20) ¿Cómo se desarrolla una **tabla de encaminamiento con la técnica de "Árbol de expansión"? ¿Qué **identificadores** se utilizan para dicha tabla y cómo se obtiene el de mayor prioridad?**

Explicar cómo funciona STP

Identificador: BID, N° de puerto?

Cada SW tiene una tabla con una lista de sus puertos, una columna indica el número de puerto/interfaz y otra columna índice si es Raíz, Designado o Bloqueado ¿?

El BID de mayor prioridad es, por defecto, el del Switch de menor MAC.

El puerto de mayor prioridad es, por defecto, el menor. El administrador puede cambiar estas prioridades.

Como puerto Raíz se elige aquel que conduzca más rápido al Swtich raíz. [Yo]

21) SIFS, DIFS, PIFS. Para qué se utilizan, qué tramas usan.

SEMI-REPETIDA: 19/12/2012

26/02/2014 - Echazú

22)a) Enuncie 3 diferencias entre x.25 y Frame Relay

b) Cuáles son los campos para controlar la congestión que dispone Frame Relay.

REPETIDA: 19/12/2012, 18/12/2013

22)a) Definición de NEXT, en que mide y cómo es su cálculo.

- **Near End cross Talk:** es la diafonía o interferencia entre pares, medida en el mismo extremo
- El peor caso que puede ocurrir es que el par de transmisión en el conector que transmite interfiera la señal en el par de recepción (justo donde la sensibilidad de la recepción es más alta).

• Se calcula como:

$$\text{NEXT [db]} = 10 \log (\text{Pot par tx/Pot par rx}) = 10 \log (P2/P1)$$

• La diafonía depende de:

—Calidad de la mano de obra

—Desarmado de las **trenzas**

—La **frecuencia** (o la **velocidad**)

• La dificultad de la diafonía es el poder determinar el punto exacto donde ocurre

Lo ideal es una diafonía infinitamente negativa (P2 = 0). [UD3 - RI (LAN Cableado_Estructurado) UD 3]

22)b) Los 3 tipos de tecnologías Wireless y un **gráfico de Seudoruido.**

REPETIDA (b): 18/12/2013

Tecnologías

• **Infrarroja (IR):**

— celda individual limitada a un salón

— la luz IR no penetra paredes opacas

• **Radio por espectro expandido (SS):** operan en banda de microondas para usos industriales

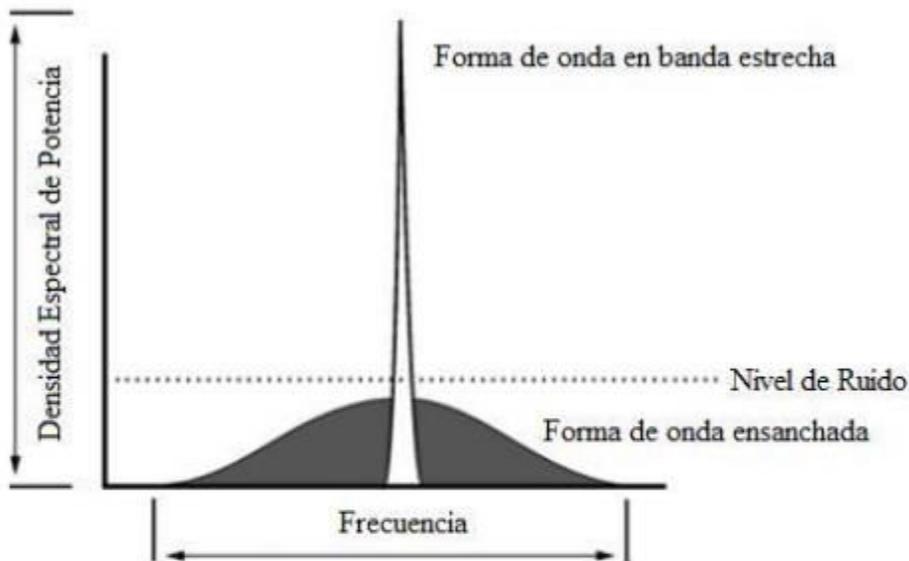
—No requieren licencia

• **Microondas (radioenlaces):** frecuencias fijas

—En algunos casos requiere licencia

[Para ampliar ver: 40-Redes inalambricas-1.pdf] [RI (LAN inalambricas) UD 4]

SECUENCIA DIRECTA



SALTO DE FRECUENCIA

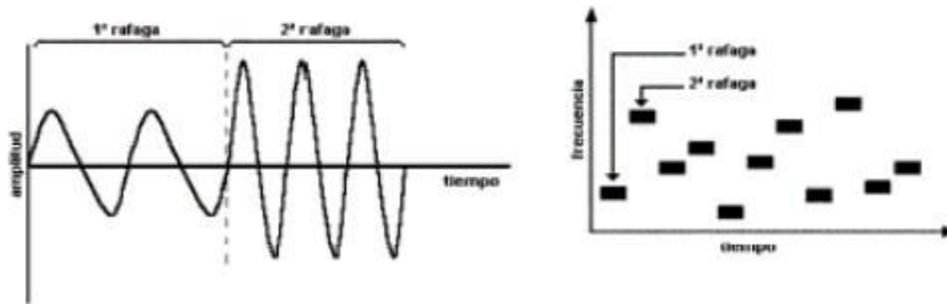


Figura 9: Gráfica de Codificación con Salto en Frecuencia

16/07/2014 – Perez?

23) 802.11. DIFS, SIFS – Para qué se utilizan.

REPETIDA.

24) IPv6. Cabeceras de extensión. Qué son, para qué se utilizan. En qué casos no le sigue ninguna.

Cabecera de extensión: Permite definir campos adicionales sin cambiar el protocolo. Sin embargo, no se puede asumir que estos campos sean reconocibles por el destinatario.

Cabecera de Extensión	Tipo	Descripción
Opciones salto a salto (<i>Hop-By-Hop Options</i>)	0	Contiene datos que deben ser examinados por cada nodo a través de la ruta de envío de un paquete

Enrutamiento (<i>Routing</i>)	43	Métodos para especificar la forma de rutear un datagrama. (Usado con IPv6 móvil)
Cabecera de fragmentación (<i>Fragment</i>)	44	Contiene parámetros para la fragmentación de los datagramas
Cabecera de autenticación (<i>Authentication Header (AH)</i>)	51	Contiene información para verificar la autenticación de la mayor parte de los datos del paquete (Ver IPsec)
Encapsulado de seguridad de la carga útil (<i>Encapsulating Security Payload (ESP)</i>)	50	Lleva la información cifrada para comunicación segura (Ver IPsec)
Opciones para el destino (<i>Destination Options</i>)	60	Información que necesita ser examinada solamente por los nodos de destino del paquete
No Next Header	59	Indica que no hay más cabeceras

25) IP/MPLS. Describir el protocolo. Ventaja (utilidad) sobre ATM para transportar datagramas.

MultiProtocol Label Switching

- Mecanismo de conmutación basado en etiquetas (labels)
- Diseñado para transportar múltiples protocolos de capa 3
- Las etiquetas MPLS identifican las redes Destino

Beneficios[PPT Koval]

- Ruteo de IP unicast y multicast
- VPN
- QoS
- MPLS reduce la tarea de conmutación en el “core”
- Puede transportar otros protocolos, no solo IP

Beneficios [ppt Fusario]

- Tiene las funciones de capa 3 con el rendimiento de capa 2
- Ruteo más criterioso e independiente de la arquitectura de la red
- Permite hacer túneles más eficientes que IP
- Mejora precio, desempeño, escalabilidad
- Soporta ingeniería de tráfico y calidad de servicio (QoS)

MPLS está reemplazando rápidamente a FR y a ATM como la tecnología preferida para llevar datos de alta velocidad y voz digital en una sola conexión.

MPLS no sólo proporciona una mayor fiabilidad y un mayor rendimiento, sino que a menudo puede reducir los costos generales mediante una mayor eficiencia de la red. Su capacidad para dar prioridad a los paquetes que transportan tráfico de voz hace que sea la solución perfecta para llevar las llamadas VoIP.

En MPLS el camino que se sigue está prefijado desde el origen (se conocen todos los saltos de antemano) :

Se pueden utilizar etiquetas para identificar cada comunicación y en cada salto se puede cambiar de etiqueta (mismo principio de funcionamiento que VPI/VCI en ATM, o que DLCI en Frame Relay).

- Las etiquetas con el mismo destino y tratamiento se agrupan en una misma etiqueta: Los nodos mantienen mucha menos información de estado que por ejemplo ATM. Las etiquetas se pueden apilar, de modo que se puede encaminar de manera jerárquica.

- MPLS asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers intermedios (sólo se mira la etiqueta, no la dirección de destino). [WikiPérez]

30/07/2014

26) Control de flujo. Mecanismo utilizado en TCP. Campos que intervienen.

Mecanismo de ventana deslizante. Campos: N° de sec, N° ACK y Tamaño de ventana.

SEMI-REPETIDA: 19/12/2012

https://es.wikipedia.org/wiki/Transmission_Control_Protocol#Ventanas_deslizantes

https://es.wikipedia.org/wiki/Ventana_deslizante

27) Celda ATM. Pide longitud, función y capacidades del mecanismo implementado en el campo ... ¿?

SEMI-REPETIDA: 13/02/2013

28) Algoritmo exponencial binario 802.3. 3 diferencias con mecanismo 802.11

El AEB se encarga de calcular el tiempo que debe esperar cada terminal para volver a intentar enviar su trama luego de una colisión. [Yo]

En 802.11 se busca EVITAR la colisión. Es CSMA/CA y no CSMA/CD. Acceso múltiple con escucha de portadora.

Backoff = $N^{\circ}\text{Random} * TS * CW$. CW(ventana de contención) = $2^i - 1$. $i = 3$ a 8

03/09/2014 - Echazú

29) Algo de "código hash". "cómo se hace".

Una función de Hash toma una entrada de longitud arbitraria y genera una salida de longitud fija

La salida, de longitud fija, se llama "Digest"

Un algoritmo para ser considerado como una función de Hash, debe cumplir determinados requisitos (4):

- Consistencia: la **misma entrada** debe generar siempre la **misma salida**

- Aleatoriedad: Que impida adivinar el mensaje original

- Unicidad: Debe ser prácticamente **imposible** encontrar **dos mensajes** que generen el **mismo Digest**

- One way: **Para un Digest** dado, debe ser muy difícil, sino **imposible acertar el mensaje de entrada** (¿cuál es la diferencia con aleatoriedad?)

Las funciones de Hash garantiza la integridad del mensaje

Las funciones de Hash más comunes son:

- Message Digest 4 (MD4)

- Message Digest 5 (MD5)

- Secure Hash Algorithm (SHA)

MD5 procesa su entrada en bloques de 512 bits y genera un Digest de 128 bits. SHA también procesa la entrada de a 512 bits y produce un Digest de 160 bits (requiere de mayor poder de procesamiento y corre más lento)

30) Algo de 802.11

Probablemente REPETIDA.

03/12/2014

31) 802.11. Backoff_time. ¿Qué es? DIFS, SIFS

SEMI-REPETIDA: 30/07/2014

Es un tiempo random que debe esperar una estación para volver a censar el medio una vez que lo encontró ocupado. $Backoff = N^{\circ}Random * TS * CW$. $CW(\text{ventana de contención}) = 2^{i-1}$. $i = 3 \text{ a } 8$

32) AAL (ATM). Tipo de tráfico que maneja cada subcapa.

- AAL 1: Audio y video sin comprimir.
- AAL 2: video comprimido
- AAL 3 y 4: Datos en general. Lo usa TCP, X.25
- AAL 5: servicio con menor overhead y mejor detección de errores. TCP, X.25, LAN

Tabla 11.4. Protocolos y servicios AAL.

	CBR	rt-VBR	nrt-VBR	ABR	UBR
AAL 1	Emulación de circuitos, RDSI, voz sobre ATM				
AAL 2		Voz y vídeo VBR			
AAL 3/4			Servicios generales de datos		
AAL 5	Emulación de redes LAN	Voz bajo demanda, emulación LANE	Retransmisión de tramas, ATM, emulación LANE	Emulación LANE	IP sobre ATM

CAPAS AAL SEGÚN REQUERIMIENTOS DE SERVICIOS

REQUERIMIENTO	CLASE A	CLASE B	CLASE C	CLASE D
TIEMPO ENTRE FUENTE Y DESTINO	REQUERIDO (SENSIBLE A DEMORAS) <i>rt</i>		NO REQUERIDO (NO SENSIBLE A DEMORAS) <i>nrt</i>	
BIT RATE	CONSTANTE <i>CBR</i>	<i>rt-VBR</i>	VARIABLE <i>nrt-VBR</i>	
MODO DE CONEXIÓN	ORIENTADO A LA CONEXIÓN			NO ORIENTADO A LA CONEXIÓN

AAL 1

AAL 2

AAL 3/AAL 4

AUDIO Y VIDEO S/COMP

VIDEO COMP

DATOS EN GENERAL

AAL 5 **SERVICIO CON MENOR OVERHEAD Y MEJOR DETECCION DE ERRORES**
EMULACIÓN LAN, FR, ATM, IP SOBRE ATM

33) Congestión en redes. **Flags de FR y ATM.**

El problema de la congestión se produce cuando el número de paquetes que se transmite a través de una red comienza a aproximarse al límite de la capacidad de gestión de paquetes de la misma.

FR: FECN, BECN, DE. ATM: El 2° bit del campo "Tipo de Carga Útil" indica 1=Congestión, 0=No Congestión. El bit/campo CLP (Prioridad de la Carga) indica 1=Puede ser descartada.

11/02/2015

34) Explique el mecanismo de control de acceso al medio DCF utilizado por 802.11. ¿En qué difiere del PCF?

DCF. **Ad-hoc?** Usa DIFS. Cada terminal censa el medio un tiempo DIFS antes de enviar un RTS (tiene que estar libre).

PCF. Infraestructura. Usa AP (Access Point), funciona como orquestador, análogo a Token Ring. Usa PIFS < DIFS por lo tanto tiene prioridad. [Yo]

<https://www.vocal.com/networking/802-11-distributed-coordination-function-dcf/>

35) ¿Qué función cumple un protocolo de ruteo? ¿En qué se diferencia un protocolo "Link State" de uno "Distance Vector"?

El protocolo de ruteo se encarga de calcular y hallar la mejor ruta para encaminar un paquete desde una terminal A a una B. Esta función la cumplen los routers.

En link state o estado de enlace el criterio de cuál es la mejor ruta depende del AB, cantidad de saltos, calidad del medio, etc. Cada router se comunica con un conjunto de routers cercanos e intercambian información de sus tablas.

En Distance Vector o Vector-Distancia la mejor ruta es la que tenga menos saltos. Cada router se comunica solo con sus vecinos. Mantiene un vector.

36)a) TCP. ¿Qué mecanismo implementa el campo "Windows" de la cabecera? ¿Qué longitud tiene este campo? ¿Cuál es el "crédito" máximo? ¿Conoce algún mecanismo para extenderlo?

SEMI-REPETIDA.

El mecanismo es Ventana Deslizante. Long: 16 bits. Crédito máximo está definido por el tamaño del campo $(2^{16})-1$. Si bien el campo no puede extenderse, se usa un factor de escalado (TCP Window Scale) que es una opción para incrementar la ventana.

https://es.wikipedia.org/wiki/Transmission_Control_Protocol#Ventanas_deslizantes

https://es.wikipedia.org/wiki/Segmento_TCP

https://en.wikipedia.org/wiki/TCP_window_scale_option

b) TCP. RTO: Explique el significado y la utilidad de esta variable. ¿Cómo se calcula? ¿Qué efectos produce una subestimación/sobrestimación de su valor?

Retransmission Time Out (RTO). A cada segmento almacenado en buffer se le asigna este timer. Cuando llega a 0, se retransmite. El objetivo es que no se pierdan paquetes y controlar que lleguen todos y en el orden correcto.

Efecto que produce: delays y degradación de performance.

Cálculo: $RTO = 2 * RTTs$ (suavizado)

The important part of calculating RTO is to determine how long it takes for a segment to go to the receiver and for ACK to come back from receiver to sender. This is a Round Trip Time.

<https://www.fdi.ucm.es/profesor/rubensm/ASOR/Trasparencias/Tema%203-%20Conceptos%20Avanzados%20del%20Protocolo%20TCP.pdf>

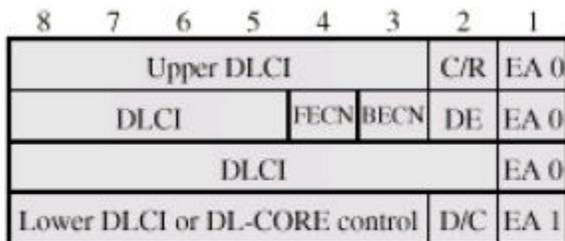
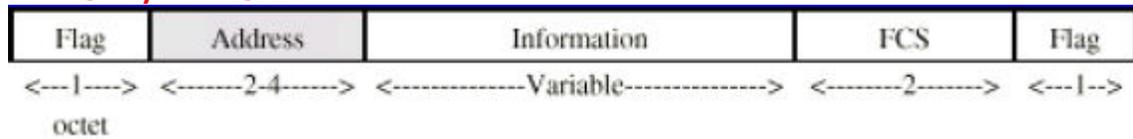
<https://www.extrahop.com/community/blog/2016/retransmission-timeouts-rtos-application-performance-degradation/>

<http://sgros.blogspot.com.ar/2012/02/calculating-tcp-rto.html>

18/02/2015 – Echazú?

37) Indique cuál es el formato de un cuadro FRAME RELAY PAB-F, indicando sus campos, detallando el campo de dirección y dando el procedimiento para ampliarlo.

REVISAR/REPASAR



(d) Address field - 4 octets

- EA Address field extension bit
- C/R Command/response bit
- FECN Forward explicit congestion notification
- BECN Backward explicit congestion notification
- DLCI Data link connection identifier
- D/C DLCI or DL-CORE control indicator
- DE Discard eligibility

38) Seleccione la respuesta correcta dando una breve justificación

2.1 ¿Cuál es el método de control de errores utilizado en el protocolo MAC de Lan Ethernet o IEEE 802.3? Seleccione la respuesta correcta.

c) CRC-32 (porque usa 4 bytes)

2.2 ¿Cuál de estas afirmaciones corresponde a "piggyback" en el contexto del método ARQ?

c) Es un método de confirmación usado en protocolos.

Consiste en que el receptor no envía inmediatamente el ACK sino que espera a tener algo para enviar y entonces envía el ACK junto con este mensaje. [Yo]

2.3 El valor de la impedancia característica del coaxil que se emplea en las LAN 10B5 es de ...

a) 50 ohms

39) Considerando las tecnologías de red WAN X 25, FRAME RELAY y ATM, indique sobre cada una lo siguiente: Velocidad de transmisión típica. Servicio orientado a la conexión o sin conexión. Tipo de tráfico más adecuado.

Respondido en 18/12/2013

25/02/2015 – Perez (creo)

40) IPv6. ¿Qué son los encabezados de extensión? ¿Qué encabezado de extensión va luego del encabezado de extensión de TCP?

REPETIDA 17/07/2014

Después del encabezado TCP no sigue ningún encabezado de extensión ¿?

41) Qué es una congestión en redes y con qué flags lo manejan los protocolos FR y ATM?

REPETIDA 03/12/2014

42) IPsec. ¿Qué diferencia hay entre AH y ESP.

REPETIDA 13/02/2013 Y 11/12/2013

26/05/2015 - Koval (creo)

43) Explicar el método de control de acceso al medio PCF usado en 802.11, y cuáles son las diferencias con DCF.

REPETIDA 11/02/2015

44) ¿Para qué sirve el protocolo ICMP? ¿En qué casos se genera el mensaje "Destino inalcanzable"? ¿Quién es el remitente y quién es el destinatario en ese caso?

REPETIDA: 22/12/2012

Internet Control Message Protocol (ICMP)

Es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado. También puede ser utilizado para transmitir mensajes ICMP Query.

Los mensajes de este protocolo se utilizan con **fines de diagnóstico o control** y se generan en **respuesta a los errores en operaciones IP** .

DESTINATARIO: **Estos errores del protocolo ICMP se dirigen a la dirección IP de origen del paquete originario. [Wikipedia]**

PPT KOVAL

- Comunica Errores a nivel de red
- Informa acerca de eventos inesperados
- Informa acerca de la red, en respuesta a consultas
- Solo informa el error, no especifica que acción correctiva tomar

PPT FUSARIO

- ICMP: **utilizado por los router para informar al origen** los problemas detectados a su nivel
- Descrito en la RFC 792
- Transferencia de mensajes de control de routers y computadoras a las computadoras
- Es una realimentación ante la existencia de problemas
- No son mensajes confiables porque van encapsulados en datagramas IP
- El checksum del encabezamiento IP detecta errores de transmisión
- Los mensajes ICMP **van encapsulados en datagramas IP, ocupando el campo de datos**
- Hay varios formatos de mensajes
- Son funciones ICMP
 - Ping (prueba de enlace)
 - Redireccionar
 - Tiempo excedido (se descartó datagrama por tiempo de vida)

Destino inalcanzable: https://es.wikipedia.org/wiki/ICMP_Destination_Unreachable
https://es.wikipedia.org/wiki/Internet_Control_Message_Protocol#Destino_de_Mensaje_Inalcanzable

http://www.wildpackets.com/resources/compendium/tcp_ip/unreachable

El **Destino Inalcanzable se genera por el host o en la puerta de enlace entrante** para informar al cliente de que el destino es inalcanzable por alguna razón.

Ejemplos:

- El paquete necesita ser fragmentado pero el bit DF=1.
- La conexión física con el host no existe.
- El usuario ingresó una red no existente en la línea de comandos.
- Máscara mal configurada en el router.
- Puerto dañado.

15/07/2015

Tema A

45) FR. Retransmisión de tramas. ¿Qué protocolos utiliza a nivel capa de control y a nivel capa de usuario? ¿Cuál es la función que cumple cada uno? (Se refería a LAP-D y LAP-F).

Estudiar esto!

Plano de Control

- Entre el usuario y la red
- Separa canales lógicos y establece un circuito virtual
- Capa enlace de datos
 - LAPD (Q.921)
 - Control de enlace confiable
 - Control de errores y de flujo
 - Entre el usuario (TE) y la red (NT)
 - Usado para intercambiar mensajes de control Q.933

Plano de Usuario

- Funcionalidad entre extremos
- LAPF (Link Access Procedure for Frame Mode Bearer Services) Q.922
 - Tramas delimitadas, alineadas y transparentes
 - Multiplexa tramas usando campo identificador de conexión del enlace de datos (DLCI) de 10 bits
 - Asegura que las tramas tienen cantidad entera de octetos (no hay inserción/extracción de bits)
 - Asegura que las tramas no sean muy largas ni muy cortas
 - Hay funciones de control de congestión

LAPD para establecer la conexión y LAPF para transmisión de datos.

46) IPv6. ¿Qué protocolos no admiten cabecera de extensión?

Las cabeceras de transporte no admiten cabecera siguiente ¿?. A mi entender le seguiría la cabecera de Sesión, luego Presentación, luego Aplicación y finalmente los datos puros.

Cabeceras de transporte: TCP, UDP, SPX (OSI.pdf)

Según PPT Fusario, solo TCP y UDP.

47) ATM. ¿Cuál es la diferencia a nivel capa AAL entre la transmisión de voz, datos y video?

REPETIDA?

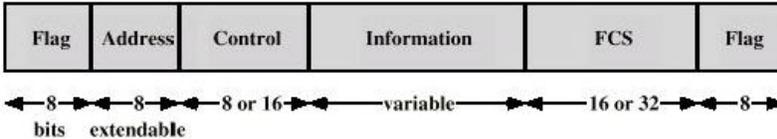
Esperaba las distinciones entre AAL1, 2, 3, 4 y 5?

Tema B

48) Describir tramas de control de HDLC. Compara el funcionamiento del HDLC con el de PPP

REPETIDA: 07/12/2011

Repasar Trama completa de HDLC (y sus tipos)

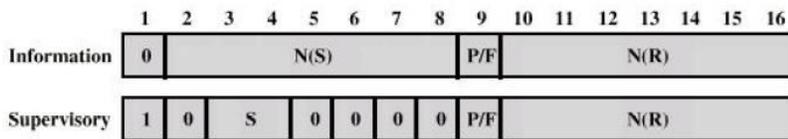


Formatos

	1	2	3	4	5	6	7	8
I: Information	0	N(S)			P/F	N(R)		
S: Supervisory	1	0	S	P/F	N(R)			
U: Unnumbered	1	1	M	P/F	M			

N(S) = Send sequence number
 N(R) = Receive sequence number
 S = Supervisory function bits
 M = Unnumbered function bits
 P/F = Poll/Final bit

(c) 8-bit control field format



Estudiar PPP!

Ventajas de PPP sobre HDLC

- Es más confiable
- Puede trabajar con diversos enlaces (E1, modems)
- Está bien normalizado por las RFC
- Permite mayor seguridad
- Permite compresión de datos

49) Describir funcionamiento de 802.11 y por qué se puede afirmar que es orientado a la conexión. Ésta tiene que estar mal porque no es orientado a la conexión SEMI-REPETIDA

802.11 no es orientado a la conexión. TCP, X.25, HDLC, FR, ATM, MPLS sí lo son.

50) Que cálculo hay que hacer para saber el grado de interferencia en un cableado estructurado.

SEMI-REPETIDA

$NEXT [dB] = 10\log (P2/P1)$

02/12/2015 – Perez?

51) DATAGRAMA IPv4: Campo OPCIONES: explique su utilidad y nombre al menos dos de las mismas

NO SIEMPRE SE EMPLEA. LONGITUD VARIABLE. USO PARA PRUEBAS DE RED O DEPURACIÓN.
Relleno: para tener longitud múltiplo de 32 bits

Actualmente hay cinco opciones definidas, aunque no todos los encaminadores las reconocen: **Seguridad, Enrutamiento estricto desde el origen, Enrutamiento libre desde el origen, Registrar ruta y Marca de tiempo.**

Más info: <http://apuntesdenetworking.blogspot.com.ar/2011/08/el-datagrama-ip-ipv4-ip-datagram.html>

52) QUE DIFERENCIA EXISTE ENTRE LOS PROTOCOLOS DE SEGURIDAD AH Y ESP

REPETIDA 13/02/2013, 11/12/2013, 25/02/2015

53) COMO SE IDENTIFICAN LAS SUBREDES EN IPv6

Las direcciones IPv6 son de 128 bits. Son todas /64. Los siguientes 16 bits a los primeros 48, se utilizan para subredes.

Prefijos IPv6

Se utiliza la misma representación que en CIDR

Dirección/Longitud del prefijo

2001:DB8:2A0:2F3B::/64 es un prefijo de red

2001:DB8:3F::/48 es un prefijo de ruta sumarizada

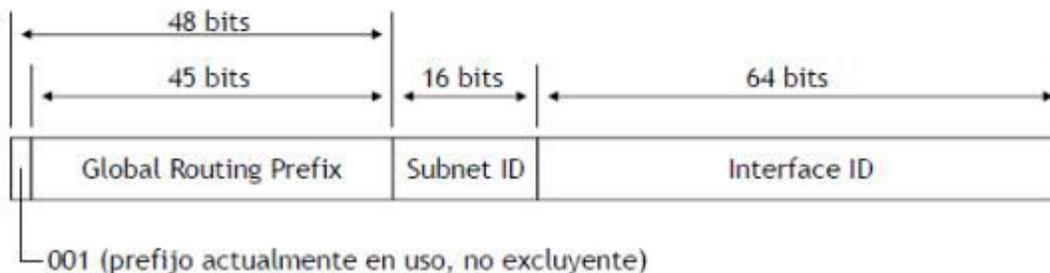
Un prefijo menor a 64 es una ruta sumarizada o un rango de direcciones que sumariza una porción del espacio de direcciones v6.

En IPv6 las redes son todas /64, por lo que no se necesita expresar el prefijo.

Tipos de direcciones

• Global Unicast Addresses

- Equivalentes a una dirección IPv4 registrada
- Diseñadas para ser sumarizadas



09/12/2015 – Echazú?

54) MPLS. ¿Cuál es el principio básico de funcionamiento? Qué significan los acrónimos **LSR, FEC y LSP**? Qué ventajas ofrece?

SEMI-REPETIDO 16/07/2014

En MPLS el camino que se sigue está prefijado desde el origen (se conocen todos los saltos de antemano): se pueden utilizar etiquetas para identificar cada comunicación y en cada salto se puede cambiar de etiqueta (mismo principio de funcionamiento que VPI/VCI en ATM, o que DLCI en Frame Relay).

Elementos

LER (Label Edge Router): elemento que inicia o termina el túnel (extrae e introduce cabeceras). Es decir, el elemento de entrada/salida a la red MPLS. Un router de entrada se conoce como Ingress Router y uno de salida como Egress Router. Ambos se suelen denominar Edge Label Switch Router ya que se encuentran en los extremos de la red MPLS.

LSR (Label Switching Router): elemento que conmuta etiquetas.

LSP (Label Switched Path) o Intercambio de rutas por etiqueta: nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del **túnel MPLS establecido entre los extremos**. A tener en cuenta que un LSP **es unidireccional**.

LDP (Label Distribution Protocol): un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.

FEC (Forwarding Equivalence Class): nombre que se le da al **tráfico que se encamina bajo una etiqueta**. Subconjunto de paquetes tratados del mismo modo por el conmutador.

Ventajas. Pregunta REPETIDA 16/07/2014

55) Seleccione la respuesta correspondiente dando una breve justificación ¿Cuál de los siguientes protocolos está orientado a la NO conexión? TCP LAP-B UDP LAP-F Ninguno

UDP está orientado a la NO conexión.

La firma digital provee esencialmente: a. Encriptación b. autenticidad y rapidez c. autenticidad e. integridad d. sólo autenticidad e. ninguno
c) autenticidad y e) integridad

Qué afirmación relativa al cableado estructurado con UTP es incorrecta?
Varias opciones

La a) era la incorrecta. Decía que lo deseable es tener un NEXT de 0 dB, sin embargo lo ideal es tener una diafonía infinitamente negativa ($P2=0$)

56) Considerando las tecnologías de red WAN X 25, FRAME RELAY y ATM, indique sobre cada una lo siguiente: Tipo de servicio -velocidad de transmisión máxima y nivel donde se produce la conmutación -tipo de tráfico más adecuado

SEMI-REPETIDA 18/02/2015, respondida en 18/12/2013

Nivel conmutación: x.25 – por software (mayor procesamiento). FR – por software (menor procesamiento). ATM – por hardware (menor retardo)

16/12/2015 - Koval?

57) Que es el control de flujo, y que campos de TCP se utilizan para hacerlo.
REPETIDA/RESPONDIDA 30/07/2014, 19/12/2012

58) Explicar el método de control de acceso al medio PCF usado en 802.11, y cuáles son las diferencias con DCF.

<http://www.utnianos.com.ar/foro/tema-aporte-final-redes-de-informaci%C3%B3n-26-05-2015?pid=433099#pid433099>

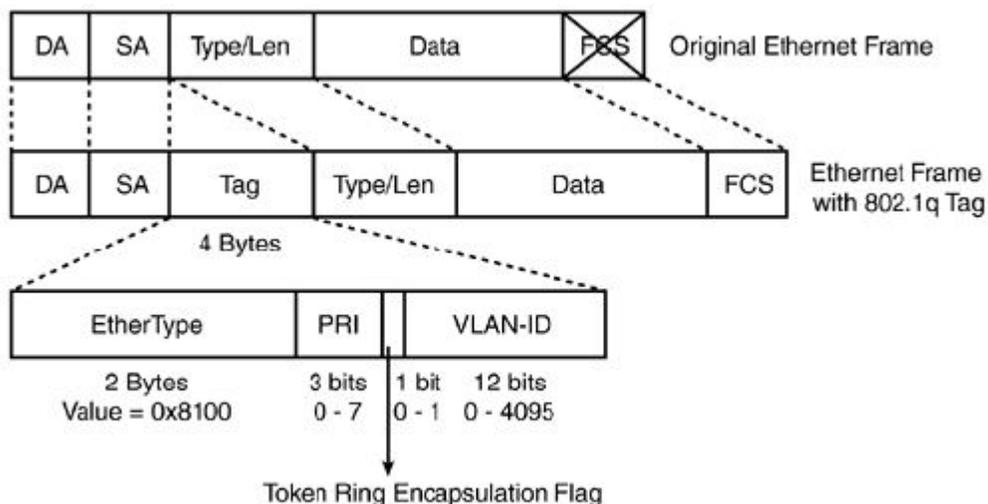
PCF tiene al AP como orquestador. Este sensa el medio durante un tiempo PIFS (tiempo previo a la autorizacion para transmitir), y se asegura de acceder al medio. Una vez que accede, empieza el periodo de libre contencion y pollea a cada estacion para ver si hay algo que transmitir. Despues de un poll se espera un ACK y datos (si no tiene nada, manda nulo). Y despues 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 que cuando volver a intentar, el AP envia beacons a todas las estaciones constantemente para que seteen su tiempo de libre contencion (NAV).

La diferencia con DFC es que DFC utiliza DIFS como espacio de tiempo entre cada transmision. Como DIFS es mas grande que PIFS, siempre PCF tendra prioridad de acceso al medio. Ademas DFC utiliza los mensajes RTS y CTS.

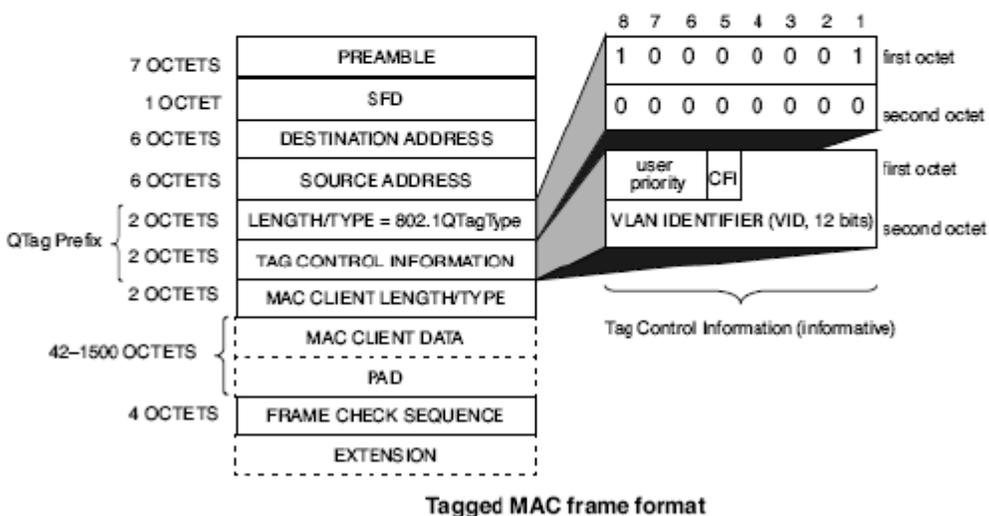
REPETIDA/RESPONDIDA 26/05/2015 y 11/02/2015

59) Describir la trama Ethernet y como es modificada por la norma 802.1q

La normal 802.1q es la de etiquetado de VLANs. Agrega 4 bytes a la trama de Ethernet antes del campo tipo/logitud. Lo agrega un SW y lo saca otro SW ¿?



802.1Q TAG



10/02/2016 – Perez

Igual al 02/12/2015. Cambió solo el 2do punto teórico:

Arquitectura de Frame Relay en Control y Usuario

Es lo de LAP-D y LAP-F creo → REPETIDA 15/07/2015

17/02/2016 – Echazú

Igual al 09/12/2015

24/02/2016 – Koval

1) ¿Qué es control de flujo y que campos usa TCP para realizarlo?

REPETIDA

2) Describa la trama Ethernet y cómo la modifica la 802.1q

REPETIDA

3) Cuales son las diferencias entre PFC y DFC.

REPETIDA

Las tres igual al final: (16/12/2015) – Koval?

24/05/2016 – Koval

4to punto (teoría): Explicar cómo funciona PCF y que diferencia tiene con DCF.

REPETIDA

5to punto (teoría): que es CIDR y que cosas pueden provocar un mensaje "Destino Inalcanzable"

(que la IP destino no sea válida o que el mensaje tenga que fragmentarse por su excesivo tamaño pero el flag de DF esté activado).

Preguntar por CIDR es nuevo:

CIDR (Classless Inter-Domain Routing) – Enrutamiento entre Dominios sin Clase

Representa la última mejora en el modo de interpretar las direcciones IP. Su introducción permitió una **mayor flexibilidad** al dividir rangos de direcciones IP en redes separadas. De esta manera permitió:

Un **uso más eficiente de las cada vez más escasas direcciones IPv4** (*ya se agotaron*)

Un mayor uso de la jerarquía de direcciones (**agregación de prefijos de red**), disminuyendo la sobrecarga de los enrutadores principales de Internet para realizar el encaminamiento.

CIDR reemplaza la sintaxis previa para nombrar direcciones IP, las clases de redes. En vez de asignar bloques de direcciones en los límites de los octetos, que implicaban prefijos «naturales» de 8, 16 y 24 bits, **CIDR usa la técnica VLSM (Variable Length Subnet Mask, en español «máscara de subred de longitud variable»)** para hacer posible la asignación de prefijos de longitud arbitraria.

https://es.wikipedia.org/wiki/Classless_Inter-Domain_Routing

13/07/2016 – Koval

1) Explique en detalle como realizan la **DETECCIÓN** y la **CORRECCIÓN** de errores los siguientes protocolos: HDLC, IP, TCP

Nunca se había tomado, no así al menos.

2) Detalle el mecanismo de control de acceso al medio utilizado en redes 802.11

REPETIDA 11/02/2015

27/07/2016 - Pérez

Tema A – Igual al 10/02/2016 que es igual al 02/12/2015 salvo por el 2do teórico.

Tema B

1. Explicar "Árbol de expresión" de Spanning Tree. (no la recuerdo textual)

SEMI-REPETIDA 04/12/2013

2. Indicar como se mide la interferencia en un cable trenzado. (Tenías que explicar el concepto de NEXT básicamente)

REPETIDA 15/07/2015

3. IP/MPLS. Describa el protocolo y explique su utilidad sobre ATM para transportar datagramas.

REPETIDA 16/02/2014

Más antiguos:

15/02/2012

1. Describir los campos de la trama ATM UNI (Cambia sólo un campo!)

Repetido

4. Dibujar y nombrar los elementos que componen un cableado estructurado. (Backbone, cableado horizontal, vertical, router, Rack, etc) Luego te pedía que representes al NEXT y FEXT y que diferencia había entre ellas.

No creo que se tome

5. Te pedía que expliques los campos de la trama frame delay y que luego te daba datos (DLCI=500, DE=0, FECN=BECN=1) y tenías que armar la trama y luego pasarla a hexa.

Repetido

29/02/2012

1. Describir como se establece / transfiere datos / desconecta una conexión en TCP.

Para establecerse la conexión se usa el three-way-handshake

→SYN seq=x

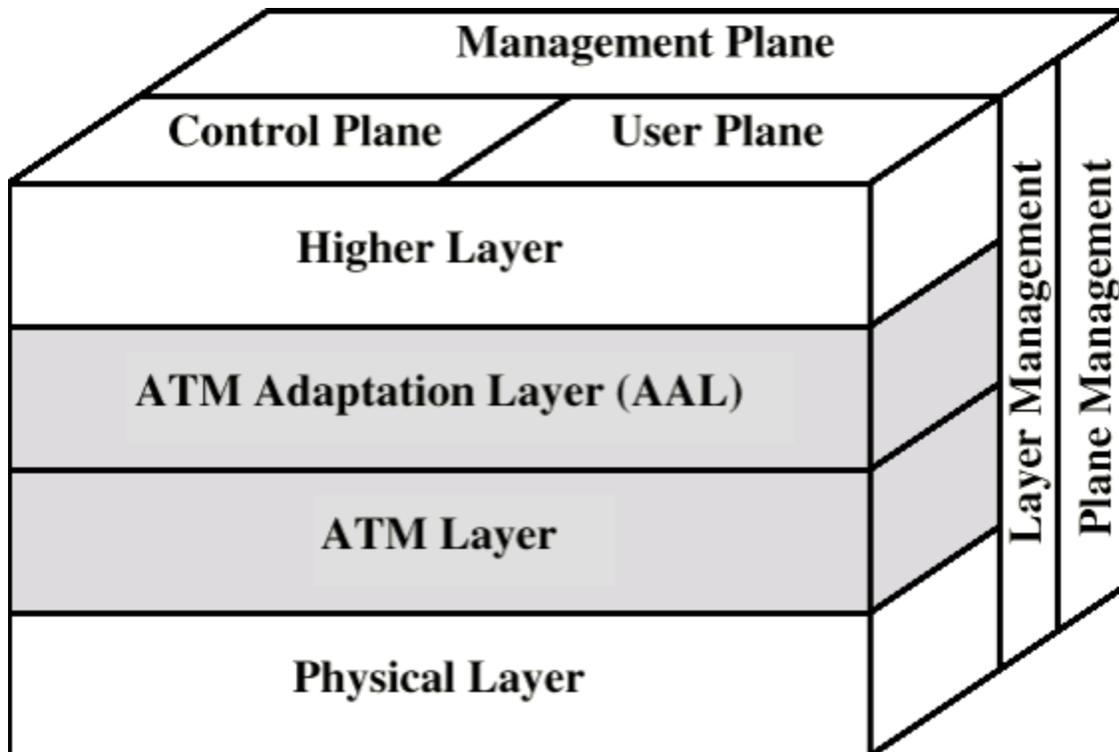
SYN-ACK ack=x+1 seq=y←

→ACK ack=y+1 seq=x+1

Los datos se transfieren una vez establecida la conexión, y viajan acompañados del número de secuencia y número de ACK.

Para finalizar la comunicación se usa el 4-way-handshake (FIN, ACK, FIN, ACK)

2. Grafique la Arquitectura de ATM, las capas de gestión, control y usuario. Describa cada una de ellas.



PLANOS DE OPERACIÓN

- DE USUARIO: TRANSFERENCIA DE INFO USUARIO Y CONTROLES ASOCIADOS (DE FLUJO Y ERRORES)
- DE CONTROL: CONTROLES DE LLAMADA Y DE CONEXIÓN
- DE GESTIÓN
 - DE PLANO: COORDINACIÓN ENTRE PLANOS Y COMO UN TODO
 - DE CAPA: RECURSOS Y PARÁMETROS DE PROTOCOLOS

Convergencia: Independiza la pila de protocolos que está debajo de ella de las capas superiores. Identificar mensajes, recuperar señal de reloj.

Segmentación y reensamblable: Segmentar la información de las capas superiores. Permite manejar cuadros de longitud mayor que las celdas (Ej: LAN). Adapta la información a los 48 Byte, acorde a la clase de servicio que se trate. Reensamblado.

ATM: Multiplexión. Armado de celdas. Introducción y extracción del header. Control de congestiones y ruteos (flujo) en UNI.

3. Que es un **ataque activo**, como se clasifican.

Es un ataque que busca alterar el contenido de un mensaje. Es más fácil de detectar que el ataque pasivo (que sólo observa) pero más difícil de combatir.

22/12/2012

4) Cómo maneja HDLC el control de flujo y el control de errores?

a) Qué campos de la trama intervienen?

b) **Compararlo con el manejo para esos mecanismos que realiza TCP.**

Control de flujo: Ventana Deslizante-N.

Control de errores: FCS → CRC-16

Recuperación/Corrección de errores: Retransmisión

Campos: N(S), N(R), SS (bits de supervisión) aunque estos son más para corrección de errores TCP también implementa ventana deslizante.

La mayor diferencia es que TPC es un protocolo de capa 4 mientras HDLC es de capa 2.

TCP no tiene mensajes como REJ o SREJ.

5) Qué tipo de protocolo es ICMP o para qué se usa, algo así y después pedía ejemplos en los que se enviara un mensaje "**Destino inalcanzable**" y otro de "**Tiempo de Vida excedido**"

Repetido 26/05/2015

07/12/2011

1) Detallar la estructura de la trama HDLC (tramas de información, supervisión y no numerada) y PPP. Comparar ambos protocolos.

15/07/2015

2) Dados los primeros bytes de una trama de Frame Relay: 7E 08 45 FA ..., identifique el DLCI utilizado. Existe congestión en la red? En caso afirmativo, quién es el culpable? Qué garantías me da la red de que esta trama llegue a destino?

Se tomo algo parecido

21/12/2011

1) Señal de transmisión en los siguientes estándares:

10BaseT

100BaseF

100Base Algo que no me acuerdo

¿?

2) ¿ Que campos Utiliza X.25 para multiplexar canales lógicos?

Utiliza el campo LCI

3) Diferencias básicas entre AES y DES

Conceptos de seguridad informática. Tipos de cifrado.

10/02/2010

Protocolos de enrutamiento que operan mediante los métodos:

- Estado del enlace
- Vector de distancia

Funcionamiento y dos ejemplos de cada uno.

Graficar la topología y explicar el funcionamiento y conectividad en una LAN inalámbrica multicelda. **La celda es el canal?**

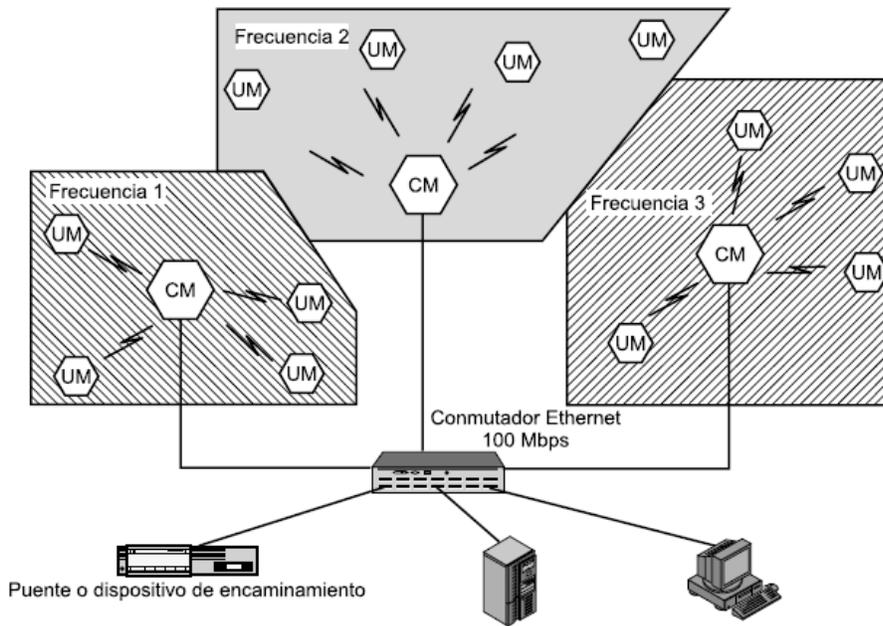


Figura 17.2. Ejemplo de configuración de una LAN inalámbrica de celdas múltiples.

17/02/2010

- 2) ¿De qué manera se realiza la delimitación de tramas en Frame Relay? Detalle el contenido del campo "Dirección". ¿Es extensible este campo? Explíquelo.
- 3) ¿Cómo identifica TCP la necesidad de retransmitir un segmento perdido o dañado? ¿Qué extremo detecta esta necesidad? ¿Qué campos de la cabecera se utilizan para el mecanismo de corrección de errores?

La delimitación de trama en FR se realiza con el flag de un byte: 01111110 al ppio y final de cada trama. Para permitir la transparencia de datos se utiliza la técnica de bit stuffing/inserción de ceros.

TCP detecta la necesidad de retransmitir a través de la ausencia de ACK luego de un determinado tiempo (time-out).

El receptor detecta por **checksum/crc** error en el segmento/trama y descarta el paquete→no envía ACK. El receptor percibe la ausencia de este ACK y prosigue a retransmitir.

22/12/2010

- 2) Enuncie las capas del modelo OSI e indique en qué capa(s) se realiza el control de errores.
- 3) Detalle el formato de la celda ATM e indique como interviene el HEC en:
 - a) detección de errores
 - b) obtención/mantenimiento del sincronismo.

NOTAS:

- **PSH** (1 bit): Push. El receptor debe pasar los datos a la aplicación tan pronto como sea posible, no teniendo que esperar a recibir más datos.

Fuente: https://es.wikipedia.org/wiki/Segmento_TCP

En el lado del servidor (este receptor también puede ser una PC o alguna estación terminal) se comprueba si el puerto está abierto, es decir, si existe algún proceso escuchando en ese puerto, pues se debe verificar que el dispositivo de destino tenga este servicio activo y esté aceptando peticiones en el número de puerto que el cliente intenta usar para la sesión. En caso de no estarlo, se envía al cliente un paquete de respuesta con el bit **RST** activado, lo que significa el rechazo del intento de conexión

LAPD para establecer la conexión y LAPF para transmisión de datos.

Tramas AH y ESP

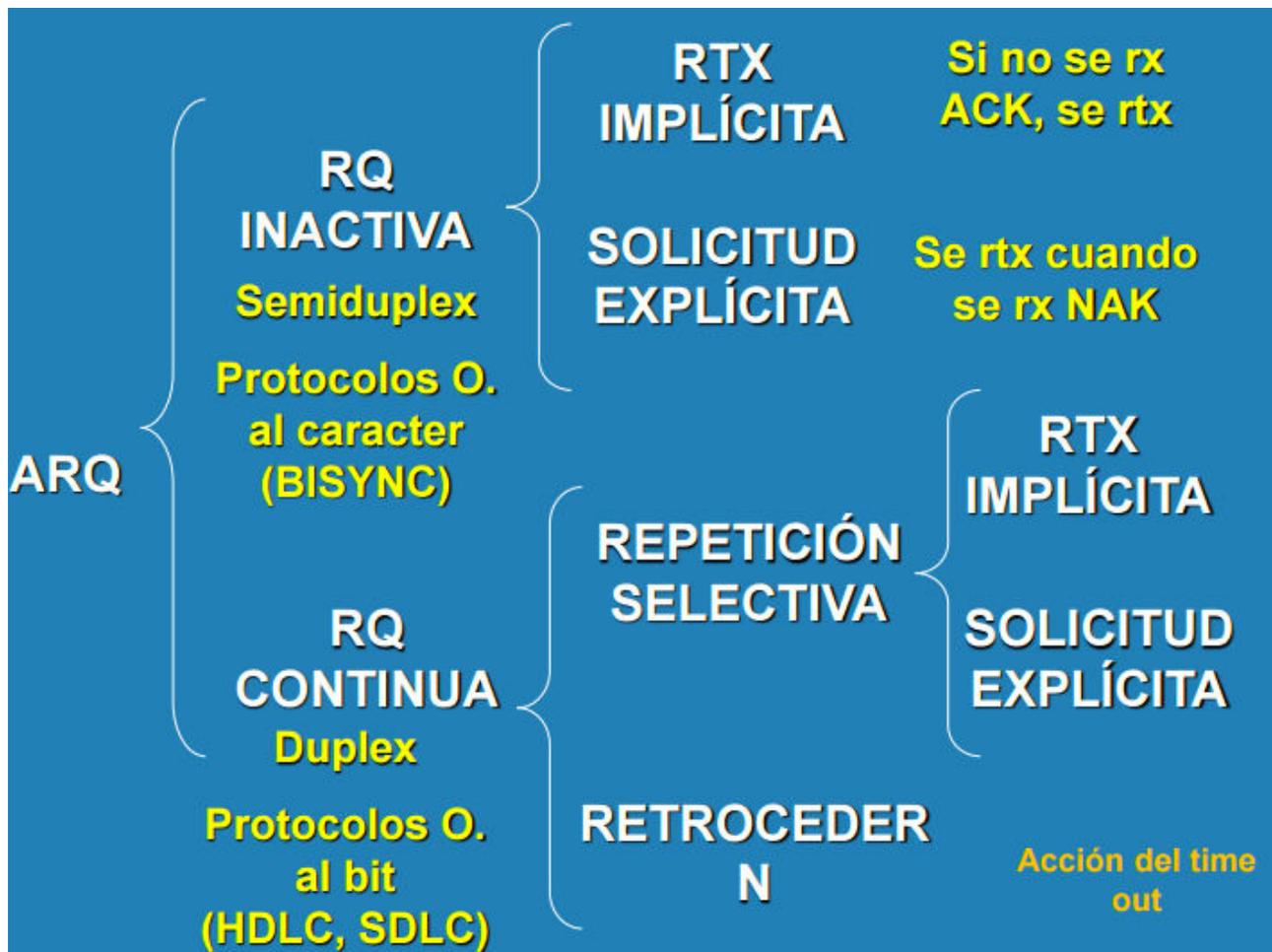
Fragmentación

El receptor es el responsable de reensamblar todos los fragmentos en el orden correcto para obtener el datagrama original y entregarlos al protocolo de nivel superior. El reensamblaje se espera que ocurra en el equipo receptor, pero en la práctica puede ocurrir también en routers intermedios, por ejemplo, **NAT** puede necesitar reensamblar fragmentos para traducir flujos de datos, e.g. el protocolo de control de FTP, como se describe en el RFP 2993.

Fuente: https://es.wikipedia.org/wiki/Fragmentaci%C3%B3n_IP

La firma digital provee

Autenticidad e Integridad Ya que solo se puede descifrar con la clave pública de quien la haya cifrado (**Autenticidad**, o no repudio de origen más que nada...) y si el paquete sufrió alguna modificación, ya no se puede descifrar correctamente (**integridad**)



Parciales Echazú

1. ¿Cómo se logra la transparencia en el protocolo HDLC? Explique el método.
2. En el cuadro del protocolo LAP-F, explique el procedimiento para extender el campo de dirección y en cuánto se puede extender.
3. Qué es un PAD? En qué modo de operación y tecnología de WAN se utiliza?
4. Qué diferencia existe entre la celda ATM de la UNI y la NNI? Qué capa del ATM se ocupa de conformar la celda?
5. Respecto de las tecnologías de WAN X.25, FR y ATM: cuál es orientada a la conexión y cuál sin conexión; en qué nivel se realiza la conmutación en cada una; y cuáles son las velocidades de transmisión máximas alcanzables en cada una.
6. Respecto de la tecnología de red MPLS: para qué sirve la etiqueta y qué ventajas integra?
7. Sobre el protocolo PPP, en qué nivel opera y qué funciones incluye?

1. Explique los dos modos de operación previstos en las redes X.25. Qué es el PAD y en qué modo se usa?
2. Qué es un RACK? La U que significado tiene como parámetro de los RACK?

1. Explique los dos modos de operación previstos en las redes X.25. Qué es el PAD y en qué modo se usa?
2. Qué planos de operación comprende la arquitectura de protocolos de ATM? Explicar. Las clases de servicio CBR y rt-VBR, a qué se refiere? Explicar.
3. Cómo es la denominación de la PDU en el IP v6? Indique el formato esquemático de esta PDU. Cómo es el espacio de direcciones del IP v6?
4. Explique qué es MPLS? Qué ventajas ofrece? Qué es un LSR?

5. Especifique el formato de una trama ETHERNET indicando el nombre de los campos, los bytes por campo, y total de la trama. También explique qué control de errores hace y sobre qué campos se aplica.
6. Para una LAN de 10 Mbps se indica que el RTT máximo es de 51,2 microsegundos. ¿Cómo se obtiene este valor? ¿Cuál es el valor para una red FAST ETHERNET?
3. Qué mecanismo implementa TCP y UDP para realizar el control de flujo? Explique brevemente en que consiste cada uno.
4. Explique qué es CSMA/CD y desarrolle brevemente.
5. Conteste brevemente las siguientes preguntas:
 - a. Para qué se utiliza el campo de 16 bits de identificación de un datagrama?
 - b. Mencione que protocolos de N3 y N4 de la suite TCP/IP son orientados a la conexión
 - c. Qué control de errores se lleva a cabo en un datagrama IP?
 - d. Qué equipo se ocupa de la fragmentación de los datagramas IP ? Qué es la MTU?