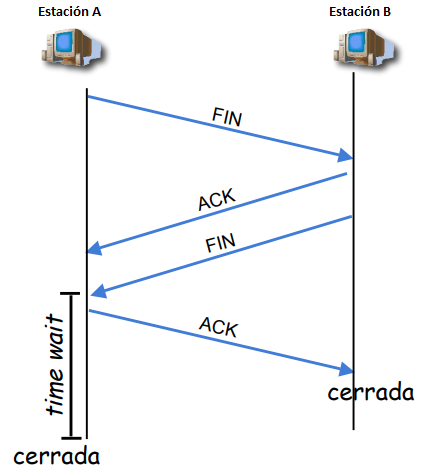
**TCP - UDP**

1. ***¿Cómo se realiza el cierre de conexión en TCP? ¿Y en UDP?***

En TCP cada extremo cierra su mitad de la conexión. La estación A envía un FIN. Pasa a un estado FIN WAIT. La estación B va a responder con un ACK confirmando el FIN. Luego la estación B va a enviar un FIN y la estación A va a responder con un ACK.

******

En UDP no se realiza el cierre de la conexión porque es un protocolo NO orientado a la conexión.

1. ***¿Qué provoca la retransmisión de un segmento en TCP? ¿Cómo se detecta la necesidad de retransmitir?***

Retransmisión de paquetes se provoca por:

* Paquete Perdido
* Paquete Retrasado
* Paquete Corrompido

Se detecta cuando el emisor no considera que el receptor ha recibido la información, debido a que no obtuvo un ACK como respuesta, es decir se detecta cuando se cancela el RTO.

1. ***¿Cuántos y cuáles son los campos de la cabecera UDP?***

Los campos de la cabecera UDP son 4: puerto origen, puerto destino, longitud total, checksum (opcional).

1. ***¿Cómo realiza TCP el control de flujo? ¿Qué campo(s) de la cabecera interviene? Compárelo con el mecanismo utilizado por HDLC.***

TCP usa control de flujo para evitar que un emisor envié datos de forma más rápida de la que el receptor puede recibirlos y procesarlos.

Para el control de Flujo se utiliza un mecanismo de la forma de “Ventana deslizante”, tal como HDLC, también llamado “Esquema de otorgamiento de créditos”.

A diferencia de HDLC, separa la confirmación de datos recibidos del permiso para enviar más.

En el establecimiento de la conexión, el servidor y el cliente se informan hasta cuantos bytes le puede enviar el otro sin esperar confirmación. Este valor va en el campo window.

Para una mayor eficiencia en redes de gran ancho de banda, debe ser usado un tamaño de ventana mayor. El campo TCP de tamaño de ventana controla el movimiento de datos y está limitado a 16 bits, es decir, a un tamaño de ventana de 65.535 bytes.

Como el campo de ventana no puede expandirse se usa un factor de escalado. La escala de ventana TCP (TCP window scale) es una opción usada para incrementar el máximo tamaño de ventana desde 65.535 bytes, a 1 Gigabyte.

La opción de escala de ventana TCP es usada solo durante la negociación en tres pasos que constituye el comienzo de la conexión.

Los campos de la cabecera que intervienen son:

* *Sequence Number*
* *ACK Number:* Para ordenar y controlar el flujo y orden de los segmentos TCP.
* *Checksum:* Para la comprobación de errores.
* *Temporizadores:* Para detectar retrasos o perdidas

1. ***Explique los mecanismos utilizados por TCP para:***
2. ***Detección de errores y Corrección de errores.***

TCP utiliza Checksum de 16 bits como en CAPA 2. Lo que hace TCP es basarse en la confirmación positiva de la recepción (“recibí bien hasta el bit X”) y retransmite cuando la confirmación no llega dentro de un período determinado RTO. En TCP no existe una confirmación de rechazo. Es responsabilidad del otro extremo reenviar el X+1.

1. ***Control de Flujo***

TCP usa control de flujo para evitar que un emisor envié datos de forma más rápida de la que el receptor puede recibirlos y procesarlos. Evitar la congestión al receptor.

Para el control de Flujo se utiliza un mecanismo de la forma de “Ventana deslizante”, tal como HDLC, también llamado “Esquema de otorgamiento de créditos”.

A diferencia de HDLC, separa la confirmación de datos recibidos del permiso para enviar más.

En el establecimiento de la conexión, el servidor y el cliente se informan hasta cuantos bytes le puede enviar el otro sin esperar confirmación. Este valor va en el campo window.

Para una mayor eficiencia en redes de gran ancho de banda, debe ser usado un tamaño de ventana mayor. El campo TCP de tamaño de ventana controla el movimiento de datos y está limitado a 16 bits, es decir, a un tamaño de ventana de 65.535 bytes.

Como el campo de ventana no puede expandirse se usa un factor de escalado. La escala de ventana TCP (TCP window scale) es una opción usada para incrementar el máximo tamaño de ventana desde 65.535 bytes, a 1 Gigabyte.

La opción de escala de ventana TCP es usada solo durante la negociación en tres pasos que constituye el comienzo de la conexión.

1. ***Control de Congestión***

Se utiliza para Impedir que un conjunto de transmisores sobrecargue la red, es decir evitar la congestión en la red. TCP usa una serie de mecanismos para conseguir un alto rendimiento y evitar la congestión de la red (la idea es enviar tan rápido como el receptor pueda recibir). Estos mecanismos incluyen el uso de [ventana deslizante](https://es.wikipedia.org/wiki/Ventana_deslizante), que controla que el transmisor mande información dentro de los límites del [búfer](https://es.wikipedia.org/wiki/Buffer_de_datos) del receptor, y algoritmos de control de flujo, tales como el algoritmo de [evitación de la congestión](https://es.wikipedia.org/wiki/Evitaci%C3%B3n_de_la_congesti%C3%B3n)(congestion avoidance), el de [comienzo lento](https://es.wikipedia.org/wiki/Comienzo_lento) (slow-start), el de [retransmisión rápida](https://es.wikipedia.org/wiki/Retransmisi%C3%B3n_r%C3%A1pida), el de [recuperación rápida](https://es.wikipedia.org/wiki/Recuperaci%C3%B3n_r%C3%A1pida) (fast recovery), y otros.

Cnwd= Ventana de congestión, en segmentos. Usada por TCP en el comienzo y durante períodos de congestión.

* *Slow-Start:* Cuando se inicia una nueva conexión, se inicializa cnwd = 1. Cada vez que se recibe una confirmación, se incrementa en 1. Cuando un segmento se pierde (caduca RTO), cnwd vuelve a valer 1 y comienza nuevamente.
* *Fast Retransmit:* Cuando la fuente recibe un ACK duplicado, significa :
  + El segmento fue demorado – pero finalmente llegará
  + El segmento se perdió – deberá retransmitirse

En lugar de esperar a que caduque el RTO, si se reciben 3 ACK duplicados, se retransmite el segmento perdido.

* *Fast Recovery:* Esta variante permite al transmisor evitar volver al Slow-Start en caso de perderse un segmento.

Cuando se recibe el 3er ACK duplicado, se setea cwnd = cwnd / 2

1. ***¿Cuál es la función del RTO?***

RTO es un timer. Cada uno de los extremos mantiene un valor de RTO para estimar cuanto tiempo debería esperar por la confirmación de un segmento. El transmisor transmite un segmento, si el receptor no se lo confirma dentro de un intervalo RTO, lo va a retransmitir.

1. ***¿Cuál será el efecto de utilizar un valor de RTO muy bajo/corto? ¿Y de uno muy alto/largo?***

RTO muy bajo genera retransmisión innecesaria.

RTO muy alto genera mucha pérdida de tiempo esperando.

1. ***¿Qué utilidad incorpora la opción WS (Window Scale Factor)?***

Incrementar el máximo tamaño de ventana desde 65535 bytes a 1GB.

1. ***¿Cómo identifica TCP la necesidad de retransmitir un segmento perdido o dañado? ¿Qué extremo detecta esta necesidad? ¿Qué campo de la cabecera interviene?***
2. ***¿Qué mecanismo se implementa en el campo Window de TCP? ¿Qué identifica su contenido?***

Un campo ventana está relacionado con el mecanismo de control de flujo. Su contenido identifica la cantidad de bytes, comenzando por el indicado en el campo ACK, que el receptor está dispuesto a recibir.

Mecanismos:

* + Slow Start
  + Fast Retransmit
  + Fast Recovery

**HDLC**

1. ***¿De qué manera se realiza la delimitación de tramas en HDLC? ¿En qué consiste el mecanismo de inserción de ceros y para qué se utiliza?***

Se delimita usando el flag (7e). Mediante el mecanismo de “inserción de ceros” garantiza la transparencia del protocolo. El mecanismo consiste en asegurar que no existirá en el campo de datos una secuencia “01111110”. Para realizarlo inmediatamente después de la aparición de la secuencia 1111111, si inserta un 0 sin importar que bit sigue a continuación. El receptor es el encargado de “retirar” ese cero, luego de recibir una secuencia 111111.

**Frame Relay**

1. ***¿Qué es el CIR? ¿Cómo se calcula?***

*CIR (Commited Information Rate):* Es la tasa de transmisión, en bits por segundo, que la red garantiza transmitir, bajo condiciones normales.

CIR = Bc / Tc

*Bc (Committed Burst Size):* Es la cantidad máxima de bits que la red garantiza su entrega, durante Tc. Bajo condiciones normales.

*Tc (Committed Rate Measurement Interval):* Intervalo de tiempo durante el cual se mide la tasa de transmisión.

1. ***¿Qué es un PVC (Circuito Virtual Permanente)? ¿Cómo los identifica FR?***

**PVC** es un circuito virtual permanente que conecta dos puntos remotos definidos por el cliente.

Frame Relay lo identifica a través de **DLCI** que son identificadores de linkeo de datos. Tiene importancia solo en la red local. El switch FR define los DLCI entre dos routers hasta llegar al destino final creando un PVC.

1. ***¿Qué efecto tiene la recepción de una trama con BECN encendido? ¿Y con FECN?***

BECN (Notificación de la congestión retrospectiva): Bit establecido en una trama que notifica a un router que el **dispositivo emisor** debe iniciar procedimientos para evitar la congestión. Cuando un switch Frame Relay detecta congestión en la red, envía un paquete BECN al **router origen**, instruyendo al router para que reduzca la velocidad a la cual está enviando los paquetes. Si el router recibe cualquier BECN durante el intervalo de tiempo en curso, reduce la velocidad de transmisión un 25%.

FECN (Notificación explícita de la congestión): Bit establecido en una trama que notifica a un router que el **dispositivo receptor** debe iniciar procedimientos para evitar la congestión. Cuando un switch Frame Relay detecta la existencia de congestión en la red, envía un paquete FECN al **dispositivo destino**, indicando que se ha producido la congestión.

1. ***Explique los conceptos de CIR y EIR. ¿Cómo interviene el bit DE en la operación del protocolo?***

*CIR (Commited Information Rate):* Es la tasa de transmisión, en bits por segundo, que la red garantiza transmitir, bajo condiciones normales.

CIR = Bc / Tc

*Bc (Committed Burst Size):* Es la cantidad máxima de bits que la red garantiza su entrega, durante Tc. Bajo condiciones normales.

*Tc (Committed Rate Measurement Interval):* Intervalo de tiempo durante el cual se mide la tasa de transmisión.

EIR (Extended Information Rate): Es la velocidad de información en exceso que se calcula:

EIR = Be/Tc

Be (Extended Burst Size): Es la cantidad máxima de bits por encima del CIR, que la red intentará entregar, durante Tc.

DE (Indicador de posible para descarte): Bit establecido que indica que la trama se puede descartar para darle prioridad a otras tramas si se produce congestión. Cuando el router detecta congestión de red, el switch Frame Relay descarta en primer lugar los paquetes con el bit DE. El bit DE se establece en el tráfico sobresuscrito (es decir, el tráfico recibido después de alcanzar la CIR).

**ATM**

1. ***¿Para qué se utilizan las opciones AAL1 y AAL2 en ATM? ¿En qué se diferencian?***
2. ***¿Qué clase de servicio implementa el AAL2 en ATM? ¿Qué características tiene este tráfico?***

IMPLEMENTA SERVICIOS DE AUDIO Y VIDEO COMPRIMIDOS.

1. ***¿Qué características tienen las clases de servicios A y B?***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **CLASE A** | **CLASE B** | **CLASE C** | **CLASE D** |
| **Características** | TASA BIT CONSTANTE | TASA BIT VARIABLE | CONEXIÓN ORIENTADA A DATOS | CONNECTION LESS DATA |
| **Sincronización entre Origen y Destino** | REQUERIDA | | NO REQUERIDA | |
| **Tasa Bit** | CONSTANTE | VARIABLE | | |
| **Tipo de Conexión** | ORIENTADA A LA CONEXIÓN | | | CONNECTION LESS |
| **Capa de Adaptación** | AAL1 | AAL2 | AAL5 | AAL 3/4 |
| **Utilización** | IMPLEMENTA SERVICIOS DE AUDIO Y VIDEO SIN COMPRIMIR, COMO SER VIDEO CONFERENCIA Y AUDIO INTERACTIVO | IMPLEMENTA SERVICIOS DE AUDIO Y VIDEO COMPRIMIDOS | TRANSMISIÓN DE DATOS + CONEXIÓN ORIENTADA A DATOS | TRANSMISIÓN DE DATOS + CONNECTION LESS DATA |

1. ***¿Qué parámetros de Calidad de Servicio controla?***

* *Peak-to-Peak Cell Delay Variation:* Variación máxima soportada en el retardo. Se mide entre el umbral de descarte y el maxCTD.
* *Maximum Cell Transfer Delay:* Tiempo entre la transmisión del último bit en la UNI, y la recepción del primer bit en la UNI destino
* *Cell Loss Ratio:* Tasa de pérdida máxima soportada en la conexión

1. ***¿Qué representan los campos VPI/VCI?***

Los VPI son identificadores de caminos virtuales y los VCI son identificadores de canales virtuales. Los VPI, junto con los VCI, se utilizan para identificar el próximo destino de una celda a medida que atraviesa una seria de switches ATM hasta llegar a su destino.

1. ***¿Cuál es la función de la capa de adaptación al ATM (AAL)?***

* Manejo de los errores en la transmisión
* Segmentación y reensamblado
* Manejo de las celdas perdidas o mal insertadas
* Control de flujo

**MPLS**

***Otros Profesores:***

1. ***MPLS vs ATM***

Los beneficios de MPLS sobre ATM es que permiten correr varios protocolos sobre el mismo, por ej IP o el mismo ATM, y permiten tener caminos preestablecidos para distintos tipos de datos. Los datos son clasificados con etiquetas al entrar en una red MPLS, y pueden ser tratados más eficientemente en conjunto de esta manera; por ejemplo, enviando datos de tipo real time por redes de baja latencia. En cambio ATM requiere establecer una conexión ante cada tráfico de datos, y requieren un adaptador ATM en el final de cada circuito (virtual o físico). Además, MPLS permite transmitir todo tipo de datos uniformemente, mientras que en ATM depende de la capa AAL usada.

1. ***UDP. Control de errores y flujo***

El sistema destino recibe el datagrama. Verifica el puerto destino con los puertos activos en ese momento.

* Sino coincide, envia un ICMP “destino inalcanzable”
* Si coincide, y hay lugar en el buffer, lo encola
* Sino hay lugar, lo descarta. No envia mensaje de error.

No realiza control de flujos.

**VPN**

1. ***La suite IPSec contempla dos protocolos y dos modos de operación. ¿Cuáles son?***

Dos modos de operación:

* Modo Transporte
* Modo Túnel

Dos protocolos:

* AH protocol
* ESP protocol

**Criptografía**

1. ***¿Qué características debe cumplir una función de “Hash”?***

* **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.

**Ipv6**

1. ***¿Cómo se representa una dirección IPv6?***

Representación Hexadecimal, agrupado de a 16 bits, separados por “:”. Existen 2 técnicas para facilitar la representación: la supresión de ceros y la compresión de ceros.

1. ***¿En qué consisten la compresión y supresión de ceros?***

La **supresión y compresión de ceros** se usan para facilitar la notación de las direcciones Ipv6.

La supresión de ceros consiste en eliminar los ceros más significativos (los de la izquierda de cada grupo entre los dos puntos).

Por ejemplo:

2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

Notación con supresión de ceros:

2001:DB8:0:2F3B:2AA:FF:FE28:9C5A

Entonces esta dirección con los ceros suprimidos, ven que estos cuatro ceros se transforman en uno solo y que 00FF se transforma en FF. Se sabe que en cada sección hay que completar con ceros a izquierda hasta extenderlo a 128 bits.

La **compresión de ceros** nos permite comprimir una larga secuencia. Consiste en eliminar una secuencia seguida de grupos de todos ceros. Solo se puede utilizar una sola vez.

Por ejemplo, la dirección local FE80:0:0:0:2AA:FF:FE9A:4CA2

Se representa como: FE80::2AA:FF:FE9A:4CA2

Acá habíamos tenido cuatro ceros, cuatro ceros, cuatro ceros, y todo esto se reemplaza por dos puntos, dos puntos. Esto significa que en el medio hay que llenar con ceros. ¿Cuántos? Todos los que hagan falta para que esto llegue a los 128 bits. Solamente se puede utilizar una sola vez.

1. ***¿Cómo se representa la dirección de loopback?***

::1

1. ***¿Cómo se identifican el prefijo de red y el identificador de interfaz?***

|  |  |  |
| --- | --- | --- |
|  | **16-bits-subred** | **64-bits-ID-Interfaz** |
| **128 bits** | | |

El prefijo de red usa CIDR.

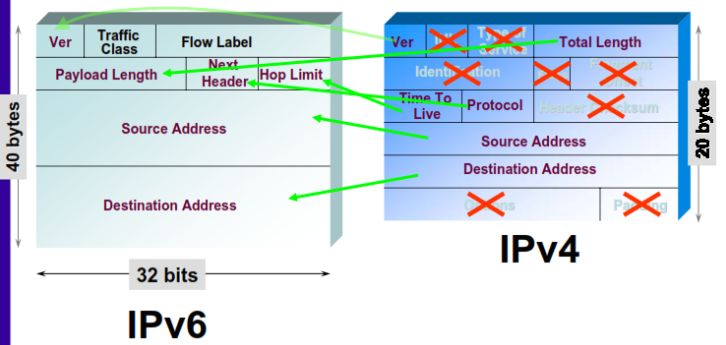
Para el identificador de interfaz puede usarse la MAC, pero como no alcanza para llenar los 64 bits entre el OUI (Identificador del Fabricante) y el DUI (Identificador del dispositivo) se mete FE.

::/0 Default Route

En IPV6 las redes son todas /64, por lo que no se necesita expresar el prefijo

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

1. ***Compare las cabeceras IP versión 6 y versión 4:***
   1. ***¿Qué campos están presentes en ambas cabeceras? Detalle las características.***
   2. ***¿Cuáles ya no están presentes en la versión 6?***
   3. ***¿Cómo identifica cada uno de ellos la dirección de “Broadcast”?***



1. Versión: Indica si es ipv4 o ipv6

Payload Length/Total Length = Tamaño Máximo de un Datagrama

Next Header/Protocol: Identifica la próxima cabecera, o el protocolo usuario del servicio (ICMPv6, UDP, TCP)

Ip origen/Ip destino: Dirección lógica de origen y destino

TTL o Hop limit:

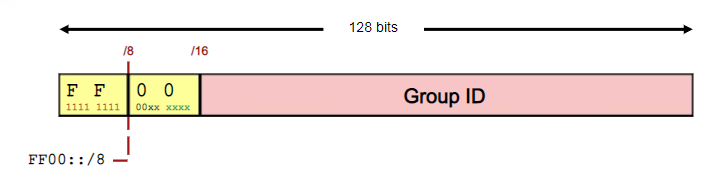
* Máxima cantidad de saltos
* Decrementado por cada router
* Cuando llega a 0 (cero) el datagrama es descartado

1. En Ipv6 no están presentes los siguientes campos:

* Longitud de la cabecera
* Tipo de servicio
* Identificación: Identifica unívocamente a cada datagrama
* Flags
* Desplazamiento de Fragmento (Offset)
* Checksum del Encabezado
* Opciones
* Relleno

1. IPv4 utiliza una ip reservada, que corresponde a la última dirección de la red

IPv6 utiliza multicast, los primeros 8 bit (0xFF), los siguientes 4 bit flags, los siguientes 4 bit scope, el resto group id.



**Otros Profesores:**

1. **Especificar los campos que forma la cabecera Ipv6, indicando su tamaño y una breve explicación.**

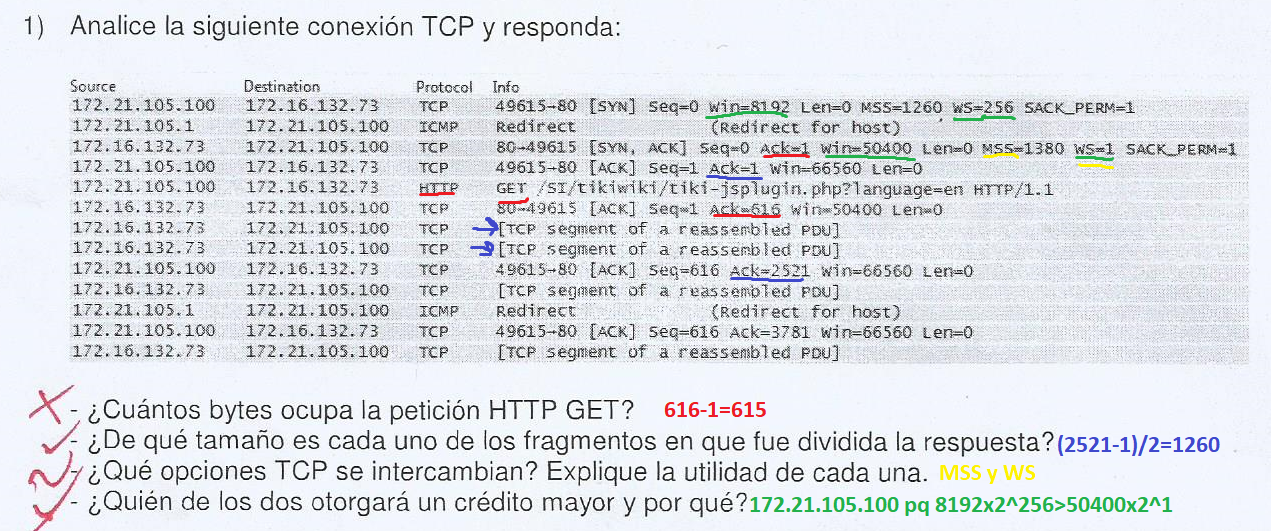
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IPv6 (8600)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0 |  |  |  | 4 |  |  |  | 8 |  |  |  | 12 |  |  |  | 16 |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 31 |
| **Versión** | | | | **Clase de tráfico** | | | | | | | | **Etiqueta del flujo** | | | | | | | | | | | | | | | | | | | |
| 4 bits | | | | 8 bits | | | | | | | | 20 bits | | | | | | | | | | | | | | | | | | | |
| **Long. Paquete** | | | | | | | | | | | | | | | | **Next header** | | | | | | | | **Hops limit** | | | | | | | |
| 16 bit | | | | | | | | | | | | | | | | 8 bits | | | | | | | | 8 bits | | | | | | | |
| **IP Origen** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 128 bits | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **IP Destino** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 128 bits | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

* *Versión:* Número de Versión del protocolo de Internet = 6
* *Clase de Tráfico:* 6 bits para clase de tráfico (prioridad - DSCP) 2 bits para ECN.
* *Etiqueta del Flujo:* Identifica el datagrama como perteneciente a una secuencia específica entre origen y destino.
* *Longitud del Paquete:* Longitud total de la carga (incluye cabeceras adicionales).
* *Next Header:* Identifica la próxima cabecera, o el protocolo usuario del servicio (ICMPv6, UDP, TCP).
* *Hop Limit:* Máxima cantidad de Saltos.

1. **Explicar que sucede en Ipv6 si es necesario realizar una fragmentación.**

[IPv6](https://es.wikipedia.org/wiki/IPv6) ya no permite a los routers fragmentar los paquetes. El emisor siempre está informado con un mensaje ICMP cuando una fragmentación será necesaria. Así el emisor puede bajar su tamaño de paquete para esta conexión y la fragmentación ya no es necesaria. En caso de requerirse una fragmentación; el host, es quien debe hacerla.

**Práctica**

****

WS me permite aumentar el tamaño de la ventana.

MSS es la opción que permite determinar cuál tiene que ser el valor de segmento para que quepa dentro de un datagrama IP sin fragmentar.

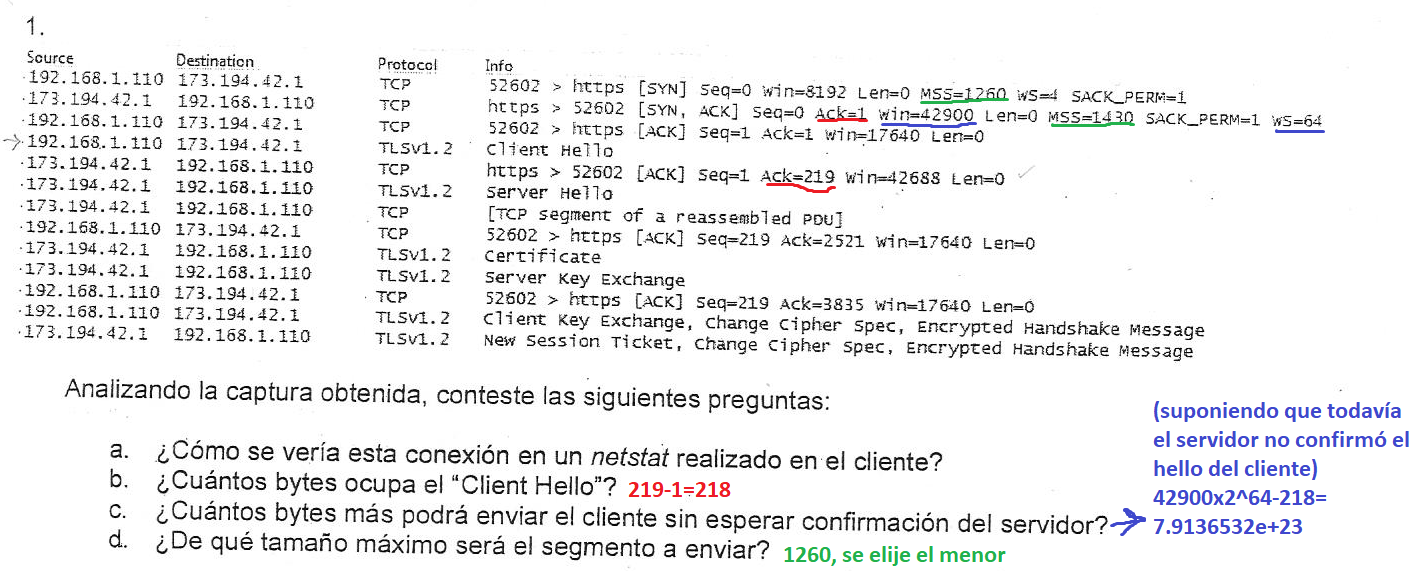
SACK\_PERM permite que se retransmita nada más los paquetes que se perdieron.

Más info:

The window scale factor is used in an interesting way. If the source proposes a window of size k big and proposes to scale it by n, then the destination understands that the window proposed by the source is k x 2n (that is, it increases the width of the window by n bits).

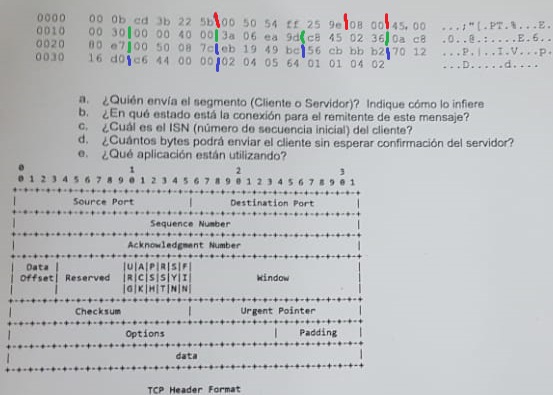
SACK is an acronym for Selective ACKknowledgment.

<http://packetlife.net/blog/2010/jun/17/tcp-selective-acknowledgments-sack/>



a)

|  |  |  |  |
| --- | --- | --- | --- |
| Proto | Dirección Local | Dirección Remota | Estado |
| TCP | 192.168.1.110:52602 | 173.194.42.1:https | ESTABLISHED |



a) source port = 0050 = 80 => Es menor a 1024, entonces es puerto del servidor.

b) 12 = 0001 0010 => ACK=1 y SYN=1 => el remitente está en estado SYN\_RECV

c) ISN=acknowledge number - 1

d) window

e) http

Tener en Cuenta:

* ESTABLISHED – El socket tiene una conexión establecida.
* SYN\_SENT – El socket intenta iniciar una conexión.
* SYN\_RECV – La red recibió una petición de conexión.
* FIN\_WAIT1 – El socket está cerrado, y la conexión está finalizando.
* FIN\_WAIT2 – La conexión está cerrada, y el socket espera que finalice la conexión remota.
* TIME\_WAIT – El socket espera después de cerrarse que terminen los paquetes que siguen en la red.
* CLOSED – El socket no se usa.
* CLOSE\_WAIT – La conexión remota ha terminado, y está a la espera que se cierre el socket.
* LAST\_ACK – La conexión remota ha finalizado, y se espera que se cierre el socket. Esperando el acknowledgement.
* LISTEN – El socket está a la espera de posibles conexiones entrantes.
* CLOSING – Ambos sockets han terminado pero aún no se enviaron todos los datos.
* UNKNOWN – El estado del socket es desconocido.
* DELETE\_TCB – Se está eliminando el búfer del control de transmisión (TCB) para la conexión TCP.