- En modulación FSK, una frecuenca alta representa un 1 y una frecuencia baja representa un 0. Si la tasa de bits de una señal FSK es 2400 bps, la tasa en baudios es

2400

Justificación: baudios=bits por segundos (bps) en este caso FSK, puede que no pase en otros casos.

- En el sistema de codificación en línea RZ (retorno a cero) el 1 se representa con una tensión positiva y el 0 se representa con tensión negativas y ambas vuelven a 0 en un intervalo de bit. ¿es un buen sistema de señalización?

Si, ya que se diferencia cada bit en una secuencia larga de 1s o 0s

- Si el ancho de banda de una señal es 3000KHz y la frecuencia mas baja es 300KHZ, ¿Cuál es la frecuencia mas alta?

3300KHZ, pues el ancho de banda es igual a frecuencia mas alta - frecuencia mas baja

- ¿Que problema tenía el sistema de codificación NRZI? ¿Cómo se solucionaba?

Cuando hay que transmitir una secuencia larga de ceros, emisor y receptor pueden desincronizarse. Es por ello que junto a la codificación NRZI se emplea la codificación 4B/5B para que nunca halla mas de 3 ceros consecutivos.

- ¿La comprensión/descomprensión de datos es responsabilidad de la capa?

6: Presentación

- El servicio FTP es proporcionado por la capa nº…

7: Aplicación

- En una trama, el campo datos contiene:

El paquete de la capa 3

- En la transmisión de una trama se pueden producir errores en los bits. Señala las dos causas principales:

Ruido, atenuación de señal

- Sean los siguientes cables de fibra óptica: 8/125 62,5/125 ¿Cuál dirías que es multimodo?

El núcleo de fibra multimodo de 62,5 es mayor para que puedan circular los diferentes haces de luz, cada uno siguiendo una trayectoria.

- Cuando se transmiten datos del host A al B, la cabecera de la capa de transporte de A es leída ¿por qué capa de B?

Transporte

- ¿Por qué un punto de acceso es un dispositivo de capa 2?

Porque conecta directamente cada host a un dispositivo de red mediante un cable punto a punto.

- ¿Cuál de las siguientes medidas contribuyen a mejorar la resistencia al ruido EMI?

Trenzado de hilos

Transmisión de señales diferenciales

Terminación adecuada de los conectores

***Todas las respuestas son correctas***

- ¿Cuál de las siguientes no es una fuente de ruido EMI?

Motor eléctrico

Descargas atmosféricas

***Diafonía***

Iluminación fluorescente

- ¿Cuál de las siguientes es una tecnología LAN?

Frame-Relay

***Wi-FI***

ATM

PPP

- La transmisión en Ethernet es banda base

Verdadero

- En la transmisión banda base, el ancho de banda del medio es dividido en canales (bandas). Cada canal es capaz de transferir una señal de datos de forma independiente.

Falso (solo se transmite una señal por el medio físico)

- Cuando un hub recibe una trama, la envía por todos sus puertos excepto por el origen

Verdadero (inundación)

- Un switch recibe una trama por el puerto Gi0/1. La MAC destino de la trama es 22-… y la de origen es 34-… Por tanto, si el switch no tuviera en su tabla CAM la entrada [22-… | Gi0/1] ¿debería registrarla en ese instante?

Falso (El switch realizará una inundación hasta encontrar esa MAC de destino)

- El switch se comporta como un HUB cuando la tabla CAM está vacía

Verdadero

- Cuando hablamos de tecnologías de red nos referimos a las capas 1, 2 y 3 del modelo OSI

Falso (solo capa 3)

- 1000BaseT, a diferencia de 100BaseTx, utiliza los ocho hilos del cable de par trenzado para transmitir datos

Verdadero

- A igual potencia, las señales generadas por un dispositivo Wi-Fi que funciona en la banda de 5Ghz tienen menor alcance que las generadas por un dispositivo que funciona a 2,4 Ghz

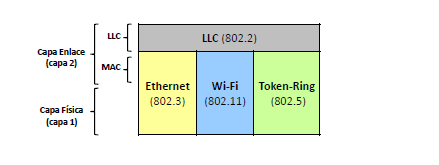
Verdadero

- En los tendidos de fibra óptica hay que evitar las fuentes de ruido EMI

Falso (La fibra tiene como factores intrínsecos la dispersión y como factores extrínseco la curvatura del cable)

- El estándar Wi-Fi 802.11 abarca la capa física y la subcapa MAC de la capa de enlace

Verdadero, abarca ambas



- El puerto Ethernet de un router tiene una dirección MAC

Verdadero, la del host que tenga conectado.

- Cuando, en el equipo destino, llega un segmento a la capa 4, se extrae su cabecera

Verdadero

- Un hub puede leer una cabecera de capa 2

Falso (un hub es prácticamente de capa 1)

- El protocolo ARP se utiliza para descubrir la IP de un nombre de dominio

Falso (Se emplea nslookup ej: nslookup google.com). El ARP se emplea para descubrir la dirección física de una IP

- Cuando accedo a un servidor FTP, se abre una conexión en mi ordenador que tiene como puerto origen un puerto conocido, en este caso el 21

Falso (Nuestro ordenador (cliente) se conectará desde un puerto aleatorio no privilegiado (mayor a 1024) al puerto control del servidor (21)

- En un dominio, la gestión de usuarios es llevada a cabo por el equipo que tiene instalado un sistema operativo.

Creo que verdadero, ya que la gestión de usuarios es llevada por quien tiene permisos administrativos en ese sistema operativo.

- Si está instalado el servicio “Compartir impresoras y archivos para redes Microsoft”, podre acceder a carpetas compartidas de otros usuarios de la red.

Falso

MODELO OSI

- Aplicación: *Datos*

Proporciona servicios de red a las aplicaciones

- Presentación:

Formatea la información que se va a transmitir

Encripta/desencripta la información

Comprime/descomprime la información

- Sesión:

Abrir y cerrar sesiones entre las aplicaciones origen y destino (autenticación y autorización)

Reanuda una transmisión interrumpida

Sincroniza un diálogo

- Transporte: *Segmentos*

Segmenta el mensaje en unidades más pequeñas (segmentos)

Asegura que todos los segmentos lleguen al host destino (acuse de recibo, retransmisión)

Controla el flujo de datos para que no se sobrecargue el host de destino (ventana)

Permite que un host pueda tener varias conexiones a la vez (puertos)

Asigna un numero de identificación a cada conexión (socket)

- Red: *Paquete*

Direccionamiento lógico (IPv4)

Establecer la ruta por la que se enviarán los datos

Encaminar los datos por la ruta hasta alcanzar el host destino

- Enlace: *Trama*

Direccionamiento físico (MAC)

Detectar errores en los datos recibidos

Arbitrar el acceso al medio

Aislar las capas superiores de la tecnología de red utilizada

- Físico *Bits*

Definir las características físicas del medio y de los conectores

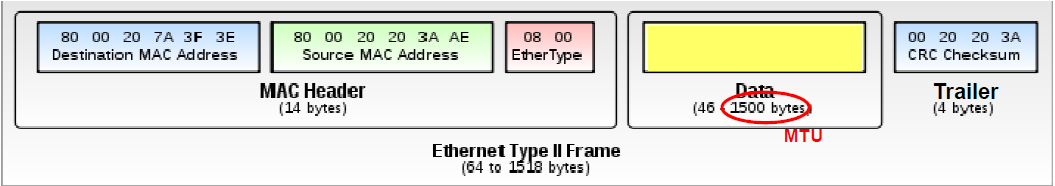
Codificar o modular los datos para su transporte por el medio

Link-Local (*169.254.0.0/16*)

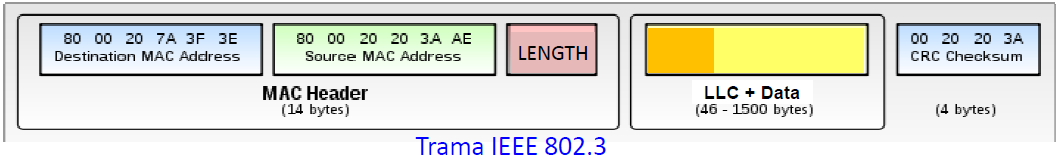
Si un equipo no tiene asignada una dirección IP (o no consigue contactar con el servidor DHCP para que le proporcione una dirección IP) y su sistema operativo tiene habilitada la función de autoconfiguración, configurará automáticamente una IP Link-Local.

Los equipos que tienen una dirección Link-Local no tienen acceso a Internet, sólo pueden comunicarse con equipos que están en la misma red.

Entramado capa de enlace (Ethernet)



Entramado capa de enlace (IEEE 802.3)



LLC

En la trama 802.3, IEEE estableció que el **tipo del protocolo de capa 3 y otros datos de servicio** irían en un encabezado adicional denominado LLC (**Control de Enlace Lógico**) perteneciente a la capa 2. El encabezado LLC se sitúa dentro del campo datos de la trama. LLC está definido en el estándar IEEE 802.2.

LLC también está presente en **Wi-Fi y Token Ring**

¿Un switch tiene MAC?

Switch de capa 2, solo tiene una MAC propia y esa MAC pertenece al BACKPLANE.

El blackplane también es conocido como `Bus´, conecta todos los puertos del switch internamente (en el switch).

Las otras MACs que pueda tener se almacenan en la tabla CAM donde cada puerto tendrá su host de destino.

Banda base vs Banda ancha

- Solo se transmite **una señal** por el medio físico (Ethernet)

- Se transmiten **varias señales** a la vez por el medio físico (ADSL: banda para servicio telefónico, banda para enviar datos y banda para recibir datos)

Conexión FTP: Puerto activo vs puerto pasivo

*Activo*

El cliente se conecta desde un puerto aleatorio no privilegiado (N>1024) al puerto control del servidor (21)

El cliente empezará a recibir en el puerto N+1 y envía este puerto de control al servidor

El servidor se conectará al cliente en el puerto N+1 desde su puerto de datos (20)

*Pasivo*

El cliente abre dos puertos aleatorios no privilegiados (N>1024 y N+1)

El primer puerto se conecta al puerto 21 y envía el comando PASV

Luego el servidor abre un puerto no privilegiado (P>1024) y envía PORT al cliente

Finalmente, el cliente inicia una conexión desde N+1 al puerto P para transferir datos.

Keep-alive

Una conexión HTTP con keep-alive **permite realizar más de una petición por la misma conexión** establecida, **evitando establecer una conexión nueva para cada recurso** asociado a dicha web (**audio, imágenes**…). Es decir, el objetivo de tener habilitado keep-alive es crear conexiones persistentes con un servidor web.

Antes de que esta característica existiese, se necesitaba una conexión TCP separada para cada petición. Una para el html, otra para cada imagen, otra para cada audio,...

Los principales beneficios al usar conexiones persistentes son:

Al abrirse menos conexiones TCP, se ahorran recursos (CPU, memoria, etc.).

Se permite al cliente hacer múltiples peticiones sin esperar a las respuestas.

Reducción de la latencia en peticiones al utilizar varias veces un canal ya abierto.

Keep-alive se establece en el campo Connection de la cabecera HTTP.

En el frame nº 4 de la captura2 de la práctica de laboratorio 9 puede verse que el navegador web (cliente) al pedir la página /products de www.dji.com establece el Connection: keep-alive, el cual es aceptado por el servidor ya que en el frame nº 19 éste responde tambien con un Connection: keep-alive aceptando por tanto que la conexión sea persistente, si dicho servidor web, por el motivo que fuera, estuviese configurado de tal forma que no permita conexiones persistentes respondería con un Connection: close.

IF-MODIFIED-SINCE

If-modified-since es uno de los campos de la cabecera HTTP que **permite solicitar** **(con GET)** **un recurso a un servidor web pero sólo si ha sido modificado desde una fecha determinada**. Es decir, **si el cliente ya dispone de dicho recurso (en caché)** porque previamente ya lo había solicitado, y sabe por tanto la fecha y hora que obtuvo dicho recurso, entonces **mediante ese GET condicional** **solicitamos al servidor ese mismo recurso**, pero **sólo si ha sido modificado desde esa fecha** que le hemos indicado.

El servidor si efectivamente tiene una copia de ese fichero con modificación posterior a esa fecha, contestará con el código 200 OK y envia ese fichero, por el contrario si ese fichero no ha sufrido modificaciones desde entonces, responderá con un 304 Not Modified ahorrándose de envíar de nuevo el fichero.

En el frame nº 21 de la captura2 de la práctica de laboratorio 9 puede verse que el navegador web (cliente) al pedir la página / (home del sitio) de www.dji.com en dicho GET establece If-Modified-Since: Mon, 16 Feb 2015 10:42:15 GMT (porque ya tendrá una copia en caché de dicha página desde esa fecha/hora). En el frame nº 23 el servidor responde con un 304 Not Modified y por tanto no envía nada ya que dicho recurso no ha sufrido modificación desde esa fecha.

SACK-PERM

Está opción se envía sólo en un segmento SYN (fase establecimiento de la conexión) y aparece si está activada como SACK\_PERM=1, tal y como aparece en los frames nº 7 y 8 de la captura de la práctica 11, con esto se indica en la negociación que se está dispuesto a emplear la opción SACK durante la fase de transferencia de datos, es decir se permiten hacer confirmaciones selectivas de segmentos TCP. ¿Y qué es eso de SACK o confirmaciones selectivas?

SACK (Selective Acknowledgment)

Permite informar al emisor de los octetos de datos de segmentos de información no contiguos que han sido recibidos correctamente y evitar vencimientos de temporizadores y retransmisiones innecesarias. Implícitamente, indica qué octetos de datos se han perdido o no han llegado todavía.

Si el receptor no ha recibido la opción SACK\_PERM=1 en el establecimiento de la conexión, no debe usar la opción SACK en la fase de transferencia de datos.

Se recomienda la opción SACK cuando hay múltiples pérdidas de segmentos TCP

Por congestiones en los routers IP

Por errores físicos en el nivel de enlace, especialmente, en entornos inalámbricos (CRC de la trama).

De esta forma se evitan innecesarias retransmisiones de los octetos de datos de segmentos de información no contiguos que ya fueron entregados al receptor.

MSS

MSS (Maximum Segment Size). Es la **cantidad máxima de bytes de datos** que puede contener un **segmento**. Al establecerse una conexión TCP, los equipos deben acordar y establecer el MSS que pueden aceptar. Como la cabecera IP y TCP ocupan al menos 20 Bytes cada una, tenemos que:

MSS = MTU – cabecera IP – cabecera TCP

Que normalmente suele ser:

MSS = MTU – 40

¿Y qué es el MTU?

MTU (Máximum Transmission Unit

Se conoce como Unidad Máxima de Transmisión a la **cantidad máxima de datos** que una **trama** de la capa de enlace **puede transportar**. En otras palabras, cuando un datagrama se encapsula en una trama, el tamaño total del datagrama debe ser menor que este tamaño máximo. Dicho tamaño está definido por restricciones impuestas por la tecnología de red.

Ejemplos de MTU:

Ethernet: 1500 Bytes

Wifi: 2312 Bytes

PPPoE: 1492 Bytes

Usos 0.0.0.0

1.- La ruta predeterminada local **0.0.0.0** se utiliza cuando el **paquete no coincide con otras instrucciones** especificadas en la **tabla de enrutamiento**. El **paquete** se envía hacia el **gateway** desde la PC para un **procesamiento adicional**.

2.- En el contexto de servidores, 0.0.0.0 significa “todas las direcciones IPv4 en la maquina local”. Si un host tiene dos direcciones IP y un servidor está activado para escuchar 0.0.0.0, llegaran ambas IPs a este.

3.- Es la **dirección** que el host reclama como propia cuando **no** se le es **asignada** **ninguna** **dirección** aún por el **DHCP**.

*Cuando un servicio está escuchando en 0.0.0.0 esto significa que el servicio está escuchando en todas las interfaces de red configurada.*

*Cuando escuchando en 127.0.0.1 el servicio está limitado sólo a la interfaz de loopback (sólo disponible en el equipo local)*

DHCP ( Dynamic Host Configuration Protocol )

Es un **servidor** que usa protocolo de red de tipo cliente/servidor en el que generalmente, un servidor **posee** **una** **lista** **de direcciones IP dinámicas** y las **va** **asignando** **a los clientes** según queden libres. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente.

TCP y UDP

**TCP** ( Transsmision Control Protocol)

El protocolo IP de la capa de red no garantiza la entrega de paquetes (IP envía paquetes sin saber si han sido recibidos por el equipo destino), por lo que es un protocolo no confiable.

En su defecto, esta garantía la puede proporcionar la capa de transporte mediante el protocolo TCP.

**TCP garantiza la entrega**

En una conexión TCP existen 3 etapas:

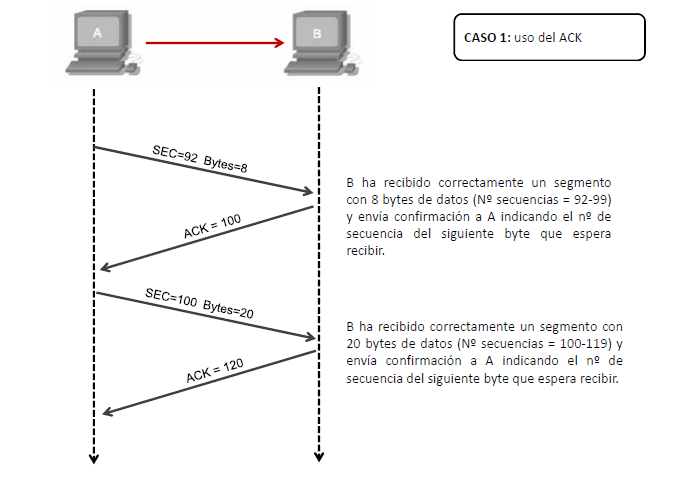
- Establecimiento de la conexión

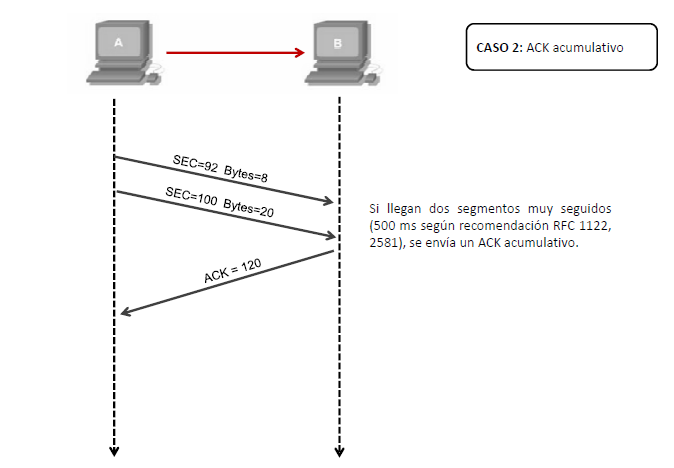
- Transferencia de datos

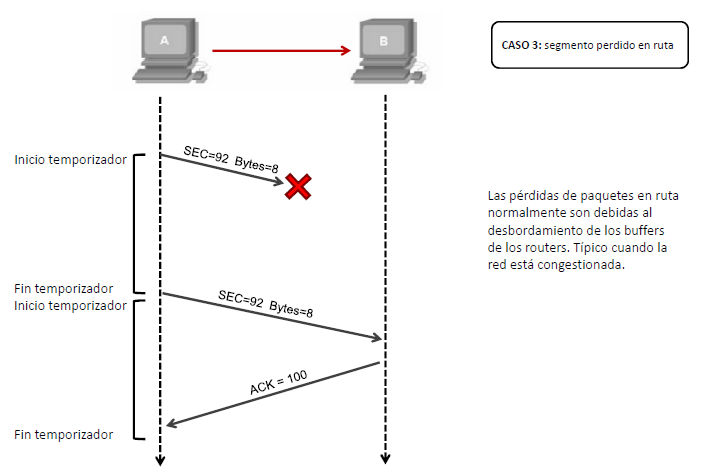
- Fin de la conexión

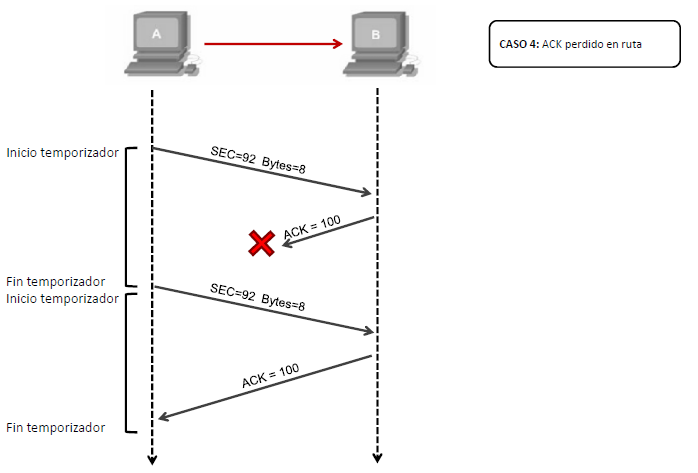
El TCP además confirma al emisor los bytes de datos que han sido recibidos correctamente mediante los ACK (acuse de recibo). Un ACK es el número de secuencia del siguiente byte que se espera recibir, quedando confirmados los bytes anteriores.

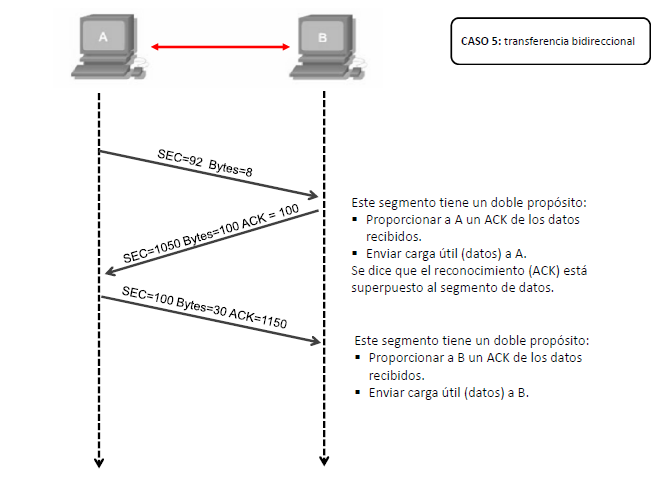
Podemos diferenciar 5 casos:





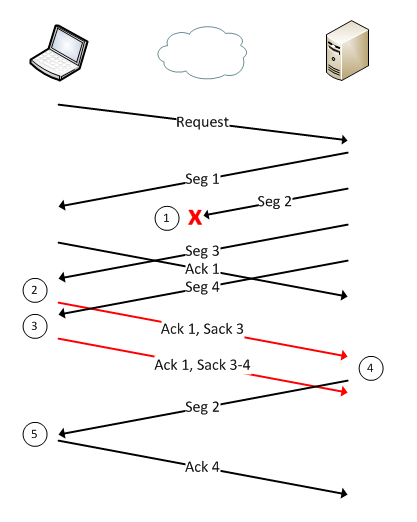
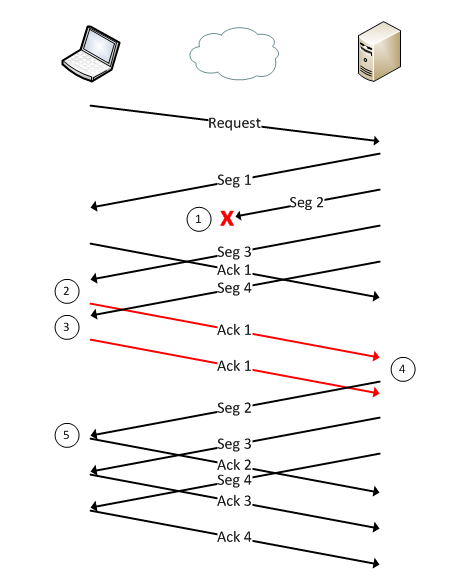






SACK

El SACK le permite al cliente decir “Solo tengo el paquete uno en orden, pero también he recibido el 3 y el 4, no hace falta que los envíes de nuevo”



WS (Window Scale)

Es utilizado para establecer control de flujo.

Máximo 65.535 Bytes, pero existe una opción de factor de escala para incrementar este valor.

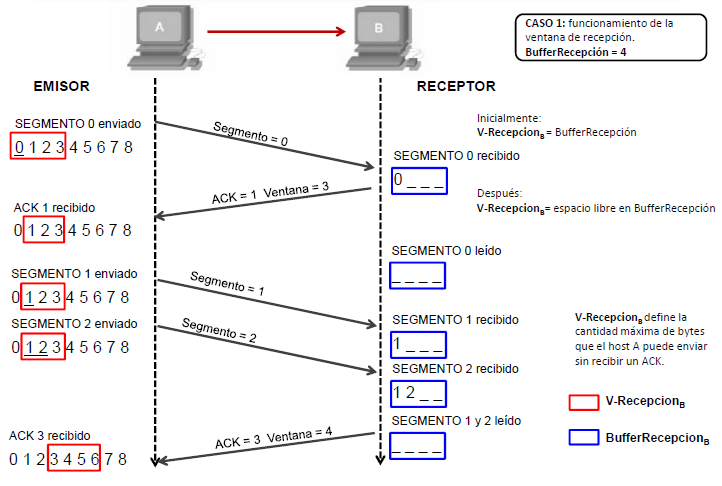
Dicho Factor de Escala de la Ventana (definido en RFC 1323): Permite ampliar el campo VENTANA (Window size). La escala de ventana TCP (TCP window scale) es una opción usada para incrementar el máximo tamaño de ventana desde 65.535 bytes, a 1 Gigabyte.

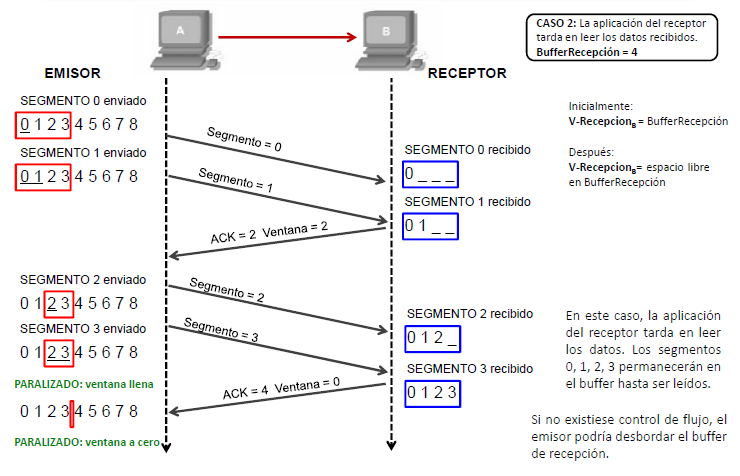
La opción de escala de ventana TCP es usada solo durante la negociación en tres pasos que constituye el comienzo de la conexión. El valor de la escala representa el número de bits desplazados a la izquierda de los 16 bits que forman el campo del tamaño de ventana. El valor de la escala puede ir desde 0 (sin desplazamiento) hasta 14. Hay que recordar que un número binario desplazado un bit a la izquierda es como multiplicarlo en base decimal por 2.

Por tanto para calcular el nuevo tamaño de ventana lo que se hace es:

Nueva Ventana = Ventana actual x 2F donde F va de 0 a 14.

Podemos diferenciar dos casos:

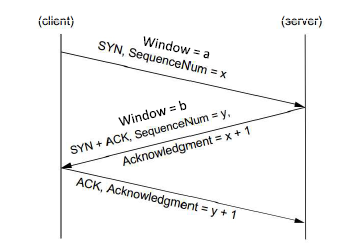




Establecimiento de la conexión (saludo de 3 vias)

**Antes de transmitir datos**, cada **host** debe **poner en conocimiento** del otro su **número de secuencia inicial** y el **tamaño inicial de su ventana de recepción**.

Esta primera fase se denomina saludo de tres vías:



**UDP**

**No garantiza la entrega ni el control del flujo**

Ciertas aplicaciones prefieren utilizar el protocolo UDP porque es más rápido, aunque éste no garantice la entrega.

En este caso, son los protocolos de la capa de aplicación los que gestionan los errores.

¿Qué aplicaciones utilizan UDP?

- Aplicaciones que requieren velocidad y toleran pequeñas pérdidas de datos. En estos casos, resulta más importante transmitir a alta velocidad que garantizar la entrega de paquetes. Ejemplo: VoIP, streaming, juegos on-line.

- Aplicaciones que transmiten pequeñas cantidades de datos. Estas pequeñas cantidades de datos no justifican toda la información de control que se debe transmitir durante las fases de establecimiento y finalización de la conexión en el protocolo TCP. Ejemplo: la mayoría de las consultas-respuestas DNS.

- Aplicaciones que desean integrar los mecanismos de transferencia confiable en su código. Es posible que una aplicación proporcione transporte confiable utilizando UDP. Esto se puede conseguir si las características de fiabilidad se incorporan en la propia aplicación.

NAT y PAT y Puertos

El NAT (Network address translation) **mapea una dirección IP privada a una dirección pública**. El router asignará a a cada dirección privada una dirección pública distinta. Las **correspondencias entre direcciones privadas y pública**s se registran en una tabla del router denominada **tabla NAT**.

El PAT (Port address translation) o NAT con sobrecarga, **asigna la misma dirección pública a todas las direcciones privadas de la red**. Para **diferenciar** las entradas en la tabla NAT, se **utilizan los números de puerto**.

Ambos pueden funcionar a la vez en el router.

La combinación de la dirección **IP** y el número de **puerto** se denomina **socket**. Un socket identifica un proceso de red de manera única en Internet.

Los puertos más conocidos son:

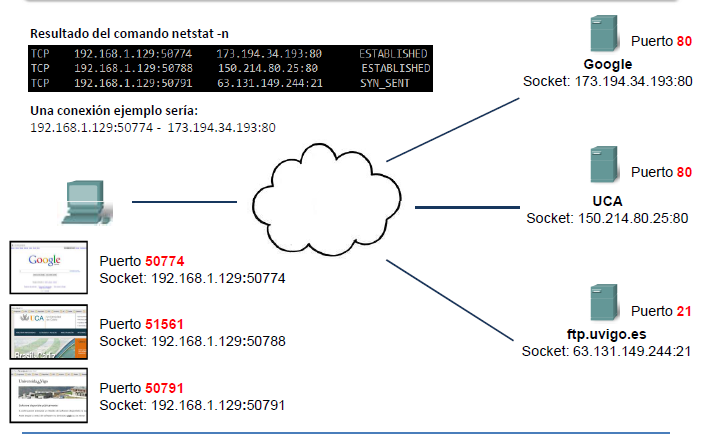
- FTP=21

- TELNET=23

- DNS=53

- HTTP=80

Un ejemplo donde aparecen los puertos puede ser este:



Hemos usado el comando Netstat, el cual comprueba el estado de las conexiones que mantiene el PC, donde los estados TCP pueden ser:

- SYN\_SENT: El cliente inicia la conexión enviando un segmento SYN al servidor. Después de enviar este segmento, el cliente entra en el estado SYN\_SENT.

*SYN es un bit de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales de una conexión en el procedimiento de establecimiento de tres fases (3 way handshake)*

*Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo).*

- ESTABLISHED: Cuando el cliente recibe respuesta del servidor, le envía el ACK correspondiente y entra en estado ESTABLISHED. Durante este estado, cliente y servidor se envían segmentos que contengan **datos** de **carga útil.**

**IMPORTANTE:** Cuando ambos equipos transmiten carga útil, se dice que la transferencia es bidireccional.



- FIN\_WAIT. Cuando el cliente decide cerrar la conexión, envía un segmento FIN al servidor. Luego le devolverá otro FIN\_WAIT\_2 el servidor donde el bit de FIN estará puesto a 1.

DNS

DNS, abreviatura del inglés que significa servicio de nombres de dominio, permite controlar la configuración de correo electrónico y sitio web de tu nombre de dominio. Cuando los visitantes van a tu nombre de dominio, la configuración de DNS controla a cuál servidor de la empresa se dirigen.

Por ejemplo, si utilizas la configuración de DNS de GoDaddy, los visitantes llegarán a los servidores de GoDaddy cuando utilicen tu nombre de dominio. Si quieres cambiar esa configuración para usar los servidores de otra empresa, las visitas irán a ellos en lugar de a nosotros cuando visiten tu dominio.

Se divide en 4 niveles, jerárquicamente:

- Root o raíz: maneja todos los servidores (suele ser el punto .)

- Niveles top: (com, net…geográficos como es…)

- Segundo nivel: nombre del dominio (pe google)

- Tercer nivel: servidor web, correo, ftp, etc

Pasos de funcionamiento: (ej www.capacity.com)

1.- El cliente le preguntará a su DNS local por la dirección (pe los dns de google 8.8.8.8)

2.- Si el nombre está en el registro del caché del DNS del router o servidor le responderá directamente al cliente con la dirección. Esto se conoce como consulta recursiva.

3.- Si no conoce la respuesta le preguntara al DNS ISP.

4.- Si tampoco tiene la dirección, este le pregunta al root server y le dice al ISP que busque la dirección en los servidores .com de los niveles top

5.- El ISP pregunta ahora al nivel top y este le responde donde se halla la dirección de capacity

6.- Por ultimo, el ISP va al segundo nivel que tiene un registro del tipo A donde dice cual es la dirección IP local del servidor web de capacity y se la devuelve al ISP y este al pc.

Para saber el nombre por dominios de una máquina a partir de la IP o para acceder a la abundante información de la que disponen los servidores DNS, puedes utilizar el comando ***nslookup*** (pe nslookup www.google.es)

**WIRESHARK**

Protocolos

*ARP*

ARP es un protocolo de capa de red responsable de encontrar la dirección de hardware (MAC) que corresponde a una determinada dirección IP. Para ello se envía una consulta ARP (ARP request) a la dirección de broadcast MAC (FF:FF:FF:FF:FF) consultando por la dirección IP y se espera a que esta máquina responda (ARP reply) con la dirección MAC que le corresponde. Cada máquina mantiene luego una caché con las direcciones traducidas para reducir el retardo y la carga. Para acceder a dicha tabla usamos el comando arp-a.

*TCP*

TCP es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen o van al nivel inferior del modelo OSI (IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). TCP es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

Las principales características del protocolo TCP son las siguientes:

- TCP permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.

- TCP permite que el monitoreo del flujo de los datos y así evita la saturación de la red.

- TCP permite que los datos se formen en segmentos de longitud variada para "entregarlos" al protocolo IP.

- TCP permite multiplexar los datos, es decir, que la información que viene de diferentes fuentes (por ejemplo, aplicaciones) en la misma línea pueda circular simultáneamente.

- Por último, TCP permite comenzar y finalizar la comunicación amablemente.

CNAME

Canonical Name - (Nombre Canónico) Se usa para crear nombres de hosts adicionales, o alias, para los hosts de un dominio. Es usado cuando se están corriendo múltiples servicios (como ftp y web server) en un servidor con una sola dirección IP. Cada servicio tiene su propia entrada de DNS (como ftp.ejemplo.com. y www.ejemplo.com.). Esto también es usado cuando corres múltiples servidores http, con diferentes nombres, sobre el mismo host.

Tipos de servidores DNS

- Servidor autoritativo: Con este nombre se conoce al servidor que contiene los registros de recursos para una zona (SOA y NS).

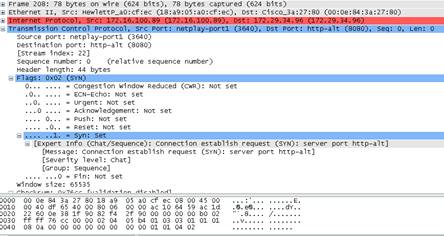
*NS = Name Server - (Servidor de Nombres) Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.*

*SOA = Start of authority - (Autoridad de la zona) Proporciona información sobre la zona.*

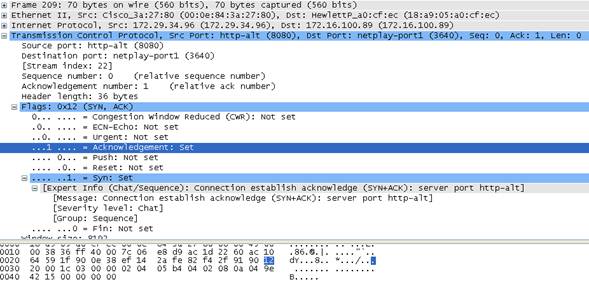
Cada zona puede tener uno o más servidores de nombres de dominio autoritarios. Uno de ellos debe ser primario, que manejará la información del dominio. Si tiene varios, el resto pueden ser secundarios o caché.

Establecimiento de conexión (handshake de tres vías)

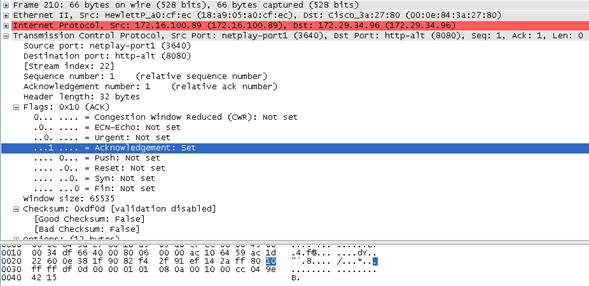
**1. SYN**



**2. SYN /ACK**



**3. ACK**



Lo cual podemos ver claramente reflejado en la opción diagráma de flujo

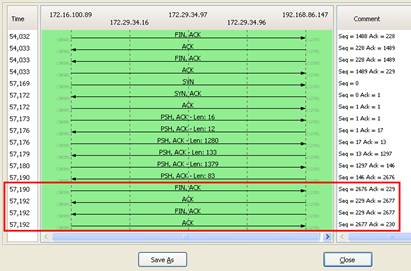


Cierre de Conexión

La fase de finalización de la conexión usa una [negociación](http://www.monografias.com/trabajos10/bane/bane.shtml) en cuatro pasos, terminando la conexión desde cada lado independientemente.

Cuando uno de los dos extremos de la conexión desea parar su "mitad" de conexión transmite un paquete FIN, que el otro interlocutor asentirá con un ACK. Por tanto, una desconexión típica requiere un par de segmentos FIN y ACK desde cada lado de la conexión.

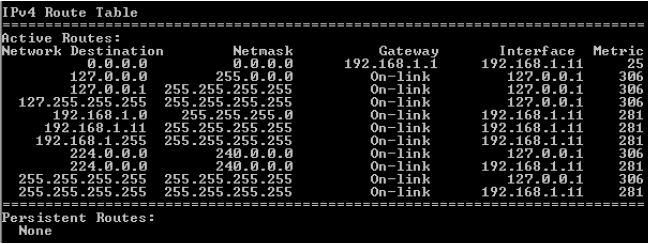
Para el ejemplo utilizado, esto sucede finalmente con el cierre del navegador, a partir del paquete 876



Carga útil

Cuando nos referimos a carga útil, nos referimos a si el nivel actual (por ejemplo ethernet) ha recibido información del nivel de red (o sea, todo su PDU con las cabeceras incluidas)

Tabla de ruta (Práctica)



El resultado muestra cinco tipos diferentes de rutas activas:

• La ruta predeterminada local **0.0.0.0** se utiliza cuando el **paquete no coincide con otras instrucciones** especificadas en la **tabla de enrutamiento**. El **paquete** se envía hacia el **gateway** desde la PC para un **procesamiento adicional**. En este ejemplo, el paquete se envía hacia 192.168.1.1 desde 192.168.1.11.

• Las direcciones de **loopback, 127.0.0.0 – 127.255.255.255**, están relacionadas con la conexión directa y **prestan servicios al host local**.

• Todas las direcciones para la subred, **192.168.1.0 – 192.168.1.255**, están relacionadas con el **host y la red local**. Si el **destino** final del paquete **está en la red local**, el paquete **sale** de la interfaz **192.168.1.11**.

- La dirección de la ruta local 192.168.1.0 representa todos los dispositivos en la red 192.168.1.0/24.

- La dirección del host local es 192.168.1.11.

- La dirección de broadcast de la red 192.168.1.255 se utiliza para enviar mensajes a todos los hosts en la red local.

• Las direcciones **multicast** de clase D especiales **224.0.0.0** **están reservadas** para ser utilizadas a través de la interfaz **loopback (127.0.0.1)** o del **host (192.168.1.11).**

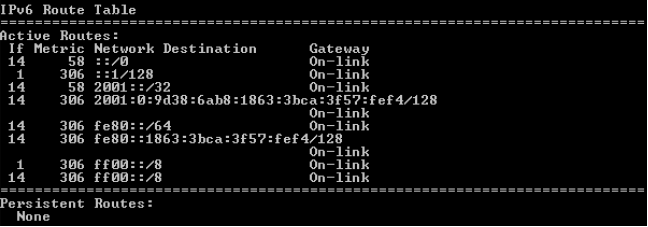
• La dirección de **broadcast local 255.255.255.255** se puede utilizar a través de la interfaz **loopback (127.0.0.1)** o del **host (192.168.1.11).**

**Según el contenido de la tabla de enrutamiento IPv4, si la PC deseara enviar un paquete a 192.168.1.15, ¿qué haría y adónde enviaría el paquete?**

La PC consultaría la tabla de rutas IPv4 y haría coincidir la dirección IP de destino con la entrada 192.168.1.0 de Network Destination para mostrar que el host está en la misma red (On-link). Luego, la PC enviaría el paquete hacia el destino final mediante su interfaz local (192.168.1.11).

**Si la PC deseara enviar un paquete a un host remoto ubicado en 172.16.20.23, ¿qué haría y adónde enviaría el paquete?**

La PC consultaría la tabla de rutas IPv4 y encontraría que no hay una coincidencia exacta para la dirección IP de destino. Luego, elegiría la ruta predeterminada local (red 0.0.0.0, máscara de red 0.0.0.0) para revelar que debe reenviar el paquete a la dirección de gateway 192.168.1.1 (la dirección de un dispositivo de gateway, como una interfaz del router en la red local). Luego, la PC reenviaría el paquete hacia el Gateway mediante su interfaz local (192.168.1.11). A continuación, el dispositivo de gateway determina la siguiente ruta que debe tomar el paquete para llegar a la dirección de destino final, 172.16.20.23.



En este ejemplo, en la ilustración se muestra la sección de la tabla de rutas IPv6 que se genera con el comando netstat –r para mostrar los siguientes destinos de red:

• **::/0**: es el equivalente en IPv6 a la **ruta predeterminada local**. En la columna Gateway, se proporciona la dirección link-local del router predeterminado.

• **::1/128**: equivale a la dirección de **loopback** IPv4 y proporciona servicios al host local.

• **2001::/32**: es el prefijo de red **unicast global**.

• **2001:0:9d38:6ab8:1863:3bca:3f57:fef4/128**: es la **dirección IPv6 unicast global** de la PC local.

• **fe80::/64**: es la **dirección de la ruta de red de enlace local** y representa a todas las PC en la red IPv6 de enlace local.

• **fe80::1863:3bca:3f57:fef4/128**: es la dirección **IPv6 link-local** de la PC local.

**• ff00::/8:** son direcciones **multicast** de clase D especiales y reservadas que equivalen a las direcciones IPv4 224.x.x.x.

**La tabla de enrutamiento del host para IPv6 contiene información similar a la de la tabla de enrutamiento IPv4. ¿Cuál es la ruta predeterminada local para IPv4 y para IPv6?**

Para IPv4, la ruta predeterminada local es 0.0.0.0 0.0.0.0 (quad zero) y, para IPv6, ::/0.

**¿Cuál es la dirección de loopback y la máscara de subred para IPv4? ¿Cuál es la dirección IP de loopback para IPv6?**

Para IPv4, 127.0.0.1 0.0.0.0 0.0.0.0, y para IPv6, ::1/128.

**¿Cuántas direcciones IPv6 se asignaron a esta PC?**

Hay dos direcciones IP. La dirección link-local y la dirección unicast global.

**¿Cuántas direcciones de broadcast tiene la tabla de enrutamiento IPv6?**

Ninguna. IPv6 no utiliza direcciones de broadcast.

**Reflexión**

**1. ¿Cómo es el número de bits para la red que se indica para IPv4? ¿Y cómo es para IPv6?**

IPv4 utiliza una máscara de subred decimal punteada de 32 bits con la forma a.b.c.d. IPv6 utiliza un número con barra.

**2. ¿Por qué hay información tanto de IPv4 como de IPv6 en las tablas de enrutamiento de host?**

En la actualidad, las PC ejecutan ambos protocolos, y los ISP suelen asignar direcciones IPv4 e IPv6 para admitir el acceso a los servidores en Internet que ejecutan cualquiera de los dos protocolos.

Examen Septiembre 2016

- ¿Es bueno el sistema NR?

Si, ya que nos permite diferenciar cada bit en una secuencia larga de 1s o 0s

- ¿De qué formas podemos monitorizar un puerto?

Accediendo a el conectándonos a un hub, ya que este inunda todos los puertos

Habilitando un puerto de monitoreo en un switch

Mediante un ataque de MAC en el que el swtich abra todos los puertos por fallos de seguridad

- Un PC descarta un paquete con la ruta 192…. ¿por qué lo hace y explicalo matemáticamente?

Esto se debe a que el router ya tiene una ruta por defecto (0.0.0.0) utilizada para llegar a destinos que no son resueltos por las demás rutas de la tabla de enrutamiento (generalmente los routers la usan para el trafico que se dirige a internet)

Matematicamente:

1.- El router obtiene la dirección destino del paquete

2.- El router lee la primera ruta de la tabla de enrutamiento

3.- El router realiza la operación Dirección destino AND Máscara de la ruta

4.- Al ser la ruta de defecto 0.0.0.0, el destino enmascarado no coincide con la dirección red de la ruta, descartando finalmente el paquete.

- Un pc solicita un GET y mira tu tabla ARP y está vacía. ¿Debe solicitar una solicitud ARP?

(El protocolo ARP se encarga de descubrir la dirección MAC de un dispositivo sabiendo su dirección IP. Cada dispositivo tiene una tabla ARP donde guarda las equivalencias (arp –a para verla)

Si debe solicitar una solicitud ARP con la MAC de origen de nuestro pc, la MAC destino no la sabemos aún y la IP destino será una consulta (ARP-Request) a todos los equipos de la red/subred hasta que el equipo con esa IP envíe una respuesta con su MAC.

- Un servidor tiene karma.es, etc…

Tipo de registro:

Contenido del registro:

…

- PAT

Ip privada:

Puerto:

Ip pública:

Puerto Público: