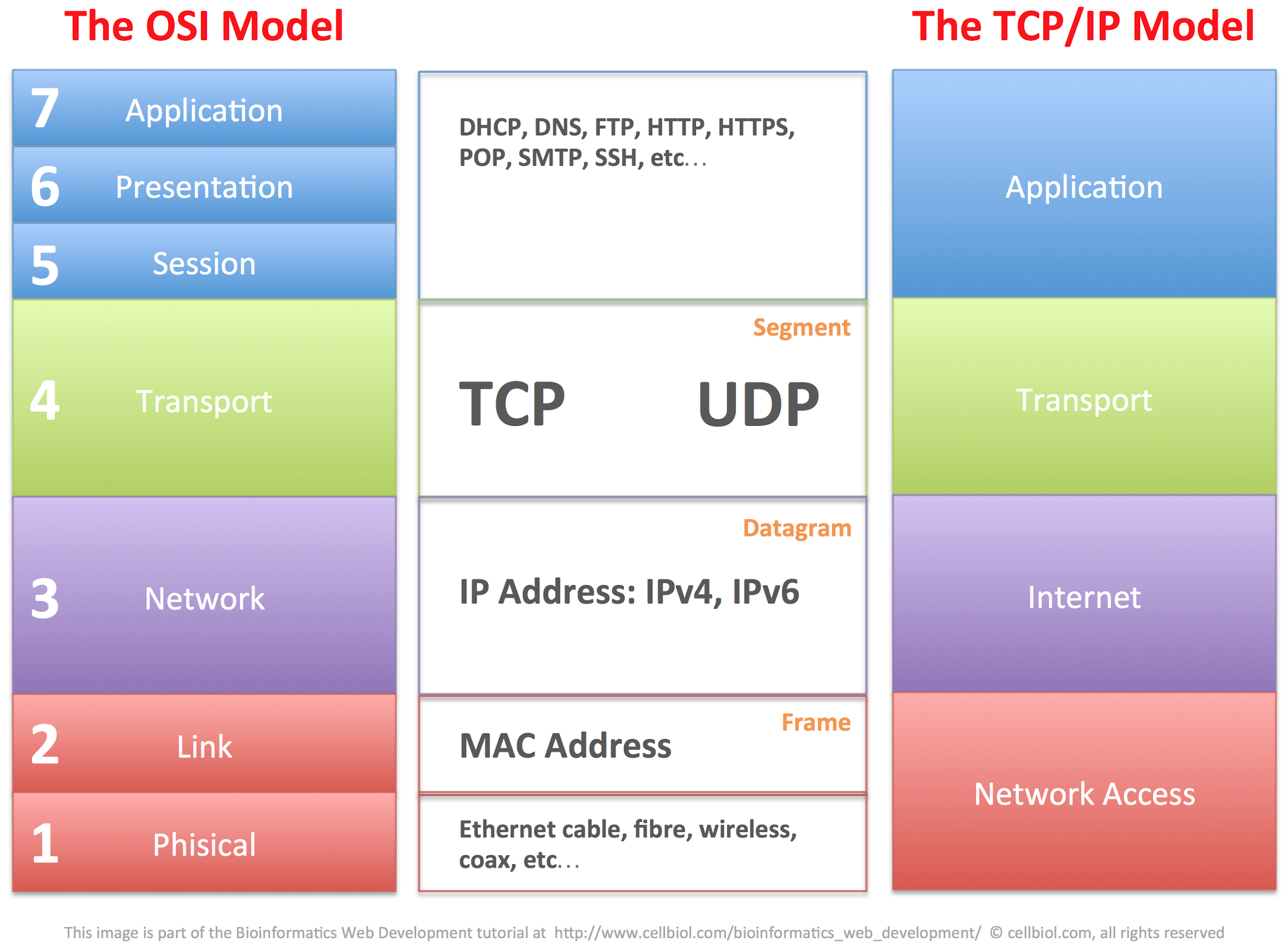
1. Dibuja los modelos OSI y TCP/IP e indica mediante colores la equivalencia de los niveles de ambos modelos.



2. Indica los puertos y protocolos de capa de transporte que usan los siguientes protocolos: HTTP, HTTPS, DNS, SSH

|  |  |  |
| --- | --- | --- |
| **HTTP** | **80** | **TCP** |
| **HTTPS** | **443** | **TCP** |
| **DNS** | **53** | **TCP / UDP** |
| **SSH** | **22** | **TCP** |

3. Explica y razona cómo realiza la retransmisión de los paquetes el protocolo UDP, cuando no se ha recibido un ACK pasados “5 tics”

**El protocolo de datagramas de usuario es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera**.

**Si no se recibe el ACK, es que no ha recibido ningún cliente dicho paquete pero al ser un paquete UDP, no hay límite de “tics” como se plantea en esta pregunta, ya que un Streaming por ejemplo no va a pararse por no haber nadie al otro lado, si no que seguirá retransmitiendo hasta que el cliente lo pare.**

4. ¿Qué máscara de red (la más ajustada) debería usar si quiero disponer de, al menos, 63 máquinas conectadas a la red?

**255.255.255.128 = 11111111.11111111.11111111.10000000 = 25**

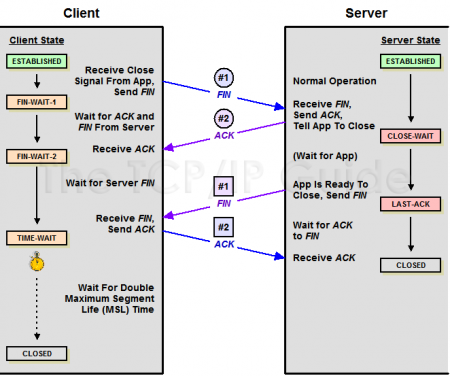
**192.168.0.2 - 192.168.0.65**

**De esta forma entran 126 hosts.**

5. Explica detalladamente (y dibuja) como se establece una conexión TCP.

**Primero el cliente recibe la señal de cerrado desde la aplicación y envía FIN al Server. Después el Server, tras recibir el SYN, envía un ACK que dice a la aplicación que se va a cerrar.**

**Una vez el cliente recibe el ACK, espera a que termine la aplicacion del cliente. El cliente espera que el Server envie un FIN. Cuando el Server tiene la aplicación lista para cerrar envía SYN. El cliente recibe SIN y envía ACK. Finalmente el Server recibe el ACK.**



6. Representa la IP 192.168.1.23 con máscara 255.255.192.0 en notación CIDR

|  |  |  |
| --- | --- | --- |
| **Address** | **192.168.1.23** | **11000000.10101000.00 000001.00010111** |
| **Netmask** | **255.255.192.0 = 18** | **11111111.11111111.11 000000.00000000** |
| **Wildcard** | **0.0.63.255** | **00000000.00000000.00 111111.11111111** |
| **Network** | **192.168.0.0/18** | **11000000.10101000.00 000000.00000000** |
| **HostMin** | **192.168.0.1** | **11000000.10101000.00 000000.00000001** |
| **HostMax** | **192.168.63.254** | **11000000.10101000.00 111111.11111110** |
| **Broadcast** | **192.168.63.255** | **11000000.10101000.00 111111.11111111** |
| **Hosts/Net** | **16382** |  |

7. Define, con tus propias palabras, los siguientes conceptos:

a. Switch

**Dispositivo para interconectar más dispositivos en una red**

b. Router

**Dispositivo que enruta los datos de la red. Está situado en la tercera capa OSI.**

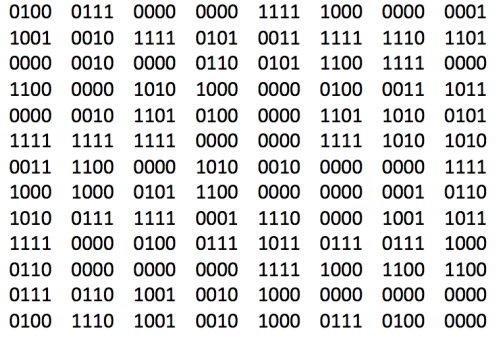
c. Firewall

**Es un programa que es capaz de bloquear puertos del equipo, darles permiso, etc. (controla el tráfico y sus puertos)**

d. NAT

**(Network Address Translation) Es un sistema de comunicación entre diferentes redes. De esta forma se simula estar en la misma red local.**

8. Dado el siguiente paquete IP (paquete teórico), indica cual es que direcciones IP y puertos se están comunicando, así como el protocolo de capa 7 que se seguramente se esté empleando. Además, indica cuantos “saltos” dará el paquete antes de descartarse.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4 Bits | 4 Bits | 8 Bits | 3 Bits | 13 Bits |
| Versión  **0100**  **(4 - IPv4)** | Tamaño Cabecera  **0111**  **(7)** | Tipo Servicio  **0000 0000**  **(0)** | Longitud Total  **1111 1000 0000 0001**  **(63489)** | |
| Identificador  **1001 0010 1111 0101**  **(37621)** | | | Flags  **001**  **(1)** | Posición de Fragmento  **1 1111 1110 1101**  **(8173)** |
| Time To Live (TTL)  **0000 0010**  **(2)** | | Protocolo  **0000 0110**  **(6)** | Suma de Control de Cabecera  **0101 1100 1111 0000**  **(23792)** | |
| Dirección IP Origen  **1100 0000 1010 1000 0000 0100 0011 1011**  **(192.168.4.59)** | | | | |
| Dirección IP Destino  **0000 0010 1101 0100 0000 1101 1010 0101**  **(2.212.13.165)** | | | | |

**(Protocolo 6 => Encabezado TCP)**

|  |  |  |  |
| --- | --- | --- | --- |
| 8 Bits | 8 Bits | 8 Bits | 8 Bits |
| Puerto Origen  **1111 1111 1111 0000**  **(65520)** | | Puerto Destino  **0000 1111 1010 1010**  **(4010)** | |
| Número de Secuencia  **0011 1100 0000 1010 0010 0000 0000 1111**  **(1007296527)** | | | |
| Número de Acuse de Recibo  **1000 1000 0101 1100 0000 0000 0001 0110**  **(2287730710)** | | | |
| Longitud del encabezado  **1010 0111**  **(167)** | Reservado  **1111 0001**  **(241)** | Bits de Control  **1110 0000**  **(224)** | Ventana  **1001 1011**  **(155)** |
| Checksum  **1111 0000 0100 0111**  **(61511)** | | Urgente  **1011 0111 0111 1000**  **(46968)** | |
| Opciones  **0110 0000 0000 0000 1111 1000 1100 1100**  **(1610676428)** | | | |
| Datos de la capa de aplicación  **01110110100100101000000000000000**  **(1989312512)** | | | |

9. Dada la red 192.160.0.0/11, indica y razona:

a. La máscara de red

La máscara de red es 11, por lo que será **11111111.11100000.00000000.0000000**

**(255.224.0.0)**

b. El número de host disponibles **(2097150)**

c. La dirección de broadcast **(192.191.255.255)**

d. Calcula si 192.191.13.80 y 192.168.90.45 están en la misma red

**Si, estarán en la misma red**

**11000000.10111111.00001101.01010000 = 192.191.13.80**

**11000000.10101000.01011010.00101101 = 192.168.90.45**

|  |  |  |
| --- | --- | --- |
| **Address** | **192.168.0.0** | **11000000.10100000.00000000.00000000** |
| **Netmask** | **255.224.0.0 = 11** | **11111111.11100000.000 000000.00000000** |
| **Wildcard** | **0.31.255.255** | **00000000.00011111.11 111111.11111111** |
| **Network** | **192.168.0.0/11** | **11000000.10100000.00000000.00000000** |
| **HostMin** | **192.168.0.1** | **11000000.10100000.00000000.00000001** |
| **HostMax** | **192.192.255.254** | **11000000.11000000.11111111.11111110** |
| **Broadcast** | **192.191.255.255** | **11000000.10111111.11111111.11111111** |
| **Hosts/Net** | **2097150** |  |

10. Enumera y explica detalladamente (con tus propias palabras) todos los ataques de red que conoces, tanto para IPv4 como para IPv6

**MITM**

Man In the Middle, o también conocido como Hombre en Medio, es un ataque en red que se apodera de la información que fluye por dicha red desde los dispositivos conectados a internet. De ésta manera un atacante tiene el control sobre la red.

**ARP - Spoofing:**

Se basa en un ataque de sniffing. Con este ataque haremos que todo el tráfico que vaya del Wifi conectado a Internet, pasará por el atacante antes donde se pueden recuperar formularios con datos, editar el DOM del HTML, inyectar JavaScript en cualquier navegador, suplantar imágenes, robo de sesiones…

**DNS Spoofing:**

Dentro de un MITM, pueden hacer este tipo de ataque para confundir a nuestro equipo y darnos una web que realmente ha sido suplantada por otra. ¿Como se hace? Ésta técnica infecta el DNS de la red para hacer creer a los equipos conectados que la dirección [www.google.com](http://www.google.com) es realmente Google y no un Scam de Phising.

**DDoS**

También conocido como Deny of Service, es un ataque a base de peticiones de forma masiva contra una sola máquina. De ésta forma, haremos que el sistema atacado colapse de peticiones. Con esto conseguimos que dicho sistema se quede colgado o que se apague. Normalmente, para hacer un ataque DDoS, suele usarse alguna Botnet donde hayan muchas máquinas infectadas (zombies) para ser ellos quienes hagan dicho ataque desde muchas partes del mundo.

**SSLStrip**

SSLStrip es un módulo que se ha creado para saltarnos los certificados de seguridad HTTPS sin que una víctima se de cuenta en una misma red, por ejemplo. De ésta forma, la persona atacada intentará entrar a facebook.com y le redirigirá a HTTP en vez de al seguro, haciendo que el formulario de login (por ejemplo) sea transparente en red y el atacante pueda interceptar dichas credenciales.