HOJA DE TRUCOS

1. MÁSCARAS DE RED

CIDR	Máscara	Número de IPs
/30	255.255.255.252	4
/29	255.255.255.248	8
/28	255.255.255.240	16
/27	255.255.255.224	32
/26	255.255.255.192	64
/25	255.255.255.128	128
/24	255.255.255.0	256
/23	255.255.254.0	512
/22	255.255.252.0	1024
/21	255.255.248.0	2048
/20	255.255.240.0	4096

Direcciones IP de Clase C

- Para direcciones IP de Clase C, los primeros tres octetos (24 bits / 3 bytes) representan el ID de red, y el último octeto (8 bits / 1 bytes) es el ID de host.
- Las direcciones IP de Clase C van desde 192.0.0.0 hasta 223.255.255.255, con una máscara predeterminada 255.255.255.0 (o /24 en CIDR).
- La Clase C se traduce a 2,097,152 (221) redes y 254 (28-2) direcciones utilizables por red.

Direcciones IP de Clase D y Clase E

- Las últimas dos clases son la Clase D y la Clase E.
- Las direcciones IP de Clase D están reservadas para multidifusiones. Ellas ocupan el rango desde 224.0.0.0 hasta 239.255.255.255.
- Las direcciones IP de Clase E son experimentales, y son cualquiera arriba de 240.0.0.0

2. TABLA DE RUTAS

Dirección Base	Máscara	Siguiente Salto
192.168.45.0	255.255.255.128	--
192.168.45.128	255.255.255.240	192.168.45.161

3. FÓRMULAS DE SHANNON

3.1. FORMULA ORIGINAL

$$C = B * log2\,(1 + SNR)$$

3.2. DESPEJE DE B (ANCHO DE BANDA)

$$B = \frac{C}{log2(1 + SNR)}$$

3.3. DESPEJE DE SNR (RELACIÓN SEÑAL/RUIDO)

$$SNR = 2^{\frac{C}{B}} - 1$$

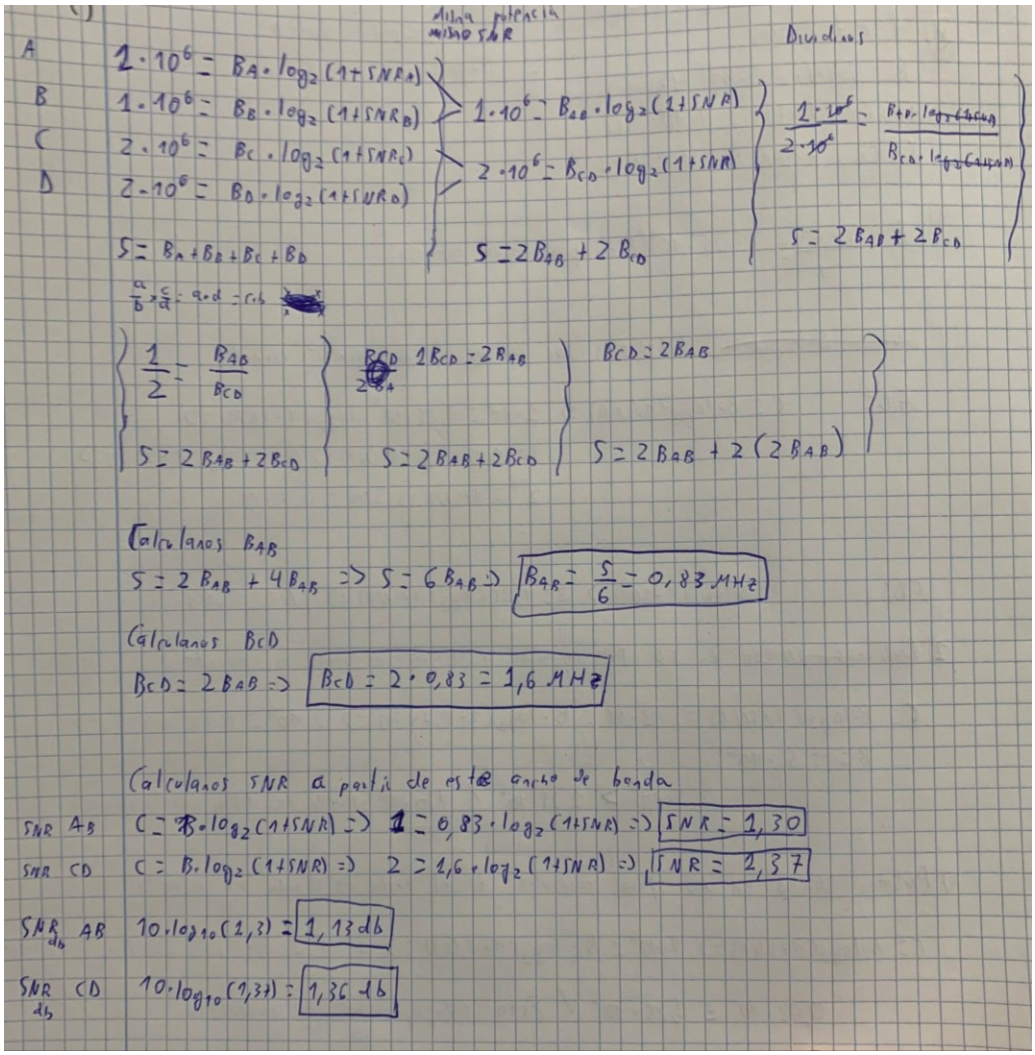
3.4. DESPEJE DE SNR (DECIBELIOS)

$$SNRdb = 10 * log10\,(SNR - 1)$$

3.5. DESPEJE PARA SNR SOBRE SNRdb

$$SNR = \ 10^{\frac{SNRdb}{10}}$$

Un ejemplo de como hacer el repato óptimo sería:



4. TABLAS DE MENSAJES

4.1 WIFI:

RTS – CTS – Mensaje – ACK

Correcto para redes Wi-Fi con control de acceso opcional RTS/CTS (Request to Send / Clear to Send), que se utiliza para evitar colisiones en redes con mucho tráfico o grandes distancias.

Flujo típico:

- RTS: El emisor solicita permiso para enviar.
- CTS: El receptor concede permiso.
- Mensaje: El emisor envía los datos.
- ACK: El receptor confirma la recepción de los datos (a nivel de enlace, obligatorio en 802.11).

4.2 Ethernet:

ARP Request – ARP Reply – Mensaje

Correcto para escenarios en los que la dirección MAC del destino no está en la tabla ARP del emisor.

Flujo típico:

- ARP Request: Si el emisor no conoce la MAC asociada a una IP, hace una solicitud ARP por broadcast.
- ARP Reply: El dispositivo con esa IP responde directamente con su dirección MAC.
- Mensaje: Una vez resuelta la dirección, se envían los datos.

4.3 TCP:

SYN – SYN-ACK – ACK

TCP requiere un handshake de tres vías para establecer una conexión fiable antes de transmitir datos:

Apertura:

- SYN (Synchronize): El cliente envía un paquete SYN al servidor para solicitar la conexión.
- SYN-ACK: El servidor responde con un paquete SYN-ACK indicando que acepta la conexión.
- ACK (Acknowledgment): El cliente envía un paquete ACK para confirmar la conexión.

Cierre:

- FIN: El nodo que desea cerrar la conexión (cliente o servidor) envía un paquete FIN.
- ACK: El receptor del FIN responde con un ACK para confirmar que ha recibido el FIN.
- FIN: El receptor envía su propio paquete FIN cuando esté listo para cerrar la conexión.
- ACK: El primer nodo responde con un ACK para confirmar el cierre.

4.4 DNS:

Consulta – Respuesta

El DNS (Domain Name System) traduce nombres de dominio legibles para humanos en direcciones IP numéricas utilizadas por los dispositivos.

Flujo típico:

- Consulta DNS: El cliente envía una solicitud a un servidor DNS para resolver un nombre de dominio (por ejemplo, www.ejemplo.com).
- Respuesta DNS: El servidor DNS responde con la dirección IP correspondiente al nombre de dominio solicitado.

4.5 DHCP:

Discover – Offer – Request – Acknowledgement (DORA)

El DHCP (Dynamic Host Configuration Protocol) asigna dinámicamente direcciones IP y otros parámetros de configuración a los dispositivos en una red.

Flujo típico:

- DHCP Discover: El cliente envía una solicitud broadcast buscando servidores DHCP disponibles.
- DHCP Offer: Los servidores DHCP responden ofreciendo una dirección IP y configuración de red.
- DHCP Request: El cliente acepta una de las ofertas y solicita esa configuración específica al servidor.
- DHCP Acknowledgement (ACK): El servidor confirma y asigna la dirección IP al cliente.

4.6 ICMP (Internet Control Message Protocol):

Echo Request – Echo Reply

ICMP no establece conexiones; simplemente envía mensajes como ping (Echo Request y Echo Reply).

Los mensajes terminan cuando se recibe una respuesta o expira el tiempo.

4.7 EJEMPLOS

PC1 – ROUTER 1 – ROUTER 2- PC2 (todo por ethernet)

Mensaje TCP de PC1 a PC2

Tabla 2: Mensajes a nivel de transporte (Capa 4)

Paso	Emisor	Receptor	Mensaje	Descripción
1	PC1	PC2	**TCP SYN**	**PC1** inicia una conexión TCP enviando un segmento SYN a **PC2**.
2	PC2	PC1	**TCP SYN-ACK**	**PC2** responde con un segmento SYN-ACK para aceptar la conexión.
3	PC1	PC2	**TCP ACK**	**PC1** confirma con un segmento ACK, completando el handshake de tres vías.
4	PC1	PC2	**Datos TCP**	**PC1** envía los datos a **PC2** a través de segmentos TCP.
5	PC2	PC1	**TCP ACK**	**PC2** envía ACKs para confirmar la recepción de los datos.
6	PC1	PC2	**TCP FIN**	**PC1** inicia el cierre de la conexión enviando un segmento FIN.
7	PC2	PC1	**TCP FIN-ACK**	**PC2** responde con FIN-ACK para cerrar la conexión.
8	PC1	PC2	**TCP ACK**	**PC1** envía un ACK final, confirmando el cierre de la conexión.

Notas:

- Los mensajes a nivel de transporte son intercambiados **directamente entre PC1 y PC2**, sin intervención de los routers en este nivel.
- Los routers solo encaminan los paquetes basándose en la información de la capa de red (direcciones IP).
- El handshake de tres vías (pasos 1-3) establece una conexión confiable antes de la transferencia de datos.
- El proceso de cierre de conexión (pasos 6-8) asegura que ambos extremos acuerden finalizar la comunicación.

Tabla 1: Mensajes a nivel de enlace (Capa 2)

Paso	Emisor	Receptor	Mensaje	Descripción
1	PC1	Broadcast	**ARP Request**	**PC1** envía una solicitud ARP en broadcast para averiguar la dirección MAC del **Router1** (puerta de enlace predeterminada).
2	Router1	PC1	**ARP Reply**	**Router1** responde con su dirección MAC a **PC1**.
3	PC1	Router 1	**Trama Ethernet**	**PC1** envía una trama Ethernet a **Router1** con el paquete IP que contiene el segmento TCP.
4	Router1	Broadcast	**ARP Request** (si necesario)	**Router1** puede enviar una solicitud ARP para obtener la dirección MAC de **Router2** si no la tiene en caché.
5	Router2	Router 1	**ARP Reply**	**Router2** responde con su dirección MAC a **Router1**.
6	Router1	Router 2	**Trama Ethernet**	**Router1** reenvía la trama Ethernet a **Router2** con el paquete IP dirigido a **PC2**.
7	Router2	Broadcast	**ARP Request** (si necesario)	**Router2** envía una solicitud ARP para obtener la dirección MAC de **PC2**.
8	PC2	Router 2	**ARP Reply**	**PC2** responde con su dirección MAC a **Router2**.
9	Router2	PC2	**Trama Ethernet**	**Router2** entrega la trama Ethernet a **PC2** con el paquete IP y el segmento TCP original.

Notas:

- Los pasos de ARP (1-2, 4-5, 7-8) ocurren solo si la dirección MAC no está en la tabla ARP de cada dispositivo.
- A nivel de enlace, las tramas Ethernet se envían entre dispositivos adyacentes (nodo a nodo).
- Cada router desempaqueta la trama Ethernet, consulta la tabla de enrutamiento y vuelve a encapsular el paquete IP en una nueva trama Ethernet para el siguiente salto.

Mensaje DNS por TCP

Tabla 1: Mensajes a nivel de enlace (Capa 2)

Paso	Emisor	Receptor	Mensaje	Descripción
1	PC1	Broadcast	**ARP Request**	**PC1** envía una solicitud ARP en broadcast para averiguar la dirección MAC de **Router1** (puerta de enlace predeterminada).
2	Router1	PC1	**ARP Reply**	**Router1** responde con su dirección MAC a **PC1**.
3	PC1	Router 1	**Trama Ethernet**	**PC1** envía una trama Ethernet a **Router1** con el paquete IP que contiene el segmento TCP y el mensaje DNS.
4	Router1	Broadcast	**ARP Request** (si necesario)	**Router1** envía una solicitud ARP para obtener la dirección MAC de **Router2** si no la tiene en caché.
5	Router2	Router 1	**ARP Reply**	**Router2** responde con su dirección MAC a **Router1**.
6	Router1	Router 2	**Trama Ethernet**	**Router1** reenvía la trama Ethernet a **Router2** con el paquete IP dirigido a **PC2**.
7	Router2	Broadcast	**ARP Request** (si necesario)	**Router2** envía una solicitud ARP para obtener la dirección MAC de **PC2**.
8	PC2	Router 2	**ARP Reply**	**PC2** responde con su dirección MAC a **Router2**.
9	Router2	PC2	**Trama Ethernet**	**Router2** entrega la trama Ethernet a **PC2** con el paquete IP y el segmento TCP que contiene el mensaje DNS.

Notas:

- Los pasos de ARP ocurren solo si la dirección MAC no está en la tabla ARP de cada dispositivo.
- A nivel de enlace, las tramas Ethernet se envían entre dispositivos adyacentes (nodo a nodo).
- Cada router desencapsula y reencapsula el paquete IP en una nueva trama Ethernet para el siguiente salto.

Tabla 2: Mensajes a nivel de transporte (Capa 4)

Paso	Emisor	Receptor	Mensaje	Descripción
1	PC1	PC2	**TCP SYN**	**PC1** inicia una conexión TCP con **PC2** para enviar la consulta DNS.
2	PC2	PC1	**TCP SYN-ACK**	**PC2** responde aceptando la conexión TCP.
3	PC1	PC2	**TCP ACK**	**PC1** confirma la conexión TCP establecida.
4	PC1	PC2	**Consulta DNS**	**PC1** envía la consulta DNS a **PC2** a través de la conexión TCP.
5	PC2	PC1	**Respuesta DNS**	**PC2** responde con la información solicitada en la consulta DNS.
6	PC1	PC2	**TCP FIN**	**PC1** inicia el cierre de la conexión TCP.
7	PC2	PC1	**TCP FIN-ACK**	**PC2** confirma el cierre de la conexión TCP.
8	PC1	PC2	**TCP ACK**	**PC1** finaliza la conexión TCP.

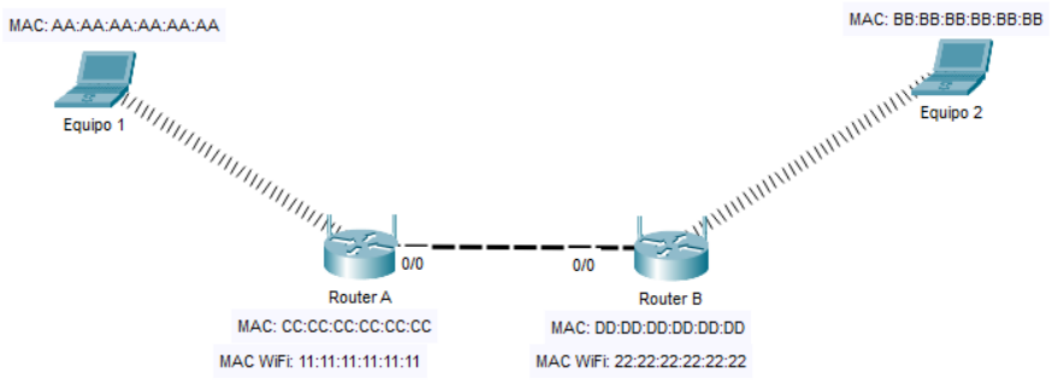
Notas:

- **DNS sobre TCP** se utiliza cuando las respuestas son demasiado grandes para UDP o para tareas como la transferencia de zonas (AXFR).
- El establecimiento y cierre de la conexión TCP garantiza una comunicación confiable entre **PC1** y **PC2**.
- Los routers intermedios no intervienen en el nivel de transporte; solo encaminan los paquetes basándose en las direcciones IP.

Ejercicio 3 (3 puntos)

Se tiene una red como la de la figura, en la que los Equipos 1 y 2 son portátiles conectados mediante WiFi a los Router A y B, que tienen una conexión cableada entre ellos.

Si se asume que un administrador ha configurado de forma estática las IPs de los dos *routers* y del Equipo 1, mientras que el Equipo 2 ha obtenido la suya del Router B mediante DHCP. Tras esto, el Equipo 1 envía un ping al Equipo 2 y este le responde. **Describe el proceso de mensajes intercambiados** (asume como punto de inicio del envío del mensaje el instante después de que el Equipo 2 recibe su IP mediante DHCP), explicando por qué se genera cada mensaje a nivel de enlace y **completa una tabla** especificando las MACs de origen y destino de cada mensaje, además del tipo de información enviada.



G

Se abreviará ICMP Echo Request (ping) como “ping” y ICMP Echo Reply (pong) como “pong”.

No hacemos ARP en wifi, suponemos que equipo1 y router A ya se conocen. Muy largo si no.

Origen	Destino	Mensaje
E1	R1	RTS
R1	E1	CTS
E1	R1	Mensaje ping
R1	E1	ACK
R1	BROADCAST	ARP Request
R2	R1	ARP Reply
R1	R2	Mensaje ping
R2	E2	RTS
E2	R2	CTS
R2	E2	Mensaje ping
E2	R2	ACK
E2	R2	RTS
R2	E2	CTS
E2	R2	Mensaje pong
R2	E2	ACK
R2	R1	Mensaje pong
R1	E1	RTS
E1	R1	CTS
R1	E1	Mensaje pong
E1	R1	ACK

A nivel de Trasnporte si es TCP

Origen	Destino	Mensaje
E1	E2	TCP SYN
E2	E1	TCP SYN-ACK
E1	E2	TCP ACK
E1	E2	Mensaje ping
E2	E1	ACK
E2	E1	Mensaje pong
E1	E2	ACK
E1	E2	TCP FIN
E2	E1	TCP FIN-ACK
E1	E2	TCP ACK

5. EJEMPLO MENSAJE INVERSO:

```
Router#ping 150.20.30.55

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.20.30.55

Reply to request 0 from 150.20.30.52, 0 ms
Reply to request 0 from 150.20.30.53, 0 ms
Reply to request 0 from 150.20.30.49, 0 ms
Reply to request 0 from 150.20.30.51, 0 ms
Reply to request 0 from 150.20.30.50, 0 ms
```

Figura 1: Respuesta en consola a un ping realizado en el Router A por la interfaz 0

```
Router#ping 150.20.30.95

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.20.30.95

Reply to request 0 from 150.20.30.90, 0 ms
Reply to request 0 from 150.20.30.80, 0 ms
```

Figura 2: Respuesta en consola a un ping realizado en el Router A por la interfaz 1

```
Router#ping 150.20.30.95

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.20.30.95,

Reply to request 0 from 150.20.30.70, 0 ms
Reply to request 0 from 150.20.30.90, 0 ms
```

Figura 3: Respuesta en consola a un ping realizado en el Router B por la interfaz 0

Layer 3: IP Header Src. IP: 150.20.30.34, Dest. IP: 150.20.30.31 ICMP Message Type: 0
Layer 2: Ethernet II Header 00D0.BCDE.EE09 >> 0030.A3B5.A402
Layer 1: Port GigabitEthernet0/1

Figura 4: Datos capturados en el Router B por la interfaz 1. Contienen la respuesta a un ping enviado por el Router B por la interfaz 1.