

ICMP

Existen dos tipos de mensajes ICMP : ICMP V4 y ICMP v6

El protocolo ICMP envía los siguientes tipos de mensajes:

- Host Reachability.
- Destination or service reachability.
- Time exceeded.

Host Reachability

LocalHost sends ICMP “Echo” Request al host. → Si el host puede ser alcanzado, el host responde con un “echo” reply.

Destination or service Unreachable

ICMPV4	ICMPV6
0 Net unreachable	0 No route to destination
1 Host unreachable	1 Firewall issue (no es este mensaje tal cual)
2 Protocol Unreachable	2 Beyond Scope of source address.
3 Port Unreachable	3. Address Unreachable
	4. Port Unreachable

.

Time Exceeded

El TTL ha expirado. En ICMPv4 se llama TTL y en ICMPv6 se llama Hop Limit

ICMPv6 Messages

Dynamic Address Allocation:

Router Solicitation → RS

Router Advertisement → RA

Neighbor Messages (Para detección de direcciones duplicadas).

Neighbor Solicitation → NS

Neighbor Advertisement → NA

Router Solicitation → RA

Lo envían los routers con IPv6 NIC activada.

Envían cada 200 segundos la siguiente información.

- Prefijo
- Prefix Length

- DNS Add
- Domain Name

****NOTA**** → Si el dispositivo ha sido configurado mediante SLAAC configura su gateway como la dirección **Link-Local** router.

RS → El dispositivo solicita un router → El router le responde con un mensaje RA

Neighbor Solicitation → NS(Dynamic Address Detection)

Un dispositivo envía un mensaje NS con una dirección Link-Local-Unicast.

Si otro dispositivo la tiene responde con la misma dirección y su dirección MAC.

Neighbor Advertisement → NA

La respuesta del NS

Módulo 14 Capa de Transporte

La capa de transporte se encarga de gestionar el envío y recepción de la transmisión de datos entre aplicaciones de origen y destino.

Funciones de la capa de transporte:

- Segmentación de datos
- Seguimiento de conversaciones individuales

Socket: IP y número de puerto.

Doble socket: IP origen y puerto de destino \ Ip destino número puerto destino → Conver única en internet.

- Identificación de las aplicaciones. Para ello utiliza el número de puerto indicado anteriormente

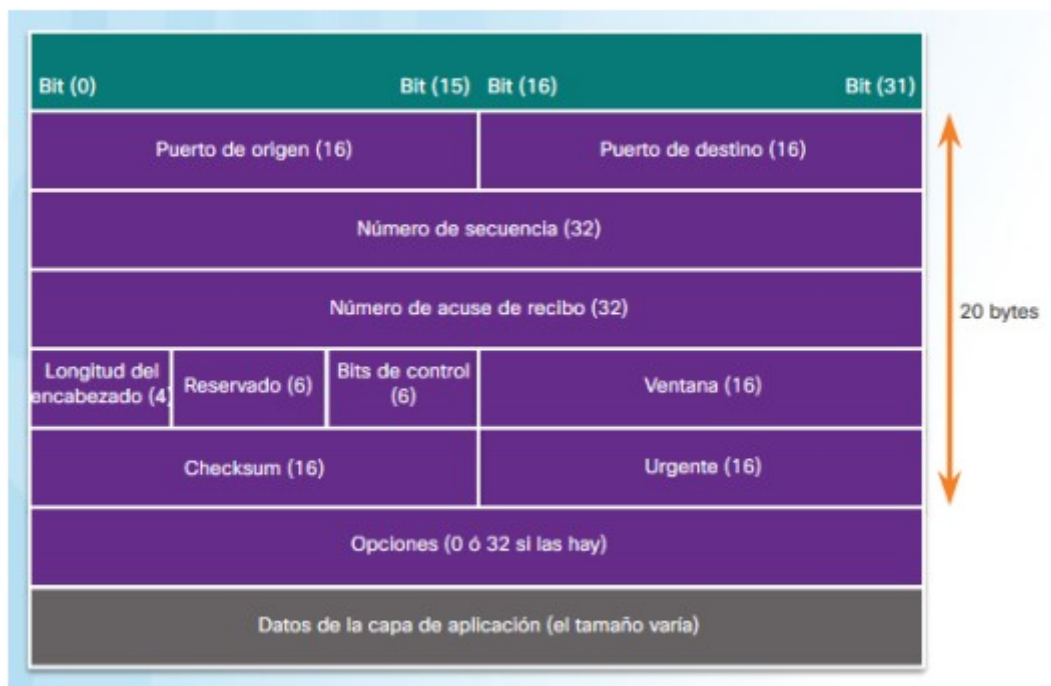
TCP (Protocolo de Control de Transmisión)

Confiable: Acuses de recibo Reenvío de segmento perdidos

Reordenación de segmentos en el destino antes de pasárselos a la aplicación Desventaja: Gran sobrecarga(De procesos y de tráfico. Mayor número de campos para poder controlar la confiabilidad)

Establecimiento de sesión.

Encabezado TCP



UDP(Protocolo de Datagrama de Usuario)

Máximo esfuerzo

No reencia los segmentos perdidos.

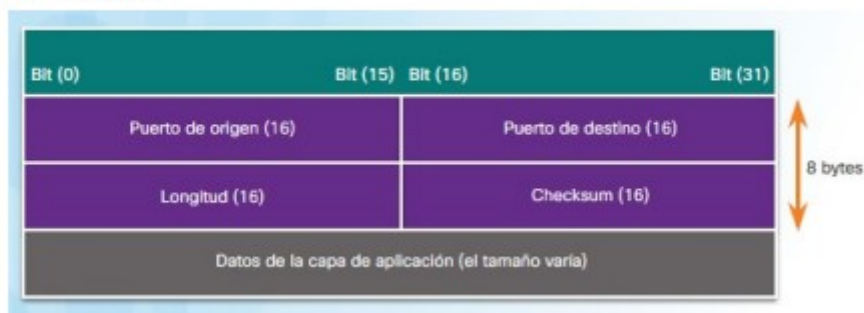
No reordena los datagramas en la llegada.

Ventaja:

No sobrecarga las redes.

No sobrecarga los procesos.

Cabecera UDP:



Cuándo se utiliza TCP vs UDP

UDP

- Mensaje corto

- Pérdida o desorden de **datagramas** no importante
- VOIP o Video Conferencia Online.

TCP

- HTTP /HTTPS
- Database Transaction
- Email (SMTP/IMAP/POP3)

PUERTO

- Número de puerto de origen
- número de puerto de destino(corresponde a la aplicación de destino).

Multiplexación

Consiste en intercalar(en el tiempo) por el medio físico(cable, fibra, ...) segmentos de distintas aplicaciones/usuarios/dispositivos. De este modo nadie acapara el medio y todos perciben que el ancho de banda esté dedicado a él.

Número de secuencia: TCP numera cada segmento con un número llamado **Número de secuencia** para poder reconstruir el mensaje original en el destino(cada segmento en su posición/orden correcto). El número de secuencia de cada segmento es la posición que le corresponde al primer byte de cada segmento empezando en 1(también se le llama **desplazamiento del segmento** por que indica la distancia desde el origen del mensaje).

Ejemplo:

Tamaño	Número de secuencia
1º segmento 168 bytes	1 La posición del primer byte del primer segmento es siempre 1
2º segmento 200 bytes	Nº de secuencia 169 (1+168) Nº de secuencia anterior + tamaño del segmento anterior
Tercer segmento de tamaño 102 bytes	Nº de secuencia 369 (169+200) Nº de secuencia anterior + tamaño del segmento anterior

1º segmento	2º segmento	3º segmento
1	169	369

Por seguridad el número del primer byte del primer segmento no es 1 sino un número aleatorio conocido como **número de secuencia inicial(ISN)** (Arriba lo simplificamos para poder explicarlo mejor). Supongamos que en el ejemplo anterior el número aleatorio(ISN) generado es 3000. Entonces quedaría así:

Tamaño	Número de secuencia
1º segmento 168 bytes	3001 La posición del primer byte del primer segmento es siempre 0
2º segmento 200 bytes	Nº de secuencia 3169 (3001+168) Nº de secuencia anterior + tamaño del segmento anterior
Tercer segmento de tamaño 102 bytes	Nº de secuencia 3369 (3169+200) Nº de secuencia anterior + tamaño del segmento anterior

