Module 13 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 unreachable.
- Time exceeded.

Host reachability

Localhost sends a ICMP “Echo” request to the host → If the host can be reached, the host responds with a “echo” repply

Mensajes de error.

ICMPV4	ICMPV6
0 Net unreachable	0 No route to destination
1 Host unreachable	1 Communication with the destination is administratively prohibited (firewall issue)
2 Protocol Unreachable	2 Beyond Scope of source address.
3 Port Unreachable	3. Address Unreachable
	4. Port Unreachable

Time exceeded
En ICMPv4 se llama TTL
En ICMPv6 se llama Hop Limit.

También son utilizados por la herramienta traceroute.

ICMPv6 Messages

Mensajes de un dispositivio con el router.
RS → Router solicitation
RA → Router Advertisement.

Mensajes entre dispositivos: (DAD duplicate address detection)
NS → Neighbor solicitation
NA → Neighbor Advertisement.

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.

  Neighbor Solicitation → NS(Dynamic Address Detection)

  Un dispositivo envía un mensaje NS con una dirección **Unicast o 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. En uno o varios dispositivos.

Las subdivisiones de mensajes se denominan:

Segmentos en TCP y Datagramas en UDP

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)

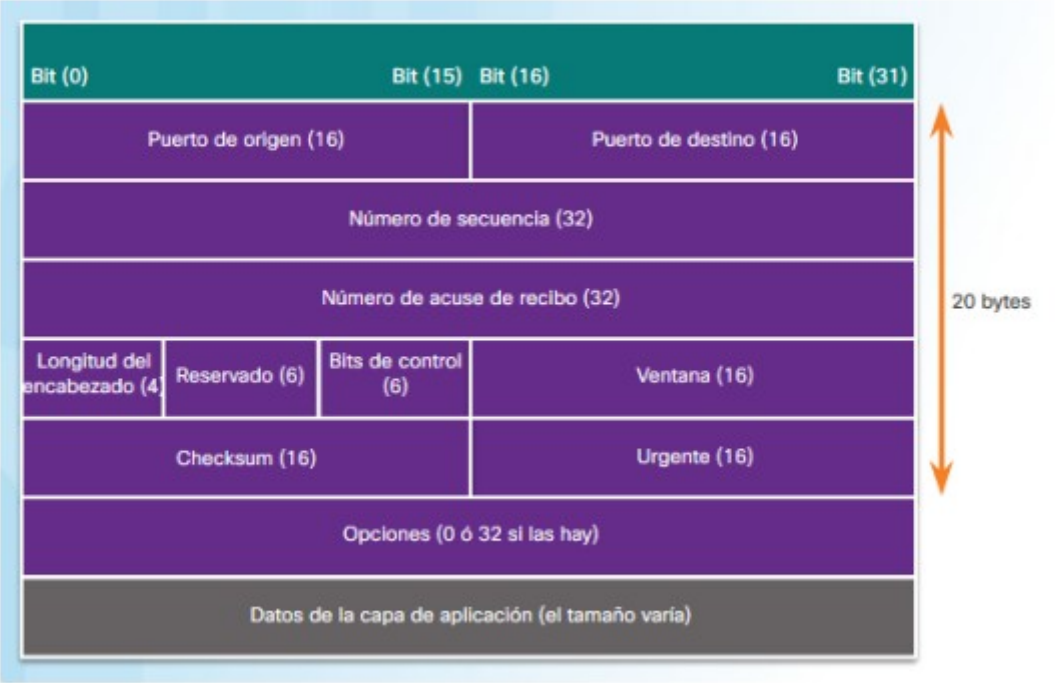
Confiable: Acuses de recibo Reenvío de segmento perdidos

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 reenvía 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 que se puede enviar en un único segmento. (DHCP o DNS)

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

TCP

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

Partes del encabezado TCP/IP

Numero de secuencia →

El número de secuencia del primer segmento es el 1.

Si el primer segmento tiene una longitud de 168 bytes el segundo segmento tendrá un número de secuencia de 169

El número de secuencia inicial se genera de forma aleatoria.

Número de acuse de recibo

Indica el segmento que espera recibir después.

Si tenemos un ACK 370 quiere decir que hemos recibido los anteriores 369 bytes de segmentos.

Flag

SYN → Sincronización (El origen quiere establecer una sesión)

ACK → Indica al destino que el campo (ACKnowledgement Number) contiene un valor en expectativa para indicar los segmentos recibidos.

PUSH →

RESET → Reestablecimiento de sesión en caso de producirse muchos errores o pasa mucho tiempo sin transmitir información.

URG → Si este campo de flag está activo se lee el campo URG pointer de la cabecera que indica cuáles son los bytes urgentes que debería priorizar.

FIN → El origen indica que no quiere retransmitir mas y quiere finalizar la sesión. El destino reenvía un segmento con el ACK flag activado para confirmar el final de la sesión.

Ventana

Con este valor, el protocolo TCP del receptor de los datos, indica al emisor cuantos bytes le puede transmitir seguidos, este último al primero, sin que el primero(el receptor) le acuse recibo de los segmentos que le lleguen.

PUERTO

- Número de puerto de origen

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

Multiplexación

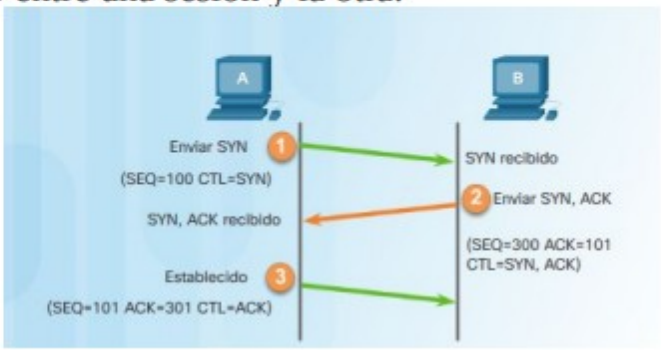
Consiste en intercalar(en el tiempo) por el medio físico(cable, fibra, ...) segmentos de distintas aplicaciones/usuarios/dispositivos. De este modo nadie acapara el medio y todos perciben que el ancho de banda esté dedicado a él.

3 way handshake

bit(flag, marcador, ...) ACK activado para confirmar el final de la sesión.

Establecimiento de sesión de tres vías TCP

Tenga en cuenta que no se establece una sola sesión. Realmente se establecen dos sesiones en tres pasos. Una sesión entre A y B, otra segunda sesión entre B y A. Además los números de secuencia no tienen nada que ver entre una sesión y la otra.



Cuando dos dispositivos se comunican utilizando el protocolo TPC, antes de transmitir datos entre si, inician una sesión. Para ello:

Punto 1: A inicia el establecimiento de sesión. A envía a B un mensaje cuyo segmento lleva activo el marcador SYN y el campo número de secuencia lleva el valor 100(ISN-Número de secuencia inicial generado por A).

Punto 2: B responde a A con un mensaje cuyo segmento lleva activo el marcador ACK y SYN.

- B acusa recibo a A. El ACK va activo para indicarle a A que B recibió el segmento de inicio de sesión(SYN) y que el próximo byte que espera recibir B por parte de A es el que figura en el valor del campo ACKnowledgement Number 101(realmente es el byte 1[101-100]).
- Por otra parte, el bit de SYN está activo porque B indica que quiere iniciar una sesión con A. Por lo tanto el número de secuencia lleva el valor 300 generado por B(es el NSI). No tiene nada que ver con el 100 que A pasó a B).

Punto 3: A responde a B con un acuse de recibo. El mensaje lleva activo el flag ACK para indicarle que está de acuerdo con el inicio de sesión de B con A. El flag ACK también indica que el campo ACKnowledgement Number lleva el valor 301, que es el primer byte que A espera recibir de B en el próximo envío de datos de B hacia A. Además el número de

Finalización de sesión.

Finalización de sesión TCP:

Para cerrar cada una de las sesiones de “una vía” TCP(Recuerde que hay dos sesiones iniciadas, una en cada sentido) se utiliza un enlace de dos vías(Es decir, un mensaje en cada sentido) por cada una de las vías(sesiones), que consta de un segmento FIN y un segmento de reconocimiento (ACK).

Los segmentos 1(activa el marcador FIN para indicar que A quiere finalizar la sesión con B) **y 2**(Activa el marcador ACK para indicar que B esta de acuerdo con finalizar la sesión) **finalizan la sesión de A con B.**

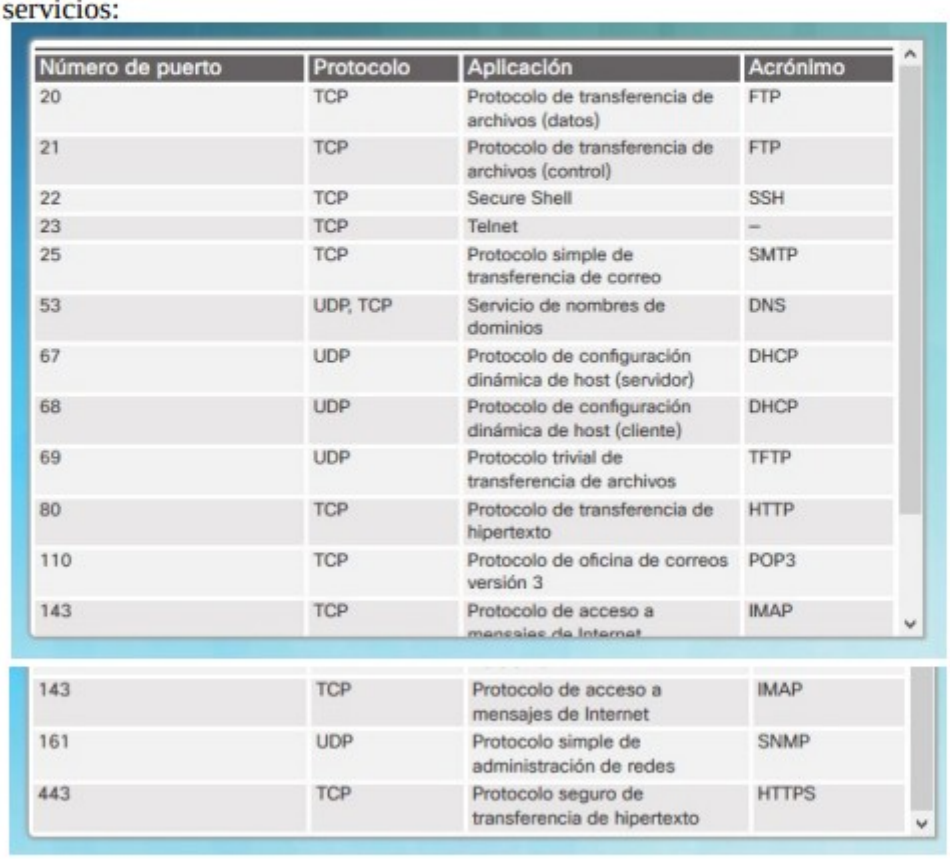
Los segmentos 3 y 4 Finalizan la sesión de B con A.

Puertos

Números de puerto

Rango de números de puerto	Grupo de puertos
Entre 0 y 1023	Puertos bien conocidos
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

1. **Bien conocidos.** Son lo que se conocen como puertos por defectos. Están reservados por la IANA para poner a determinados servicios en los servidores. De este modo los clientes utilizan estos puertos como puertos de destino por defecto para acceder a esos servicios:



Número de puerto	Protocolo	Aplicación	Acrónimo
20	TCP	Protocolo de transferencia de archivos (datos)	FTP
21	TCP	Protocolo de transferencia de archivos (control)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	–
25	TCP	Protocolo simple de transferencia de correo	SMTP
53	UDP, TCP	Servicio de nombres de dominios	DNS
67	UDP	Protocolo de configuración dinámica de host (servidor)	DHCP
68	UDP	Protocolo de configuración dinámica de host (cliente)	DHCP
69	UDP	Protocolo trivial de transferencia de archivos	TFTP
80	TCP	Protocolo de transferencia de hipertexto	HTTP
110	TCP	Protocolo de oficina de correos versión 3	POP3
143	TCP	Protocolo de acceso a mensajes de Internet	IMAP
161	UDP	Protocolo simple de administración de redes	SNMP
443	TCP	Protocolo seguro de transferencia de hipertexto	HTTPS

Por ejemplo, cuando usamos un navegador(Chrome, Firefox, …) para obtener una página Web de un servidor web, podemos especificar el puerto de destino en el cual escucha la aplicación de servidor: "www.google.es:80" . El puerto de destino 80 no se suele especificar cuando accedemos a un servicio web porque el navegador utilizará por si solo el puerto por defecto establecido por la IANA(el 80).

Puertos dinámicos o privados (números 49152 a 65535): también conocidos como puertos efímeros, usualmente el SO del cliente los asigna de forma dinámica cuando se inicia una conexión a un servicio. El puerto dinámico se utiliza para identificar la aplicación cliente durante la comunicación. También se pueden utilizar para este fin los puertos registrados que no estén siendo utilizados en un dispositivo.