Modulo 13 Resumen
ICMP

13.1 Mensajes ICMP

- Mensajes ICMPv4 e ICMPv6 → IP es un protocolo de mayor esfuerzo, TCP/IP se encarga de proporcionar mensajes de error e información. Estos mensajes se envían mediante ICMP, proporcionan respuesta acerca de temas relacionados con el procesamiento de paquetes IP. No son obligatorios y no se permiten dentro de la red por seguridad.

Tipos de mensajes ICMP: Accesibilidad al host, destino o servicio inaccesible y tiempo superado.

- Accesibilidad al host → Se produce un mensaje eco ICMP para probar la accesibilidad de un host. El host envía solicitud de eco ICMP a un host. Si el host está disponible responde el eco. Es la base de ping. Eco solicitud y Eco Respuesta.
- Destino o servicio inaccesible → Cuando un host o gateway recibe un paquete que no puede entregar, puede utilizar un ICMP de destino inalcanzable. El mensaje incluye un código que indica el motivo por el cual no se puede entregar el paquete.

Códigos destino inalcanzables ICMPv4:	Códigos destino inalcanzables ICMPv6:
0: Red inalcanzable	0: No hay ruta para el destino
1: host inalcanzable	1: Comunicación prohibida (firewall)
2: Protocolo inalcazable	2: Más allá del alcance de la dirección origen
3: Puerto inalcanzable	3: No se pudo alcanzar la dirección
	4: Puerto inalcanzable

- Tiempo excedido → Los Router los utilizan para indicar que un paquete no puede reenviarse debido al campo de tiempo de duración (TTL) fue a 0. Descarta el paquete y envía un mensaje de tiempo superado al host de origen. ICMPv6 También envía este mensaje si el router no puede reenviar un IPv6 porque el paquete caducó. También usa el campo Límite de salto IPv6 para determinar si el paquete ha expirado.
- Mensajes ICMPv6 → Los mensajes ICMPv6 están encapsulados en IPv6. ICMPv6 incluye 4 mensajes nuevos como parte del protocolo de detección de vecinos.

Los mensajes router-host, incluida asignación dinámica de direcciones son:
Mensaje de solicitud de router (RS) y Mensaje de anuncio de router (RA)

Los mensajes de dispositivos IPv6, incluida detección de vecinos y resolución de direcciones son:
Mensaje de solicitud de vecino (NS) y Mensaje de anuncio de vecino (NA)

RA → Los Routers con IPv6 envían RA cada 200 segundos para proporcionar direccionamiento. Puede incluir información como prefijo, longitud, DNS y dominio. Un host SLAAC y establece su gateway en la dirección de enlace local del router que envío RA.

RS→ Un router envía un RA en respuesta a un RS. Se puede usar para determinar como recibir dinámicamente su dirección IPv6.

NS→ Para verificar' la unicidad de una dirección, el dispositivo envía un mensaje NS con su IPv6. Si otro dispositivo de la red tiene esta dirección, responde con un mensaje NA. NA notifica al emisor que la dirección está en uso.

NA→ El dispositivo si tiene una IPv6 duplicada se devuelve este tipo de mensaje, que contiene da dirección de MAC Ethernet.

13.2 Pruebas ping y traceroute

- **Ping: prueba de conectividad→** Ping es una utilidad de prueba que utiliza ICMP y mensajes eco para probar conectividad entre hosts. Si se envía un ping se envía un mensaje eco y si se recibe se responde con una respuesta eco. Proporciona el tiempo entre el envío y respuesta del mensaje. Se tiene un tiempo de respuesta, si el tiempo se agota proporciona un mensaje que no se recibió respuesta. Es común que el primer ping se agote si es necesario realizar la resolución de direcciones (ARP o ND). Tipos de pruebas con ping: Ping a loopback local, ping a gateway, ping a host remoto.
- **Hacer ping a loopback →** Se puede usar para probar la configuración interna IPv4 o IPv6. Se envía ping a dirección de bucle de retorno local. 127.0.0.1 ó ::1. Una respuesta indica que IP está instalado correctamente en un host, Proviene de la capa de red. Solo proviene de esa capa por lo que no indica nada del estado de capas inferiores o gateway. Un mensaje de error indica que TCP/IP no funciona en el host.
- **Hacer ping al gateway predeterminado→** Se puede hacer ping para probar la capacidad de un host para comunicarse con la LAN. Un exito indica que el host y la interfaz del router que sirve como gateway están operando correctamente. Si no responde, ping se puede enviar a la IP de otro host en la red local que se sabe este operando. Si el gateway no responde pero el host si puede haber un error con el gateway. Hace ping con mensajes eco.
- **Hacer ping a un host remoto→** Se usa para probar conectividad de un host local para comunicarse en una red remota. Si hay exito se puede verificar el funcionamiento de una amplia porción de redes remotas, indicando la comunicación correcta. Se puede tambien verificar la funcionalidad del módulo remoto de E/S. Si el módulo remoto E/S no hubiera respondido no habría comunicación fuera de la red local.

Traceroute: Prueba el camino → Es el comando tracert es una utilidad que genera una lista de saltos que se alcanzaron con éxito a lo largo de la ruta. Si los datos llegan al destino, el rastreo indica la interfaz de cada router que aparece en la ruta entre los hosts. Si falla el último router que respondió puede indicar dónde se encuentra el problema o restricciones de seguridad.

Tiempo de ida y vuelta (RTT) → Proporciona tiempo de ida y vuelta en cada salto, indica si el salto responde o no. Se usa (*) para indicar un paquete perdido o no respondido. Esto ayuda en la detección de router problemáticos, mal ruteo, sobrecarga.

TTL de IPv4 y Límite de saltos en IPv6 → La primera secuencia de mensajes enviados desde traceroute tiene un valor de 1 en el campo TTL. Esto indica que se agotó el tiempo de espera del paquete IPv4 en cualquier router. El router responde con ICMP de tiempo extendido. Traceroute incrementa el campo TTL para cada secuencia de mensajes, proporcionando el rastro con la dirección de cada salto a medida que los paquetes caducan más adelante en la ruta.