



ESCUELA
POLITÉCNICA
NACIONAL

ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS



PROTOCOLOS ARP, ICMP, L2TP

E quipo #3:

- Aidan Carrasco
- Zenan Fernández
- Josue Palma
- Andrés Merino
- Mathew Verdezoto

Profesor: Ing. Juan Herrera
Fecha: 07/01/2026



ARP: FUNCIONAMIENTO Y ESTRUCTURA

Anatomía de ARP

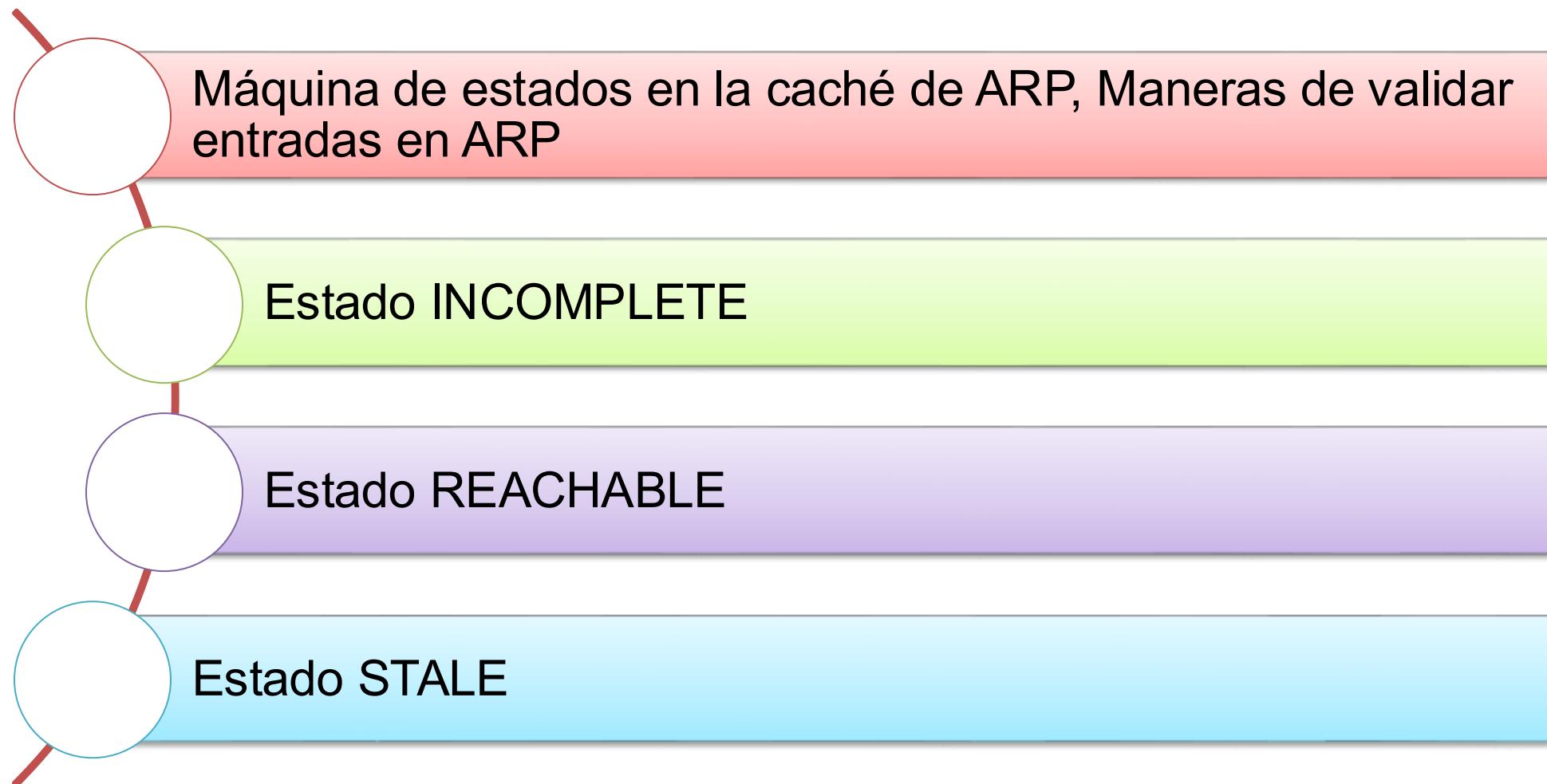
Hardware Type (HTYPE): Define el tipo de enlace de 2 bytes.

Protocol Type (PTYPE): Define el protocolo de capa superior de 2 bytes.

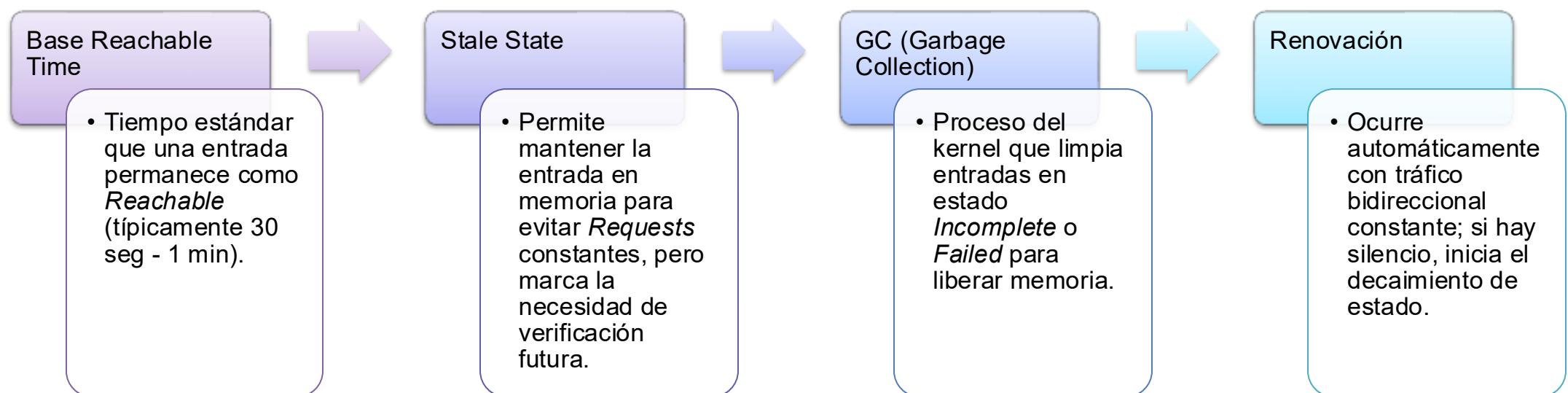
(HLEN y PLEN): (HLEN) es la longitud de dirección física (6 bytes para MAC), (PLEN) es la longitud de dirección lógica (4 bytes para IPv4), con 1 byte cada uno.

Opcode: Define la operación: 1 para APR request y 2 para APR reply.

Validación de Entradas: ARP



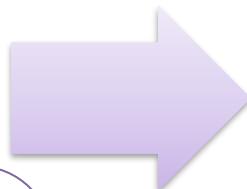
ARP Aging



Resolución de Direcciones

Local

- El Host verifica la máscara de subred.
- Target IP está en el mismo segmento.
- **ARP Request:** Busca la MAC del host de destino directamente.



Remota

- El Host detecta que la Target IP está fuera de la red.
- **ARP Request:** Busca la MAC del **default gateway (Router)**.
- *Diferencia Técnica:* La IP destino en la cabecera IP es el host remoto, pero la MAC destino en la trama Ethernet es el Router.



ARP: Variantes Avanzadas y Vulnerabilidades

Gratuitous ARP

¿Qué es?

- GARP es un mensaje ARP que un host envía sin haber recibido una solicitud previa. El equipo anuncia: “Esta IP pertenece a esta MAC” a toda la red.

Usos

- Detección de conflictos de IP:
- Actualización de tablas ARP:

Riesgo

- Puede ser explotado para envenenar tablas ARP, ya que los hosts confían en esto sin validación.

Proxy ARP

- Permite que un dispositivo responda solicitudes ARP en nombre de otro host que está en otra red.

¿Cómo funciona?

- Un host cree que el destino está en su misma red.
- El router responde con su propia MAC, como intermediario.
- El tráfico pasa por el router sin que el host tenga un gateway configurado.

Ventajas

- Permite comunicación entre subredes sin modificar configuraciones de hosts.
- Útil en redes heredadas o mal configuradas.

ARP Spoofing / Poisoning

¿En qué consiste?

- El atacante envía respuestas ARP falsas sin que nadie las haya solicitado, asociando:
 - IP del Gateway
 - IP de la víctima

Consecuencias

- El atacante intercepta, modifica, o espía el tráfico.
- Robo de credenciales
- Secuestro de sesiones

¿Por qué funcionan?

- ARP no cuenta con autenticación
- Los Hosts aceptan respuestas ARP no solicitadas
- Las tablas ARP se actualizan automáticamente

ESTRUCTURA DEL ENCABEZADO Y MENSAJES DE ERROR

Estructura General del Mensaje ICMP

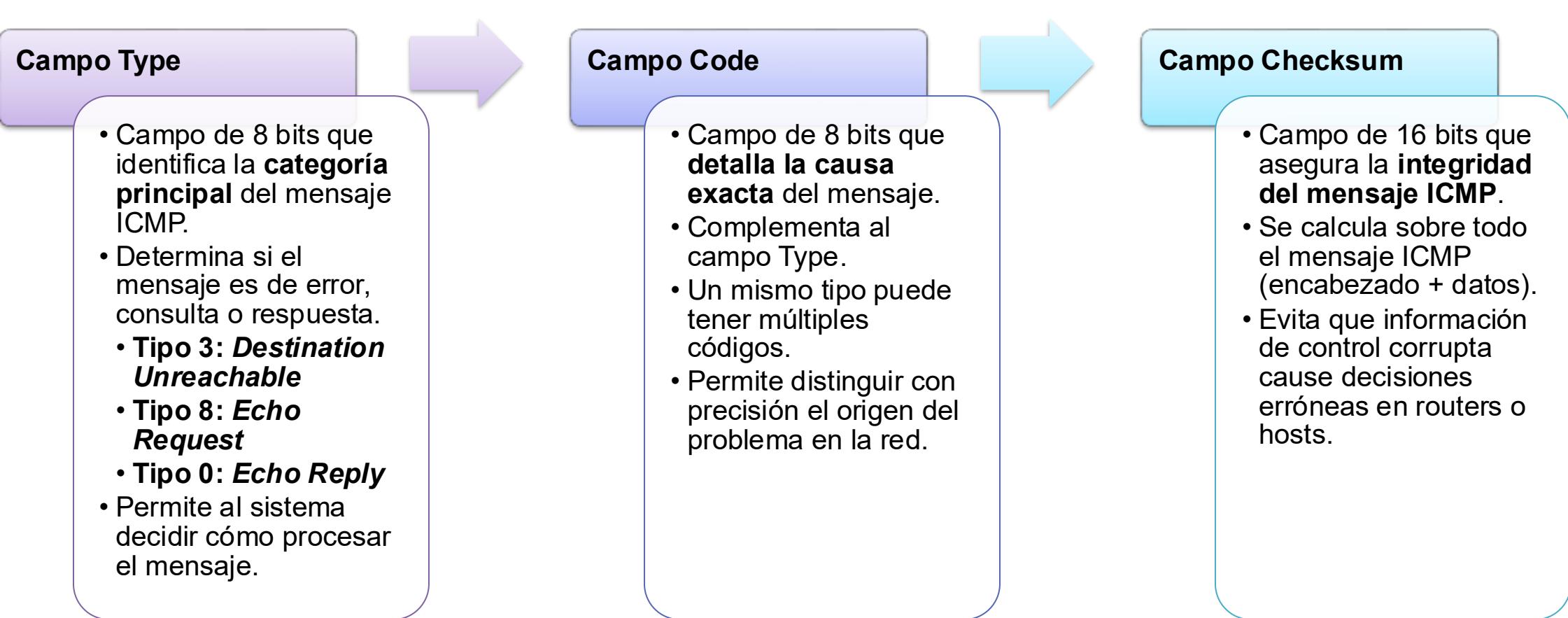
ICMPv4 es un protocolo auxiliar de la capa de red (Capa 3).

Sus mensajes viajan encapsulados dentro de datagramas IP.

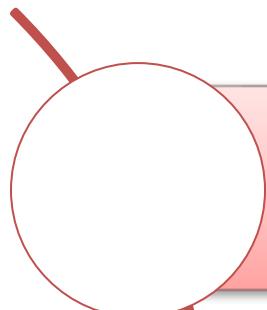
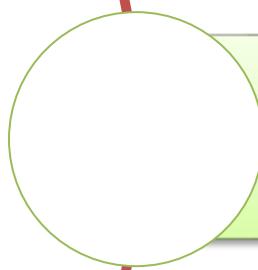
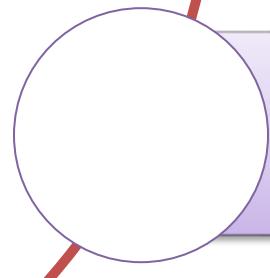
El mensaje ICMP posee un encabezado fijo de 8 bytes seguido de datos variables.

El encabezado define el tipo de mensaje, su causa específica y su integridad.

CAMPOS



Datos del Mensaje ICMP

-  Incluye el encabezado IP original del paquete que causó el error.
-  Contiene los primeros 8 bytes del payload original.
-  Permite identificar la sesión, el protocolo de transporte y los puertos involucrados.

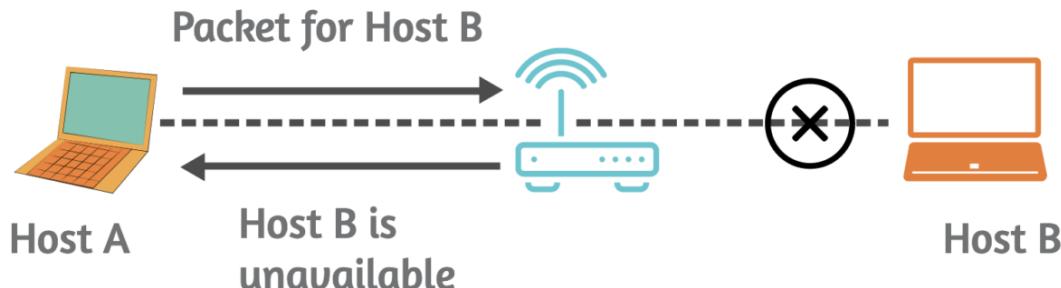
Mensajes de Error ICMP – Destination Unreachable

Función del Mensaje Destination Unreachable

Indica que un paquete IP no pudo ser entregado a su destino final.

Es uno de los mensajes de error más importantes de ICMP.

La causa exacta se identifica mediante el campo Code.



Códigos

Código 0: Network Unreachable

- No existe una ruta conocida hacia la red destino.
- Error de **Capa 3 (Enrutamiento)**.
- El router no tiene rutas estáticas, dinámicas ni ruta por defecto.

Código 1: Host Unreachable

- La red destino es conocida, pero el host no responde.
- Error típico de **Capa 2 (ARP)**.
- Ocurre cuando el host está apagado o desconectado.

Código 3: Port Unreachable

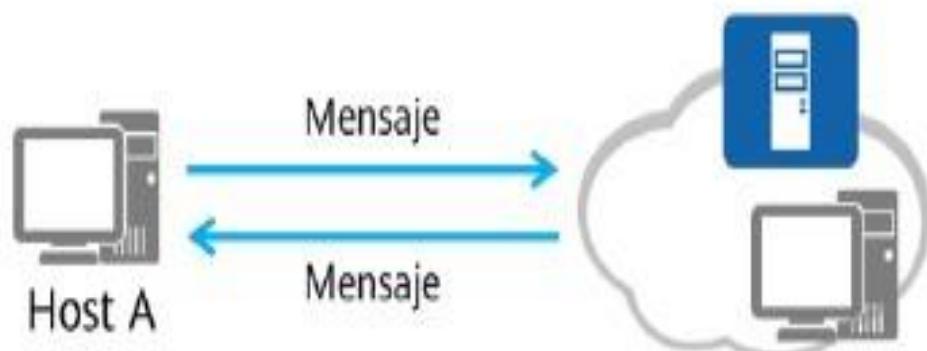
- El paquete llegó correctamente al host destino.
- No existe ninguna aplicación escuchando en el puerto destino.
- Error de **Capa 4 (Transporte / Aplicación)**.
- Fundamental para protocolos sin conexión como UDP.

Código 4: Fragmentation Needed / DF Set

- El paquete supera la MTU del enlace de salida.
- El bit DF está activado, por lo que no puede fragmentarse.
- Es esencial para el **Path MTU Discovery (PMTUD)**.
- Permite optimizar el tamaño de los paquetes y evitar fragmentación.

Cabecera Ethernet	Cabecera IP	Mensaje ICMP	cola Ethernet
-------------------	-------------	--------------	---------------

Temas del mensaje ICMP		
Tipo	Código	Descripción
0	0	Respuesta de eco
3	0	Red no disponible
3	1	Host no disponible
3	2	Protocolo no disponible
3	3	Puerto no disponible
5	0	Redireccionar
8	0	Solicitud de eco



Importancia de Destination Unreachable

Indica que un paquete IP **no pudo ser entregado a su destino final.**

Es uno de los mensajes de error más importantes de ICMP.

La causa exacta se identifica mediante el campo Code. Permite diagnosticar fallos en distintas capas de la red.

Proporciona retroalimentación precisa al host origen.

Contribuye a la estabilidad y eficiencia del tráfico IP.

Mecánica de Traceroute

Envío inicial: Host envía el paquete con TTL = 1.



En el router: El primer router reduce TTL a 0 y descarta el paquete.



Identificación: El Host registra la IP del router y repite con TTL = 2, 3, ...



Respuesta ICMP: El router envía el mensaje "Time Exceeded".

PMTU Discovery

El problema ocurre cuando un paquete es mayor al MTU del router y tiene la bandera y envía el error Type 3, Code 4 (Fragmentation Needed) activada.

El ICMP actúa cuando el router descarta el paquete y envía el error y envía el error Type 3, Code 4 (Fragmentation Needed).

El resultado es que permite al Host origen descubrir el tamaño máximo real de la ruta para optimizar el envío de datos.

ICMP Redirect

Mecanismo para actualizar dinámicamente las tablas de enrutamiento de los hosts.

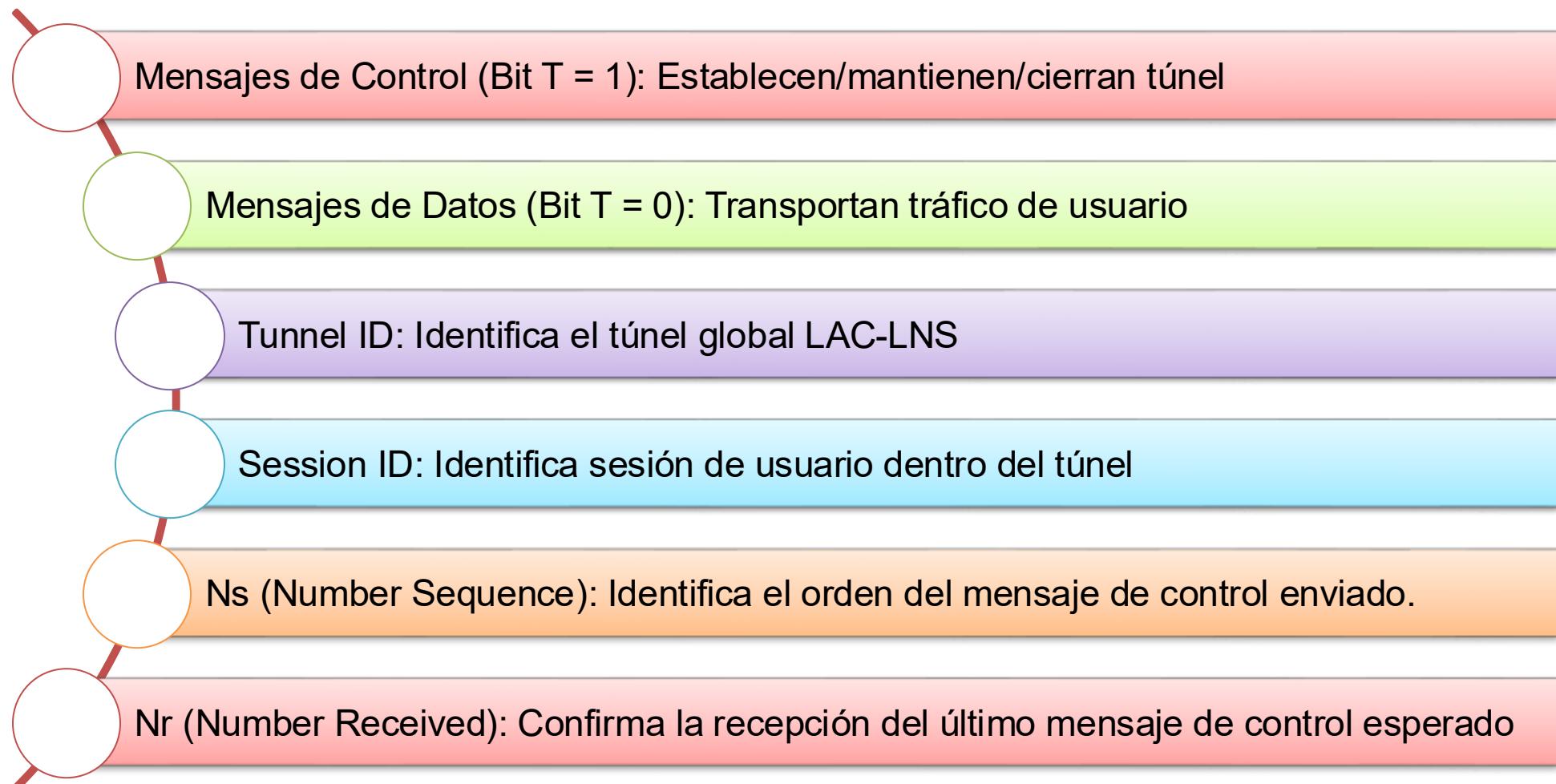
El Router detecta una mejor ruta (Next Hop) hacia el destino dentro del mismo segmento de red.

Envía un ICMP Redirect (Type 5) para que el host use la ruta óptima en el futuro.



L2TP

Estructura del paquete L2TP



Arquitectura L2TP

LAC (L2TP Access Concentrator)

- Punto de entrada del túnel (ISP o software cliente)
- Encapsula tramas PPP en L2TP/UDP
- Se conecta virtualmente con LNS usando túneles

LNS (L2TP Network Server)

- Punto de terminación en red corporativa
- Desencapsula, autentica y asigna IP
- Procesa tráfico como conexión local

Sesión L2TP

- Conexión transparente a través de Internet
- Independiente del medio físico (fibra, 4G, Wi-Fi)
- Para el LNS siempre aparece como interfaz PPP directa

Protocolo de túnel de capa 2

Estandar de la IETF (Internet Engineering Task Force) definido en la RFC (Request for Comments) 2661.

Extiende conexiones PPP (Protocolo Punto a Punto) a través de Internet, encapsulando tramas PPP en paquetes IP.

Encapsula tramas **PPP** (Point-to-Point Protocol) dentro de paquetes **UDP** (User Datagram Protocol).

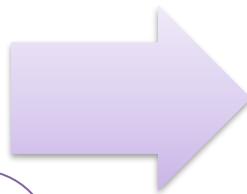
Usa UDP (User Datagram Protocol) puerto 1701 para reducir sobrecarga y latencia.

Utiliza solo tunelización y es normalmente usado para VPNs

Handshake L2TP: Establecimiento de Conexión

Establecimiento del túnel de control

- **SCCRQ (Start-Control-Connection-Request):**
 - El LAC solicita apertura del túnel y propone parámetros.
- **SCCRP (Start-Control-Connection-Reply):**
 - El LNS acepta y confirma los parámetros.
- **SCCN (Start-Control-Connection-Connected):**
 - El LAC confirma. Túnel de control activo.



Establecimiento de Sesión

- **ICRQ (Incoming-Call-Request):**
 - El LAC informa al LNS que un usuario solicita acceso.
- **ICRP (Incoming-Call-Reply):**
 - El LNS responde asignando un Session ID único y reservando recursos.
- **ICCN (Incoming-Call-Connected):**
 - El LAC confirma. Comienza el tráfico de datos (PPP).

AVPs

¿Qué es?

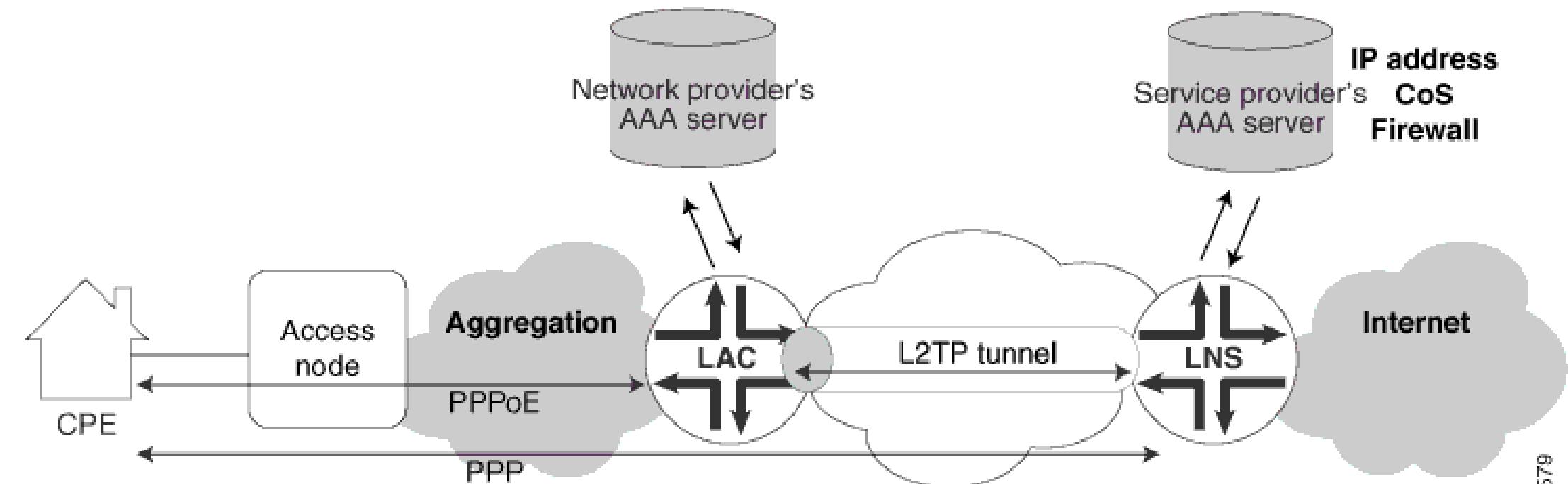
- Son bloques de datos modulares que transportan información de configuración dentro de los mensajes de control de L2TP

Estructura

- Longitud
- ID de Vendedor
- Tipo de Atributo
- Valor del dato

Mandatory Bit

- Es un indicador de obligatoriedad, define si un atributo debe ser reconocido y procesado por el dispositivo receptor
- M=1 (Crítico): Receptor debe reconocerlo o cerrar conexión.
- M=0 (Opcional): Receptor puede ignorarlo.



CONCLUSIONES

ARP e ICMP actúan como los cimientos operativos de la red, resolviendo la interacción crítica entre la capa de enlace y la capa de red. Mientras ARP garantiza la entrega local mediante la asociación dinámica de direcciones IP y MAC , ICMP proporciona la inteligencia necesaria para el diagnóstico y control, gestionando mensajes de error y validación de rutas para asegurar la estabilidad del tráfico.

L2TP permite la escalabilidad de la red mediante la creación de túneles de capa 2 a través de Internet. Al encapsular sesiones PPP dentro de paquetes UDP, este protocolo facilita conexiones remotas transparentes y la implementación de VPNs, permitiendo extender la red corporativa de forma segura independientemente del medio físico de acceso.