PROTOCOLOS CAPA 2: ENLACE DE DATOS

IIE456 IIE230 IIE547

Protocolos de Comunicaciones y Sistemas Embebidos

REPASO
FUNCIONES DEL PROTOCOLO DE COMUNICACIÓN

- Es un conjunto de reglas, normas y procedimientos que garantizan la integridad y correcta secuencia de los datos transmitidos.
- Asegura que todos los nodos de una red informática, emiten y reciben datos organizados en la misma forma.
- Ejemplo: Protocolo TCP/IP. Todo par de computadoras conectadas a Internet, deben seguir las normas del protocolo TCP/IP, para intercambiar datos.

REPASO
FUNCIONES DEL PROTOCOLO DE COMUNICACIÓN

- Establecer que un nodo está listo para comunicarse.
- Verificar y recuperar errores.
- Numerar los mensajes, para comprobar que llegan en la secuencia correcta.
- Controlar el destino de los mensajes.
- Decidir qué elemento emitir y cuál recibir.

CAPA 2: ENLACE DE DATOS

- La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico.
- Recibe peticiones de la capa 3 (Red) y utiliza los servicios ofrecidos por la capa 1 (Física).

CAPA 2: ENLACE DE DATOS

- Como es sabido, al realizar una transferencia de datos, siempre se está afecto a la potencial aparición de errores, además de la posible necesidad de regulación de la velocidad de datos por parte del receptor.

CAPA 2: ENLACE DE DATOS

- Es necesario incluir en cada dispositivo de comunicación una capa que regule y controle los posibles errores que se pueden generar.
- Esta capa se conoce como Nivel de Enlace de Datos y corresponde a la capa 2 del modelo OSI.

SLIP (SERIAL LINE INTERNET PROTOCOL)

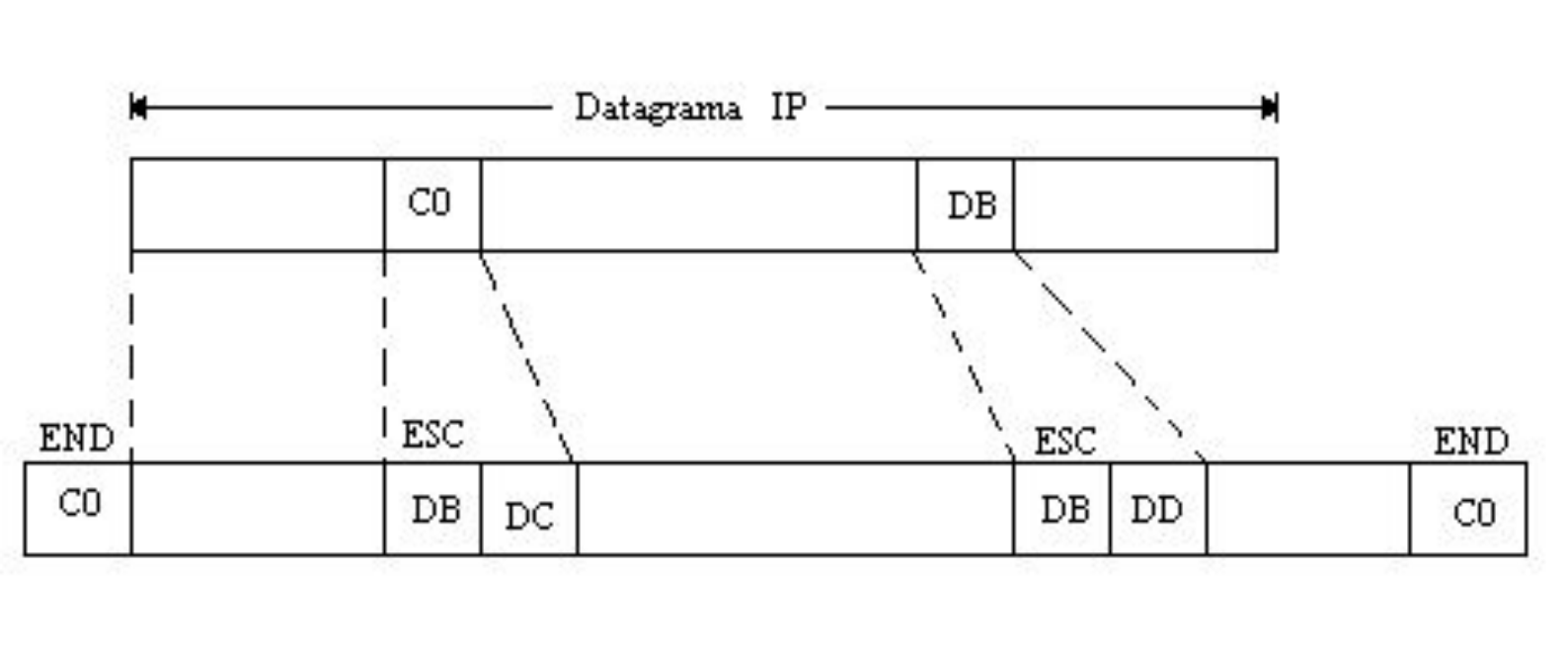
- Está definido bajo el RFC 1055.
- Fue diseñado en 1984 por Rick Adams para conectar estaciones de trabajo SUN a Internet a través de una línea de discado usando un Modem.
- Permite enviar y recibir paquetes IP como si estuviese directamente conectado a la red sólo utilizando una conexión de modem.
- Cualquier aplicación que utilice el protocolo TCP/IP funcionará de forma adecuada.

FORMATO DE SLIP

- Los datos se transmiten byte a byte, debiéndose marcar el inicio y el final de los paquetes.
- Para este propósito, SLIP define dos caracteres especiales END y ESC (no confundir con ESC del código ASCII)
  - END = 0xC0
  - ESC = 0xDB
- Cada datagrama IP es terminado por el carácter especial END. Para prevenir ruido de línea se acostumbra mandar uno al principio también; de modo que se de por terminada cualquier tipo de conexión errónea anterior.
- Si el carácter END se presenta en el contenido del datagrama; se utiliza la secuencia de dos bytes DB, DC.
- Si en el contenido se presenta el carácter de ESC, se reemplaza por la secuencia DB, DD.

FORMATO DE SLIP

- SLIP deja a las capas superiores la detección



DESVENTAJAS Y LIMITACIONES

- Admite solamente TCP/IP. No puedes utilizar SLIP para transferir directamente otros protocolos de red, tales como IPX/SPX o NetBEUI.
- Se requiere una dirección IP estática. SLIP solicita al cliente que configure todos los parámetros de configuración de TCP/IP, tales como las direcciones IP, antes de establecer una conexión con el servidor.
- Depende de la autentificación de inicio de sesión basada en texto y, normalmente, requiere de archivos de comandos para automatizar el proceso de inicio de sesión.

DESVENTAJAS Y LIMITACIONES

Debido al ruido existente en líneas telefónicas se producen errores a la hora de transmitir paquetes y a causa de la baja velocidad de estas líneas es muy elevado el coste de reenvío.

DESVENTAJAS Y LIMITACIONES

Se debe tener en cuenta que la detección de errores no es estrictamente necesaria debido a que el protocolo IP detecta los paquetes erróneos. De todos modos, sería recomendable que SLIP tuviera un sistema de detección y corrección de errores por sí mismo.

DESVENTAJAS Y LIMITACIONES

- Transmite las contraseñas de autentificación mediante texto, lo que puede ser peligroso para la seguridad porque las contraseñas no se encriptan durante la autentificación del usuario.

PPP (POINT TO POINT PROTOCOL)

- A finales de la década del 80, el Protocolo Internet de enlace serial (SLIP) representaba una limitación para el crecimiento de Internet.
- PPP se creó para solucionar los problemas de conectividad remota de Internet.
- PPP era necesario para poder asignar direcciones IP de forma dinámica y permitir el uso de múltiples protocolos.
- PPP suministra conexiones de router a router y de host a red a través de circuitos síncronos y asíncronos.
- Está diseñado pensando en enlaces simples que transporten paquetes entre dos entidades homólogas. Estos enlaces proporcionan operación bidireccional dúplex simultánea y se asume que entrega los paquetes de manera ordenada.

PPP

- PPP busca resolver los problemas de conectividad de Internet mediante tres componentes básicos:
  - Un método para encapsular datagramas a través de enlaces seriales. PPP utiliza el Control de enlace de datos de alto nivel (HDLC) como base para encapsular datagramas a través de enlaces punto a punto.
  - Un Protocolo de control de enlace (LCP) para establecer, configurar y probar la conexión de enlace de datos.
  - Una familia de Protocolos de control de red (NCP) para establecer y configurar distintos protocolos de capa de red. PPP está diseñado para permitir el uso simultáneo de múltiples protocolos de capa de red. En la actualidad, PPP soporta otros protocolos además de IP, incluyendo intercambio de paquetes de internetworking (IPX) y Appletalk.

FUNCIONAMIENTO PPP

Dirección	Control	Protocolo	Información	FCS
1 byte	1 byte	2 bytes	1500 bytes máx.	2 bytes

- Utiliza estructura de tramas tipo HDLC.
- Dirección: dirección de difusión HDLC. Este campo siempre tiene el valor 0xFF (broadcast: difusión masiva).
- Control: Comando HDLC para información no numerada. Este campo siempre tiene el valor 0x03.
- Protocolo: Identifica el protocolo encapsulado dentro del campo de información.
- Información: datos o protocolo de nivel superior.
- FCS: valor del cálculo de suma de comprobación de la trama.

CARACTERÍSTICAS DE PPP

- Control de la configuración del enlace de datos.
- Proporciona asignación dinámica de direcciones IP.
- Es multiprotocolo, una comunicación soporta simultáneamente varios protocolos a nivel de red.
- Configuración de enlace y verificación de la calidad del enlace.
- Detección de errores.
- Opciones de negociación para destrezas tales como negociación de la dirección de capa de red y negociaciones de compresión de datos
- Proporciona una solución común para una fácil conexión de una amplia variedad de host, puentes y routers.

PARAMETROS DE LOS PROTOCOLOS DE CAPA 2

Control de enlace lógico

- El control de enlace lógico (LLC) coloca información en la trama que identifica qué protocolo de capa de red está siendo utilizado por la trama. Esta información permite que varios protocolos de la Capa 3, tales como IP e IPX, utilicen la misma interfaz de red y los mismos medios.

Control de acceso al medio

- El control de acceso al medio (MAC) proporciona a la capa de enlace de datos el direccionamiento y la delimitación de datos de acuerdo con los requisitos de señalización física del medio y al tipo de protocolo de capa de enlace de datos en uso.

MAC

- Es un identificador de 48 bits (6 bloques de un Byte) expresados en hexa y separados por ":"
- Se la conoce también como dirección física, y es única para cada dispositivo.

PROTOCOLO ETHERNET

- Fue desarrollado por DEC, Intel, Xerox.
- Está definido por el estándar IEEE 802.3
- Utiliza una topología de bus y CSMA/CD (acceso múltiple con escucha de portadora y detección de colisiones) como método de acceso.

- Destino: Dirección MAC de destino
- Origen: Dirección MAC de origen
- Longitud: Tipo de protocolo encapsulado o longitud de la trama.
- Unidad de datos: paquete encapsulado (datos o protocolo interno)
- FCS: Secuencia de comprobación de trama (Frame Check Sequence)

Destino	Origen	Longitud	Unidad de datos+relleno	FCS
6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

Destino	Origen	TTL	Longitud	Unidad de datos+relleno	FCS
6 Bytes	6 Bytes	1 Byte	2 Bytes	15-1500 Bytes	4 Bytes