

**SEP**

SECRETARÍA DE  
EDUCACIÓN PÚBLICA



**TECNOLÓGICO NACIONAL DE MÉXICO**  
INSTITUTO TECNOLÓGICO DE TIZIMÍN

*“CIENCIA Y TECNOLOGÍA AL SERVICIO DEL HOMBRE”*

**ASIGNATURA: Int. De tecnologías WAN**

**TEMA: Resumen Capitulo 2**

**DOCENTE: Juan Alberto Vivas Burgos**

**ESTUDIANTE: Alex Ricardo Puc Kumul**

**CARRERA: Ingeniería informática**

**Fecha de entrega: 17 de septiembre del 2019**



## **¿Cómo funciona la comunicación serial?**

Ya sabe que la mayoría de las PC cuentan con puertos paralelos y seriales. También sabe que la electricidad sólo puede desplazarse en una velocidad. Una forma de obtener bits para desplazarse más rápidamente a través del cable es comprimir los datos de manera que se reduzcan la cantidad de bits y se requiera menos tiempo en el cable. Otra posibilidad para aumentar la velocidad es transmitir simultáneamente los bits. Aunque las computadoras utilizan conexiones paralelas relativamente cortas entre los componentes interiores, emplean un bus serial para convertir las señales para la mayoría de las conexiones externas.

### **Estándares de comunicación serial**

Todas las comunicaciones de largo alcance y la mayoría de las redes informáticas utilizan conexiones seriales, ya que el costo del cable y las dificultades de la sincronización hacen que las conexiones paralelas no sean prácticas. La ventaja más importante es que el cableado es más sencillo. Además, los cables seriales pueden ser más extensos que los cables paralelos, ya que hay menos interacción (crosstalk) entre los conductores del cable. En este capítulo, concentraremos nuestro interés en las comunicaciones seriales que conectan las LAN y WAN.

### **Multiplexación por división temporal**

Bell Laboratories creó la multiplexación por división temporal (TDM, Time Division Multiplexing) para maximizar el flujo de tráfico de voz que se transmite mediante un medio. Antes de la multiplexación, cada llamada telefónica solicitaba su propio enlace físico. Esta solución era costosa y difícil de implementar. La TDM divide el ancho de banda de un solo enlace en canales separados o en periodos de tiempo. La TDM transmite dos o más canales a través del mismo enlace mediante la asignación de diferentes intervalos de tiempo (periodo de tiempo) para la transmisión de cada canal. En efecto, los canales se turnan para emplear el enlace.

TDM es un concepto de capa física. No considera la naturaleza de la información que se somete a la multiplexación en el canal de salida. La TDM es independiente del protocolo de Capa 2 que utilizaron los canales de entrada.

La TDM puede explicarse por analogía al tráfico de autopistas. Para transportar el tráfico desde cuatro rutas a otra ciudad, puede enviar todo el tráfico por un solo carril si las rutas de alimentación cuentan con el mismo flujo de tráfico y si éste está sincronizado. De manera que, si cada una de las cuatro rutas coloca un automóvil en la autopista principal cada cuatro segundos, la autopista obtendrá un vehículo a la velocidad de uno por segundo. Siempre y cuando la velocidad de los automóviles esté sincronizada, no habrá colisión. En el destino, sucede lo contrario y los automóviles son retirados de la autopista y se les coloca en las rutas locales mediante el mismo mecanismo síncrono.

Este es el principio que se utiliza en la TDM síncrona al enviar los datos mediante un enlace. La TDM aumenta la capacidad del enlace de transmisión mediante la división del tiempo en intervalos más cortos, de manera que el enlace transmita los bits desde diferentes fuentes de entrada. Esto aumenta, con efectividad, la cantidad de bits transmitidos por segundo. Con la TDM, tanto el transmisor como el receptor saben exactamente cuál es la señal que se envía.

### **Multiplexación estadística por división temporal**

Como otra analogía, compare la TDM con 32 vagones de un tren. Cada uno es propiedad de una empresa de transporte diferente y todos los días el tren parte con los 32 vagones. Si una de las empresas tiene una carga que enviar, el vagón se carga. Si la empresa no tiene nada que enviar, el vagón permanece vacío, pero sigue siendo parte del tren. No es rentable transportar contenedores vacíos. La TDM comparte esta deficiencia cuando el tráfico es intermitente, ya que, incluso en este caso, se asigna un periodo de tiempo cuando el canal no tiene datos para transmitir.

Multiplexación estadística por división temporal (STDM, Statistical time-division multiplexing) fue diseñada para superar esta deficiencia. La STDM utiliza una extensión variable para el periodo de tiempo, lo que permite que los canales compitan para obtener cualquier espacio libre del periodo. Utiliza un búfer de memoria que almacena temporalmente los datos durante los periodos correspondientes a las horas picos de tráfico. La STDM no desperdicia el tiempo de la línea de alta velocidad con canales inactivos con este esquema. La STDM exige que cada transmisión transmita la información de identificación (un identificador de canal).

### **Punto de demarcación**

Antes de la desregulación en América del Norte y en otros países, las empresas telefónicas eran dueñas del bucle local, incluidos el cableado y el equipo en las instalaciones de los clientes. La desregulación forzó a las empresas telefónicas a individualizar su infraestructura de bucle local para permitir que otros proveedores proporcionen el equipo y los servicios. Esto creó la necesidad de delinear qué parte de la red pertenecía a la empresa telefónica y qué parte pertenecía al cliente. Este punto de la delimitación es el punto de demarcación o demarc. El punto de demarcación marca el punto en donde su red se interconecta con la red que pertenece a otra organización. En la terminología telefónica, ésta es la interfaz entre el equipo terminal del abonado (CPE, customer-premises equipment) y el equipo del proveedor de servicios de red. El punto de demarcación es el lugar de la red donde finaliza la responsabilidad del proveedor de servicios.

## **DTE-DCE**

Desde el punto de vista de la conexión a la WAN, una conexión serial posee un dispositivo DTE en un extremo de la conexión y un dispositivo DCE en el otro extremo. La conexión entre los dos dispositivos DCE es la red de transmisión del proveedor de servicios WAN. En este caso:

- el CPE, que en general es un router, es el DTE. El DTE también podría ser un terminal, una computadora, una impresora o una máquina de fax si se conectaran directamente a la red del proveedor de servicios.
- El DCE, en general un módem o CSU/DSU, es el dispositivo que se utiliza para convertir los datos del usuario del DTE en una forma que sea aceptable para el enlace de la transmisión del proveedor del servicio WAN. La señal se recibe en el DCE remoto, que decodifica la señal nuevamente en una secuencia de bits. El DCE remoto luego señala esta secuencia al DTE remoto.

La Asociación de Industrias Electrónicas (EIA, Electronics Industry Association) y el Sector de Normalización de las Telecomunicaciones de la Unión de Telecomunicaciones Internacional (UIT-T, International Telecommunication Union Telecommunications Standardization Sector) han trabajado muy activamente en el desarrollo de estándares que permiten que los DTE se comuniquen con los DCE. La EIA denomina al DCE como el equipo de comunicación de datos, mientras que la ITU-T lo llama equipo de terminación de circuitos de datos.

## **Estándares de los cables**

Originalmente, el concepto de los DCE y los DTE se basó en dos tipos de equipos: el equipo terminal que generaba o recibía datos y el equipo de comunicación que sólo transmitía datos. En el desarrollo del estándar RS-232, había razones que justificaban la necesidad de un cableado diferente para los conectores RS-232 de 25 pins en estos dos tipos de equipos. Aunque estas razones ya no son importantes, tenemos dos tipos diferentes de cables: uno para la conexión de un DTE con un DCE y otro para la conexión directa entre dos DTE.

La interfaz DTE/DCE para un estándar en particular define las siguientes especificaciones:

- Mecánica/física: número de pins y tipo de conector
- Eléctrica: define los niveles de tensión para 0 y 1
- Funcional: especifica las funciones que se ejecutan al asignar significados a cada una de las líneas de señalización de la interfaz
- Procesal: especifica la secuencia de eventos para la transmisión de los datos

## Protocolos de encapsulación WAN

En cada conexión WAN, los datos se encapsulan dentro de tramas, antes de cruzar el enlace WAN. Para asegurar que se utiliza el protocolo correcto, usted debe configurar el tipo de encapsulación de la Capa 2 adecuado. La elección del protocolo depende de la tecnología WAN y del equipo de comunicación. En la imagen, se muestran los protocolos WAN más comunes y el lugar donde se utilizan; luego, se observan descripciones breves.

- HDLC: el tipo de encapsulación predeterminada en las conexiones punto a punto, los enlaces dedicados y las conexiones conmutadas por circuito cuando el enlace utiliza dos dispositivos Cisco. El HDLC es ahora la base para el PPP síncrono, empleado por muchos servidores para conectarse a una WAN, más comúnmente a Internet.
- PPP: suministra conexiones de router a router y de host a red, a través de circuitos síncronos y asíncronos. El PPP funciona con varios protocolos de capa de red, como IP e intercambio de paquetes de internetworking (IPX, Internetwork Packet Exchange). El PPP también tiene mecanismos de seguridad incorporados como el PAP y el CHAP. La mayor parte de este capítulo trata del PPP.
- Protocolo Internet de línea serial (SLIP, Serial Line Internet Protocol): un protocolo estándar para conexiones seriales punto a punto que usan TCP/IP. SLIP ha sido desplazado en gran medida por PPP.
- X.25/procedimiento de acceso al enlace balanceado (LAPB, Link Access Procedure, Balanced): estándar de la UIT-T que define cómo se mantienen las conexiones entre DTE y DCE para el acceso remoto a terminales y las comunicaciones informáticas en las redes de datos públicas. X.25 especifica a LAPB, un protocolo de capa de enlace de datos. X.25 es un predecesor de Frame Relay.
- Frame Relay: un protocolo estándar industrial, de capa de enlace de datos, conmutado, que maneja múltiples circuitos virtuales. Frame Relay es un protocolo que pertenece a una generación inmediatamente posterior a X.25. Frame Relay descarta algunos de los procesos que consumen el tiempo (como la corrección de errores y el control del flujo) utilizados en X.25. El próximo capítulo trata sobre Frame Relay.
- ATM: el estándar internacional para relay de celdas mediante el cual los dispositivos envían múltiples tipos de servicio (como, por ejemplo, voz, vídeo o datos) en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento se lleve a cabo en el hardware, lo que disminuye los retrasos en el tránsito. ATM aprovecha los medios de transmisión de alta velocidad, como E3, SONET y T3.

## **Encapsulación HDLC**

HDLC es un protocolo orientados a bit síncrono de capa de enlace de datos, desarrollado por la Organización Internacional de Normalización (OIE). El estándar actual para HDLC es ISO 13239. HDLC se desarrolló a partir del estándar control de enlace de datos síncrono (SDLC, Synchronous Data Link Control) propuesto en la década de 1970. El HDLC brinda servicio orientado a la conexión y sin conexión.

El HDLC utiliza transmisión serial síncrona para brindar comunicación libre de errores entre dos puntos. El HDLC define una estructura del entramado de Capa 2 que permite el control del flujo y el control de errores mediante el uso de acuses de recibo. Cada trama presenta el mismo formato, ya sea una trama de datos o una trama de control.

### **¿Qué es el PPP?**

Recuerde que HDLC es el método de encapsulación serial predeterminada al conectar dos routers Cisco. Con un campo tipo protocolo agregado, la versión de HDLC de Cisco está patentada. Por lo tanto, el HDLC de Cisco sólo puede funcionar con otros dispositivos de Cisco. Sin embargo, cuando necesite conectarlo a un router que no sea Cisco, debe utilizar la encapsulación PPP.

La encapsulación PPP se diseñó cuidadosamente para que sea compatible con los hardware de soporte que más se usan. El PPP encapsula tramas de datos para la transmisión a través de los enlaces físicos de la Capa 2. El PPP establece una conexión directa mediante cables seriales, líneas telefónicas, líneas troncales, teléfonos celulares, enlaces de radio especializados o enlaces de fibra óptica. Existen muchas ventajas al usar el PPP, incluido el hecho de que no está patentado. Además, incluye varias funciones que no están disponibles en el HDLC:

- la función Administración de calidad del enlace monitorea la calidad del mismo. Si se detectan muchos errores, el PPP desactiva el enlace.
- El PPP admite la autenticación PAP y CHAP. Esta función se explica y se practica en secciones subsiguientes.

El PPP contiene tres componentes principales.

- El protocolo HDLC para la encapsulación de datagramas a través de enlaces punto a punto.
- Un protocolo de control de enlace (LCP, Link Control Protocol) extensible para establecer, configurar y probar la conexión de enlace de datos.
- Una familia de protocolos de control de red (NCP, Network Control Protocols) para establecer y configurar distintos protocolos de capa de red. El PPP permite el uso simultáneo de múltiples protocolos de capa de red.

## **Arquitectura PPP**

Una arquitectura de capas es un modelo, diseño o plan lógico que ayuda a la comunicación entre las capas interconectadas. La imagen traza la arquitectura de capas del PPP en contraste con el modelo de interconexión de sistema abierto (OSI, Open System Interconnection). EL PPP y OSI comparten la misma capa física, pero el PPP distribuye las funciones del LCP y el NCP de manera diferente.

En la capa física, puede configurar el PPP en una variedad de interfaces, las que incluyen:

- Serial asíncrona
- Serial síncrona
- HSSI
- ISDN

## **Protocolo de autenticación PAP**

PPP define un LCP extensible que permite la negociación de un protocolo de autenticación para autenticar su peer antes de permitir que los protocolos de capa de red transmitan a través del enlace. RFC 1334 define dos protocolos para autenticación.

PAP es un proceso muy básico de dos vías. No hay encriptación: el nombre de usuario y la contraseña se envían en texto sin cifrar. Si esto se acepta, la conexión se permite. CHAP es más seguro que PAP. Implica un intercambio de tres vías de un secreto compartido. Más adelante, en este mismo capítulo, se describirá este proceso.

La fase de autenticación de una sesión PPP es opcional. Si se usa, se puede autenticar el peer, luego de que el LCP establezca el enlace y elija el protocolo de autenticación. Si se utiliza, la autenticación se lleva a cabo antes de que comience la fase de configuración del protocolo de la capa de red.

Las opciones de autenticación requieren que la parte del enlace que realiza la llamada introduzca la información de autenticación. Esto ayuda a garantizar que el usuario tenga el permiso del administrador de la red para efectuar la llamada. Los routers pares intercambian mensajes de autenticación.

## **Iniciando PAP**

PAP ofrece un método sencillo para que un nodo remoto establezca su identidad por medio del protocolo de enlace de dos vías. PAP no es interactivo. Cuando se utiliza el comando `ppp authentication pap`, el nombre de usuario y la contraseña se envían como un paquete de datos LCP, en lugar de que el servidor envíe un aviso de inicio de sesión y espere una respuesta. La imagen muestra que luego de que PPP completa la fase de establecimiento de enlace, el nodo remoto envía

repetidamente un par nombre de usuario-contraseña a través del enlace hasta que el nodo que envía lo reconoce o finaliza la conexión.

### **Protocolo de autenticación de intercambio de señales (CHAP)**

Una vez que se establece la autenticación con PAP, esencialmente deja de funcionar. Esto deja la red vulnerable para los ataques. A diferencia de PAP, que sólo autentica una vez, CHAP realiza comprobaciones periódicas para asegurarse de que el nodo remoto todavía posee un valor de contraseña válido. El valor de la contraseña es variable y cambia impredeciblemente mientras el enlace existe.

Después de completar la fase de establecimiento del enlace PPP, el router local envía un mensaje de comprobación al nodo remoto.