



**Ingeniería en Desarrollo de Software**  
**Semestre 6**

Programa de la unidad didáctica:  
**Interconectividad de redes**

**Unidad 2.**  
**Interconectividad de redes de área extensa WAN**

Ciudad de México, octubre del 2025

Clave:  
**15143634**

**Universidad Abierta y a Distancia de México**





### Índice

Presentación de la unidad .....	3
Logros .....	3
Competencia específica .....	3
2.1. Elementos de interconectividad de redes .....	4
2.1.1. Dispositivos de interconectividad de redes WAN .....	5
2.1.2. Tunelización de protocolos .....	6
2.1.3. Creación de redes virtuales .....	6
2.2. Protocolos de redes WAN .....	8
2.2.1. HDLC .....	8
2.2.2. PPP .....	9
2.2.3. Metro Ethernet .....	11
2.2.4. DSL .....	13
2.3.1. Tipos de uniones y conexiones .....	15
2.3.2. Conexiones seriales .....	17
2.3.3. TDM .....	19
2.3.4. DTE y DCE .....	21
Cierre de la unidad .....	23
Para saber más .....	23
Fuentes de consulta .....	24



### Unidad 2. Interconectividad de área extensa WAN

#### Presentación de la unidad

En esta segunda unidad se desarrollarán temas acerca de la interconectividad de redes de área extensa o WAN. Verás los elementos necesarios para diseñar una interconectividad, así como los protocolos y tipos de conexiones más comunes.

Entender el proceso de interconectividad entre redes WAN es importante porque te apoyará en la comprensión de la forma en que operan y se interconectan, además contarás con un panorama más amplio sobre los beneficios y las limitaciones que proporciona este tipo de interconectividad.

Es por ello que se requiere que aprendas a analizar y distinguir los elementos de interconectividad de redes WAN, y así realices un diseño de servicio de red para aplicar los elementos de interconectividad, y configures las aplicaciones según se requiera en una empresa u organización.

Una interconectividad de área extensa se requiere, por ejemplo, cuando una empresa crece y agrega sucursales, pues sus necesidades de uso de tecnologías de información aumentan y, por ende, una red LAN ya no es suficiente. Actualmente las empresas necesitan acceso a redes WAN, con el fin de mantener sus operaciones incluso más allá de las fronteras de su propio país. La interconectividad de área extensa (WAN) es aquella comunicación que existe entre dos o más redes de diferentes regiones geográficas (CiscoSystems, 2008a).

#### Logros

Al término de esta unidad lograrás:

- Identificar los elementos de interconectividad de redes.
- Distinguir los tipos de protocolos de redes WAN.
- Relacionar las uniones y conexiones WAN a partir de un diseño.

#### Competencia específica

- Realizar un diseño de servicio de red para aplicar los elementos de interconectividad de redes de área extensa a partir de los requerimientos específicos.



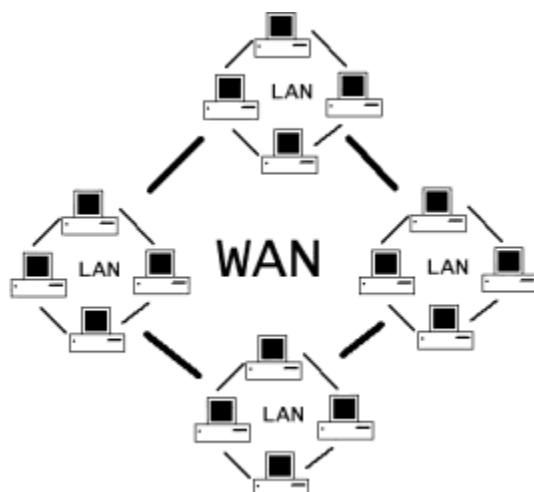
### 2.1. Elementos de interconectividad de redes

Como recordarás, las redes se clasifican de acuerdo con su tamaño geográfico; por lo tanto, existen de área local (LAN) y amplia (WAN), principalmente.

Para que exista la interconectividad WAN, es necesario que antes haya interconectividad LAN. Para que esta última exista es necesario contar con los siguientes elementos físicos (Laporta, 2005):

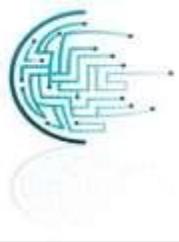
- **Ordenadores y periféricos:** por ordenadores se debe entender equipos de cómputo tales como las computadoras de escritorio, laptops, notebooks, smartphones; mientras que los periféricos incluyen dispositivos conectados a la red, tales como impresoras o scanners.
- **Interfaces de red:** son aquellos dispositivos que, conectados a una computadora o periférico, permiten tener conectividad a la red, sea por medio de conexiones alámbricas o inalámbricas; por ejemplo, las tarjetas de red inalámbricas o alámbricas. Actualmente, este tipo de dispositivos ya vienen integrados en cualquier equipo de cómputo, aunque también se venden por separado, para integrar de más de una interfaz de red a un equipo de cómputo.
- **Equipos de interconexión de red:** en este apartado se encuentran los repetidores o hubs, switches, routers, etcétera. Un equipo de interconexión de red es aquel que provee de interconectividad. Mediante éste es posible que uno o más equipos se interconecten a una red.

En la siguiente imagen se ilustra cómo la interconectividad WAN existe a partir de la LAN.



Ejemplo de red WAN.

González, A. (2010). Ejemplo de red WAN [Imagen]. <http://fitcomputerve.blogspot.mx/2010/10/redes-lan-man-wan.html>



Una vez que existe la interconectividad LAN en los lugares donde se requiera establecer comunicación, se puede generar una interconectividad WAN a partir de dos formas. La primera y más común es a través de un operador de servicios de operadoras, como, por ejemplo, proveedores de servicios de cable de televisión, de telefonía y sistemas satelitales.

La segunda forma es a través de dispositivos de interconectividad WAN, comúnmente se usan routers con conexiones seriales, las cuales se explicarán más adelante en el subtema 2.3.2.

A la primera forma se le denomina interconectividad WAN pública, y a la segunda interconectividad WAN privada. En ambas formas es necesaria la utilización de un **router**. A continuación, se explicará más a detalle este tipo de dispositivos.

### 2.1.1. Dispositivos de interconectividad de redes WAN

Los dispositivos de interconectividad también se conocen con el nombre de hardware intermedio. Su función es interconectar diferentes dispositivos en una red (Laporta, 2005).

Como se comentó anteriormente, el dispositivo de interconectividad WAN es el router. Te preguntarás entonces ¿Por qué se dice dispositivos y no sólo dispositivo en singular? Simplemente porque existen dos tipos: de conexión pública y de conexión privada.

Los routers de conexión pública, comúnmente llamados módems, son aquellos que permiten conectarse a Internet, que es una red WAN, desde casa u oficina. Ejemplos de

estos son todos aquellos que instalan los proveedores de telefonía alámbrica, televisión de paga, u operadores de telefonía celular. Los routers de conexión privada son aquellos equipos que normalmente tienen las grandes empresas o corporaciones.

Como recordarás, un router es un dispositivo de red que trabaja sobre la **capa 3** del modelo OSI. La interconectividad de redes WAN se lleva a cabo principalmente en la capa física (capa 1) y enlace de datos (capa 2) del modelo OSI, respectivamente. La capa 3 o nivel de red se encarga de enviar el paquete a su destino final (Cisco Systems, 2008a).

Los protocolos de la capa 1 del modelo OSI son los encargados de enviar o recibir las conexiones eléctricas u ópticas entre origen y destino. La capa 2 define cómo se encapsularán los datos para su transmisión a lugares remotos, así como los



Mecanismos de transferencia de las tramas que utilizan tecnologías como: Metro Ethernet y ATM (CiscoSystems, 2008a), las cuales se explicarán a detalle en el tema 2.2.

Hasta aquí se explicó brevemente cómo interactúan las capas 1, 2 y 3 del modelo de referencia OSI para la interconectividad de redes. A continuación, se explicará por qué existe un modo especial que permite enviar datos a nivel de capa 2 del modelo OSI Enlace de datos, al cual se le conoce como tunelización de protocolos.

### 2.1.2. Tunelización de protocolos

La técnica de tunelización de protocolos consiste en encapsular un mensaje de un protocolo dentro de sí mismo, aprovechando ciertas propiedades del paquete externo, con el objetivo de que sea tratado de forma diferente a como lo habría sido encapsulado. De esta forma un paquete puede ser usado para evitar un firewall (Blanco, Huidobro y Jordán, 2008).

Esto quiere decir que la técnica de tunelización de protocolos permite meter un protocolo dentro de otro (Cisco Systems, 2008a), con el fin de que un mensaje enviado de origen a destino (entre computadoras) sea tratado como el protocolo que lo encierra. Por ejemplo, una petición Telnet (conexión a equipos remotos) sea tratada como un protocolo de http (conexión a páginas web). Esto se hace con el fin de enmascarar o de ocultar el protocolo real a usar. Esto ayuda a que viaje de manera segura a través de una red, en este caso la WAN.

Otro uso de la tunelización de protocolos es la creación de las redes privadas virtuales, lo cual se revisará a continuación.

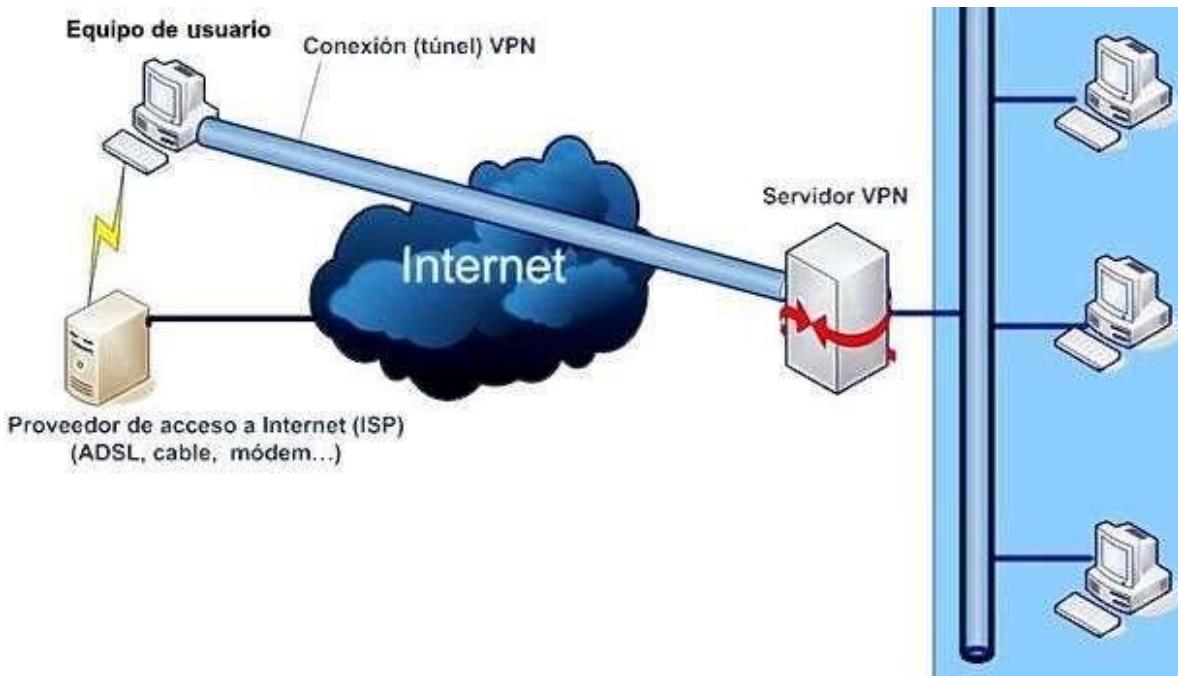
### 2.1.3. Creación de redes virtuales

Una red privada virtual VPN (*Virtual Private Network*) se define como una extensión de red (LAN) que usa redes públicas (Internet), y que hace posible la transmisión de datos como si estuvieran en la misma LAN (Cobo, 2005). Una red privada virtual se crea, a partir de la tunelización de protocolos, para dar conectividad a redes que son privadas; por ejemplo, un caso de uso de una red privada virtual que tiene como objetivo dar acceso a los empleados de una organización a la red interna a través de Internet, esto para garantizar y facilitar el acceso seguro a recursos privados.

Por recursos privados entiéndase una red corporativa o Intranet. Es importante mencionar que el enlace que se crea con la red privada virtual es **privado**, invisible a instancias ajenas al ámbito de aplicación; para lograrlo, los datos enviados a través de la red privada virtual son cifrados. La acción de cifrar se entiende como guardar algo muy valioso bajo llave; en el ámbito de los datos que viajan en una red es la acción



mediante la cual los datos confidenciales se cifran con un algoritmo de cifrado, además de una clave que los hace ilegibles si no se la conoce (Microsoft, 2005), con lo cual se garantiza la confidencialidad de los datos enviados. Los datos son confidenciales ya que, si alguien los intercepta, para descifrarlos necesitará la clave del cifrado (Cobo, 2005). En la Unidad 3. Seguridad de redes se revisarán los conceptos de seguridad y cifrado de la información.



Ejemplo de VPN.

Universidad de Chile. (2013). Ejemplo de VPN [Imagen]. <http://soporte.uchile.cl/mediawiki/images/4/4b/Esquema-vpn.png>

En la imagen anterior se ilustra el funcionamiento de una conexión VPN. Se toma como ejemplo que la conexión a Internet del usuario es a través de un proveedor de servicios de Internet ISP (*Internet Service Provider*). La conexión a la VPN funciona de la siguiente manera:

1. El **equipo** del usuario con una conexión establecida a Internet mediante su ISP, se **conecta** al servidor de VPN mediante sus **credenciales** (usuario/password).
2. Una vez validadas las credenciales, se establece un **túnel** virtual entre el equipo del usuario y el servidor de VPN, esto hará que todas las conexiones que desee establecer el usuario no las procese el ISP sino el servidor de VPN; es decir, el usuario tendrá **conexión directa** con la red interna que interconecta el servidor de VPN, la cual puede ser de una organización o de una empresa.

De esta manera, el equipo del usuario será capaz de estar conectado remotamente; es decir, conectado a la Intranet de la organización desde una localidad que no sea la empresa, por ejemplo, su casa, un café internet, de un estado a otro, etcétera.



¿Serán suficientes los elementos de interconectividad revisados en este capítulo para que exista la interconectividad WAN? La respuesta es no, faltan por revisar los protocolos de redes.

### 2.2. Protocolos de redes WAN

Los elementos de interconectividad de redes WAN que se han revisado no funcionarían adecuadamente sin el uso de **protocolos**, como recordarás en la unidad didáctica *Fundamentos de redes*, un protocolo se define como el conjunto de reglas que controlan la comunicación entre dos o más computadoras (Tanenbaum, 2003).

Los protocolos de redes WAN funcionan a nivel de capa de enlace de datos del modelo de referencia OSI. Esta capa define cómo se encapsulan los datos para su transmisión a lugares remotos, así como también los mecanismos de transferencia de las tramas. Se utiliza una variedad de tecnologías diferentes, tales como HDLC, PPP, Metro Ethernet o DSL, entre otras (Cisco Systems, 2008a). Las cuales se revisarán continuación.

Antes de entrar en materia, recuerda qué es un protocolo. Según Forouzan (2003, p. 100), un protocolo es “un conjunto de reglas que controla la interacción de diferentes dispositivos en una red o en un conjunto de redes interconectadas”. Con base en esta definición puede decirse que un protocolo de red WAN es aquel conjunto de reglas que controla la interacción de diferentes dispositivos en una red WAN, o en el conjunto de redes LAN, MAN o PAN interconectadas entre sí, mediante la red WAN.

#### 2.2.1. HDLC

Existen diversos protocolos de interconectividad de encapsulación de red, los cuales permiten llevar cabo funcionalidades en la red WAN, con el fin de hacer que los paquetes viajen de origen a destino. El HDLC es la base de muchos protocolos de interconectividad WAN, por ello será el primero que se revisará.

El control de enlace de datos de alto nivel HDLC (*High-Level Data Link Control*) es un protocolo de comunicaciones síncrono (para pueda establecerse la comunicación el transmisor debe coordinarse con el receptor; esto es, que emisor y receptor se ponen de acuerdo sobre la manera en que se enviarán los datos), de propósito general punto a punto y punto a multipunto (punto a punto, es una comunicación que se da sólo en dos dispositivos; es decir, emisor y receptor. Punto a multipunto, es cuando existe un emisor y múltiples receptores), que opera a nivel de enlace de datos (Cisco Systems, 2008a).

El protocolo HDLC usa las siguientes tres fases para establecer comunicación en una interconectividad de redes WAN (Latorre, 2013):



1. **Conexión y establecimiento del circuito:** para este paso ya deben estar conectados físicamente los dispositivos; es decir, **conectados** a la red mediante un cable o una conexión inalámbrica. Una vez hecho esto se establece una conexión lógica, con la cual emisor y receptor se ponen de acuerdo en cómo se va a llevar a cabo la **comunicación**; es decir, ponen las variables usadas en la comunicación a cero (como cuando inicializa un programa). Esto se lleva a cabo enviando **tramas** de control entre los dispositivos. Como recordarás, una trama es la unidad mínima de información usada en la capa de enlace de datos; esta trama es un conjunto de unos y ceros.
2. **Transporte o transferencia de datos:** en esta fase se produce el **intercambio** de datos entre emisor y receptor, entre las tramas de datos (que son en sí la información que debe de viajar entre emisor y receptor). Se pueden **enviar** tramas de control con el fin de inspeccionar el flujo de información entre emisor y receptor.
3. **Desconexión de circuito:** una vez finalizada la transferencia de datos se **desconecta** este circuito virtual; es decir, emisor y receptor **liberan** los recursos que utilizaron para llevar a cabo la comunicación, tales como el ancho de banda reservado y las tramas de control que recibían, las cuales se borran.

HDLC usa un **método** para **encapsular** datos de enlaces seriales síncronos (Cisco Systems, 2008a), los cuales se verán a detalle más adelante, en el subtema 2.3.2. Este tipo de encapsulación es la predeterminada en equipos de conexiones WAN; además, HDLC es la base para el protocolo PPP (*Point to Point Protocol*), el cual se revisará a continuación.

### 2.2.2. PPP

El protocolo punto a punto (*Point to point Protocol*), suministra conexiones de router a router y de host a red, a través de circuitos síncronos y asíncronos (como se observó anteriormente, **síncrono** es cuando se ponen de acuerdo emisor y receptor en el establecimiento de la comunicación; por ende, el emisor entrega al receptor paquetes de datos en intervalos de tiempos regulares. **Asíncrono** es todo lo contrario; es decir, los paquetes llegan a intervalos irregulares de tiempo). El PPP funciona con varios protocolos de capa de red, como IP e IPX (de Novell). El PPP también tiene mecanismos de seguridad incorporados como el protocolo de autenticación de contraseña PAP (*Password Authentication Protocol*) y el protocolo de autenticación por desafío mutuo CHAP (*Challenge Handshake Authentication Protocol*) (Cisco Systems, 2008a). Los dos últimos se explicarán a continuación.

**PAP:** el router que deseé enviar paquetes a otro router, deberá demostrar, mediante la autenticación (usuario y password), que se trata de ese router; es decir, esta autenticaciones a nivel de identificación de conexión, por ello las credenciales no viajan encriptadas, no se cifran o viajan de manera insegura a través de la red. En la unidad 3



se explicará a detalle el concepto de encriptación. (Cisco Systems, 2008a).

**CHAP**: es un protocolo con características de seguridad que evita el acceso no autorizado (Cisco Systems, 2008a). Los routers son clientes remotos ya que interconectan redes WAN y, como éstas ocupan grandes extensiones, la mayoría de las veces los routers no estarán conectados en una misma área geográfica, el protocolo CHAP verifica periódicamente la identidad del cliente remoto; es decir, un router, mediante un intercambio de información que se realiza en tres etapas:

1. El router emisor **establece un enlace**. Inmediatamente el sistema o el router receptor pide que se autentifique el usuario.
2. El router emisor **responde** con un hash o cadena de texto con su suma de verificación en MD5 (algoritmo de que permite cifrar datos) de manera que, al aplicarlo en alguna palabra, por ejemplo, *hola*, el resultado será algo así como *d41d8cd98f00b204e9800998ecf8427e*. Esta nueva cadena ya no es un *hola* normal sino **encriptada**. MD5 también ayuda a verificar que los archivos que se envían o reciben estén íntegros; para ello es necesario aplicar el algoritmo al archivo que se desea probar, el resultado se deberá de comparar con la cadena original que emite el emisor con el fin de verificar la autenticidad; es decir, que el archivo no haya sido modificado por alguien más.
3. El sistema que pide la autentificación **verifica** la autenticidad del usuario con el hash y el MD5. Lleva a cabo sus propios cálculos, si la verificación es correcta el enlace se **mantiene**, de lo contrario lo elimina y **termina** la conexión.

En intervalos aleatorios el sistema vuelve a pedir al router usuario que se autentifique nuevamente, con lo que el proceso arriba descrito se repite.

Como se ha visto, el protocolo punto a punto usa como base el HDLC.

¿Qué es el PPP?



HDLC es el método de encapsulación predeterminada entre los routers Cisco.



Usa la encapsulación PPP para conectarte a los routers que no son Cisco.

Ejemplo de *Point to Point Protocol*.

Maltez, A. (2011). *Ejemplo de Point to Point Protocol [Imagen]*.  
<http://adolfomaltez.wordpress.com/category/Cisco/>



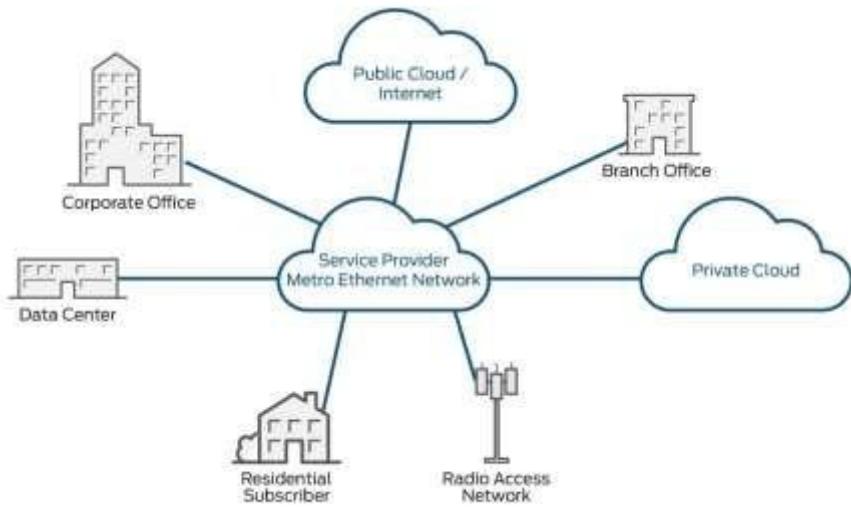
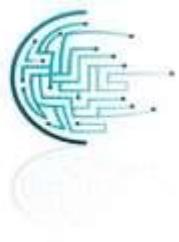
La figura anterior muestra el uso de un enlace con el protocolo punto a punto. Como se puede observar, sólo existen dos routers que se nombran **origen** y **destino**, la línea roja simboliza la **conexión** que existe entre los dos. El protocolo PPP se deberá usar siempre que no se conecten dos routers de Cisco, ya que el HDLC está patentado por dicha empresa,<sup>1</sup> y al conectarse con otros que no sean de la corporación se deberá utilizar el protocolo PPP.

### 2.2.3. Metro Ethernet

La creciente demanda de tecnologías que ofrecen mayores capacidades de ancho de banda y velocidades de transmisión más rápidas ha sido evidente. En las telecomunicaciones, el objetivo actual es unificar servicios como voz, datos y video en una red amplia de alta velocidad. Esta red debe tener la capacidad de transferir cualquier tipo de información, sin importar cuánto ancho de banda se requiera, y hacerlo de manera simple. Para lograr esto, se han desarrollado diversas tecnologías, como ATM (Modo de Transferencia Asíncrona), cableado de fibra y SDH (Jerarquía Digital Sincrónica), pero una solución innovadora e integradora que ha surgido en la actualidad es Metro Ethernet, que combina las redes locales (LAN) y las redes metropolitanas (WAN) de una manera revolucionaria.

Ethernet ha sido una de las tecnologías más influyentes para las redes de área local (LAN) y ahora se está preparando para su implementación en redes metropolitanas y de área amplia. Las actividades en los organismos de normalización reflejan el nuevo papel de Ethernet, a menudo denominada "metro o WAN Ethernet" (Brockers et. al, 2003).

El inicio de la tecnología Metro Ethernet se remonta a finales de la década de 1990 y principios de la década de 2000. Metro Ethernet es una tecnología de red que extiende los conceptos de Ethernet, utilizados en redes locales (LAN), a nivel metropolitano. Permite la construcción de redes de área metropolitana (MAN) de alto rendimiento y eficiencia.



Ejemplo de *Metro Ethernet*

Juniper. (2023). Ejemplo de Metro Ethernet [Imagen].

<https://www.juniper.net/mx/es/research-topics/what-is-metro-ethernet.html>

Metro Ethernet es una alternativa a la tecnología tradicional de multiplexación por división de tiempo (TDM). Aunque TDM se utiliza para entregar servicios de voz y de líneas arrendadas, es ineficiente para entregar las aplicaciones emergentes orientadas a datos. Los servicios Ethernet pueden ofrecer el servicio de línea punto a punto o servicios LAN multipunto a multipunto. Los servicios LAN conectan múltiples sitios que pertenecen a la misma empresa en diferentes ubicaciones físicas en una LAN virtual como si todos los sitios existieran en un edificio local (Huynh y Mohapatra, 2007).



*Beneficios de Metro Ethernet.*

Juniper. (2023). Beneficios de Metro Ethernet [Imagen].

<https://www.juniper.net/mx/es/research-topics/what-is-metro-ethernet.html>

Como se ha mencionado, HDLC, PPP son tecnologías WAN para enlaces **privados**. A continuación, se explicará un protocolo para enlaces **no privados**: DSL.

### 2.2.4. DSL

La línea digital del suscriptor DSL (*Digital Subscriber Line*) es un protocolo de interconectividad WAN, y además una serie de tecnologías que permite la transmisión de alta velocidad por medio de enlaces de cobre (Amaya, 2010).

Se dice que son una serie de tecnologías porque DSL **agrupa** más tecnologías; de hecho, como tecnología se le conoce como xDSL, donde la **x** indica a **todas** las agrupaciones que abarca. Las tecnologías DSL, según España (2003), son:

1. DSL
2. HDSL
3. SHDSL

Antes de entrar en detalle con cada una, es importante aclarar que todas estas técnicas tienen una característica en particular:

- Son técnicas de **transmisión** en la red de acceso, no va de extremo a extremo o de

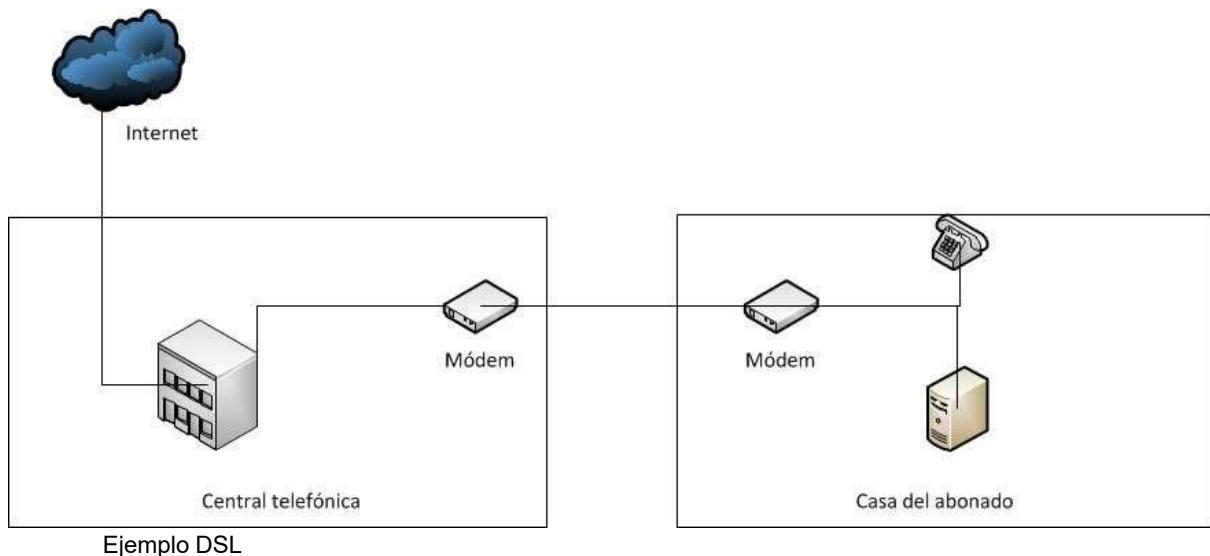


emisor a receptor directamente, sino que se sitúa un módem en la central local y otro con el **abonado** (manera en que se le llama comúnmente al usuario final); por ejemplo, el abonado en una red de Telmex sería el usuario que disfruta del servicio de telefonía e Internet, y la **central local** donde este cliente final se conecta. Estas centrales son sucursales que no están abiertas al público, se les denomina centrales locales, ahí se interconectan los usuarios más próximos, y dichas centrales a su vez se pueden conectar con una regional o con la principal; de manera que todas las centrales deben de estar **conectadas** y, por ende, todos los usuarios.

DSL: es el primero de los sistemas xDSL con el que es posible alcanzar velocidades de transmisión de 160 Kb/s sobre un sólo par de cables de cobre (España, 2003).

HDSL: línea de abonado digital de alta velocidad binaria (*High-bit rate Digital Subscriber Line*). Es el siguiente paso de DSL, es decir, es la evolución de DSL. Con ella es posible alcanzar **velocidades** de hasta **2048 Mb/s** con dos cables pares de cobre.

SHDSL: un sólo par de líneas de abonado digital de alta velocidad binaria (*Single pair High-bit rate Digital Subscriber Line*). Este es el siguiente paso de HDSL. Con un sólo par de cables de cobre se alcanzan las velocidades de HDSL.



En la figura anterior se muestra, a grandes rasgos, cómo se conecta una tecnología DSL con el abonado o cliente. En este esquema se presenta, por un lado, la central telefónica, y por el otro la casa de un abonado; éstos se **interconectan** a través de un módem.

Como se pudo observar, en este tema se dio una visión general de los protocolos que se usan para conexiones WAN, privados y públicos.



### 2.3. Enlaces WAN

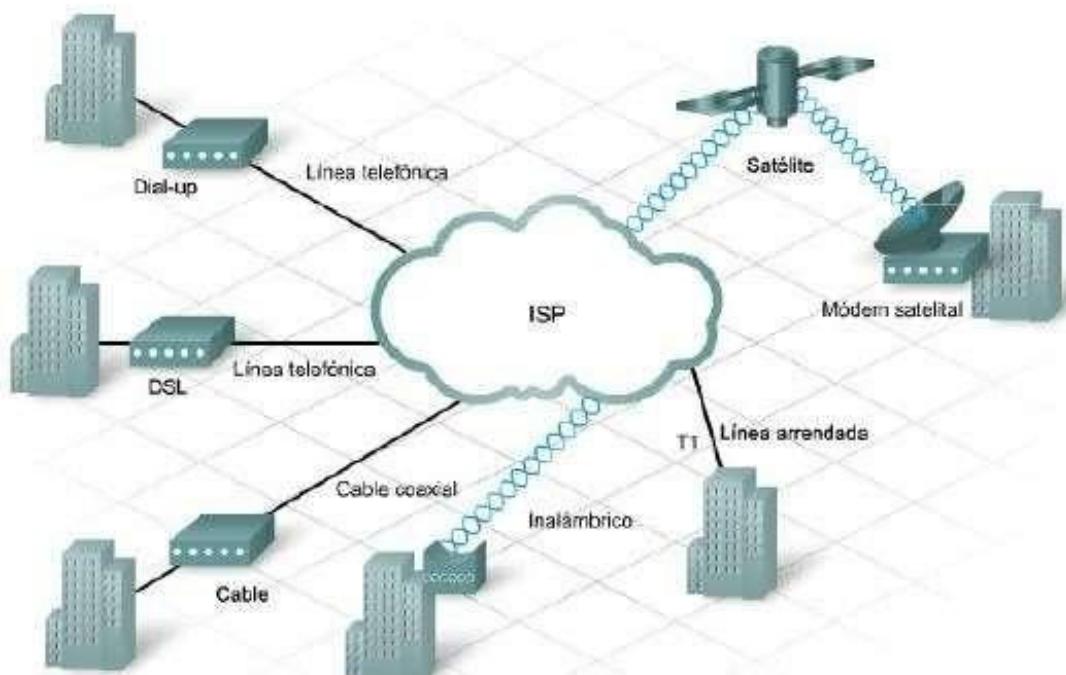
Un enlace WAN es la conexión física y lógica que existe entre dos equipos distantes, cada uno de ellos desde su red LAN (Dordogne, 2003). Las conexiones físicas son los medios de transmisión guiados y no guiados; por ejemplo, las conexiones guiadas pueden ser el cable de cobre y la fibra óptica; mientras que en las no guiadas se incluyen el Bluetooth, Wi-Fi, microondas.

Por conexiones lógicas se entiende los protocolos de interconexión tales como HDLC, PPP, Metro Ethernet, DSL que se revisaron a grandes rasgos en el tema anterior. Éstos definen el modo en el que el emisor y receptor van a trabajar en el proceso de la comunicación.

En el marco de interconectividad WAN, las conexiones físicas pueden ser cableadas o satelitales; mientras que las conexiones lógicas son los protocolos de interconectividad WAN mencionados anteriormente. A continuación, se explicará de qué manera se conectan físicamente las redes WAN.

#### 2.3.1. Tipos de uniones y conexiones

Hasta este momento se ha visto que los enlaces de interconectividad WAN pueden ser públicos o privados; además se revisaron los protocolos más comunes usados en ese tipo de conexiones. Las conexiones satelitales también forman parte de los tipos de enlaces WAN. En la siguiente figura se observa un ejemplo:



Ejemplo de enlaces más comunes WAN.

Cisco Systems. (2006). Ejemplo de enlaces más comunes WAN [Imagen]. <http://www.ie.itcr.ac.cr/egarcia/Presentaciones/Modulo3/Microsoft%20PowerPoint%20-%20Chapter7.pdf>



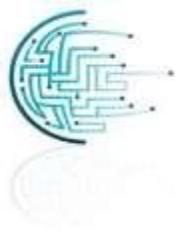
En la figura anterior se muestran los enlaces WAN más comunes, brevemente se explica a continuación cada uno de ellos (Cisco, 2006):

- **Dial-up:** este tipo de conexión ya no se usa, pero en ella era obligatorio el uso de un módem telefónico en las computadoras, el cual llamaba telefónicamente a otro módem con el fin de establecer la conexión a la red.
- **DSL:** ya se explicó que consiste en usar un par trenzado para las comunicaciones de datos. Esta tecnología fue la que desplazó a las conexiones Dial-up.
- **Cable:** en el diagrama anterior, la palabra **cable** se refiere a los proveedores de televisión de paga, ellos también pueden proveer el servicio de Internet.
- **Inalámbrico:** este tipo de conexión no se utiliza en México, pero un ejemplo de dicha tecnología es WiMax; para describir a grandes rasgos cómo funciona, es posible decir que se trata de una especie de Wi-Fi de largo alcance, el cual comúnmente sólo soporta algunos metros de distancia, pero el WiMax, kilómetros.
- **Línea arrendada:** son los tipos de enlace privados; es decir, un enlace dedicado es una línea arrendada que proveen un acceso a la WAN.
- **Satélite:** proveen enlaces inalámbricos a través de microondas, las cuales establecen la conectividad a la WAN.

Existe una relativamente *nueva* tecnología para conectarse a la WAN, o para la interconectividad de redes, la cual funciona mediante una red Ethernet. Una red LAN recibe el nombre de red Ethernet cuando se interconecta a través de cables de red; es decir, el cable de red UTP con el conector rj45. Este nombre se le quedó como legado, ya que a la tecnología de cablear con cables UTP a las computadoras se le conocía como Ethernet. Te preguntarás ¿qué tiene que ver una red LAN con una WAN? Pues en estos momentos la tecnología Ethernet, que sólo se usaba para entornos LAN, ya se puede emplear en redes WAN. A esta tecnología se le conoce como Metro Ethernet.

Metro Ethernet es una tecnología de red que está avanzando con rapidez, y que lleva Ethernet a las redes públicas mantenidas por empresas de telecomunicaciones. Utiliza switches Ethernet (soportan la tecnología de Metro Ethernet) que leen la información IP, y permiten a los proveedores ofrecer a las empresas servicios convergentes de voz, datos y video; por ejemplo, telefonía IP, streaming video, generación de imágenes y almacenamiento de datos. Al extender Ethernet a las áreas metropolitanas, las empresas pueden proporcionar a sus oficinas remotas un acceso confiable a las aplicaciones y los datos de la LAN de la sede principal corporativa (Cisco Systems, 2008a).

Podría existir confusión cuando se habla de WAN y redes metropolitanas. Te preguntarás si una red Metropolitana también es una MAN. La respuesta es sí (Metropolitan Area Network), pero actualmente los principales tipos de redes son dos: LAN y WAN. La primera abarca todas las redes de corto alcance, mientras que la segunda el largo.

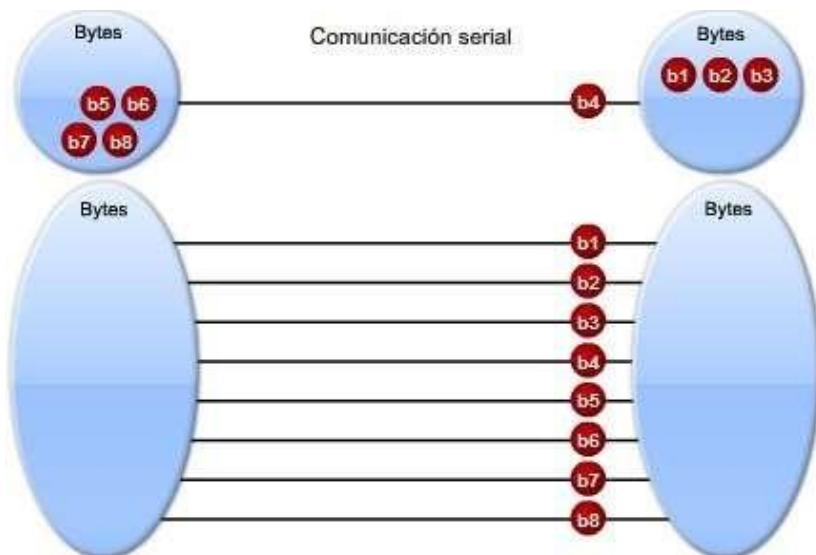


Como ya se observó, las redes WAN se llevan a cabo mediante el esquema de interconectividad. En la ilustración anterior se puede apreciar la interconectividad WAN a través de varios enlaces. Para crear o tener una red de este tipo es necesario que existan conexiones seriales en los enlaces, ya que éstos forman lo que se denomina su columna vertebral: Internet.

### 2.3.2. Conexiones seriales

Una de las conexiones WAN más frecuentes es la **punto a punto**. Ésta se utiliza para interconectar las LAN con la WAN del proveedor del servicio. A una conexión punto a punto también se le conoce como **serial** o **línea arrendada** (Cisco Systems, 2008a).

Esta **conexión serial** o **línea arrendada** se alquila con una empresa de telecomunicaciones, que por lo general es una compañía telefónica. Esta línea es para uso exclusivo y privado de quien la alquila. Se le conoce con dicho nombre porque envía los datos de manera serial.



Ejemplo de conexión serial y paralela.  
Cisco Systems. (2008b). Ejemplo de conexión serial y paralela [Imagen].

En el esquema anterior se observan dos diagramas, el de la parte superior se refiere a una conexión de tipo serial, mientras que el de la parte inferior se refiere a una conexión de tipo **paralelo**.

En una **conexión serial** se **envía** un bit de datos a la vez por medio del **único cable** que conecta a origen con destino. Como ejemplo de estas conexiones se tiene al conector de nueve pines que se usa en la mayoría de las computadoras. Es importante mencionar que a pesar de que el conector serial, al cual se le conoce también como db9, tenga nueve



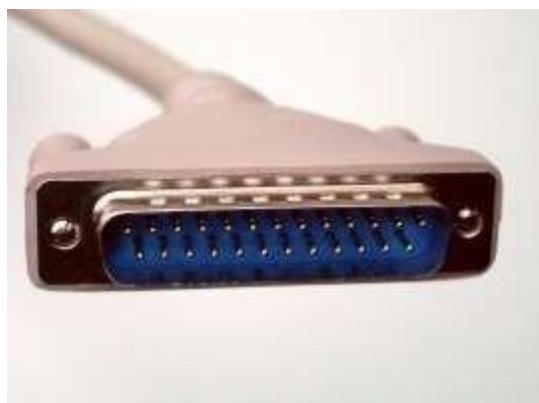
pinos y cables, sólo usa uno de éstos para transmitir información.



Ejemplo de cable db9

Mercado Libre. (s.f.). Ejemplo de cable DB9 [Imagen]. [http://articulo.mercadolibre.com.ve/MLV-415321205-extension-cable-db9-serial-18-metros-hembra-hembra-\\_JM?redirectedFromParent=MLV413001946](http://articulo.mercadolibre.com.ve/MLV-415321205-extension-cable-db9-serial-18-metros-hembra-hembra-_JM?redirectedFromParent=MLV413001946)

Con una **conexión paralela**, por el contrario, se envían más de un bit a la vez por medio de los cables que conectan a origen con destino. Como ejemplo de estas conexiones se tiene a los puertos y conectores de 25 pinos llamados puertos paralelos, conectores de cables paralelos, o db25, en alusión a sus 25 pinos, de los cuales se usan ocho para el envío de datos, los demás son para control y la energía del dispositivo conectado.



Ejemplo de conector db25

Wikipedia. (s.f.). Ejemplo de conector DB25 [Imagen].

Como se puede intuir, sería más rápida la transferencia de datos usando cables de 25 pinos que de nueve, ya que en un envío en conexión serial sólo se transmite un bit; por el contrario, en una conexión serial en un envío se transmite un byte (ocho bits). La afirmación anterior se hace considerando una situación ideal; es decir, en una situación sin problemas. Existen dos conceptos que se revisarán a continuación, los cuales son alteraciones que afectan a la transmisión.



**Sesgo de reloj:** se refiere al **retraso** existente en el envío de bits de origen a destino; éste existe porque los bits no se envían al mismo tiempo. Desde la fuente los bits se irán generando uno a uno, y cada que se genere uno se envía (Cisco Systems, 2008a).

**Interferencia:** se refiere al ruido que se genera en el ambiente y afecta a los bits enviados entre origen y destino. Por **ruido** deberá entenderse todas las **ondas** que afectan al mensaje original. Una manera de ejemplificar esto es cuando una persona habla con otra; en un ambiente ideal no existirá ningún otro sonido que interfiera la comunicación, pero existe la plática de otras personas, el ruido de algún carro, música, etcétera.

Actualmente ya no se usan las conexiones paralelas, esto debido a los problemas de interferencia que se mencionaron anteriormente. Lo que usa en la actualidad son las conexiones seriales, más eficientes porque no son tan susceptibles a las interferencias ni a los sesgos de reloj, como pasa en las comunicaciones paralelas.

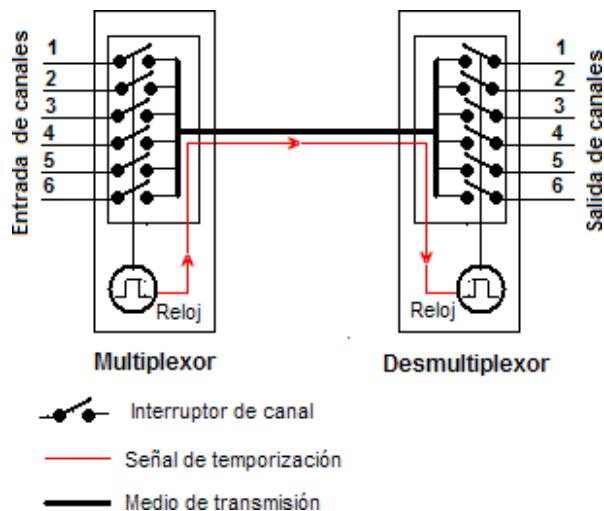
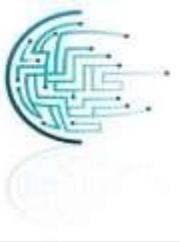
Aunque las conexiones seriales son más eficientes que las paralelas, se ha buscado mejorar este tipo de comunicaciones; ejemplo de ello es la tecnología denominada TDM, la cual se verá a continuación.

### 2.3.3 TDM

La multiplexación por división de tiempo TDM (*Time Division Multiplexing*) es una tecnología que **optimiza** el uso de un enlace (Cisco Systems, 2008a). La multiplexación consiste en combinar los canales de información en uno solo, y así enviar dos o más señales diferentes a través de un único medio de transmisión.

TDM permite transmitir varias señales simultáneamente si las distintas partes de cada una de ellas se entremezclan. Este método se puede realizar empleando señales de cada señal de un bit o de bytes (ocho bits). Al número de bits que constituyen estos bloques o porciones de señal se les llama **ranuras temporales**; así cada trama enviada por el medio consta de un conjunto de ranuras temporales (Gil, Pomares y Candelas, 2010).

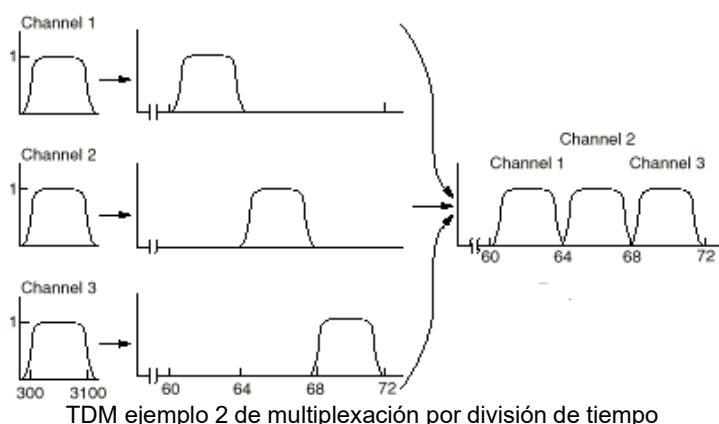
En otras palabras, TDM es una tecnología que mezcla señales de varias fuentes para mandarlas por un único medio. Imagina que las fuentes de información son unas llaves de agua, y el medio por el que se van a transmitir es un río, toda el agua que las llaves sacan será enviada por el río, y una vez el río llegue al destino, tendría diferentes caminos por los cuales el agua se irá.



TDM ejemplo 1 de multiplexación por división de tiempo.

Wikipedia. (2013). TDM ejemplo 1 de multiplexación por división de tiempo [Imagen].  
<http://upload.wikimedia.org/wikipedia/commons/e/e7/Multiplexor.png>

En la figura anterior se observan dos equipos: un multiplexor y un desmultiplexor. El primero **canaliza** (junta) las entradas que tiene (lo que está etiquetado como entrada de canales); es decir, **une** lo que entra por cada canal y lo **envía** a través del medio de transmisión; éste **interconecta** el multiplexor con el desmultiplexor, el cual se encarga de descanalizar (separar) las entradas para **entregar** los datos tal como los **recibió** a la entrada el multiplexor. De tal manera, la entrada 1 deberá ser la salida 1, la entrada 2 será la salida 2, y así sucesivamente hasta que todas las **entradas** tengan su **salida**.



En el esquema anterior se muestra otra manera de enviar la información multiplexada por división de tiempo. Supón que el eje x está en términos de tiempo, mientras que el de las y es la información que se envía, en este supuesto, cada cresta que representa un período de tiempo [las curvas del tiempo de la gráfica 3 (Channel 3) 68 al 72, de la gráfica 2 (Channel 2) 64 al 68 y de la gráfica 1 (Channel 1) 60 al 64; es la información que se **envía** desde diferentes fuentes, Gráfica 1 (Channel 1), Gráfica 2 (Channel 2) y Gráfica 3 (Channel 3)].



Como puede observarse cada gráfica o canal sólo usa **un tiempo**, y deja los demás sin usar. Cuando se multiplexan estos canales se envía la información de los tres por un mismo medio; de esta manera se **optimiza** el enlace entre emisor y receptor. El resultado de esta multiplexación se puede observar del lado derecho de la misma gráfica. Se metió al mismo enlace (o en la gráfica, en este caso) la información de los canales 1, 2 y 3.

Un ejemplo de TDM es la red de celulares. Seguramente has visto las antenas de las principales compañías celulares, existen en muchas partes. A este tipo de antenas se les denomina **radio bases**, usan TDM que **multiplexa** todas las señales de todas las llamadas hechas en una radio base, a la cual se **conectan** varios usuarios a través de su teléfono móvil. Cuando se realiza una llamada, la radio base la multiplexa y la **envía** sobre un sólo canal a la central telefónica, de manera tal que **viaja** a través de un enlace que proporciona dicha radio base, lo cual hace posible **comunicarse** con otros usuarios a través de la red celular.

La multiplexación ayuda a **optimizar** y aprovechar al máximo una conexión serial, pero ésta no tiene sentido si no se usan dispositivos DTE/DCE para que la información que se transmite sea **entendible** para los dispositivos finales. Se explicará a continuación que es un DTE y un DCE.

### 2.3.4 DTE y DCE

Los equipos terminales de datos DTE (*Data Terminal Equipment*) y los de comunicación de datos DCE (*Distributed Computing Environment*) juegan un papel muy importante en la interconexión de redes, en este caso para las redes WAN.

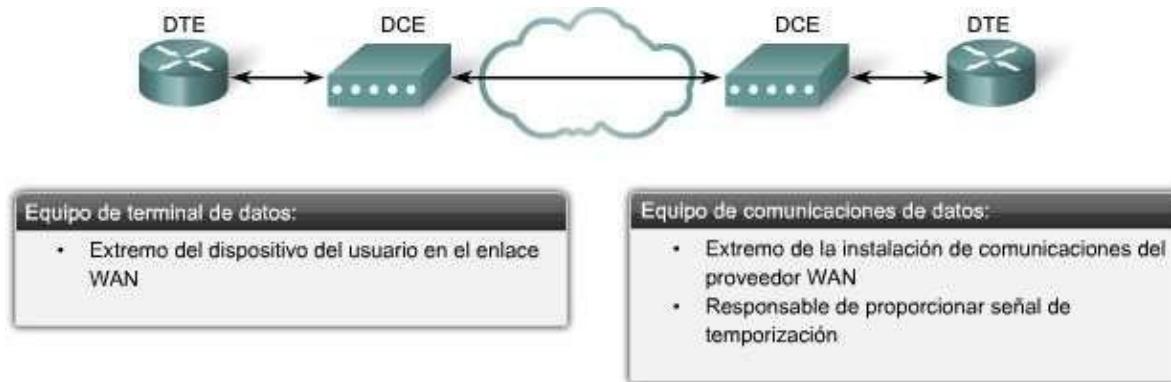
DCE es un **equipo de comunicación de datos**, como su nombre lo indica, que proporciona una **conexión física** con la red, **envía** tráfico de datos y **suministra** una señal de reloj que se usa para sincronizar el envío entre DTE y DCE. Ejemplos de estos equipos son los módems, o las tarjetas de interfaz de red, de los dispositivos DTE (CiscoSystems, 2008a). Un equipo terminal de datos (DTE) está situado en el **extremo** del usuario que actúa como origen o destino (Cisco Systems, 2008a).

Un DCE es un equipo que se utiliza para **convertir** los datos del usuario del DTE en una forma que sea aceptable para transmitir a través de la red WAN.

Un ejemplo de equipos DCE son los routers o módems (como los que entrega Telmex y los operadores de cable que proporcionan servicios de triple play). Ejemplo de DTE son las computadoras, laptop, Tablet, etcétera. Como te puedes dar cuenta, los conceptos DTE y DCE son muy similares a los equipos terminales e intermedios de red, respectivamente. Entonces te preguntarás, ¿Por qué se usa otra terminología? Un DTE no siempre será una PC o laptop,



pero sí el equipo inmediato que se encuentra después del DCE.



Cisco Systems. (2008b).

Cisco Systems. (2008b). Ejemplo de dispositivos DCE y DTE y su conectividad a través de la WAN [Imagen].

Como se observa en la figura anterior, los DCE se encuentran directamente conectados a través de la WAN que en el esquema está representada por la **nube**, la cual en los esquemas de redes siempre simboliza **redes** que no se conocen o que no son relevantes en la explicación del esquema. El DCE debe ser capaz de poder **enviar** datos a través de la WAN; es decir, debe entender protocolos de envío WAN como por ejemplo PPP, HDLC, etcétera.

El equipo DTE mostrado en el esquema anterior corresponde a un router (la simbología usada es la común en diagramas de red), que es el origen y destino para enviar y recibir los datos. Funge como origen de datos ya que, comúnmente en esta arquitectura, un router es el gateway de una red, que es la **salida** para todos los dispositivos de la red; gracias éste se tiene conectividad a Internet. En otras palabras, aunque una computadora sea el origen del envío/recepción, no puede enviar ni recibir datos directamente, ya que no tiene una IP que pueda ser usada en Internet sino una privada, que sólo sirve para tener conectividad en la Intranet o en la red interna.

Como se ha podido observar, DCE y DTE son los equipos que permiten que haya comunicación a través de una red WAN. Todo lo visto en esta unidad, esta interrelacionado para crear la interconectividad de redes de área extensa WAN.



### Cierre de la unidad

En esta unidad se expuso, a grandes rasgos, el modo de funcionamiento y los equipos que se requieren para exista una interconectividad de redes. Se explicaron los elementos, así como los protocolos de uso común en redes y enlaces WAN. Te preguntarás ¿de qué me sirve cómo futuro ingeniero de software, el saber sobre interconectividad de redes WAN? Pues simplemente porque las aplicaciones que vas a desarrollar o crear, seguramente funcionarán en redes de este tipo. El ejemplo más común de una red WAN es Internet; por ello es muy importante que tengas una idea de cómo funcionan y puedas, en caso de ser necesario, cómo solucionar problemas que se puedan presentar por el hecho de usarlas.

La seguridad en el uso de las redes es un tema que cobra importancia en todo momento, debido a que éstas son un medio muy práctico de transmisión de información que puede ser confidencial, o que simplemente no se debe compartir a niveles públicos; ante ello, en la tercera unidad abordarás los temas que te permitirán saber cómo se puede realizar una interconectividad de redes en forma segura.

### Para saber más

Si deseas informarte más sobre la aplicación de las redes informáticas, puedes visitar los siguientes sitios:

- Rivera Rodríguez, R., Tamayo Fernández, R., Serrano Santoyo, A., y Armenta Ramade, A., (2011). *Sistema móvil de teleasistencia médica para la atención en tiempo real de casos de urgencia*. México: UNAM Revista de Ingeniería Investigación y Tecnología.  
<https://www.redalyc.org/articulo.oa?id=4042321001>
- Biga, D. R. (2020, marzo 11). VPNs (Virtual private networks).  
<https://repositoriocyt.unlam.edu.ar/handle/123456789/430>
- Mercado Manga, J. F. Solución de dos Escenarios Presentes en Entornos Corporativos Bajo uso de la Tecnología CISCO.  
<https://repository.unad.edu.co/handle/10596/35459>

Puedes consultar otros artículos sobre el uso de las redes en el portal editorial de la Facultad de Ingeniería de la UNAM. En el sitio de Publicaciones recientes que puedes localizar en esta dirección:

<http://www.ingenieria.unam.mx/>



### Fuentes de consulta

#### Fuentes Básicas

- Amaya, J. (2010). *Sistemas de información Gerencial*. Bogotá: Ecoe.
- Blanco, A., Huidobro, J. y Jordán, J. (2008). *Redes de área local: administración de sistemas informáticos*. Madrid: Paraninfo. <https://tinyurl.com/y2wowo5>
- Brockners, F., Finn, N. y Phillips, S. (2003) "Metro Ethernet: implementación del campus extendido utilizando tecnología Ethernet", 28.<sup>a</sup> Conferencia internacional anual de IEEE sobre redes informáticas locales. doi: 10.1109/LCN.2003.1243186
- Cisco. (2012). *Contact Cisco*. [https://www.cisco.com/c/dam/assets/cdc\\_content\\_elements/docs/annualreports/ar2012.pdf](https://www.cisco.com/c/dam/assets/cdc_content_elements/docs/annualreports/ar2012.pdf)
- Cisco. (2008a). *CCNA Exploration 4.0: acceso a la WAN*. Pennsylvania: CISCO.
- Cisco Systems (2008b). CCNA Exploration 4.0: Acceso a la WAN tema 3.1.1 Introducción a la tecnología Frame Relay.
- Cisco. (2006). *Introducción al enrutamiento y la conmutación de la empresa*. <https://fdocuments.mx/document/-2006-cisco-systems-inc-todos-los-derechos-reservadosinformacion-publica-de-cisco-1-conmutacion-de-una-red-empresarial-introduccion-al-enrutamiento.html>
- Cobo, A. (2005). *Estudio científico de las redes de ordenadores*. Madrid: Visión Libros.
- Dordogne, J. (2003). *Windows XP profesional: preparación para el examen MCSE, MCSA. Números 70-270*. Barcelona. ENI Ediciones.
- España, M. (2003). *Servicios avanzados de telecomunicación*. Madrid: Ediciones Díaz de Santos.
- Forouzan, B. (2003). *Introducción a la ciencia de la computación: de la manipulación de datos a la teoría de la computación*. México: International Thompson.
- Gil, P., Pomares, J. y Candelas, F. (2010). *Redes y transmisión de datos*. Alicante: Universidad de Alicante.
- Huynh, M. y Mohapatra, P. (2007). Red Ethernet Metropolitana: un paso de LAN a MAN. Redes de Computadoras. <https://doi.org/10.1016/j.comnet.2007.08.001>



- Laporta, J. (2005). *Fundamentos de telemática*. Valencia: Universidad Politécnica de Valencia.
- Latorre, H. (2013). *Protocolo HDLC*.  
[http://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/28691/Redes\\_Cap06.pdf?sequence=6&isAllowed=y](http://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/28691/Redes_Cap06.pdf?sequence=6&isAllowed=y)
- Microsoft (2005). *Windows Server. Cifrado de datos*.  
<http://technet.microsoft.com/es-es/library/cc785633%28v=ws.10%29.aspx>
- Rivera, R., Tamayo, R., Serrano, A. y Armenta, A. (2011). Sistema móvil de teleasistencia médica para la atención en tiempo real de casos de urgencia. México. *Revista de Ingeniería Investigación y Tecnología*.  
<https://www.redalyc.org/articulo.oa?id=40423210001>
- Stallings, W. (2004). *Comunicaciones y redes de computadores*. Madrid: Pearson educación.
- Tanenbaum, A. (2003). *Redes de computadoras*. México: Pearson Educación.