

# CAPITULO 9 Ethernet

## 9.0 Introducción del capítulo

### 9.0.1 Introducción del capítulo

Hasta este punto del curso, cada capítulo se concentró en las diferentes funciones de cada una de las capas de los modelos OSI y de protocolo TCP/IP, y en cómo se utilizan los protocolos para lograr la comunicación de red. Estos análisis hacen referencia constantemente a diversos protocolos clave (TCP, UDP e IP), ya que brindan las bases sobre cómo funcionan actualmente desde la red más pequeña hasta la red más grande, la Internet. Estos protocolos comprenden el stack de protocolos TCP/IP y, dado que la Internet se creó utilizando dichos protocolos, Ethernet es en la actualidad la tecnología LAN preponderante a nivel mundial.

El grupo de trabajo de ingeniería de Internet (IETF) mantiene los protocolos y servicios funcionales para la suite de protocolos TCP/IP de las capas superiores. Sin embargo, diversas organizaciones especializadas en ingeniería (IEEE, ANSI, ITU) o empresas privadas (protocolos propietarios) describen los protocolos y servicios funcionales de la capa de Enlace de datos y la capa física del modelo OSI. Dado que Ethernet se compone de estándares en estas capas inferiores, puede decirse que en términos generales se entiende mejor con referencia al modelo OSI. El modelo OSI separa las funcionalidades de la capa de Enlace de datos de direccionamiento, entramado y acceso a los medios desde los estándares de la capa física de los medios. Los estándares de Ethernet definen los protocolos de Capa 2 y las tecnologías de Capa 1. Si bien las especificaciones de Ethernet admiten diferentes medios, anchos de banda y otras variaciones de Capa 1 y 2, el formato de trama básico y el esquema de direcciones son los mismos para todas las variedades de Ethernet.

Este capítulo analiza las características y el funcionamiento de la Ethernet en términos de su evolución desde una tecnología de medios compartidos de comunicación de datos basada en contenciones hasta convertirse en la actual tecnología full-duplex de gran ancho de banda.

### Objetivos de aprendizaje

Al completar este capítulo, podrá realizar lo siguiente:

- Describir la evolución de Ethernet.
- Explicar los campos de la trama de Ethernet.
- Describir la función y las características del método de control de acceso a los medios utilizado por el protocolo Ethernet.
- Describir las funciones de la capa física y de la capa de enlace de datos de Ethernet.
- Comparar y contrastar los hubs y switches de Ethernet.
- Explicar el Protocolo de resolución de direcciones (ARP).



Ethernet es la tecnología LAN predominante en uso hoy en día.

# 9.1 Descripción general de Ethernet

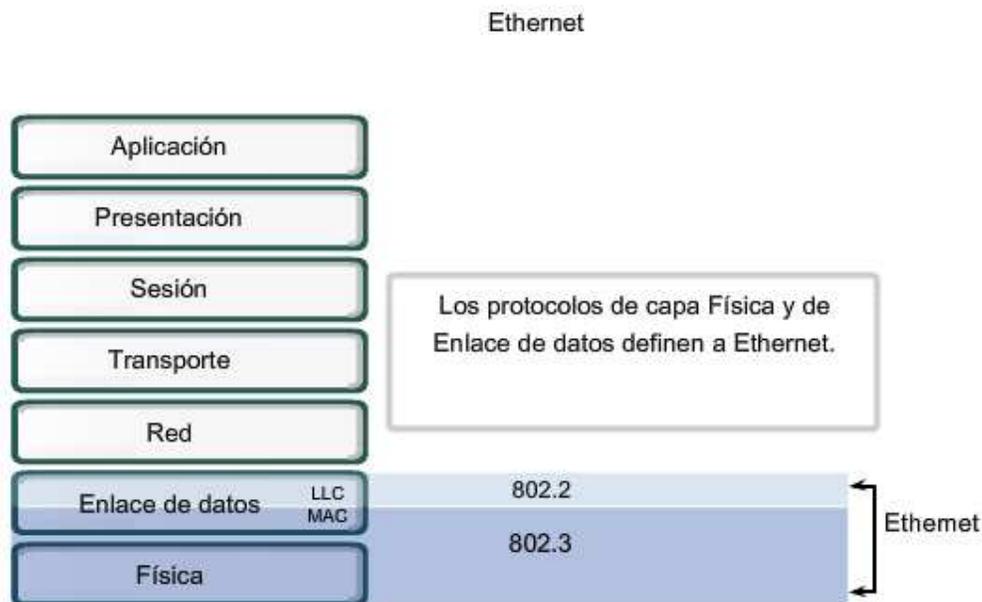
## 9.1.1 Ethernet: estándares e implementación

### Estándares de IEEE

La primera LAN (Red de área local) del mundo fue la versión original de Ethernet. Robert Metcalfe y sus compañeros de Xerox la diseñaron hace más de treinta años. El primer estándar de Ethernet fue publicado por un consorcio formado por Digital Equipment Corporation, Intel y Xerox (DIX). Metcalfe quería que Ethernet fuera un estándar compartido a partir del cual todos se podían beneficiar, de modo que se lanzó como estándar abierto. Los primeros productos que se desarrollaron a partir del estándar de Ethernet se vendieron a principios de la década de 1980.

En 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN. Estos estándares comienzan con el número 802. El estándar para Ethernet es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con los del modelo OSI de la Organización Internacional para la Estandarización (ISO). Para garantizar la compatibilidad, los estándares IEEE 802.3 debían cubrir las necesidades de la Capa 1 y de las porciones inferiores de la Capa 2 del modelo OSI. Como resultado, ciertas pequeñas modificaciones al estándar original de Ethernet se efectuaron en el 802.3.

Ethernet opera en las dos capas inferiores del modelo OSI: la capa de enlace de datos y la capa física.



### 9.1.2 Ethernet: Capa 1 y Capa 2

Ethernet opera a través de dos capas del modelo OSI. El modelo ofrece una referencia sobre con qué puede relacionarse Ethernet, pero en realidad se implementa sólo en la mitad inferior de la capa de Enlace de datos, que se conoce como subcapa Control de acceso al medio (Media Access Control, MAC), y la capa física.

Ethernet en la Capa 1 implica señales, streams de bits que se transportan en los medios, componentes físicos que transmiten las señales a los medios y distintas topologías. La Capa 1 de Ethernet tiene un papel clave en la comunicación que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones.

Tal como lo muestra la figura, Ethernet en la Capa 2 se ocupa de estas limitaciones. Las subcapas de enlace de datos contribuyen significativamente a la compatibilidad de tecnología y la comunicación con la computadora. La subcapa MAC se ocupa de los componentes físicos que se utilizarán para comunicar la información y prepara los datos para transmitirlos a través de los medios.

La subcapa Control de enlace lógico (Logical Link Control, LLC) sigue siendo relativamente independiente del equipo físico que se utilizará para el proceso de comunicación.

## Direcciones de la Capa 2 Limitaciones de la Capa 1

Limitaciones de la Capa 1	Funciones de la Capa 2
No se puede comunicar con capas superiores	Se conecta con las capas superiores mediante control de enlace lógico (LLC)
No pueden identificar dispositivos	Utiliza esquemas de direccionamiento para identificar dispositivos
Sólo reconoce streams de bits	Utiliza tramas para organizar los bits en grupos
No puede determinar la fuente de la transmisión cuando transmiten múltiples dispositivos	Utiliza control de acceso al medio (MAC) para identificar fuentes de transmisión

### 9.1.3 Control de enlace lógico: Conexión con las capas superiores

Ethernet separa las funciones de la capa de Enlace de datos en dos subcapas diferenciadas: la subcapa Control de enlace lógico (LLC) y la subcapa Control de acceso al medio (MAC). Las funciones descritas en el modelo OSI para la capa de Enlace de datos se asignan a las subcapas LLC y MAC. La utilización de dichas subcapas contribuye notablemente a la compatibilidad entre diversos dispositivos finales.

Para Ethernet, el estándar IEEE 802.2 describe las funciones de la subcapa LLC y el estándar 802.3 describe las funciones de la subcapa MAC y de la capa física. El Control de enlace lógico se encarga de la comunicación entre las capas superiores y el software de red, y las capas inferiores, que generalmente es el hardware. La subcapa LLC toma los datos del protocolo de la red, que generalmente son un paquete IPv4, y agrega información de control para ayudar a entregar el paquete al nodo de destino. La Capa 2 establece la comunicación con las capas superiores a través del LLC.

El LLC se implementa en el software y su implementación depende del equipo físico. En una computadora, el LLC puede considerarse como el controlador de la Tarjeta de interfaz de red (NIC). El controlador de la NIC (Tarjeta de interfaz de red) es un programa que interactúa directamente con el hardware en la NIC para pasar los datos entre los medios y la subcapa de Control de Acceso al medio (MAC).

<http://standards.ieee.org/getieee802/download/802.2-1998.pdf>

<http://standards.ieee.org/regauth/llc/llctutorial.html>

[http://www.wildpackets.com/support/compendium/reference/sap\\_numbers](http://www.wildpackets.com/support/compendium/reference/sap_numbers)

## Control de enlace lógico (LLC)

- Establece la conexión con las capas superiores
- Entrama el paquete de la capa de Red
- Identifica el protocolo de capa de Red
- Permanece relativamente independiente del equipo físico



### 9.1.4 MAC: envío de datos a los medios

El Control de acceso al medio (MAC) es la subcapa de Ethernet inferior de la capa de Enlace de datos. El hardware implementa el Control de acceso al medio, generalmente en la Tarjeta de interfaz de red (NIC).

La subcapa MAC de Ethernet tiene dos responsabilidades principales:

- Encapsulación de datos
- Control de Acceso al medio

#### Encapsulación de datos

La encapsulación de datos proporciona tres funciones principales:

- Delimitación de trama
- Direccionamiento
- Detección de errores

El proceso de encapsulación de datos incluye el armado de la trama antes de la transmisión y el análisis de la trama al momento de recibir una trama. Cuando forma una trama, la capa MAC agrega un encabezado y un tráiler a la PDU de Capa 3. La utilización de tramas facilita la transmisión de bits a medida que se colocan en los medios y la agrupación de bits en el nodo receptor.

El proceso de entramado ofrece delimitadores importantes que se utilizan para identificar un grupo de bits que componen una trama. Este proceso ofrece una sincronización entre los nodos transmisores y receptores.

El proceso de encapsulación también posibilita el direccionamiento de la capa de Enlace de datos. Cada encabezado Ethernet agregado a la trama contiene la dirección física (dirección MAC) que permite que la trama se envíe a un nodo de destino.

Una función adicional de la encapsulación de datos es la detección de errores. Cada trama de Ethernet contiene un tráiler con una comprobación cíclica de redundancia (CRC) de los contenidos de la trama. Una vez que se recibe una trama, el nodo receptor crea una CRC para compararla con la de la trama. Si estos dos cálculos de CRC coinciden, puede asumirse que la trama se recibió sin errores.

#### Control de acceso al medio

La subcapa MAC controla la colocación de tramas en los medios y el retiro de tramas de los medios. Como su nombre lo indica, se encarga de administrar el control de acceso al medio. Esto incluye el inicio de la transmisión de tramas y la recuperación por fallo de transmisión debido a colisiones.

## Topología lógica

La topología lógica subyacente de Ethernet es un bus de multiacceso. Esto significa que todos los nodos (dispositivos) en ese segmento de la red comparten el medio. Esto significa además que todos los nodos de ese segmento reciben todas las tramas transmitidas por cualquier nodo de dicho segmento.

Debido a que todos los nodos reciben todas las tramas, cada nodo debe determinar si debe aceptar y procesar una determinada trama. Esto requiere analizar el direccionamiento en la trama provisto por la dirección MAC.

Ethernet ofrece un método para determinar cómo comparten los nodos el acceso al medio. El método de control de acceso a los medios para Ethernet clásica es el Acceso múltiple con detección de portadora con detección de colisiones (CSMA/CD). Este método se describe más adelante en este capítulo.

<http://standards.ieee.org/regauth/groupmac/tutorial.html>

### MAC—Llevar datos a los medios



## 9.1.5 Implementaciones físicas de Ethernet

La mayor parte del tráfico en Internet se origina y termina en conexiones de Ethernet. Desde su inicio en la década de 1970, Ethernet ha evolucionado para satisfacer la creciente demanda de LAN de alta velocidad. Cuando se introdujo el medio de fibra óptica, Ethernet se adaptó a esta nueva tecnología para aprovechar el mayor ancho de banda y el menor índice de error que ofrece la fibra. Actualmente, el mismo protocolo que transportaba datos a 3 Mbps puede transportar datos a 10 Gbps.

El éxito de Ethernet se debe a los siguientes factores:

- Simplicidad y facilidad de mantenimiento
- Capacidad para incorporar nuevas tecnologías
- Confiabilidad
- Bajo costo de instalación y de actualización

La introducción de Gigabit Ethernet ha extendido la tecnología LAN original a distancias tales que convierten a Ethernet en un estándar de Red de área metropolitana (MAN) y de WAN (Red de área extensa).

Ya que se trata de una tecnología asociada con la capa física, Ethernet especifica e implementa los esquemas de codificación y decodificación que permiten el transporte de los bits de trama como señales a través de los medios. Los dispositivos Ethernet utilizan una gran variedad de especificaciones de cableado y conectores.

En las redes actuales, la Ethernet utiliza cables de cobre UTP y fibra óptica para interconectar dispositivos de red a través de dispositivos intermediarios como hubs y switches. Dada la diversidad de tipos de medios que Ethernet admite, la estructura de la trama de Ethernet permanece constante a través de todas sus implementaciones físicas. Es por esta razón que puede evolucionar hasta cumplir con los requisitos de red actuales.

## Dispositivos físicos que implementan Ethernet



Patch panels UTP en un bastidor



Switches Ethernet



Conectores de fibra Ethernet



Switch Ethernet

## 9.2 Ethernet: comunicación a través de LAN

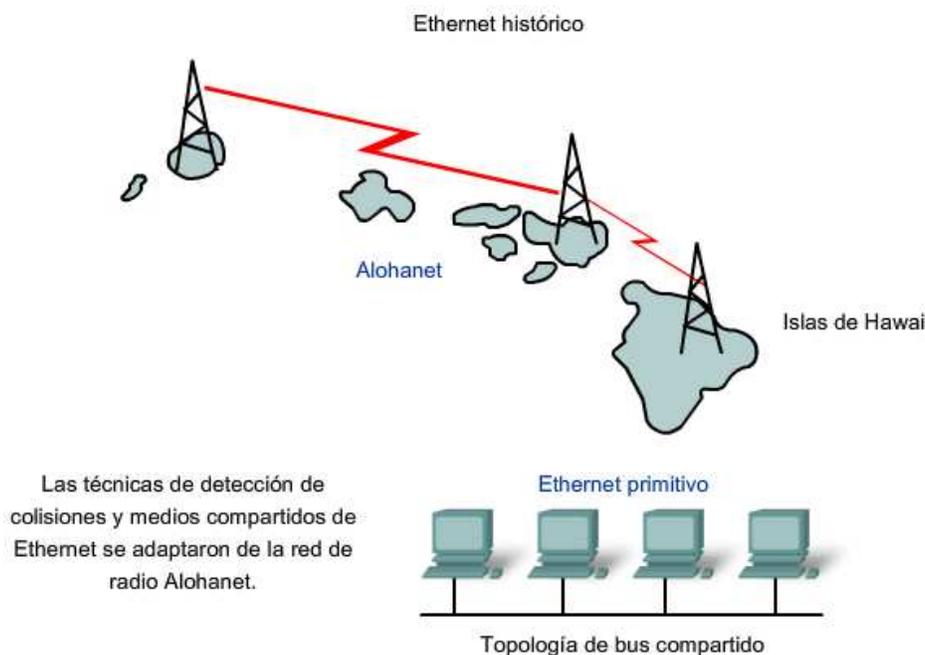
### 9.2.1 Ethernet histórica

Los cimientos de la tecnología Ethernet se fijaron por primera vez en 1970 mediante un programa llamado Alohanet. Alohanet era una red de radio digital diseñada para transmitir información por una frecuencia de radio compartida entre las Islas de Hawai.

Alohanet obligaba a todas las estaciones a seguir un protocolo según el cual una transmisión no reconocida requería una retransmisión después de un período de espera breve. Las técnicas para utilizar un medio compartido de esta manera se aplicaron posteriormente a la tecnología cableada en forma de Ethernet.

La Ethernet se diseñó para aceptar múltiples computadoras que se interconectaban en una topología de bus compartida.

La primera versión de Ethernet incorporaba un método de acceso al medio conocido como Acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD). El CSMA/CD administraba los problemas que se originaban cuando múltiples dispositivos intentaban comunicarse en un medio físico compartido.



## Primeros medios Ethernet

Las primeras versiones de Ethernet utilizaban cable coaxial para conectar computadoras en una topología de bus. Cada computadora se conectaba directamente al backbone. Estas primeras versiones de Ethernet se conocían como Thicknet (10BASE5) y Thinnet (10BASE2).

La 10BASE5, o Thicknet, utilizaba un cable coaxial grueso que permitía lograr distancias de cableado de hasta 500 metros antes de que la señal requiriera un repetidor. La 10BASE2, o Thinnet, utilizaba un cable coaxial fino que tenía un diámetro menor y era más flexible que la Thicknet y permitía alcanzar distancias de cableado de 185 metros.

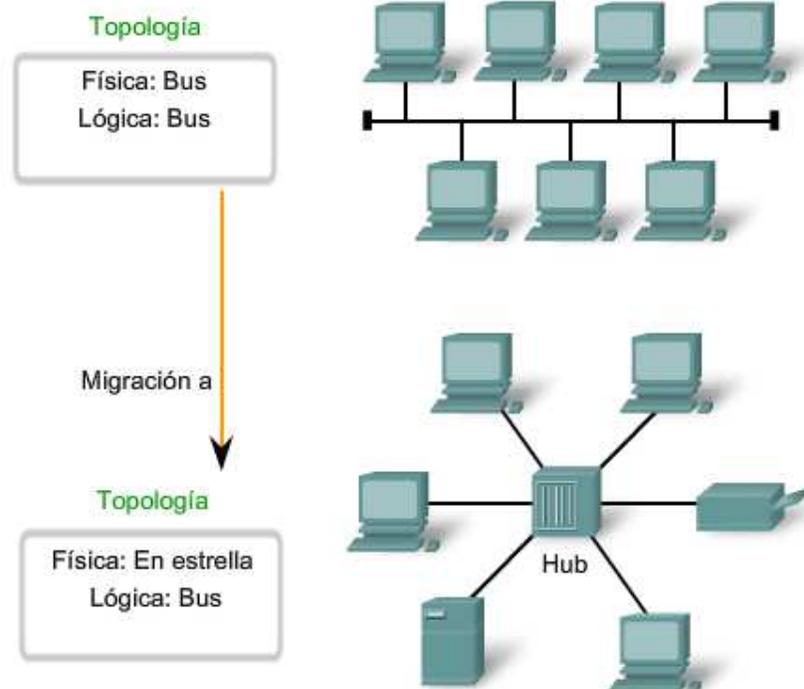
La capacidad de migrar la implementación original de Ethernet a las implementaciones de Ethernet actuales y futuras se basa en la estructura de la trama de Capa 2, que prácticamente no ha cambiado. Los medios físicos, el acceso al medio y el control del medio han evolucionado y continúan haciéndolo. Pero el encabezado y el tráiler de la trama de Ethernet han permanecido constantes en términos generales.

Las primeras implementaciones de Ethernet se utilizaron en entornos LAN de bajo ancho de banda en los que el acceso a los medios compartidos se administraba mediante CSMA y, posteriormente, mediante CSMA/CD. Además de ser una topología de bus lógica de la capa de Enlace de datos, Ethernet también utilizaba una topología de bus física. Esta topología se volvió más problemática a medida que las LAN crecieron y que los servicios LAN demandaron más infraestructura.

Los medios físicos originales de cable coaxial grueso y fino se reemplazaron por categorías iniciales de cables UTP. En comparación con los cables coaxiales, los cables UTP eran más fáciles de utilizar, más livianos y menos costosos.

La topología física también se cambió por una topología en estrella utilizando hubs. Los hubs concentran las conexiones. En otras palabras, toman un grupo de nodos y permiten que la red los trate como una sola unidad. Cuando una trama llega a un puerto, se lo copia a los demás puertos para que todos los segmentos de la LAN reciban la trama. La utilización del hub en esta topología de bus aumentó la confiabilidad de la red, ya que permite que cualquier cable falle sin provocar una interrupción en toda la red. Sin embargo, la repetición de la trama a los demás puertos no solucionó el problema de las colisiones. Más adelante en este capítulo se verá cómo se manejaron las cuestiones relacionadas con colisiones en Ethernet mediante la introducción de switches en la red.

Topología y primeros medios de Ethernet



## 9.2.2 Administración de colisiones en Ethernet

## Ethernet antigua

En redes 10BASE-T, el punto central del segmento de red era generalmente un hub. Esto creaba un medio compartido. Debido a que el medio era compartido, sólo una estación a la vez podía realizar una transmisión de manera exitosa. Este tipo de conexión se describe como comunicación half-duplex.

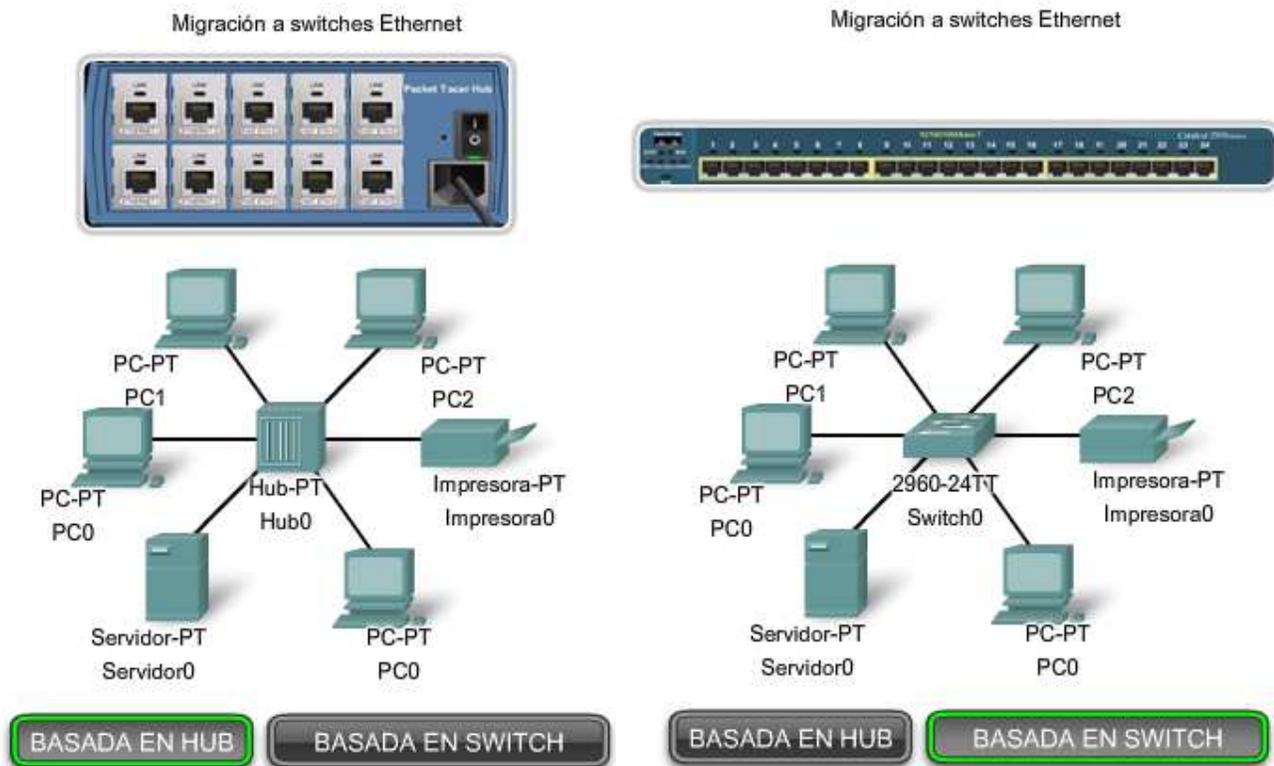
A medida que se agregaban más dispositivos a una red Ethernet, la cantidad de colisiones de tramas aumentaba notablemente. Durante los períodos de poca actividad de comunicación, las pocas colisiones que se producían se administraban mediante el CSMA/CD, con muy poco impacto en el rendimiento, en caso de que lo hubiera. Sin embargo, a medida que la cantidad de dispositivos y el consiguiente tráfico de datos aumenta, el incremento de las colisiones puede producir un impacto significativo en la experiencia del usuario.

A modo de analogía, sería similar a cuando salimos a trabajar o vamos a la escuela a la mañana temprano y las calles están relativamente vacías. Más tarde, cuando hay más automóviles en las calles, pueden producirse colisiones y generar demoras en el tráfico.

## Ethernet actual

Un desarrollo importante que mejoró el rendimiento de la LAN fue la introducción de los switches para reemplazar los hubs en redes basadas en Ethernet. Este desarrollo estaba estrechamente relacionado con el desarrollo de Ethernet 100BASE-TX. Los switches pueden controlar el flujo de datos mediante el aislamiento de cada uno de los puertos y el envío de una trama sólo al destino correspondiente (en caso de que se lo conozca) en vez del envío de todas las tramas a todos los dispositivos.

El switch reduce la cantidad de dispositivos que recibe cada trama, lo que a su vez disminuye o minimiza la posibilidad de colisiones. Esto, junto con la posterior introducción de las comunicaciones full-duplex (que tienen una conexión que puede transportar señales transmitidas y recibidas al mismo tiempo), permitió el desarrollo de Ethernet de 1 Gbps y más.



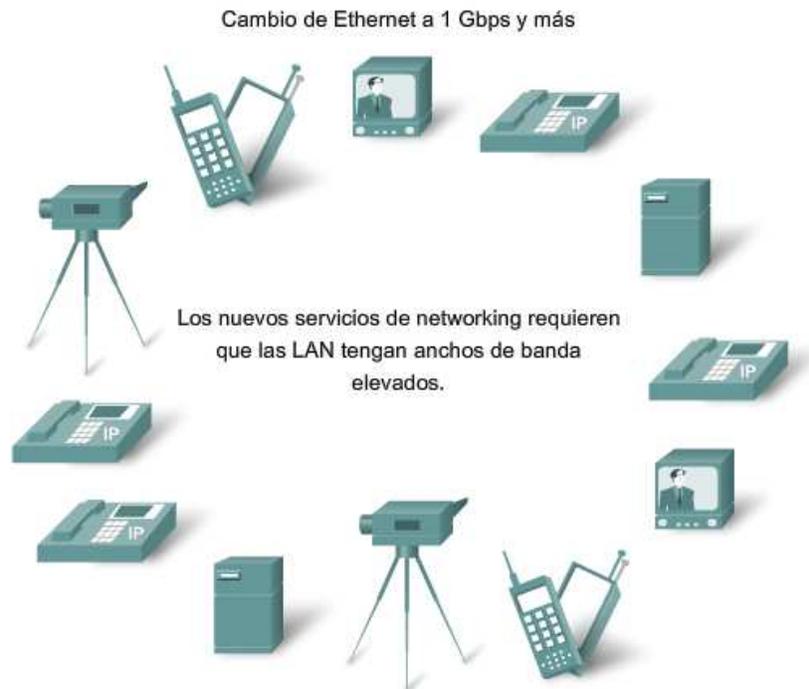
### 9.2.3 Cambio a 1 Gbps y más

Las aplicaciones que atraviesan enlaces de red a diario ponen a prueba incluso a las redes más sólidas. Por ejemplo, el uso cada vez mayor de servicios de Voz sobre IP (VoIP) y multimedia requiere conexiones más rápidas que Ethernet de 100 Mbps.

Gigabit Ethernet se utiliza para describir las implementaciones de Ethernet que ofrecen un ancho de banda de 1000 Mbps (1 Gbps) o más. Esta capacidad se creó sobre la base de la capacidad full-duplex y las tecnologías de medios UTP y de fibra óptica de versiones anteriores de Ethernet.

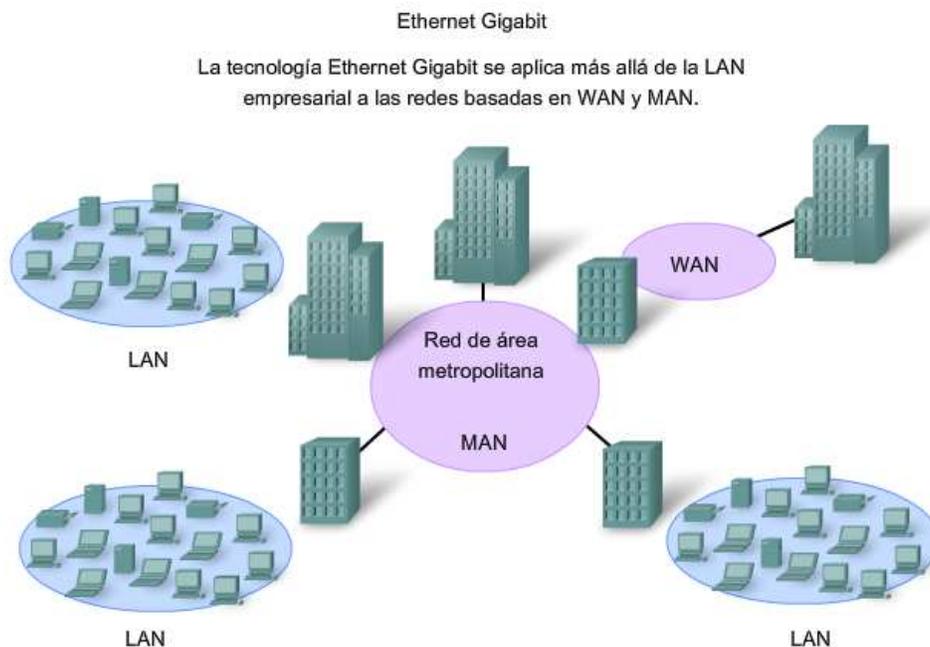
El aumento del rendimiento de la red es significativo cuando la velocidad de transmisión (throughput) potencial aumenta de 100 Mbps a 1 Gbps y más.

La actualización a Ethernet de 1 Gbps no siempre implica que la infraestructura de red de cables y switches existente debe reemplazarse por completo. Algunos equipos y cableados de redes modernas bien diseñadas e instaladas podrían trabajar a mayores velocidades con sólo una actualización mínima. Esta capacidad tiene el beneficio de reducir el costo total de propiedad de la red.



## Ethernet más allá de la LAN

Las mayores distancias de cableado habilitadas por el uso de cables de fibra óptica en redes basadas en Ethernet disminuyeron las diferencias entre las LAN y las WAN. La Ethernet se limitaba originalmente a sistemas de cableado LAN dentro de un mismo edificio y después se extendió a sistemas entre edificios. Actualmente, puede aplicarse a través de toda una ciudad mediante lo que se conoce como Red de área metropolitana (MAN).



## 9.3 La trama de Ethernet

### 9.3.1 La trama: encapsulación del paquete

La estructura de la trama de Ethernet agrega encabezados y tráilers a la PDU de Capa 3 para encapsular el mensaje que se envía.

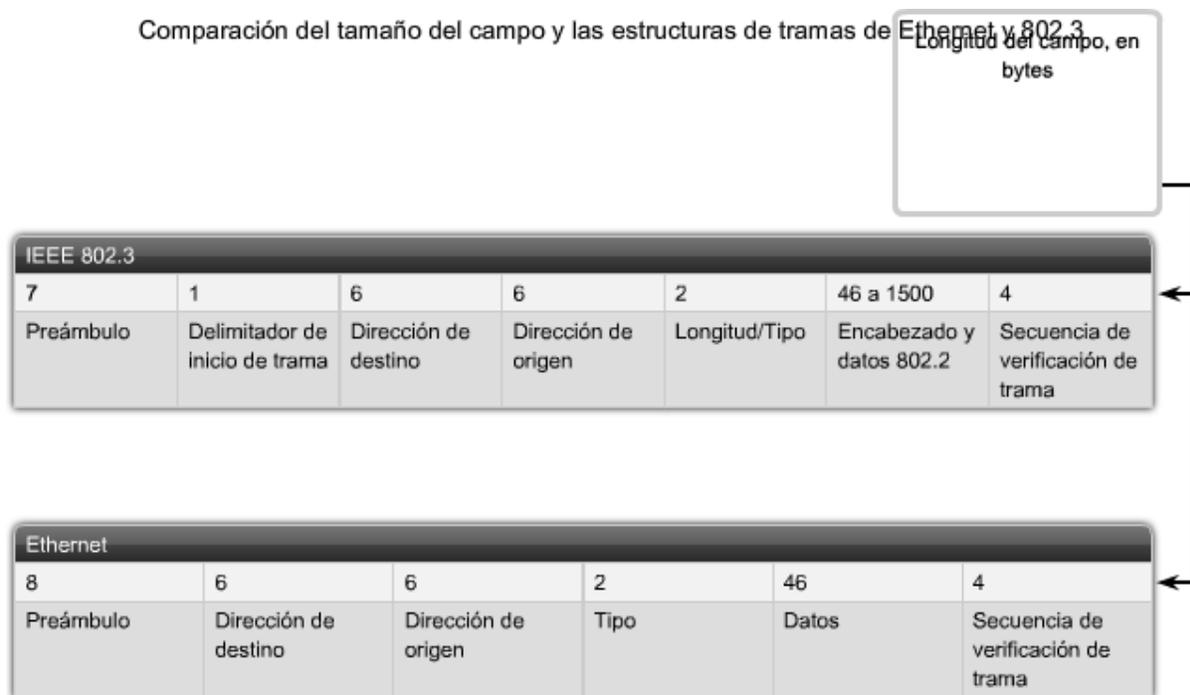
Tanto el encabezado como el tráiler de Ethernet tienen varias secciones de información que el protocolo Ethernet utiliza. Cada sección de la trama se denomina campo. Hay dos estilos de tramas de Ethernet: el IEEE 802.3 (original) y el IEEE 802.3 revisado (Ethernet).

Las diferencias entre los estilos de tramas son mínimas. La diferencia más significativa entre el IEEE 802.3 (original) y el IEEE 802.3 revisado es el agregado de un delimitador de inicio de trama (SFD) y un pequeño cambio en el campo Tipo que incluye la Longitud, tal como se muestra en la figura.

#### Tamaño de la trama de Ethernet

El estándar Ethernet original definió el tamaño mínimo de trama en 64 bytes y el tamaño máximo de trama en 1518 bytes. Esto incluye todos los bytes del campo Dirección MAC de destino a través del campo Secuencia de verificación de trama (FCS). Los campos Preámbulo y Delimitador de inicio de trama no se incluyen en la descripción del tamaño de una trama. El estándar IEEE 802.3ac, publicado en 1998, amplió el tamaño de trama máximo permitido a 1522 bytes. Se aumentó el tamaño de la trama para que se adapte a una tecnología denominada Red de área local virtual (VLAN). Las VLAN se crean dentro de una red conmutada y se presentarán en otro curso.

Si el tamaño de una trama transmitida es menor que el mínimo o mayor que el máximo, el dispositivo receptor descarta la trama. Es posible que las tramas descartadas se originen en colisiones u otras señales no deseadas y, por lo tanto, se consideran no válidas.



Los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD) (1 byte) se utilizan para la sincronización entre los dispositivos de envío y de recepción. Estos ocho primeros bytes de la trama se utilizan para captar la atención de los nodos receptores. Básicamente, los primeros bytes le indican al receptor que se prepare para recibir una trama nueva.

#### Campo Dirección MAC de destino

El campo Dirección MAC de destino (6 bytes) es el identificador del receptor deseado. Como recordará, la Capa 2 utiliza esta dirección para ayudar a los dispositivos a determinar si la trama viene dirigida a ellos. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.

#### Campo Dirección MAC de origen

El campo Dirección MAC de origen (6 bytes) identifica la NIC o interfaz que origina la trama. Los switches también utilizan esta dirección para ampliar sus tablas de búsqueda. El rol de los switches se analizará más adelante en este capítulo.

## Campo Longitud/Tipo

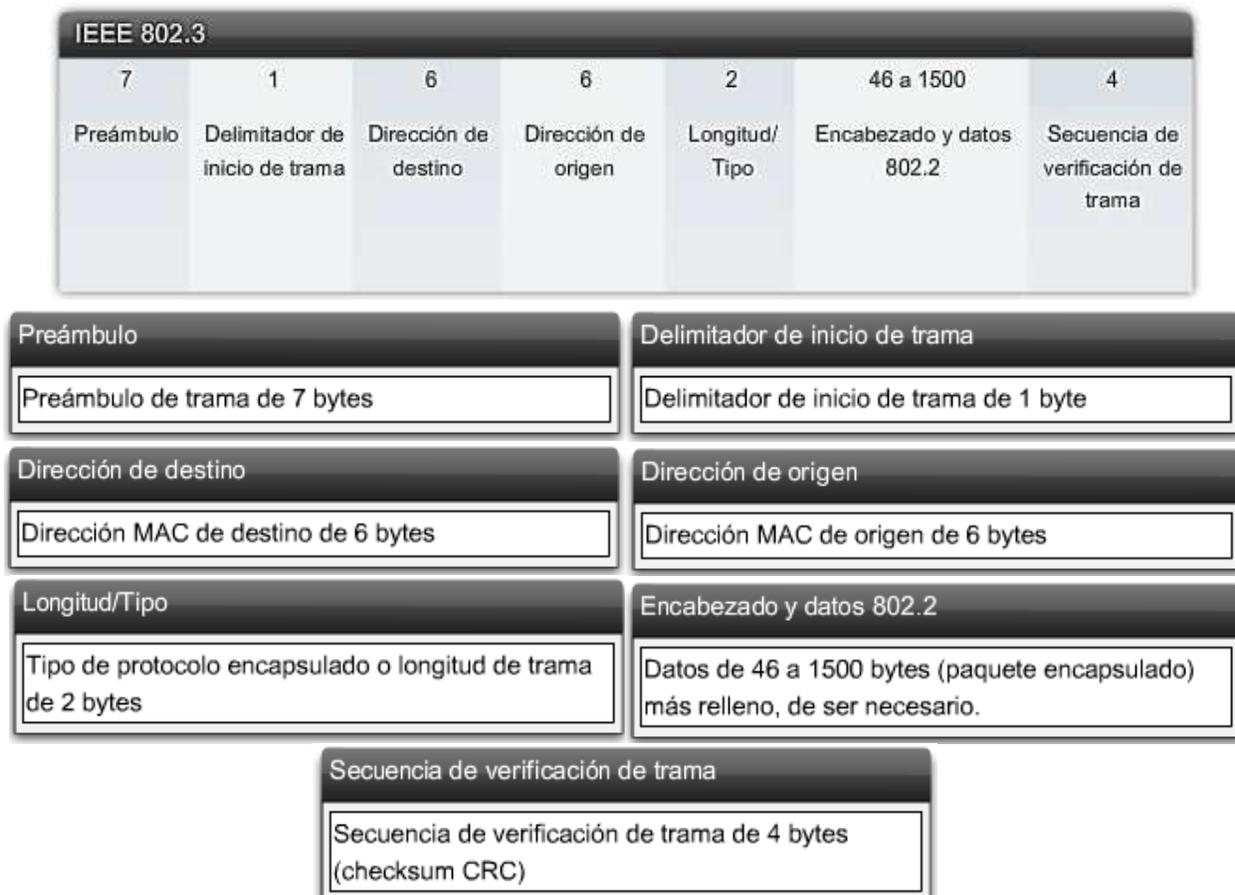
El campo Longitud/Tipo (2 bytes) define la longitud exacta del campo Datos de la trama. Esto se utiliza posteriormente como parte de la FCS para garantizar que el mensaje se reciba adecuadamente. En este campo debe ingresarse una longitud o un tipo. Sin embargo, sólo uno u otro podrá utilizarse en una determinada implementación. Si el objetivo del campo es designar un tipo, el campo Tipo describe qué protocolo se implementa.

El campo denominado Longitud/Tipo sólo aparecía como Longitud en las versiones anteriores del IEEE y sólo como Tipo en la versión DIX. Estos dos usos del campo se combinaron oficialmente en una versión posterior del IEEE, ya que ambos usos eran comunes. El campo Tipo de la Ethernet II se incorporó a la actual definición de trama del 802.3. La Ethernet II es el formato de trama de Ethernet que se utiliza en redes TCP/IP. Cuando un nodo recibe una trama, debe analizar el campo Longitud/Tipo para determinar qué protocolo de capa superior está presente. Si el valor de los dos octetos es equivalente a 0x0600 hexadecimal o 1536 decimal o mayor que éstos, los contenidos del campo Datos se codifican según el protocolo indicado.

## Campos Datos y Relleno

Los campos Datos y Relleno (de 46 a 1500 bytes) contienen los datos encapsulados de una capa superior, que es una PDU de Capa 3 genérica o, con mayor frecuencia, un paquete IPv4. Todas las tramas deben tener al menos 64 bytes de longitud. Si se encapsula un paquete pequeño, el Pad se utiliza para aumentar el tamaño de la trama hasta alcanzar este tamaño mínimo.

### Campos de trama Ethernet



## Campo Secuencia de verificación de trama

El campo Secuencia de verificación de trama (FCS) (4 bytes) se utiliza para detectar errores en la trama. Utiliza una comprobación cíclica de redundancia (CRC). El dispositivo emisor incluye los resultados de una CRC en el campo FCS de la trama.

El dispositivo receptor recibe la trama y genera una CRC para detectar errores. Si los cálculos coinciden, significa que no se produjo ningún error. Los cálculos que no coinciden indican que los datos cambiaron y, por consiguiente, se descarta la trama. Un cambio en los datos podría ser resultado de una interrupción de las señales eléctricas que representan los bits.



Si la FCS calculada por el receptor (basada en los contenidos de la trama recibida) no es igual a la FCS calculada por el origen (la cual está incluida en la trama), la trama se considera inválida y se la descarta.

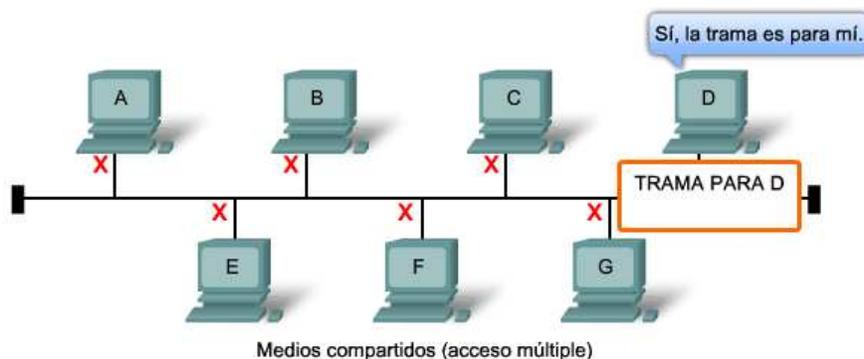
## 9.3.2 La dirección MAC de Ethernet

Inicialmente, la Ethernet se implementaba como parte de una topología de bus. Cada uno de los dispositivos de red se conectaba al mismo medio compartido. En redes con poco tráfico o pequeñas, ésta era una implementación aceptable. El problema más importante que debía resolverse era cómo identificar cada uno de los dispositivos. La señal podía enviarse a todos los dispositivos, pero ¿cómo podía determinar cada uno de los dispositivos si era el receptor del mensaje?

Se creó un identificador único, denominado dirección de Control de acceso al medio (MAC), para ayudar a determinar las direcciones de origen y destino dentro de una red Ethernet. Independientemente de qué variedad de Ethernet se estaba utilizando, la convención de denominación brindó un método para identificar dispositivos en un nivel inferior del modelo OSI.

Como recordará, la dirección MAC se agrega como parte de una PDU de Capa 2. Una dirección MAC de Ethernet es un valor binario de 48 bits expresado como 12 dígitos hexadecimales.

La dirección MAC— Direccionamiento en Ethernet



Todos los nodos Ethernet comparten los medios.  
Para recibir los datos que se le enviaron, cada nodo necesita una dirección única.

## Estructura de la dirección MAC

El valor de la dirección MAC es el resultado directo de las normas implementadas por el IEEE para proveedores con el objetivo de garantizar direcciones únicas para cada dispositivo Ethernet. Las normas establecidas por el IEEE obligan a los proveedores de dispositivos Ethernet a registrarse en el IEEE. El IEEE le asigna a cada proveedor un código de 3 bytes, denominado Identificador único organizacional (OUI).

El IEEE obliga a los proveedores a respetar dos normas simples:

- Todas las direcciones MAC asignadas a una NIC u otro dispositivo Ethernet deben utilizar el OUI que se le asignó a dicho proveedor como los 3 primeros bytes.
- Se les debe asignar un valor exclusivo a todas las direcciones MAC con el mismo OUI (Identificador exclusivo de organización) (código del fabricante o número de serie) en los últimos 3 bytes.

La dirección MAC se suele denominar dirección grabada (BIA) porque se encuentra grabada en la ROM (Memoria de sólo lectura) de la NIC. Esto significa que la dirección se codifica en el chip de la ROM de manera permanente (el software no puede cambiarla).

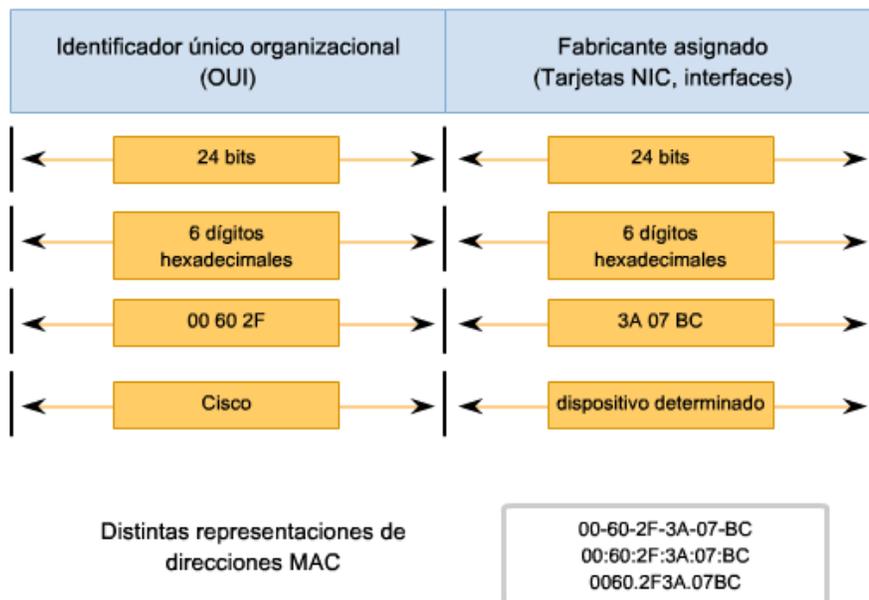
Sin embargo, cuando se inicia el equipo la NIC copia la dirección a la RAM (Memoria de acceso aleatorio). Cuando se examinan tramas se utiliza la dirección que se encuentra en la RAM como dirección de origen para compararla con la dirección de destino. La NIC utiliza la dirección MAC para determinar si un mensaje debe pasarse a las capas superiores para procesarlo.

## Dispositivos de red

Cuando el dispositivo de origen reenvía el mensaje a una red Ethernet, se adjunta la información del encabezado dentro de la dirección MAC. El dispositivo de origen envía los datos a través de la red. Cada NIC de la red visualiza la información para determinar si la dirección MAC coincide con su dirección física. Si no hay coincidencia, el dispositivo descarta la trama. Cuando la trama llega al destino donde la MAC de la NIC coincide con la MAC de destino de la trama, la NIC pasa la trama hasta las capas OSI (Interconexión de sistema abierto), donde se lleva a cabo el proceso de desencapsulación.

Todos los dispositivos conectados a una LAN Ethernet tienen interfaces con direcciones MAC. Diferentes fabricantes de hardware y software pueden representar las direcciones MAC en distintos formatos hexadecimales. Los formatos de las direcciones pueden ser similares a 00-05-9A-3C-78-00, 00:05:9A:3C:78:00 ó 0005.9A3C.7800. Las direcciones MAC se asignan a estaciones de trabajo, servidores, impresoras, switches y routers (cualquier dispositivo que pueda originar o recibir datos en la red).

Estructura de la dirección MAC Ethernet



### 9.3.3 Numeración hexadecimal y direccionamiento

## Numeración hexadecimal

El método hexadecimal ("Hex") es una manera conveniente de representar valores binarios. Así como el sistema de numeración decimal es un sistema de base diez y el binario es un sistema de base dos, el sistema hexadecimal es un sistema de base dieciséis.

El sistema de numeración de base 16 utiliza los números del 0 al 9 y las letras de la A a la F. La figura muestra los valores decimales, binarios y hexadecimales equivalentes para los binarios 0000 hasta 1111. Nos resulta más conveniente expresar un valor como un único dígito hexadecimal que como cuatro bits.

## Comprensión de los bytes

Dado que 8 bits (un byte) es una agrupación binaria común, los binarios 00000000 hasta 11111111 pueden representarse en valores hexadecimales como el intervalo 00 a FF. Los ceros iniciales se muestran siempre para completar la representación de 8 bits. Por ejemplo, el valor binario 0000 1010 se muestra en valor hexadecimal como 0A.

## Representación de valores hexadecimales

**Nota:** Es importante distinguir los valores hexadecimales de los valores decimales en cuanto a los caracteres del 0 al 9, tal como lo muestra la figura.

El valor hexadecimal se representa generalmente en texto mediante el valor precedido por 0x (por ejemplo, 0x73) o un 16 en subíndice. Con menor frecuencia, puede estar seguido de una H, como por ejemplo, 73H. Sin embargo, y debido a que el texto en subíndice no es reconocido en entornos de línea de comando o de programación, la representación técnica de un valor hexadecimal es precedida de "0x" (cero X). Por lo tanto, los ejemplos anteriores deberían mostrarse como 0x0A y 0x73, respectivamente.

El valor hexadecimal se utiliza para representar las direcciones MAC de Ethernet y las direcciones IP versión 6. Ya hemos visto que los valores hexadecimales se utilizan en el panel Bytes de paquetes de Wireshark para representar los valores binarios dentro de tramas y paquetes.

## Conversiones hexadecimales

Las conversiones numéricas entre valores decimales y hexadecimales son simples, pero no siempre es conveniente dividir o multiplicar por 16. Si es necesario realizar dichas conversiones, generalmente es más fácil convertir el valor decimal o hexadecimal a un valor binario y después convertir dicho valor binario a un valor decimal o hexadecimal, según corresponda.

Con la práctica, es posible reconocer los patrones de bits binarios que coinciden con los valores decimales y hexadecimales. La figura ilustra dichos patrones para valores seleccionados de 8 bits.

### Números hexadecimales

Equivalentes decimales y binarios del 0 al F hexadecimal

Decimal	Binario	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Equivalentes decimales, binarios y hexadecimales escogidos

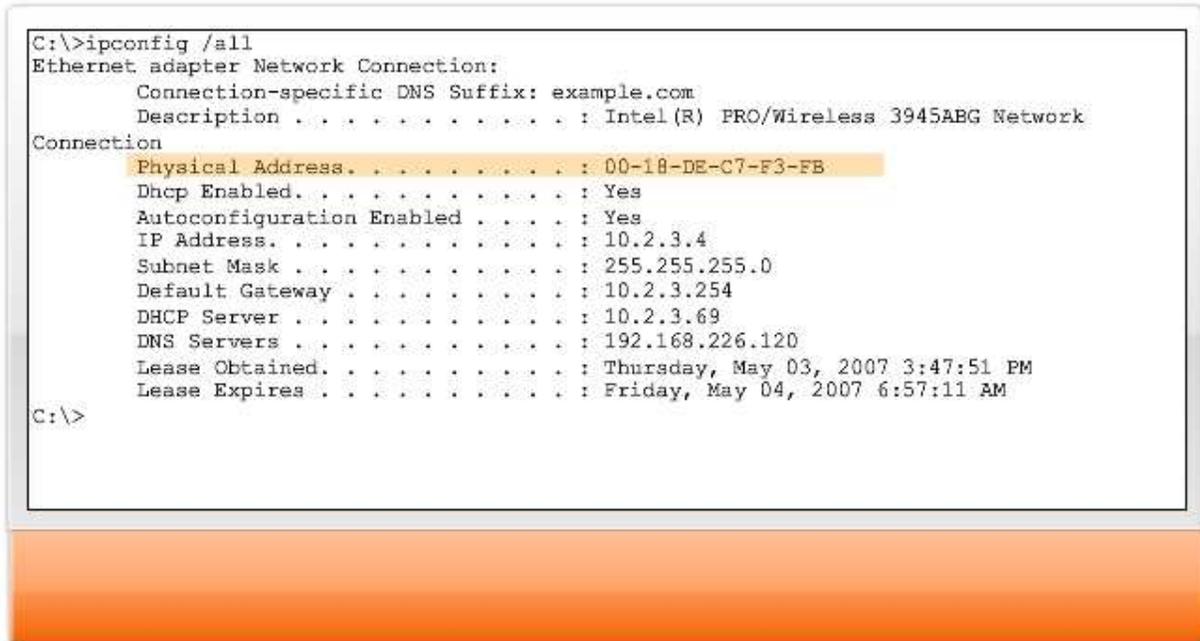
Decimal	Binario	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

## Visualización de la MAC

Una herramienta útil para analizar la dirección MAC de nuestra computadora es `ipconfig /all` o `ifconfig`. En el gráfico, observe la dirección MAC de esta computadora. Si el usuario tiene acceso, es posible que desee intentar esto en su equipo.

Quizás quiera buscar el OUI de la dirección MAC para determinar quién es el fabricante de su NIC.

### Visualización de la dirección MAC



```
C:\>ipconfig /all
Ethernet adapter Network Connection:
    Connection-specific DNS Suffix: example.com
    Description . . . . . : Intel(R) PRO/Wireless 3945ABG Network
Connection
    Physical Address. . . . . : 00-18-DE-C7-F3-FB
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.2.3.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.2.3.254
    DHCP Server . . . . . : 10.2.3.69
    DNS Servers . . . . . : 192.168.226.120
    Lease Obtained. . . . . : Thursday, May 03, 2007 3:47:51 PM
    Lease Expires . . . . . : Friday, May 04, 2007 6:57:11 AM
C:\>
```

## 9.3.4 Otra capa de direccionamiento

### Capa de Enlace de datos

El direccionamiento físico de la capa de Enlace de datos (Capa 2) de OSI, implementado como dirección MAC de Ethernet, se utiliza para transportar la trama a través de los medios locales. Si bien brindan una dirección host única, las direcciones físicas no son jerárquicas. Estas direcciones se asocian a un dispositivo en particular, independientemente de su ubicación o de la red a la que esté conectado.

Estas direcciones de Capa 2 no tienen ningún significado fuera de los medios de la red local. Es posible que un paquete deba atravesar una serie de tecnologías de conexión de datos diferentes en redes locales y de área amplia antes de llegar a su destino. Por lo tanto, un dispositivo de origen no tiene conocimiento de la tecnología utilizada en redes intermedias y de destino o de sus direcciones de Capa 2 y estructuras de trama.

### Capa de Red

Las direcciones de capa de Red (Capa 3), como por ejemplo, las direcciones IPv4, brindan el direccionamiento general y local que se comprende tanto en el origen como en el destino. Para llegar a su último destino, un paquete transporta la dirección de destino de Capa 3 desde su origen. Sin embargo, debido a que diferentes protocolos de la capa de Enlace de datos la traman durante el trayecto, la dirección de Capa 2 que recibe cada vez se aplica sólo a esa porción local del trayecto y sus medios.

En resumen:

- La dirección de capa de red permite el envío del paquete a su destino.
- La dirección de capa de enlace de datos permite el transporte del paquete utilizando los medios locales a través de cada segmento.



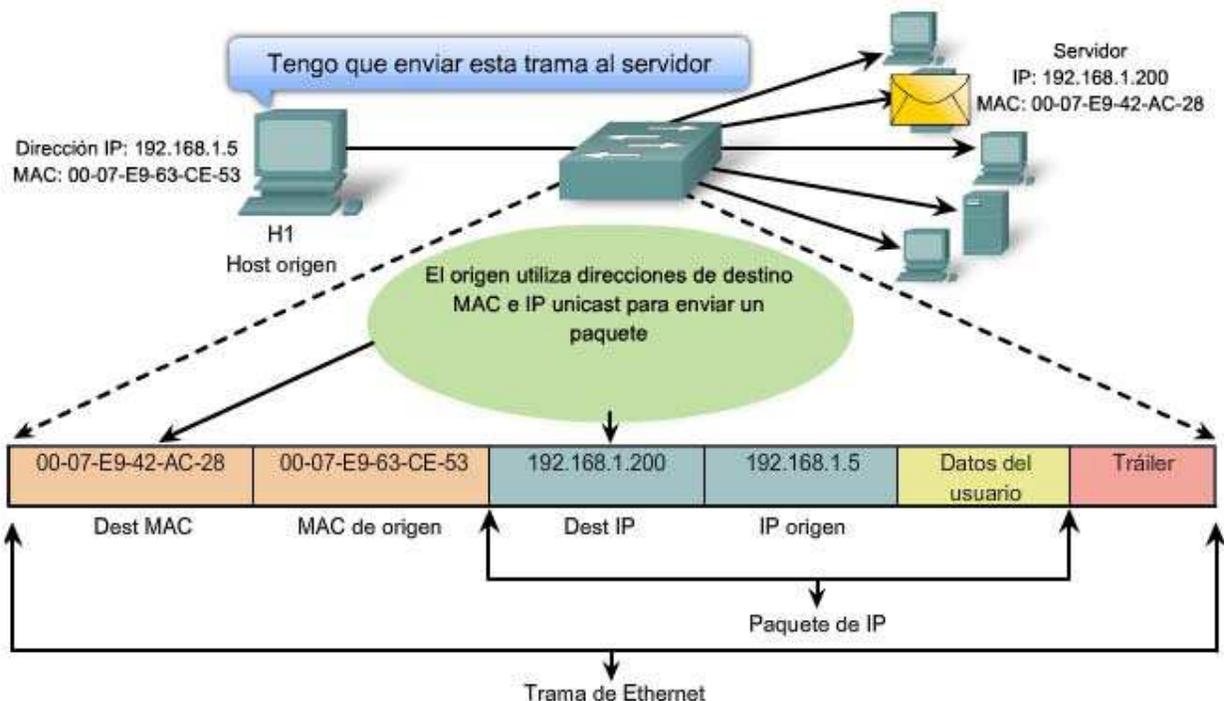
### 9.3.5 Ethernet unicast, multicast y broadcast

En Ethernet se utilizan distintas direcciones MAC para la capa 2: comunicaciones **unicast**, **multicast** y **broadcast**.

#### Unicast

Una dirección MAC unicast es la dirección exclusiva que se utiliza cuando se envía una trama desde un dispositivo de transmisión único hacia un dispositivo de destino único.

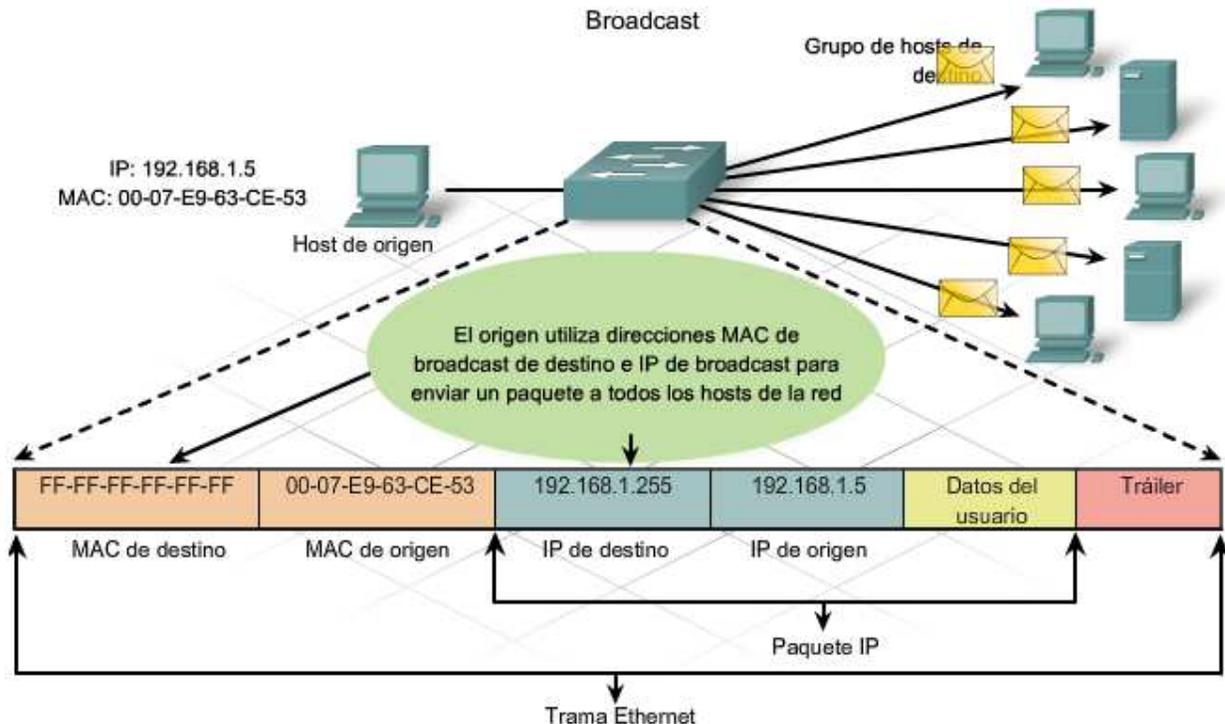
En el ejemplo que se muestra en la figura, un host con una dirección IP 192.168.1.5 (origen) solicita una página Web del servidor en la dirección IP 192.168.1.200. Para que se pueda enviar y recibir un paquete unicast, el encabezado del paquete IP debe contener una dirección IP de destino. Además, el encabezado de la trama de Ethernet también debe contener una dirección MAC de destino correspondiente. La dirección IP y la dirección MAC se combinan para enviar datos a un host de destino específico.



## Broadcast

Con broadcast, el paquete contiene una dirección IP de destino con todos unos (1) en la porción de host. Esta numeración en la dirección significa que todos los hosts de esa red local (dominio de broadcast) recibirán y procesarán el paquete. Una gran cantidad de protocolos de red utilizan broadcast, como el Protocolo de configuración dinámica de host (DHCP) y el Protocolo de resolución de direcciones (ARP). Más adelante en este capítulo se analizará cómo el ARP utiliza los broadcasts para asignar direcciones de Capa 2 a direcciones de Capa 3.

Tal como se muestra en la figura, una dirección IP de broadcast para una red necesita un dirección MAC de broadcast correspondiente en la trama de Ethernet. En redes Ethernet, la dirección MAC de broadcast contiene 48 unos que se muestran como el hexadecimal FF-FF-FF-FF-FF-FF.



## Multicast

Recuerde que las direcciones multicast le permiten a un dispositivo de origen enviar un paquete a un grupo de dispositivos. Una dirección IP de grupo multicast se asigna a los dispositivos que pertenecen a un grupo multicast. El intervalo de direcciones multicast es de 224.0.0.0 a 239.255.255.255. Debido a que las direcciones multicast representan un grupo de direcciones (a veces denominado un grupo de hosts), sólo pueden utilizarse como el destino de un paquete. El origen siempre tendrá una dirección unicast.

Ejemplos de dónde se utilizarían las direcciones multicast serían el juego remoto, en el que varios jugadores se conectan de manera remota pero juegan el mismo juego, y el aprendizaje a distancia a través de videoconferencia, en el que varios estudiantes se conectan a la misma clase.

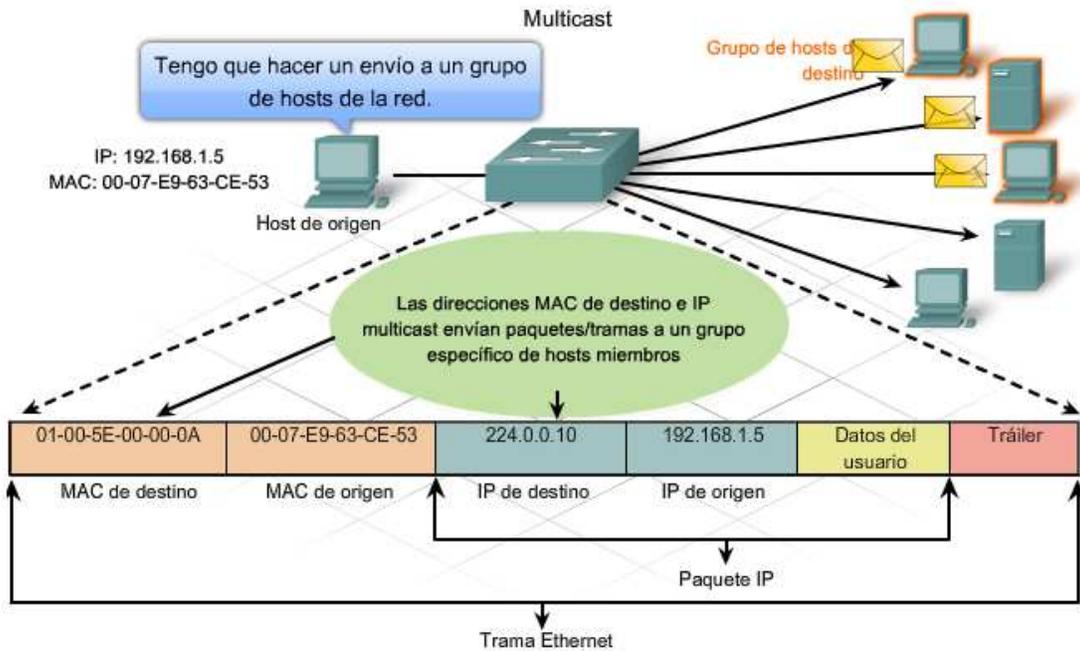
Al igual que con las direcciones unicast y de broadcast, la dirección IP multicast requiere una dirección MAC multicast correspondiente para poder enviar tramas en una red local. La dirección MAC multicast es un valor especial que comienza con 01-00-5E en hexadecimal. El valor termina con la conversión de los 23 bits inferiores de la dirección IP del grupo multicast en los 6 caracteres hexadecimales restantes de la dirección de Ethernet. El bit restante en la dirección MAC es siempre "0".

Un ejemplo, tal como se muestra en el gráfico, es el hexadecimal 01-00-5E-00-00-0A. Cada caracter hexadecimal es 4 bits binarios.

<http://www.iana.org/assignments/ethernet-numbers>

[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/waas/acns/v51/configuration/central/guide/51ipmul.html](http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/v51/configuration/central/guide/51ipmul.html)

[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/ipmulti.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ipmulti.htm)



## 9.4 Control de acceso al medio de Ethernet

### 9.4.1 Control de acceso al medio en Ethernet

En un entorno de medios compartidos, todos los dispositivos tienen acceso garantizado al medio, pero no tienen ninguna prioridad en dicho medio. Si más de un dispositivo realiza una transmisión simultáneamente, las señales físicas colisionan y la red debe recuperarse para que pueda continuar la comunicación.

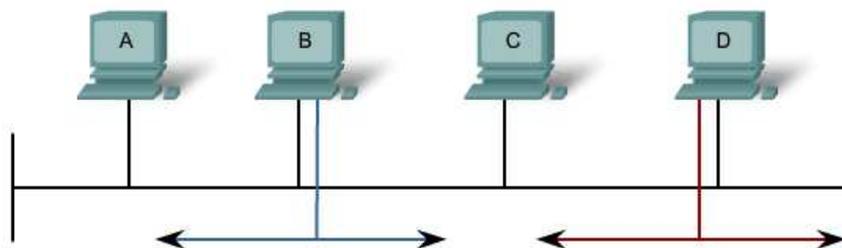
Las colisiones representan el precio que debe pagar la Ethernet para obtener el bajo costo relacionado con cada transmisión.

La Ethernet utiliza el acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD) para detectar y manejar colisiones y para administrar la reanudación de las comunicaciones.

Debido a que todas las computadoras que utilizan Ethernet envían sus mensajes en el mismo medio, se utiliza un esquema de coordinación distribuida (CSMA) para detectar la actividad eléctrica en el cable. Entonces, un dispositivo puede determinar cuándo puede transmitir. Cuando un dispositivo detecta que ninguna otra computadora está enviando una trama o una señal portadora, el dispositivo transmitirá en caso de que tenga algo para enviar.

Control de acceso al medio en Ethernet

Acceso múltiple por detección de portadora y  
detección de colisiones (CSMA/CD)



CSMA/CD controla el acceso a los medios compartidos. Si hay una colisión, se detecta y las tramas se retransmiten.

## 9.4.2 CSMA/CD: El proceso

### Detección de portadora

En el método de acceso CSMA/CD, todos los dispositivos de red que tienen mensajes para enviar deben escuchar antes de transmitir.

Si un dispositivo detecta una señal de otro dispositivo, esperará durante un período especificado antes de intentar transmitir.

Cuando no se detecte tráfico, un dispositivo transmitirá su mensaje. Mientras se lleva a cabo la transmisión, el dispositivo continúa escuchando para detectar tráfico o colisiones en la LAN. Una vez que se envía el mensaje, el dispositivo regresa a su modo de escucha predeterminado.

### Multiacceso

Si la distancia existente entre los dispositivos es tal que la latencia de las señales de un dispositivo denota que un segundo dispositivo no detecta las señales, el segundo dispositivo puede comenzar también a transmitir. Los medios tienen entonces dos dispositivos que transmiten sus señales al mismo tiempo. Sus mensajes se propagarán por todos los medios hasta que se encuentren. En ese punto, las señales se mezclan y el mensaje se destruye. Si bien los mensajes se corrompen, la mezcla de señales restantes continúa propagándose a través de los medios.

### Detección de colisiones

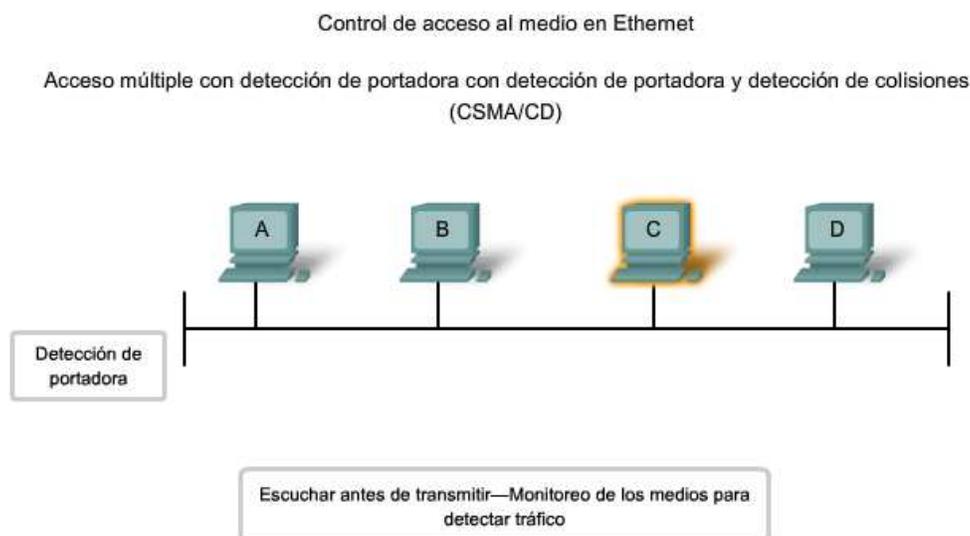
Cuando un dispositivo está en modo de escucha, puede detectar una colisión en el medio compartido. La detección de una colisión es posible porque todos los dispositivos pueden detectar un aumento de la amplitud de la señal por encima del nivel normal.

Una vez que se produce una colisión, los demás dispositivos que se encuentren en modo de escucha (como así también todos los dispositivos transmisores) detectarán el aumento de la amplitud de la señal. Una vez detectada la colisión, todos los dispositivos transmisores continuarán transmitiendo para garantizar que todos los dispositivos de la red detecten la colisión.

### Señal de congestión y postergación aleatoria

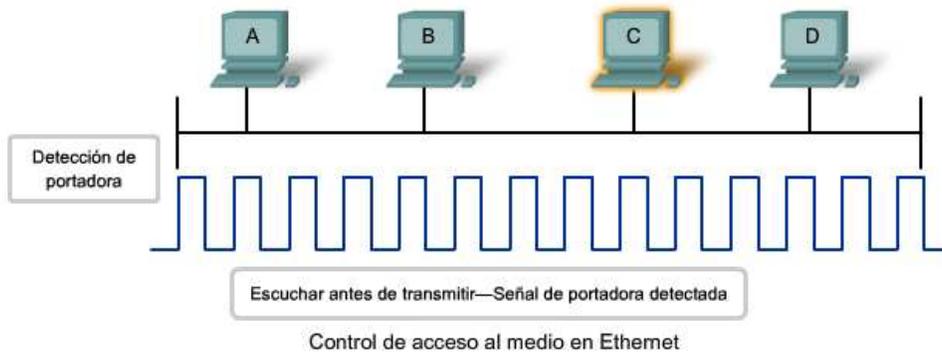
Cuando los dispositivos de transmisión detectan la colisión, envían una señal de congestión. Esta señal interferente se utiliza para notificar a los demás dispositivos sobre una colisión, de manera que éstos invocarán un algoritmo de postergación. Este algoritmo de postergación hace que todos los dispositivos dejen de transmitir durante un período aleatorio, lo que permite que las señales de colisión disminuyan.

Una vez que finaliza el retraso asignado a un dispositivo, dicho dispositivo regresa al modo "escuchar antes de transmitir". El período de postergación aleatoria garantiza que los dispositivos involucrados en la colisión no intenten enviar su tráfico nuevamente al mismo tiempo, lo que provocaría que se repita todo el proceso. Sin embargo, esto también significa que un tercer dispositivo puede transmitir antes de que cualquiera de los dos dispositivos involucrados en la colisión original tenga la oportunidad de volver a transmitir.

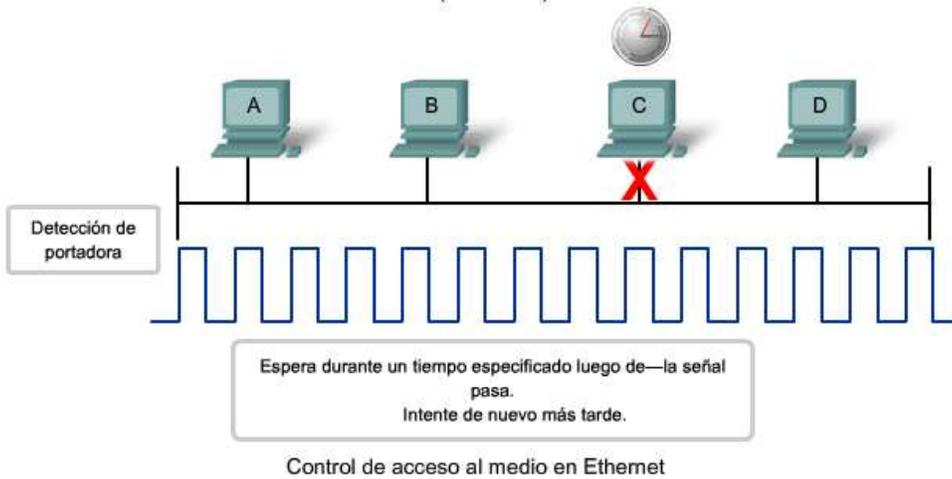


## Control de acceso al medio en Ethernet

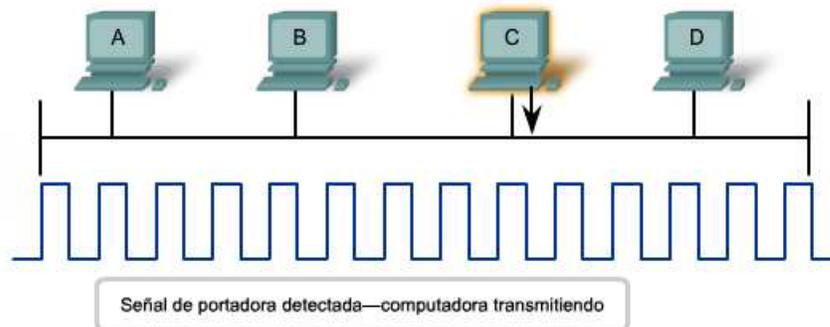
Acceso múltiple con detección de portadora con detección de portadora y detección de colisiones (CSMA/CD)



Acceso múltiple con detección de portadora con detección de portadora y detección de colisiones (CSMA/CD)



Acceso múltiple con detección de portadora con detección de portadora y detección de colisiones (CSMA/CD)



## Hubs y dominios de colisiones

Dado que las colisiones se producirán ocasionalmente en cualquier topología de medios compartidos (incluso cuando se emplea CSMA/CD), debemos prestar atención a las condiciones que pueden originar un aumento de las colisiones. Debido al rápido crecimiento de la Internet:

- Se conectan más dispositivos a la red.
- Los dispositivos acceden a los medios de la red con una mayor frecuencia.
- Aumentan las distancias entre los dispositivos.

Recuerde que los hubs fueron creados como dispositivos de red intermediarios que permiten a una mayor cantidad de nodos conectarse a los medios compartidos. Los hubs, que también se conocen como repetidores multipuerto, retransmiten las señales de datos recibidas a todos los dispositivos conectados, excepto a aquél desde el cual se reciben las señales. Los hubs no desempeñan funciones de red tales como dirigir los datos según las direcciones.

Los hubs y los repetidores son dispositivos intermediarios que extienden la distancia que pueden alcanzar los cables de Ethernet. Debido a que los hubs operan en la capa física, ocupándose únicamente de las señales en los medios, pueden producirse colisiones entre los dispositivos que conectan y dentro de los mismos hubs.

Además, la utilización de hubs para proporcionar acceso a la red a una mayor cantidad de usuarios reduce el rendimiento para cada usuario, ya que debe compartirse la capacidad fija de los medios entre cada vez más dispositivos.

Los dispositivos conectados que tienen acceso a medios comunes a través de un hub o una serie de hubs conectados directamente conforman lo que se denomina dominio de colisiones. Un dominio de colisiones también se denomina segmento de red. Por lo tanto, los hubs y repetidores tienen el efecto de aumentar el tamaño del dominio de colisiones.

Tal como se muestra en la figura, la interconexión de los hubs forma una topología física que se denomina estrella extendida. La estrella extendida puede crear un dominio de colisiones notablemente expandido.

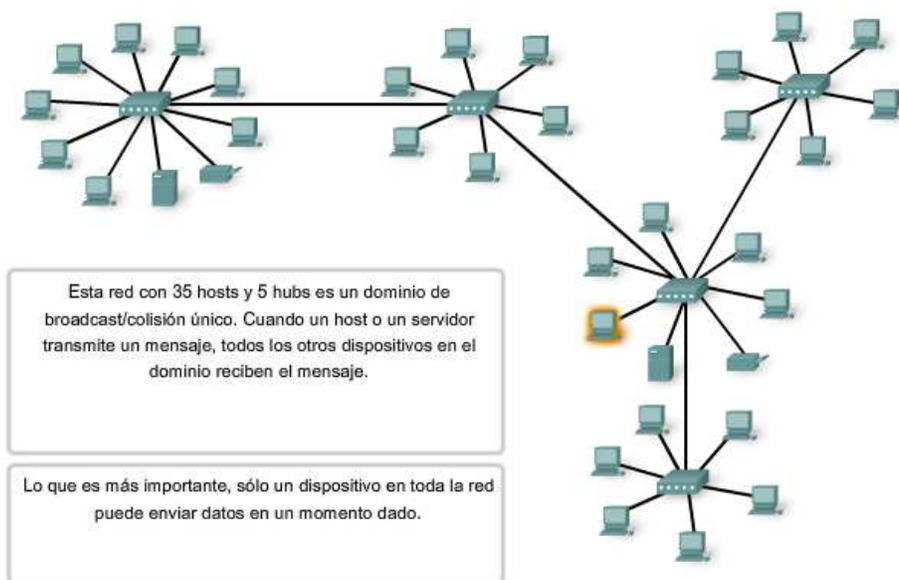
Un mayor número de colisiones reduce la eficiencia y la efectividad de la red hasta que las colisiones se convierten en una molestia para el usuario.

Si bien el CSMA/CD es un sistema de administración de colisiones de tramas, dicho sistema se diseñó para administrar colisiones sólo para una cantidad limitada de dispositivos y en redes con poco uso de red. Por lo tanto, se requiere de otros mecanismos cuando existen grandes cantidades de usuarios que quieren tener acceso y cuando se necesita un acceso a la red más activo.

Comprobaremos que la utilización de switches en lugar de hubs puede ser un comienzo para reducir este problema.

<http://standards.ieee.org/getieee802/802.3.html>

La utilización de hubs en topologías en estrella extendidas puede crear grandes dominios de colisión



### 9.4.3 Temporización de Ethernet

Las implementaciones más rápidas de la capa física de Ethernet introducen complejidades en la administración de colisiones.

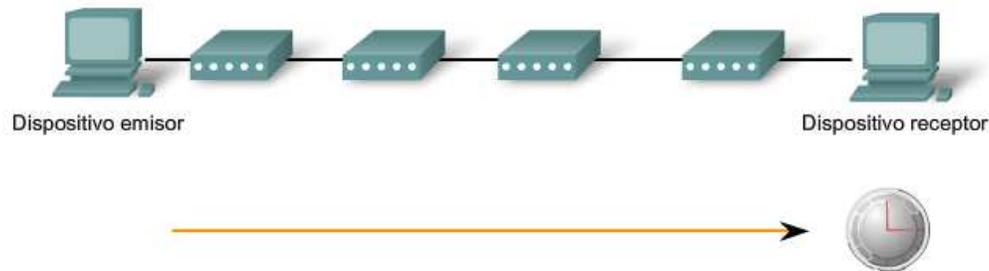
#### Latencia

Tal como se analizó anteriormente, cada dispositivo que desee transmitir debe "escuchar" primero el medio para verificar la presencia de tráfico. Si no hay tráfico, la estación comenzará a transmitir de inmediato. La señal eléctrica que se

transmite requiere una cantidad determinada de tiempo (latencia) para propagarse (viajar) a través del cable. Cada hub o repetidor en la ruta de la señal agrega latencia a medida que envía los bits desde un puerto al siguiente.

Este retardo acumulado aumenta la probabilidad de que se produzcan colisiones, porque un nodo de escucha puede transformarse en señales de transmisión mientras el hub o repetidor procesa el mensaje. Debido a que la señal no había alcanzado este nodo mientras estaba escuchando, dicho nodo pensó que el medio estaba disponible. Esta condición produce generalmente colisiones.

#### Retardo Ethernet (latencia)



A una trama Ethernet le lleva un tiempo considerable trasladarse desde el dispositivo emisor hasta el receptor. Cada dispositivo intermediario contribuye a la latencia general.

### Temporización y sincronización

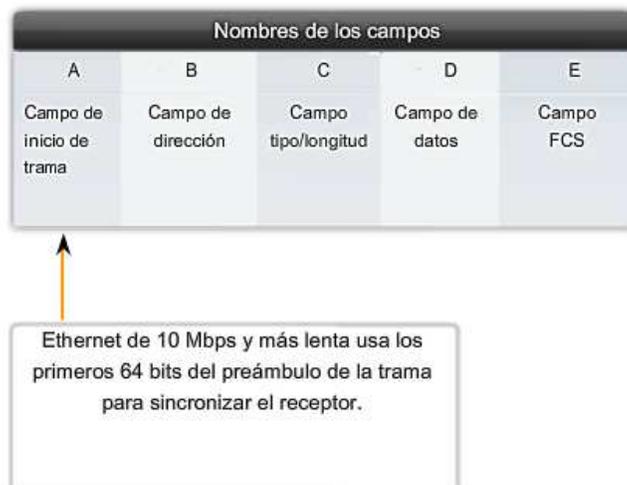
En modo half-duplex, si no se produce una colisión, el dispositivo emisor transmitirá 64 bits de información de sincronización de temporización, lo que se conoce como el Preámbulo.

El dispositivo emisor transmitirá a continuación la trama completa.

La Ethernet con velocidades de transmisión (throughput) de 10 Mbps y menos es asíncrona. Una comunicación asíncrona en este contexto significa que cada dispositivo receptor utilizará los 8 bytes de información de temporización para sincronizar el circuito receptor con los datos entrantes y a continuación descartará los 8 bytes.

Las implementaciones de Ethernet con velocidades de transmisión (throughput) de 100 Mbps y más son síncronas. La comunicación síncrona en este contexto significa que la información de temporización no es necesaria. Sin embargo, por razones de compatibilidad, los campos Preámbulo y Delimitador de inicio de trama (SFD) todavía están presentes.

Sincronización de tramas para comunicaciones asíncronas



## Tiempo de bit

Para cada velocidad de medios diferente se requiere un período de tiempo determinado para que un bit pueda colocarse y detectarse en el medio. Dicho período de tiempo se denomina tiempo de bit. En Ethernet de 10 Mbps, un bit en la capa MAC requiere de 100 nanosegundos (ns) para ser transmitido. A 100 Mbps, ese mismo bit requiere de 10 ns para ser transmitido. Y a 1000 Mbps, sólo se requiere 1 ns para transmitir un bit. A menudo, se utiliza una estimación aproximada de 20,3 centímetros (8 pulgadas) por nanosegundo para calcular el retardo de propagación en un cable UTP. El resultado es que para 100 metros de cable UTP se requiere un poco menos de 5 tiempos de bit para que una señal 10BASE-T recorra la longitud del cable.

Para que el CSMA/CD de Ethernet funcione, el dispositivo emisor debe detectar la colisión antes de que se haya completado la transmisión de una trama del tamaño mínimo. A 100 Mbps, la temporización del dispositivo apenas es capaz de funcionar con cables de 100 metros. A 1000 Mbps, ajustes especiales son necesarios porque se suele transmitir una trama completa del tamaño mínimo antes de que el primer bit alcance el extremo de los primeros 100 metros de cable UTP. Por este motivo, no se permite el modo half-duplex en la Ethernet de 10 Gigabits.

Estas consideraciones de temporización deben aplicarse al espacio entre las tramas y a los tiempos de postergación (ambos temas se analizan en la próxima sección) para asegurar que cuando un dispositivo transmita su próxima trama, se ha reducido al mínimo el riesgo de que se produzca una colisión.

## Intervalo de tiempo

En Ethernet half-duplex, donde los datos sólo pueden viajar en una dirección a la vez, el intervalo de tiempo se convierte en un parámetro importante para determinar cuántos dispositivos pueden compartir una red. Para todas las velocidades de transmisión de Ethernet de o por debajo de 1000 Mbps, el estándar describe cómo una transmisión individual no puede ser menor que el intervalo de tiempo.

La determinación del intervalo de tiempo es una compensación entre la necesidad de reducir el impacto de la recuperación en caso de colisión (tiempos de postergación y retransmisión) y la necesidad de que las distancias de red sean lo suficientemente grandes como para adaptarse a tamaños razonables de red. El compromiso fue elegir un diámetro de red máximo (2500 metros aproximadamente) para después establecer la longitud mínima de una trama que fuera suficiente como para garantizar la detección de todas las peores colisiones.

El intervalo de tiempo para Ethernet de 10 y 100 Mbps es de 512 tiempos de bit o 64 octetos. El intervalo de tiempo para Ethernet de 1000 Mbps es de 4096 tiempos de bit o 512 octetos.

El intervalo de tiempo garantiza que si está por producirse una colisión, se detectará dentro de los primeros 512 bits (4096 para Gigabit Ethernet) de la transmisión de la trama. Esto simplifica el manejo de las retransmisiones de tramas posteriores a una colisión.

El intervalo de tiempo es un parámetro importante por las siguientes razones:

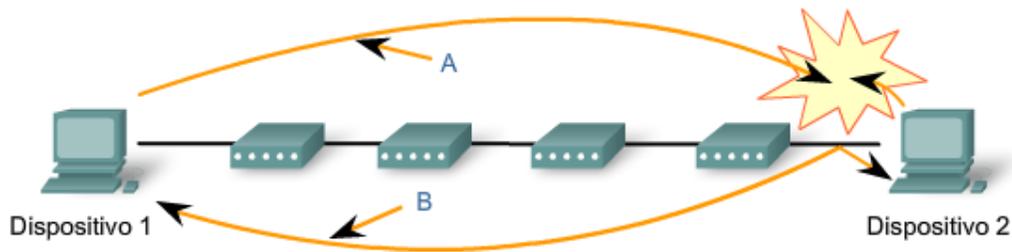
- El intervalo de tiempo de 512 bits establece el tamaño mínimo de una trama de Ethernet en 64 bytes. Cualquier trama con menos de 64 bytes de longitud se considera un "fragmento de colisión" o "runt frame" y las estaciones receptoras la descartan automáticamente.
- El intervalo de tiempo determina un límite para el tamaño máximo de los segmentos de una red. Si la red crece demasiado, pueden producirse colisiones tardías. Las colisiones tardías se consideran una falla en la red, porque un dispositivo detecta la colisión demasiado tarde durante la transmisión de tramas y será manejada automáticamente mediante CSMA/CD.

El intervalo de tiempo se calcula teniendo en cuenta las longitudes máximas de cables en la arquitectura de red legal de mayor tamaño. Todos los tiempos de retardo de propagación del hardware se encuentran al máximo permisible y se utiliza una señal de congestión de 32 bits cuando se detectan colisiones.

**El intervalo de tiempo real calculado es apenas mayor que la cantidad de tiempo teórica necesaria para realizar una transmisión entre los puntos de máxima separación de un dominio de colisión, colisionar con otra transmisión en el último instante posible y luego permitir que los fragmentos de la colisión regresen a la estación transmisora y sean detectados.** Ver la figura.

Para que el sistema funcione correctamente, el primer dispositivo debe estar al tanto de la colisión antes de que termine de enviar la trama legal de menor tamaño.

Para que una Ethernet de 1000 Mbps pueda operar en modo half-duplex, se agregó a la trama el campo de extensión cuando se envían tramas pequeñas, con el sólo fin de mantener ocupado al transmisor durante el tiempo que sea necesario para que vuelva un fragmento de colisión. Este campo sólo se incluye en los enlaces en half-duplex de 1000 Mbps y permite que las tramas de menor tamaño duren el tiempo suficiente para satisfacer los requisitos del intervalo de tiempo. El dispositivo receptor descarta los bits de extensión.



Velocidad	Intervalo de tiempo	Intervalo de tiempo
10 Mbps	512 tiempo de bit	51,2 $\mu$ s
100 Mbps	512 tiempo de bit	5,12 $\mu$ s
1 Gbps	4096 tiempo de bit	4,096 $\mu$ s
10 Gbps	no corresponde	no corresponde

## 9.4.4 Espacio entre tramas y postergación

### Espacio entre tramas

Los estándares de Ethernet requieren un espacio mínimo entre dos tramas que no hayan sufrido una colisión. Esto le otorga al medio tiempo para estabilizarse antes de la transmisión de la trama anterior y tiempo a los dispositivos para que procesen la trama. Este tiempo, llamado espacio entre tramas, se mide desde el último bit del campo FCS de una trama hasta el primer bit del Preámbulo de la próxima trama.

Una vez enviada la trama, todos los dispositivos de una red Ethernet de 10 Mbps deben esperar un mínimo de 96 tiempos de bit (9,6 microsegundos) antes de que cualquier dispositivo pueda transmitir la siguiente trama. En versiones de Ethernet más veloces, el espacio sigue siendo el mismo, 96 tiempos de bit, pero el tiempo del espacio entre tramas se vuelve proporcionalmente más corto.

Los retardos de sincronización entre dispositivos pueden ocasionar la pérdida de algunos de los bits del preámbulo de la trama. A su vez, esto puede producir una reducción mínima del espacio entre tramas cuando los hubs y repetidores regeneran los 64 bits completos de la información de temporización (el Preámbulo y el SFD) al comienzo de cada trama que se reenvía. En Ethernet de mayor velocidad, algunos dispositivos sensibles al tiempo podrían eventualmente no reconocer las tramas individuales lo que originaría una falla de comunicación.

### Separación entre tramas Ethernet

Velocidad	Separación entre tramas	Tiempo necesario
10 Mbps	96 tiempo de bit	9,6 $\mu$ s
100 Mbps	96 tiempo de bit	0,96 $\mu$ s
1 Gbps	96 tiempo de bit	0,096 $\mu$ s
10 Gbps	96 tiempo de bit	0,0096 $\mu$ s

El tiempo entre tramas se reduce a medida que aumenta la velocidad de Ethernet



## Señal de congestión

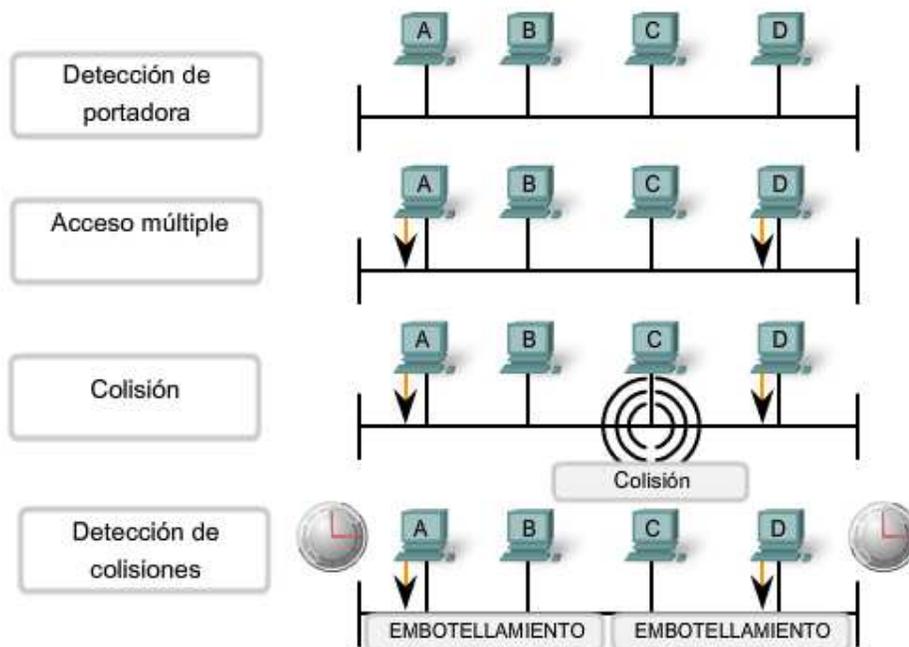
Como recordará, la Ethernet permite que los dispositivos compitan para el tiempo de transmisión. En caso de que dos dispositivos transmitan simultáneamente, el CSMA/CD de la red intenta resolver el problema. Sin embargo, recuerde que cuando se agrega un mayor número de dispositivos a la red, es posible que las colisiones sean cada vez más difíciles de resolver.

Tan pronto como se detecta una colisión, los dispositivos transmisores envían una señal de congestión de 32 bits que la impone. Esto garantiza que todos los dispositivos de la LAN detectarán la colisión.

Es importante que la señal de congestión no se detecte como una trama válida; de lo contrario, no podría identificarse la colisión. El patrón de datos que se observa con mayor frecuencia para una señal de congestión es simplemente un patrón de 1, 0, 1, 0 que se repite, al igual que el Preámbulo.

Los mensajes corrompidos, transmitidos de forma parcial, generalmente se conocen como fragmentos de colisión o runts. Las colisiones normales tienen menos de 64 octetos de longitud y, por lo tanto, reprobaban tanto la prueba de longitud mínima como la FCS, lo que facilita su identificación.

Las estaciones que detectan una colisión envían una señal de embotellamiento.

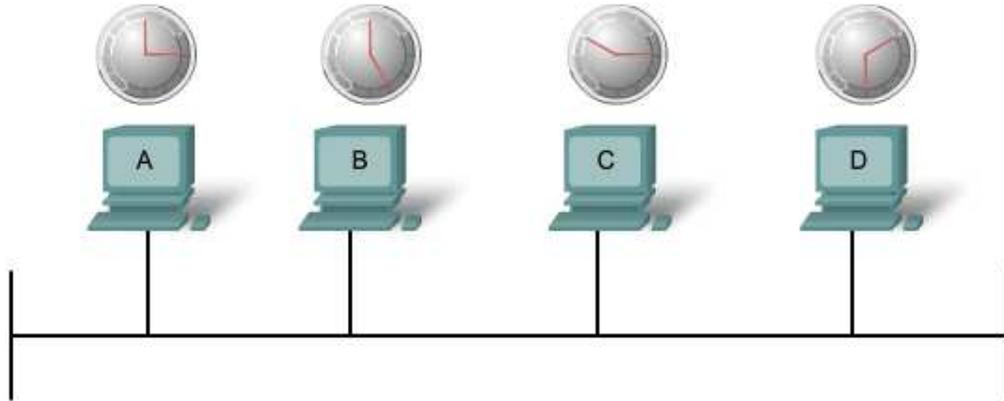


## Temporización de postergación

Una vez producida la colisión y que todos los dispositivos permitan que el cable quede inactivo (cada uno espera que se cumpla el espacio completo entre tramas), los dispositivos cuyas transmisiones sufrieron la colisión deben esperar un período adicional, y cada vez potencialmente mayor, antes de intentar la retransmisión de la trama que sufrió la colisión. El período de espera está intencionalmente diseñado para que sea aleatorio de modo que dos estaciones no demoren la misma cantidad de tiempo antes de efectuar la retransmisión, lo que causaría colisiones adicionales. Esto se logra en parte al aumentar el intervalo a partir del cual se selecciona el tiempo de retransmisión aleatorio cada vez que se efectúa un intento de retransmisión. El período de espera se mide en incrementos del intervalo de tiempo del parámetro.

Si la congestión en los medios provoca que la capa MAC no pueda enviar la trama después de 16 intentos, abandona el intento y genera un error en la capa de Red. Este tipo de sucesos es raro en una red que funciona correctamente y sólo sucedería en el caso de cargas de red extremadamente pesadas o cuando se produce un problema físico en la red. Los métodos descritos en esta sección permitían a Ethernet proporcionar un servicio superior en una topología de medios compartidos basándose en el uso de hubs. En la sección de switches que aparece a continuación, veremos cómo, mediante el uso de switches, la necesidad de utilizar el CSMA/CD comienza a disminuir o, en algunos casos, a desaparecer por completo.

## Temporización de postergación



Una vez que se recibe una señal de embotellamiento, todas las estaciones dejan de transmitir y cada una espera un periodo de tiempo aleatorio—establecido por el temporizador de postergación—antes de intentar enviar otra trama.

## 9.5 Capa física de Ethernet

### 9.5.1 Descripción general de la capa física de Ethernet

Las diferencias que existen entre Ethernet estándar, Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet tienen lugar en la capa física, generalmente denominada Ethernet PHY.

La Ethernet se rige por los estándares IEEE 802.3. Actualmente, se definen cuatro velocidades de datos para el funcionamiento con cables de fibra óptica y de par trenzado:

- 10 Mbps - Ethernet 10Base-T
- 100 Mbps - Fast Ethernet
- 1000 Mbps - Gigabit Ethernet
- 10 Gbps - 10 Gigabit Ethernet

Si bien existe una gran cantidad de implementaciones de Ethernet diferentes para estas diversas velocidades de transmisión de datos, aquí sólo se presentarán las más comunes. La figura muestra algunas de las características de la Ethernet PHY.

En esta sección se analizará la porción de Ethernet que opera en la capa física, comenzando por 10Base-T y continuando con las variedades de 10 Gbps.

## Tipos de Ethernet

Tipo de Ethernet	Ancho de banda	Tipo de cable	Duplex	Distancia máxima
10Base-5	10 Mbps	Coaxial thicknet	Half	500 m
10Base-2	10 Mbps	Coaxial thinnet	Half	185 m
100Base-TX	10 Mbps	UTP Cat3/Cat5	Half	100 m
100Base-TX	100 Mbps	UTP Cat5	Half	100 m
100Base-TX	200 Mbps	UTP Cat5	Full	100 m
100Base-TX	100 Mbps	Fibra multimodo	Half	400 m
1000Base-T	200 Mbps	Fibra multimodo	Full	2 km
1000Base-TX	1 Gbps	UTP Cat5e	Full	100 m
1000Base-SX	1 Gbps	UTP Cat6	Full	100 m
1000Base-LX	1 Gbps	Fibra multimodo	Full	550 m
10GBase-CX4	1 Gbps	Fibra monomodo	Full	2 km
10GBase-T	10 Gbps	Twinaxial	Full	100 m
10GBase-LX4	10 Gbps	UTP Cat6a/Cat7	Full	100 m
10GBase-LX4	10 Gbps	Fibra multimodo	Full	300 m
10 Mbps	10 Gbps	Fibra monomodo	Full	10 km

### 9.5.2 Ethernet de 10 y 100 Mbps

Las principales implementaciones de 10 Mbps de Ethernet incluyen:

- 10BASE5 con cable coaxial Thicknet
- 10BASE2 con cable coaxial Thinnet
- 10BASE-T con cable de par trenzado no blindado Cat3/Cat5

Las primeras implementaciones de Ethernet, 10BASE5 y 10BASE2 utilizaban cable coaxial en un bus físico. Dichas implementaciones ya no se utilizan y los más recientes estándares 802.3 no las admiten.

#### Ethernet de 10 Mbps - 10BASE-T

La 10BASE-T utiliza la codificación Manchester para dos cables de par trenzado no blindado. Las primeras implementaciones de la 10BASE-T utilizaban cableado Cat3. Sin embargo, el cableado Cat5 o superior es el que se utiliza generalmente en la actualidad.

La Ethernet de 10 Mbps se considera como la Ethernet clásica y utiliza una topología en estrella física. Los enlaces de Ethernet 10BASE-T pueden tener hasta 100 metros de longitud antes de que requieran un hub o repetidor.

La 10BASE-T utiliza dos pares de cables de cuatro pares y finaliza en cada extremo con un conector RJ-45 de 8 pins. El par conectado a los pins 1 y 2 se utiliza para transmitir y el par conectado a los pins 3 y 6 se utiliza para recibir. La figura muestra la salida de pins RJ45 utilizada con Ethernet 10BASE-T.

La 10BASE-T generalmente no se elige para instalaciones de LAN nuevas. Sin embargo, todavía existen actualmente muchas redes Ethernet 10BASE-T. El reemplazo de los hubs por los switches en redes 10BASE-T aumentó notablemente la velocidad de transmisión (throughput) disponible para estas redes y le otorgó a la Ethernet antigua una mayor longevidad. Los enlaces de 10BASE-T conectados a un switch pueden admitir el funcionamiento tanto half-duplex como full-duplex.

## Salidas 10Base-T Ethernet RJ-45



Número de Pin	Señal
1	TD+ (Transmitir datos, señal diferencial positiva)
2	TD- (Transmitir datos, señal diferencial negativa)
3	RD+ (Recibir datos, señal diferencial positiva)
4	No se utiliza
5	No se utiliza
6	RD- (Recibir datos, señal diferencial negativa)
7	No se utiliza
8	No se utiliza

### 100 Mbps - Fast Ethernet

Entre mediados y fines de la década de 1990 se establecieron varios estándares 802.3 nuevos para describir los métodos de transmisión de datos en medios Ethernet a 100 Mbps. Estos estándares utilizaban requisitos de codificación diferentes para lograr estas velocidades más altas de transmisión de datos.

La Ethernet de 100 Mbps, también denominada Fast Ethernet, puede implementarse utilizando medios de fibra o de cable de cobre de par trenzado. Las implementaciones más conocidas de la Ethernet de 100 Mbps son:

- 100BASE-TX con UTP Cat5 o mayor
- 100BASE-FX con cable de fibra óptica

Ya que las señales de mayor frecuencia que se utilizan en Fast Ethernet son más susceptibles al ruido, Ethernet de 100 Mbps utiliza dos pasos de codificación por separado para mejorar la integridad de la señal.

#### 100BASE-TX

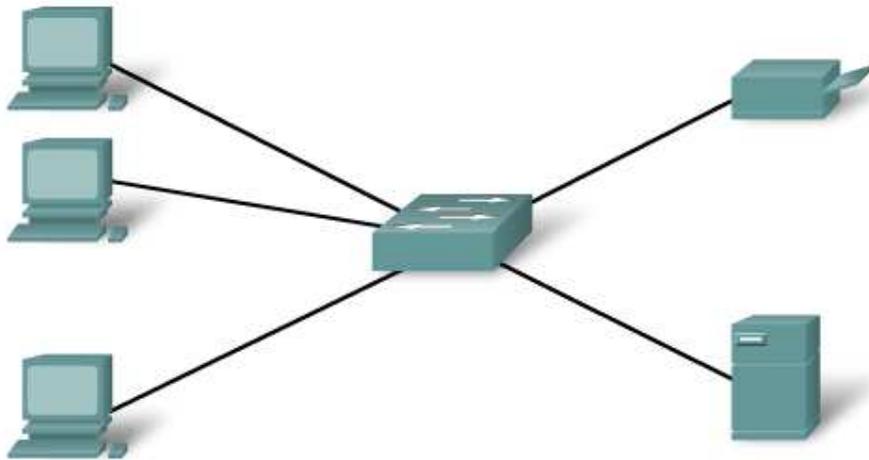
100BASE-TX fue diseñada para admitir la transmisión a través de dos hilos de fibra óptica o de dos pares de cable de cobre UTP de Categoría 5. La implementación 100BASE-TX utiliza los mismos dos pares y salidas de pares de UTP que la 10BASE-T. Sin embargo, la 100BASE-TX requiere UTP de Categoría 5 o superior. La codificación 4B/5B se utiliza para la Ethernet 100BASE-T.

Al igual que con la 10BASE-TX, la 100BASE-TX se conecta como estrella física. La figura muestra un ejemplo de una topología en estrella física. Sin embargo, a diferencia de la 10BASE-T, las redes 100BASE-TX utilizan generalmente un switch en el centro de la estrella en vez de un hub. Aproximadamente al mismo tiempo que las tecnologías 100BASE-TX se convirtieron en la norma, los switches LAN también comenzaron a implementarse con frecuencia. Estos desarrollos simultáneos llevaron a su combinación natural en el diseño de las redes 100BASE-TX.

#### 100BASE-FX

El estándar 100BASE-FX utiliza el mismo procedimiento de señalización que la 100BASE-TX, pero lo hace en medios de fibra óptica en vez de cobre UTP. Si bien los procedimientos de codificación, decodificación y recuperación de reloj son los mismos para ambos medios, la transmisión de señales es diferente: pulsos eléctricos en cobre y pulsos de luz en fibra óptica. La 100BASE-FX utiliza conectores de interfaz de fibra de bajo costo (generalmente llamados conectores SC duplex).

Las implementaciones de fibra son conexiones punto a punto, es decir, se utilizan para interconectar dos dispositivos. Estas conexiones pueden ser entre dos computadoras, entre una computadora y un switch o entre dos switches.



### 9.5.3 Ethernet de 1000 Mbps

#### 1000 Mbps - Gigabit Ethernet

El desarrollo de los estándares de Gigabit Ethernet dio como resultado especificaciones para cobre UTP, fibra monomodo y fibra multimodo. En redes de Gigabit Ethernet, los bits se producen en una fracción del tiempo que requieren en redes de 100 Mbps y redes de 10 Mbps. Gracias a que las señales se producen en menor tiempo, los bits se vuelven más susceptibles al ruido y, por lo tanto, la temporización tiene una importancia decisiva. La cuestión del rendimiento se basa en la velocidad con la que el adaptador o la interfaz de red puedan cambiar los niveles de voltaje y en la manera en que dicho cambio de voltaje pueda detectarse de un modo confiable a 100 metros de distancia en la NIC o la interfaz de recepción.

A estas mayores velocidades, la codificación y decodificación de datos es más compleja. La Gigabit Ethernet utiliza dos distintos pasos de codificación. La transmisión de datos es más eficiente cuando se utilizan códigos para representar el stream binario de bits. La codificación de datos permite la sincronización, el uso eficiente del ancho de banda y características mejoradas de relación entre señal y ruido.

#### Ethernet 1000BASE-T

La Ethernet 1000BASE-T brinda una transmisión full-duplex utilizando los cuatro pares de cable UTP Categoría 5 o superior. La Gigabit Ethernet por cables de cobre permite un aumento de 100 Mbps por par de cable a 125 Mbps por par de cable o 500 Mbps para los cuatro pares. Cada par de cable origina señales en full-duplex, lo que duplica los 500 Mbps a 1000 Mbps.

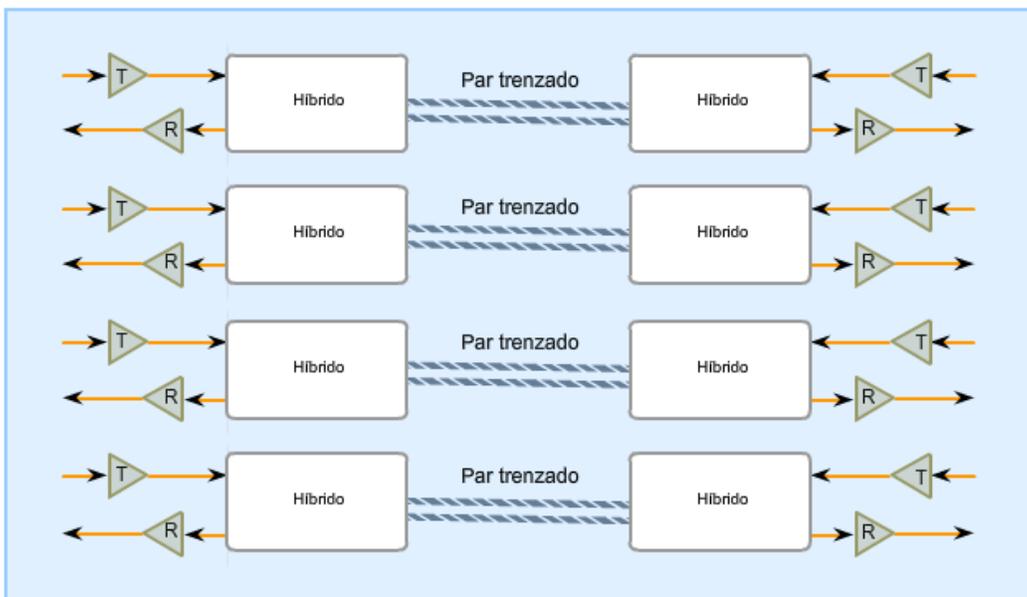
La 1000BASE-T utiliza codificación de línea 4D-PAM5 para obtener un throughput de datos de 1 Gbps. Este esquema de codificación permite señales de transmisión en cuatro pares de cables simultáneamente. Traduce un byte de 8 bits de datos en una transmisión simultánea de cuatro símbolos de código que se envían por los medios, uno en cada par, como señales de Modulación de amplitud de pulsos de 5 niveles (PAM5). Esto significa que cada símbolo se corresponde con dos bits de datos. Debido a que la información viaja simultáneamente a través de las cuatro rutas, el sistema de circuitos tiene que dividir las tramas en el transmisor y reensamblarlas en el receptor. La figura muestra una representación del sistema de circuitos que utiliza la Ethernet 1000BASE-T.

La 1000BASE-T permite la transmisión y recepción de datos en ambas direcciones (en el mismo cable y al mismo tiempo). Este flujo de tráfico crea colisiones permanentes en los pares de cables. Estas colisiones generan patrones de voltaje complejos. Los circuitos híbridos que detectan las señales utilizan técnicas sofisticadas tales como la cancelación de eco, la corrección del error de envío de Capa 1 (FEC) y una prudente selección de los niveles de voltaje. Al utilizar dichas técnicas, el sistema alcanza un throughput de 1 Gigabit.

Para contribuir a la sincronización, la capa física encapsula cada trama con delimitadores de inicio y finalización de stream. La temporización de loops se mantiene mediante streams continuos de símbolos INACTIVOS que se envían en cada par de cables durante el espacio entre tramas.

A diferencia de la mayoría de las señales digitales, en las que generalmente se encuentra un par de niveles de voltaje discretos, la 1000BASE-T utiliza muchos niveles de voltaje. En períodos inactivos, se encuentran nueve niveles de voltaje en el cable. Durante los períodos de transmisión de datos, se encuentran hasta 17 niveles de voltaje en el cable. Con este gran número de estados, combinado con los efectos del ruido, la señal en el cable parece más analógica que digital. Como en el caso del analógico, el sistema es más susceptible al ruido debido a los problemas de cable y terminación.

Circuitos 1000BASE-T



### Ethernet 1000BASE-SX y 1000BASE-LX por fibra óptica

Las versiones de fibra óptica de la Gigabit Ethernet (1000BASE-SX y 1000BASE-LX) ofrecen las siguientes ventajas sobre el UTP: inmunidad al ruido, tamaño físico pequeño y distancias y ancho de banda aumentados y sin repeticiones.

Todas las versiones de 1000BASE-SX y 1000BASE-LX admiten la transmisión binaria full-duplex a 1250 Mbps en dos hebras de fibra óptica. La codificación de la transmisión se basa en el esquema de codificación 8B/10B. Debido al gasto de esta codificación, la velocidad de transferencia de datos sigue siendo 1000 Mbps.

Cada trama de datos se encapsula en la capa física antes de la transmisión y la sincronización de los enlaces se mantiene enviando un stream continuo de grupos de códigos INACTIVOS durante el espacio entre tramas.

Las principales diferencias entre las versiones de fibra de 1000BASE-SX y 1000BASE-LX son los medios de enlace, los conectores y la longitud de onda de la señal óptica. Estas diferencias se ilustran en la figura.

Soporte de enlace de fibra 1000Base-X		
Configuración del enlace	1000Base-SX (850 nm de longitud de onda)	1000Base-LX (1300 nm de longitud de onda)
125/62.5 µm fibra óptica multimodo	Compatible	Compatible
fibra óptica multimodo de 125/50 µm	Compatible	Compatible
fibra óptica monomodo de 125/10 µm	No compatible	Compatible

## 9.5.4 Ethernet: Opciones futuras

Se adaptó el estándar IEEE 802.3ae para incluir la transmisión en full-duplex de 10 Gbps en cable de fibra óptica. El estándar 802.3ae y los estándares 802.3 para la Ethernet original son muy similares. La Ethernet de 10 Gigabits (10GbE) está evolucionando para poder utilizarse no sólo en LAN sino también en WAN y MAN.

Debido a que el formato de trama y otras especificaciones de Ethernet de Capa 2 son compatibles con estándares anteriores, la 10GbE puede brindar un mayor ancho de banda para redes individuales que sea interoperable con la infraestructura de red existente.

10Gbps se puede comparar con otras variedades de Ethernet de este modo:

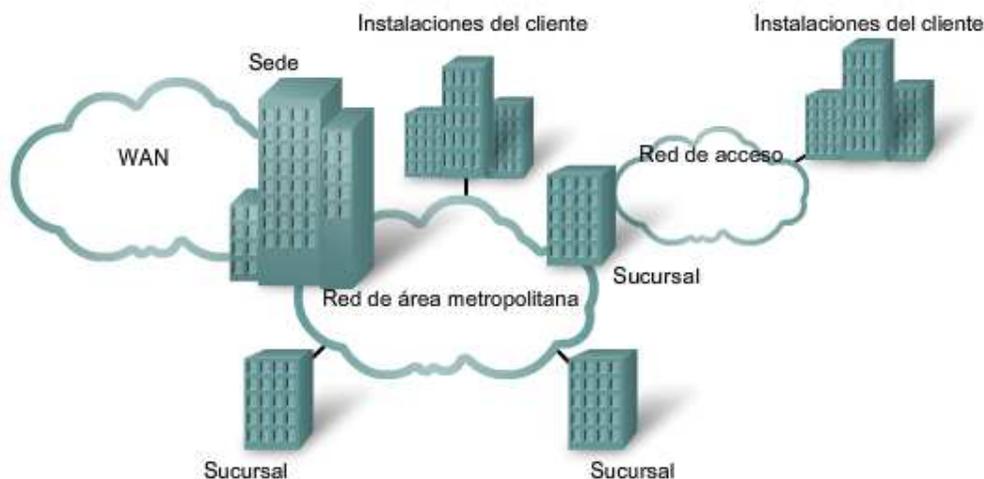
- El formato de trama es el mismo, permitiendo así la interoperabilidad entre todos los tipos de tecnologías antiguas, fast, gigabit y 10 Gigabit Ethernet, sin la necesidad de retramado o conversiones de protocolo.
- El tiempo de bit ahora es de 0,1 nanosegundos. Todas las demás variables de tiempo caen en su correspondiente lugar en la escala.
- Ya que sólo se utilizan conexiones de fibra óptica full-duplex, no hay ningún tipo de contención de medios ni se necesita el CSMA/CD.
- Se preserva la mayoría de las subcapas de 802.3 de IEEE dentro de las Capas OSI 1 y 2, con algunos pocos agregados para que se adapten a enlaces de fibra de 40 km y la posibilidad de interoperabilidad con otras tecnologías en fibra.

Con 10Gbps Ethernet es posible crear redes de Ethernet flexibles, eficientes, confiables, a un costo punto a punto relativamente bajo.

### Futuras velocidades de Ethernet

Si bien la Ethernet de 1 Gigabit es muy fácil de hallar en el mercado y cada vez es más fácil conseguir los productos de 10 Gigabits, el IEEE y la Alianza de Ethernet de 10 Gigabits trabajan actualmente en estándares para 40, 100 e inclusive 160 Gbps. Las tecnologías que se adopten dependerán de un número de factores que incluyen la velocidad de maduración de las tecnologías y de los estándares, la velocidad de adopción por parte del mercado y el costo de los productos emergentes.

La trama común Ethernet se puede aplicar a diferentes tipos de red



Ethernet					
8	6	6	2	46 a 1500	4
Preámbulo	Dirección de destino	Dirección de origen	Tipo	Datos	Secuencia de verificación de trama

## 9.6 Hubs y switches

### 9.6.1 Ethernet antigua: Utilización de hubs

En secciones anteriores, vimos cómo la Ethernet clásica utiliza medios compartidos y control de acceso al medio basado en contenciones. La Ethernet clásica utiliza hubs para interconectar los nodos del segmento de LAN. Los hubs no realizan ningún tipo de filtro de tráfico. En cambio, el hub reenvía todos los bits a todos los dispositivos conectados al hub. Esto obliga a todos los dispositivos de la LAN a compartir el ancho de banda de los medios.

Además, esta implementación de Ethernet clásica origina a menudo grandes niveles de colisiones en la LAN. Debido a estos problemas de rendimiento, este tipo de LAN Ethernet tiene un uso limitado en las redes actuales. Las implementaciones de Ethernet con hubs se utilizan generalmente en la actualidad en LAN pequeñas o LAN con pocos requisitos de ancho de banda.

El hecho de que los dispositivos compartan medios crea problemas significativos a medida que la red crece. La figura ilustra algunas de los problemas que aquí se presentan.

#### Escalabilidad

En una red con hubs, existe un límite para la cantidad de ancho de banda que los dispositivos pueden compartir. Con cada dispositivo que se agrega al medio compartido, el ancho de banda promedio disponible para cada dispositivo disminuye. Con cada aumento de la cantidad de dispositivos en los medios, el rendimiento se ve degradado.

#### Latencia

La latencia de la red es la cantidad de tiempo que le lleva a una señal llegar a todos los destinos del medio. Cada nodo de una red basada en hubs debe esperar una oportunidad de transmisión para evitar colisiones. La latencia puede aumentar notablemente a medida que la distancia entre los nodos se extiende. La latencia también se ve afectada por un retardo de la señal en los medios, como así también por el retardo añadido por el procesamiento de las señales mediante hubs y repetidores. El aumento de la longitud de los medios o de la cantidad de hubs y repetidores conectados a un segmento origina una mayor latencia. A mayor latencia, mayor probabilidad de que los nodos no reciban las señales iniciales, lo que aumenta las colisiones presentes en la red.

#### Falla de red

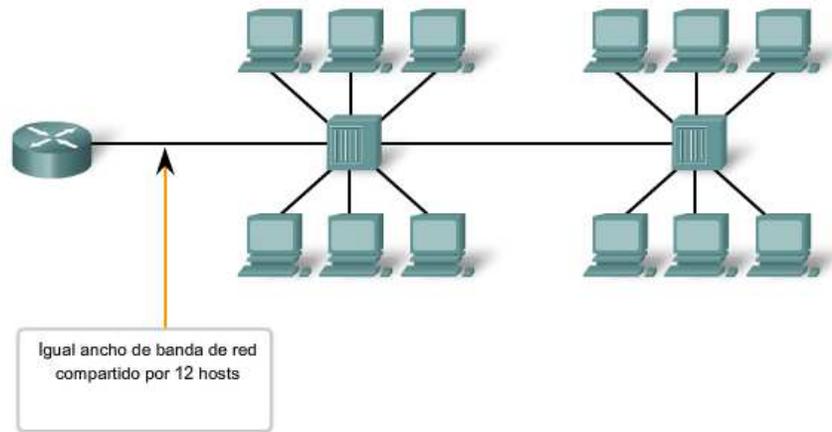
Debido a que la Ethernet clásica comparte los medios, cualquier dispositivo de la red puede potencialmente ocasionar problemas para otros dispositivos. Si cualquier dispositivo conectado al hub genera tráfico perjudicial, puede verse impedida la comunicación de todos los dispositivos del medio. Este tráfico perjudicial puede deberse a una velocidad incorrecta o a los ajustes de full-duplex de la NIC.

#### Colisiones

Según el CSMA/CD, un nodo no debería enviar un paquete a menos que la red esté libre de tráfico. Si dos nodos envían paquetes al mismo tiempo, se produce una colisión y los paquetes se pierden. Entonces, ambos nodos envían una señal de congestión, esperan una cantidad de tiempo aleatoria y retransmiten sus paquetes. Cualquier parte de la red en donde los paquetes de dos o más nodos puedan interferir entre ellos se considera como un dominio de colisiones. Una red con una gran cantidad de nodos en el mismo segmento tiene un dominio de colisiones mayor y, generalmente, más tráfico. A medida que aumenta la cantidad de tráfico en la red, aumentan las posibilidades de colisión.

Los switches brindan una alternativa para el entorno basado en contenciones de la Ethernet clásica.

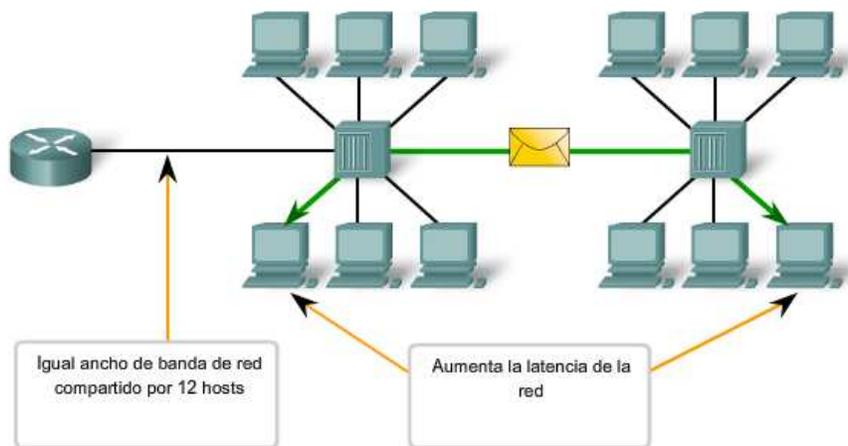
Rendimiento deficiente de las LAN basadas en hubs



Redefinir **Falta de escalabilidad** Mayor latencia

Más colisiones

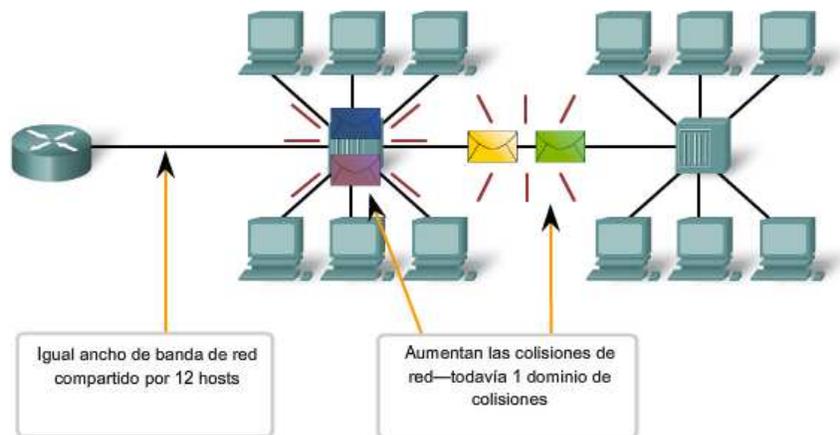
Rendimiento deficiente de las LAN basadas en hubs



Redefinir Falta de escalabilidad **Mayor latencia**

Más colisiones

Rendimiento deficiente de las LAN basadas en hubs



Redefinir Falta de escalabilidad Mayor latencia

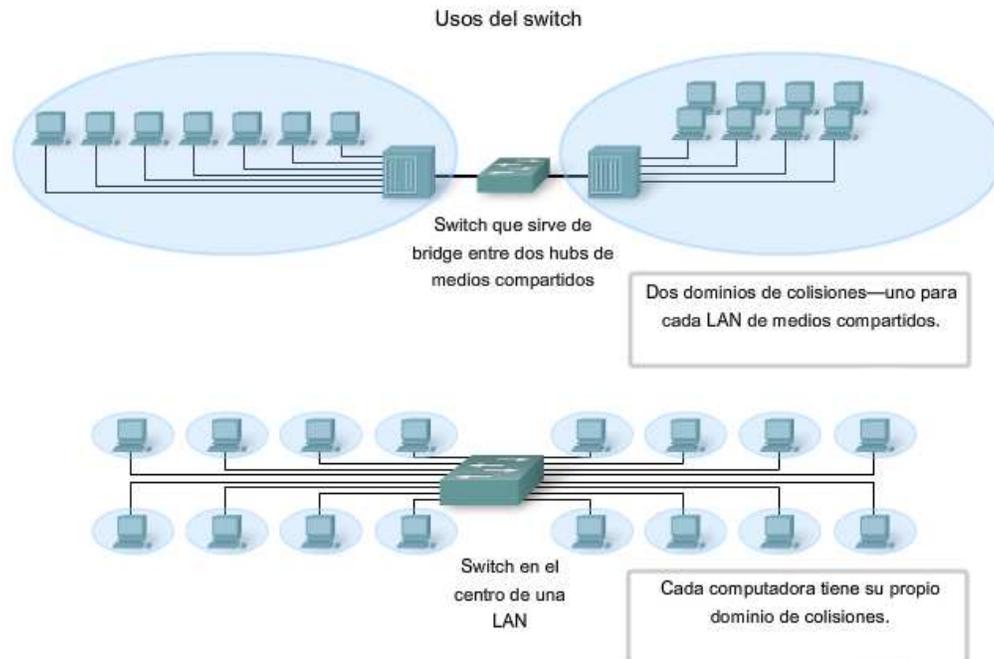
**Más colisiones**

## 9.6.2 Ethernet antigua: Utilización de switches

En los últimos años, los switches se convirtieron rápidamente en una parte fundamental de la mayoría de las redes. Los switches permiten la segmentación de la LAN en distintos dominios de colisiones. Cada puerto de un switch representa un dominio de colisiones distinto y brinda un ancho de banda completo al nodo o a los nodos conectados a dicho puerto. Con una menor cantidad de nodos en cada dominio de colisiones, se produce un aumento en el ancho de banda promedio disponible para cada nodo y se reducen las colisiones.

Una LAN puede tener un switch centralizado que conecta a hubs que todavía brindan conectividad a los nodos. O bien, una LAN puede tener todos los nodos conectados directamente a un switch. Estas topologías se ilustran en la figura.

En una LAN en la que se conecta un hub a un puerto de un switch, todavía existe un ancho de banda compartido, lo que puede producir colisiones dentro del entorno compartido del hub. Sin embargo, el switch aislará el segmento y limitará las colisiones para el tráfico entre los puertos del hub.



### Los nodos se conectan directamente

En una LAN en la que todos los nodos están conectados directamente al switch, el throughput de la red aumenta notablemente. Las tres principales razones de este aumento son:

- Ancho de banda dedicado a cada puerto
- Entorno libre de colisiones
- Operación full-duplex

Estas topologías físicas en estrella son esencialmente enlaces punto a punto.

### Ancho de banda dedicado

Cada nodo dispone del ancho de banda de los medios completo en la conexión entre el nodo y el switch. Debido a que un hub replica las señales que recibe y las envía a todos los demás puertos, los hubs de Ethernet clásica forman un bus lógico. Esto significa que todos los nodos deben compartir el mismo ancho de banda para este bus. Con los switches, cada dispositivo tiene una conexión punto a punto dedicada entre el dispositivo y el switch, sin contención de medios.

A modo de ejemplo, pueden compararse dos LAN de 100 Mbps, cada una de ellas con 10 nodos. En el segmento de red A, los 10 nodos se conectan a un hub. Cada nodo comparte el ancho de banda de 100 Mbps disponible. Esto ofrece un promedio de 10 Mbps para cada nodo. En el segmento de red B, los 10 nodos se conectan a un switch. En este segmento, los 10 nodos tienen el ancho de banda completo de 100 Mbps disponible.

Incluso en este ejemplo de red pequeña, el aumento del ancho de banda es significativo. A medida que la cantidad de nodos aumenta, la discrepancia entre el ancho de banda disponible para las dos implementaciones aumenta significativamente.

## Entorno libre de colisiones

Una conexión punto a punto dedicada a un switch también evita contenciones de medios entre dispositivos, lo que permite que un nodo funcione con pocas colisiones o ninguna colisión. En una red Ethernet clásica de tamaño moderado que utiliza hubs, aproximadamente entre el 40% y el 50% del ancho de banda se consume en la recuperación por colisiones. En una red Ethernet con switch, en la que prácticamente no hay colisiones, el gasto destinado a la recuperación por colisiones se elimina casi por completo. Esto le ofrece a la red con switches tasas de throughput significativamente mejoradas.

## Funcionamiento full-duplex

La utilización de switches también le permite a una red funcionar como entorno de Ethernet full-duplex. Antes de que existieran los switches, la Ethernet sólo era half-duplex. Esto implicaba que en un momento dado un nodo podía transmitir o recibir. Con la característica full-duplex habilitada en una red Ethernet con switches, los dispositivos conectados directamente a los puertos del switch pueden transmitir y recibir simultáneamente con el ancho de banda completo de los medios.

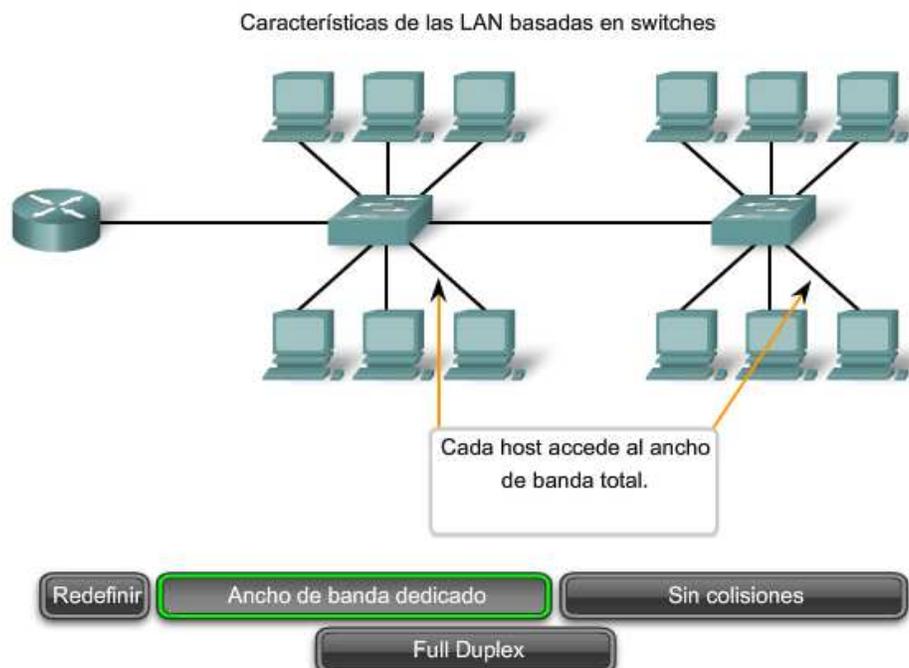
La conexión entre el dispositivo y el switch está libre de colisiones. Esta disposición efectivamente duplica la velocidad de transmisión cuando se la compara con la half-duplex. Por ejemplo, si la velocidad de la red es de 100 Mbps, cada nodo puede transmitir una trama a 100 Mbps y, al mismo tiempo, recibir una trama a 100 Mbps.

## Utilización de switches en lugar de hubs

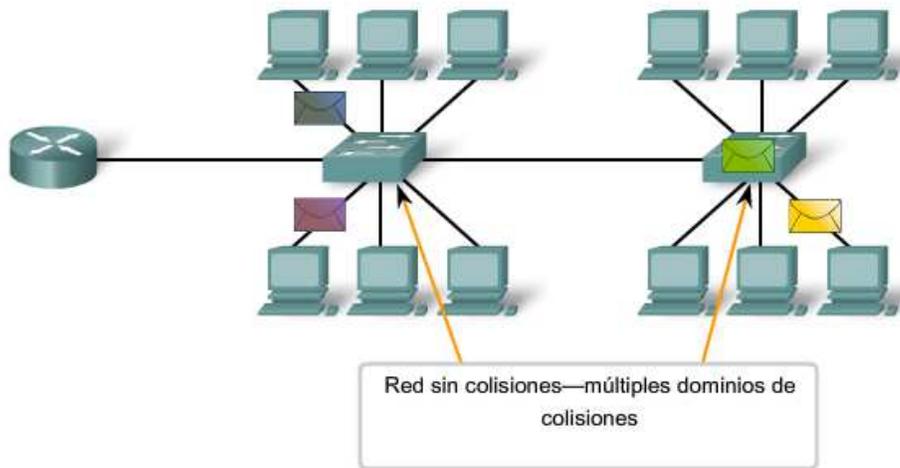
Gran parte de la Ethernet moderna utiliza switches para los dispositivos finales y opera en full duplex. Debido a que los switches brindan mucho más throughput que los hubs y aumentan el rendimiento tan notablemente, es justo preguntarse: ¿por qué no utilizamos switches en todas las LAN Ethernet? Existen tres razones por las que los hubs siguen utilizándose:

- Disponibilidad: los switches de LAN no se desarrollaron hasta comienzos de la década de 1990 y no estuvieron disponibles hasta mediados de dicha década. Las primeras redes Ethernet utilizaban hubs de UTP y muchas de ellas continúan funcionando hasta el día de hoy.
- Económicas. En un principio, los switches resultaban bastante costosos. A medida que el precio de los switches se redujo, la utilización de hubs disminuyó y el costo es cada vez menos un factor al momento de tomar decisiones de implementación.
- Requisitos: Las primeras redes LAN eran redes simples diseñadas para intercambiar archivos y compartir impresoras. Para muchas ubicaciones, las primeras redes evolucionaron hasta convertirse en las redes convergentes de la actualidad, lo que originó una necesidad imperante de un mayor ancho de banda disponible para los usuarios individuales. En algunos casos, sin embargo, será suficiente con un hub de medios compartidos y estos productos permanecen en el mercado.

La siguiente sección estudia la operación básica de los switches y cómo un switch logra el rendimiento mejorado del que ahora dependen nuestras redes. En un curso posterior se presentarán más detalles y tecnologías adicionales relacionadas con la conmutación.

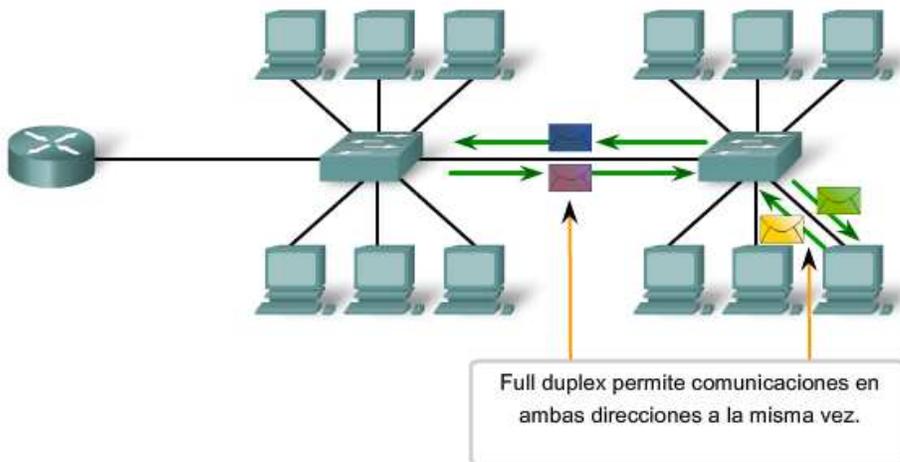


### Características de las LAN basadas en switches



Redefinir Ancho de banda dedicado Sin colisiones Full Duplex

### Características de las LAN basadas en switches



Redefinir Ancho de banda dedicado Sin colisiones Full Duplex

## 9.6.3 Switches: Reenvío selectivo

Los switches Ethernet reenvían selectivamente tramas individuales desde un puerto receptor hasta el puerto en el que esté conectado el nodo de destino. Este proceso de reenvío selectivo puede pensarse como la posibilidad de establecer una conexión punto a punto momentánea entre los nodos de transmisión y recepción. La conexión se establece sólo durante el tiempo suficiente como para enviar una sola trama. Durante este instante, los dos nodos tienen una conexión de ancho de banda completa entre ellos y representan una conexión lógica punto a punto.

Para ser más precisos en términos técnicos, esta conexión temporal no se establece entre los dos nodos de manera simultánea. Básicamente, esto hace que la conexión entre los hosts sea una conexión punto a punto. De hecho, cualquier nodo que funcione en modo full-duplex puede transmitir en cualquier momento que tenga una trama, independientemente de la disponibilidad del nodo receptor. Esto sucede porque un switch LAN almacena una trama entrante en la memoria búfer y después la envía al puerto correspondiente cuando dicho puerto está inactivo. Este proceso se denomina almacenar y enviar.

Con la conmutación almacenar y enviar, el switch recibe la trama completa, controla el FSC en busca de errores y reenvía la trama al puerto indicado para el nodo de destino. Debido a que los nodos no deben esperar a que el medio esté inactivo, los nodos pueden enviar y recibir a la velocidad completa del medio sin pérdidas ocasionadas por colisiones o el gasto asociado con la administración de colisiones.

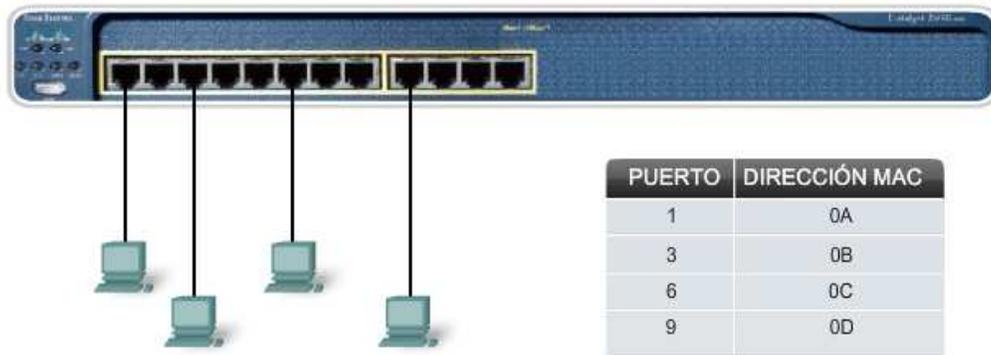
### El reenvío se basa en la MAC de destino

El switch mantiene una tabla, denominada tabla MAC que hace coincidir una dirección MAC de destino con el puerto utilizado para conectarse a un nodo. Para cada trama entrante, la dirección MAC de destino en el encabezado de la trama se compara con la lista de direcciones de la tabla MAC. Si se produce una coincidencia, el número de puerto de la tabla que se asoció con la dirección MAC se utiliza como puerto de salida para la trama.

La tabla MAC puede denominarse de diferentes maneras. Generalmente, se la llama tabla de switch. Debido a que la conmutación deriva de una tecnología más antigua denominada bridging transparente, la tabla suele denominarse tabla del puente. Por esta razón, muchos de los procesos que realizan los switches LAN pueden contener las palabras bridge o bridging en su nombre.

Un bridge es un dispositivo que se utilizaba con mayor frecuencia en los inicios de la LAN para conectar dos segmentos de red física. Los switches pueden utilizarse para realizar esta operación, a la vez que permiten la conectividad del dispositivo final con la LAN. Muchas otras tecnologías se desarrollaron en torno a los switches LAN. Muchas de estas tecnologías se presentarán en otro curso. Un entorno en el que prevalecen los bridges son las redes inalámbricas. Utilizamos bridges inalámbricos para interconectar dos segmentos de red inalámbrica. Por lo tanto, encontrará que la industria de redes utiliza ambos términos, conmutación y bridging.

Switches: reenvío selectivo

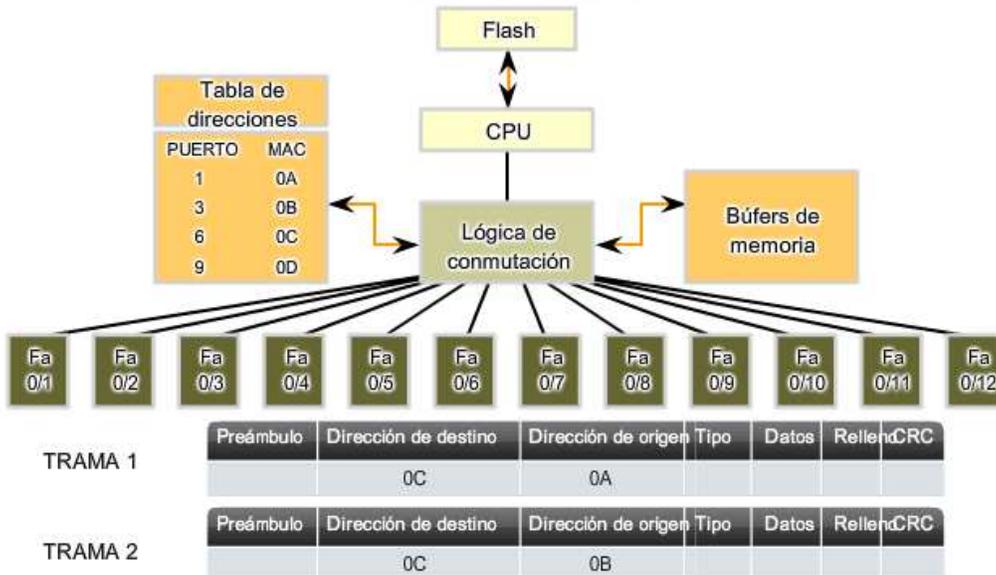


TRAMA 1	Preámbulo	Dirección de destino	Dirección de origen	Tipo	Datos	Relleno	CRC
		0C	0A				

TRAMA 2	Preámbulo	Dirección de destino	Dirección de origen	Tipo	Datos	Relleno	CRC
		0C	0D				

Switches: reenvío selectivo



## Funcionamiento del switch

Para lograr su fin, los switches LAN Ethernet realizan cinco operaciones básicas:

- Aprendizaje
- Actualización
- Inundación
- Reenvío selectivo
- Filtrado

### Aprendizaje

La tabla MAC debe llenarse con las direcciones MAC y sus puertos correspondientes. El proceso de aprendizaje permite que estos mapeos se adquieran dinámicamente durante el funcionamiento normal.

A medida que cada trama ingresa al switch, el switch analiza la dirección MAC de origen. Mediante un proceso de búsqueda, el switch determina si la tabla ya contiene una entrada para esa dirección MAC. Si no existe ninguna entrada, el switch crea una nueva entrada en la tabla MAC utilizando la dirección MAC de origen y asocia la dirección con el puerto en el que llegó la entrada. Ahora, el switch puede utilizar este mapeo para reenviar tramas a este nodo.

### Actualización

Las entradas de la tabla MAC que se adquirieron mediante el proceso de Aprendizaje reciben una marca horaria. La marca horaria se utiliza como instrumento para eliminar las entradas antiguas de la tabla MAC. Después de que se crea una entrada en la tabla MAC, un proceso comienza una cuenta regresiva utilizando la marca horaria como el valor inicial. Una vez que el valor alcanza 0, la entrada de la tabla se actualizará la próxima vez que el switch reciba una trama de ese nodo en el mismo puerto.

### Flooding

Si el switch no sabe a qué puerto enviar una trama porque la dirección MAC de destino no se encuentra en la tabla MAC, el switch envía la trama a todos los puertos, excepto al puerto en el que llegó la trama. El proceso que consiste en enviar una trama a todos los segmentos se denomina inundación. El switch no reenvía la trama al puerto en el que llegó la trama porque cualquier destino de ese segmento ya habrá recibido la trama. La inundación también se utiliza para tramas que se envían a la dirección MAC de broadcast.

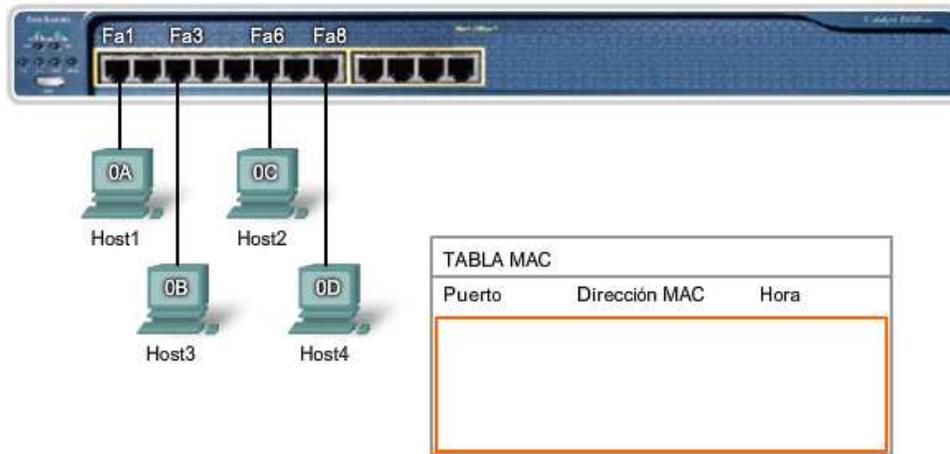
### Reenvío selectivo

El reenvío selectivo es el proceso por el cual se analiza la dirección MAC de destino de una trama y se la reenvía al puerto correspondiente. Ésta es la función principal del switch. Cuando una trama de un nodo llega al switch y el switch ya aprendió su dirección MAC, dicha dirección se hace coincidir con una entrada de la tabla MAC y la trama se reenvía al puerto correspondiente. En lugar de saturar la trama hacia todos los puertos, el switch envía la trama al nodo de destino a través del puerto indicado. Esta acción se denomina reenvío..

### Filtrado

En algunos casos, la trama no se reenvía. Este proceso se denomina filtrado de la trama. Uno de los usos del filtrado ya se describió: un switch no reenvía una trama al mismo puerto en el que llega. El switch también descartará una trama corrupta. Si una trama no aprueba la verificación CRC, dicha trama se descarta. Otra razón por la que una trama se filtra es por motivos de seguridad. Un switch tiene configuraciones de seguridad para bloquear tramas hacia o desde direcciones MAC selectivas o puertos específicos.

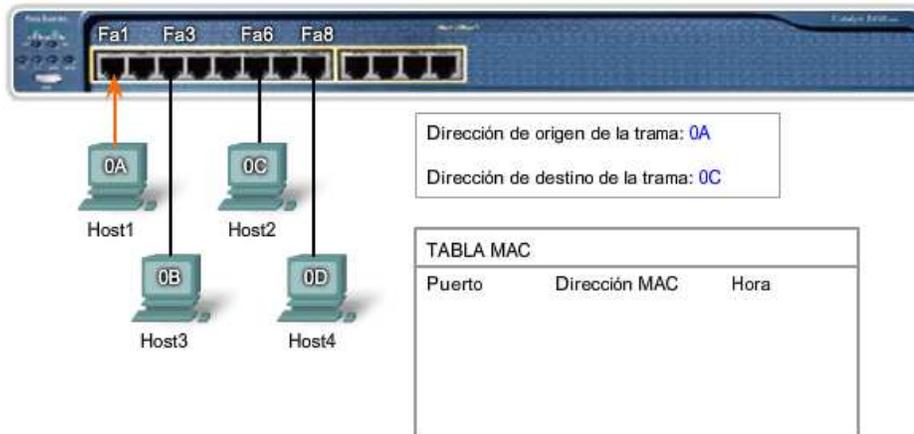
### Funcionamiento del switch



Al iniciar el switch, la tabla de direcciones MAC está vacía.



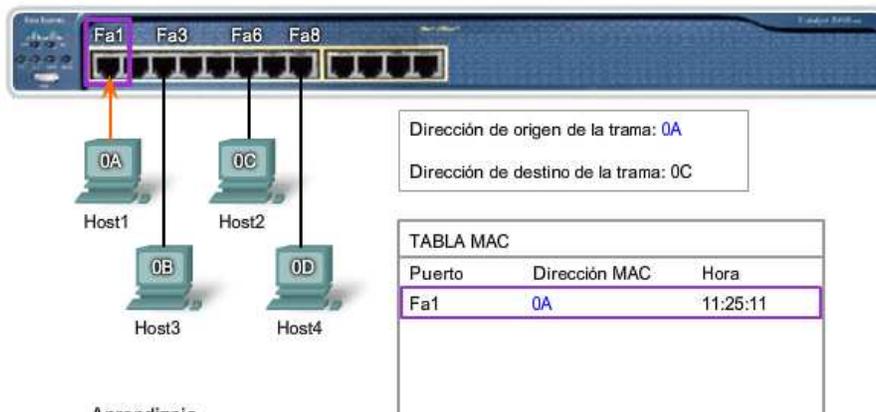
### Funcionamiento del switch



El Host1 envía datos al Host2. La trama enviada contiene una dirección MAC de origen y una dirección MAC de destino.



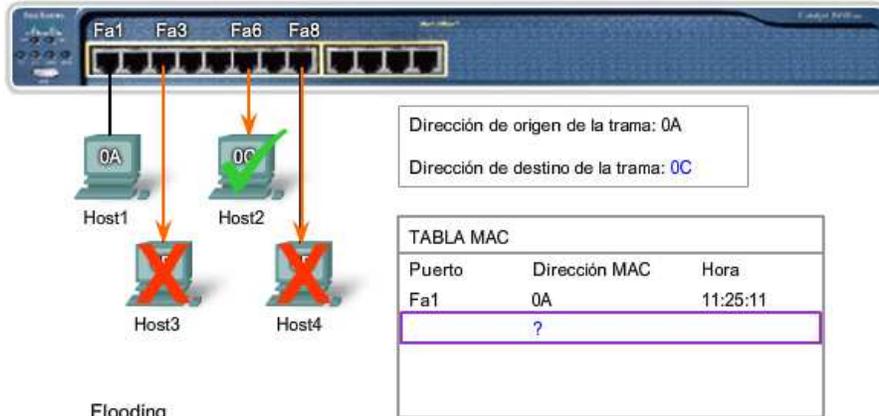
### Funcionamiento del switch



### Aprendizaje

El switch lee la dirección MAC de origen, 0A, de la trama recibida en el puerto Fa1 y la almacena en la tabla de direcciones MAC para utilizarla en el reenvío de tramas al Host1.

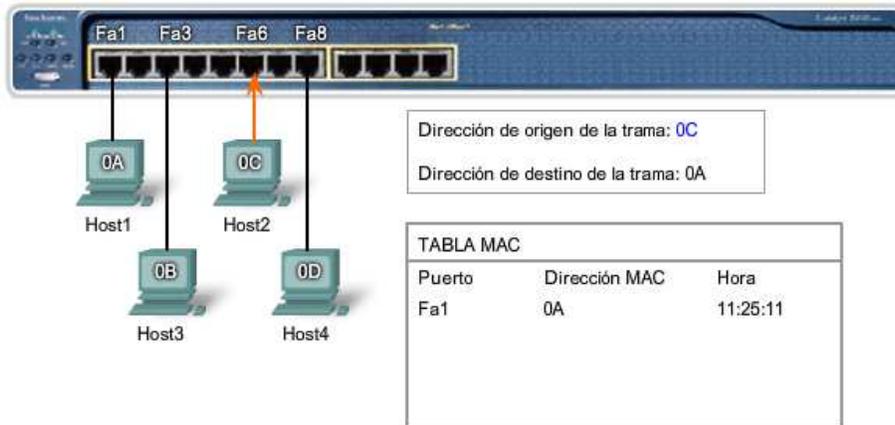
Funcionamiento del switch



Flooding

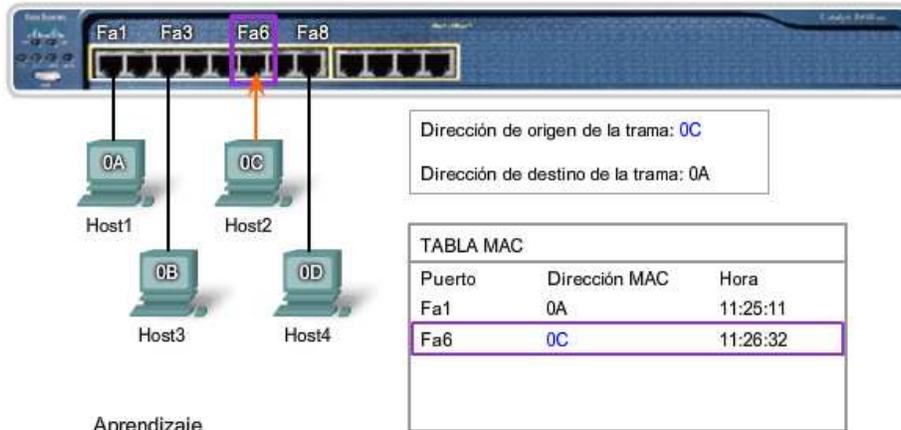
La dirección MAC de destino, 0C, no está en la tabla MAC. El switch inunda la trama desde todos los puertos excepto Fa1, el puerto del emisor. Host3 y Host4 la reciben, pero la dirección que está en la trama no coincide con sus direcciones MAC. Descartan la trama. La dirección MAC de destino en la trama coincide con Host2 y éste acepta la trama.

Funcionamiento del switch



Host2 le envía a Host1 una trama que contiene una respuesta. La dirección de origen en la trama es la dirección MAC de Host2. La dirección de destino en la trama coincide con la dirección MAC de Host1.

### Funcionamiento del switch

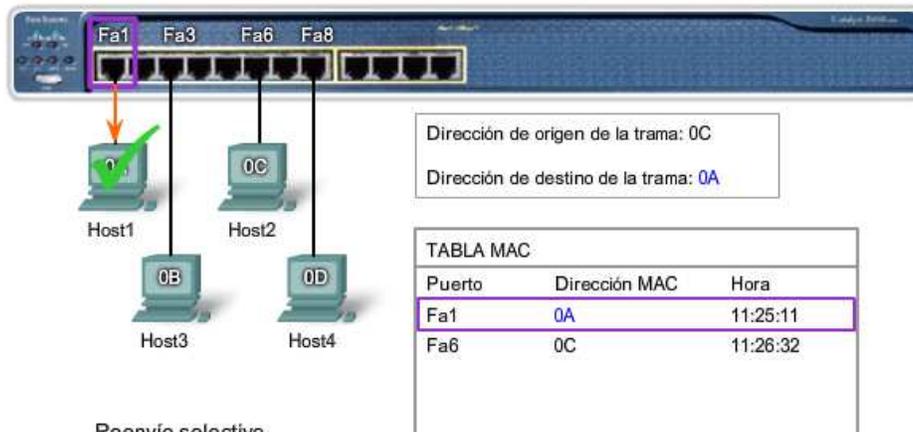


#### Aprendizaje

El switch lee la dirección MAC de origen, 0C, de la trama recibida en el puerto Fa6 y la almacena en la tabla de direcciones MAC para utilizarla en el reenvío de tramas a Host2.



### Funcionamiento del switch



#### Reenvío selectivo

La dirección MAC de destino, 0A, está en la tabla de direcciones MAC. El switch envía selectivamente la trama sólo desde el puerto Fa1. La dirección MAC de destino en la trama coincide con la dirección MAC de Host1. Host 1 acepta la trama.



## 9.6.4 Ethernet: comparación de hubs y switches

### Actividad

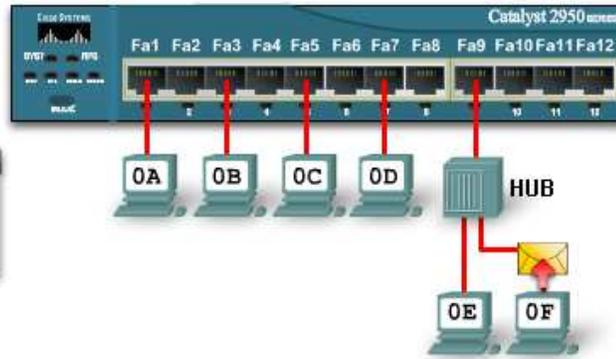
Determine el modo en que el switch envía una trama según las direcciones MAC de origen y de destino y la información en la tabla MAC del switch.

Conteste las preguntas a continuación utilizando la

Preambulo	MAC de destino	MAC de origen	Tipo de longitud	Datos encapsulados	Fin de la trama
	0A	0F			

Tabla MAC					
Fa1	Fa2	Fa3	Fa4	Fa5	Fa6
Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
		0E	0F		



1. ¿Adónde enviará el switch la trama?

- Fa1     Fa4     Fa7     Fa10  
 Fa2     Fa5     Fa8     Fa11  
 Fa3     Fa6     Fa9     Fa12

2. Cuando el switch envía la trama, ¿qué enunciado o enunciados son correctos?

- El switch agrega la dirección MAC de origen a la tabla MAC.  
 La trama es una trama de broadcast que se enviará a todos los puertos.  
 La trama es una trama unicast que se enviará sólo al puerto específico.  
 La trama es una trama unicast que se enviará por inundación a todos los puertos.  
 La trama es una trama unicast pero se descartará en el switch.

## 9.7 Address Resolution Protocol (ARP)

### 9.7.1 El proceso de ARP: Mapeo de direcciones IP a direcciones MAC

El protocolo ARP ofrece dos funciones básicas:

- Resolución de direcciones IPv4 a direcciones MAC.
- Mantenimiento de una caché de las asignaciones.

#### Resolución de direcciones IPv4 a direcciones MAC

Para que una trama se coloque en los medios de la LAN, debe contar con una dirección MAC de destino. Cuando se envía un paquete a la capa de Enlace de datos para que se lo encapsule en una trama, el nodo consulta una tabla en su memoria para encontrar la dirección de la capa de Enlace de datos que se mapea a la dirección IPv4 de destino. Esta tabla se denomina tabla ARP o caché ARP. La tabla ARP se almacena en la RAM del dispositivo.

Cada entrada o fila de la tabla ARP tiene un par de valores: una dirección IP y una dirección MAC. La relación entre los dos valores se denomina mapa, que simplemente significa que usted puede localizar una dirección IP en la tabla y descubrir la dirección MAC correspondiente. La tabla ARP almacena el mapeo de los dispositivos de la LAN local en la memoria caché.

Para comenzar el proceso, un nodo transmisor intenta localizar en la tabla ARP la dirección MAC mapeada a un destino IPv4. Si este mapa está almacenado en la tabla, el nodo utiliza la dirección MAC como la MAC de destino en la trama que encapsula el paquete IPv4. La trama se codifica entonces en los medios de la red.

#### Mantenimiento de una tabla ARP

La tabla ARP se mantiene dinámicamente. Existen dos maneras en las que un dispositivo puede reunir direcciones MAC. Una es monitorear el tráfico que se produce en el segmento de la red local. A medida que un nodo recibe tramas de los medios, puede registrar las direcciones IP y MAC de origen como mapeos en la tabla ARP. A medida que las tramas se transmiten en la red, el dispositivo completa la tabla ARP con los pares de direcciones.

Otra manera en la que un dispositivo puede obtener un par de direcciones es emitir una solicitud de ARP. El ARP envía un broadcast de Capa 2 a todos los dispositivos de la LAN Ethernet. La trama contiene un paquete de solicitud de ARP con la dirección IP del host de destino. El nodo que recibe la trama y que identifica la dirección IP como si fuera la suya

responde enviando un paquete de respuesta de ARP al emisor como una trama unicast. Esta respuesta se utiliza entonces para crear una entrada nueva en la tabla ARP.

Estas entradas dinámicas de la tabla MAC tienen una marca horaria similar a la de las entradas de la tabla MAC en los switches. Si un dispositivo no recibe una trama de un determinado dispositivo antes de que venza la marca horaria, la entrada para este dispositivo se elimina de la tabla ARP.

Además, pueden ingresarse entradas estáticas de mapas en una tabla ARP, pero esto no sucede con frecuencia. Las entradas estáticas de la tabla ARP caducan cuando pasa el tiempo y deben eliminarse en forma manual.

## Creación de la trama

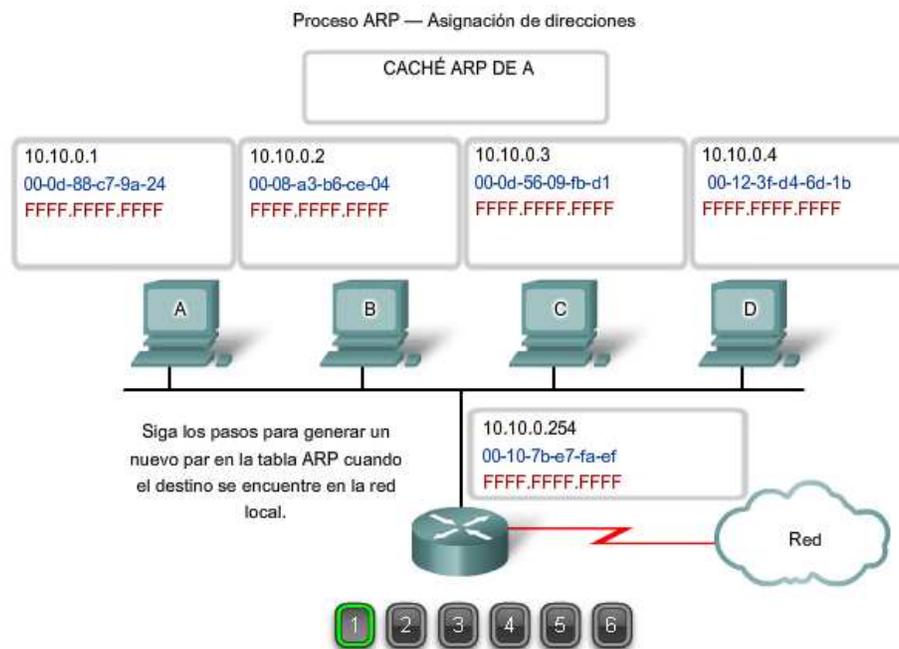
¿Qué hace un nodo cuando debe crear una trama y la caché ARP no contiene un mapa de una dirección IP hacia una dirección MAC de destino? Cuando el ARP recibe una solicitud para mapear una dirección IPv4 a una dirección MAC, busca el mapa almacenado en su tabla ARP. Si no encuentra la entrada, la encapsulación del paquete IPv4 no se realiza y los procesos de Capa 2 notifican al ARP que necesita un mapa.

Los procesos ARP envían entonces un paquete de solicitud de ARP para descubrir la dirección MAC del dispositivo de destino de la red local. Si un dispositivo que recibe la solicitud tiene la dirección IP de destino, responde con una respuesta ARP. Se crea un mapa en la tabla ARP. Los paquetes para esa dirección IPv4 pueden ahora encapsularse en tramas.

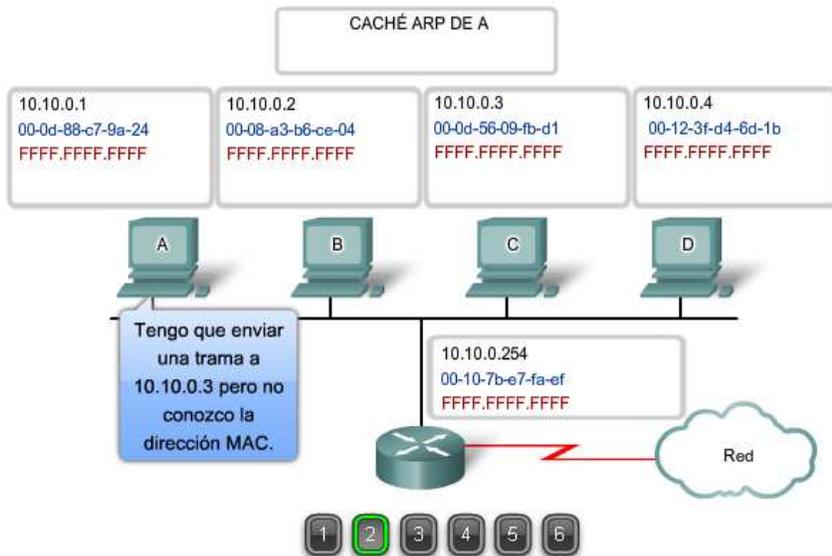
Si ningún dispositivo responde a la solicitud de ARP, el paquete se descarta porque no puede crearse una trama. Esta falla de encapsulación se informa a las capas superiores del dispositivo. Si el dispositivo es un dispositivo intermedio, como por ejemplo, un router, las capas superiores pueden optar por responder al host de origen con un error en un paquete ICMPv4.

Haga clic en los números de los pasos que aparecen en la figura para ver el proceso que se utiliza para obtener la dirección MAC de un nodo de la red física local.

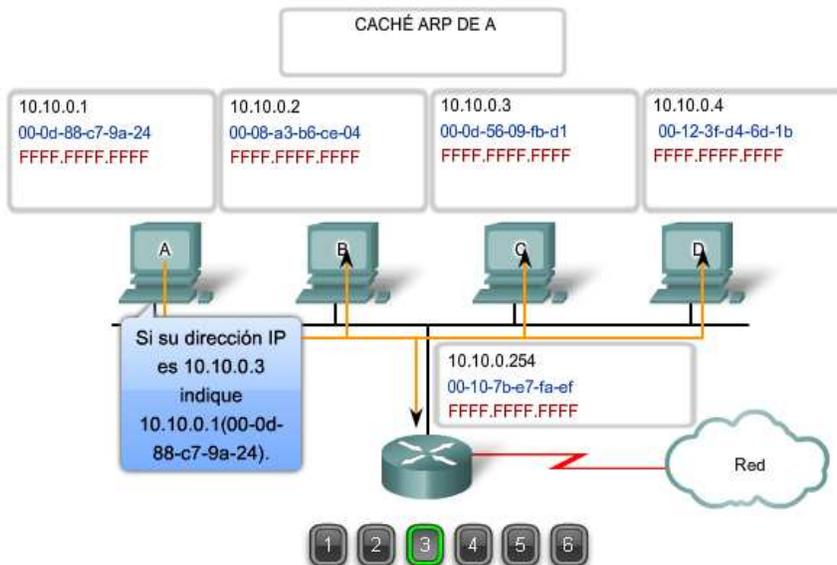
En la práctica de laboratorio, utilizará Wireshark para observar las solicitudes y respuestas de ARP en toda una red.



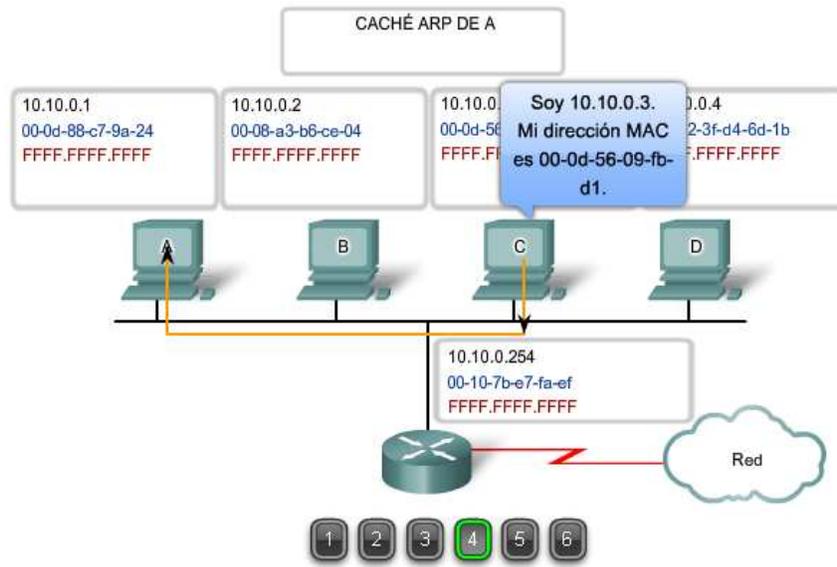
Proceso ARP — No hay entrada ARP



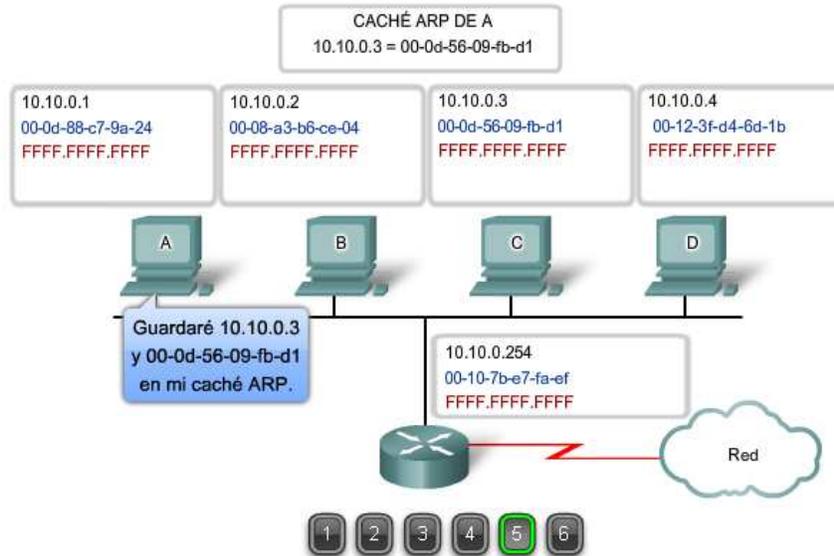
Proceso ARP — Solicitud de ARP broadcast a los dispositivos



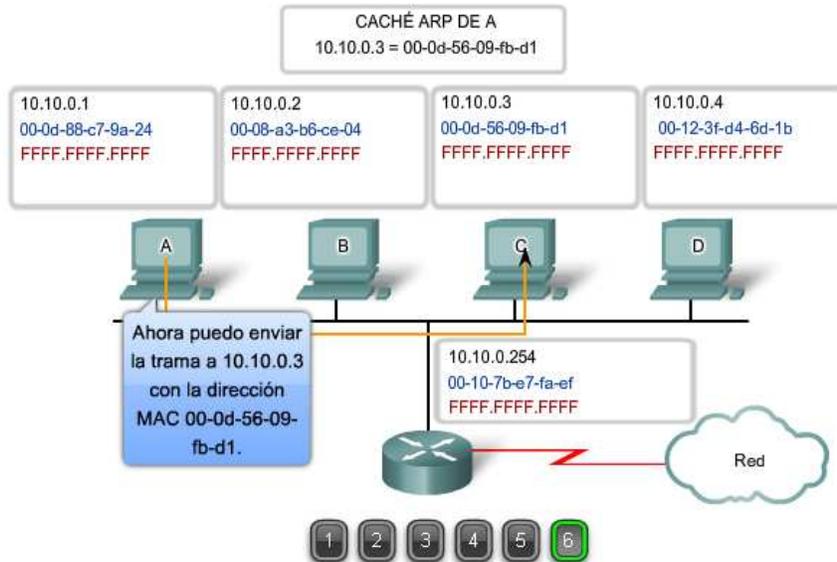
Proceso ARP — Respuesta ARP unicast con la dirección MAC



Proceso ARP — Direcciones IP y MAC almacenadas en caché ARP



Proceso ARP — Entrada ARP habilita el envío de la trama



## 9.7.2 El proceso de ARP: Destinos fuera de la red local

Todas las tramas deben enviarse a un nodo de un segmento de la red local. Si el host IPv4 de destino se encuentra en la red local, la trama utilizará la dirección MAC de este dispositivo como la dirección MAC de destino.

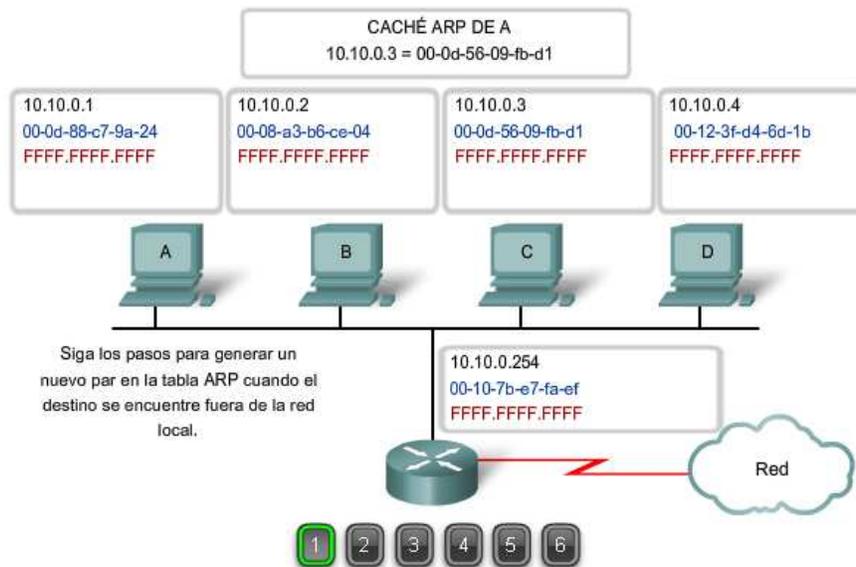
Si el host IPv4 de destino no se encuentra en la red local, el nodo de origen necesita enviar la trama a la interfaz del router que es el gateway o el siguiente salto que se utiliza para llegar a dicho destino. El nodo de origen utilizará la dirección MAC del gateway como dirección de destino para las tramas que contengan un paquete IPv4 dirigido a hosts que se encuentren en otras redes.

La dirección de gateway de la interfaz del router se almacena en la configuración IPv4 de los hosts. Cuando un host crea un paquete para un destino, compara la dirección IP de destino con su propia dirección IP para determinar si las dos direcciones IP se encuentran en la misma red de Capa 3. Si el host receptor no se encuentra en la misma red, el origen utiliza el proceso de ARP para determinar una dirección MAC para la interfaz del router que sirve de gateway.

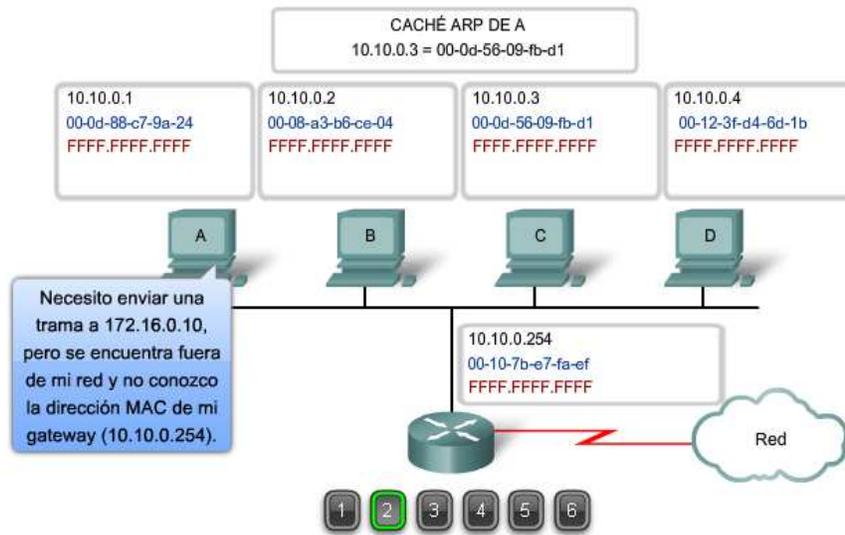
En caso de que la entrada de gateway no se encuentre en la tabla, el proceso de ARP normal enviará una solicitud de ARP para recuperar la dirección MAC asociada con la dirección IP de la interfaz del router.

Haga clic en los números de pasos que aparecen en la figura para ver el proceso que se utiliza para obtener la dirección MAC del gateway.

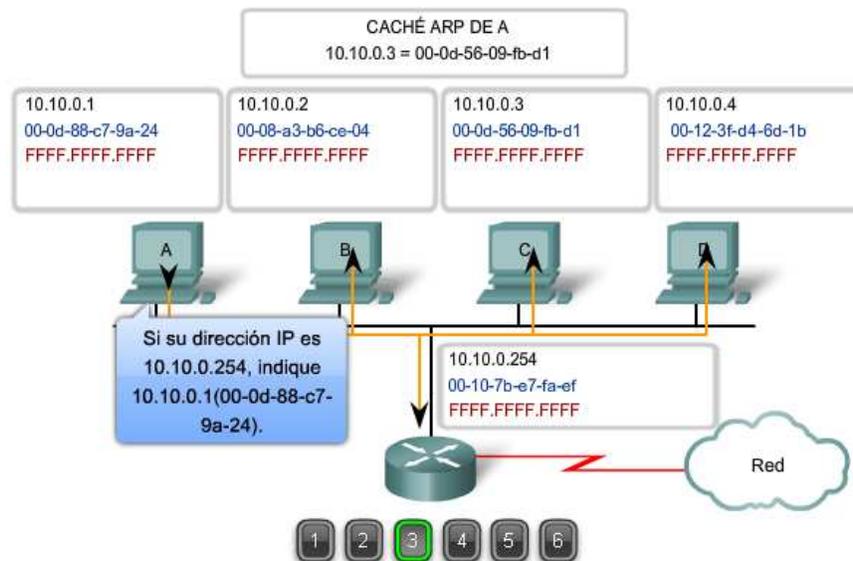
### ARP—Comunicación fuera de la red local



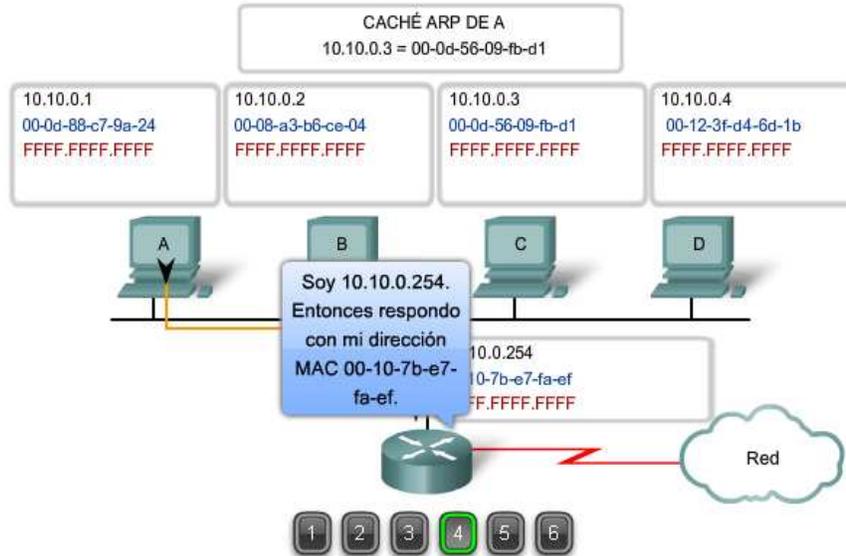
### ARP—No hay entrada ARP para el gateway



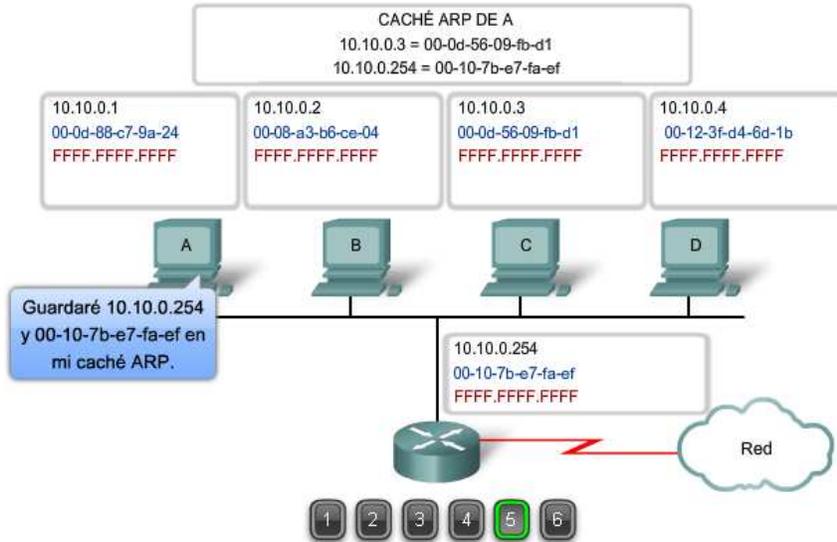
### ARP—Solicitud de ARP broadcast a los dispositivos



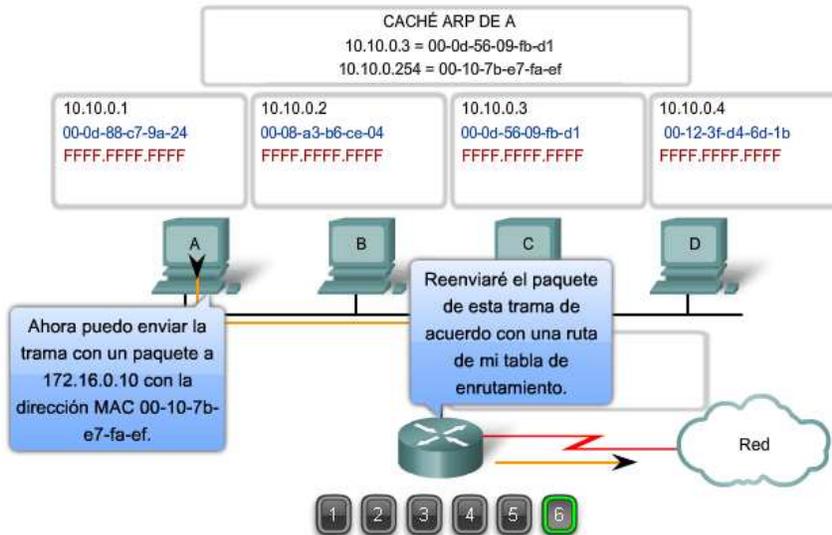
ARP—Respuesta con la dirección MAC del gateway



Proceso ARP —Direcciones IP y MAC almacenadas en caché ARP



Proceso ARP —Entrada ARP habilita el envío de la trama



## ARP proxy

Hay ocasiones en las que un host puede enviar una solicitud de ARP con el objetivo de mapear una dirección IPv4 fuera del alcance de la red local. En estos casos, el dispositivo envía solicitudes de ARP para direcciones IPv4 que no se encuentran en la red local en vez de solicitar la dirección MAC asociada a la dirección IPv4 del gateway. Para proporcionar una dirección MAC para estos hosts, una interfaz de router puede utilizar un ARP proxy para responder en nombre de estos hosts remotos. Esto significa que la caché de ARP del dispositivo solicitante contendrá la dirección MAC del gateway mapeada a cualquier dirección IP que no se encuentre en la red local. Con el proxy ARP, una interfaz de router actúa como si fuera el host con la dirección IPv4 solicitada por la solicitud de ARP. Al "simular" su identidad, el router acepta la responsabilidad de enrutar paquetes al destino "real".

Uno de los usos que se le da a dicho proceso es cuando una implementación más antigua de IPv4 no puede determinar si el host de destino se encuentra en la misma red lógica que el origen. En estas implementaciones, el ARP siempre envía solicitudes de ARP para la dirección IPv4 de destino. Si el ARP proxy se desactiva en la interfaz del router, estos hosts no pueden comunicarse fuera de la red local.

Otro caso en el que se utiliza el ARP proxy es cuando un host cree que está directamente conectado a la misma red lógica que el host de destino. Esto ocurre generalmente cuando un host se configura con una máscara inapropiada.

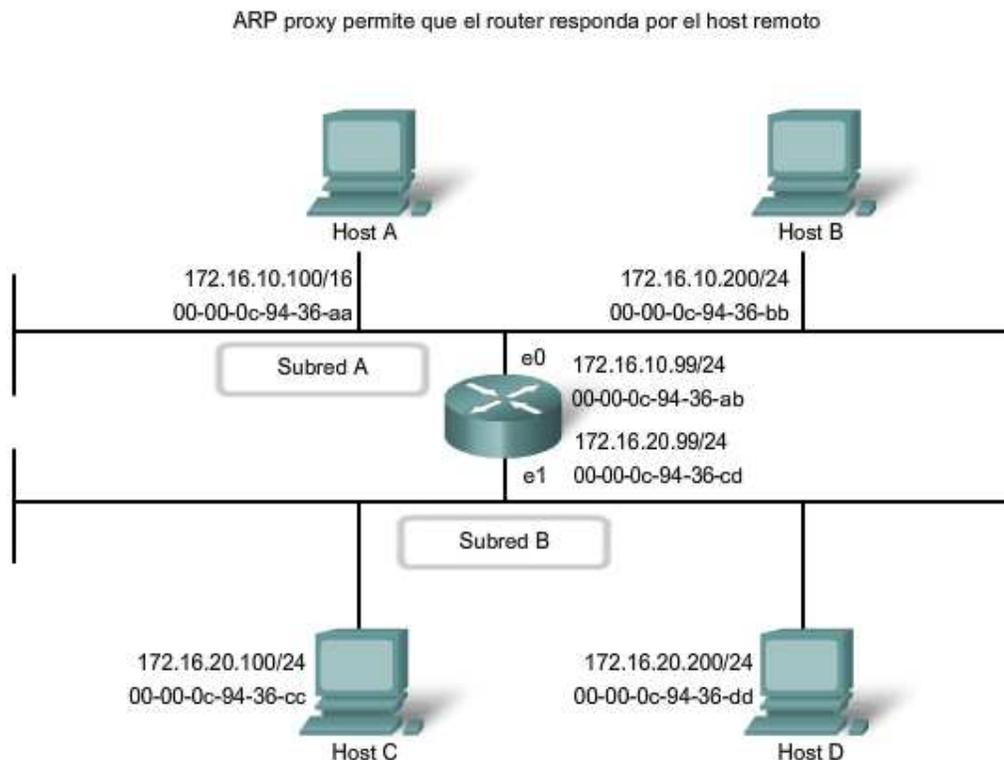
Tal como se muestra en la figura, el Host A se configuró inapropiadamente con una máscara de subred /16. Este host cree que está directamente conectado a la red 172.16.0.0 /16 en vez de a la subred 172.16.10.0 /24.

Cuando se intenta comunicar con cualquier host IPv4 en el intervalo de 172.16.0.1 a 172.16.255.254, el Host A enviará una solicitud de ARP para esa dirección IPv4. El router puede utilizar un ARP proxy para responder a las solicitudes de dirección IPv4 del Host C (172.16.20.100) y el Host D (172.16.20.200). Como resultado, el Host A tendrá entradas para estas direcciones mapeadas a la dirección MAC de la interfaz e0 del router (00-00-0c-94-36-ab).

Otro uso que se le puede dar al ARP proxy es cuando un host no está configurado con un gateway por defecto. El ARP proxy puede ayudar a que los dispositivos de una red alcancen subredes remotas sin la necesidad de configurar el enrutamiento o un gateway por defecto.

Por defecto, los router Cisco poseen un proxy ARP habilitado en las interfaces LAN.

<http://www.cisco.com/warp/public/105/5.html>

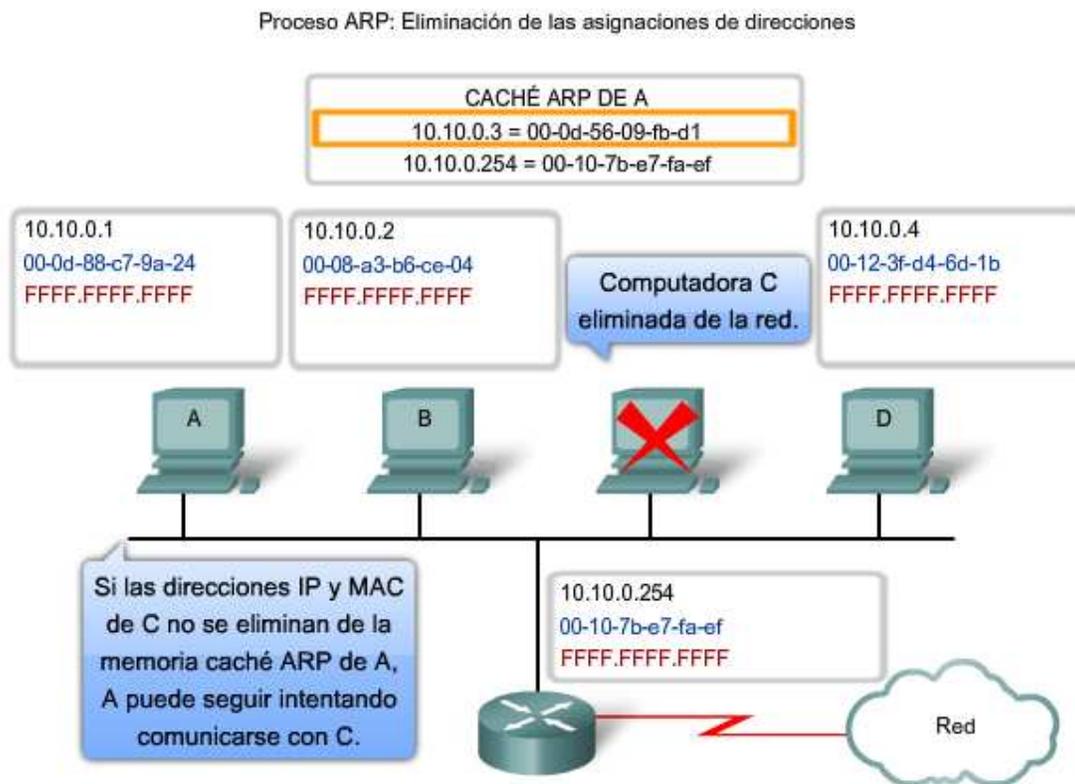


### 9.7.3 El proceso de ARP: Eliminación de mapeos de direcciones

Para cada dispositivo, un temporizador de caché de ARP elimina las entradas ARP que no se hayan utilizado durante un período de tiempo especificado. Los tiempos difieren dependiendo del dispositivo y su sistema operativo. Por ejemplo, algunos sistemas operativos de Windows almacenan las entradas de caché de ARP durante 2 minutos. Si la entrada se utiliza nuevamente durante ese tiempo, el temporizador ARP para esa entrada se extiende a 10 minutos.

También pueden utilizarse comandos para eliminar manualmente todas o algunas de las entradas de la tabla ARP. Después de eliminar una entrada, el proceso para enviar una solicitud de ARP y recibir una respuesta ARP debe ocurrir nuevamente para ingresar el mapa en la tabla ARP.

En la práctica de laboratorio para esta sección, utilizará el comando arp para visualizar y borrar los contenidos de la caché de ARP de una computadora. Observe que este comando, a pesar de su nombre, no invoca en absoluto la ejecución del Protocolo de resolución de direcciones. Sólo se utiliza para mostrar, agregar o eliminar las entradas de la tabla ARP. El dispositivo integra el servicio ARP dentro del protocolo IPv4 y lo implementa. Su funcionamiento es transparente para aplicaciones y usuarios de capa superior.



### 9.7.4 Broadcast de ARP: Problemas

#### Sobrecarga en los medios

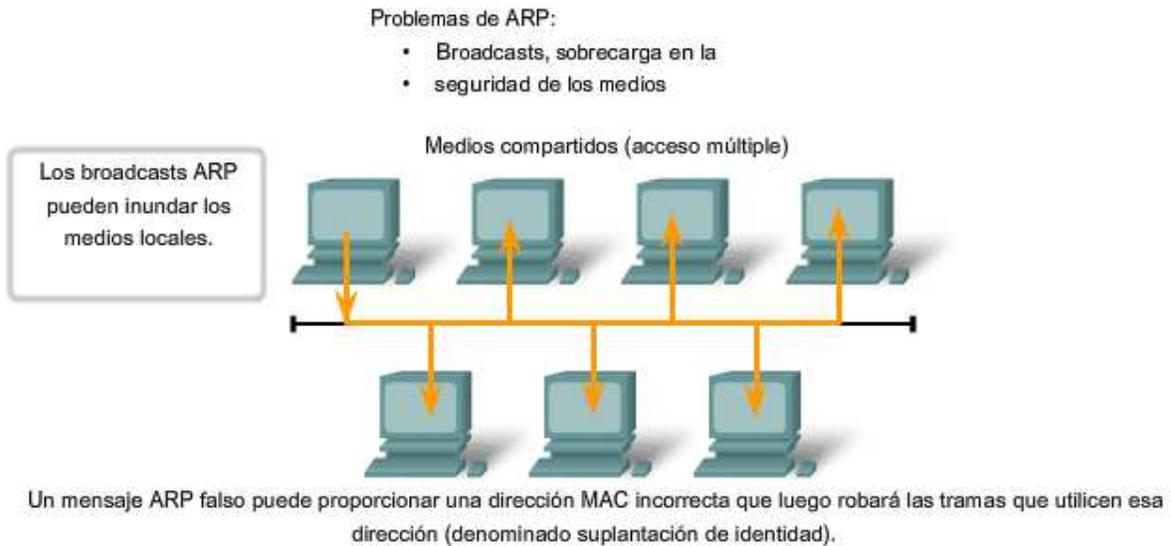
Todos los dispositivos de la red local reciben y procesan una solicitud de ARP debido a que es una trama de broadcast. En una red comercial típica, estos broadcasts tendrían probablemente un impacto mínimo en el rendimiento de la red. Sin embargo, si un gran número de dispositivos se encendiera y todos comenzaran a acceder a los servicios de la red al mismo tiempo, podría haber una disminución del rendimiento durante un período de tiempo breve. Por ejemplo, si todos los estudiantes de una práctica de laboratorio inician sesión en computadoras del aula e intentan acceder a Internet al mismo tiempo, podría haber demoras.

Sin embargo, una vez que los dispositivos envían los broadcasts de ARP iniciales y que aprenden las direcciones MAC necesarias, se minimizará todo impacto en la red.

#### Seguridad

En algunos casos, la utilización del ARP puede ocasionar un riesgo potencial de seguridad. La suplantación ARP o el envenenamiento ARP es una técnica que utiliza un atacante para introducir una asociación de direcciones MAC incorrecta en una red emitiendo solicitudes de ARP falsas. Un atacante falsifica la dirección MAC de un dispositivo y a continuación pueden enviarse tramas al destino equivocado.

La configuración manual de asociaciones ARP estáticas es una manera de evitar el ARP spoofing. Las direcciones MAC autorizadas pueden configurarse en algunos dispositivos de red para que limiten el acceso a la red para sólo los dispositivos indicados.



Ethernet					
8	6	6	2	46 a 1500	4
Preámbulo	Dirección de destino	Dirección de origen	Tipo	Datos	Secuencia de verificación de trama

## 9.9 Resumen del capítulo

### 9.9.1 Resumen y revisión

Ethernet es un protocolo de acceso de red TCP/IP efectivo y ampliamente utilizado. Su estructura de trama común se implementó a través de una variedad de tecnologías de medios, tanto de cobre como de fibra, lo que la convierten en el protocolo LAN que más se utiliza en la actualidad.

Como implementación de los estándares IEEE 802.2/3, la trama de Ethernet brinda direccionamiento MAC y verificación de errores. Dado que era una tecnología de medios compartidos, la Ethernet inicial debía aplicar un mecanismo CSMA/CD para administrar la utilización de los medios por parte de dispositivos múltiples. El reemplazo de hubs por switches en la red local redujo las probabilidades de colisiones de tramas en enlaces half-duplex. Sin embargo, las versiones actuales y futuras funcionan inherentemente como enlaces de comunicaciones full-duplex y no necesitan administrar la contención de medios con tanta precisión.

El direccionamiento de Capa 2 provisto por Ethernet admite comunicaciones unicast, multicast y broadcast. La Ethernet utiliza el Protocolo de resolución de direcciones para determinar las direcciones MAC de los destinos y mapearlas con direcciones de capa de Red conocidas.

**En este capítulo, aprendió a:**

- Identificar las características básicas de los medios de red utilizados en Ethernet.
- Describir las características de la capa Física y la capa de Enlace de datos de Ethernet.
- Describir el funcionamiento y las características del método de control de acceso al medio utilizado por el protocolo Ethernet.
- Explicar la importancia del direccionamiento de Capa 2 utilizado para la transmisión de datos y determinar cómo los diferentes tipos de direccionamiento afectan el funcionamiento y rendimiento de la red.
- Comparar y contrastar la aplicación y los beneficios de la utilización de switches Ethernet en una LAN con la utilización de hubs.
- Explicar el proceso de ARP.