1.2. EL modelo OSI y sus capas

Capa de Modelo OSI	Descripción
7 - Aplicación	La capa de aplicación contiene protocolos utilizados para las comunicaciones de proceso a proceso.
6 - Presentación	La capa de presentación proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación.
5 - Sesión	La capa de sesión proporciona servicios a la capa de presentación para organizar su diálogo y gestionar el intercambio de datos.
4 - Transporte	La capa de transporte define servicios para segmentar, transferir y reensamblar los datos para comunicaciones individuales entre los dispositivos finales.
3 - Red	La capa de red proporciona servicios para intercambiar los datos individuales a través de la red entre dispositivos finales identificados.
2 - Enlace de datos	Los protocolos de la capa de enlace de datos describen métodos para intercambiar tramas de datos entre dispositivos a través de un medio común
1 - Física	Los protocolos de la capa física describen los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar las conexiones físicas para una transmisión de bits hacia y desde un dispositivo de red.

Figura 4: Funcionalidad de cada capa referente al modelo OSI (Fuente: https://ccnadesdecero.es/)

1.3. El modelo TCP/IP y sus capas

Capa de modelo TCP / IP	Descripción
4 - Aplicación	Representa datos para el usuario, además de codificación y control de diálogo.
3 - Transporte	Admite la comunicación entre varios dispositivos a través de diversas redes.
2 - Internet	Determina la mejor ruta a través de la red.
1 - Acceso a la red	Controla los dispositivos de hardware y los medios que conforman la red.

Figura 5: Funcionalidad de cada capa referente al modelo TCP/IP (Fuente: https://ccnadesdecero.es/)

3. Lectura complementario

3.1. Cable directo y cruzado

Pineado UTP:

- Cable Recto: Transmisión por distintos pares de pines.
- Cable Cruzado: Transmisión por el mismo para de pines.

En la siguiente ilustración, se aprecian 2 grupos de dispositivos que se diferencian en la transmisión de datos por ciertos pines. Bajo este contexto, el conjunto de hardware que transmite por pines 1,2 se les conoce como MDI (Interfaz medianamente dependiente), por contra parte, los equipos que transmiten por los pines 3,6 se les conoce como MDI-X (Interfaz medianamente dependiente crossover)

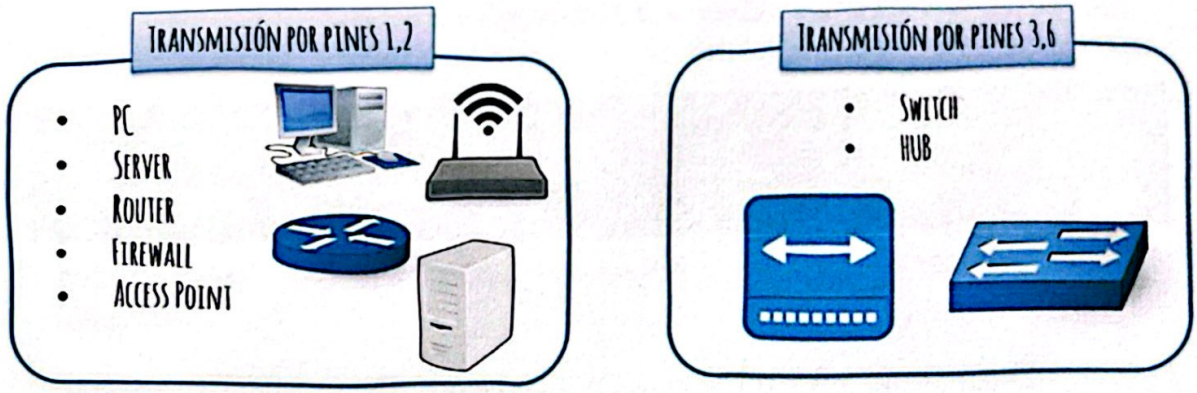


Figura 3: Pines de transmisión según el hardware

En virtud de lo señalado, se puede resumir el tipo de conexiones de la siguiente manera:

Tipo de cable	Conexión
Directo	- Switch a Router - PC a Switch - PC a Hub
Cruzado	- Switch a Switch - Switch a Hub - Hub a Hub - Router a Router - PC a PC - PC a Router

Figura 4: Tabla resumen de las conexiones asociadas a un cable directo y cruzado

3.2. Tablas comparativas de los distintos cableados

Nombre común	Estándar IEEE	Nombre alternativo	Velocidad	Medio físico, longitud máxima
Ethernet	802.3i	10Base-T	10 Mbps	Cobre, 100 m
Fast Ethernet	802.3u	100Base-TX	100 Mbps	Cobre, 100 m
Gigabit Ethernet	802.3z	1000Base-LX 1000Base-SX	1000 Mbps	Fibra, 550 m (SX), 5 km (LX)
Gigabit Ethernet	802.3ab	1000Base-T	1000 Mbps	Cobre, 100 m

Figura 5: Tabla comparativa asociados a los distintos cables Ethernet.

Problemas de Implementación	Cableado UTP	Cableado de fibra óptica
Ancho de banda compatible	10 Mb/s – 10 Gb/s	10 Mb/s – 100 Gb/s
Distancia	Relativamente corto (1 – 100 metros)	Relativamente largo (1 – 100,000 metros)
Inmunidad a EMI y RFI	Bajo	Alto (completamente inmune)
Inmunidad a los riesgos eléctricos.	Bajo	Alto (completamente inmune)
Costos de medios y conectores	Más bajo	Más alto
Habilidades de instalación requeridas	Más bajo	Más alto
Precauciones de seguridad	Más bajo	Más alto

Figura 6: Tabla comparativa entre cableado UTP y Cableado de fibra óptica (Fuente: https://ccnadesdecero.es/)

1. Lectura complementaria

1.1. Hardware básico de red

Se considera hardware de red todo dispositivo físico que permita la interconexión de una red. Existen diferentes tipos de hardware, cada uno con propiedades y finalidades diferentes. Los más reconocidos son el Router, Bridge, Switch, y el Hub.

- **Router:** O enrutador permite interconectar redes de ordenadores (Capa 3 ISO/OSI). Se encarga de encaminar datagramas de una red a otra.
- **Bridge:** Dispositivo de interconexión que funciona a nivel de capa 2 ISO/OSI. Interconecta segmentos de red haciendo la transferencia de datos de una red hacia otra con base en la dirección física de destino de cada paquete. El bridge posee baja densidad de puertas en comparación al Switch (típicamente 2 a 4).
- **Switch:** Es un Bridge con mayor densidad de puertas, realiza conmutación de datos a alta velocidad pues es la evolución tecnológica del Bridge. Sus funcionalidades son similares al Bridge.
- **Hub:** Es un repetidor de señal multi-puerta cuya principal función radica en repetir la señal de entrada para permitir abarcar mayores distancias, es un dispositivo de capa 1 ISO/OSI.

La mayoría de las aplicaciones de red para modelado o simuladores posee una simbología para representar estos distintos hardware. Para el caso de Cisco y el caso específico de su simulador Packet Tracer, se utiliza la simbología presentada en la Figura 7.

Figura 7: Algunos iconos representativos de Packet Tracer.

1.2. Topología de red

La topología de red corresponde a la organización del hardware de la red de comunicación (e.g: links, nodos, etc.) La topología permite definir y/o describir de mejor manera la infraestructura de comunicación. Tradicionalmente, las topologías de red son representadas por grafos, donde los vértices corresponden hardware de comunicación y las aristas los links de comunicación. Una topología puede ser lógica o física. La representación física modela la ubicación de los componentes de la red, mientras que la red lógica, se enfoca en como los datos fluyen por la red.

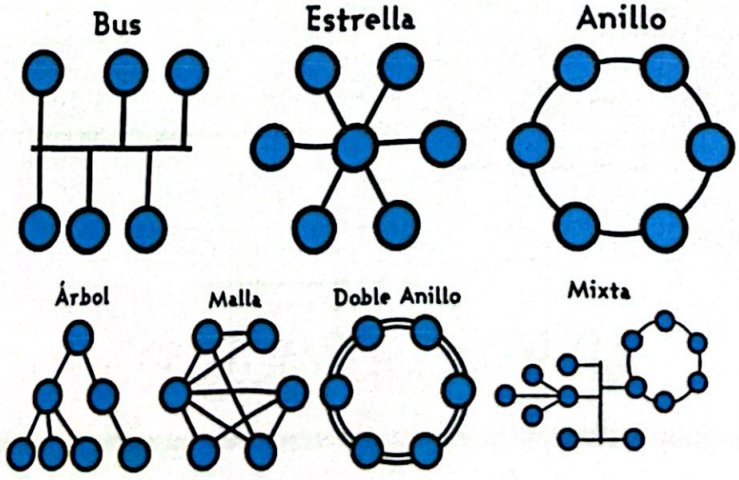


Figura 8: Topologías de red

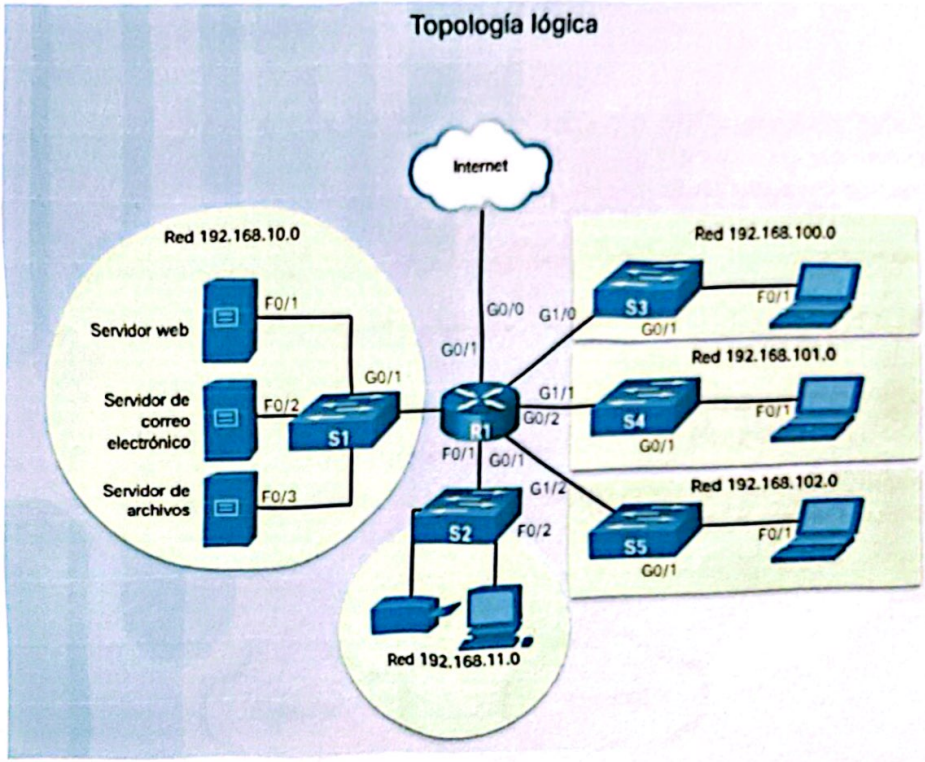


Figura 9: Topología lógica

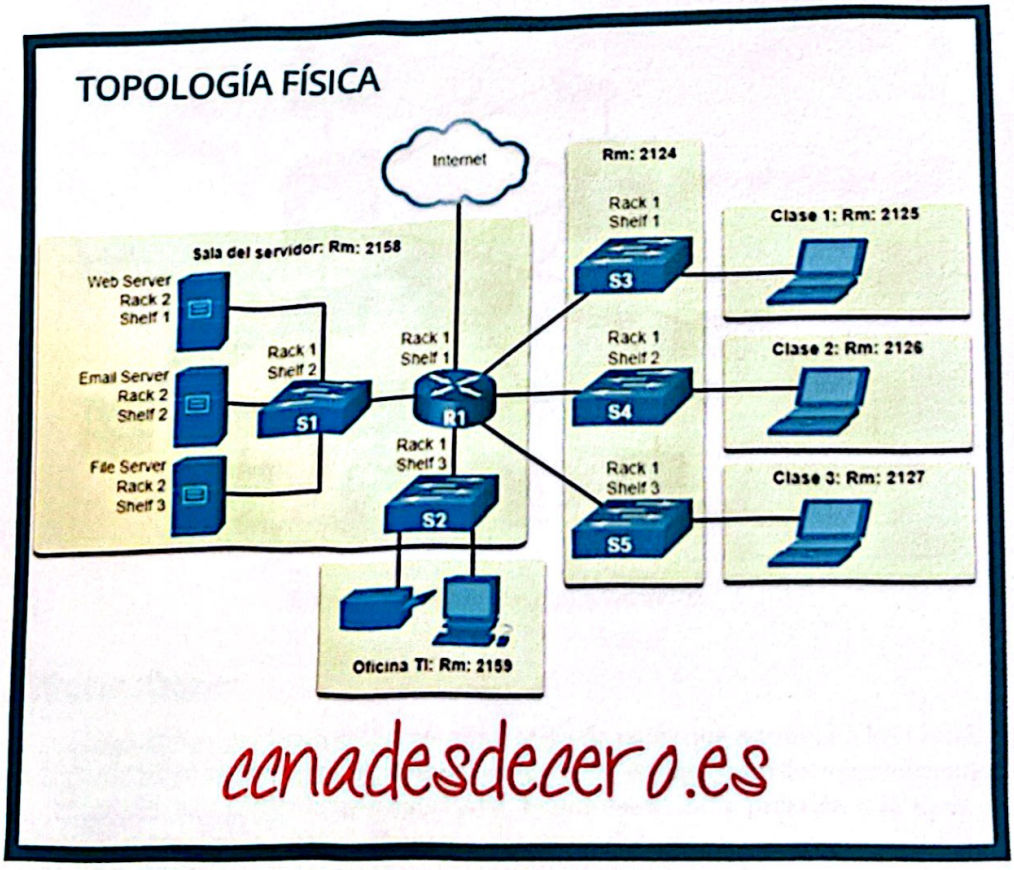


Figura 10: Topología Física

1.3. Diseño jerárquico de redes

1.3.1. Redundancia

La redundancia hace referencia a la capacidad que posee una red para mantenerse operativa en situaciones donde se produzcan caídas en algún servicio o dispositivo en particular. En este contexto, una buena práctica para optimizar los recursos de una red y mejorar su redundancia, consiste en distribuir la red en capas, donde cada una de ellas cumple cierta función y todas conectadas en sí.

Un diseño típico de red LAN jerárquica de campus empresarial inclute las siguientes tres capas:

- **Capa de acceso:** Se compone de switchs que interactúan directamente con host finales (PCs, impresoras, televidores, etc).
- **Capa de distribución:** Se compone de switchs de mayor capacidades que las de la capa de acceso y en ella se aplica redundancia, donde se utilizan múltiples enlaces hacia las diferentes capas.
- **Capa de núcleo:** Contiene dispositivos críticos de red y efectúa funciones como el enrutamiento. Los hardware que se ubican en está capa son routers o switch de muy alto rendimiento que se comunican con la capa de distribución.

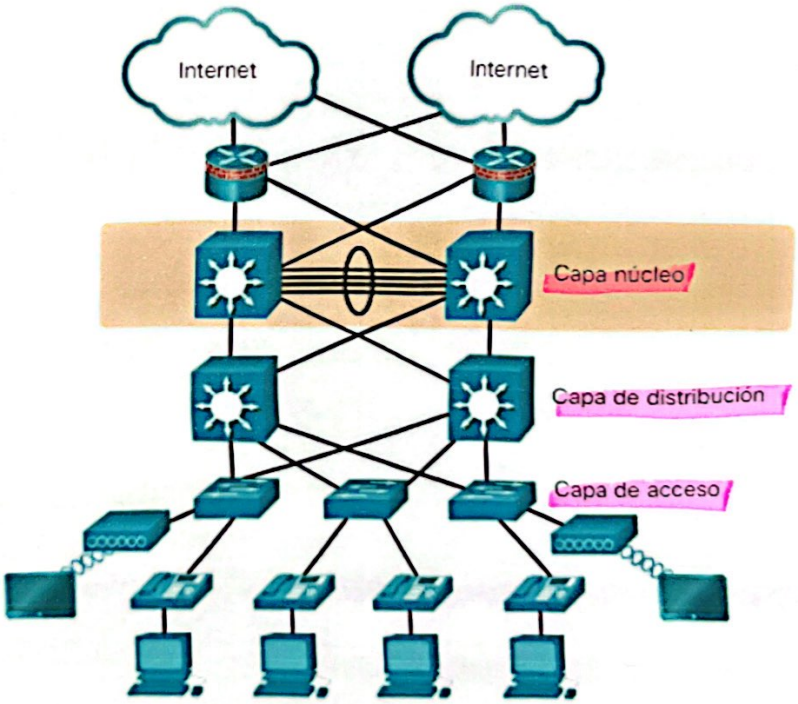


Figura 11: Diseño de red jerárquico.

1.4. Cisco Packet Tracer

Packet Tracer es una potente plataforma gráfica de simulación de redes que estimula a los alumnos a experimentar con el comportamiento de las redes. Funciona como complemento de los equipos físicos permitiendo a los estudiantes crear una red con un número casi ilimitado de dispositivos, lo que estimula la práctica y la detección, comprensión y solución de problemas[6].

[6] https://www.netacad.com/es/courses/packet-tracer

1.4.1. Interfaz Packet Tracer

La Figura 12 presenta una vista del entorno de trabajo del simulador de redes Cisco una vez inicializado. El espacio de trabajo en Packet Tracer se puede dividir en los espacios que se observan en la figura, donde:

- **Barra de herramientas:** Herramientas del espacio de trabajo en Packet Tracer.
- **Zona de menús:** Opciones de gestión del Packet Tracer.
- **Espacio lógico o físico:** Corresponde al área donde se realiza la simulación. El apartado físico, hace referencia a un plano de las instalaciones. Por otro lado, la pestaña lógica, refleja el funcionamiento del esquema de red, asimismo, no considera la escala física y limitaciones de construcción.
- **Área de dispositivos:** área que permite seleccionar los dispositivos a desplegar en el espacio de trabajo.
- **Dispositivos de red específicos:** área donde se presentan los dispositivos incluidos de acuerdo con la numeración utilizada por Cisco System.
- **Modo de ejecución Real Time o Simulation:** este espacio posibilita análisis más detallado de todas las **PDU**[7] de los diferentes protocolos que intervienen en la comunicación, además permite variar el modo de ejecución entre Real Time o Simulation.

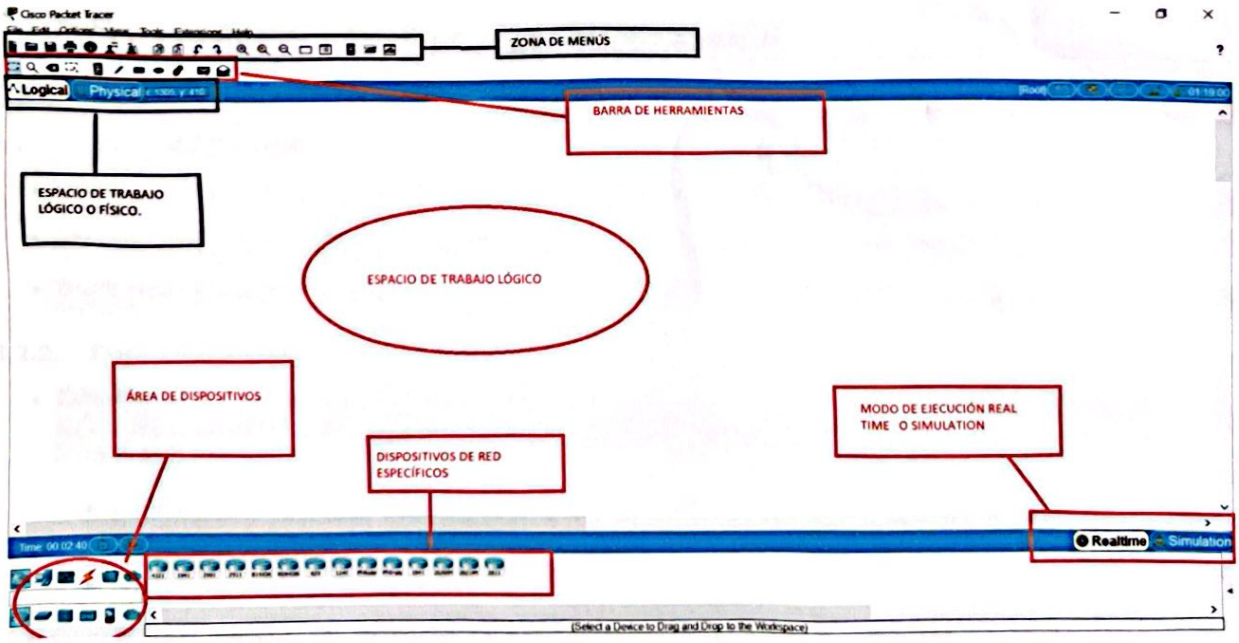


Figura 12: Reconocimiento de escenario.

[7] PDU: Protocol Data Unit.

Fin de Guía Nº 3

3. Lectura complementaria

Nota: Gran parte del texto aquí presentado ha sido tomado del material disponible online en `https://ccnadesdecero.es/` *según se indica en Capítulo 6: Capa de enlace de datos, "Trama Enlace De Datos 2 también en* `https://www.ionos.es/digitalguide/servidores/know-how/trama-ethernet/`

3.1. Principios de diseño de la capa de enlace de datos

La capa de enlace de datos hace lo siguiente:

- Permite que las capas superiores accedan a los medios. El protocolo de capa superior desconoce por completo el tipo de medio que se utiliza para reenviar los datos.
- Permite que las capas superiores accedan a los medios. El protocolo de capa superior desconoce por completo el tipo de medio que se utiliza para reenviar los datos.
- Controla cómo se colocan y reciben los datos en los medios.
- Intercambia tramas entre puntos finales a través de los medios de red.
- Recibe datos encapsulados, generalmente paquetes de Capa 3, y los dirige al protocolo de capa superior adecuado.
- Realiza la detección de errores y rechaza cualquier trama corrupta.

3.2. Manejo de Errores en la transmisión

3.2.1. Tipos de Errores

- Single bit error: En la trama recibida, solo se ha corrompido un bit, es decir, se cambió de 0 a 1 o de 1 a 0.
- Multiple bits error: En la trama recibida, más de un bit está dañado. → seguidos
- Burst error: En la trama recibida, más de un bit consecutivo está dañado. → en cualquier orden.

3.2.2. Detección vs corrección de errores

- **Detección:** Esta estrategia considera incluir suficiente redundancia para permitir que el receptor sepa que ha ocurrido un error (pero no qué error) y entonces solicite una retransmisión. Los códigos de detección de errores son:
  - Paridad.
  - Checksum.
  - Cyclic Redundant Checks (CRC).
- **Corrección:** En esta estrategia se considera incluir suficiente información redundante en cada bloque de datos transmitido para que el receptor pueda deducir lo que debió ser el carácter transmitido. Los códifos de correción de errores son:
  - Backward Error Correction.
  - Forward Error Correction (FEC)
    - Hamming Codes
    - Binary Convolution Code
    - Reed – Solomon Code
    - Low-Density Parity-Check Code

3.3. Subcapa LLC y MAC

La capa de enlace de datos se divide en dos subcapas:

- **Control de enlace lógico (LLC):** se trata de la subcapa superior, que define los procesos de software que proporcionan servicios a los protocolos de capa de red. El LLC coloca en la trama información que identifica qué protocolo de capa de red se utiliza para la trama.
- **Control de acceso al medio (MAC):** se trata de la subcapa inferior, que define los procesos de acceso al medio que realiza el hardware. Proporciona el direccionamiento de la capa de enlace de datos y la delimitación de los datos de acuerdo con los requisitos de señalización física del medio y con el tipo de protocolo de capa de enlace de datos en uso.

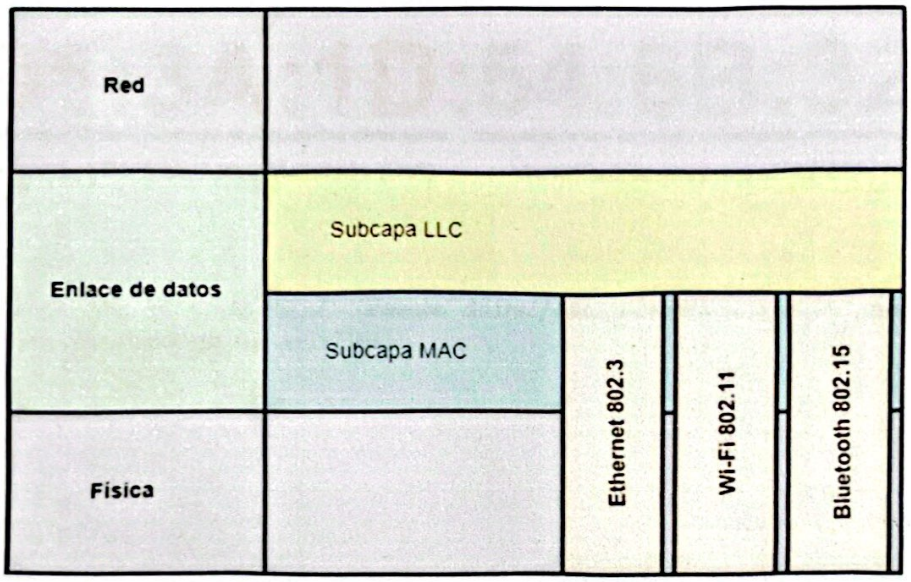


Figura 5: Subcapa LLC y MAC

3.4. Ethernet II

Una trama Ethernet debe tener al menos 64 bytes para que funcione la detección de colisiones y puede tener un máximo de 1518 bytes.

El paquete comienza con un preámbulo, que controla la sincronización entre el emisor y el receptor, y un SFD (Start Frame Delimiter), que define la trama. Ambos valores son secuencias de bits en el formato "10101010 ....". La trama en sí contiene información sobre las direcciones de origen y destino (formato MAC), información de control (en el caso de Ethernet II el campo de tipo, una especificación de longitud), seguida por el registro de datos que se envía (Data). Una secuencia de comprobación de trama (FCS) es un código de detección de errores que cierra la trama (si no se cuenta al preámbulo y al SFD). El paquete se completa con una Inter Frame Gap, que define una pausa de transmisión de 9.6 s.

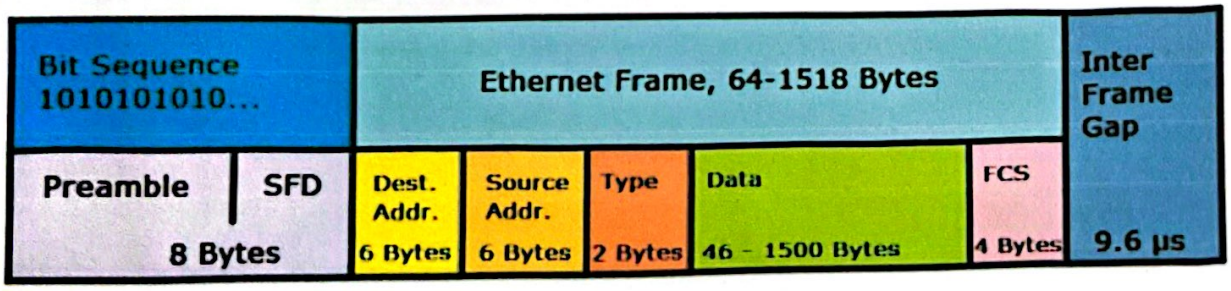


Figura 6: La estructura de trama clásica de Ethernet II, con una característica especial que es el campo tipo (type) (Fuente: https://www.ionos.es/digitalguide/servidores/know-how/trama-ethernet/)

3.5. Dirección MAC

Media Acces Control (MAC) es un identificador único asignado por el fabricante de hardware, la intención de esto es que cada dispositivo puede ser identificado en la red. Esta dirección física está compuesta por 6 octetos, cada uno de 8 bits, los primeros 3 octetos corresponden al identificador del fabricante, mientras que los últimos tres al del producto.

Figura 7: Ejemplo de una dirección MAC (Fuente :https://computerhoy.com/reportajes/tecnologia/que-es-direccion-mac-tu-ordenador-movil-que-sirve-317181).

Fin de Guía Nº 4

- **CSMA no persistente:** En este protocolo se hace un intento consciente por ser menos egoísta que en el previo. Como antes, una estación escucha el canal cuando desea enviar una trama y, si nadie más está transmitiendo, comienza a hacerlo. Pero si el canal ya está en uso, la estación no lo escuchará de manera continua con el fin de tomarlo de inmediato al detectar el final de la transmisión anterior, sino que esperará un periodo aleatorio y repetirá el algoritmo. En consecuencia, este algoritmo conduce a un mejor uso del canal pero produce mayores retardos que el CSMA persistente-1.
- **CSMA persistente-p:** Cuando una estación está lista para enviar, escucha el canal. Si se encuentra inactivo, la estación transmite con una probabilidad p. Con una probabilidad $q = 1 - p$, se posterga hasta la siguiente ranura.

3.2.1. CSMA/CD: Carrier sense multiple access / Collision detection

El protocolo CSMA/CD se subdivide en varios pasos. Cuando una estación tiene datos por transmitir:

- primero escucha el canal para saber si otra está transmitiendo en ese momento
- Si el canal está ocupado, la estación espera hasta que se desocupa.
- Cuando la estación detecta un canal inactivo, transmite una trama.
- Si ocurre una colisión, la estación espera una cantidad aleatoria de tiempo y comienza de nuevo.

Si se detecta una colisión, el host que la detecta interrumpe de inmediato la transmisión y en su lugar envía una señal de interferencia conocida como señal JAM, que informa a todas las estaciones de la red de dicha colisión. Por consiguiente, el host espera un tiempo aleatorio establecido por una técnica llamada Back-Off (BO) exponencial binario y vuelve a intentar la transmisión. En la colisión i se esperan 0 a 2^{i-1} slots (random).

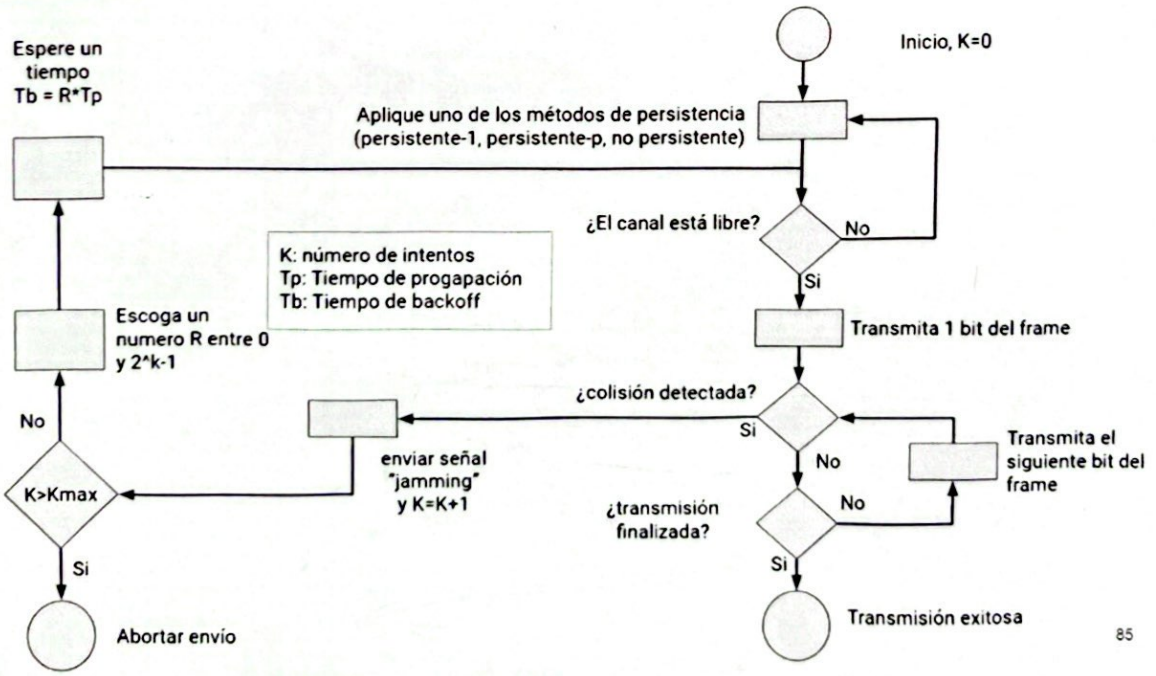


Figura 6: Diagrama de flujo asociado al protocolo CSMA/CD

3.2.2. CSMA/CA Carrier Sense Multiple Access with Collision

El procolo CSMA/CA resulta bastante similar en cuanto a modo de operar del protocolo CSMA/CD pero agrega una pequeña característica, que consiste en el envío de una notificación antes de transmitir datos. Es decir, primero se examina el medio en busca de alguna señal, y si está libre, envía una notificación informando al resto de dispositivos su intención de utilizarlo.

→ similar a CD, solo que avisa si el medio esta libre para usarlo.

Fin de Guia Nº 5

1. Lectura complementaria

1.1. Protocolo de Internet e identificadores

El *Internet Protocol* (IP) es un protocolo de comunicaciones de capa 3 (según modelo ISO/OSI) diseñado para sistemas interconectados de redes de computadores. Este protocolo permite transmitir bloques de datos llamados datagramas desde un origen hacia un destino, donde origen y destino se encuentran identificados por identificadores IP o *Internet Protocol Address*. Este es un protocolo *host-to-host* dado que en una red busca llevar datagramas hacia un siguiente *gateway* o host de destino. Este proceso de encaminamiento hacia el destino es llevado a cabo en base a el identificador IP, identificador lógico del dispositivo en la red. Este identificador para la versión 4 del protocolo consta de 4 Bytes.

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
A	0.0.0.0	127.255.255.255	128*	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	no aplica	no aplica	Multicast
E	240.0.0.0	255.255.255.255	no aplica	no aplica	Investigación

* El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza.

Figura 5: Tabla de identificadores IP y sus clases.

1.2. Dirección MAC

Media Acces Control (MAC) es un identificador único asignado por el fabricante de hardware, la intención de esto es que cada dispositivo puede ser identificado en la red. Esta dirección física está compuesta por 6 octetos, cada uno de 8 bits, los primeros 3 octetos corresponden al identificador del fabricante, mientras que los últimos tres al del producto.

Figura 6: Ejemplo de una dirección MAC (Fuente :https://computerhoy.com/reportajes/tecnologia/que-es-direccion-mac-tu-ordenador-movil-que-sirve-317181).

1.3. ARP

El *Address Resolution Protocol* (ARP) es un protocolo de comuniaciones que permite encontrar la dirección de Hardware (MAC) a través de la dirección IP realizando un broadcast en una red. Gracias a este protocolo se puede identificar a cada dispositivo de red. En el modelo TCP / IP, este protocolo opera entre la capa de acceso a la red y la capa de internet.

ARP asume únicamente que cada host sabe la correspondencia existente entre su propia dirección de hardware y su dirección de protocolo.

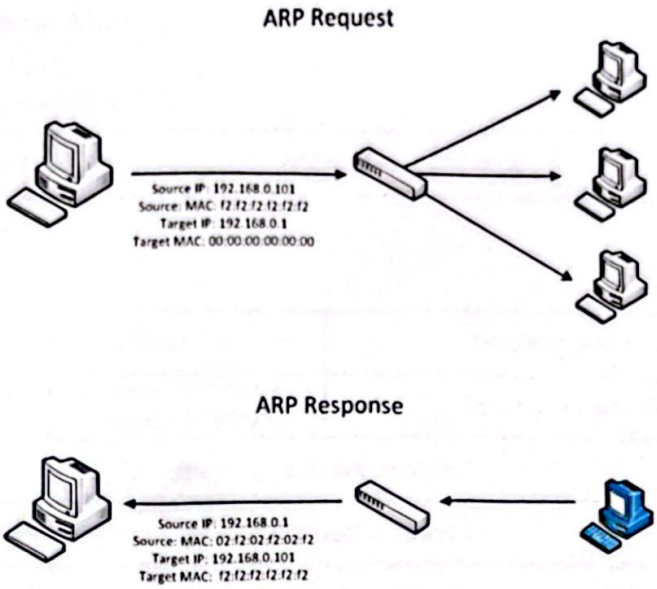


Figura 7: Ejemplo de ARP Request y la respectiva respuesta(Response) de un Host

1. Mensaje ARP Request

Encabezado				Mensaje ARP
Encabezado MAC		Encabezado IP		
MAC Destino	MAC Origen	IP Destino	IP Origen	¿Cual es tu dirección MAC?
FF:FF:FF:FF:FF:FF	01:00:D1:B5:D4:F1	200.59.4.5	200.59.4.1	

Dirección MAC Broadcast **Dirección IP consultada**

2. Mensaje ARP Reply

Encabezado				Mensaje ARP
Encabezado MAC		Encabezado IP		
MAC Destino	MAC Origen	IP Destino	IP Origen	¿Cual es tu dirección MAC?
01:00:D1:B5:D4:F1	F1:01:E1:B5:F4:14	200.59.4.1	200.59.4.5	

Figura 8: Contenido de ARP Request y la respectiva respuesta(Response) de un Host

1.3.1. Formato de paquete ARP

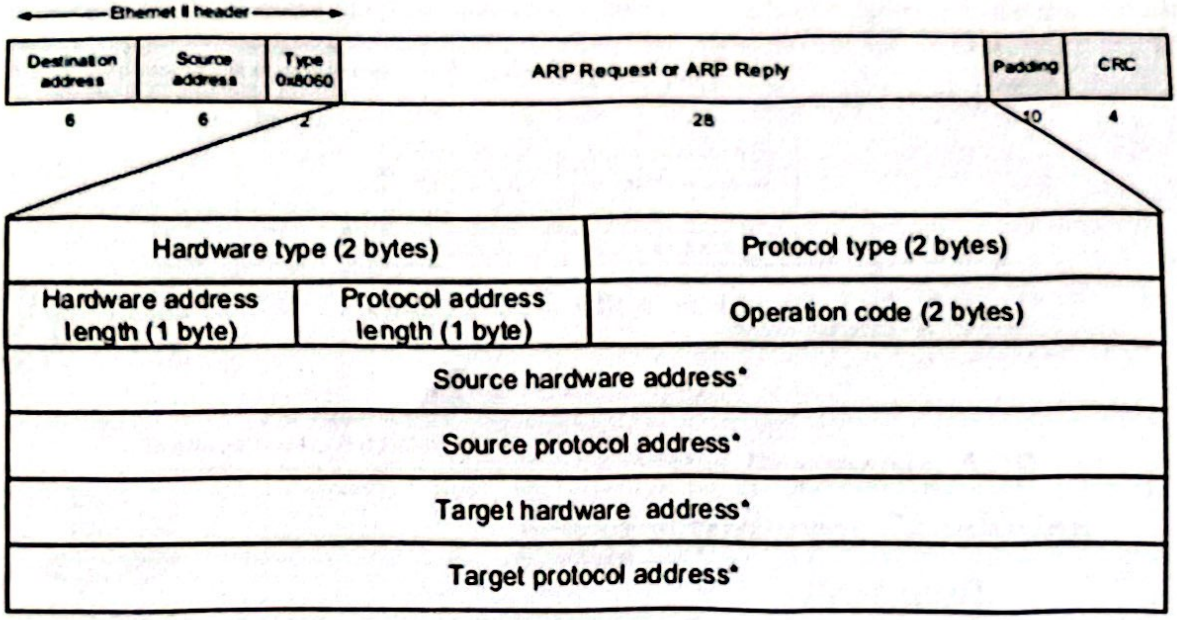


Figura 9: Formato de paquete ARP

- **Tipo de hardware o Hardware Type (HTYPE):** este campo especifica el tipo de protocolo de enlace. Ejemplo: Ethernet es 1.
- **Tipo de protocolo o Protocol Type (PTYPE):** este campo especifica el protocolo de interconexión de redes para las que se destina la petición ARP. Para IPv4, esto tiene el valor 0x0800.
- **Longitud Hardware (HLEN):** longitud (en octetos) de una dirección de hardware. En Ethernet el tamaño de direcciones es de 6.
- **Longitud del Protocolo (PLEN):** longitud (en octetos) de direcciones utilizadas en el protocolo de capa superior. El protocolo de capa superior especificado en PTYPE. IPv4 tamaño de la dirección es de 4.
- **Operación:** especifica la operación que el emisor está realizando: 1 para la petición, 2 para la respuesta.
- **Dirección de hardware del remitente (SHA):** Dirección de capa 2 del remitente.
- **Remitente dirección de protocolo (SPA):** dirección de capa 3 del remitente.
- **Dirección de hardware de destino (THA):** Dirección de capa 2 del destino. Este campo se ignora en las solicitudes.
- **Dirección de protocolo target (TPA):** Dirección de capa 3 del destino

1.4. Cache ARP

Con el fin de disminuir la cantidad de difusiones, ARP mantiene en caché la asignación de direcciones para usarla posteriormente. La cache de ARP puede incluir entradas dinámicas y estáticas, las dinámicas cambian con el tiempo. mientras que las estáticas permanecen en caché solamente hasta reiniciar el equipo. IONOS (2019) afirma:

> *La memoria caché del ARP hace referencia a un listado en forma de tabla de las direcciones MAC que se necesitan con mayor frecuencia, donde cada una de las entradas es generada por el protocolo de red o manualmente. Las primeras entradas, que también pueden describirse como dinámicas, están dotadas de una fecha y, cuando esta vence, dichas entradas se eliminan de la caché. Por último, las entradas de direcciones estáticas están disponibles hasta que el dispositivo se apaga o se vuelve a encender y la caché del ARP se borra por completo.*

1.4.1. Tabla ARP

Cada uno de los Host que haga referencia a un equipo en particular crea y almacena su propia tabla ARP. Cuando se logra encontrar la dirección MAC asociada a una dirección IP en particular, esta se almacena en memoria temporalmente, pues los datos de las direcciones pueden cambiar con el tiempo, por ejemplo cuando un equipo es sustituido o simplemente si se realizaron cambios de dirección IP.

Dirección IP	Dirección MAC
202.2.3.4	ee.ee.ee.ee.ee.ee
202.2.3.3	cc.cc.cc.cc.cc.cc
202.2.3.1	xx.xx.xx.xx.xx.xx

Cuadro 1: Tabla ARP de un dispositivo

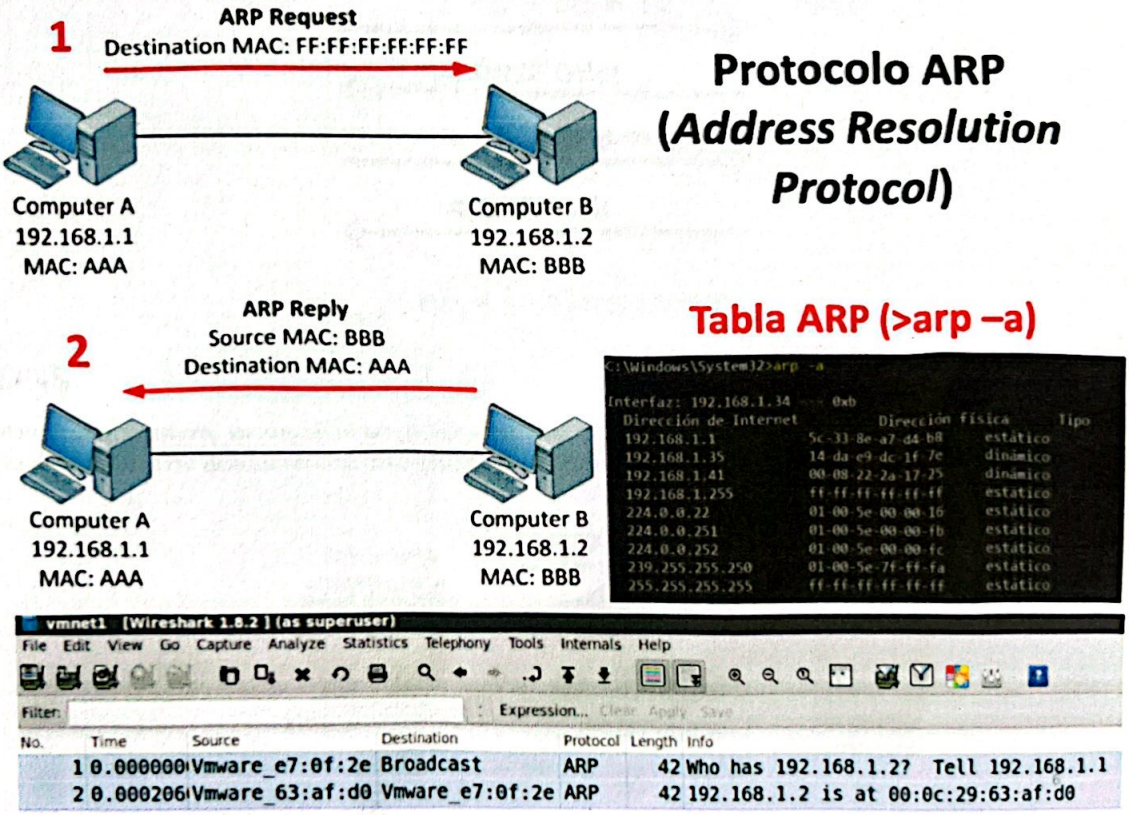


Figura 10: Ejemplo del contenido de una tabla ARP de un Host de SO windows

1.5. RARP

Reverse Address Resolution Protocol (RARP). Cada usuario de una red posee una dirección lógica(IP) y física(MAC), puede darse el caso en que un equipo no conozca su propia dirección IP, por ejemplo cuando no posee almacenamiento propio en el cual guardar dichos datos. En esta situación se utiliza el protocolo RARP, que basándose en su dirección MAC, este protocolo puede determinar cual la dirección IP. Para llevar a cabo esta tarea debe haber un dispositivo especializado el cual pueda responder estas solicitudes RARP. este protocolo es la contra parte de ARP y actualmente esta en desuso debido a que nuevos protocolos lo han sustituido.

1.6. DHCP

El *Dynamic Host Configuration Protocol* (DHCP) es un protocolo de red de tipo cliente/servidor que opera en la capa 7 (según modelo ISO/OSI), se utiliza para distribuir y actualizar de forma automática las direcciones IP y

configuraciones dentro de una red. La asignación de direcciones mediante este protocolo de configuración dinámica se realiza en cuatro pasos realizando broadcast entre el servidor y el cliente, los cuales se mencionan a continuación:

- DHCP Discover: Busca servidores.
- DHCP Offer: El servidor ofrece una dirección IP al cliente.
- DHCP Request: El cliente elige la dirección IP ofrecida.
- DHCP ACK: Luego el servidor comunica que asignara la IP que confirma el cliente.

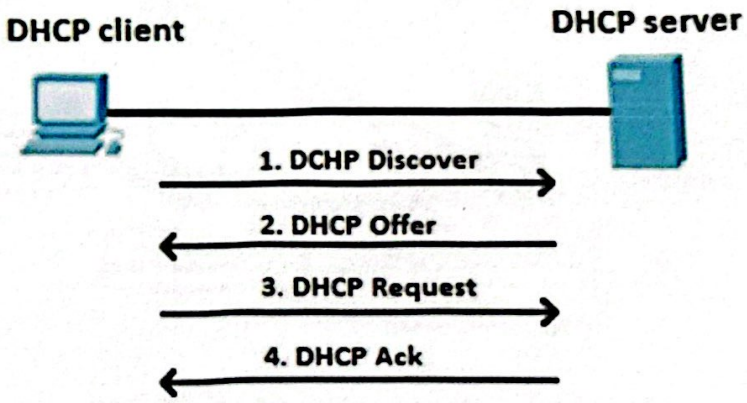


Figura 11: Ejemplo DHCP

1.7. DNS

Domain Name System, es un sistema jerárquico que opera en la capa 7 (según modelo ISO/OSI), permite la asociación de nombres de dominios con direcciones IP. A continuación se presentan algunos ejemplos representativos:

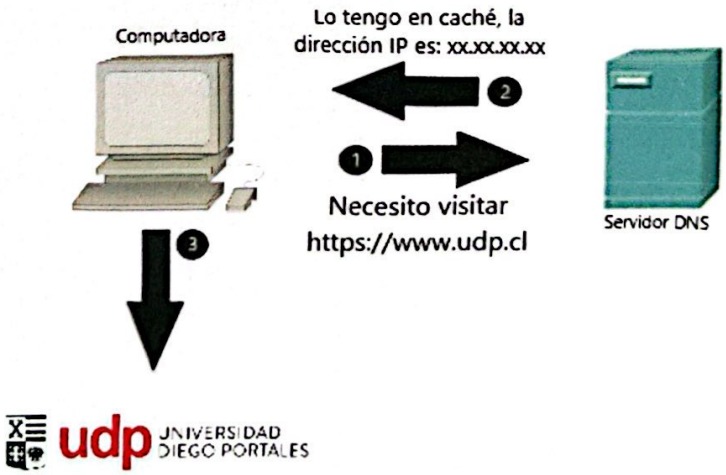


Figura 12: Ejemplo DNS

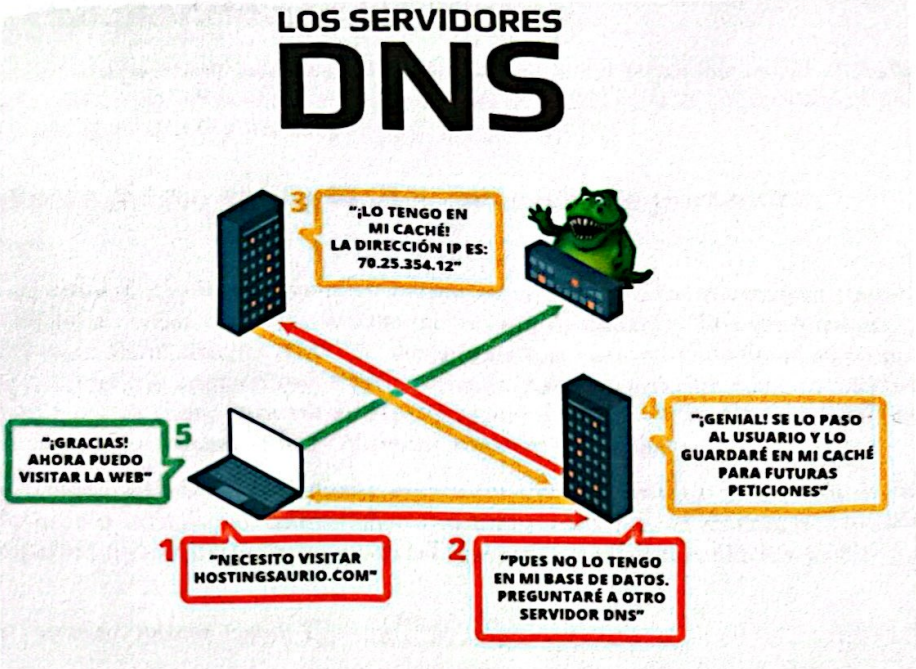


Figura 13: Segundo ejemplo de DNS (Fuente: https://www.hostingnet.cl/blog/como-funciona-internet-que-son-las-dns-y-para-que-sirven/)

3. Lectura Complementaria:

Nota: Gran parte del texto aquí presentado ha sido tomado del material disponible online en `https://www.ionos.es/digitalguide/servidores/know-how/trama-ethernet/`. *"CSMA/CD: protocolo de transmisión anticolisiones". Página consultada el 17 de abril del 2021*

3.1. Protocolos de acceso aleatorio SIN detección de portadora

3.1.1. Aloha Puro

La idea básica de un sistema ALOHA es sencilla: permitir que los usuarios transmitan cuando tengan datos por enviar. Por supuesto, habrá colisiones y las tramas en colisión se dañarán. Los emisores necesitan alguna forma de saber si éste es el caso. En el sistema ALOHA, después de que cada estación envía su trama a la computadora central, ésta vuelve a difundir la trama a todas las estaciones. Así, una estación emisora puede escuchar la difusión de la estación terrena maestra (hub) para ver si pasó su trama o no. En otros sistemas, como las LAN alámbricas, el emisor podría ser capaz de escuchar si hay colisiones mientras transmite.

Si la trama fue destruida, el emisor simplemente espera un tiempo aleatorio y la envía de nuevo. El tiempo de espera debe ser aleatorio o las mismas tramas chocarán una y otra vez, en sincronía. Los sistemas en los cuales varios usuarios comparten un canal común de modo tal que puede dar pie a conflictos se conocen como sistemas de contención.

- El tiempo de frame se obtiene como: $T_f = \frac{frame\_size(bits)}{throughtput(bps}$
- Tiempo de vulnerabilidad: Tiempo en el cual ninguna estación puede transmitir $T_{vulnerabilidad} = 2 \cdot T_f$
- Troughput (S):
  - Donde G es la cantidad promedio de frames enviados durante el tiempo de un frame (Tf). Mejor caso con G = 0.5. S = $G \cdot e^{-2G}$

3.1.2. Aloha Ranurado

Poco después de que ALOHA apareció en escena, Roberts (1972) publicó un método para duplicar la capacidad de un sistema ALOHA. Su propuesta fue dividir el tiempo en intervalos discretos llamados ranuras, cada uno de los cuales correspondía a una trama. Este método requiere que los usuarios acuerden límites de ranura. Una manera de lograr la sincronización sería tener una estación especial que emitiera una señal al comienzo de cada intervalo, como un reloj.

- El tiempo de frame se obtiene como: $T_f = \frac{frame\_size(bits)}{throughtput(bps}$
- Tiempo de vulnerabilidad: Tiempo en el cual ninguna estación puede transmitir $T_{vulnerabilidad} = T_f$
- Troughput (S):
  - Donde G es la cantidad promedio de frames enviados durante el tiempo de un frame (Tf). Mejor caso con G = 1 S = $G \cdot e^{-G}$

3.2. Protocolos de acceso múltiple con detección de portadora

Con el ALOHA ranurado, el mejor aprovechamiento de canal que se puede lograr es 1/e. Este resultado tan bajo no es muy sorprendente pues, con estaciones que transmiten a voluntad propia, sin prestar atención a lo que están haciendo las demás estaciones, es inevitable que haya muchas colisiones. Sin embargo, en las redes LAN es posible que las estaciones detecten lo que están haciendo las demás estaciones y adapten su comportamiento con base en ello.

- **CSMA (Acceso Múltiple con Detección de Portadora, del inglés Carrier Sense Multiple Access) persistente-1:** Cuando una estación tiene datos por enviar, primero escucha el canal para saber si alguien más está transmitiendo en ese momento. Si el canal está inactivo, la estación envía sus datos. Por el contrario, si el canal está ocupado, la estación espera hasta que se desocupa. A continuación, la estación transmite una trama. Si ocurre una colisión, la estación espera una cantidad aleatoria de tiempo y comienza de nuevo. El protocolo se llama persistente-1 porque la estación transmite con una probabilidad de 1 cuando encuentra que el canal está inactivo

1. Lectura complementaria

Nota: Gran parte del texto aquí presentado ha sido tomado del material disponible online en https://ccnadesdecero.es/ según se indica en Capítulo 6: VLAN - CCNA 2, "Segmentación de VLAN: Introducción".

1.1. Virtual LAN (Red de área local y virtual)

"Las VLAN proporcionan una manera de agrupar dispositivos dentro de una LAN. Un grupo de dispositivos dentro de una VLAN se comunica como si estuvieran conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas".

En términos más sencillos, permite crear redes lógicas de forma independiente, no obstante, estas se encuentran dentro de una misma red física.
Observación: Un usuario puede disponer de varias VLANs dentro de un mismo router o switch.

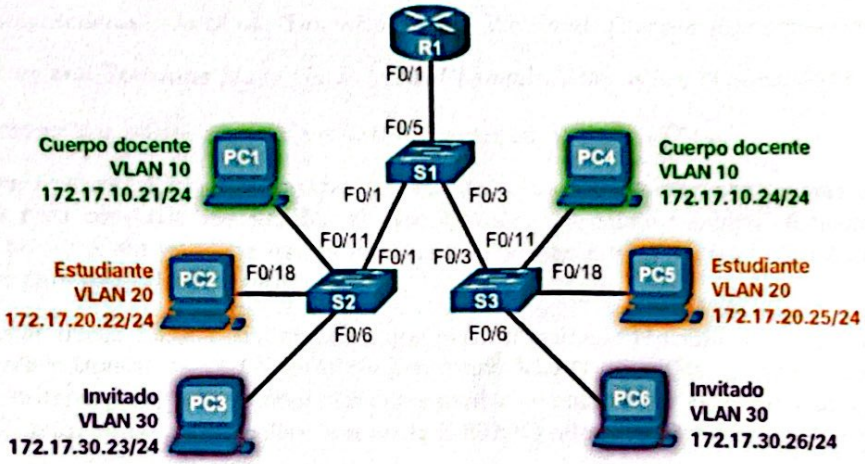


Figura 4: Ejemplo Vlan (Fuente: https://ccnadesdecero.es/examenes/)

1.1.1. Ventajas de las VLANs

- **Seguridad:** Los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial. En la figura 4 los computadores del Cuerpo Docente se encuentran en la VLAN 10 y están completamente separados del tráfico de datos de los Invitados y de los Estudiantes.
- **Mejor rendimiento:** La división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.
- **Mitigación de la tormenta de broadcast:** La división de una red en varias VLANs reduce la cantidad de dispositivos que pueden participar en una tormenta de broadcast e impide que esta se propague a toda la red.
- **Mayor eficiencia del personal de TI:** Las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN.
- **Administración de aplicación o de proyectos más simples:** Las VLANs agregan dispositivos de red y usuarios para admitir los requerimientos geográficos o comerciales. Tener funciones separadas hace que gestionar un proyecto o trabajar con una aplicación especializada sea más fácil, por ejemplo, una plataforma de desarrollo de e-learning para el cuerpo docente. También es fácil determinar el alcance de los efectos de la actualización de los servicios de red.

1.1.2. Desventajas de las VLANs

Nota: Gran parte del texto aquí presentado ha sido tomado del material disponible online en https://www.escueladeinternet.com/ventajas-y-limites-de-usar-redes-privadas-virtuales/.

- **Administración compleja.** Tener varias VLAN supone el mismo trabajo que gestionar diversas LAN, por lo que se debe configurar cada switch.
- **Aislamiento del tráfico.** En redes grandes puede ser necesario contar con varios routers para que las VLAN se puedan comunicar.
- **Agujero de seguridad.** Sin un virus llega a infectar un ordenador, se puede reproducir «fácilmente» por toda la red lógica.
- **Latencia limitada.** Las VLAN son más eficaces que una WAN en cuanto a la latencia, pero menos que una LAN.

1.2. Modo de puertos de un switch

Nota: textos (leves modificaciones) tomados de:

- *"Redes de Computadoras", 5a ed, A. Tanenbaum y D. Wetherall, Pearson Educación, 2012*
- *"CCNA Routing and Switching Study Guide", Todd Lammle, John Wiley & Sons, 2013.*

Modos switchport en que puede operar un puerto Ethernet en un switch Cisco:

- *Switch port mode access:* Coloca la interfaz (puerto de acceso) de manera permanente en non-trunk y hace negociaciones para convertir una interfaz al otro extremo del enlace también en no-trunk. La interfaz se convierte en no-trunk sin importar que la interfaz vecina pueda estar en modo trunk.etiquetados, y por lo general se usa para conectar dispositivos finales.
- *Switchport mode trunk:* Es una configuración que permite manejar el tráfico de varias VLAN en un mismo puerto. Un enlace troncal de VLAN no pertenece a una VLAN específica, ya que, es un conducto para las VLAN entre switches y routers. Existen diferentes modos de enlaces troncales, sin embargo, en la actualidad se usa 802.1Q, pues un puerto de enlace troncal IEE 802.1Q admite tráfico etiquetado y sin etiquetar.
- *Switchport mode dynamic auto:* Permite convertir una interfaz en un enlace en modo trunk si la interfaz vecina está en modo trunk o en modo desirable. Generalmente el modo switchport por defecto en los switch Cisco es dynamic auto, en cambio en los nuevos modelos el que está por defecto es dynamic desirable.
- *Switchport mode dynamic desirable:* Cuando se encuentra en este estado, la interfaz intenta convertir el enlace en uno troncal. La interfaz se convierte en interfaz trunk si la interfaz vecina está configurada como trunk, desirable o en modo auto.
- Switchport nonegotiate: Impide que la interfaz genere tramas DTP(Dynamic Trunking Protocol, usado para establecer si una conexión entre dos switch será en modo acces o trunk). Se puede usar solo cuando el modo del switch está en modo trunk o acces, la interfaz adyacente se debe configurar manualmente como trunk si se quiere que el enlace opere como trunk.

1.3. Tipos de VLAN

Nota: Gran parte del texto aquí presentado ha sido tomado del material disponible online en https://ccnadesdecero.es/ según se indica en Capítulo 6: VLAN - CCNA 2, "Segmentación de VLAN: Introducción".

1. **VLAN DE DATOS:** Una VLAN de datos es una VLAN configurada para transportar tráfico generado por usuarios. Una VLAN que transporta tráfico de administración o de voz no sería una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos.
2. **VLAN PREDETERMINADA:** Todos los puertos de switch se vuelven parte de la VLAN predeterminada después del arranque inicial de un switch que carga la configuración predeterminada. La VLAN predeterminada para los switches Cisco es la VLAN 1. La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no se le puede cambiar el nombre ni se puede eliminar. Todo el tráfico de control de capa 2 se asocia a la VLAN 1 de manera predeterminada.

3. **VLAN NATIVA:** Una VLAN nativa está asignada a un puerto troncal 802.1Q. Los puertos de enlace troncal 802.1Q admiten el tráfico proveniente de muchas VLAN (tráfico con etiquetas), así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar).El tráfico con etiquetas hace referencia al tráfico que tiene una etiqueta de 4 bytes insertada en el encabezado de la trama de Ethernet original (ver Figura 5), que especifica la VLAN a la que pertenece la trama. El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa, que es la VLAN 1 de manera predeterminada.

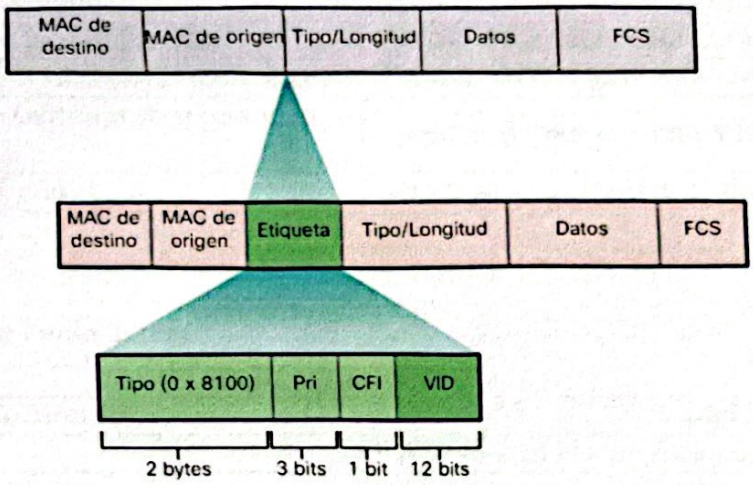


Figura 5: Campos en una trama Ethernet 802.1Q (Fuente: https://ccnadesdecero.es/examenes/)

- **Tipo:** es un valor de 2 bytes denominado "ID de protocolo de etiqueta" (TPID). Para Ethernet, este valor se establece en 0x8100 hexadecimal.
- **Prioridad de usuario:** es un valor de 3 bits que admite la implementación de nivel o de servicio.
- **Identificador de formato canónico (CFI):** es un identificador de 1 bit que habilita las tramas Token Ring que se van a transportar a través de los enlaces Ethernet.
- **ID de VLAN (VID):** es un número de identificación de VLAN de 12 bits que admite hasta 4096 ID de VLAN.

4. **VLAN de administración:** Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch.

1.4. Creación de una VLAN

Comando	Función
switch>enable	Acceso a modo privilegiado
switch# configure terminal	Acceso a modo de configuración global
switch(config)# vlan id_vlan	Añadir VLAN
switch(config - vlan)# vlan id_vlan	Nombre de la VLAN añadida

Cuadro 1: Comandos esenciales en la creación de una VLAN

Nota: Gran parte del texto aquí presentado ha sido tomado del material disponible online en `https://ccnadesdecero.es/` *según se indica en Capítulo 6: VLAN - CCNA 2, "Implementaciones de VLAN".*

1.5. Asignación de puertos a las redes VLAN

1.5.1. Configuración modo Access

Comando	Función
switch>enable	Acceso a modo privilegiado
switch# configure terminal	Acceso a modo de configuración global
switch(config)# interface id_interfaz	Acceso a modo de configuración de una interfaz
switch(config - if) # switchport mode access	Establecer el puerto en modo de acceso.
switch(config - if)# switchport access vlan id_vlan	Asignar el puerto a una VLAN.
switch(config - if)# end	Volver al modo privilegiado

Cuadro 2: Tabla de Asignación de puertos a las VLAN.

1.5.2. Configuración modo Trunk

Comando	Función
switch>enable	Acceso a modo privilegiado
switch# configure terminal	Acceso a modo de configuración global
switch(config)# interface id_interfaz	Acceso a modo de configuración de una interfaz
switch(config - if) # switchport mode trunk	Hacer que el enlace sea un enlace troncal
switch(config - if)# switchport trunk native vlan id_vlan	Especificar una vlan nativa para las tramas sin etiquetas
switch(config - if)# switchport trunk allowed vlan lista_vlan	Especificar la lista de VLAN que se permitiran en el enlace troncal.
switch(config - if)# end	Volver al modo privilegiado

Cuadro 3: Tabla de Configuración de enlaces troncales

1.6. Verificación de información de VLAN

Comando	Función
switch# show vlan	Mostrar información para todas las VLAN en el Switch
switch# show vlan brief	Mostrar solo el nombre, el estado y los puertos asociados de la VLAN
switch# show vlan name test	Mostrar la información de VLAN para una VLAN específica por nombre
switch# show vlan summary	Mostrar información sobre la cantidad de VLAN configuradas en el Switch

Cuadro 4: Tabla de comando show vlan

Nota: Gran parte del texto aquí presentado ha sido tomado del material disponible online en `https://ccnadesdecero.es/` *según se indica en Capítulo 6: VLAN - CCNA 2, "Implementaciones de VLAN".*

1.7. Eliminación de la asignación de VLAN

Comando	Función
switch>enable	Acceso a modo privilegiado
Switch#configure terminal	Acceso a modo de configuración global
Switch(config)# interface id_interfaz	Acceso a modo de configuración de una interfaz
Switch(config-if)# no switchport access vlan	Eliminar la asignación de la VLAN del puerto

Cuadro 5: Tabla de Eliminación de la asignación de VLAN.

1.8. Restablecimiento de valores configurados en enlaces troncales

Comando	Función
switch>enable	Acceso a modo privilegiado
Switch#configure terminal	Acceso a modo de configuración global
Switch(config)# no switchport trunk allowed vlan	Establecer el enlace troncal para permitir todas las VLAN.
Switch(config-if)# no switchport trunk native vlan	Restablecer la VLAN nativa al valor predeterminado.

Cuadro 6: Tabla de Restablecimiento de valores configurados en enlaces troncales.

1.9. Routing entre VLAN con routers

Nota: Gran parte del texto aquí presentado ha sido tomado del material disponible online en `https://ccnadesdecero.es/` *según se indica en Capítulo 6: VLAN - CCNA 2, "Routing entre VLAN con routers".*

Hay tres opciones para el routing entre VLAN:

- **Routing entre VLAN antiguo:** El routing entre VLAN antiguo se realiza mediante la conexión de diferentes interfaces físicas del router a diferentes puertos físicos de switch.

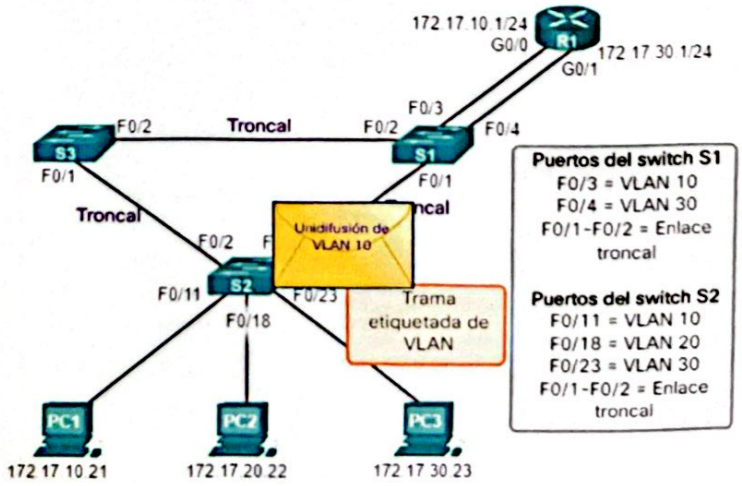


Figura 6: Ejemplo de routing entre vlan antiguo (Fuente: https://ccnadesdecero.es/examenes/)

- **Router-on-a-stick:** Es un tipo de configuración de router en la cual una única interfaz física enruta el tráfico entre varias VLAN en una red.

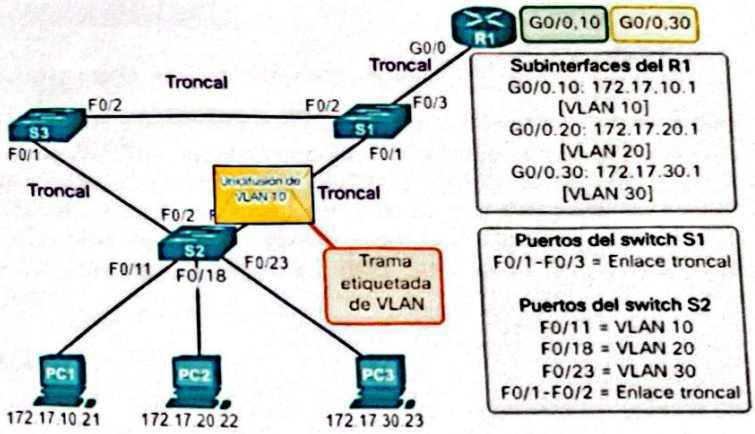


Figura 7: Ejemplo de ROUTER-ON-A-STICK (Fuente: https://ccnadesdecero.es/examenes/)

- **Switching de capa 3 mediante las SVI**

1. Lectura complementaria

1.1. Protocolo de Internet e identificadores

El *Internet Protocol* (IP) es un protocolo de comunicaciones de capa 3 (según modelo ISO/OSI) diseñado para sistemas interconectados de redes de computadores. Este protocolo permite transmitir bloques de datos llamados datagramas desde un origen hacia un destino, donde origen y destino se encuentran identificados por identificadores IP o *Internet Protocol Address*. Este es un protocolo *host-to-host* dado que en una red busca llevar datagramas hacia un siguiente *gateway* o host de destino. Este proceso de encaminamiento hacia el destino es llevado a cabo en base a el identificador IP, identificador lógico del dispositivo en la red. Este identificador para la versión 4 del protocolo consta de 4 Bytes.

1.1.1. Dirección IPV4

Características:

- Formada por 32 Bits o $32/8 = 4$ bytes.
- Está agrupado en 4 octetos. Ejemplo:
  11000000.10100000.00000000.00000000
- Normalmente se representa en decimal, agrupado por octetos y separado con puntos:
  192.168.0.1

1.1.2. Direccionamiento Classful (con clase) Vs Classless (sin clase)

En 1981, las direcciones IPv4 se dividieron en 5 clases (Vea la Fig 7)

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
A	0.0.0.0	127.255.255.255	128*	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	no aplica	no aplica	Multicast
E	240.0.0.0	255.255.255.255	no aplica	no aplica	Investigación

* El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza.

Figura 7: Tabla de identificadores IP y sus clases.

, donde

- **Clase A:** El primer bit del primer octeto es siempre '0', por lo cual las direcciones van desde la 0.0.0.0 a 127.255.255.255. Los primeros 8 bits pertenecen a red mientras que los 24 bits restantes representan host, es decir que su máscara de subred se expresa como 255.0.0.0
- **Clase B:** El primer octeto comienza siempre con '10', por lo cual las direcciones van desde la 128.0.0.0 hasta la 191.255.255.255. Los primeros 16 bits pertenecen a red, mientras que los 24 bits restantes representan host, es decir que su máscara de subred se expresa como 255.255.0.0
- **Clase C:** El primer octeto comienza siempre con '110', por lo cual las direcciones van desde la 192.0.0.0 hasta la 223.255.255.255. Los primeros 24 bits pertenecen a red, mientras que los 6 bits restantes representan host, es decir que su máscara de subred se expresa como 255.255.255.0
- **Clase D:** Representa una dirección de multidifusión, el primer octeto comienza siempre con '1110', por lo cual las direcciones van entre 224.0.0.0 hasta la 239.255.255.255
- **Clase E:** Son direcciones reservadas para fines investigativos. El primer octeto siempre comienza con '1111', por lo cual las direcciones van desde la 240.0.0.0 hasta la 255.255.255.255.

Bajo el esquema anteriormente presentado, ¿existirán desventajas?

La respuesta es sí, pues ¿y si alguien quiere 3000 direcciones útilizables?, ¿qué tan óptimo resultaría abordar este requerimiento con direccionamiento con clase?

Para resolver el inconveniente anteriormente mencionado, se introdujo CIDR (Enrutamiento entre dominios sin clase).

CIDR se introdujo en 1993 con la finalidad de reemplazar el direccionamiento con clase, permitiendo utilizar VLSM.

Por lo tanto, gracias a CIDR se pueden crear máscaras de subred de longitus variable y reducir el desperdicio de direccionamiento IP.

1.1.3. Direcciones Públicas y Privadas

- **Direcciones IP públicas:** Son visibles en todo Internet.
- **Direcciones IP privadas (reservadas):** Son visibles únicamente por otros nodos de su propia red o de otras redes privadas interconectadas por routers

1.2. Máscara de red

Corresponde a una máscara de 32-bits utilizada para discriminar dentro de las direcciones IP, el prefijo de la red y los hosts de esta. Cómo toda máscara oculta parte de la dirección para discriminar que parte de la dirección corresponde a el prefijo de red y cual a los hosts de esta. Para llevar a cabo el proceso de enmascaramiento se utiliza una operación AND al bit entre la dirección IP y la máscara seleccionada. En términos simples, la máscara define cuan grande es una red. En la Figura 8 se presenta un ejemplo del funcionamiento de la máscara.

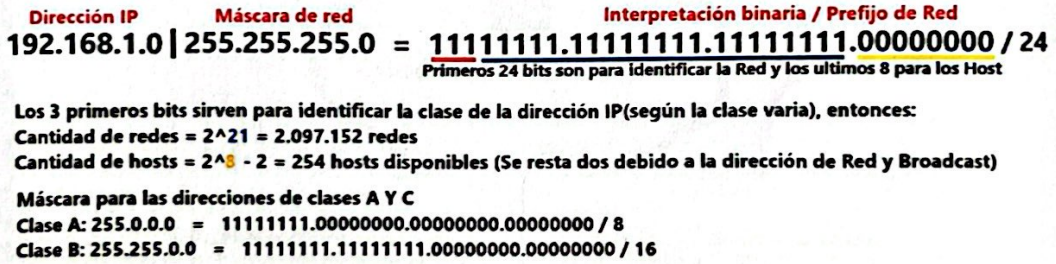


Figura 8: Ejemplo de una mascara de red asociada a una dirección IP en particular.

1.3. Sistema de numeración Binario y Decimal

1.3.1. Sistema Decimal

El sistema de numeración decimal consta de 10 dígitos para su representación: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Es decir, es un sistema en base 10.

1.3.2. Sistema Binario

El sistema binario consta de los dígitos 0 y 1 llamados bits que utiliza para su representación, asimismo, es un sistema en base 2. Cabe mencionar, que es importante comprender el sistema binario y decimal ya que:

"Las direcciones IPv4 comienzan como binarias, una serie de solo 1 y 0. Estos son difíciles de administrar, por lo que los administradores de red deben convertirlos a decimales"

decimal	0	1	2	3	4	5	6	7	8	9	10
binario	0	1	10	11	100	101	110	111	1000	1001	1010

Figura 9: Diferencia entre sistema Decimal y Binario

ccnadesdecero.es, afirma:

"Es importante que comprendamos el binario porque los hosts, servidores y dispositivos de red usan direccionamiento binario. Específicamente, usan direcciones binarias IPv4, como se muestra en la imagen, para identificarse entre sí."

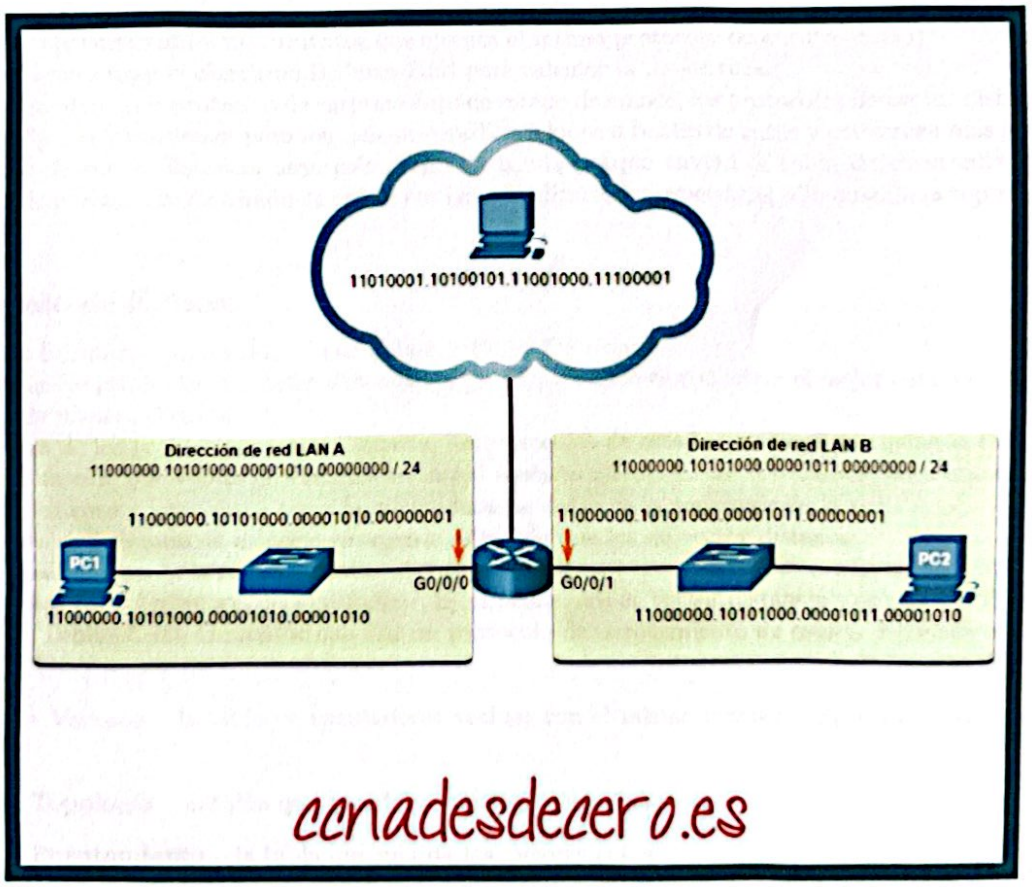


Figura 10: Direcciones binarias e IPv4 (Fuente: https://ccnadesdecero.es/)

1.4. División por Mascara de Red FIJA

- Nº subredes = $2^{bits\ de\ subred}$
- Nº host x subred = $2^{bits\ de\ host} - 2$

1. Lectura Complementaria

Nota: Gran parte del texto aquí presentado ha sido tomado del material disponible online en https://ccnadesdecero.com/curso/ según se indica en CNNA 200-301 (Volumen 1); V.Enrutamiento IPv4.

1.1. Vector Distancia

¿Qué es el Enrutamiento por Vector Distancia y Cómo Funciona?

Como indica su nombre, los protocolos de enrutamiento de vector distancia usan la distancia para determinar la mejor ruta para llegar a un red.

Cuando un enrutador aprende la ruta de una red, aprende tres factores importantes relacionados al enrutador:

- La red de destino.
- La distancia (métrica).
- El vector (el enlace y el enrutador del siguiente salto a usar como parte de la ruta).

Muchas veces, la distancia es el número de saltos (enrutadores) hasta la red de destino.

El protocolo de vector distancia generalmente envía la tabla de enrutamiento completa a cada vecino (un vecino esta directamente conectado a un enrutador que ejecuta el mismo protocolo de enrutamiento).

Estos protocolos usan el algoritmo Bellman-Ford para calcular la mejor ruta.

En comparación con el protocolo de enrutamiento de estado de enlace, los protocolos de vector distancia son más fáciles de configurar y mantener, pero son más susceptibles a loops o bucles de rutas y convergen más lento. Además los protocolos de vector distancia usan más ancho de banda porque envían la tabla de enrutamiento completa, mientras que los protocolos de estado de enlace envían actualizaciones especificas sólo cuando la topología de la red cambia.

1.2. Estado de Enlace

¿Qué es el Enrutamiento por Estado de Enlace y Cómo Funciona?

Al igual que los protocolos de vector distancia, el propósito básico es encontrar el mejor camino hacia el destino, pero lo hace de manera distinta.

A diferencia de los protocolos vector distancia, los protocolos de estado de enlace no envían la tabla de enrutamiento completa sino que avisan de cambios en la red (enlaces directamente conectados, enrutadores vecinos...), al final todos los enrutadores van a tener la misma base de datos de la topología de la red.

Los protocolos de estado de enlace convergen más rápido que los de vector distancia.

Envía actualizaciones de la red usando direcciones de multicast y usa actualizaciones de enrutamiento en cadena.

Requiere más CPU y memoria del enrutador que los protocolos de vector distancia y es más difícil de configurar.

Tipos de Tablas Cada enrutador que usa un protocolo de enrutamiento de estado de enlace crea tres tablas diferentes:

- Tabla de **Vecinos** – la tabla de enrutadores vecinos con el mismo protocolo de enrutamiento de estado de enlace.
- Tala de **Topología** – la tabla que guarda la topología de toda la red.
- abla de **Enrutamiento** – la tabla que guarda las mejores rutas.

1.3. Algoritmo de un protocolo de enrutamiento

El algoritmo de un protocolo de enrutamiento es una de sus mayores particularidades y éste puede ser:

- **Vector Distancia** o Distance Vector (DV) Ejemplo de protocolo: RIP e IGRP.
- **Estado de Enlace** o Link State (LS) Ejemplo de Protocolo: OSPF e ISIS.

Vector Distancia VS Estado de Enlace

Bases a comparar	Vector Distancia	Estado de Enlace
Algoritmo	Bellman-Ford	Dijsktra
Vista de la red	Información desde el punto de vista del vecino	Información completa de la topología de red
Cálculo del mejor camino	Basado en el menor número de saltos	Basado en el «costo»
Actualizaciones	Tabla de enrutamiento completa	Actualización del estado de los enlaces
Frecuencia de las actualizaciones	Actualizaciones periódicas	Actualizaciones especificas
CPU y memoria	Bajo uso	Alto uso
Simplicidad	Muy simple	Más complejo
Tiempo de convergencia	Moderado	Rápida
Actualizaciones (red)	Broadcast	Multicast
Estructura jerárquica	No	Si
Nodos intermedios	No	Si

Figura 10:

1.5. ¿Qué es la Métrica?

Si un enrutador aprende dos caminos diferentes para la misma red con el mismo protocolo de enrutamiento, éste debe decidir cuál ruta es mejor y la agregará a la tabla de enrutamiento.

La métrica es la medida usada para decidir la mejor ruta. Cada protocolo de enrutamiento usa su propia métrica. Por ejemplo, RIP usa el conteo por saltos como métrica, mientras que OSPF usa el costo.

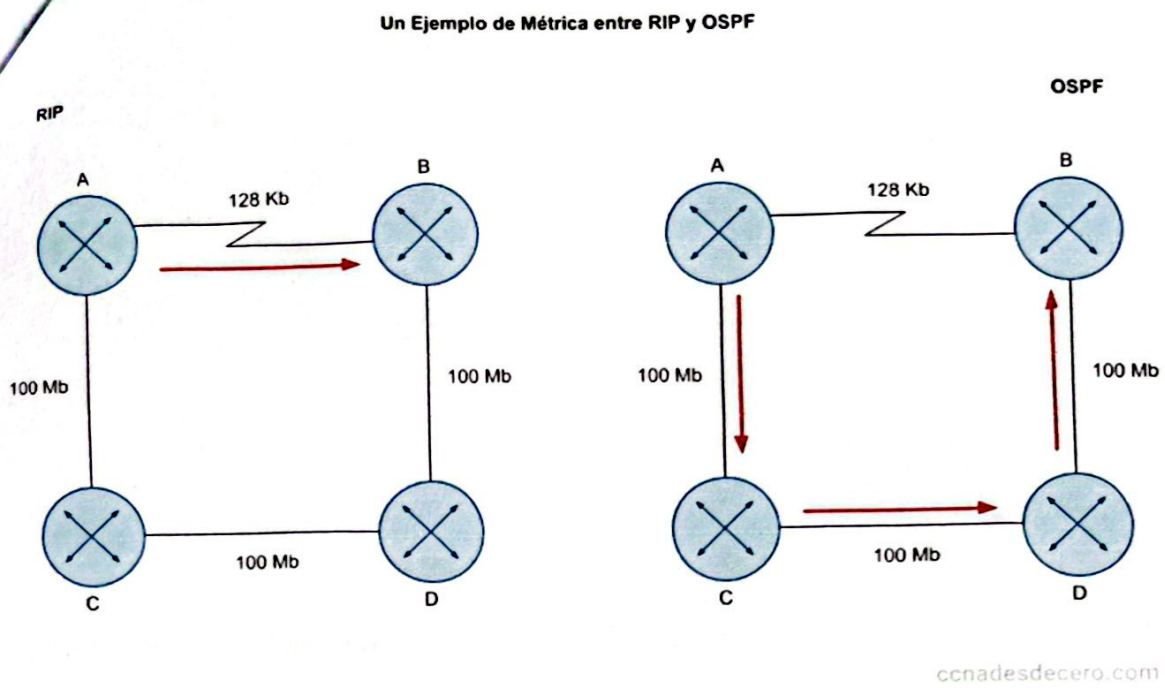


Figura 11: Ejemplo del Camino Más Óptimo, Más Corto o el Mejor Camino

La siguiente lista muestra algunos protocolos de enrutamiento y el tipo de métrica que usan.

Protocolo de enrutamiento	Métrica
RIP	Saltos
EIGRP	Ancho de banda, delay (retraso)
OSPF	Costo (ancho de banda)

1.6. Convergencia

El proceso necesario para que todos los nodos tengan una visión consistente de la red se conoce como **convergencia**.

- **Tiempo de convergencia:** es el tiempo que se necesita para que todos los router actualicen sus tablas después de que un cambio en la topología de la red haya tenido lugar. Cabe destacar, que cada protocolo de enrutamiento posee un método diferente para actualizar su tabla de routing. Bajo este contexto el tiempo de convergencia va a variar dependiendo del enrutamiento empleado.

  Nota: El tiempo de convergencia tiene que ser el más preferible posible.

1.7. Routing Information Protocol (RIP)

RIP (Routing Information Protocol) es un protocolo de vector distancia. Se usa generalmente para redes pequeñas y es muy simple de configurar y mantener. Pero carece de ciertas ventajas frente a otros protocolos de enrutamiento como OSP o EIGRP.

Existen tres versiones del protocolo: RIPv1, RIPv2 y RIPng.

Todas las versiones del protocolo RIP usan los saltos como métrica, soporta máximo 15 saltos y cualquier ruta mayor a esto sera inalcanzable.

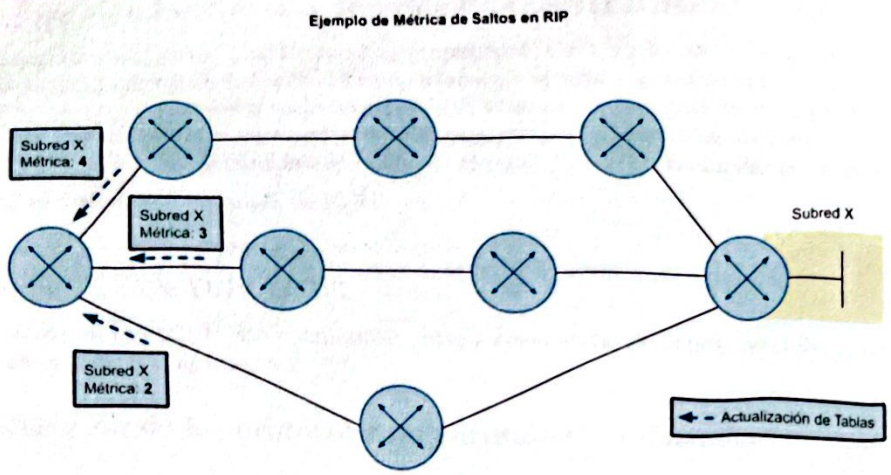


Figura 12: Ejemplo métrica de saltos RIP

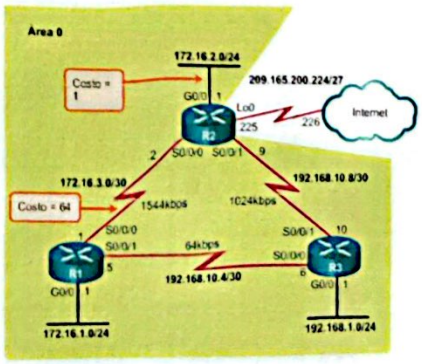
1.8. Open Shortest Path First (OSPF):

- es un protocolo LS que aplica Dijkstra o también conocido como Shortest Path First Algorithm.
- al tener información completa de la red puede calcular el camino óptimo aplicando este algoritmo.
- Dijkstra calcula la ruta más corta o óptima entre un origen a todo el resto de los nodos

1.8.1. Métrica de OSPF

- OSPF utiliza el costo como métrica para determinar la mejor ruta.
  - La mejor ruta tendrá el costo más bajo.
  - El costo está basado en el ancho de banda de la interfaz.
  - En la Figura 13 se aprecia la formula para calcular el costo y una tabla resumen.

Tipo de interfaz	Ancho de banda de referencia en bps		Ancho de banda predeterminado en bps	Costo
10 Gigabit Ethernet 10 Gbps	100,000,000	÷	10,000,000,000	1
Gigabit Ethernet 1 Gbps	100,000,000	÷	1,000,000,000	1
Fast Ethernet 100 Mbps	100,000,000	÷	100,000,000	1
Ethernet 10 Mbps	100,000,000	÷	10,000,000	10
Serial 1,544 Mbps	100,000,000	÷	1,544,000	64
Serial 128 kbps	100,000,000	÷	128,000	781
Serial 64 kbps	100,000,000	÷	64,000	1562



Costo OSPF = 10^8/BW (bps)

Figura 13: Definición del costo en OSPF

1.9. Enhanced Interior Gateway Routing Protocol (EIGRP)

Enchanced interior Gateway Routing Protocol, es propiedad de Cisco y además, es la versión mejorada de IGRP, el cual es un protocolo de vector de distancia. El comportamiento en esta nueva versión recae en que puede aprender del las otras redes en base a los que sus vecinos que están directamente conectados le enseñan, por esto, se dice que es un protocolo de enrutamiento de tipo vector de distancia avanzado, pues toma las características de vector de distancia y estado de enlace con la finalidad de aumentar el rendimiento. En resumidas cuentas, tenemos:

- El EIGRP es una versión mejorada de IGRP.
- Al igual que IGRP es un protocolo Distance Vector.
- Soporta routing classless, VLSM y CIDR.
- Métricas similares con IGRP, son compatibles entre ambas: ancho de banda, retardo, confiabilidad y carga. EIGRP usa un cálculo más avanzado.

1.10. Clasificación de los protocolos de enrutamiento dinámico

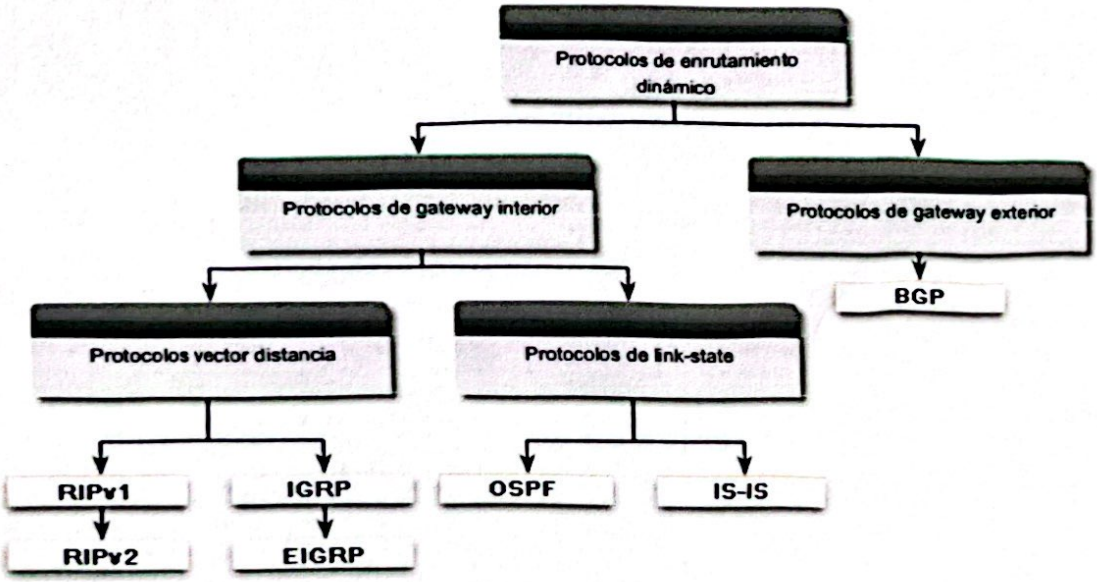


Figura 14: Fuente: Cisco System, Inc

	Vector distancia				Estado de enlace	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Velocidad de convergencia	Lento	Lento	Lento	Rápido	Rápido	Rápido
Escalabilidad: tamaño de la red	Pequeño	Pequeño	Pequeño	Grande	Grande	Grande
Uso de VLSM	No	Sí	No	Sí	Sí	Sí
Uso de recursos	Bajo	Bajo	Bajo	Medio	Alto	Alto
Implementación y mantenimiento	Simple	Simple	Simple	Complejo	Complejo	Complejo

Figura 15: Tabla comparativa de los protocolos de enrutamiento