- la IP publica el servidor web recibe un paquete del otro computador. en donde recibe la IP publica.
- Dentro de la LAN uno usa IP privada.
- Tabla ARP, tabla nat eo

RESUMEN TELECOMUNICACIONES

1. Redes de datos

1.1 Introducción

Red de datos: conjunto de infraestructura que permite a dos o más computadores comunicarse entre sí. Se representan por un grafo. /se representan por un grafo.

infraestructura → empresas → router usuarios

Tipos de comunicación /dependen del escenario

- **Full-duplex:** cuando el dispositivo puede transmitir y recibir al mismo tiempo. /gritos dentro sala.
- **Half-duplex:** cuando el dispositivo puede transmitir y recibir pero NO al mismo tiempo. /walki-teki
- **Simplex:** cuando el dispositivo solo puede transmitir. / radio → frecuencia en particular.

Tipos de conección → se usaban para telefono.

Los dispositivos están conectados a través de medios de transmisión como cables de cobre, fibras ópticas y espacio libre. → fibra optica es lo mas usado y lo nuevo.

¿Qué nos ofrecen los ISP? → Internet System Probible

Red de última milla

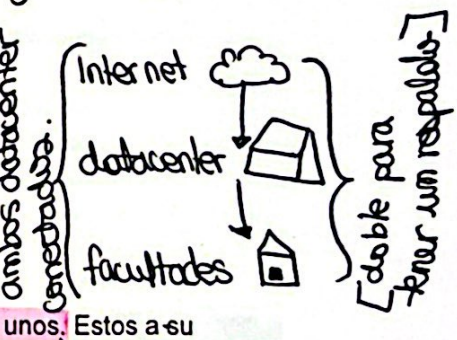
- Medio de transmisión
- Velocidad bajada/subida (simétrica o asimétrica)

Dispositivos de red

NAT/CGNAT → tecnologias para reutilizar IP privada.

- SA nos permite comunicarnos con otros SA

ambos datacenter conectados.



¿Qué transmitimos por Internet?

Transmitimos impulsos de luz o electricidad, que se traducen en ceros y unos. Estos a su vez se pueden convertir a otras bases, más fáciles de trabajar para un usuario final como ASCCI y Hexadecimal.

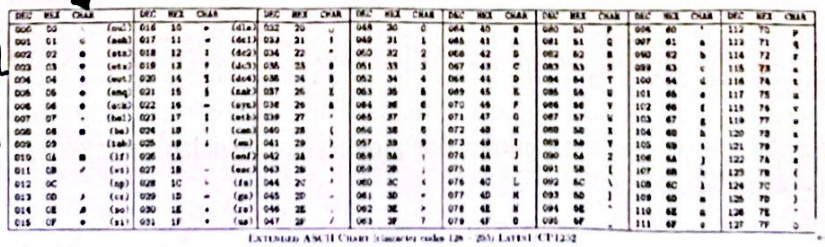
(info bruto) → fibra optica → cable coaxial, circuitos → ausencia → presencia

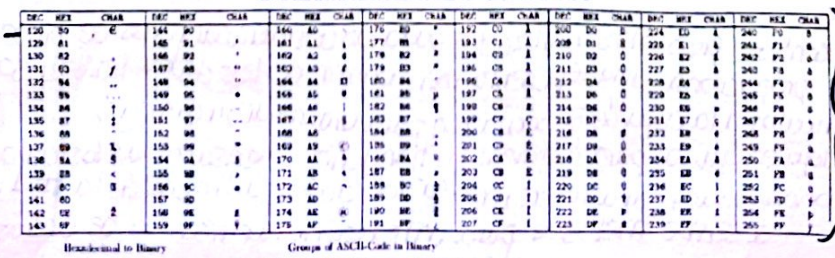
tasa de refresco: luz parpadea. ventana de tiempo: cada cierto tiempo se apaga o se prende, se define eso y se traduce en 1 o 0.

1 caracter HEXADECIMAL

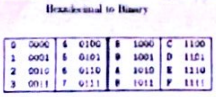
4 bits = 2^4 = 16 valores [0 a la 15]

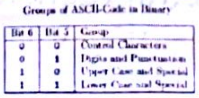
TABLA ASCCI



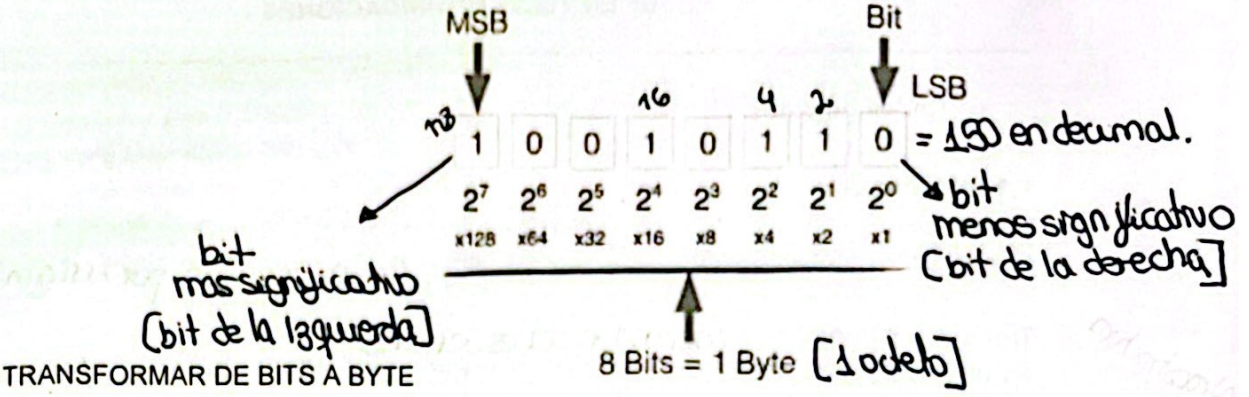


extendido ASCII.



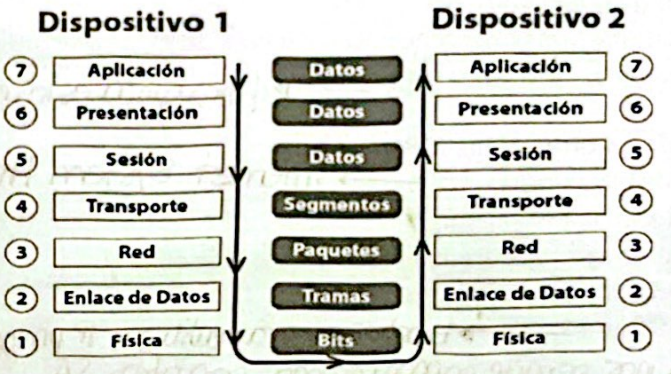


- Neutralidad de la red: ley de latencia maxima, perdida de paquetes, etc.
- tasa de aparicion se ve tasa de reventa de un proveedor de internet.



TRANSFORMAR DE BITS A BYTE

¿Cómo el receptor sabe cómo interpretar todos los bits recibidos? Mediante la capa OSI.



Jerarquías de Protocolos

La mayoría de las redes están organizadas en una serie de niveles o capas, cada una construida sobre la anterior, el objetivo del diseño en capas es abstraer la implementación, definiendo una API (Application Program Interface) o conjunto de servicios entregados a la capa superior.

Los mensajes tienen una estructura base, compuesta de un header y un payload o cuerpo del mensaje. A veces, además, incluye un trailer o información adicional después del cuerpo. El mecanismo de colocar un mensaje de una capa en el contenido de otro se llama "encapsulación" y es fundamental para varios protocolos y tecnologías de redes.

MODELO OSI

- Cuenta con 7 capas.

Datos.
7. Aplicación: contiene protocolos utilizados para las comunicaciones de proceso a proceso.
6. Presentación: proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación.
5. Sesión: da servicios a la capa de presentación para organizar su diálogo

segmentos / paquet / frames / bits /
4. Transporte: define servicios para segmentar, transferir y reensamblar los datos para comunicaciones
3. Red: proporciona servicios para intercambiar los datos a través de la red entre dispositivos finales.
2. Enlace de Datos: describe métodos para intercambiar tramas de datos entre dispositivos, a través de un medio común.
1. Física

→ describe 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.

• sistema autónomo: conjunto de redes IP y routers que opera bajo una administración común y comparte una política de enrutamiento única.

Diseño de capas

- Cada capa necesita un mecanismo para identificar a los emisores y a los receptores.
- Como se tienen muchos computadores, se necesita un método para que un proceso en una máquina especifique con cuál de ellas quiere hablar.
- Como se pueden tener muchos destinos, se necesita alguna forma de direccionamiento a fin de precisar un destino específico.
- El control de errores es un aspecto importante, ya que los circuitos físicos no son perfectos. Para esto, el receptor debe tener algún medio en donde le diga al emisor que el mensaje se ha recibido correctamente y cuál no. Ambos extremos deben estar de acuerdo con que código de detección y corrección vayan a usar.
- No todos los canales de comunicación conservan el orden en que se les envían los mensajes, para tratar con un posible pérdida de secuencia, el protocolo debe incluir un mecanismo que permita al receptor volver a unir los pedazos en forma adecuada. → TCP cuenta con distintos flags
- Además en cada nivel se debe evitar que un emisor rápido sature de datos al receptor más lento, para esto se puede realizar algún tipo de retroalimentación del receptor al emisor, directa o indirectamente, dependiendo de la situación actual del receptor. O limitar al emisor a una velocidad acordada (control de flujo).

Entidades estandarizadoras

1. ITU (International Telecommunication Union): regula las tecnologías de la información y la comunicación a nivel internacional.
2. La ANSI (American National Standards Institute): supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos.
3. La IEEE (Institute of Electrical and Electronics Engineers): desarrolla estándares técnicos.
4. El NIST (National Institute of Standards and Technology).
5. La IETF (Internet Engineering Task Force): se centra en el desarrollo y la promoción de estándares de Internet.
6. La IRTF (Internet Research Task Force): se centra en la investigación a largo plazo relacionada con Internet, impulsando la investigación y el desarrollo de tecnologías emergentes que podrían ser relevantes en el futuro.

Dispositivos de red → Limitancia física de cables, para regenerar la señal.

Tienen como propósito aumentar el alcance de una red, localizar el tráfico de la red, aislar los problemas de la red, así los problemas pueden ser diagnosticados más fácilmente.

TIPOS

1. Network Interface Card: pueden ser físicas/virtuales, permiten conectarse con equipos de red. → ifconfig = interfaces de usuario. / maquina virtual → vlr br0
2. Repetidores: operan a nivel de capa 1, función principal es expandir el alcance de una red, mediante la "limpieza" y amplificación de la señal. Ej: repetidor / megafono.
3. Hubs: el repetidor es un concentrador, constituye el elemento central de la red, el área de red dentro de la cual los paquetes son originados y colisionan, se conoce como un dominio de colisión. → concentra la información → dentro de una red WIFI se usa un concentrador → manda info a la capa de app pidiendo permiso
4. Bridges: operan a nivel de la capa 2, eliminan el tráfico innecesario y minimizan las posibilidades de colisión mediante la división en segmentos y el filtrado basado en la dirección física. Son capaces de analizar los paquetes entrantes y despacharlos en base a la dirección, toman y pasan paquetes entre segmentos, controlan los mensajes de broadcast y mantienen tablas de direcciones.

→ manda info por distintas bocas, evitando repetición de paquetes en el mismo medio.

→ S capa 3 logra reconocer IP para administrar depto de internet
→ capa 2 y lee la MAC address
→ no necesita IP para comunicarse.
→ se coloca un switch cuando hay distintos dispositivos en una LAN y se quieren conectar.

5. Switches: versión más avanzada con más puertos y capacidades de rendimiento superiores en comparación con el bridge.

6. Routers: se usan para conectar redes, proveen conectividad end-to-end, mediante el paso de paquetes y tráfico de ruteo entre diferentes redes basado en información de la capa 3. Poseen la habilidad de tomar decisiones de baje al mejor camino para despachar los paquetes. Segmentan dominios de broadcast. → sirven para comunicarse entre routers para llegar al destino requerido.

rutea cuenta con algoritmos de ruteo

envía a los IPs del prefijo a la que pertenece.

7. Gateway: el dispositivo que comunica dos redes, o más bien una red con "el exterior". Un gateway puede ser cualquier equipo de red con al menos 2 puertos a los que se conectan redes distintas (tanto lógicas como físicas). → router es un gateway en una red.
→ firewall.
→ puede existir otro gateway antes del router. (autentificador).

Topologías/forma de despliegue

Corresponden a la disposición de los nodos y los medios de comunicación en una red. En una Local Area Network, las estaciones de trabajo y servidores deben estar conectados. Estas conexiones son permitidas por los medios físicos.

(como mapeamos nodos y aristas en un grafo)

TIPOS:
→ especifican el tipo de dispositivo utilizado en cada red, los puertos de conexión, los medios de red y el direccionamiento IP.

Topología lógica : Como se desempeñan.

Topología física: Se refiere a las conexiones físicas e identifica cómo se interconectan los dispositivos finales (computadores, cámaras, TV, consola de videojuegos) con los elementos de infraestructura (routers, switches y puntos de acceso inalámbrico). Además especifica la ubicación dentro de un entorno (campus, colegio, fábrica, edificio, hogar) de los terminales (computadores, cámaras, etc) y los dispositivos de infraestructura.

broadcast: método de comunicación donde un dispositivo envía un mensaje que será recibido por todos los dispositivos de una red lógica.

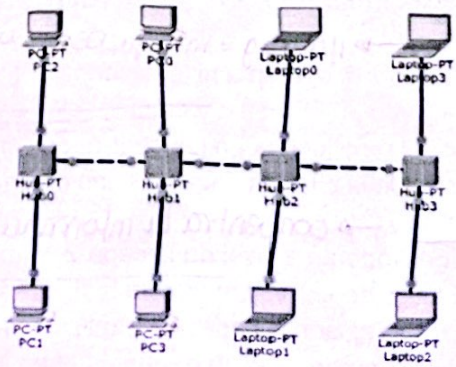
Tipos

- **Bus:** dispositivos conectados en un medio lineal (troncal/bus), cada dispositivo se conecta al medio independientemente, en cada extremo el bus tiene un terminador, que tiene como objetivo absorber la señal eléctrica y así evitar que rebote continuamente. ¡SE USAN EN REDES PEQUEÑAS, COMO SISTEMAS INDUSTRIALES.

Características:

- Soporta comunicación Half-Duplex. → señales viajan en ambas señales.
- Si la dirección de destino del fragmento no corresponde a la MAC address de la interfaz del dispositivo, entonces se ignora.
- Se utiliza mecanismo de detección de colisiones, para asegurar la transmisión una sola vez.
- No es escalable, reduce el rendimiento de la red. → cada vez que me comunico colisiona lo que me llega con lo que mando.
- Tiene como desventaja la mantención, debido al diagnóstico de la falla.

- número de equipos afecta el rendimiento.



SE USAN EN REDES METROPOLITANAS O TELECOMUNICACIONES.

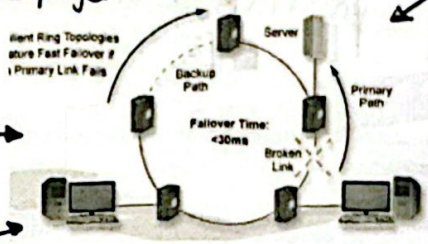
- **Anillo:** las estaciones están unidas unas con otras formando un círculo por medio de un cable común, el último nodo se conecta al primero cerrando el anillo, las señales circulan en un sentido regenerandose en cada nodo con el fin de que cada nodo examine la información enviada a través del anillo, sino va dirigida a ese nodo pasa al siguiente y así.

  Características:

  - Tiene como desventaja que si se rompe una conexión, se cae la red completa.
  - En este tipo de red la comunicación se da por el paso de un token o testigo.
  - No existen las colisiones.

señales circulan en un solo sentido, regenerandose en cada nodo.

no existen las colisiones, ya que uno habla a tiempo, sino me quedo callado.



si ocurre paso por c/u, si se rompe un enlace va hacia otro lado, pero si se cae un nodo falla completa.

topologías resilientes

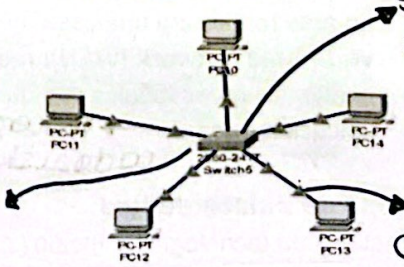
- **Estrella:** todo el tráfico pasa a través del concentrador, en una topología de este tipo, el medio va desde el concentrador hasta cada equipo conectado. (hub, switch, etc)

  Características:

  - Red más fácil de instalar, de mantener(única zona de concentración en el concentrador).
  - Si un medio se corta o sufre deterioro, sólo el aparato conectado a él queda fuera de servicio.
  - Requiere más cable para su instalación.
  - La existencia del concentrador lo convierte en un punto único de falla

SE USAN EN REDES DOMESTICAS O PEQUEÑAS OFICINAS.

switch de cuelgan los computadores



mucho cable.

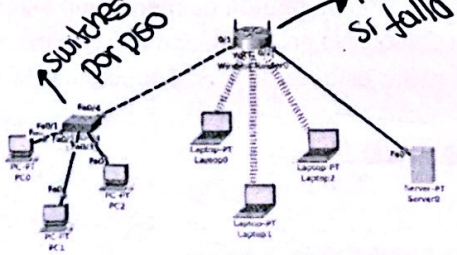
muere switch, muere todo.

- **Árbol:** los nodos están colocados en forma de árbol, la conexión es parecida a una serie de redes en estrella interconectadas. La falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

SE USAN EN REDES JERARQUICAS COMO CAMPUS O GRANDES EDIFICIOS

suntos por paso

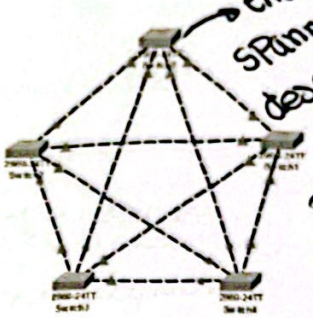
router cabecera. si falla este, falla todo



→ SE USA EN REDES CRITICAS QUE REQUIEREN ALTA REDUNDANCIA

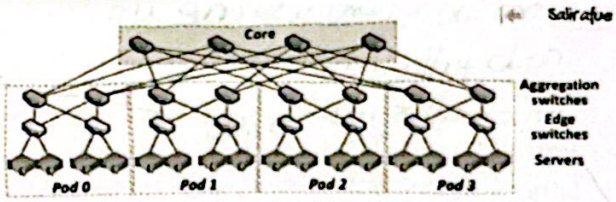
- **Malla:** topología de red en la que cada nodo está conectado a uno o más de los otros nodos, pudiendo llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada se minimiza al máximo interrupciones por corte en las comunicaciones.

→ mas resiliente.
→ redundante, Si se cae uno.
→ muy caro.
→ mayor facilidad para protocolos de transporte.



envían a todos
Spanning Tree desactiva de forma lógica puertos, para no entrar en un loop.

- **Fat-Tree:** utilizada generalmente por Datacenters.



Network Areas / cobertura

- **Body Area Network (BAN):** Es una red de comunicación inalámbrica entre dispositivos de baja potencia utilizados en el cuerpo, consiste en un conjunto móvil y compacto de comunicación.
- **Personal Area Network (PAN):** Corresponde a la interconexión de dispositivos TI, dentro del alcance de una persona, normalmente en un rango de 10 metros.
- **Local Area Network (LAN):** Corresponde a una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.
- **Wide Area Network (WAN):** red de área amplia, es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física. → convergen en un router unico para comunicarse cada sistema autonomo.

1.2 Capa de Enlace de Red

Ethernet es una tecnología de medio compartido(cable de cobre, coaxial, wireless), lo que significa que todos los dispositivos en la red deben escuchar las transmisiones y contener o negociar por la oportunidad o derecho a transmitir.

Cuando un dispositivo determina que hubo una colisión, se procede con un backoff, la retransmisión se retarda basado en un algoritmo, y el largo de ese retardo es diferente para cada dispositivo en la red, con el fin de minimizar la posibilidad de una posterior colisión. Para evitar esto, se tiene a la subcapa MAC.

Subcapa MAC

Como evitamos que multiples usuarios con la misma prioridad accedan al medio → Ethernet, WiFi, bluethoot accesos al medio.

Las redes pueden dividirse en dos categorías:

- Conexiones punto a punto
- Canales de difusión o broadcast

→ redes multicast: no todos acceden al canal. Quien usa el canal cuando existe competencia

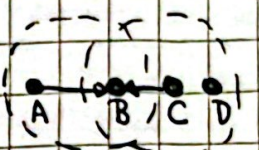
→ canalización con protocolo: no peleo por que tengo slots para el acceso (FDMA, TDMA, CDMA).

→ protocolo acceso controlado: reservamos el acceso / limitado y controlado.

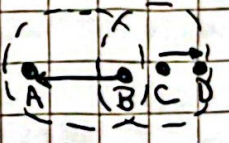
→ Protocolos de acceso aleatoreo:

- CSMA: en este protocolo un nodo verifica la ausencia de tráfico antes de transmitir en un medio compartido. Si al verificar el medio antes de transmitir una señal es detectada, el nodo espera a que la transmisión en progreso finalice antes de iniciar su propia transmisión.
- CSMA/CD: la técnica consiste en escuchar el medio mientras se transmite, si la señal escuchada es diferente a la que se transmite, se sabe que hay una colisión.
- CSMA/CA: ambiente inalámbrico con CSMA/CD las colisiones no pueden ser detectadas, además existen problemas con la detección de la portadora.

→ terminal escondido: C piensa que el medio esta libre y transmite a B interfiriendo la transmisión de A hacia B.



→ terminal expuesto: B envía a A, por otro lado, C al mismo tiempo desea enviar a D, escucha el medio y no transmite



Campos comunes trama Ethernet

- MAC Address: de destino y origen indican las direcciones físicas del dispositivo al que van dirigidos los datos y del dispositivo origen de los datos (48 bits).
- Payload: lugar donde van todos los datos de los protocolos de capas superiores. (46 - 1500 bytes.)
- secuencia de comprobación: campo de 4 bytes que contiene un valor de verificación CRC.

→ direcciones físicas: (48 bits o 6 bytes de largo).
(2 partes; 24 bits OUI: fabricante de HW; 24 bits NIS: n° de serie del dispositivo).

→ direccionamiento Ethernet:
cuando host A desea comunicarse con B dentro de la misma subred, las direcciones MAC en la trama ethernet corresponden la MAC del host A para la MAC de origen y la MAC del host B para la MAC de destino.
(La mac de destino siempre corresponde a un host que esta en la misma subred).
Si estan fuera de la subred, la MAC del host A es la MAC de origen y la MAC de default gateway para la MAC de destino.
Dirección broadcast: FF:FF:FF:FF:FF:FF; envía una trama a todos los equipos de una subred.

→ canalización con protocolo: no peleo por que tengo slots para el acceso (FDMA, TDMA, CDMA).

→ protocolo acceso controlado: reservamos el acceso / limitado y controlado. (de reserva, muestreo, paso de testigo).

→ driver: sw que actua como intermediario entre SW y HW.

Colisiones → al enviar la señal se atenua y choca con otras señales se convierte en otra señal

Para detectar si se va a producir una colisión, la estación comprueba si la señal transmitida es idéntica a la del medio de transmisión. Si no fuera así, otra estación transmitirá al mismo tiempo, distorsionando así la señal del Bus.

Un **dominio de colisión** es un segmento físico de una red en el que las estaciones comparten un medio de transmisión y pueden colisionar

Protocolos de acceso aleatorio → mecanismos de acceso al medio.

- **Carrier Sense Multiple Access (CSMA):** CSMA indica que si el transmisor desea enviar datos pero detecta una transmisión en curso, este debe esperar para el envío de estos.
  Problema: Ya que varias estaciones pueden haber detectado la transmisión y estar a la espera para transmitir cuando el canal esté desocupado, pueden colisionar ya que todas ellas desean transmitir a la vez.
  Solución: Hacer que la espera para volver a transmitir después que el canal está desocupado sea aleatoria (con algún grado de probabilidad). → agregar probabilidad distinta, para enviar en t x.
  → sensa el medio, si hay ruido en el medio espero, sino envio

  (detecta si el medio esta transmitiendo o no) (transmito y luego escucho al medio)

- **Carrier Sense Multiple Access / Collision Detection (CSMA/CD):** Como CSMA no dice qué hacer en caso de que haya una colisión mientras el nodo está transmitiendo un mensaje, en CSMA/CD, la técnica consiste en escuchar el medio mientras se transmite. Si la señal escuchada es diferente a la que se transmite, se sabe que hay una colisión. Ante la presencia de colisión se pasa a una fase de contención.
  Con el fin de asegurar que las estaciones detecten la colisión, el transmisor debe enviar a lo menos 64 bytes (largo mínimo aceptado en un segmento Ethernet). Si dos estaciones están en extremos opuestos, el transmisor debe esperar cierta cantidad de tiempo antes de detectar la colisión. Ese tiempo tiene que ser acotado.

  (encuentra las colisiones) → tiempo de backoff: tiempo aleatorio en que todos los nodos dejan de transmitir
  → timeout = 16.
  → menos, agrego padding.

- **CSMA/Collision Avoidance:** CSMA/CA difiere CSMA/CD en la naturaleza del medio. Las colisiones no pueden ser detectadas mientras se envía, por lo que la detección de colisiones no es posible.
  → ocurre en redes inalambricas / redes wi-fi → evitar

  (evitar las colisiones, solicitando el acceso)

• base para reacción de protocolos, se repite en otras capas.

Algoritmo de retroceso exponencial binario: utilizado para colisiones y en caso de no respuesta para no saturar el medio.

Ethernet: Mac Address, Mac destino, etc. / trama paquete: destino, origen, tipo y data/Unit.

MAC Address → compuestas por un preambulo.

Compuesta por dos partes

- 24 bits llamados OUI: identifica quién es el fabricante del hardware. / = vendor, there ≠ OUI
- 24 bits llamados NISI: número de serie que identifica al dispositivo fabricado.

→ se tienen 24 bits, asociados a un VENDOR (fabricante).

Direccionamiento Ethernet

Cuando un host A desea comunicarse con un host B dentro de la misma subred, las direcciones MAC en la trama ethernet corresponden la MAC del host A para la MAC de origen y la MAC del host B para la MAC de destino.

→ la MAC destino es primero en mandar que la MAC de origen, ya que para que analizo un paquete sino es para mí

→ //

Cuando un host A desea comunicarse con un host B que está fuera de la subred, las direcciones MAC en la trama ethernet corresponden la MAC del host A para la MAC de origen y la MAC del default gateway para la MAC de destino.

→ MAC Address a redes locales / mac origen del router

SIEMPRE la MAC de destino corresponde a un host que está en la misma subred que el host de origen.

Direccionamiento Broadcast:

Existe una dirección MAC llamada dirección Broadcast que permite enviar una trama a todos los equipos en una subred, siempre y cuando no pasen a través de un router.
La dirección Broadcast ethernet es FF:FF:FF:FF:FF:FF.

ARP(Address Resolution Protocol)

Protocolo de red utilizado para encontrar la dirección MAC (dirección física de capa de enlace) asociada a una dirección IP (dirección lógica de capa de red) dentro de una red local (*LAN*).
Todos los computadores que sean alcanzables colocando la dirección de capa 2 de destino en el frame están dentro del dominio de broadcast.
Para almacenar las direcciones de capa 2 de los computadores del dominio de broadcast, el computador usa la tabla ARP.

TIPOS DE COMUNICACIÓN

comunicacion multicast a todo el mundo / antena omnidireccional.
comunicacion unicast: hacia una persona / II directiva.
comunicacion Broadcast: llega un segmento de personas.

ARP:
tabla ARP se llena por monitoreo de trama en el medio.
Contiene info entre la IP y MAC / memoria CACHE.

Conmutación

Proceso por el cual un switch transporta una trama desde un puerto de entrada (asociado al nodo transmisor) hacia un puerto de salida (asociado al nodo receptor).

Para saber por cual puerto debe ser conmutada la trama, el switch utiliza la tabla Content Addressable Memory (CAM). **Una tabla CAM tiene la asociación entre la MAC address y el puerto en el switch al cual está conectado cada nodo.**

→ Tabla CAM para ver quien se encuentra detras.

Problemáticas actuales en una red

Se espera una alta disponibilidad de la red, auto-reparación y rendimiento. Para lograr esto se usa redundancia, resiliencia, topología mesh y virtualización.

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

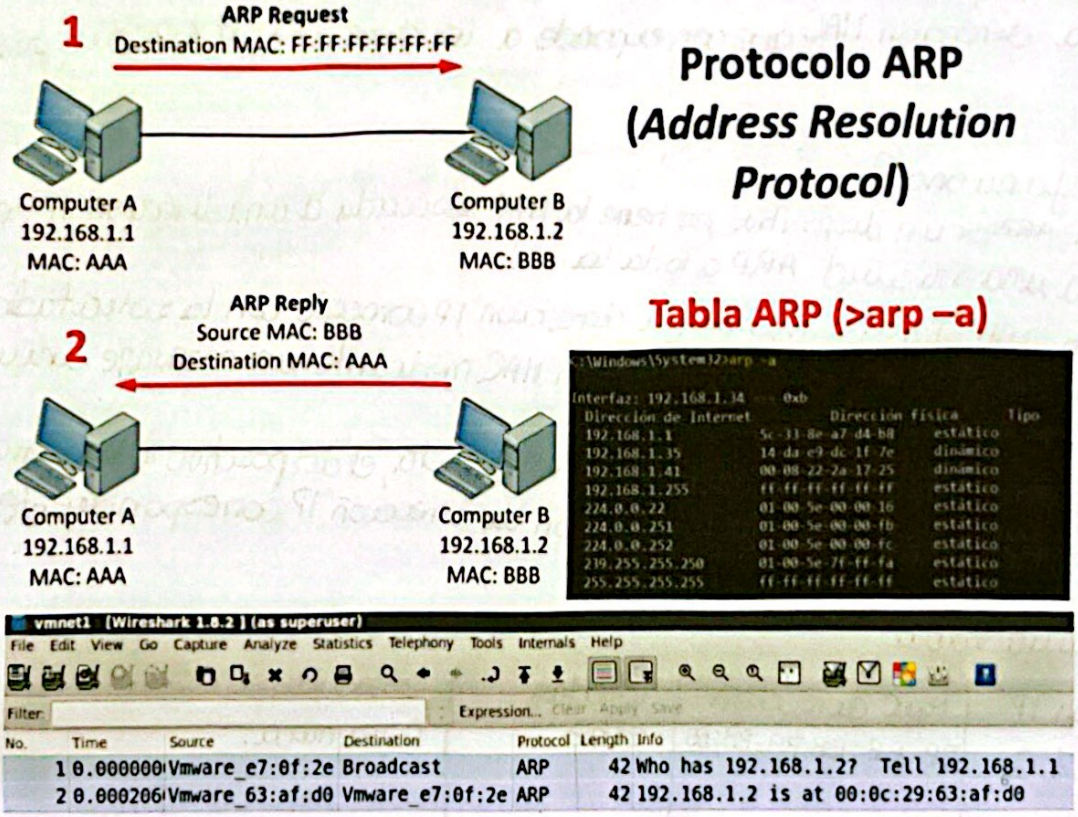


Figura 10: Ejemplo del contenido de una tabla ARP de un Host de SO windows

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

Tabla ARP:

→ estructura de datos utilizada en redes de computadoras para mapear direcciones IP a direcciones MAC.

→ esencial para la comunicación en redes locales (LAN), donde los dispositivos necesitan conocer la dirección MAC del destino para enviar paquetes a través del medio de red.

→ ARP: protocolo de resolución de direcciones (Address Resolution Protocol).

- es un protocolo de red que se encarga de convertir una dirección IP en una dirección MAC.
- Para enviar paquetes de un dispositivo a otro en la misma red local, se debe conocer la dirección MAC que corresponde a la dirección IP del dispositivo de destino.

→ ¿Como funciona?

- Solicitud ARP: Si un dispositivo no tiene la MAC asociada a una dirección IP en su tabla ARP, envía una solicitud ARP a toda la red.
- Respuesta ARP: el dispositivo cuya dirección IP coincide con la solicitada responde directamente al emisor con su dirección MAC mediante un mensaje unicast dirigido al solicitante.
- Actualizar la tabla ARP: ya recibida la respuesta, el dispositivo almacena la dirección MAC en su tabla ARP junto con la dirección IP correspondiente.

→ Estructura tabla.

Dirección IP	Mac dirección	Interfaz	estado/tipo.
192.168.1.2	BB:BB:BB:BB:BB:BB	eth0	Dinamica.

→ Si no hay comunicación durante un tiempo, la entrada puede eliminarse de la tabla, obligando a realizar otra solicitud ARP.

→ La tabla se actualiza con la que se envía.

Ej: Si A envía a C → actualiza A su tabla

→ LAN se forma a través de un switch
→ switch logra que todos los equipos conectados a el se puedan ver.

→ VLAN 1 por defecto / switch Fa0/1 = fast Ethernet / Gig1/1 = giga Ethernet.

VLAN → red virtual

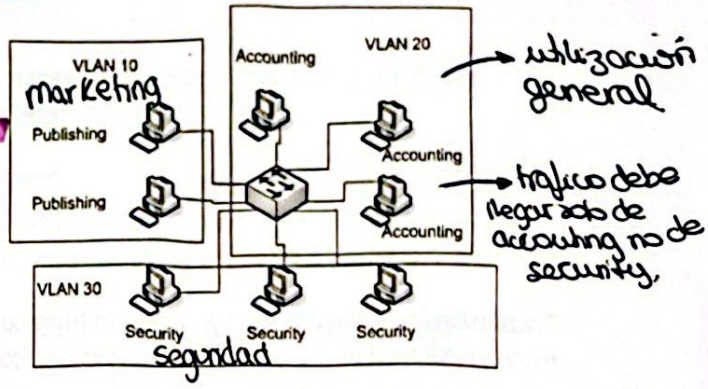
Red de área local que agrupa un conjunto de equipos de manera lógica y no física. → se puede usar dentro de cualquier red.

La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece las siguientes ventajas:

- Mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores.
- Aumento de la seguridad, ya que la información se encapsula en un nivel adicional y posiblemente se analiza.
- Disminución en la transmisión de tráfico en la red.

→ tipos:

- VLAN nivel 1: define una red virtual según los puertos de conexión del conmutador.
- VLAN nivel 2: define una red virtual según las direcciones MAC.
- VLAN nivel 3: agrupar en base al mismo protocolo en la misma red



→ utilización general

→ tráfico debe llegar solo de accounting no de security.

Enlace troncal → tráfico de varias VLAN pasan por un cable para varios switches → agregar enlaces físicos, como si fueran enlaces lógicos

En una red conmutada, un enlace troncal es un enlace punto a punto que admite varias VLAN.

El enlace troncal agrupa múltiples enlaces virtuales en un enlace físico, permitiendo que el tráfico de varias VLAN viaje a través de un solo cable entre los switches.

→ Mayor velocidad.

VLAN Trunking Protocol (VTP) 802.1Q

Protocolo que permite desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking).

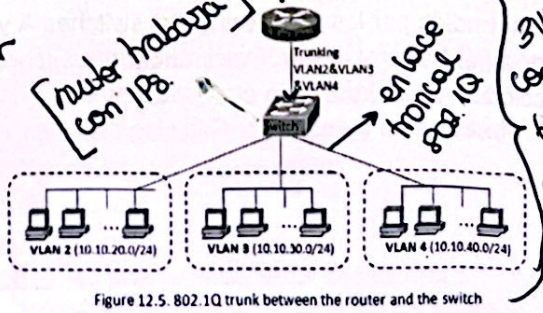
para esto se usa.

→ virtualizar multiples enlaces.

→ se crea otra interfaz para estar conectados a las distintas VLANS.

→ Baa física, puede tener multiples IP distintas (virtuales)

router trabaja con IPs. → multihome. → debe tener los IP gateway: 30.1 30.1 40.1



enlace troncal 802.1Q

3 VLAN distintas, con prefijos distintos todos conectados al switch

Figure 12.5. 802.1Q trunk between the router and the switch

Solución para que no exista cuello de botella entre switches.

Link-Aggregation

Consiste en utilizar múltiples cables de red en paralelo para aumentar la velocidad del enlace y para incrementar la redundancia para proveer una alta disponibilidad.

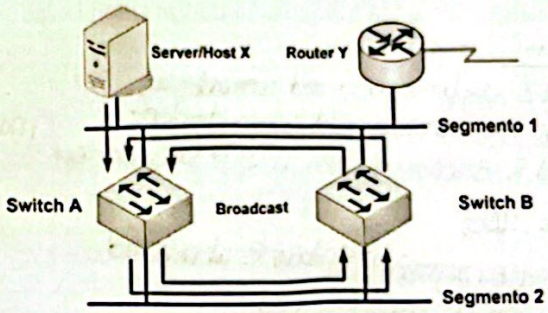
→ tratar n enlaces como si fuera una sola para agregarlos.

Redundancia física

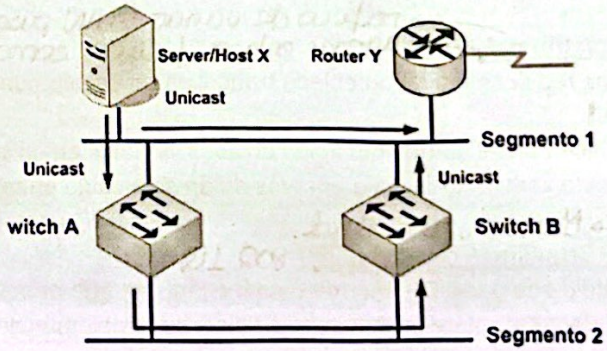
Topologías redundantes son más tolerantes a fallas, mayor disponibilidad.

- Eliminan punto único de falla Problemas:
- Tormenta de broadcast
- Transmisión múltiple
- Inestabilidad de las tablas

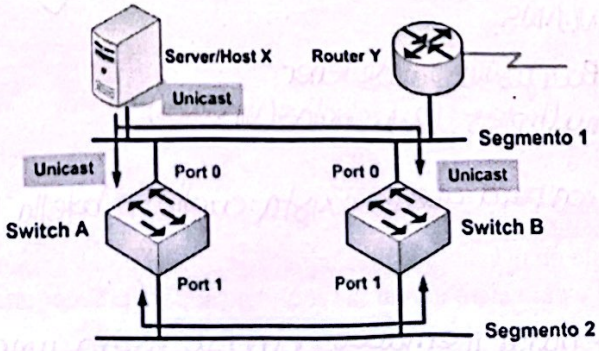
Tormenta de Broadcast: Host X envía un frame broadcast, los switches lo difunden de manera indefinida.



Transmisión Múltiple: Host X envia un frame unicast al router Y, la dirección MAC del router Y no ha sido aprendida por los switch, Router Y recibirá dos copias del mismo frame.



Inestabilidad: Host X envía un frame unicast al router Y, la dirección MAC del router no ha sido aprendida por los otros switches, switches A y B aprenden la dirección del host X por el puerto 0, el frame al router Y es inundado, switches A y B aprenden incorrectamente la dirección MAC de host X en el puerto 1.



La solución a esto son los **Spanning Tree T** de un grafo no dirigido G es un subgrafo que es un árbol que incluye todos los vértices de G, con el mínimo número posible de los enlaces. Impide la existencia de ciclos.

Spanning Tree Protocol

- Protocolo de red que garantiza topologías sin bucles dentro de una LAN Ethernet.
- Permite incluir redundancia a la topología, por sí una conexión falla.
- Crea una topología de árbol, a partir de una red de malla, deshabilitando enlaces, dejando un camino único entre 2 nodos de la red.
- Los switches y bridges que están corriendo el algoritmo STP intercambian mensajes de configuración Bridge Protocol Data Unit (BPDU).

Convergencia: tiempo que tarda la red en elegir un switch que cumpla la función de Root Bridge, además de definir los Root Ports y los Designated Ports.

STP introduce 5 estados de puertos:

1. **Bloqueado (blocking):** el puerto está no designado y no participa en el envío de frames.
2. **Escucha (listening):** el puerto se prepara para transmitir ya que STP ha determinado que puede participar.
3. **Aprende (learning):** el puerto se prepara para el envío y comienza a llenar la tabla de direcciones MAC.
4. **Reenvía (forwarding)**: el puerto envía y recibe frames.
5. **Deshabilitado (disable):** el puerto no participa en STP. Este estado se establece cuando el puerto está administrativamente deshabilitado.

Step 1 - Root Bridge Selection

Es el primer paso del proceso de convergencia. Se debe elegir un punto o nodo central para la topología STP (Root Bridge). Este es elegido basado en su Bridge ID(compuesto por 16-bit Bridge priority y 48-bit MAC address)

El número de prioridad por defecto es 32768, el switch o bridge que tiene el número de prioridad más bajo gana (es el Root Bridge). Si hay más de un switch con igual prioridad, se usa la dirección MAC más baja para elegir el root bridge.

Step 2 - Root Port Identification

El root port de cada switch es el puerto que tiene la ruta con el mínimo costo hacia el Root Bridge. Cada switch sólo puede tener un root port, el Root Bridge no puede tener un root port. El costo de la ruta es costo acumulado del camino hacia el Root Bridge y está basado en el ancho de banda de los enlaces (mayor ancho de banda, menor costo).

Step 3 - Designated Port Identification

Por cada segmento de red se debe identificar un único puerto designado. Si hay dos puertos designados se producirá un ciclo y uno de los puertos deberá ser puesto en estado bloqueado. Para la elección del puerto designado se usa el mismo procedimiento que para elegir el Root Port.

1.3 Capa de Red

El protocolo IP pretende resolver el problema de conectar diversas redes locales, que además pueden ser de diversos tipos. A este concepto se le conoce como internet working.

No hay garantías, no es confiable → TCP/IP

Cada datagrama contiene suficiente información para permitir que la red se encargue de hacerlo llegar a destino independientemente, pero este servicio no es confiable, ya que si algo anda mal y el datagrama se pierde, corrompe, se despacha a otro lugar y cualquier otra cosa, la red no hace nada para corregirlo. → pero abarata costos

En cuanto a la relación con la capa 2, la IP funciona independiente del medio de comunicación y la capa de enlace de datos se encarga de prepararlo para su transmisión en la red.

Maximum Transmission Unit (MTU):

Estructura Datagrama IP

Identification: contiene el número del datagrama el cual identifica el fragmento para su reconstrucción.

No.	Time	Source	Destination	Protocol	Length	Info
667…	0.000000000	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=1/256,
667…	0.195178687	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=2/512,
667…	0.203173492	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=3/768,
667…	0.202983697	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=4/1024,
667…	0.198656612	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=5/1280,
667…	0.203714186	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=6/1536,
667…	0.201265312	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=7/1792,
667…	0.196083432	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=8/2048,
667…	0.297671552	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=9/2304,
668…	0.414752346	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=10/2560,

```
▸ Frame 66764: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp2s0, id 0
▸ Ethernet II, Src: ArrisGro_48:8a:88 (18:35:d1:48:8a:88), Dst: IntelCor_68:a6:eb (18:1d:ea:68:a6:eb)
▾ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.24
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x7bdf (31711)
```

Ventajas de segmentar

- **Eficiencia**
  - Un segmento IP requiere estar en el mismo dominio de broadcast.
  - Si tenemos muchos nodos en el mismo segmento, aumentamos las posibilidades de colisión y disminuimos el rendimiento.
- **Seguridad**
  - Podemos aplicar reglas o filtros de tráfico entre segmentos IP.
- **Administración**
  - Definimos segmentos IP en base a funciones, que requieren tipos de servicio diferentes.
  - Cada red IP puede recibir un tratamiento diferente, distintos servicios, etc.

→ 4 octetos = binario / decimal

octeto 1	octeto 2	octeto 3	octeto 4
11000000	00000101	00100010	00001011
192	5	34	11

IPs para una LAN

IANA define un bloque de IPs reservados que permiten a las organizaciones su utilización en redes privadas sin solicitud alguna. A estos bloques reservados se les conoce como direcciones privadas, pues está prohibido su uso en redes públicas como Internet.

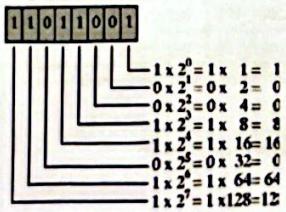
- **Direcciones IP públicas:** Son visibles en todo Internet. Un nodo con una IP pública es accesible (visible) desde cualquier otro nodo conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública. → NO SE NECESITO DENTRO DE UNA RED LOCAL.
- **Direcciones IP privadas (reservadas):** Son visibles únicamente por otros nodos de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los nodos con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy) que tenga una IP pública.

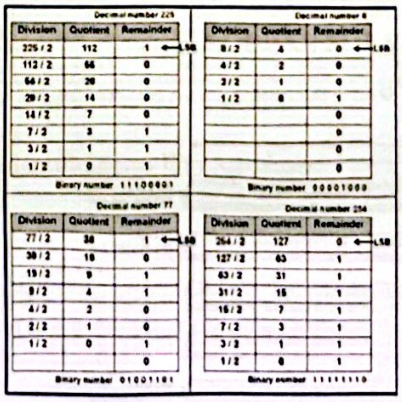
- Clase A: 127.0.0.0 /8
- Clase B 128.0.0.0 /16
- Clase C 192.0.0.0/24

240.0.0.0 – 255.255.255.254	Reservado (clase E)
10.0.0.0	Privado clase A → /8
172.16.0.0 – 172.31.0.0	Privado clase B
192.168.0.0 – 192.168.255.0	Privado clase C

NAT: Network Address Translation → permite al dispositivo con una dirección IPV4 privada acceda a recursos fuera de su red privada, como los que encuentran en Internet.

Es la solución para la escasez de IPs, ISP asigna una IP para cada hogar/empresa. Dentro de la red, cada equipo tiene un IP único perteneciente a la red privada y para lograr comunicar con el resto de las redes, se realiza un proceso de traducción entre las IP privadas a la IP pública.





/8 → 1.0.0.0

Máscara de red: compuesta por una secuencia de 1s y 0s, permite conocer rangos de IPs. Al hacer un AND con una dirección IP de una red, permite obtener la IP inicial y final de la red.

Prefijo: Formado por IP/Mask

- Tamaño del prefijo no puede ser calculado solo con la IP
- IP + tamaño: 131.108.0.0 / 16, se debe enviar el tamaño igualmente
- Subnet Mask → 16 representa número de 1's incluidos en la máscara
- IP AND Mask → Parte que representa la red

Ventajas del esquema jerárquico

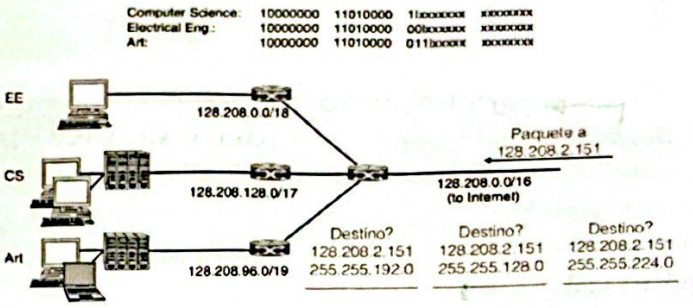
- Solo utiliza la parte de red para "rutear" paquetes disminuyendo los tamaños de las tablas de los routers.
- Cuando llega a la red de destino, se utiliza la información del host para entregar el paquete.
- Tamaño de las tablas son del orden de 300.000 prefijos, con Internet actual, lo cual le permite escalar.

Desventajas del esquema jerárquico

- Uso ineficiente de las IPs a menos que haya una cuidadosa administración.
- Si se asignan bloques de direcciones muy grandes pueden quedar muchos IPs sin uso.
- Con el crecimiento de internet las IPs son un bien escaso.

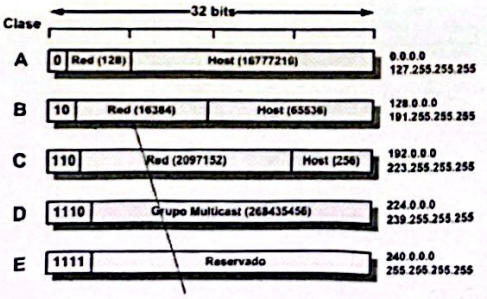
Subredes: segmentos de nodos de la red, cada segmento de la red está identificado por un prefijo de red y todos los host de dicho segmento poseen el mismo prefijo.

Ejemplo de subred



CLASES DE IPS Y SUS RANGOS

Clases de IPs



CIDR (Classless Inter Domain Routing): se utiliza para combinar rutas y reducir los datos de enrutamiento transportados por los routers centrales.

Clase	Prefijo CIDR	Rango	
A	10.0.0.0/8	10.0.0.0 - 10.255.255.255	1 dirección clase A
B	172.16.0.0/12	172.16.0.0 - 172.31.255.255	16 direcciones clase B
C	192.168.0.0/16	192.168.0.0 - 192.168.255.255	256 direcciones clase C

Subnet Mask

255	/32	0	11111111
254	/31	1	11111110
252	/30	2	11111100
248	/29	3	11111000
240	/28	4	11110000
224	/27	5	11100000
192	/26	6	11000000
128	/25	7	10000000

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.

$2^7\ 2^6\ 2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$
128 64 32 16 8 4 2 1

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.

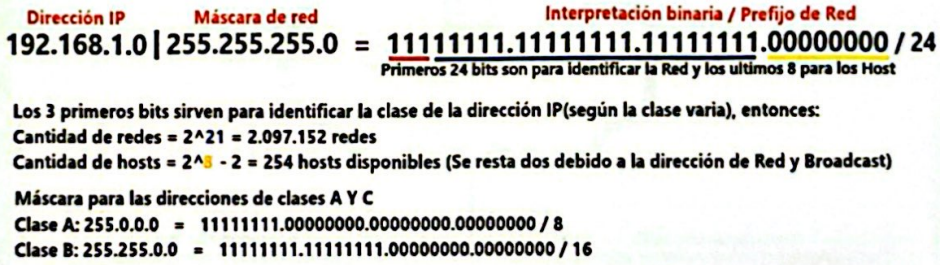


Figura 8: Ejemplo de una mascara de red asociada a una dirección IP en particular.

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."

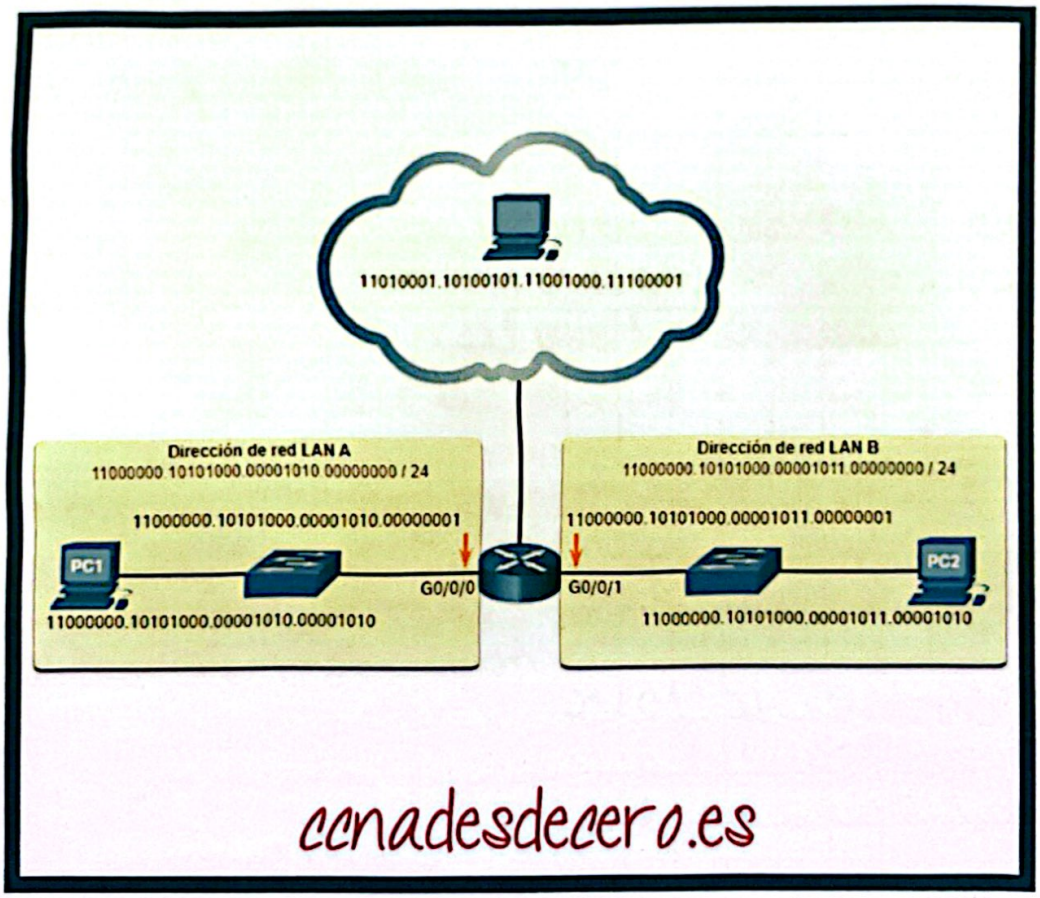


Figura 10: Direcciones binarias e IPv4 (Fuente: https://ccnadesdecero.es/)

1.4. División por Mascara de Red FIJA

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

- En enlaces PtP no usar ni de red, ni de broadcast.

VLSM de 190.196.72.0/23 ⟶ 512 IPs disponibles

1° paso: ordenar de mayor a menor la cantidad de host.

40	32	26	20	12	10	8	1	
/26	/26	/27	/27	/28	/28	/28	/30	máscara
64	64	32	32	30	16	16	2	total direcciones

- **Para 40 host**

IP de red: 190.196.72.0/26

rango IPs: 190.196.72.1 - 190.196.72.62

broadcast: 190.196.72.63

- **Para 32 host**

IP de red: 190.196.72.64/26

rango IPs: 190.196.72.65 - 190.196.72.126

broadcast: 190.196.72.127

- **Para 26 host**

IP de red: 190.196.72.128/27

rango IPs: 190.196.72.129 - 190.196.72.158

broadcast: 190.196.72.159

- **Para 20 host**

IP de red: 190.196.72.160/27

rango IPs: 190.196.72.161 - 190.196.72.190

broadcast: 190.196.72.191

- **Para 12 host**

IP de red: 190.196.72.192/28

rango IP: 190.196.72.193 - 190.196.72.206

broadcast: 190.196.72.207

- **Para 10 host**

IP de red: 190.196.72.208/28

rango IP: 190.196.72.209 - 190.196.72.222

broadcast: 190.196.72.223

- **Para 8 host**

IP de red: 190.196.72.224/28

rango IP: 190.196.72.225 - 190.196.72.238

broadcast: 190.196.72.239

- **Para 1 host**

IP de red: 190.196.72.240/30

rango IP: 190.196.72.241 - 190.196.72.242

broadcast: 190.196.72.243

- Los routers al igual que los switch tienen tablas con la ubicación del host destino, pero a diferencia de los switch, el router almacena la dirección de subred de cada destino. Por lo tanto, cuando un router recibe un paquete, inspecciona la dirección IP de destino y revisa a que subred pertenece y busca en su tabla por cual interfaz esta conectada la subred de destino.

Ej: ¿Como sabe el router a que subred de destino pertenece una dirección IP?

- mascara de subred
- IP origen: 200.1.20.45 , IP destino: 150.15.8.99
- cuando el paquete llega al router B, este analiza su tabla de ruteo

entonces teniendo.

destino: 150.15.8.99.
mascara: 255.255.255.0.

Pasando a binario

destino: 10010110.00001111.00001000.01100011 } operación AND
mascara: 11111111.11111111.11111111.00000000 } 0-0=0 / 0-1=0 / 1-0=0 / 1-1=
10010110.00001111.00001000.00000000

red destino: 150.15.8.0

Ej: ¿Calcule la subred a la que pertenece 215.45.87.12/20?

Primero: dirección IP: 215.45.87.12
mascara: /20 → 255.255.240.0.

Luego pasamos ambas a binarias.

dirección. 11010111.00101101.01010111.00001100
mascara: 11111111.11111111.11110000.00000000

Para calcular la dirección de red realizamos un AND entre ambas. obteniendo como resultado.

= 11010111.00101101.01010000.00000000
subred = 215.45.80.0

Técnicas de división de red (subnetting):

→ Nace de los siguientes problemas, imposibilidad de conmutar paquetes entre routers basado en la dirección IP de destino (1); el tamaño de una red puede ser demasiado grande para formar un solo dominio de broadcast. (2)

Problema 1:

conmutar paquetes a través de los routers a través de routers usando la dirección IP de destino es ineficiente, ya que no se puede tener una tabla de rutas donde estén las direcciones IP de todos los host del mundo, para esto se necesita realizar una agrupación de los host basado en las direcciones IP de cada uno de ellos, esta agrupación esta basada en un concepto de subred:

Subred: grupo de host que comparten el mismo dominio de broadcast, la misma dirección de subred, el mismo default gateway, están conectados por uno o más switch, pero dos host en la misma subred, no pueden estar separados por un router.

lógicamente, son todas las direcciones IP que comparten el mismo identificador de red.

Problema 2:

La división por clase permite agrupar las direcciones IP en subredes y soluciona el problema 1. El problema ahora es que cada subred, al menos la clase A y B, son demasiado grandes para ser administradas, Para solucionar esto, se divide una red en redes más pequeñas.

división por mascara de red fija:

Por obtener n subredes se deben reservar $(\log_2(n)$ de la porción de host ID.

Ej: si se tiene la dirección clase C 201.50.41.0, se solicita que esta red sea dividida en 4 subredes.

$\log_2(4)$ es igual a 2 bits. Por lo tanto, se deben tomar 2 bits de la porción de hosts

Por ende, la parte de host, ya no tiene 8 sino que 6 bits

La capacidad de cada subred es de 62 hosts:

$$n_{subredes} = 2^{bits\ de\ subred} = 2^2 = \text{subredes } 4$$

$$n_{host\ por\ subred} = 2^{bits\ de\ subred} - 2 = 2^6 - 2 = 62 \text{ host por subred.}$$

división por mascara de red variable: VLSM:

La longitud de la mascara de subred varía según la cantidad de bits que se toman prestado para una subred especifica, es decir, permite dividir un espacio de red en partes desiguales.

- Las formulas para calcular la cantidad de host por subred y la cantidad de subredes que se crean son validos para VLSM. La diferencia es que la division de subredes se puede hacer varias veces.

Ej: se tienen 5 clientes, 3 tienen 60 hosts y 2 tienen 25 hosts.
C1: 60 hosts ; C2: 60 hosts ; C3: 60 hosts ; C4 = 25 hosts ; C5: 25 hosts.
usando C: 201.50.41.0/24 ¿Como dividiria la red?
R: la C: 201.50.41.0/24 tiene 256 direcciones disp / 254 utilizables para host.
Por ende para 60 hosts, necesitamos al menos 64 direcciones / 64 utiles, por ende usamos la mascara /26. → 255.255.255.[redacted].192
Para 25 host, usamos mascara /27 que tiene 32 direcciones / 30 disponibles → 255.255.255.224.
Luego se asignan los rangos de direcciones para cada cliente

- Cliente 1: 60 hosts.
  subred: 201.50.41.0/26 / tamaño necesario: 64 direcciones.
  rango IPS: 201.50.41.0 - 201.50.41.63 → 64 direcciones, una menos que la normal
  (sumar 1 al 1° ; restar uno al mayor)
  host utilizables: 201.50.41.1 a 201.50.41.62
  (inicia en la sgte dirección del cliente 1)

- Cliente 2: 60 host. (aumentamos en 64 por las direcciones)
  subred: 201.50.41.64/26.
  rango IPS: 201.50.41.64 - 201.50.41.127 → 63 direcciones, una menos que la normal.
  host utilizables: 201.50.41.65 - 201.50.41.126
  (inicia en la sgte dirección del cliente 2)

- Cliente 3: 60 host.
  subred: 201.50.41.128/26.
  rango IPS: 201.50.41.128 - 201.50.41.191 → 63 direcciones.
  host utilizables: 201.50.41.129 - 201.50.41.190. → +1 / -1

- Cliente 4: 25 host (parte de la siguiente) 32 direcciones / 27.
  subred: 201.50.41.192/27.
  rango IP: 201.50.41.192 - 201.50.41.223 → 31 direcciones
  host utilizables: 201.50.41.193 - 201.50.41.222

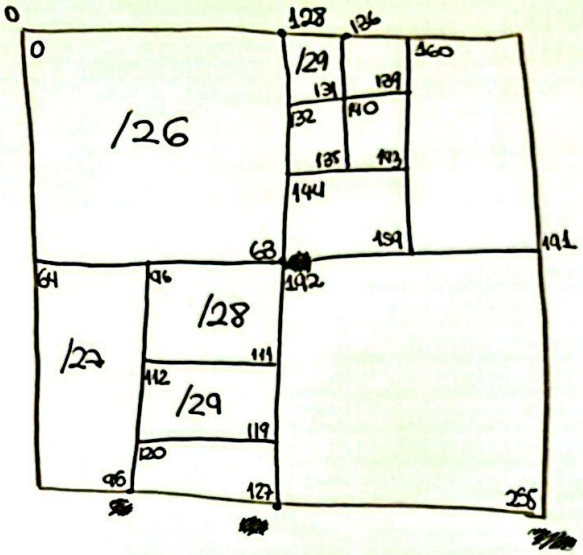
- Cliente 5: (parte del siguiente.)
  subred: 201.50.41.224/27
  rango IP: 201.50.41.224 - 201.50.41.255 / utilizables: 201.50.41.225 - 201.50.41.254.

- Para calcular la dirección broadcast.
  → conocer la dirección de red y la máscara
  (dirección de red, se obtiene aplicando un AND entre la IP de unitio y la máscara de subred)
  → Para calcular la dirección de broadcast aplica un OR entre la dirección de red y el complemento de la mascadra de subred.

Ej: red: 201.90.41.0/26
máscara: /26 → 255.255.255.192
↳ binario → 11111111.11111111.11111111.11000000
red (binaria) → 11001001.00110010.00101001.00000000
complemento máscara (invertir los bits / cambiar 1 a 0 y 0 a 1)
complemento máscara: 00000000.00000000.00000000.00111111
Por ende se hace un OR
OR → 11001001.00110010.00101001.00000000
00000000.00000000.00000000.00111111
11001001.00110010.00101001.00111111
resultado: 201.90.41.63

PROTOCOLO DHCP: protocolo de configuración dinamica de host y funcionamiento
→ Protocolo que proporciona direccionamiento IP automatico y otra información a los clientes: dirección IP, mascara de subred, dirección de puerta de enlace predeterminada y dirección del servidor DNS
→ Utiliza 3 metodos:
1. Asignación manual: asignación una dirección IP a una maquina determinada.
2. Asignación automatica: asigna automaticamente una dirección IPV4 estatica de forma permanente a un dispositivo.
3. Asignacion dinamica: asigna una dirección IPV4 de un grupo de direcciones durante un periodo de tiempo limitado elegido por el servidor o hasta que el cliente ya no necesite la dirección.

PASO A PASO TECNICA CUADRO VLSM:



se escogen de izquierda a derecha primero celda cero y la de 255 como ultima.

Se escoge de Arriba hacia abajo

- particiones se interalan entre vertical y horizontal, Siempre se parte con la vertical.
- subredes ordenadas.

Ej: 30, 16, 32, 54, 4 → 54, 32, 30, 16, 4

ordenarlas de mayor a menor. obligatorio de arriba a abajo, de izquierda a derecha de mayor a menor.

VLSM (Variable Length Subnet Masking):
• Lo que tradicionalmente se utiliza es un tamaño de máscara variable.
• Máscara variable permite adaptarse a las necesidades y reducir el desperdicio de IPs.
• La parte red y la parte host no son iguales en todas las subredes.
• Aunque las subredes pueden tener diferente tamaño no pueden solaparse

Permite dividir una red en subredes de diferentes tamaños según las necesidades específicas de cada segmento.

Cómo funciona VLSM
1.Determinar la red principal: Empieza con una red base definida por su dirección IP y máscara (por ejemplo, `192.168.0.0/24`).
2. Analizar las necesidades de cada subred: Calcula cuántos hosts requiere cada subred (acercando a la potencia de dos más cercana la cantidad de host entregados).Recuerda que cada subred necesita al menos dos direcciones: una para la red y otra para broadcast.
3. Asignar máscaras de subred específicas:
- Usa máscaras más largas (más bits para la red, menos para hosts) para subredes con pocos hosts.
- Usa máscaras más cortas (menos bits para la red, más para hosts) para subredes más grandes.

4. Dividir y asignar bloques: Divide la red principal en bloques más pequeños siguiendo las necesidades y aplica la máscara adecuada. La división debe respetar los límites binarios.
5. Asegurarse de evitar solapamientos: Las subredes deben ser disjuntas, es decir, no deben compartir direcciones IP.

Ejemplo de VLSM 1

Supongamos que tienes la red `192.168.1.0/24` y necesitas crear subredes para los siguientes requisitos:

- Subred A: 50 hosts.
- Subred B: 20 hosts.
- Subred C: 10 hosts.

Paso 1: Calcular el tamaño de las subredes

1. Subred A:
    - Se necesitan al menos 50 direcciones + 2 (red y broadcast).
    - El bloque más cercano en potencia de 2 es 64, lo que requiere una máscara `/26` (255.255.255.192).
2. Subred B:
    - Se necesitan al menos 20 direcciones + 2.
    - El bloque más cercano es 32, lo que requiere una máscara `/27` (255.255.255.224).

3. Subred C:
    - Se necesitan al menos 10 direcciones + 2.
    - El bloque más cercano es 16, lo que requiere una máscara /28 (255.255.255.240).

Paso 2: Asignar las subredes

1. Subred A: 192.168.1.0/26 (rango: 192.168.1.0 - 192.168.1.63).
2. Subred B: 192.168.1.64/27 (rango: 192.168.1.64 - 192.168.1.95).
3. Subred C: 192.168.1.96/28 (rango: 192.168.1.96 - 192.168.1.111).

Paso 3: Espacio sobrante

Después de asignar estas subredes, quedan direcciones disponibles en la red principal (de 192.168.1.112 en adelante) para futuras subredes.

Ejemplo de VLSM 2

Se tiene una red clase C cuya dirección base es **192.168.10.0/24**. Se quiere dividir dicha red en 4 subredes.

- Subred A con 50 host
- subred B con 20 host
- subred C con 10 host
- subred D con 10 host.

Determine una manera de asignar direcciones utilizando VLSM. Identifique número de hosts, rango de IPs disponibles, dirección de broadcast, y máscara de cada subred.

RESPUESTA:

RED:#	Host (2^n)	n	Red	Mascara	Rango Util	Broadcast
A: 50	64	6	192.168.10.0	255.255.255.192 /26	192.168.10.1 - 192.168.10.62	192.168.10.63
B: 20	32	5	192.168.10.64	255.255.255.224 /27	192.168.10.65 - 192.168.10.94	192.168.10.95
C:10	16	4	192.168.10.96	255.255.255.240 /28	192.168.10.97 - 192.168.10.110	192.168.10.111
D:10	16	4	192.168.10.112	255.255.255.240 /28	192.168.10.113 - 192.168.10.126	192.168.10.127

Agregación de dominios

Proceso consiste en encontrar el máximo prefijo común entre las redes.

Ventajas:

- Hace más pequeñas las tablas de enrutamiento, logrando que las búsquedas en la tabla sean más rápidas.
- Vuelve más legible la información y oculta información específica acerca de las redes agregadas.
- Los protocolos de enrutamiento dinámico pueden evitar consumir ancho de banda para las actualizaciones.

→ Busca de buscar un camino entre todos los posibles nodos en una red de paquetes cuyas topologías poseen una gran conectividad, es efectuado por los routers.

Enrutamiento

Tipos de enrutamiento

	Enrutamiento dinámico	Enrutamiento estático
Complejidad de la configuración	Por lo general es independiente del tamaño de la red	Se incrementa con el tamaño de la red
Conocimientos requeridos del administrador	Se requiere de un conocimiento avanzado	No se requieren conocimientos adicionales
Cambios de topología	Se adapta automáticamente a los cambios de topología	Se requiere la intervención del administrador
Escalamiento	Adecuado para las topologías simples y complejas	Adecuada para topologías simples
Seguridad	Es menos seguro	Más segura
Uso de recursos	Utiliza CPU, memoria y ancho de banda de enlace	No se requieren recursos adicionales
Capacidad de predicción	La ruta depende de la topología actual	La ruta hacia el destino es siempre la misma

Protocolos para caminos dinámicos

	Distance Vector	Link State
Internos	RIP, RIPv2, EIGRP	OSPF, IS-IS
Externos	BGP	

→ el protocolo requiere que un router informe a sus vecinos de los cambios en la topología periódicamente y en algunos casos cuando se detecta un cambio en la topología de red.

Distance Vector

Cada nodo mantiene un arreglo que contiene las distancias a todos los otros nodos y se la comunica a todos sus vecinos. Inicialmente la tabla tiene la información para los vecinos directos y para los otros el valor es infinito. Utiliza Bellman-Ford para calcular las rutas.

El proceso necesario para que todos los nodos tengan una visión consistente de la red, se llama convergencia.

Se envían actualizaciones a los vecinos en dos circunstancias: periódicamente a intervalos regulares y cuando se recibe una notificación de cambio desde un vecino.

→ Routing Information Protocol:

RIP cuenta los saltos efectuados hasta llegar al destino mientras que IGRP utiliza otra información como el retardo y el ancho de banda. Este proceso se conoce también como "enrutamiento por rumor" ya que los nodos utilizan la información de sus vecinos y no pueden comprobar a ciencia cierta si ésta es verdadera o no

→ se basa en calcular la dirección y la distancia hasta cualquier enlace de red.

Situación inicial

Destination	Cost	NextHop
B	1	B
C	1	C
D	INF	--
E	1	E
F	1	F
G	INF	--

Information Stored at Node	Distance to Reach Nodes						
	A	B	C	D	E	F	G
A	0	1	1	INF	1	1	INF
B	1	0	1	INF	INF	INF	INF
C	1	1	0	1	INF	INF	INF
D	INF	INF	1	0	INF	INF	1
E	1	INF	INF	INF	0	INF	INF
F	1	INF	INF	INF	INF	0	1
G	INF	INF	INF	1	INF	1	0

Situación final

Destination	Cost	NextHop
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

Information Stored at Node	Distance to Reach Nodes						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Un problema de Distance Vector se denomina count-to-infinity. → cuenta infinita, si falla la conexión entre algun link.

Una primera aproximación es definir INF=16, lo que reduce el tiempo de convergencia.

→ solucona count-to-infinity.

Éstas **técnicas afectan la velocidad de convergencia del protocolo, y por lo mismo no se usan en redes grandes.**

- Otra técnica llamada split horizon, consiste en no enviar las actualizaciones de ruta al vecino del cual se aprendieron.
- Otra técnica más fuerte es split horizon with poison reverse, que consiste en que un nodo sí le envía la actualización aprendida al nodo de quién la aprendió, pero con distancia INF.

RIPv2 (RFC 1723)

Para elegir una ruta, compara las métricas (al recibir una tabla, le suma 1 a todas sus métricas, puesto que las redes están a un router más de distancia) y se queda con la más pequeña. Si existe igualdad se queda con la ruta antigua.

Actualización de tabla:

RIP se actualiza cada 30 segundos utilizando el protocolo UDP y el puerto 520, enviando la tabla de enrutamiento completa a sus vecinos. Las rutas tienen un TTL (tiempo de vida) de 180 segundos, es decir que si en 6 intercambios la ruta no aparece activa, esta es borrada de la tabla de enrutamiento.

Distancia Administrativa:

RIP es un protocolo de enrutamiento con una distancia administrativa de 120 (cuanto menor sea la distancia administrativa el protocolo se considera más confiable) y utiliza un algoritmo de vector distancia utilizando como métrica el número de saltos.

Enrutamiento por estado de enlace:

El algoritmo de Dijkstra permite encontrar la ruta más corta entre dos nodos en un grafo. La ruta más corta no se refiere a la ruta con menos cantidad de saltos.

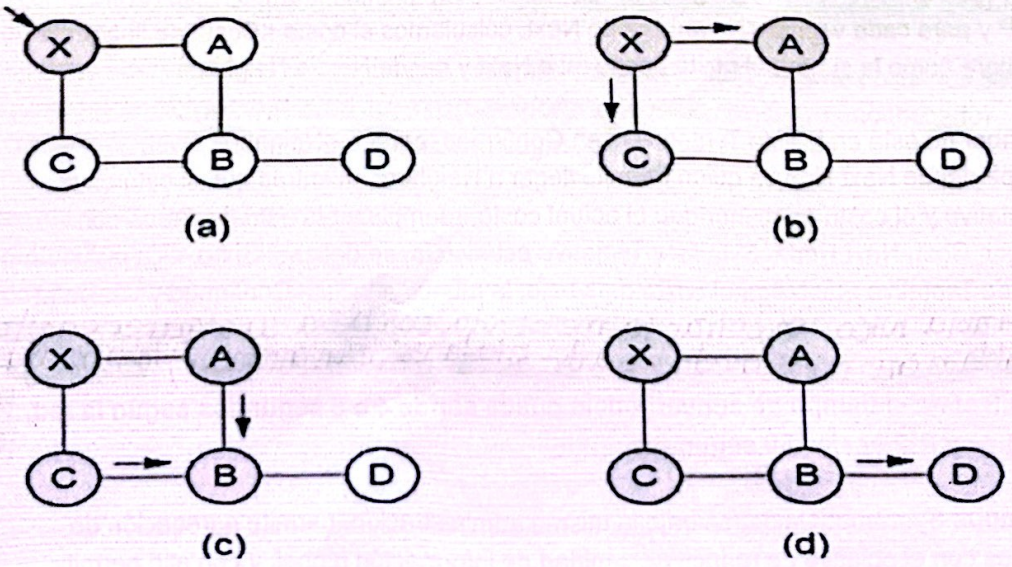
Link State

Asume que cada nodo es capaz de detectar el "estado" del enlace con sus vecinos. Cada nodo sabe como llegar a sus vecinos directos.

Toda esa información es diseminada por toda la red, con el de que cada nodo es capaz de tener una visión completa de la red y con ello poder calcular el camino más corto a cada destino.

Este tipo de protocolo se basa en comunicar a todos los miembros la situación de los enlaces, haciendo un flooding de la red, que quiere decir que cada nodo le entrega su información a todos sus vecinos y así sucesivamente.

Proceso de flooding



- **Contenido de LSP (Link-State Packets)**

- ID del nodo que creó el LSP.
- Una lista de los vecinos directamente conectados a ese nodo con el costo del enlace a cada uno.
- Un número de secuencia.
- Un TTL para el paquete.
- Los dos primeros campos se usan para calcular las rutas y los dos últimos para asegurar el proceso de flooding. La confiabilidad del proceso incluye asegurarse que todos los nodos tienen la información actualizada.

- **Proceso LSP**

Si un nodo X recibe una copia de un LSP de parte de un nodo Y, éste verifica si ya tiene información almacenada proveniente de Y, sino tiene, lo almacena y si tiene compara el número de secuencia.
Si el nuevo LSP tiene un número mayor, lo considera más nuevo y actualiza su tabla con su información, además de enviarlo a todos sus vecinos, menos aquel que nos lo envió (split-horizon), si la secuencia es menor o igual, se descarta.

- **Difusión de LSP**

Se generan en dos circunstancias:

- A intervalos regulares de tiempo. Estos intervalos son amplios (algunas horas) para reducir el sobrecosto.
- Al producirse un cambio en la topología. Para detectar éstos el protocolo envía mensajes "Hello" regularmente. Si no se ha escuchado un "Hello" desde un vecino en cierto tiempo, se declara el enlace como "fuera de servicio" y se genera un LSP para anunciarlo.

Open Shortest Path First (OSPF) → uso el ancho de banda del enlace como el costo: $\frac{10^8}{BW}$

Se mantienen dos listas: Tentative y Confirmed, donde cada entrada es de la forma <Destination, Cost, NextHop>, se inicializa Confirmed con una entrada para mi host, con costo 0. Para el nodo recién agregado la lista Confirmed, que llamaremos Next, revisaremos sus LSP y para cada vecino <Neighbor> de Next, calculamos el costo <Cost> de llegar a <Neighbor> como la suma del costo desde mi a Next y desde Next a Neighbor.

Si Neighbor no está en la lista Tentative ni en Confirmed, agregó <Neighbor, Cost, NextHop> dónde Next Hop es quien permite llegar a Neighbor, mientras que si está en la lista Tentative y el costo es menor que el actual costo, reemplazar la actual entrada con <Neighbor, Cost, Next Hop>. Si la lista Tentative está vacía, se detiene. Si no, elijo la entrada de Tentative que tenga el costo más bajo, la muevo a la lista Confirmed y vuelvo al paso 2.

tabla ruteo: encontrar la mejor ruta posible a cualquier enrutador → tabla vecina: nodos conectados a dos interfaces de un enrutador; tabla topología: rutas posibles a diferentes enrutadores.

En un link-state el tiempo de convergencia puede ser de 4 o 5 segundos según la red, en cambio en RIP es de 180 segundos

Autonomous Systems: Unidades bajo la misma administración, permite agregación de direcciones con el objetivo de reducir la cantidad de información global, y con ello permitir una mejor escalabilidad. Dentro de los AS se pueden usar protocolos internos (IGP) o externos, pero entre AS, se usan protocolos externos (EGP).

- protocolo de enrutamiento de estado por enlace, tipo de protocolo de puerta de enlace interna, diseñado para escalar y admitir redes mas extensas.
- utiliza el paquete de saludo o el temporizador keep-alive para mantener los estados de los routers adyacentes.

→ cada dominio es un dominio administrativo que opera con políticas uniformes de ruteo, independiente de otros dominios; (SA)
SA: sistema autónomo es un grupo de redes de direcciones IP que son gestionados por uno o más operadores de red que poseen una clara y única política de ruteo, tienen un número asociado que se usa como identificador en el intercambio de info extremo a extremo.

Exterior Gateway Protocol
Se basa en el sondeo periódico empleando intercambios de mensajes "Hello/I Hear You", para monitorizar la accesibilidad de los vecinos y para sondear si hay solicitudes de actualización. Trabaja con redes de diferentes sistemas autónomos, publicando sus propias redes y determinando a través de qué otro sistema autónomo se puede llegar a un tercero. Además, tiene varias funciones de filtrado para permitir informar o no sobre las rutas que tiene y a que router externo AS lo dice.

Internal Gateway Protocol
Los IGP son protocolos de enrutamiento que pertenecen a un solo AS, y es administrado por una sola entidad, ejemplos de estos son el RIP, RIPv2, OSPF, IGRP y EIGRP (Cisco). Se utilizan en routers internos y los EGP se utilizan en routers fronterizos y externos.

1.4 Capa de Transporte

Para evitar los problemas de los segmentos como recordar PDU de capa 4, pérdidas de segmentos por rutas congestionadas o enlaces caídos, segmentos llegan fuera de orden y segmentos se duplican por retardos que obligan a la retransmisión.

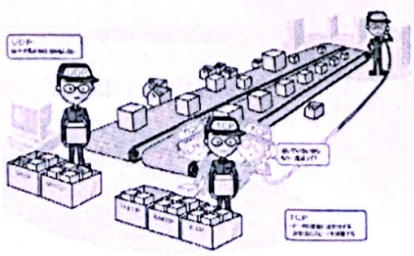
Se emplea la segmentación la cual re-ensambla segmentos para pasarlos a la aplicación de manera coherente, esto es posible gracias a la enumeración y secuenciación de los segmentos.

Aplicaciones
Identificar las aplicaciones
- Asegurar que cada aplicación en ejecución reciba los datos correctamente, para esto se utilizan puertos específicos para cada aplicación.

Maximum Segment Size: se define en la conexión TCP y permite saber el tamaño máximo de los paquetes a segmentar.

Multiplexing
La segmentación de los datos permite que múltiples conexiones de diferentes usuarios sean multiplexadas en la misma red. La capa de transporte agrega un header (o encabezado) que contiene información para identificar cada segmento de datos.

Protocolo de la capa de transporte
Los protocolos **UDP (User Datagram Protocol)** y **TCP (Transmission Control Protocol)** son dos protocolos de la capa de transporte del modelo TCP/IP que permiten la transmisión de datos entre dispositivos en una red.



Header TCP
TCP es un protocolo stateful, vale decir mantiene información acerca del estado de la comunicación, lo enviado y lo recibido.
El encabezado TCP (header) es de 20 bytes y encapsula la información de la capa de aplicación

Header UDP
UDP es un protocolo stateless, vale decir ni el receptor ni el origen deben llevar un seguimiento del estado de la comunicación. Si se requiere de confiabilidad debe ser manejada por la aplicación.Los paquetes enviados por UDP son conocidos bajo el nombre de datagramas. UDP tiene una cabecera de 8 bytes.

Puertos
Para poder realizar varias conexiones de forma simultánea, la IP tiene asignados 65536 puntos de salida y entrada de datos, algunos de ellos asignados por IANA (RFC 1700).

Tabla de ruteo:

Destino de red	mascara de red	Puerta de enlace (por donde salir)	Interfaz	metrica

→ en vínculo están en la misma LAN, no necesito rutear.

metrica: prioridad cosas específicas y luego secundarias.

→ elemento que contiene la información necesaria para dirigir paquetes de datos desde una red de origen hasta su destino final.

→ Es como una base de datos utilizada por los routers y dispositivos para determinar el camino de enviar datos.

→ cuenta con:
- destino de red: dirección IP a la que se quiere llegar.
- mascara de red: define el tamaño de la red de destino.
- puerta de enlace: dirección IP del siguiente salto, que puede ser otro router.
- interfaz: especifica que interfaz del router se debe usar para enviar el paquete.

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.

1.4. 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.

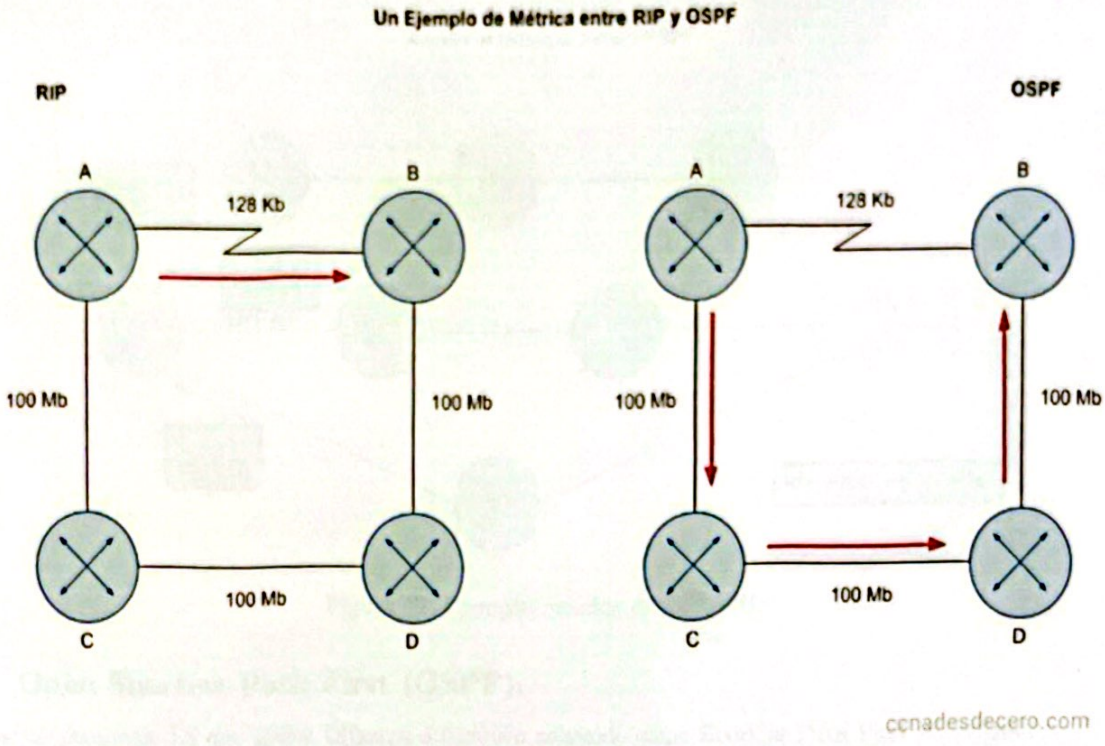


Figura 11: Ejemplo del Camino Más Óptimo, Más Corto o el Mejor Camino

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.

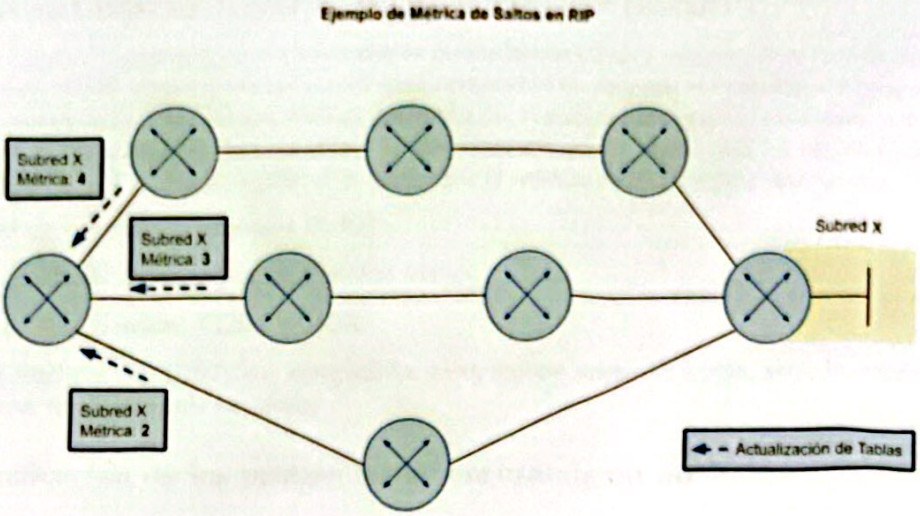


Figura 12: Ejemplo métrica de saltos RIP

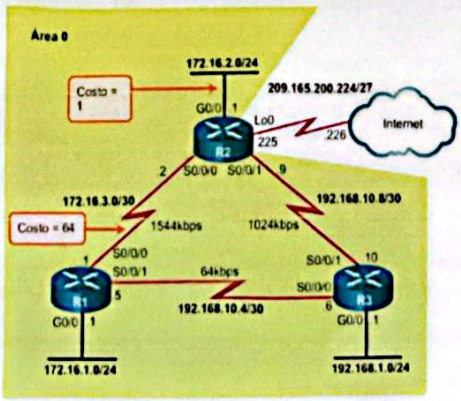
1.8. Open Shortest Path First (OSPF):

- 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

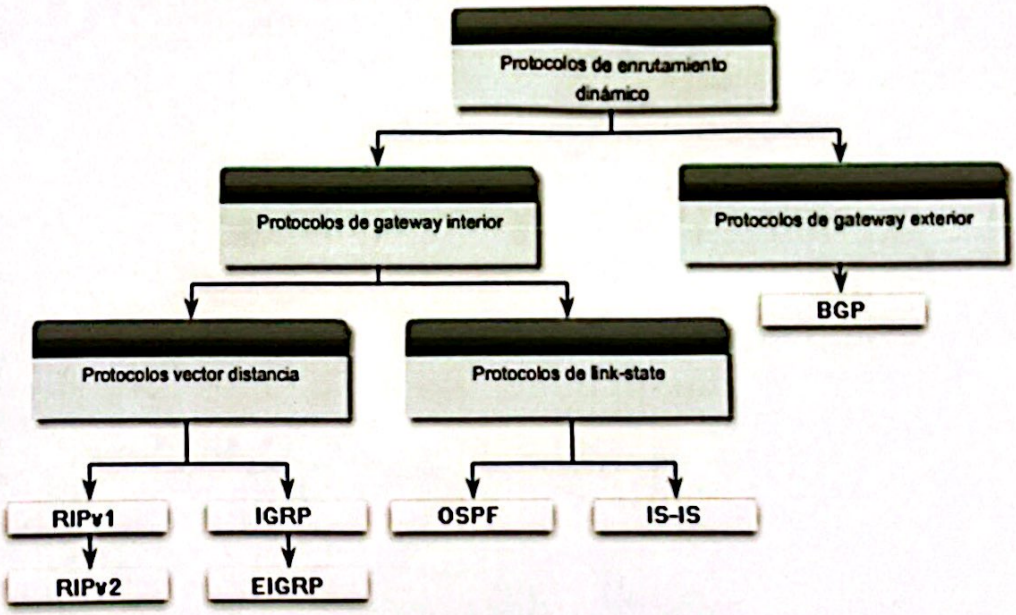


Figura 14: Fuente: Cisco System, Inc

	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