En este módulo se verá:

1. Elementos de Capa 2.
2. Funcionamiento del router.
3. HOPS.
4. Tabla de enrutamiento.
5. *Gateway*.
6. NAT.
7. Reenvío de puertos.
8. Interconectar redes aislada lógica y físicamente.
9. Establecer salidas a otras redes.
10. Determinar servicios internos accesibles desde la red pública.

Estándar Ethernet

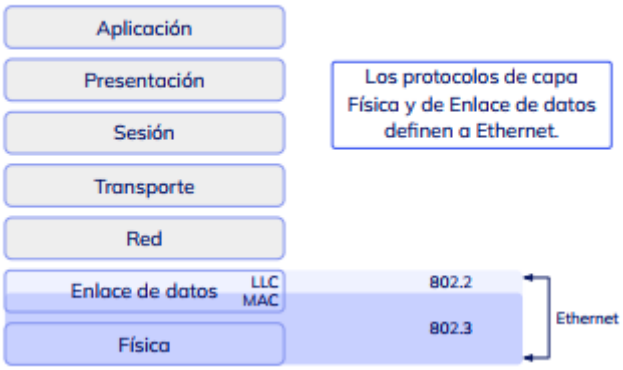
Ethernet es un **estándar de redes de área local** para computadoras, por sus siglas en español Acceso Múltiple con Escucha de Portadora y Detección de Colisiones (CSMA/CD).

Según el modelo OSI las capas:

Capa 3 Red: direccionamiento lógico.

Capa 2 Enlace de datos: direccionamiento físico (LLC y MAC).

Capa 1 Física: señalización y transporte por un medio físico.



El estándar Ethernet se ocupa de las capas 1 y 2.

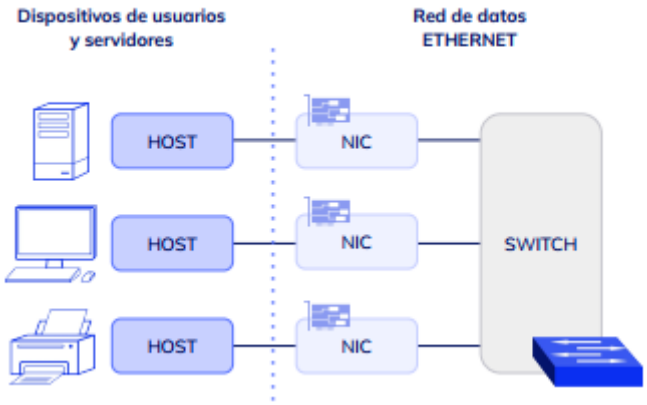
Todos los dispositivos que se usan en redes LAN en la actualidad se recuestan en esta tecnología:

Notebooks.

Smartphones.

Smart TVs.

Impresoras.



Aunque fue concebido para redes de área local, la evolución de las tecnologías utilizadas ha permitido su implementación en redes de mayor envergadura como redes MAN y WAN.

El estándar Ethernet define las tecnologías usadas a nivel físico descritas en el modelo OSI:

Cableado y medios de transporte.

Señalización (uso de pulsos eléctricos, pulsos lumínicos, etc.).

Formato de tramas.

Dispositivos de red.

Velocidad de transmisión.

Ethernet se tomó como base para la redacción del estándar internacional IEEE 802.3, siendo usualmente tomados como sinónimos.

Formato de la trama Ethernet

Los paquetes de datos son encapsulados en una unidad de datos denominada '**trama**' o '***frame***'.

Esta trama, como toda unidad de datos, está conformada por una cadena de bits, los cuales la interfaz de red vuelca al medio físico mediante un tipo de señalización. Ésta depende del tipo de medio, en el caso de medios de cobre la señalización es eléctrica, variaciones en el voltaje determinan la información: 1 y 0.

Ejemplo del formato de la trama ethernet

Estructura de la Payload en Ethernet y protocolos IP y TCP.

Preámbulo	Delimitador de inicio de trama	MAC de destino	MAC de origen	802.1Q Etiqueta (opcional)	Ethertype (Ethernet II) o longitud (IEEE 802.3)	Payload	Secuencia de comprobación (32-bit CRC)	Gap entre frames
7 Bytes	1 Byte	6 Byte	6 Bytes	(4 Bytes)	2 Bytes	De 46 (o 42) hasta 1500 Bytes	4 Bytes	12 Bytes
		64-1522 Bytes						
72-1530 Bytes								
84-1542 Bytes								

Formato de la trama Ethernet

El primer campo es el **preámbulo,** que indica el inicio de la trama y tienen el objeto de que el dispositivo que lo recibe detecte una nueva trama y se sincronice.

El **delimitador de inicio de trama** indica que el *frame* empieza a partir de él.

Los campos de **MAC** (o dirección) **de destino y origen** indican las direcciones físicas del dispositivo al que van dirigidos los datos y del dispositivo origen de los datos, respectivamente.

La **etiqueta** es un campo opcional que indica la pertenencia a una VLAN o prioridad en IEEE P802.1p.

Ethernet Type indica con qué protocolo están encapsulados los datos que contiene la *Payload*, en caso de que se usase un protocolo de capa superior.

La ***Payload*** es donde van todos los datos y, en su caso, cabeceras de otros protocolos de capas superiores que pudieran formatear a los datos que se tramiten (IP, TCP, etc).

Tiene un mínimo de 46 Bytes (o 42 si es la versión 802.1Q) hasta un máximo de 1500 Bytes. Los mensajes inferiores a 64 bytes se llaman *tramas enanas* (runt frames) e indican mensajes dañados y parcialmente transmitidos.

La **secuencia de comprobación** es un campo de 4 bytes que contiene un valor de verificación CRC (control de redundancia cíclica). El emisor calcula el CRC de toda la trama, desde el campo destino al campo CRC suponiendo que vale 0. El receptor lo recalcula, si el valor calculado es 0 la trama es válida.

El ***gap* de final de trama** son 12 bytes vacíos con el objetivo de espaciado entre tramas.

Funcionamiento

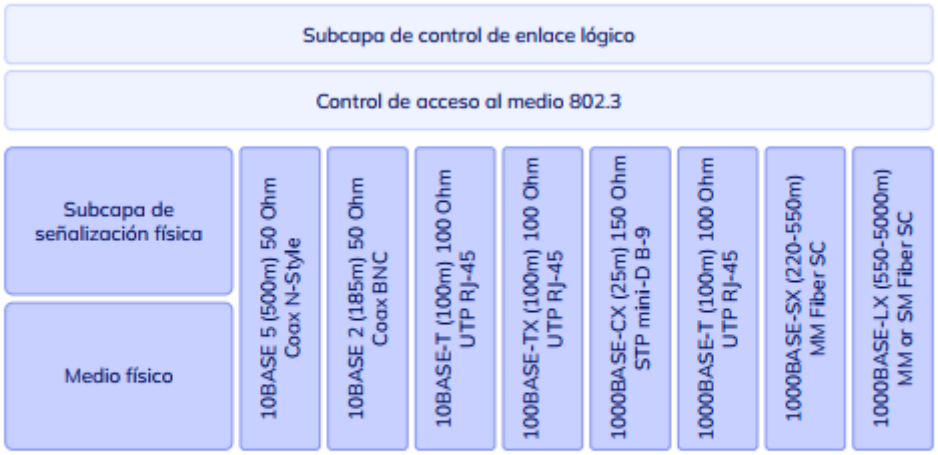
Ethernet **opera a través de dos capas** del modelo OSI.

El modelo ofrece una referencia sobre con qué puede relacionarse Ethernet, pero en realidad se implementa sólo en la mitad inferior de la capa de Enlace de datos, que se

conoce como **subcapa Control de acceso al medio** (*Media Access Control, MAC*), y la capa física.

Ethernet en la Capa 1 implica **señales**, *streams* de bits que se transportan en los medios, compo- nentes físicos que transmiten las señales a los medios y distintas topologías.

La **Capa 1** de Ethernet tiene un **papel clave en la comunicación** que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones. En la **Capa 2** se ocupa de estas **limitaciones**. Las subcapas de enlace de datos contribuyen significativamente a la compatibilidad de tecnología y la comunicación con la computadora. La subcapa MAC se ocupa de los componentes físicos que se utilizarán para comunicar la información y preparar los datos para transmitirlos a través de los medios.



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

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

Para Ethernet, el **estándar IEEE 802.2** describe las funciones de la subcapa LLC y el **estándar 802.3** describe las funciones de la subcapa MAC y de la capa física.

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

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

Medios, tecnologías y velocidades

El estándar define aspectos sobre los medios de transmisión como:

Velocidad de transmisión: velocidad a la que transmite la tecnología.

Tipo de cable: tecnología del nivel físico que usa la tecnología.

Longitud máxima: distancia máxima que puede haber entre dos nodos adyacentes (sin estaciones repetidoras).

Topología: determina la forma física de la red Bus si se usan conectores T (hoy solamente usados con las tecnologías más antiguas) y estrella si se usan hubs (estrella de difusión) o switches (estrella conmutada).

Muchas de las tecnologías fueron quedando obsoletas como el cable coaxial en topologías de bus y anillo.

Actualmente, el cable coaxial se sigue utilizando pero en otro tipo de redes, por ejemplo, se entregan conexiones a internet mediante cable coaxial que además de datos de red transmiten otros servicios como TV digital.

Versiones

La **primera versión** del IEEE 802.3 fue un intento de estandarizar ethernet aunque hubo un campo de la cabecera que se definió de forma diferente.

Posteriormente ha habido ampliaciones sucesivas al estándar que cubrieron las ampliaciones de velocidad (Fast Ethernet, Gigabit Ethernet y el de 10 Gigabits), redes virtuales, hubs, conmutadores y distintos tipos de medios, tanto de fibra óptica como de cables de cobre (tanto par trenzado como coaxial).

Cada versión nueva de Ethernet mejoraba las tecnologías tanto de dispositivos de red como de medios, incorporando el cable de par trenzado que significó un salto de gran impacto y es el tipo de medio que se usa comúnmente en redes LAN.

802.3e	1987	1BASE5 o StarLAN
802.3i	1990	10BASE-T 10 Mbit/s sobre par trenzado no blindado (*Unshielded Twisted Pair* o UTP). Longitud máxima del segmento 150 metros.
802.3j	1993	10BASE-F 10 Mbit/s sobre fibra óptica. Longitud máxima del segmento 1000 metros.
802.3u	1995	100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet a 100 Mbit/s con auto-negociación de velocidad.
802.3x	1997	Full Duplex (Transmisión y recepción simultáneos) y control de flujo.
802.3y	1998	100BASE-T2 100 Mbit/s sobre par trenzado no blindado (UTP). Longitud máxima del segmento 100 metros
802.3z	1998	1000BASE-X Ethernet de 1 Gbit/s sobre fibra óptica.
802.3ab	1999	1000BASE-T Ethernet de 1 Gbit/s sobre par trenzado no blindado
802.3ac	1999	Extensión de la trama máxima a 1522 bytes (para permitir las "Q-tag") Las Q-tag incluyen información para 802.1Q VLAN y manejan prioridades según el estándar 802.1p.
802.3ad	2000	Agregación de enlaces paralelos.

Algunas versiones del estándar Ethernet.

Velocidades

La nomenclatura con la que se denomina cada tecnología usada para interconectar los nodos tiene el siguiente formato:

Velocidad de transmisión.

Base indica el tipo de señalización: banda base (una única señal por un medio, banda

ancha múltiples señales)

Tipo, longitud máxima del medio y topologías.

Entonces si nos referimos a **10BaseT**:

10 Mbits/s

Banda base

Cable coaxial grueso, distancia máxima 500 m con topología de bus.

Este ejemplo corresponde a una tecnología ya obsoleta. A continuación veremos una tabla con la sucesión de tecnologías.

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base5	10 Mbit/s	Coaxial grueso	500 m	Bus (Conector AUI)
10Base2	10 Mbit/s	Coaxial delgado	185 m	Bus (Conector T)
10BaseT	10 Mbit/s	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbit/s	Fibra óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100 Mbit/s	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseTX	100 Mbit/s	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseFX	100 Mbit/s	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	1000 Mbit/s	Par Trenzado (categoría 5e o 6UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseTX	1000 Mbit/s	Par Trenzado (categoría 6UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseSX	1000 Mbit/s	Fibra óptica (multimodo)	550 m	Estrella. Full Duplex (switch)
1000BaseLX	1000 Mbit/s	Fibra óptica (monomodo)	5000 m	Estrella. Full Duplex (switch)
10GBaseT	10000 Mbit/s	Par Trenzado (categoría 6a o 7UTP)	100 m	
10GBaseLR	10000 Mbit/s	Fibra óptica (monomodo)	10000 m	
10GBaseSR	10000 Mbit/s	Fibra óptica (multimodo)	300 m	

Dispositivos de Red

El estándar Ethernet determina el formato de tramas, cómo esas tramas se vuelcan al medio, las tecnologías usadas y sus velocidades y los dispositivos que transportan las tramas a las NICs, en definitiva al dispositivo de usuario.

Interfaz de RED

Tarjeta de Interfaz de Red o **NIC**, permite que un dispositivo de usuario acceda a una red local. Cada tarjeta tiene una única dirección MAC que la identifica en la red. Una computadora conectada a una red se denomina nodo.

Las interfaces además de poseer una MAC, a nivel capa de Red del modelo OSI también se identifica con una dirección IP, un host puede tener más de una NIC y tener diferentes direcciones IP ya sean en la misma subred o en subredes diferentes.

Interfaz de red cableada

Las **placas de red** poseen distintos tipos de **conectores**, también definidos por el estándar Ethernet:

RJ-45 (Registered jack): 10/100/1000

BNC (Bayonet Neill-Concelman): 10

AUI (Attachment Unit Interface): 10

MII (Media Independent Interface): 100

GMII (Gigabit Media Independent Interface): 1000

NIC con conector RJ-45

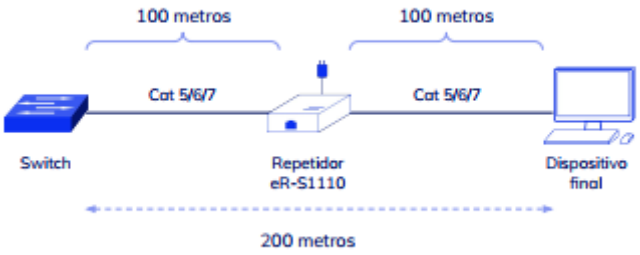
NIC con conector BNC para cable coaxial

Repetidor

Aumenta el alcance de una conexión física, recibiendo las señales y retransmitiéndolas, para evitar su degradación, a través del medio de transmisión, lográndose un alcance mayor. Usualmente se usa para unir dos áreas locales 'de igual' tecnología y solamente tiene dos puertos. **Opera en la capa física** del modelo OSI.

Las señales transmitidas por medios de cobre tienden a decaer con la distancia, un repetidor recibe las tramas por uno de sus puertos y las reenvía por el puerto conectado hacia el otro dispositivo.

El repetidor trabaja en Capa 1 o *Capa de nivel físico*, por lo tanto no tiene relación con las capas superiores, no realiza comprobaciones sobre la trama, ni opera a nivel protocolo.



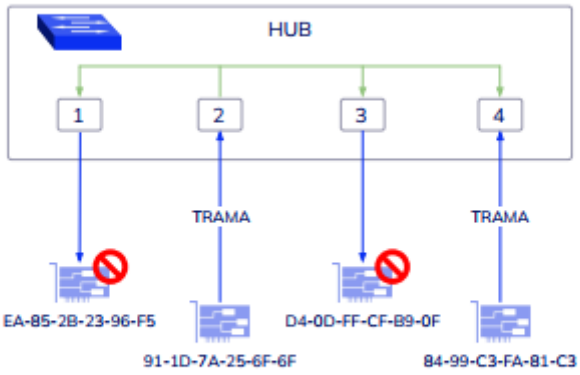
HUB

Funciona como un repetidor pero permite la **interconexión de múltiples nodos**.

Su funcionamiento es relativamente simple pues recibe una trama de ethernet, por uno de sus puertos, y la repite por todos sus puertos restantes sin ejecutar ningún proceso sobre las mismas. Opera en la capa física del modelo OSI.

Las tramas son recibidas por todas las interfaces de red, estas son descartadas en aquellas cuya dirección de destino no coincida con la dirección de la interfaz que la recibe.

Actualmente el hub es un dispositivo en desuso, aunque el término se sigue aplicado a otro tipo de dispositivos dentro de las redes datos que no tienen que ver con las redes LAN, por ejemplo centrales de distribución de internet a clientes.

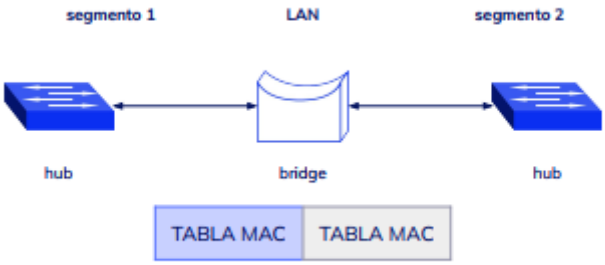


Trama MAC de origen 91-1D-7A-25-6F-6F
MAC destino 84-99-C3-FA-81-C3.

Puente de red

Un ***bridge*** o **puente de red**, **interconecta segmentos de red** haciendo el cambio de *frames* (tramas) entre las redes de acuerdo con una tabla de direcciones que le dice en qué segmento está ubicada una dirección MAC dada.

Se diseñan para uso entre las LAN que usan protocolos idénticos en la capa física y MAC (control de acceso al medio). Aunque existen *bridges* más sofisticados que permiten la conversión de formatos MAC diferentes.



Un puente opera a nivel de capa 2 del modelo OSI (enlace de datos y direccionamiento físico), por lo que puede encaminar tramas según sus direcciones de origen y destino. Esto lo ubica en un nivel superior a un repetidor e inclusive un hub.

El puente contiene lo que se denomina **Tabla de direcciones MAC**, que contiene las direcciones de las interfaces conectadas a cada segmento, de esta forma puede recibir una trama desde un segmento y pasarla al segmento siguiente.

Los puentes se utilizaban para segmentar redes físicas que crecían en tamaño en los que el medio era compartido, más hosts más probabilidades de colisiones, achicando los segmentos se lograban redes más eficientes.

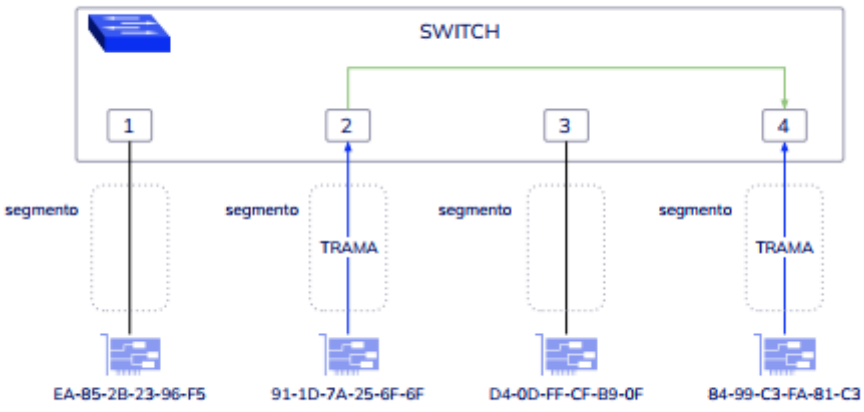
Hoy en día es bastante común encontrar los puentes que conectan distintos segmentos de red físicos que trabajan en medios distintos: la red cableada y la red wifi, nuestro teléfono y nuestra computadora estarán bajo la misma red lógica, pero conectados a la red por tecnologías distintas.

Switch o conmutador

Este dispositivo funciona como el *bridge*, pero permite la **interconexión de múltiples segmentos de red**, funciona en **velocidades más rápidas** y es **más sofisticado**.

Los switches pueden tener otras funcionalidades, como redes virtuales, y permiten su configuración a través de la propia red. Funciona básicamente en la **capa 2** del modelo OSI (enlace de datos). Por esto son capaces de procesar información de las tramas; su funcionalidad más importante es en las tablas de dirección.

Por ejemplo: una computadora conectada al puerto 1 del conmutador envía una trama a otra computadora conectada al puerto 2; el switch recibe la trama y la transmite a todos sus puertos, excepto aquel por donde la recibió; la computadora 2 recibirá el mensaje y eventualmente lo responderá, generando tráfico en el sentido contrario; ahora el switch conocerá las direcciones MAC de las computadoras en el puerto 1 y 2; cuando reciba otra trama con dirección de destino de alguna de ellas, únicamente transmitirá la trama a dicho puerto disminuyendo así el tráfico de la red y contribuyendo al buen funcionamiento de la misma.

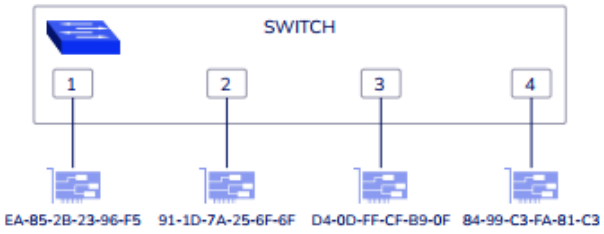


En un hub todos los hosts pertenecen a lo que se llama '**Dominio de colisión**'.

En aquellas topologías se usaba el mismo medio para transmitir y escuchar, por lo que todos los hosts estaban en el mismo segmento y las tramas iban dirigidas a todos ellos. En el caso del switch y su habilidad de cerrar circuitos entre hosts a partir del puerto de conexión y la información de origen y destino tenemos segmentos muchos más chicos: cada conexión al switch se considera un segmento.

El switch, como el puente, utiliza lo que se denomina una tabla MAC, esto es similar a la tabla ARP de las NICs que mantienen una tabla con las direcciones MAC e IP asociadas de las NICs que se encuentran en la red.

En el caso de un switch la tabla MAC mantiene una relación entre la direcciones MAC y el puerto físico de conexión.



Switch visto de frente con NICs conectadas.

TABLA MAC	
Puerto	**MAC**
1	EA-85-2B-23-96-F5
2	91-1D-7A-25-6F-6F
3	D4-0D-FF-CF-B9-0F
4	84-99-C3-FA-81-C3

Cuando una trama entra por un puerto el switch identifica la dirección física de destino y retransmite la trama al puerto correspondiente según la tabla.

Enrutamiento

El **enrutamiento** es el proceso de **reenviar paquetes entre redes,** siempre **buscando la mejor ruta** (la más corta).

Para encontrar esa ruta más óptima, se debe tener en cuenta la tabla de enrutamiento y algunos otros parámetros como la métrica, la distancia administrativa, el ancho de banda, etc.

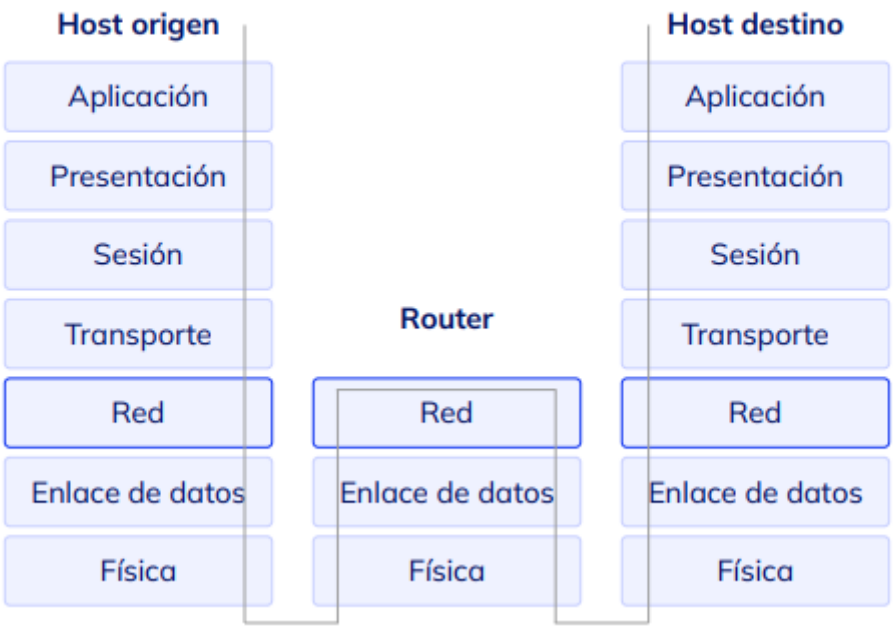
En una red los dispositivos que se encargan de llevar los paquetes entre redes son los '**router**'. **Un router es un dispositivo de capa 3 (Nivel de red) del modelo OSI.**

Router

Su función es la de **establecer la mejor ruta** que destinará a cada paquete de datos para llegar a la red y al dispositivo de destino.

Es bastante utilizado para conectarse a Internet ya que conecta la red de nuestro hogar, oficina o cualquier red a la red de nuestro proveedor de este servicio.

La mayoría de los routers que se utilizan para el hogar y oficinas tienen incorporadas otras funciones adicionales al enrutador, como por ejemplo: punto de acceso inalámbrico, que permite crear y conectarse a una red Wifi; módem, que convierte las señales análogicas a digitales y viceversa; Conmutador, que conecta varios dispositivos a través de cable, creando una red local, a a este dispositivo se lo conoce como CPE.



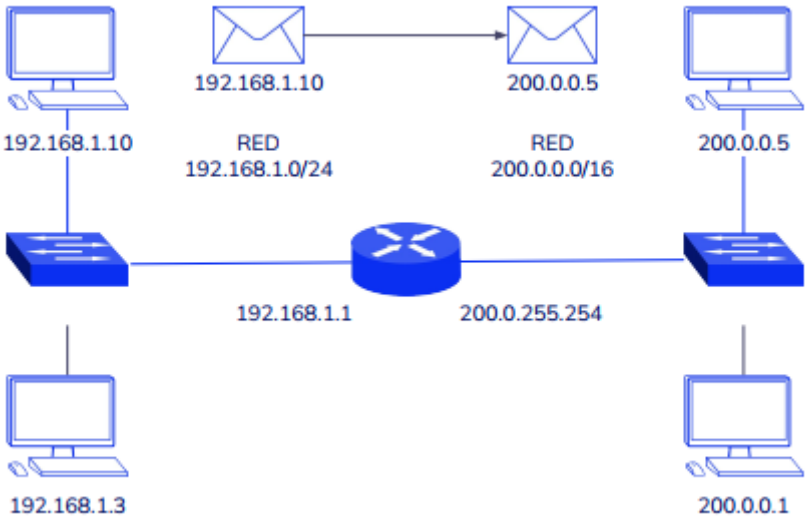
Funcionamiento

Consiste en enviar los paquetes de red por el camino o ruta más adecuada en cada momento. Para ello **almacena** los paquetes recibidos y

procesa la información de origen y destino que poseen los datagramas (paquetes de datos con direcciones IP).

Un router recibe un paquete por una interfaz de red, y lo encamina hacia la red de destino por la interfaz vinculada a la red de destino. A diferencia de un *switch,* que tiene puertos de conexión, un router posee interfaces de red como cualquier host. Nótese que el router no está listado dentro de los dispositivos Ethernet, ya que este estándar abarca de capa 2 hacia abajo.

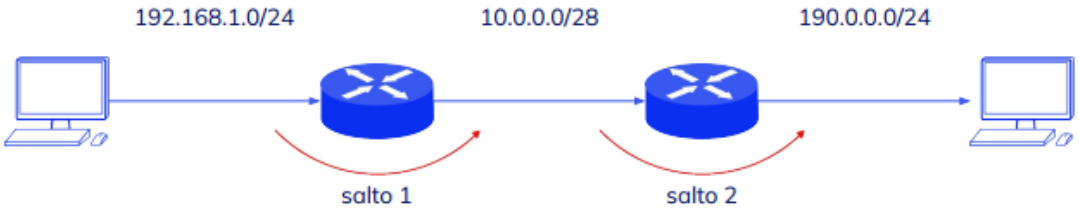
Ethernet determina las tecnologías físicas de transporte de tramas, no de paquetes.



Salto de red (*hop*)

En redes de computadoras, incluida la Internet, se produce un **salto** cuando se pasa un paquete de un segmento de red al siguiente. Los paquetes de datos pasan a través de los routers mientras viajan entre la fuente y el destino.

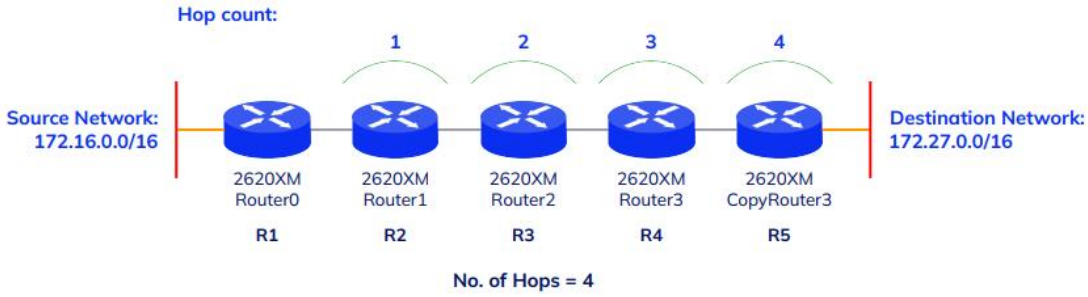
Dado que en cada salto se producen latencias de almacenamiento y reenvío y otras latencias, un gran número de saltos entre el origen y el destino implica un menor rendimiento en tiempo real.



Recuento de saltos (*hop count*)

El **recuento de saltos** se refiere al **número de dispositivos de red intermedios** por que pasa un paquete de datos.

Es una medida aproximada de la distancia entre dos hosts. Un recuento de ‘n’ saltos significa que ’n’ dispositivos separan el host de origen del de destino.



Métrica

Los protocolos de enrutamiento se encargarán de buscar la mejor ruta hacia la red destino, pero tener en cuenta **el conteo de saltos no es del todo útil para determinar la ruta óptima de la red,** ya que no tiene en cuenta la velocidad, la carga, la fiabilidad o la latencia de ningún salto en parti- cular, sino simplemente el recuento total.

No obstante, hay protocolos de enrutamiento, como el *Protocolo de Información de enrutamiento (RIP),* que utilizan el recuento de saltos como única métrica.

Hop limit

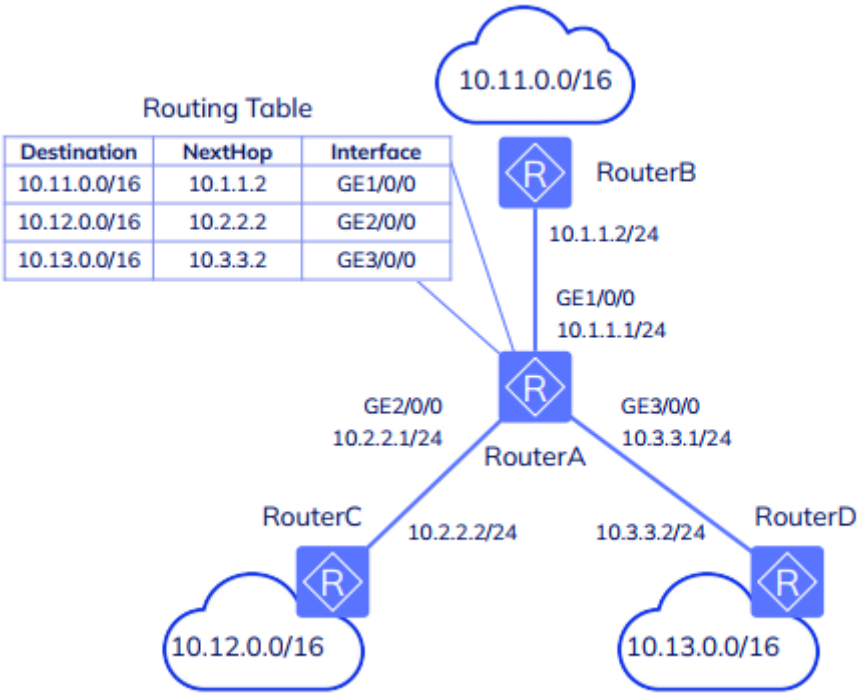
Conocido como el **tiempo de vida** (TTL) en IPv4, y **límite de saltos** en IPv6, este campo en el datagrama IP especifica un **límite** en el número de saltos que se permite a un paquete antes de ser desechado.

Los routers modifican paquetes IP a medida que se reenvían, disminuyendo el valor de los respectivos campos TTL o límite de saltos. Los routers no reenvían paquetes con un campo resultante de 0 o menos. Esto evita que los paquetes sigan un bucle infinito.

Next hop

Cuando un paquete de datos tiene una red de destino distinta a la de origen debe ser enviado a un dispositivo que se supone tiene acceso a otras redes, a este dispositivo se lo conoce como '***gateway***' y suele ser un router.

Cuando el paquete llega al *gateway* se determina si se conoce la red o si debe ser enviado a otro router que pueda conocer el camino de destino: el **siguiente salto** es la siguiente puerta a la que los paquetes deben ser reenviados a lo largo del camino a su destino final.



Trazado de ruta

El comando '**traceroute**' puede ser utilizado para el número de hops del router de un host a otro. Los recuentos de hops son a menudo útiles para encontrar fallos en una red, o para descubrir si el enrutamiento es realmente correcto.

Tabla de enrutamiento

La **tabla de enrutamiento** es un sistema de registro del router que guarda la relación entre la red de destino y la interfaz de salida.

Es mantenida de forma **estática** (por el administrador de la red) o **dinámica** (con protocolos de enrutamiento). Se interpreta de la misma forma tanto si se trata de un host como de un router.

```
educacionit@athena:~$ route
Tabla de rutas IP del núcleo
Destino         Pasarela        Genmask         Indic Métric Ref    Uso Interfaz
default         _gateway        0.0.0.0         UG    100    0        0 eno1
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 eno1
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 eno1
```

Tabla de enrutamiento de un host con GNU/Linux, se indica cual es la interfaz por donde los paquetes pueden alcanzar el gateway.

Una tabla de enrutamiento suele contener la dirección de IP de una red de **destino** y la dirección de IP de la **siguiente puerta de enlace** en el camino hacia el destino final de la red. Al almacenar sólo la información del salto siguiente, el encaminamiento o el reenvío del salto siguiente reduce el tamaño de las tablas de enrutamiento.

Una determinada puerta de enlace sólo conoce un paso en el camino, no el camino completo a un destino.

También es clave saber que los siguientes saltos listados en una tabla de enrutamiento están en redes a las que la pasarela está directamente conectada, por lo tanto un paquete puede llegar a un destino siempre que exista una ruta, en una LAN un paquete jamás llegará a un destino de internet si no existe un router conectado directamente a la red pública.

Estructura

La tabla de enrutamiento presenta en su estructura los siguientes campos:

Gateway: dirección del router utilizado para encaminar el datagrama hacia el destino. El encaminamiento puede ser de dos tipos, directo e indirecto, lo vamos a ver en las próximas slides.

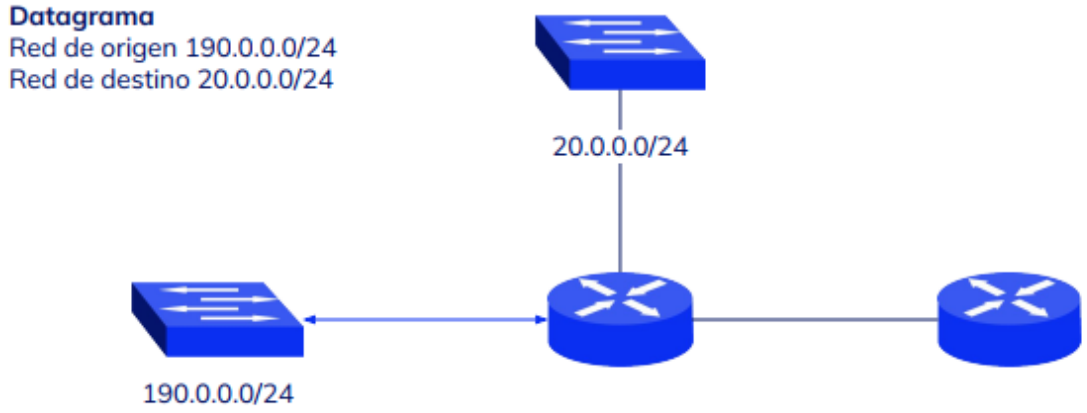
Destino: direcciones IP de redes destinos donde sabe llegar el router.

Máscara: máscara que determina el identificador de la red de la IP destino.

Interfaz: identifica la interfaz de salida por donde debe de enviarse el datagrama.

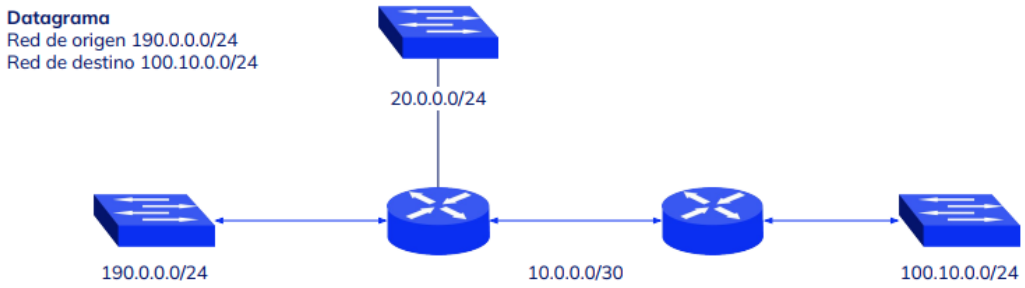
Métrica: parámetro en función del cual se escoge la mejor ruta (nº de saltos, ancho de banda, confiabilidad).

Encaminamiento directo: la interfaz de salida del router está en la misma red que la dirección destino del datagrama.



Los datagramas pasan de una red a otra, ambas redes están conectadas al mismo router.

Encaminamiento indirecto: la interfaz de salida no está en la misma red que la dirección destino del datagrama. El datagrama se envía a un router gateway que lo conducirá hacia su destino.

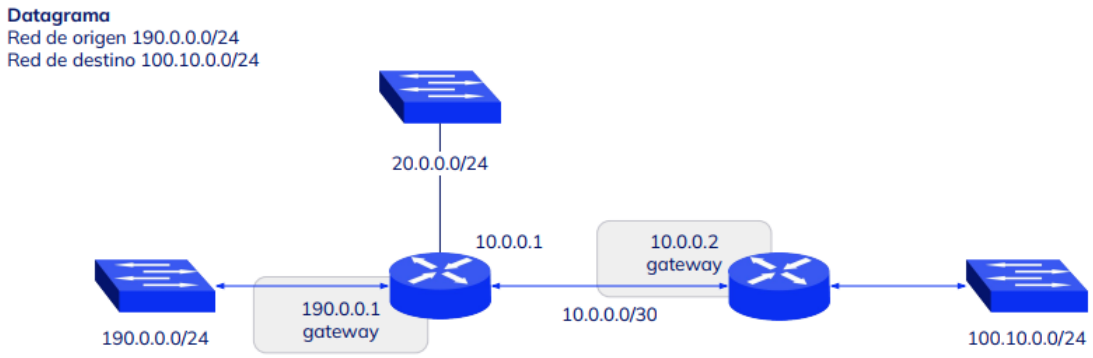


Los datagramas deben dar dos saltos para llegar a la red destino.

Funcionamiento

La tabla de enrutamiento o '*routing table*' contiene las **redes** que están **directamente conectadas** al router. Los paquetes que no tengan como destino de red una entrada en la tabla se envían a una ruta por defecto (*gateway*), esto evita que las tablas crezcan en tamaño ya que no podría albergar todas las rutas de todas las redes que conforman internet.

Un router normalmente especifica las rutas más cercanas, el resto de rutas se indican mediante una ruta o *gateway* por defecto. Al *gateway* por defecto se le envían aquellos datagramas que no se saben cómo encaminar.



Cada host, incluyendo los enrutadores, tiene definido un gateway por donde enviar paquetes cuya red destino no conozca.

Cuando el enrutador recibe un paquete se pasa a enrutar dicho paquete:

1. Extrae la IP destino.

2. Evalúa si la red de destino existe en la tabla.

3. Las entradas de la tabla se ordenan de mayor a menor bits en la máscara de red. Debido a este ordenamiento, la ruta por defecto será la última en mirarse si existe.

4. ***Routing* dinámico**: los enrutadores intercambian información con sus vecinos como la periodicidad con que se intercambian los paquetes de encaminamiento, el formato y contenido de estos paquetes, algoritmos asociados que permiten calcular el camino óptimo para decidir la interfaz de salida (e.j., algoritmos de mínimo coste).

***Routing* estático**: es el *routing* realizado por el administrador de la red, por lo tanto no es un sistema que responda automáticamente ante caídas de enlaces. Hay dos tipos de comandos que permiten introducir rutas en la tabla de *routing*: comandos que mapean IP sobre interfaces y comandos que añaden rutas hacia otras redes.

5. **La determinación de ruta**: en este punto se evalúa cuál es la mejor ruta a partir de las métricas recabadas por los protocolos y algoritmos de enrutamiento.

Topologías

Los enrutadores son la clave para que los paquetes IP lleguen de una red a otra, esto siempre que exista un camino, caso contrario se obtiene un mensaje de error "destino inalcanzable". Esto es porque se ha superado la cantidad de saltos o dentro de la red ningún enrutador puede llegar a la red de destino.

Como los hosts y switches, los enrutadores se pueden organizar de manera que permitan redundancia, tolerancia a fallos o proveer caminos a segmentos de red según la cantidad de saltos o segmento de red con funciones específicas, por ejemplo la red de servidores.

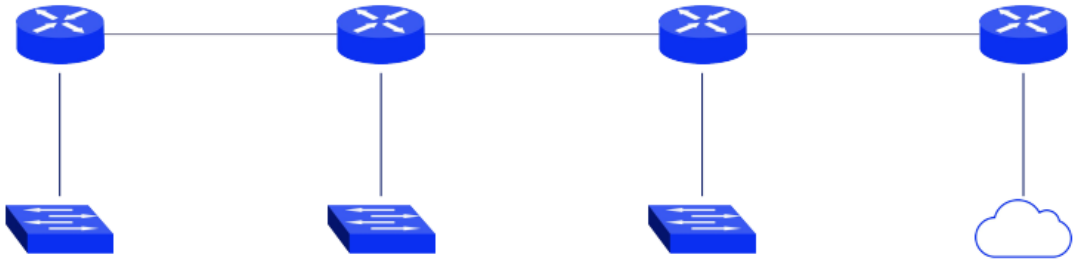
Por todo lo explicado en este capítulo podemos deducir lo siguiente:

Se organizan bajo una **distribución física**, el interconectado, es decir la **topología física**.

Se organizan bajo **redes lógicas** que comunican a los enrutadores entre sí, es decir la **topología lógica**.

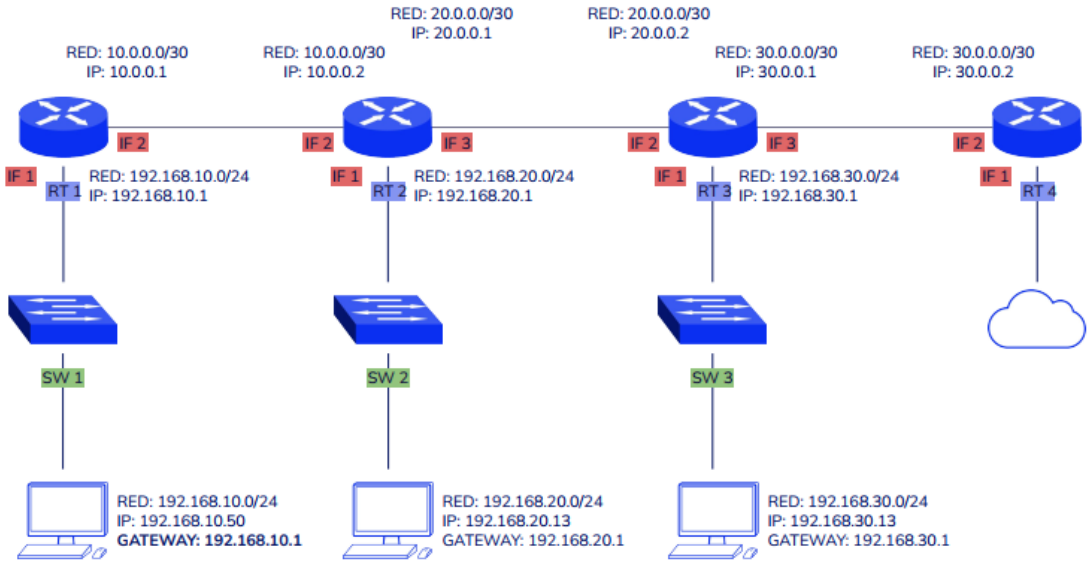
Topología física

La siguiente red presenta una topología física con *backbone* en serie. La disposición física nos da la idea de cómo las tramas llegan de dispositivo a dispositivo.



Topología lógica

Ya está definido cómo los dispositivos se interconectan entre sí a nivel físico, queda por determinar cómo los paquetes de datos llegan a nivel lógico.



Cada switch organiza un conjunto de hosts bajo una red propia y cada host puede enviar paquetes por el *gateway* por defecto de cada red.

DISPOSITIVO	RED	GATEWAY	ENRUTADOR	INTERFAZ DEL ROUTER
SW 1	192.168.10.0/24	192.168.10.1	RT 1	IF 1
SW 2	192.168.20.0/24	192.168.20.1	RT 2	IF 1
SW 3	192.168.30.0/24	192.168.30.1	RT 3	IF 1

Cada enrutador tiene tiene una conexión física con el siguiente, al mismo tiempo cada enlace entre enrutadores forman una red lógica propia.

La siguiente tabla describe las interfaces de cada router junto con sus respectivas IP y la red de pertenencia:

INTERFAZ	RT 1	RT 2	RT 3	RT 4
IF 1	192.168.10.1/24	192.168.20.1/24	192.168.30.1/24	INTERNET
IF 2	10.0.0.1/30	10.0.0.2/30	20.0.0.2/30	30.0.0.2/30
IF 3	-	20.0.0.1/30	30.0.0.1/30	

RED: 10.0.0.0/30 **RED: 20.0.0.0/30** **RED: 30.0.0.0/30**

Gateway

El *gateway*, también conocido como **puerta de enlace predeterminada**, es necesario para enviar un paquete fuera de la red local. Si la porción de red de la dirección de destino del paquete es diferente de la red del host de origen, el paquete tiene que hallar la salida fuera de la red original.

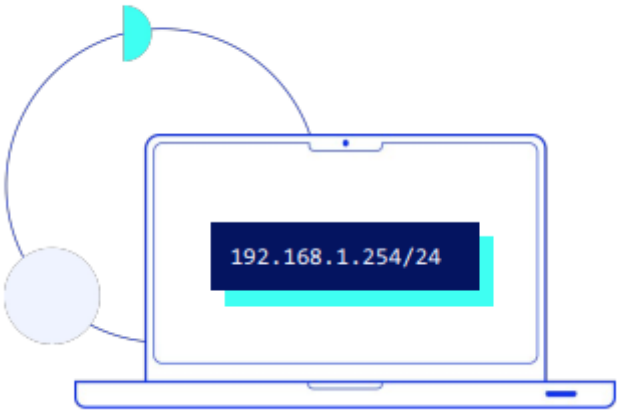
Para esto, el paquete es enviado al *gateway*. Este *gateway* es una interfaz del router conectada a la red local.

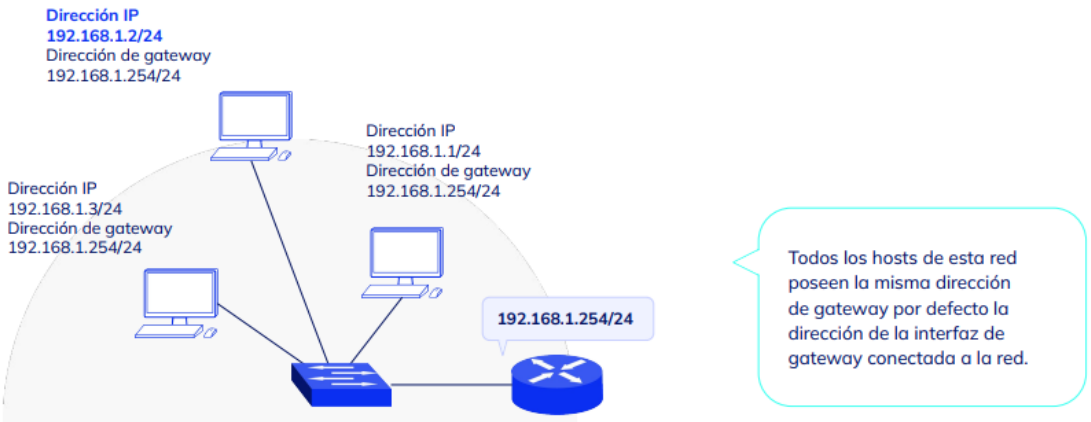
La interfaz del *gateway* tiene una dirección de capa de Red que concuerda con la dirección de red de los hosts. Los hosts están configurados para reconocer que la dirección es un *gateway*.

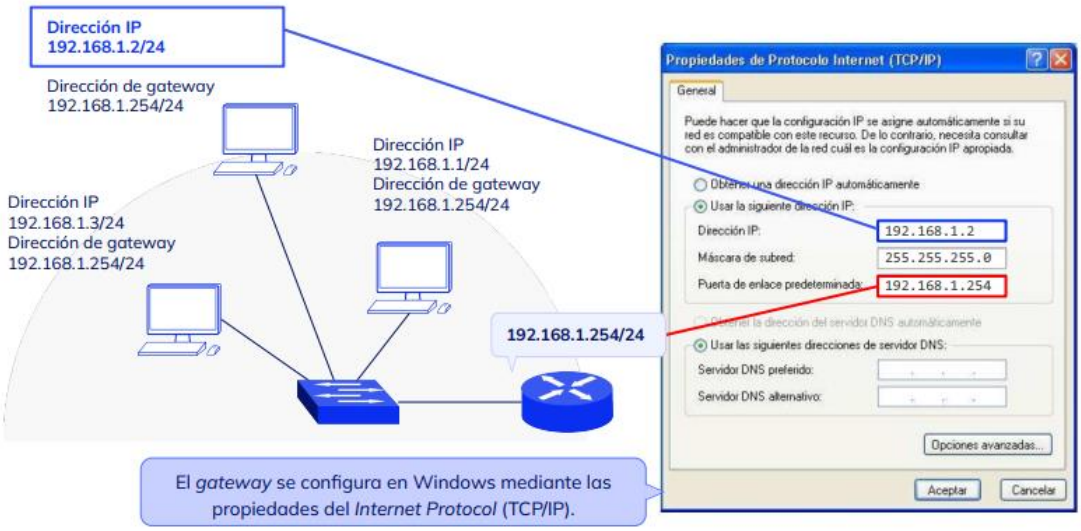
Gateway por defecto

El *gateway* por defecto está configurado en el host. En una computadora con Windows, se usan las herramientas de las Propiedades del Protocolo de Internet (TCP/IP) para ingresar la dirección IPv4 de *gateway* por defecto.

Tanto la dirección IPv4 de host como la dirección de *gateway* deben tener la misma porción de red (y subred si se utiliza) de sus respectivas direcciones.







Ningún paquete puede ser **enviado sin una ruta**. Si el paquete se origina en un host o se reenvía por un dispositivo intermediario, el dispositivo debe tener una ruta para identificar dónde enviar el paquete.

Un host debe **reenviar el paquete** ya sea al host en la red local o al *gateway*, según sea lo adecuado. Para reenviar los paquetes, el host debe tener rutas que representan estos destinos. Un router toma una decisión de reenvío para cada paquete que llega a la interfaz del *gateway*. Este proceso es denominado **enrutamiento**. Para reenviar un paquete a una red de destino, el router requiere una ruta hacia esa red.

Si una ruta a una red de destino no existe, el paquete no puede reenviarse. La red de destino puede ser un número de routers o saltos fuera del *gateway*. La ruta hacia esa red sólo indicaría el router del siguiente salto al cual el paquete debe reenviarse, no el router final.

El proceso de enrutamiento usa una ruta para asignar una dirección de red de destino hacia el próximo salto y luego envía el paquete hacia esta dirección del próximo salto.

Network Address Translation **(NAT)**

La **traducción de direcciones de red**, también llamado **enmascaramiento de IP** o **NAT** (del inglés *Network Address Translation*), es un mecanismo utilizado por routers IP para cambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en **convertir**, en tiempo real, las direcciones utilizadas en los paquetes transportados.

En un escenario normal al interconectar dos redes mediante un router estas se hacen visibles mutuamente, esto quiere decir que los paquetes son enrutados en todas direcciones gracias a la tabla de enrutamiento. Pero por el contrario cuando un segmento de red se conecta a otra red mediante NAT, se denomina “red privada”, en principio, los

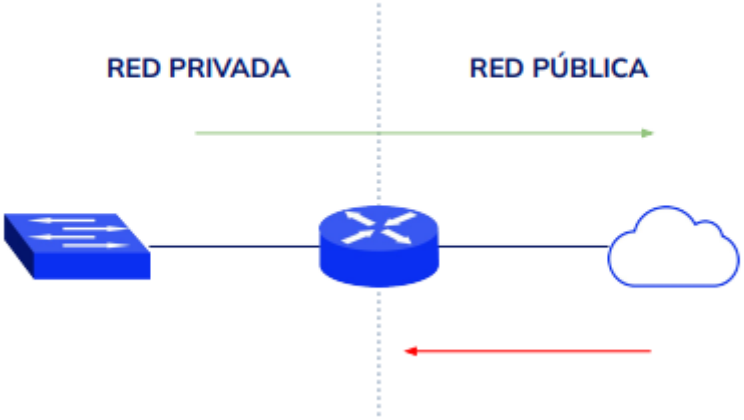
hosts de la red privada pueden llegar a cualquier destino, pero los hosts de las redes del otro lado no pueden llegar a los hosts de la red privada de forma directa.

Este tipo de configuración de red es el que se usa en las configuraciones de acceso a internet:

Desde la LAN se puede acceder a cualquier host (servidores y otros routers) dentro de

la red pública.

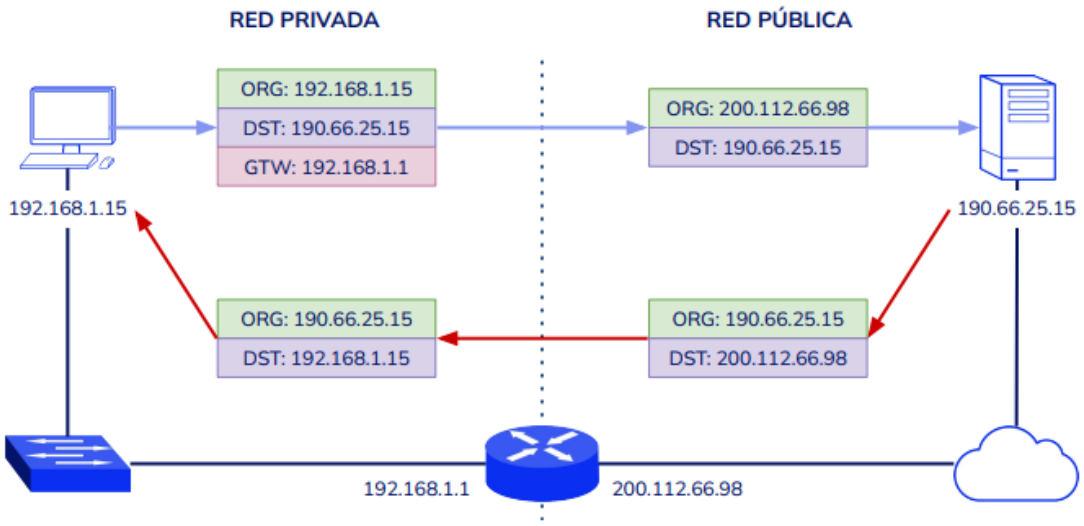
Desde la red pública no se puede acceder a los hosts de una red privada.



Funcionamiento

Un paquete cuyo destino sea una red distinta a la propia será **reenviado por el *gateway*** que es un **router NAT**. El router "enmascara" la dirección de origen por la dirección de la interfaz que está conectada a la siguiente red.

Bajo el modelo NAT los paquetes llegan al servidor como si hubiesen sido originados en el router. El servidor envía las respuestas a la IP pública del router, luego este traduce las direcciones para entregar el paquete al host correspondiente dentro de la red privada.



El paquete de datos sale del host de la red privada, para el host receptor quien envió el paquete fue un host con dirección 200.112.66.98 y es a quien dirigirá las respuestas.

Tipos de NAT

NAT de cono completo *(Full-Cone NAT)*

En este caso de comunicación completa, NAT mapeará la dirección IP y puerto interno a una dirección y puerto público diferentes. Una vez establecido, cualquier host externo puede comunicarse con el host de la red privada enviando los paquetes a una dirección IP y puerto externo que haya sido mapeado. Esta implementación NAT es la menos segura, puesto que un atacante puede adivinar qué puerto está abierto.

NAT de cono restringido *(Restricted Cone NAT)*

En este caso de la conexión restringida, la IP y puerto externos de NAT son abiertos cuando el host de la red privada quiere comunicarse con una dirección IP específica fuera de su red. La NAT bloqueará todo tráfico que no venga de esa dirección IP específica.

NAT de cono restringido de puertos *(Port-Restricted Cone NAT)*

En una conexión restringida por puerto NAT bloqueará todo el tráfico a menos que el host de la red privada haya enviado previamente tráfico a una IP y puerto específico, entonces solo en ese caso esa IP/puerto tendrán acceso a la red privada.

NAT Simétrica *(Symmetric NAT)*

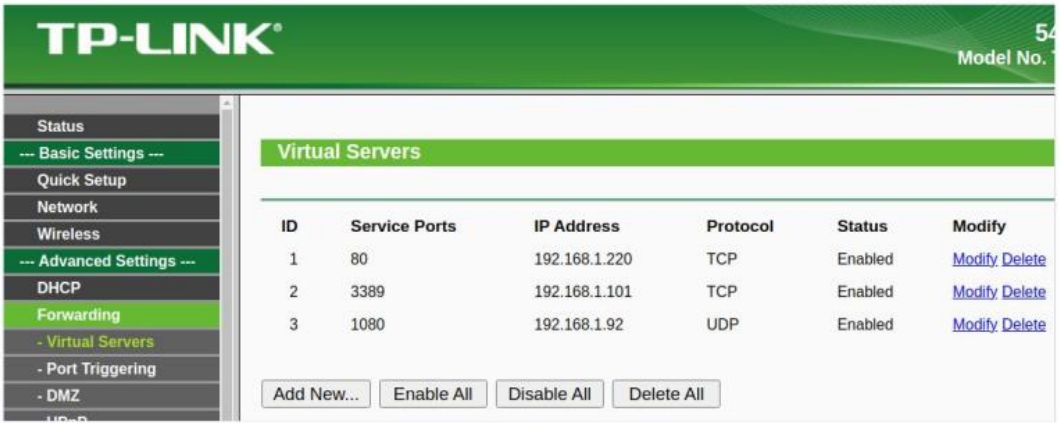
En este caso la traducción de dirección IP privada a dirección IP pública depende de la dirección IP de destino donde se quiere enviar el tráfico.

Reenvío de puertos (*Port forwarding*)

El **reenvío de puertos**, también conocido como “apertura de puertos” y “mapeo de puertos”, consiste en permitir que determinados servicios de una red privada sean **accesibles** desde redes externas.

La apertura de puertos se utiliza cuando el segmento de red detrás de un enrutador NAT debe recibir paquetes, por lo tanto peticiones de conexión desde hosts que están fuera de la red.

La mayoría de los routers hogareños (aquellos que integran wifi, switch, etc) trabajan en modo NAT siendo el puerto “WAN” el que separa la red privada de la red pública. En estos dispositivos podemos hacer la apertura desde el panel de configuración web.

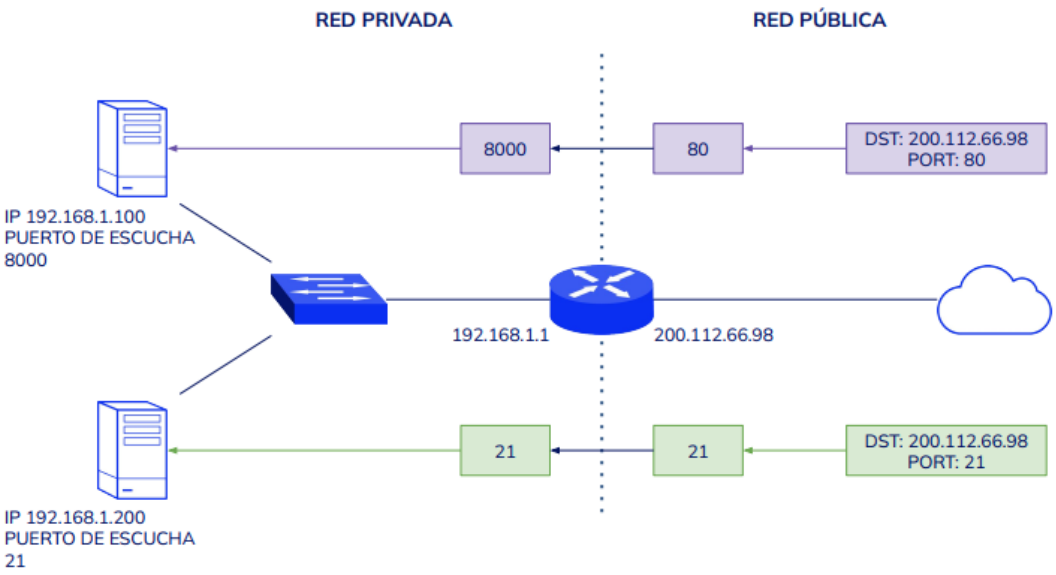


Mapeo de puertos en un router TP-Link.

Funcionamiento

Los mensajes además de tener una IP de destino tienen un **puerto de destino**, lo que permite establecer las conexiones en las que las aplicaciones intercambiarán información.

En una red NAT los hosts dentro de la red privada son inaccesibles, lo que es accesible es la dirección IP pública del router. La apertura consiste en indicar que los paquetes que tengan como destino un puerto y un protocolo determinado se reenvían a un host dentro de la red privada.



Puerto del router	Servicio	Host destino	Puerto de escucha del host	Protocolo
80	Web App	192.168.1.100	8000	TCP
21	FTP	192.168.1.200	21	TCP

Puertos y protocolos

La **apertura de puertos** se puede realizar según los siguientes criterios:

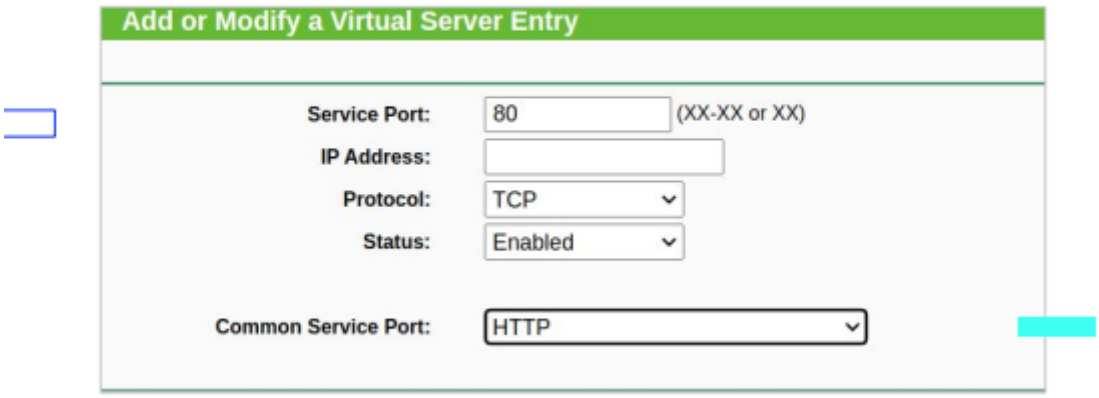
Puertos de escucha en la red pública.

Puertos de escucha de los hosts dentro de la red.

Protocolos de transporte TCP/UDP.

Rango de puertos.

Normalmente los enrutadores tienen perfiles predefinidos según el tipo de servicio.



Cabe destacar que la **apertura de puertos** apunta a **redireccionar un puerto externo** al puerto de un host dentro de la red.

Van de uno a uno, no sería posible abrir un puerto y que apunte a dos direcciones IP diferentes, a nivel lógico es imposible.