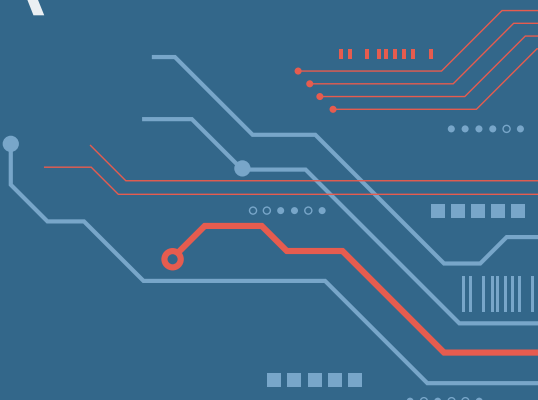


# REDES DE DATOS TUIA | FCEIA UNR

Docentes | 1C 2023

Juan Pablo Michelino  
Emiliano Pavicich  
Andrea León Cavallo  
Iván Pellejero  
Esteban Toribio

jpmich@fceia.unr.edu.ar  
pavicich@fceia.unr.edu.ar  
aleoncavallo@gmail.com  
ivan.pellejero97@gmail.com  
toribio@fceia.unr.edu.ar



# 04



## CAPA DE RED

4.1. Funciones y características.

4.2. Protocolos de la capa de red.

4.3. IPv4 e IPv6

4.4. Direcciones IPv4

4.5. Direcciones IPv6

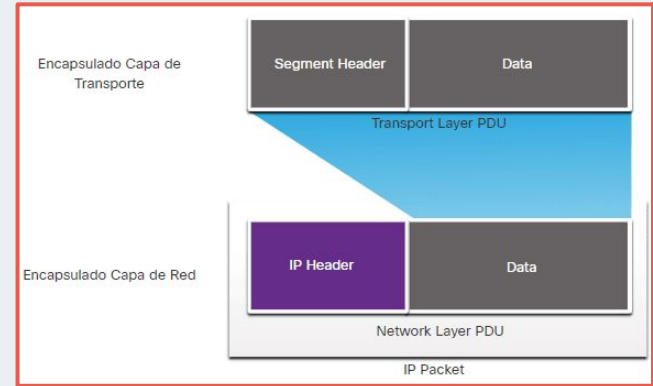




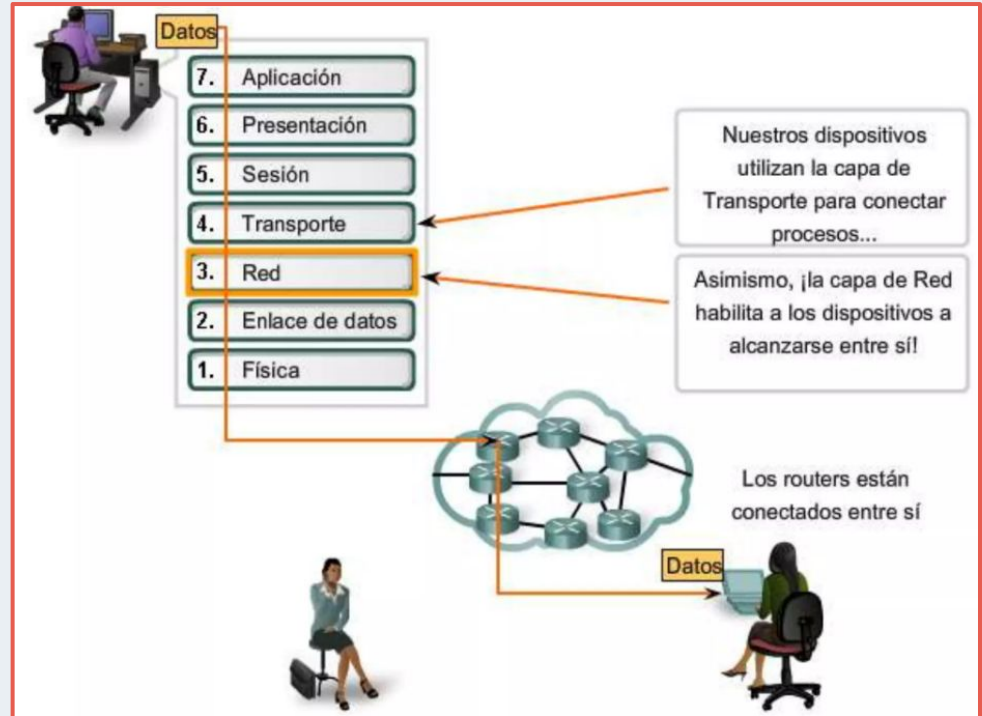
# Funciones y características

# Funciones

- **Direccionar origen y destino** para poder dirigir los segmentos de datos.
- **Encapsular** agregando un encabezado a cada paquete, antes de ser entregado a la capa inferior, para ser entregado al destino correcto.
- **Desencapsular** el paquete recibido para luego ser entregado al protocolo de capa superior (servicio) correcto.
- **Enrutar** los paquetes de datos seleccionando la ruta correcta. Durante el recorrido a través de una red, el paquete puede atravesar muchos dispositivos intermediarios.
- **Control de congestionamiento** de paquetes de un nodo a otro en la red.



# Funciones



# Características

IP está destinado a tener una sobrecarga baja y puede describirse como:

- Sin conexión.
- Mejor esfuerzo.
- Independiente de los medios:
  - No es confiable.
  - Depende de otros protocolos.
  - Establece la MTU (Unidad Máxima de Transferencia).
  - Fragmentación.

# Características

## IP Sin conexión (Connectionless)

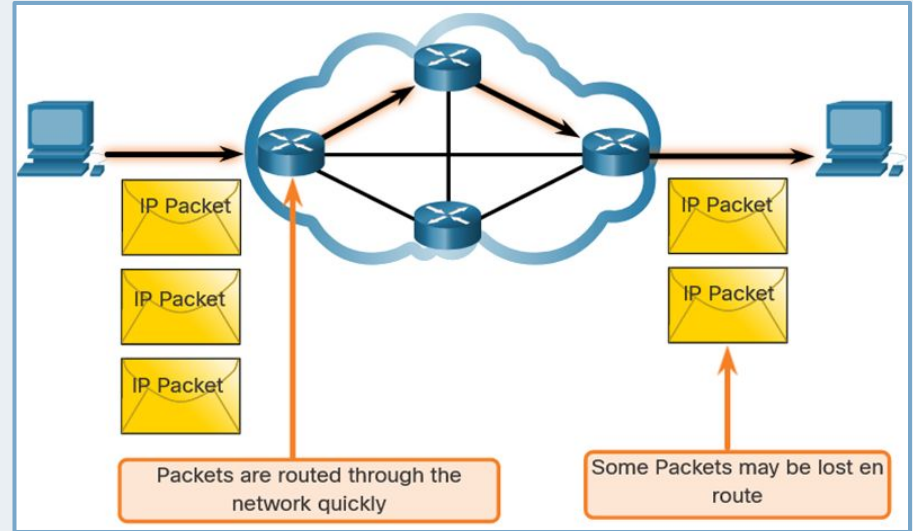
- IP no establece ninguna conexión con el destino antes de enviar el paquete.
- No se necesita información de control (sincronizaciones, confirmaciones, etc.).
- El destino recibirá el paquete cuando llegue, pero no se envían notificaciones previas por IP.



# Características

## Mejor esfuerzo:

- IP no garantizará la entrega del paquete.
- IP ha reducido la sobrecarga ya que no existe ningún mecanismo para reenviar datos que no se reciben.
- IP no espera reconocimientos.
- IP no sabe si el otro dispositivo está operativo o si recibió el paquete.

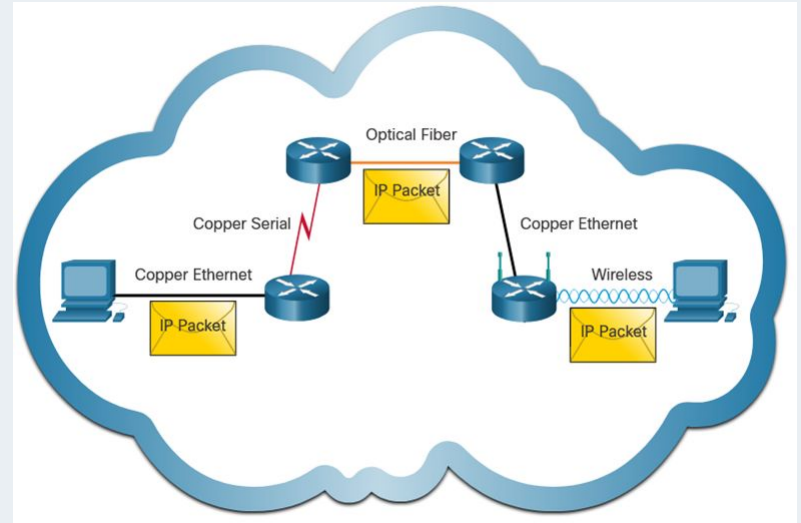




# Características

## No es confiable:

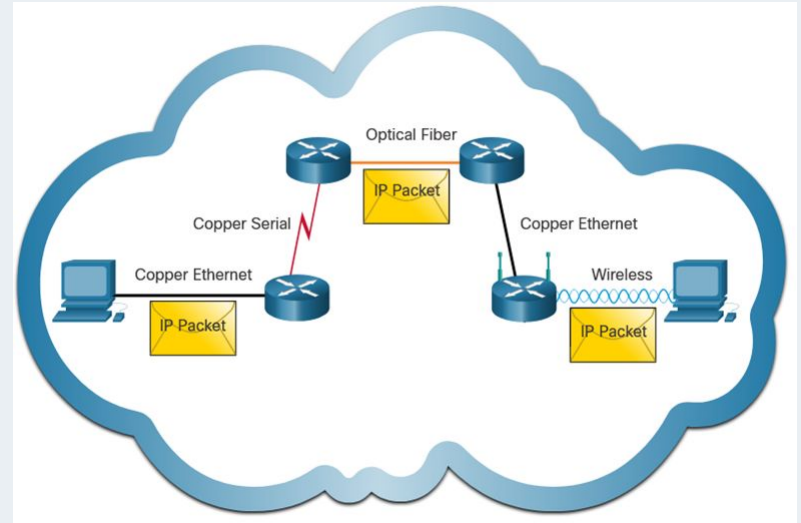
- No puede administrar ni corregir paquetes no entregados o corruptos.
- IP no puede retransmitir después de un error.
- IP no puede realinear los paquetes de secuencia.



# Características

Depender de otros protocolos para:

- IP es independiente de los medios
- IP no se refiere al tipo de trama requerido en la capa de enlace de datos ni al tipo de medio en la capa física.
- IP se puede enviar a través de cualquier tipo de medio: cobre, fibra o inalámbrica.



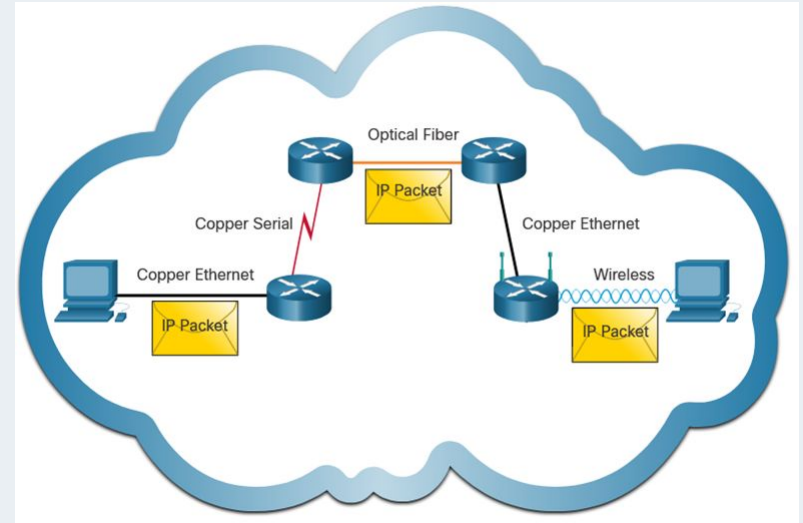
# Características

La capa de red establecerá la Unidad de Transmisión Máxima (MTU).

- La capa de red lo recibe de la información de control enviada por la capa de vínculo de datos.
- A continuación, la red establece el tamaño de MTU.

## Fragmentación:

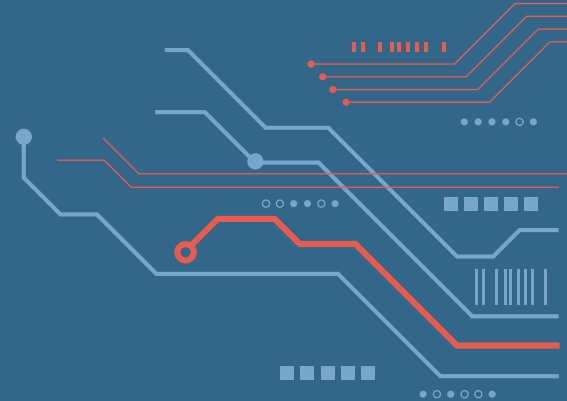
- IPv4 fragmenta en unidades más pequeñas.
- IPv6 no fragmenta paquetes.



A decorative graphic in the top-left corner consisting of stylized circuit lines in light blue and red. The lines are of varying thickness and form a complex, angular pattern. There are also small circles and squares along the lines, some in red and some in light blue.

# Protocolos de la capa de red

IP, ICMP, IGMP, ARP y Protocolos de enrutamiento



# Protocolos de la capa de red

- En la capa de red existen muchos protocolos:
  - IP
  - ICMP
  - IGMP
  - ARP
  - Protocolos de enrutamiento.
  - IPX
  - y mas...
- Nos concentramos en IP.

# Internet Protocol (IP)

- Existen dos versiones del protocolo: **IPv4** (Usada actualmente) e **IPv6** (A la que se está migrando)
- Su función principal es el uso bidireccional en origen o destino de comunicación para transmitir datos mediante un protocolo no orientado a conexión.
- Transfiere paquetes conmutados a través de distintas redes físicas previamente enlazadas según la norma OSI de enlace de datos.

# Internet Control Message Protocol (ICMP)

- Es parte del conjunto de protocolos IP.
- Es utilizado para enviar mensajes de error e información operativa: host no localizado, servicio no está disponible, etc.
- Los mensajes del protocolo ICMP se envían a la dirección IP de origen del paquete.
- No es generalmente usado para intercambiar información entre sistemas, ni tampoco por las aplicaciones de usuario.
- ICMP para IPv4 también es conocida como **ICMPv4**. IPv6 tiene su protocolo equivalente **ICMPv6**.
- Existen herramientas de diagnóstico: ping o traceroute.

# Internet Control Message Protocol (ICMP)

Los mensajes ICMP tienen un código que indica el mensaje que quiere indicar.

Código	Descripción
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation needed, but do not fragment bit set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated error (military use only)
9	The destination network is administratively prohibited
10	The destination host is administratively prohibited
11	The network is unreachable for Type Of Service
12	The host is unreachable for Type Of Service
13	Communication administratively prohibited (administrative filtering prevents packet from being forwarded)
14	Host precedence violation (indicates the requested precedence is not permitted for the combination of host or network and port)
15	Precedence cutoff in effect (precedence of datagram is below the level set by the network administrators)



# Address Resolution Protocol (ARP)

- Cada interfaz tiene tanto una dirección IP como una dirección física MAC.
- **ARP es responsable de encontrar la dirección de hardware (MAC) que corresponde a una dirección de red (IP).**
- Tiene su par inverso que se llama Reverse ARP (RARP)
- ARP se utiliza en cuatro casos referentes a la comunicación entre dos hosts:
  - Cuando dos hosts están en la misma red y uno quiere enviar un paquete a otro.
  - Cuando dos hosts están sobre redes diferentes y deben usar un gateway o router para alcanzar otro host.
  - Cuando un router necesita enviar un paquete a un host a través de otro router.
  - Cuando un router necesita enviar un paquete a un host de la misma red.

# Internet Group Management Protocol (IGMP)

- **IP multicast** es un método para transmitir datagramas IP a un grupo de receptores interesados.
- **IGMP** se utiliza para intercambiar información acerca del estado de pertenencia entre routers IP que admiten multicast y miembros de grupos multicast.
- Los hosts miembros informan acerca de su pertenencia al grupo multicast y los enrutadores multicast sondean periódicamente el estado de la pertenencia.
- El snooping de IGMP es una actividad realizada por switches para realizar el seguimiento del intercambio de paquetes relacionados con las comunicaciones IGMP y adaptar el filtrado de paquetes de multicast.
- La última versión disponible es la IGMPv3 descrita en el [RFC 3376]

# Protocolos de enrutamiento

- Son el conjunto de reglas utilizadas por un router cuando se comunica con otros para compartir información de enrutamiento. Dicha información se usa para construir y mantener las tablas de enrutamiento.
- Existen tres tipos de enrutamiento:
  - Estático.
  - Por defecto.
  - Dinámico.

# Protocolos de enrutamiento

## Enrutamiento Estático.

- Las tablas de ruteo se llenan de forma manual en todos los routers de la red.
- Tiene el problema que los routers no pueden adaptarse por sí solos a los cambios que puedan producirse en la topología de la red.
- Resulta ventajoso en las siguientes situaciones:
  - Existe una sola conexión con un solo ISP. En lugar de conocer todas las rutas globales, se utiliza una única ruta estática.
  - Un cliente no desea intercambiar información de enrutamiento dinámico.

# Protocolos de enrutamiento

## Enrutamiento Predeterminado.

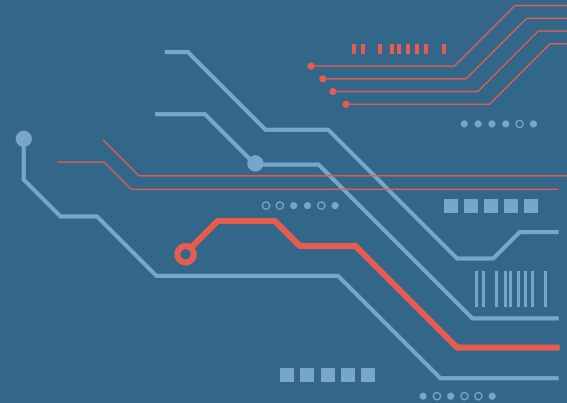
- Es una ruta estática que se refiere a una conexión de salida o Gateway de “último recurso” (Default Gateway).
- El tráfico hacia destinos desconocidos por el router se envía a dicha conexión de salida.
- Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida.

# Protocolos de enrutamiento

## Enrutamiento Dinámico.

- Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento.
- Éstos mensajes contienen información acerca de los cambios sufridos en la red para que el router actualice la tabla de enrutamiento.
- Protocolos como RIP, OSPF, IS-IS, IGRP, EIGRP y BGP son algunos ejemplos.

# IPv4 e IPv6



# IPv4: Cabecera

IPv4 es el protocolo de comunicación principal para la capa de red.

El encabezado de red tiene muchos propósitos:

- Garantiza que el paquete se envíe en la dirección correcta (al destino).
- Contiene información para el procesamiento de capas de red en varios campos.
- La información del encabezado es utilizada por todos los dispositivos de capa 3 que manejan el paquete

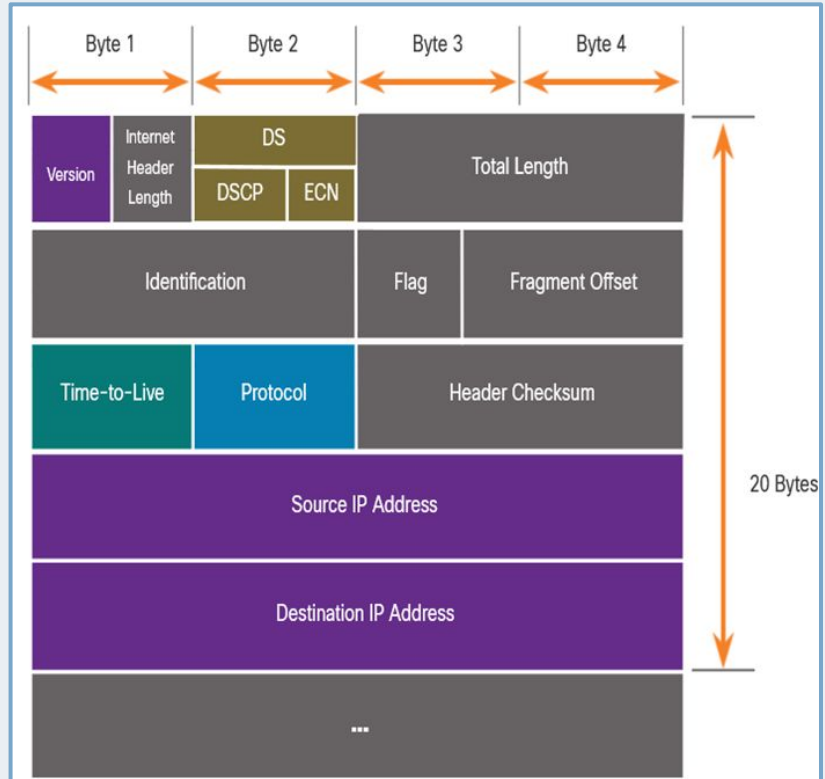


# IPv4: Campos de la cabecera

Características del encabezado de red IPv4:

- Está en binario.
- Contiene varios campos de información
- Diagrama se lee de izquierda a derecha, 4 bytes por línea
- Los dos campos más importantes son el origen y el destino.

Los protocolos pueden tener una o más funciones.



# IPv4: Campos de la cabecera

Función	Descripción
Versión	Esto será para v4, a diferencia de v6, un campo de 4 bits = 0100
Servicios diferenciados	Utilizado para QoS: campo DiffServ — DS o el anterior IntServ — ToS o Tipo de servicio
Suma de comprobación del encabezado	Detectar daños en el encabezado IPv4
Tiempo de vida (TTL) de Internet	Recuento de saltos de capa 3. Cuando se convierte en cero, el router descartará el paquete.
Dirección IPv4 de origen	Dirección de origen de 32 bits
Dirección IPV4 de destino	Dirección de destino de 32 bits

# IPv4: Limitaciones

IPv4 tiene tres limitaciones principales:

- Depleción de direcciones IPv4: Nos hemos quedado sin direccionamiento IPv4.
- Falta de conectividad de extremo a extremo: Para que IPv4 sobreviva a este largo tiempo, se crearon direcciones privadas y NAT. Esto puso fin a las comunicaciones directas con el discurso público.
- Mayor complejidad de la red:
  - NAT fue concebido como una solución temporal y crea problemas en la red como un efecto secundario de manipular los encabezados de red que direcciona.
  - NAT provoca problemas de latencia.

# IPv6: Introducción

- IPv6 fué desarrollado por IETF.
- IPv6 vence las limitaciones de IPv4.
- Mejoras que proporciona IPv6:
  - **Mayor espacio de direcciones:**  
Basado en la dirección de 128 bits, no en 32 bits.
  - **Manejo mejorado de paquetes:**  
Encabezado simplificado con menos campos.
  - **Elimina la necesidad de NAT:**  
Dado que hay gran cantidad de direcciones, no es necesario el direccionamiento privado y dirección pública compartida.

IPv4 and IPv6 Address Space Comparison

Number Name	Scientific Notation	Number of Zeros
1 Thousand	$10^3$	1,000
1 Million	$10^6$	1,000,000
1 Billion	$10^9$	1,000,000,000
1 Trillion	$10^{12}$	1,000,000,000,000
1 Quadrillion	$10^{15}$	1,000,000,000,000,000
1 Quintillion	$10^{18}$	1,000,000,000,000,000,000
1 Sextillion	$10^{21}$	1,000,000,000,000,000,000,000
1 Septillion	$10^{24}$	1,000,000,000,000,000,000,000,000
1 Octillion	$10^{27}$	1,000,000,000,000,000,000,000,000,000
1 Nonillion	$10^{30}$	1,000,000,000,000,000,000,000,000,000,000
1 Decillion	$10^{33}$	1,000,000,000,000,000,000,000,000,000,000,000
1 Undecillion	$10^{36}$	1,000,000,000,000,000,000,000,000,000,000,000,000

Legend

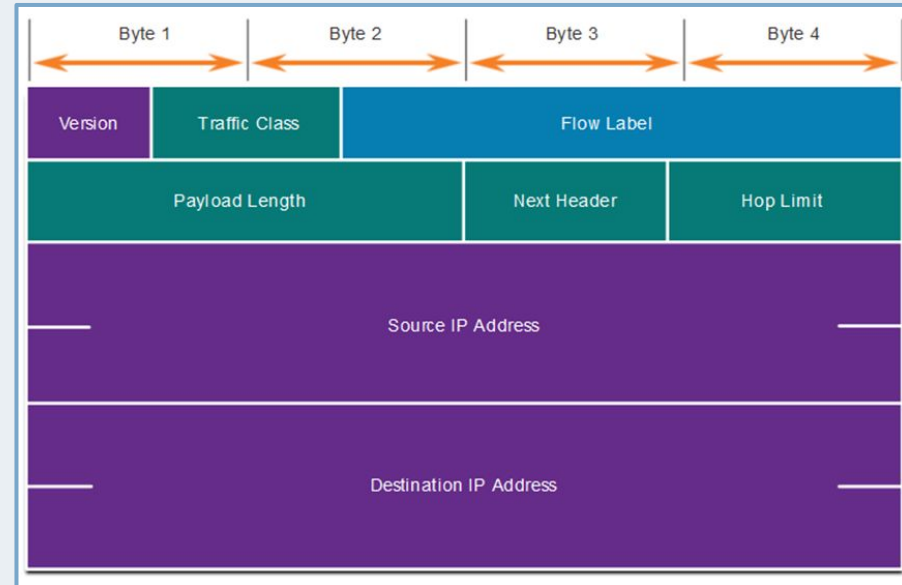


There are 4 billion IPv4 addresses

There are 340 undecillion IPv6 addresses

# IPv6: Campos de la cabecera

- El encabezado IPv6 se simplifica, pero no es más pequeño.
- El encabezado se fija en 40 octetos de longitud.
- Se eliminaron varios campos IPv4 para mejorar el rendimiento.
  - Señalador
  - Desplazamiento de fragmentos
  - Suma de comprobación del encabezado.



# IPv6: Campos de cabecera

Función	Descripción
<b>Versión</b>	Esto será para v6, a diferencia de v4, un campo de 4 bits = 0110
<b>Clase de tráfico</b>	Utilizado para QoS: Equivalente al campo DiffServ — DS
<b>Etiqueta de flujo</b>	Informa al dispositivo para manejar etiquetas de flujo idénticas de la misma manera, campo de 20 bits
<b>Longitud de carga útil</b>	Este campo de 16 bits indica la longitud de la porción de datos o la carga útil del paquete IPv6
<b>Siguiente encabezado</b>	I.D.s de siguiente nivel protocolo: ICMP, TCP, UDP, etc.
<b>Límite de saltos</b>	Reemplaza el recuento de saltos de capa 3 del campo TTL
<b>Dirección IPv4 de origen</b>	Dirección de origen de 128 bits
<b>Dirección IPV4 de destino</b>	Dirección de destino de 128 bits

# IPv6: Campos de cabecera

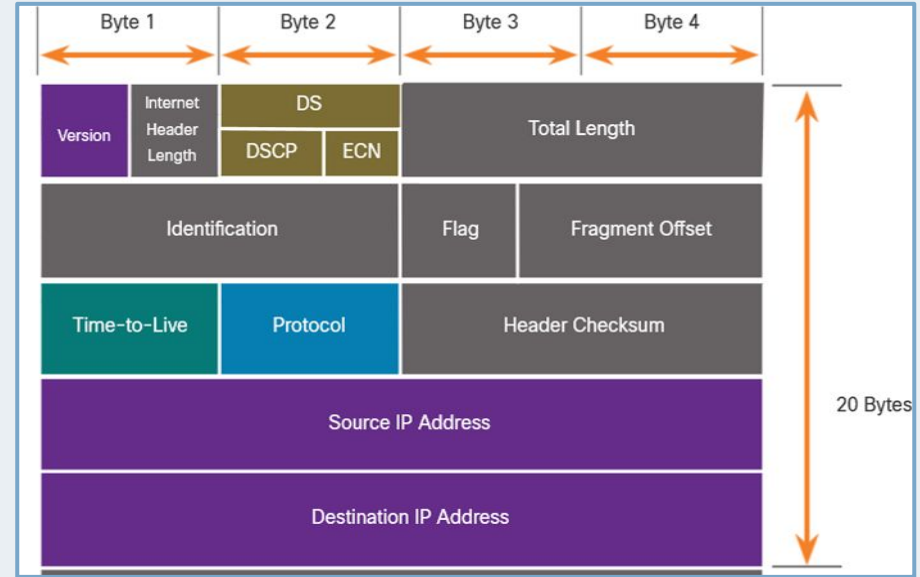
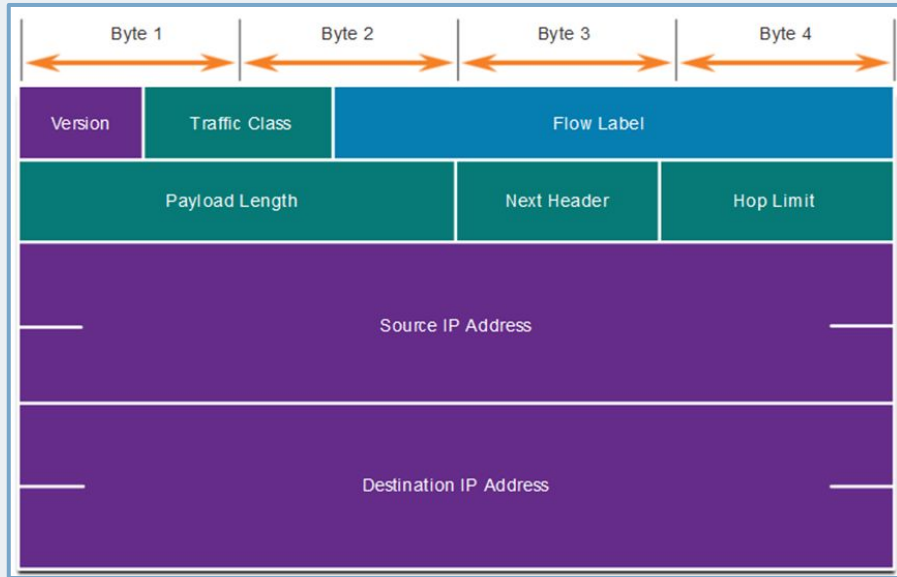
El paquete IPv6 también puede contener encabezados de extensión (EH).

Características de los encabezados EH:

- Proporcionar información de capa de red opcional
- Son opcionales
- Se colocan entre el encabezado IPv6 y la carga útil
- Puede usarse para fragmentación, seguridad, soporte de movilidad, etc.

**Nota:** a diferencia de IPv4, los routers no fragmentan los paquetes de IPv6.

# IPv4 vs IPv6

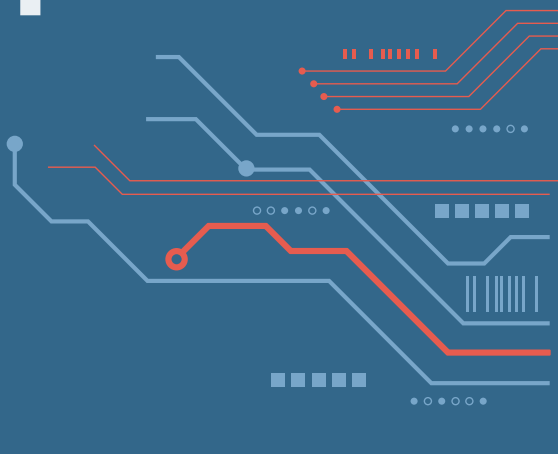






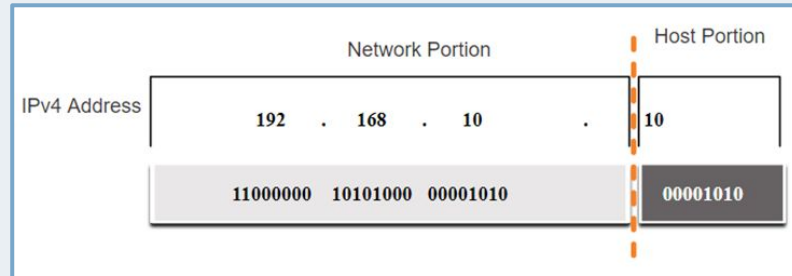
# Direcciones IPv4

Direcciones, máscara de subred, longitud de prefijo, determinación de la red, direcciones unicast/broadcast/multicast, direcciones no disponibles, direcciones públicas y privadas, asignación internacional de direcciones y división de subredes.



# Direcciones

- Las direcciones IPv4 están compuestas por cuatro octetos (8 bits = 1 Byte) separados por puntos: 32 bits en total.
- Cada octeto va desde el número 0d al 255d
- Es una dirección jerárquica que se compone de una porción de red y una porción de host.
- Al determinar la porción de red frente a la porción de host, debe mirar la secuencia de 32 bits.
- Se utiliza una máscara de subred para determinar las porciones de red y host.



# Máscara de subred

- Para identificar las porciones de red y host de una dirección, la máscara de subred se compara con la dirección bit por bit, de izquierda a derecha.
- El proceso real utilizado para identificar las porciones de red y host se llama ANDing y consiste en una multiplicación binaria.

	Network Portion			Host Portion	
IPv4 Address	192	.	168	.	10
	11000000	10101000	00001010	00001010	
Subnet Mask	255	.	255	.	0
	11111111	11111111	11111111	00000000	

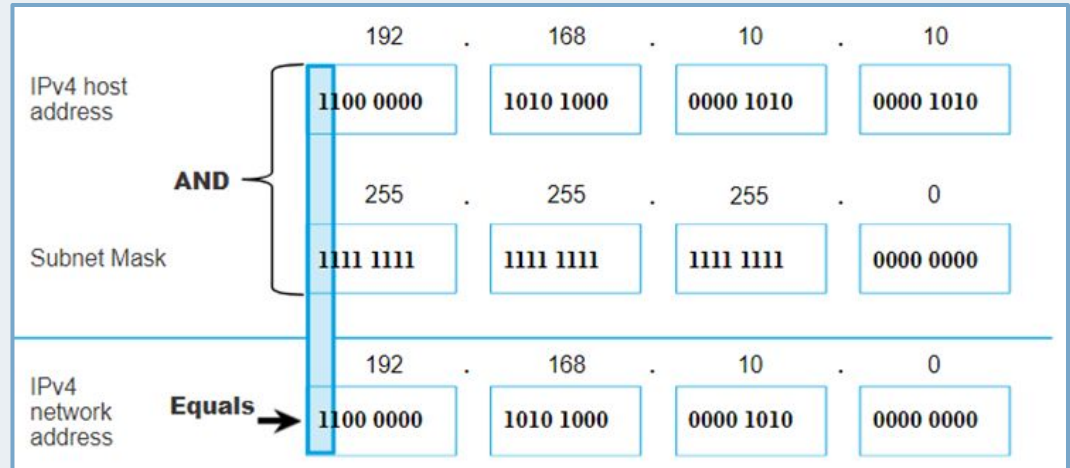
# Longitud de prefijo

- Una longitud de prefijo es un método menos engorroso utilizado para identificar una dirección de máscara de subred.
- Es el número de bits establecido en 1 en la máscara de subred.
- Está escrito en "notación de barra", por lo tanto, cuente el número de bits en la máscara de subred y añádelo con una barra.

Máscara de subred	Dirección de 32 bits	Prefijo Longitud
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

# Determinación de la red

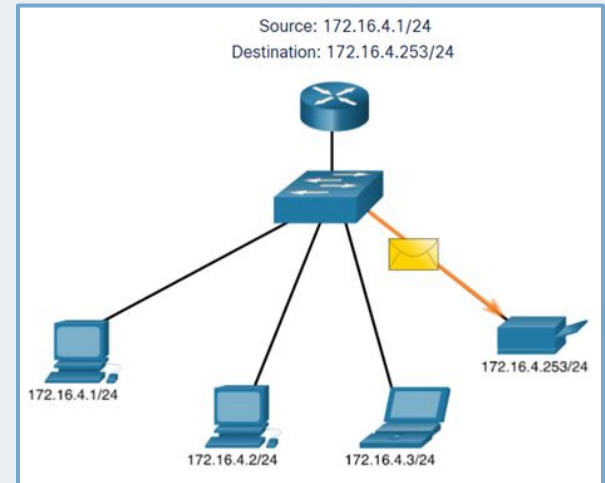
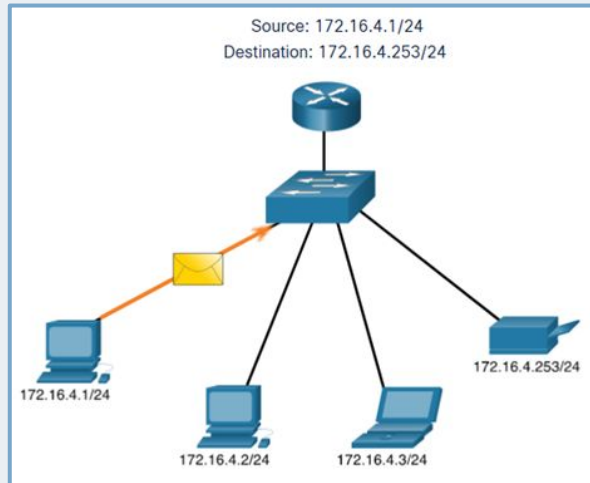
- Una operación lógica AND booleana se utiliza para determinar la dirección de red.
- La operación AND consiste en el producto de dos bit.
- Se hace un producto bit a bit entre la dirección IP y la máscara.



# IPv4 unicast, broadcast y multicast

**Unicast:** Envío de un paquete a una dirección IP de destino.

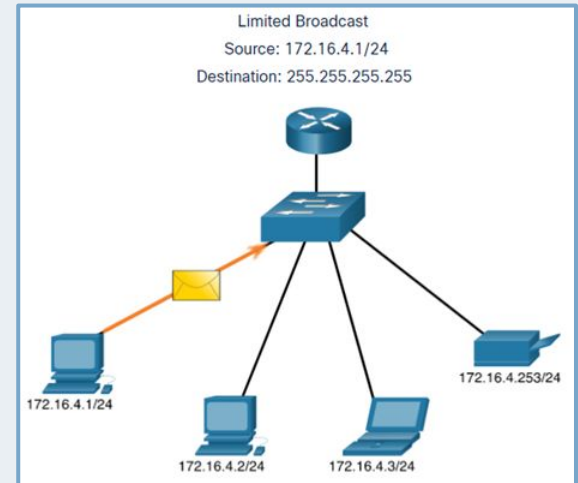
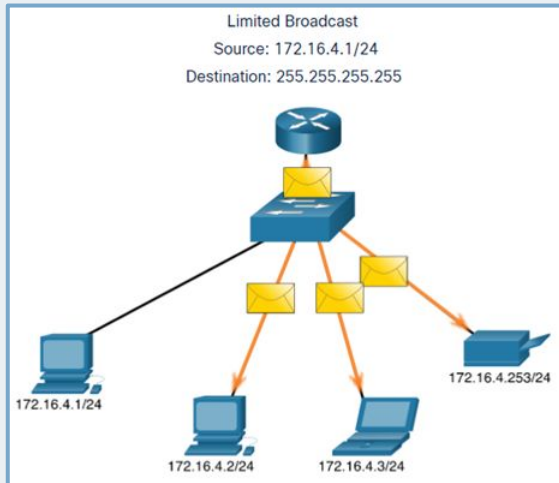
Por ejemplo, el PC en 172.16.4.1 envía un paquete unicast a la impresora en 172.16.4.253.



# IPv4 unicast, broadcast y multicast

**Broadcast:** Envío de un paquete a todas las demás direcciones IP de destino.

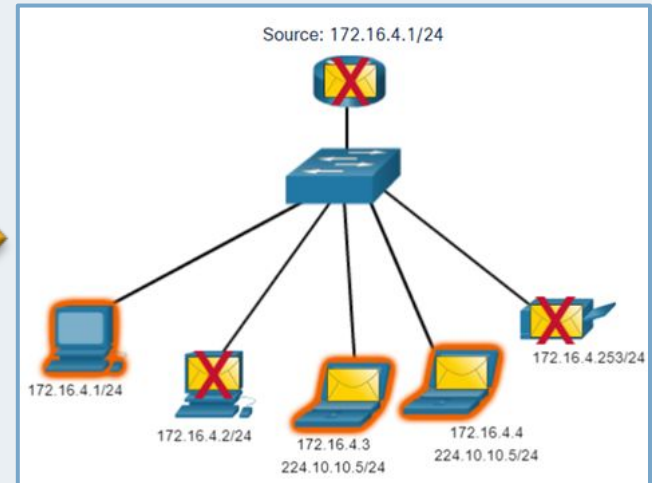
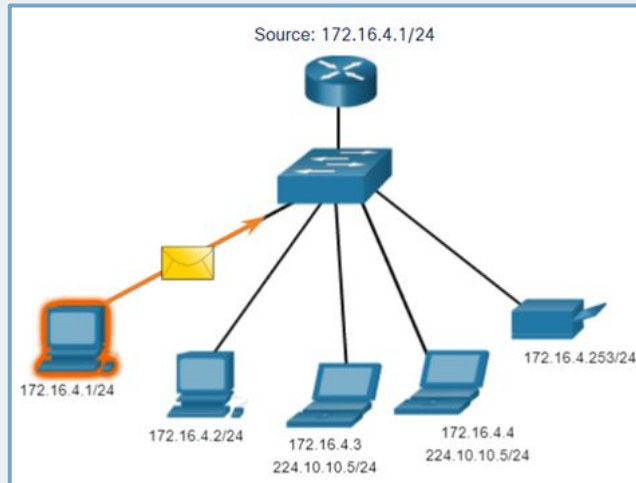
Por ejemplo, el PC en 172.16.4.1 envía un paquete broadcast a todos los hosts IPv4.



# IPv4 unicast, broadcast y multicast

**Multicast:** Envío de un paquete a un grupo de direcciones de multicast.

Por ejemplo, el PC en 172.16.4.1 envía un paquete de multicast a la dirección del grupo de multicast 224.10.10.5.





# Direcciones no disponibles

Existen dos direcciones en una subred que no se pueden asignar a ningún host:

**Dirección de la red:** Es la primera del bloque de direcciones y se usa para identificar a la red

**Dirección de broadcast:** Es la última del bloque de direcciones y se usa para envío de tráfico a toda la red.

## Ejemplos:

Host 192.168.1.25/24: 192.168.1.0 es la red y 192.168.1.255 es broadcast

Host 10.18.5.200/16: 10.18.0.0 es la red y 10.18.255.255 es broadcast

# Direcciones públicas y privadas

- Como se define en RFC 1918, las direcciones IPv4 públicas se enrutan globalmente entre routers de proveedores de servicios de Internet (ISP).
- Las direcciones privadas son bloques comunes de direcciones utilizadas por la mayoría de las organizaciones para asignar direcciones IPv4 a hosts internos.
- Las direcciones IPv4 privadas no son exclusivas y cualquier red interna puede usarlas.
- Las direcciones privadas no son enrutables globalmente.

Dirección de red y prefijo	Rango de direcciones privadas de RFC 1918
10.0.0.0/8	10.0.0.0 a 10.255.255.255
172.16.0.0/12	172.16.0.0 a 172.31.255.255
192.168.0.0/16	192.168.0.0 a 192.168.255.255

# Asignación Internacional de direcciones IP

- El Internet Assigned Numbers Authority (IANA) administra y asigna bloques de direcciones IPv4 e IPv6 a cinco Regional Internet Registry (RIR).
- Los RIR son responsables de asignar direcciones IP a los ISP que proporcionan bloques de direcciones IPv4 a ISP y organizaciones más pequeñas.



# División de subredes

- Las redes se subdividen con más facilidad en el límite del octeto de /8 /16 y /24.
- El uso de longitudes de prefijo más extensas disminuye la cantidad de hosts por subred.

Longitud de prefijo	Máscara de subred	Máscara de subred en sistema binario (n = red, h= host)	Cantidad de hosts
/8	255.0.0.0	nnnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16777214
/16	255.255.0.0	nnnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65534
/24	255.255.255.0	nnnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

# División de subredes

En la primera tabla la subred 10.0.0.0/8 se subred usando /16 y en la segunda /24.

Dirección de subred (256 subredes posibles)	Rango de host (65,534 hosts posibles por subred)	Dirección
10.0.0.0/16	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 - 10.2.255.254	10.2.255.255
10.3.0.0/16	10.3.0.1 - 10.3.255.254	10.3.255.255
10.4.0.0/16	10.4.0.1 - 10.4.255.254	10.4.255.255
10.5.0.0/16	10.5.0.1 - 10.5.255.254	10.5.255.255
10.6.0.0/16	10.6.0.1 - 10.6.255.254	10.6.255.255
10.7.0.0/16	10.7.0.1 - 10.7.255.254	10.7.255.255
...	...	...
10.255.0.0/16	10.255.0.1 - 10.255.255.254	10.255.255.255

Dirección de subred (65,536 subredes posibles)	Rango de host (254 hosts posibles por subred)	Dirección
10.0.0.0/24	10.0.0.1 - 10.0.0.254	10.0.0.255
10.0.1.0/24	10.0.1.1 - 10.0.1.254	10.0.1.255
10.0.2.0/24	10.0.2.1 - 10.0.2.254	10.0.2.255
...	...	...
10.0.255.0/24	10.0.255.1 - 10.0.255.254	10.0.255.255
10.1.0.0/24	10.1.0.1 - 10.1.0.254	10.1.0.255
10.1.1.0/24	10.1.1.1 - 10.1.1.254	10.1.1.255
10.1.2.0/24	10.1.2.1 - 10.1.2.254	10.1.2.255
...	...	...
10.100.0.0/24	10.100.0.1 - 10.100.0.254	10.100.0.255
...	...	...
10.255.255.0/24	10.255.255.1 - 10.255.255.254	10.255.255.255

# División de subredes

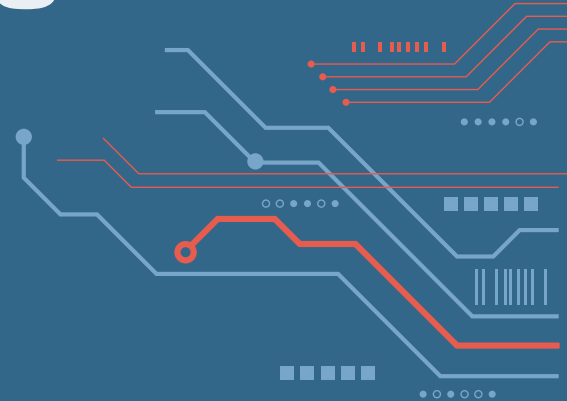
Podemos seguir subdividiendo la red usando las máscaras.

Longitud de prefijo	Máscara de subred	Máscara de subred en sistema binario (n = red, h = host)	Cantidad de subredes	Cantidad de hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2



# Direcciones IPv6

Necesidad de IPv6, coexistencia de IPv4 e IPv6, formatos de direcciones, reglas para simplificar la direcciones, longitud de prefijo, tipos de direcciones y división de subredes.



# Necesidad de IPv6

- IPv4 se está quedando sin direcciones e IPv6 es el sucesor.
- IPv6 tiene un espacio de direcciones de 128 bits mucho más grande.
- El desarrollo de IPv6 también incluyó correcciones para limitaciones de IPv4 y otras mejoras.





# Coexistencia de IPv4 e IPv6

- Tanto IPv4 como IPv6 coexisten en un futuro próximo y la transición llevará varios años.
- El IETF creó diversos protocolos y herramientas para ayudar a los administradores de redes a migrar las redes a IPv6. Las técnicas de migración pueden dividirse en tres categorías:
  - **Dual stack:** Los dispositivos ejecutan pilas de protocolos IPv4 e IPv6 de manera simultánea.
  - **Tunneling:** Es un método para transportar un paquete IPv6 a través de una red IPv4. El paquete IPv6 se encapsula dentro de un paquete IPV4.
  - **Translation:** Network Address Translation 64 (NAT64) permite que los dispositivos con IPv6 habilitado se comuniquen con dispositivos con IPv4 habilitado mediante una técnica de traducción similar a la NAT para IPv4.

**Nota:** La tunelización y la traducción son para la transición a IPv6 nativo y solo deben usarse cuando sea necesario. El objetivo debe ser las comunicaciones IPv6 nativas de origen a destino.

# Formatos de direcciones IPv6

- Las direcciones IPv6 tienen 128 bits de longitud y están escritas en hexadecimal.
- Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas.
- El formato preferido para escribir una dirección IPv6 es x: x: x: x: x: x: x: x, donde cada "x" consta de cuatro valores hexadecimales.
- En IPv6, un “hexteto” es el término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales.
- Existen reglas para simplificar la escritura de direcciones IPv6

Ejemplos de direcciones IPv6 en el formato preferido:

```
2001:0db8:0000:1111:0000:0000:0000:0200
```

```
2001:0db8:0000:00a3:abcd:0000:0000:1234
```

# Reglas para simplificar la direcciones IPv6

## Regla 1: Omitir el cero inicial

Ejemplos:

2001:0db8:0000:1111:0000:0000:0000:0200

2001: db8: 0:1111: 0: 0: 0: 200

01ab:09f0:0a00:00ab:1000:0000:0000:0af0

1ab: 9f0: a00: ab:1000: 0: 0: af0

**Nota:** Esta regla sólo es válida para los ceros iniciales, y NO para los ceros finales; de lo contrario, la dirección sería ambigua.

# Reglas para simplificar la direcciones IPv6

## Regla 2: Dos puntos dobles

Los dos puntos dobles (::) pueden reemplazar cualquier cadena única y contigua de uno o más segmentos de 16 bits (hextetos) que estén compuestas solo por ceros.

Ejemplo:

2001:0db8:0000:1111:0000:0000:0000:0200

2001: db8: 0:1111: : 200 = 2001:db8:0:1111::200

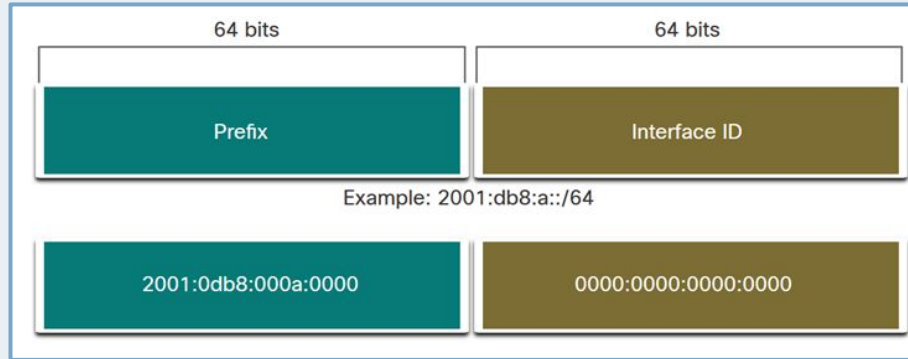
01ab:09f0:0a00:00ab:1000:0000:0000:0af0

1ab: 9f0: a00: ab:1000: : af0 = 1ab:9f0:a00:ab:1000::af0

**Nota:** Los dos puntos dobles (::) se pueden utilizar solamente una vez dentro de una dirección; de lo contrario, habría más de una dirección resultante posible.

# Longitud de prefijo IPv6

- La longitud del prefijo se representa con una barra diagonal y se usa para indicar la porción de red de una dirección IPv6.
- La longitud de prefijo puede ir de 0 a 128. La longitud de prefijo IPv6 recomendada para LAN y la mayoría de los otros tipos de redes es /64.



# Tipos de direcciones

Existen tres categorías amplias de direcciones IPv6:

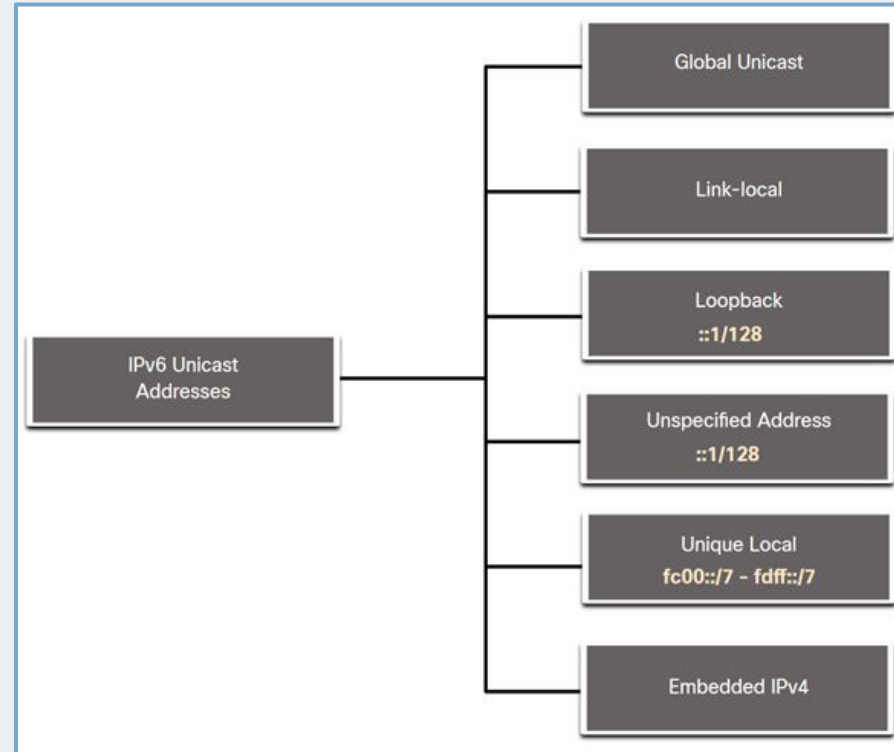
- **Unicast:** Identifica de manera única una interfaz de un dispositivo habilitado para IPv6.
- **Multicast:** Se usan para enviar un único paquete IPv6 a varios destinos.
- **Anycast:** Esta es cualquier dirección unicast de IPv6 que puede asignarse a varios dispositivos. Los paquetes enviados a una dirección de anycast se enrutan al dispositivo más cercano que tenga esa dirección.

**Nota:** A diferencia de IPv4, IPv6 no tiene una dirección broadcast. Sin embargo, existe una dirección IPv6 de multicast de todos los nodos que brinda básicamente el mismo resultado.

# Tipos de direcciones: Unicast

A diferencia de los dispositivos IPv4 que tienen una sola dirección, las direcciones IPv6 suelen tener dos direcciones unicast:

- **Global Unicast Address (GUA):** Estas son similares a las direcciones IPv4 públicas. Son direcciones enrutables de Internet globalmente exclusivas.
- **Link-local Address (LLA):** Se requiere para cada dispositivo con IPv6 y se usa para comunicarse con otros dispositivos en el mismo enlace local. Las LLAS no son enrutables y están confinadas a un único enlace.



# Tipos de direcciones: Unicast

## Estructura GUA de IPv6:

- **Prefijo de enrutamiento global:** El prefijo de enrutamiento global es la parte del prefijo, o red, de la dirección asignada por el proveedor, como un ISP, a un cliente o sitio.
- **ID de subred:** El campo ID de subred es el área entre el Prefijo de enrutamiento global y la ID de interfaz. Las organizaciones utilizan la ID de subred para identificar subredes dentro de su ubicación.
- **ID de interfaz:** La ID de interfaz IPv6 equivale a la porción de host de una dirección IPv4. Se recomienda encarecidamente que en la mayoría de los casos se utilizan subredes / 64, lo que crea una ID de interfaz de 64 bits.

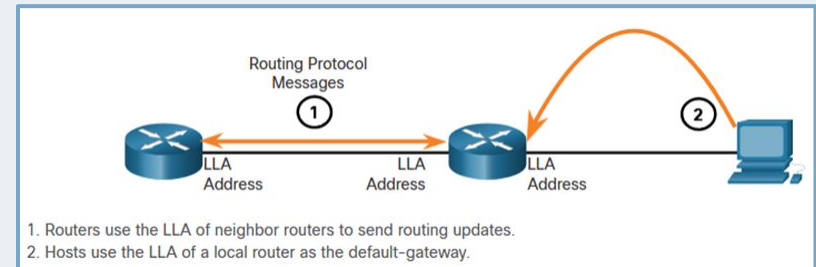


# Tipos de direcciones: Unicast

## IPv6 LLA

Una dirección local de enlace IPv6 (LLA) permite que un dispositivo se comunice con otros dispositivos habilitados para IPv6 en el mismo enlace y solo en ese enlace (subred).

- Los paquetes con una LLA de origen o destino no se pueden enrutar.
- Cada interfaz de red habilitada para IPv6 debe tener una LLA.
- Si una LLA no se configura manualmente en una interfaz, el dispositivo creará uno automáticamente.
- Las LLAS IPv6 están en el rango fe80: :/10.



# Tipos de direcciones: Multicast

Las direcciones multicast de IPv6 tienen el prefijo FF00::/8. Existen dos tipos de direcciones multicast de IPv6:

- Dirección de red multicast conocida
- Dirección multicast de nodo solicitado

**Nota:** las direcciones multicast solo pueden ser direcciones de destino y no direcciones de origen.

# Tipos de direcciones: Multicast

## Direcciones Multicast de IPv6 conocidas

Se asignan direcciones IPv6 multicast conocidas y se reservan para grupos de dispositivos predefinidos.

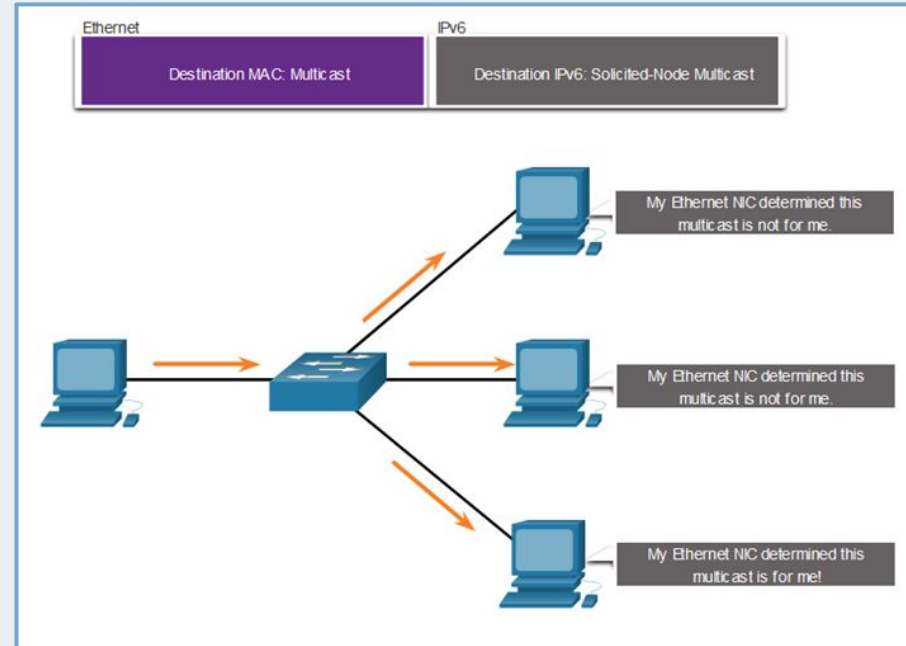
Hay dos grupos comunes de direcciones IPv6 multicast asignadas:

- **Grupo de multicast FF02::1 para todos los nodos:** Este es un grupo multicast al que se unen todos los dispositivos con IPv6 habilitado. Los paquetes que se envían a este grupo son recibidos y procesados por todas las interfaces IPv6 en el enlace o en la red.
- **ff02 :: 2 Grupo de multicast de todos los routers:** Este es un grupo multicast al que se unen todos los dispositivos con IPv6 habilitado. Un router comienza a formar parte de este grupo cuando se lo habilita como router IPv6 con el comando de configuración global `ipv6 unicast-routing`.

# Tipos de direcciones: Multicast

## Direcciones Multicast de IPv6 solicitada

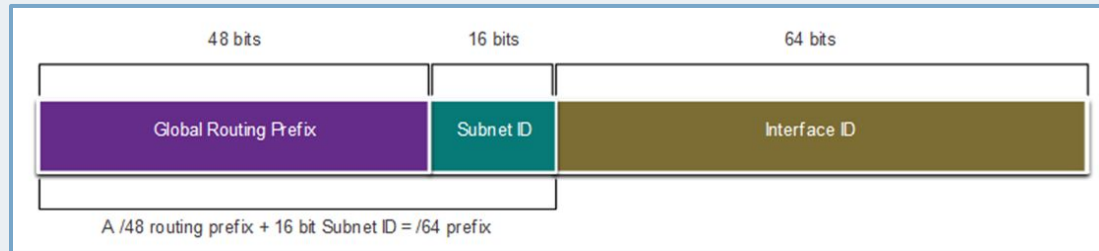
- Una dirección multicast de nodo solicitado es similar a una dirección multicast de todos los nodos.
- Una dirección multicast de nodo solicitado se asigna a una dirección especial de multicast de Ethernet.
- Esto permite que la NIC Ethernet filtre la trama al examinar la dirección MAC de destino sin enviarla al proceso de IPv6 para ver si el dispositivo es el objetivo previsto del paquete IPv6.



# División de subredes IPv6

IPv6 se diseñó teniendo en cuenta las subredes.

- Se utiliza un campo ID de subred independiente en IPv6 GUA para crear subredes.
- El campo ID de subred es el área entre el Prefijo de enrutamiento global y la ID de interfaz.

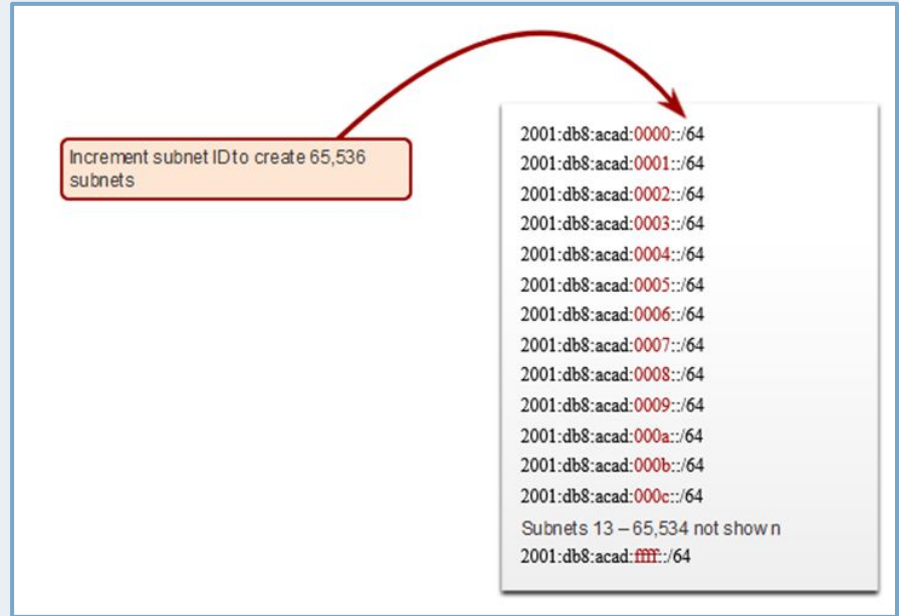


# División de subredes IPv6

## Ejemplo:

Dado el prefijo de enrutamiento global 2001:db8:acad: :/48 con un ID de subred de 16 bits.

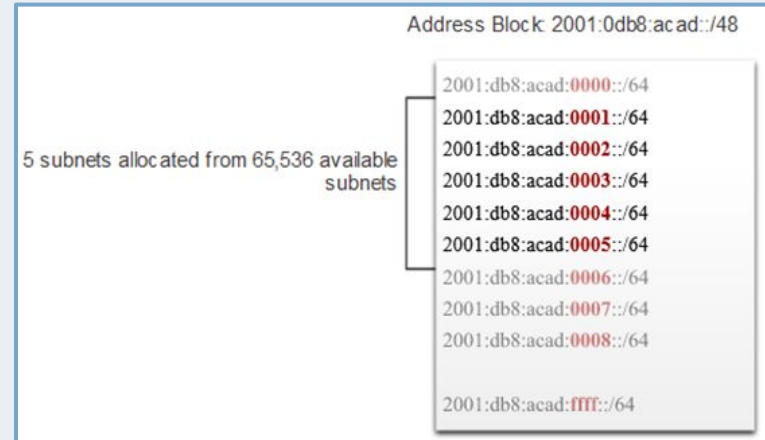
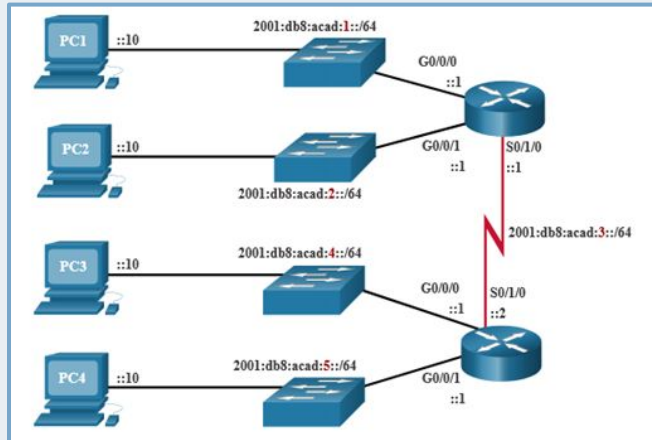
- Permite 65.536 /64 subredes
- El prefijo de enrutamiento global es igual para todas las subredes.
- Solo se incrementa el hexteto de la ID de subred en sistema hexadecimal para cada subred.



# Asignación de subred IPv6

La topología de ejemplo requiere cinco subredes, una para cada LAN, así como para el enlace en serie entre R1 y R2.

Se asignaron las cinco subredes IPv6, con el campo ID de subred 0001 a 0005. Cada subred /64 proporcionará más direcciones de las que jamás se necesitarán.



# RECURSOS BIBLIOGRÁFICOS

- Cisco NetAcad Introduction to Networks:
  - Módulo 8: “Capa de red”
- Redes de Computadoras | Tannenbaum - Wetherall (2012) | 5ta Edición WordPress:
  - Capítulo 5, párrafo 1: “Aspectos de diseño de la capa de red”
  - Capítulo 5, párrafo 6: “La capa de red de Internet”
- Comunicaciones y Redes de Computadores | Stallings (2018) | 7ma Edición Pearson
  - Capítulo 15: “Protocolo de interconexión de redes”