

# **NIVEL DE RED DIRECCIONAMIENTO IP**



# CONTENIDOS

- Nivel de red
  - Introducción
  - Objetivo
  - Funciones
  - Protocolos
  - Operaciones básicas
  - Encapsulación IP
- Protocolo IP
  - Características
  - Paquete IPv4
    - Formato
    - Ejemplo
  - Limitaciones IPv4
  - Paquete IPv6
    - Formato
    - Ejemplo
- Direccionamiento IPv4
  - Tipos de direcciones
  - Clases
  - Direcciones reservadas
  - Direcciones especiales
  - Direcciones públicas
  - Direcciones privadas
  - Máscara de subred
- Subredes
  - Necesidad
  - Subnetting
  - Ejemplos
- Protocolo ARP
  - Introducción
  - Funciones
  - Solicitud
  - Respuesta
  - Tablas ARP
  - Comandos
- Protocolo ICMP
  - Introduccion
  - Mensajes ICMP
  - Formato
- Direccionamiento IPv6

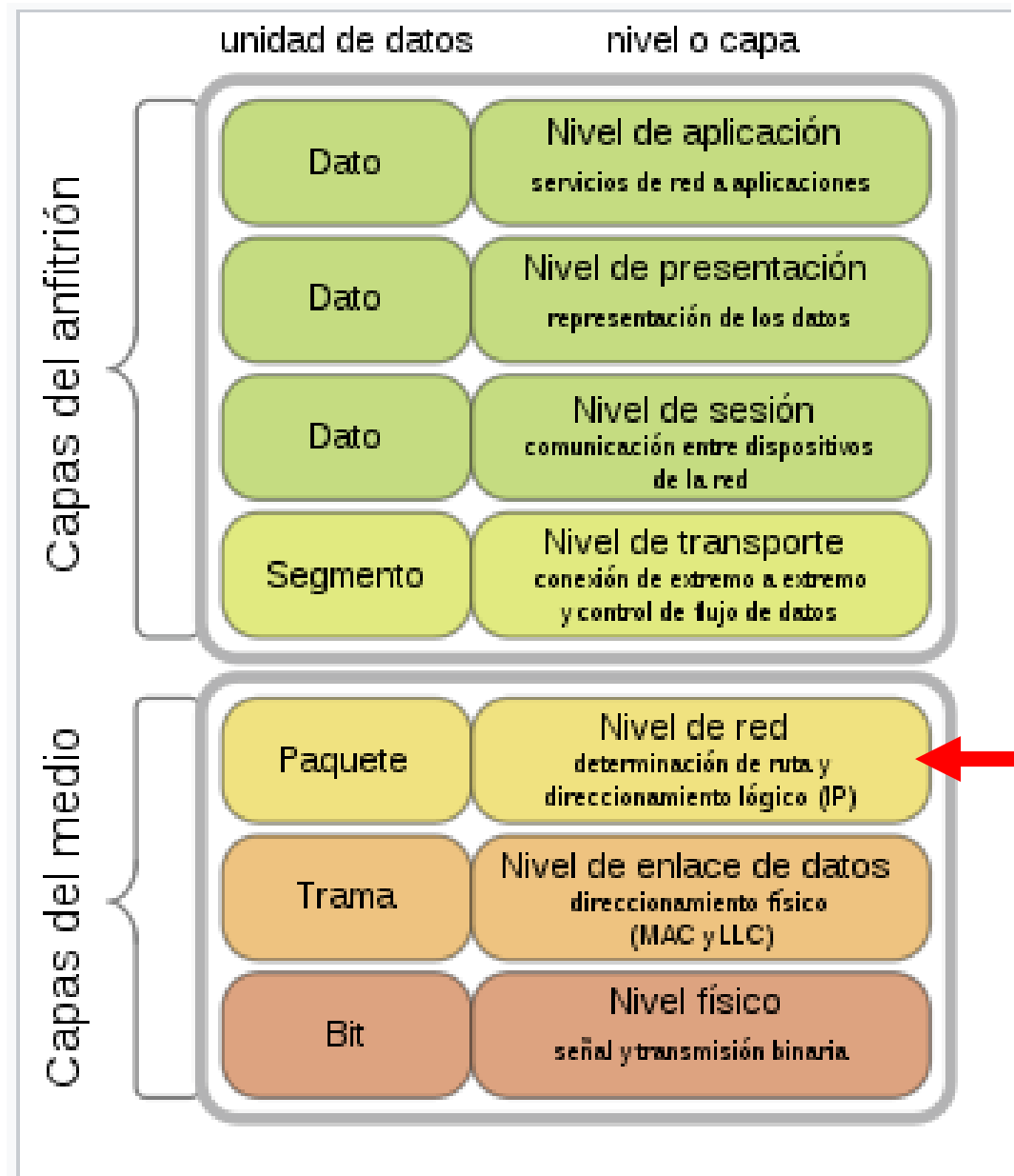


# NIVEL DE RED



# INTRODUCCIÓN

- Capa 3 del modelo OSI



# OBJETIVO

- El nivel de red es el tercer nivel del modelo OSI y se encarga de llegar los paquetes entre hosts, los cuales pueden estar ubicados en redes geográficamente distintas.
- Similitud: envío de una carta por correo ordinario sin acuse de recibo
- El nivel de red no sabe si el paquete ha llegado a su destino, esta función pertenece al nivel de transporte



# FUNCIONES

- Las funciones principales del nivel de red son

## Direccionamiento IP

- Consiste en asignar direcciones IP Únicas a cada equipo en Internet o la intranet privada
- También conocido como direccionamiento lógico

## Enrutamiento de paquetes

- Encontrar el camino óptimo entre un origen y destino
- Las técnicas de enrutamiento se basan en el estado de la red que es variable, por lo que las decisiones tomadas respecto a los paquetes de la misma conexión pueden variar en cada instante.
- Por tanto, los paquetes pueden seguir distintas rutas y llegar desordenados.

## Encapsulación de segmentos y desencapsulación de tramas

- El host emisor, en el nivel de aplicación proporciona un mensaje para enviar a otro host.
- El nivel de transporte recibe el mensaje y lo divide en segmentos
- El nivel de red recibe el segmento y lo encapsula en un paquete, añadiendo la cabecera con las direcciones IP origen y destino.
- El paquete atraviesa diferentes routers hasta su destino. Será el nivel de red quién selecciona la mejor ruta.
- Una vez en el host destino, el nivel de red desencapsula la trama para entregar el paquete al nivel de transporte

## Control de congestión

- La congestión se produce cuando un router recibe más tráfico del que puede procesar
- Para evitar esta situación, hay ciertas técnicas de prevención y control que se aplican en el nivel de red



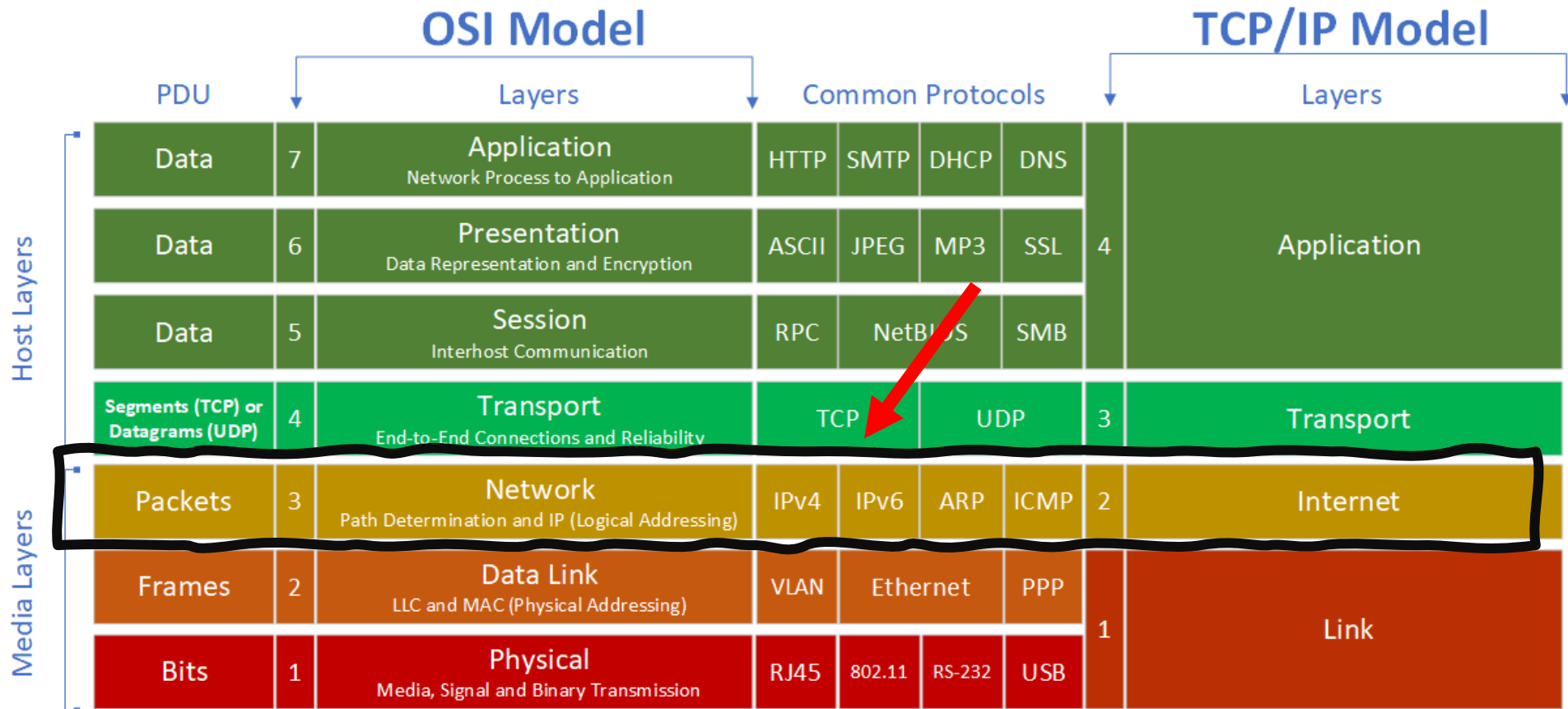
# PROTOS

- En este nivel se distinguen protocolos como:
  - Direccinamiento y encapsulamiento: IP (IPv4, IPv6)
  - Resolucin de direcciones: ARP, RARP
  - Diagnstico de red: ICMP (ICMPv4, ICMPv6)
  - Enrutamiento: RIP (RIPv1, RIPv2), OSPF, IS-IS, BGP, EIGRP
  - Seguridad: IPSec
  - Control de congestin: ENC

A lo largo de este  
mdulo se estudiarán  
estos protocolos



# PROTOCOLS





# OPERACIONES BÁSICAS

- Para lograr una **comunicación end-to-end**, los protocolos de la capa de red realizan cuatro operaciones básicas

## Direccionamiento de dispositivos finales

- Los dispositivos finales deben configurarse con una **dirección IP** única para la identificación en la red.

## Encapsulación

- La capa de red **encapsula** la unidad de datos de protocolo (PDU) de la capa de transporte en un **paquete**.
- El proceso de encapsulamiento agrega información de encabezado IP, como la dirección IP de los hosts de origen y de destino.
- El **proceso de encapsulación** lo realiza el origen del paquete IP.

## Enrutamiento

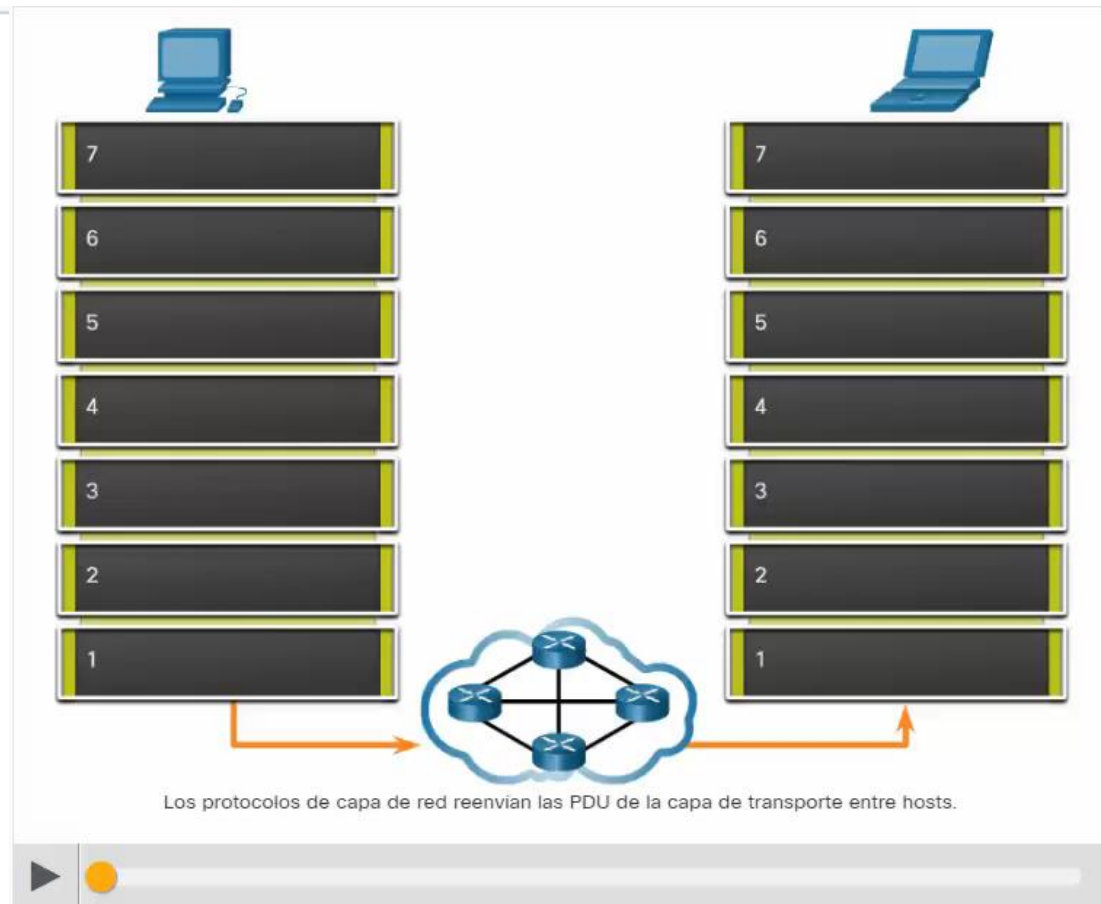
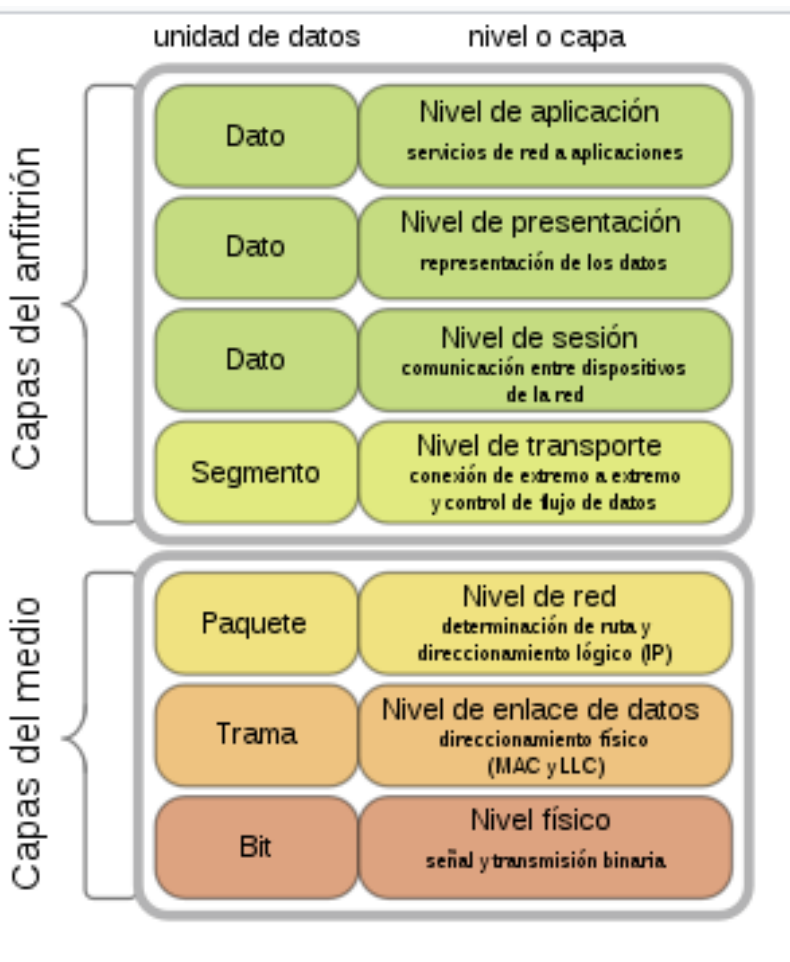
- La capa de red proporciona servicios para **dirigir los paquetes a un host de destino en otra red**.
- Para transferir un paquete a otras redes, debe procesarlo un **router** encargado de seleccionar la mejor ruta y dirigir los paquetes al host de destino en un proceso que se denomina **"enrutamiento"**.
- Un paquete puede cruzar muchos routers antes de llegar al host de destino. Se denomina **"salto"** a cada router que cruza un paquete antes de alcanzar el host de destino.

## Desencapsulación

- Cuando el paquete llega a la capa de red del host de destino, el host verifica el encabezado IP del paquete.
- Si la dirección IP de destino dentro del encabezado coincide con su propia dirección IP, se elimina el encabezado IP del paquete.
- Una vez que la capa de red desencapsula el paquete, la PDU de capa 4 que se obtiene se transfiere al servicio apropiado en la capa de transporte.
- El **proceso de desencapsulación** lo realiza el host de destino del paquete IP.

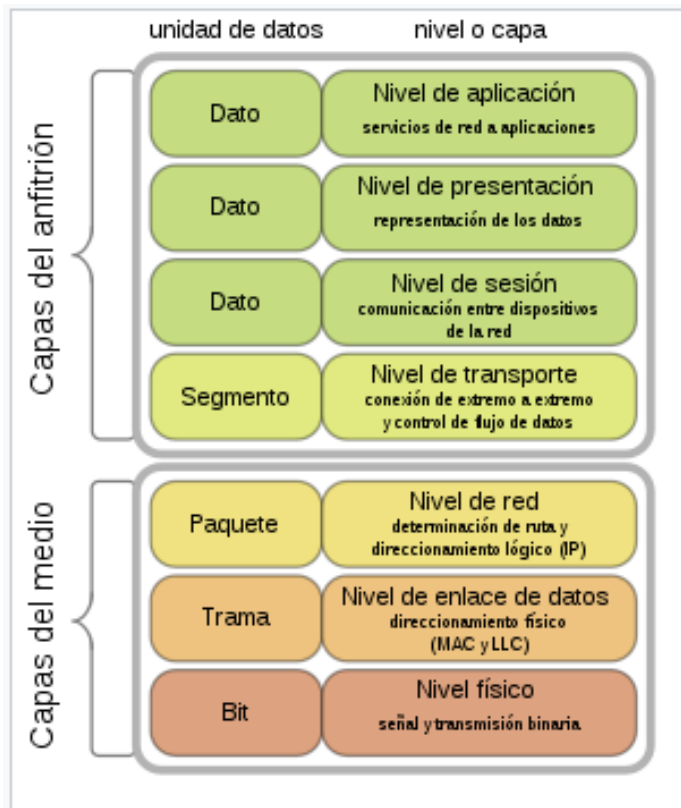


# COMUNICACIÓN END-TO-END



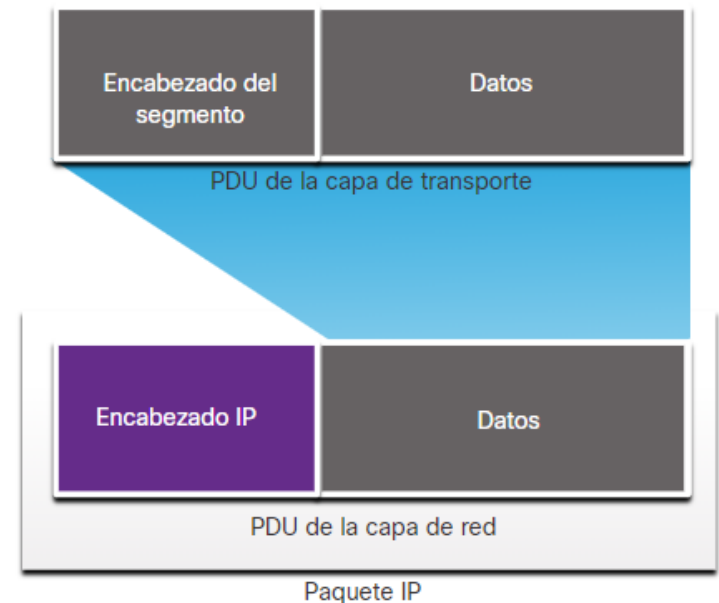
# ENCAPSULACIÓN IP

- IP encapsula el segmento de la capa de transporte (la capa justo por encima de la capa de red) u otros datos agregando un encabezado IP. El encabezado IP se usa para entregar el paquete al host de destino.



Encapsulamiento de la capa de transporte

Encapsulamiento de la capa de red



# ENCAPSULACIÓN IP



¿Para qué sirve la encapsulación? ¿Qué nos aporta?



# ENCAPSULACIÓN IP

- El proceso de encapsulamiento de datos capa por capa **permite que se desarrollen y se escalen los servicios en las diferentes capas sin afectar a las otras capas.**
- Esto significa que IPv4 o IPv6 o cualquier protocolo nuevo que se desarrolle en el futuro puede armar sin inconvenientes un paquete con los segmentos de capa de transporte.
- El encabezado IP es examinado por dispositivos de Capa 3 (es decir, routers y switches de Capa 3) a medida que viaja a través de una red a su destino.
- Los routers implementan protocolos de enrutamiento para enrutar paquetes entre redes. El enrutamiento realizado por estos dispositivos intermediarios examina el direccionamiento de la capa de red en el encabezado del paquete. En todos los casos, la porción de datos del paquete, es decir, la PDU de la capa de transporte encapsulada u otros datos, permanece sin cambios durante los procesos de la capa de red.
- Nota: los protocolos de enrutamiento se verán en otro módulo



# PROTOCOLLO IP



# CARACTERÍSTICAS DEL PROTOCOLO IP

- IP se diseñó como un protocolo con sobrecarga baja.
- Provee solo las funciones necesarias para enviar un paquete de un origen a un destino a través de un sistema interconectado de redes.
- El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones, si es necesario, están a cargo de otros protocolos en otras capas, principalmente TCP en la capa 4.
- Estas son las **características básicas** de la propiedad intelectual:
  - **No orientado a conexión:** porque cada paquete puede viajar por caminos distintos
  - **No fiable:** porque los paquetes pueden perderse, dañarse o llegar desordenados
  - **Medios independientes:** la operación es independiente del medio (es decir, cobre, fibra óptica o inalámbrico) que transporta los datos.



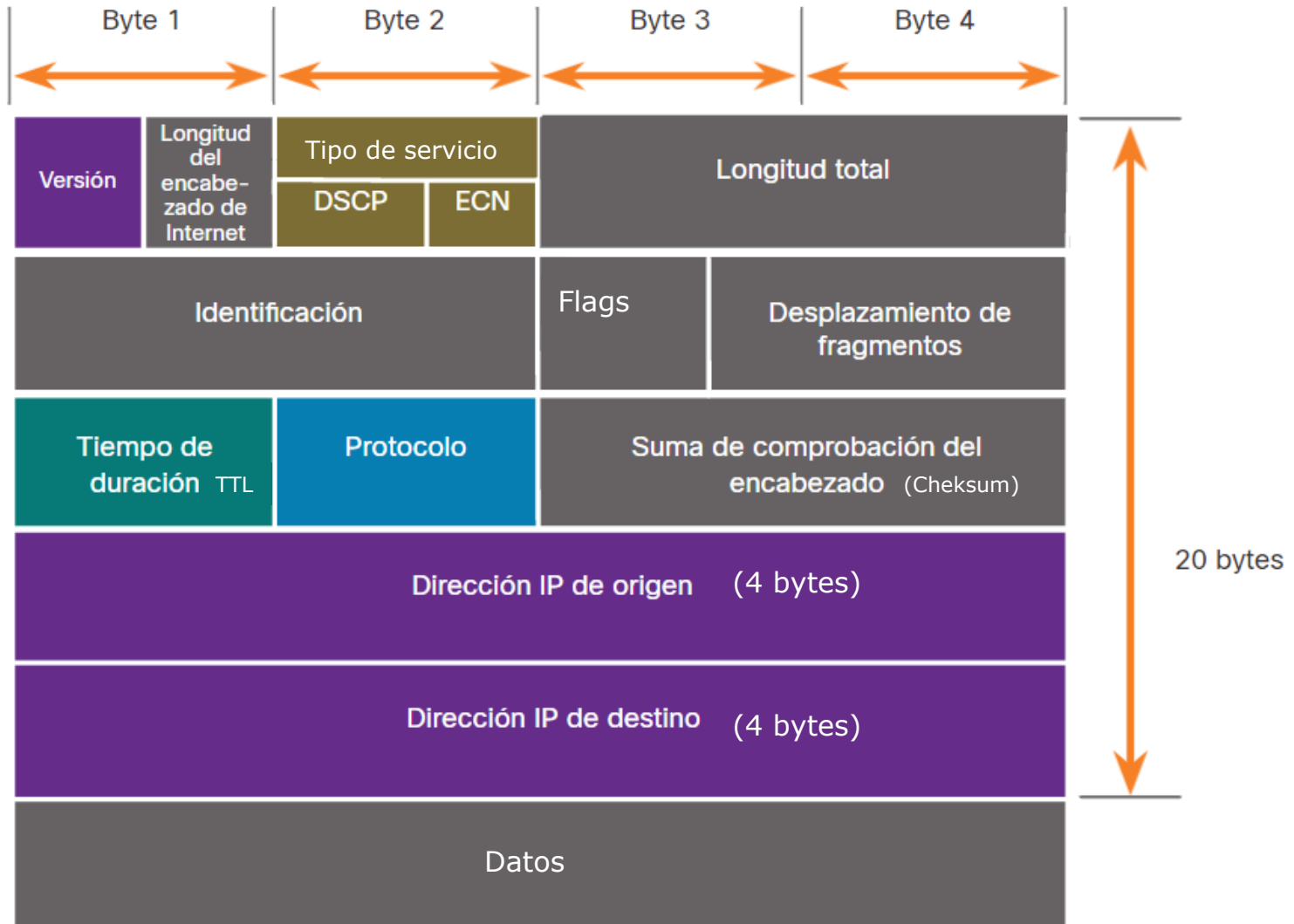
# PAQUETE IPV4

- IPv4 es uno de los protocolos de comunicación de la capa de red principal.
- El encabezado del paquete IPv4 se utiliza para garantizar que este paquete se entrega en su siguiente parada en el camino a su dispositivo final de destino.
- El encabezado de paquetes IPv4 consta de campos que contienen información importante sobre el paquete. Estos campos tienen números binarios que examinan el proceso de capa 3.





# PAQUETE IPV4: FORMATO



# PAQUETE IPV4: FORMATO

Los campos más significativos son:

- **Versión:** contiene un valor binario de 4 bits establecido en 0100 que identifica como paquete IPv4
- **Tipo de servicio:** campo de 8 bits que se utiliza para determinar la prioridad del paquete. Los seis bits más significativos del campo son los bits de punto de código de servicios diferenciados (DSCP) y los dos últimos bits son de notificación de congestión explícita (ECN)
- **Suma de comprobación de encabezado:** se utiliza para detectar los daños en el encabezado IPv4
- **Protocolo:** este campo se utiliza para identificar el protocolo del siguiente nivel. ICMP(1), TCP(6) y UDP(17)
- **Dirección IPv4 de origen:** valor binario de 32 bits con la dirección origen. La dirección IPv4 de origen es siempre una dirección unicast
- **Dirección IPv4 de destino:** valor binario de 32 bits con la dirección destino del paquete. LA dirección destino IPv4 es una dirección unicast, multicast o de difusión



# EJEMPLO DIRECCIÓN IPV4

## Video – Sample IPv4 Headers in Wireshark

This video will cover the following:

- IPv4 Ethernet packets in Wireshark
- The control information
- The difference between packets



# LIMITACIONES IPV4

- IPv4 todavía está en uso hoy en día pero IPv6 reemplazará a IPv4..
- IPv4 aún tiene tres grandes problemas:
  - **Agotamiento de la dirección IPv4:**
    - número limitado de direcciones públicas únicas disponibles.
    - hay aproximadamente 4000 millones de direcciones IPv4, el incremento en la cantidad de dispositivos nuevos con IP habilitado, las conexiones constantes y el crecimiento potencial de regiones menos desarrolladas aumentaron la necesidad de direcciones.
  - **Falta de conectividad de extremo a extremo:**
    - La traducción de direcciones de red (NAT) es una tecnología comúnmente implementada dentro de las redes IPv4.
    - NAT proporciona una manera para que varios dispositivos compartan una única dirección IPv4 pública. Sin embargo, dado que la dirección IPv4 pública se comparte, se oculta la dirección IPv4 de un host de la red interna. Esto puede ser un problema para las tecnologías que necesitan conectividad completa.
  - **Mayor complejidad de la red:**
    - mientras que NAT ha ampliado la vida útil de IPv4, solo se trataba de un mecanismo de transición a IPv6.
    - NAT en sus diversas implementaciones crea una complejidad adicional en la red, creando latencia y haciendo más difícil la solución de problemas.



# COMPARACIÓN ESPACIO DIRECCIONES

- Comparación del espacio de direcciones IPv4 e IPv6

| Nombre del número | Notación científica | Cantidad de ceros                     |
|-------------------|---------------------|---------------------------------------|
| Mil               | $10^3$              | 1000                                  |
| 1 millón          | $10^6$              | 1 000000                              |
| 1000 millones     | $10^9$              | 1000000000                            |
| 1 billón          | $10^{12}$           | 1000000000000                         |
| 1000 billones     | $10^{15}$           | 1000000000000000                      |
| 1 trillón         | $10^{18}$           | 1000000000000000000                   |
| 1000 trillones    | $10^{21}$           | 1000000000000000000000                |
| 1 cuatrillón      | $10^{24}$           | 1000000000000000000000000             |
| 1000 cuatrillones | $10^{27}$           | 1000000000000000000000000000          |
| 1 quintillón      | $10^{30}$           | 1000000000000000000000000000000       |
| 1000 quintillones | $10^{33}$           | 1000000000000000000000000000000000    |
| 1 sextillón       | $10^{36}$           | 1000000000000000000000000000000000000 |

## Leyenda



Hay 4000 millones de direcciones IPv4.

Hay 340 sextillones de direcciones IPv6.

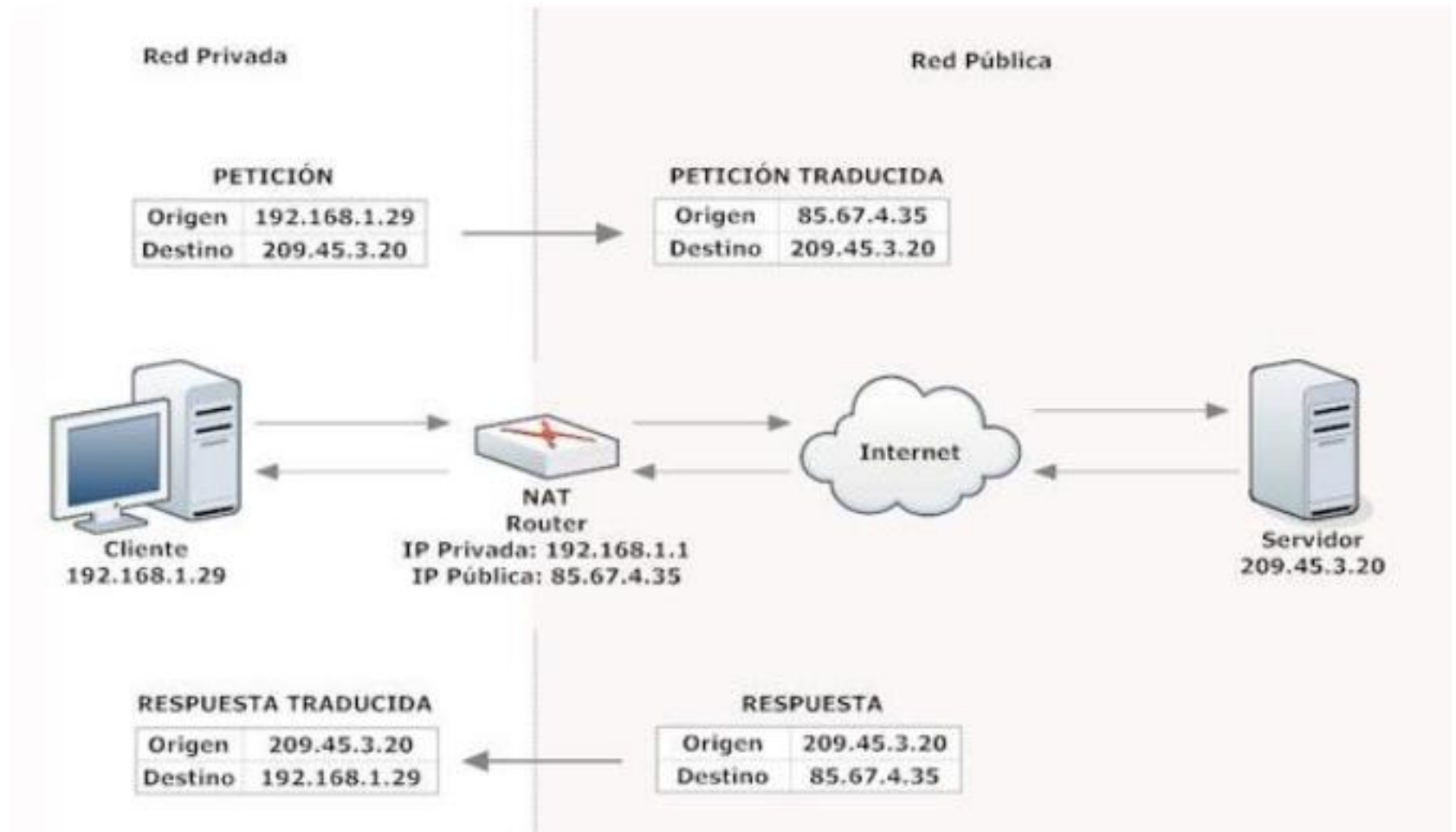


# ANTES DE CONTINUAR... QUÉ ES NAT

- Network Address Translation (o Traducción de direcciones de red) NAT
- Solución al problema de la escasez de direcciones IP públicas
- Hacer que redes de ordenadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten a Internet usando una única dirección IP (IP pública). Gracias a este “parche”, las grandes empresas sólo utilizarían una dirección IP y no tantas como máquinas hubiese en dicha empresa. También se utiliza para conectar redes domésticas a Internet.



# ANTES DE CONTINUAR... QUÉ ES NAT



# PAQUETE IPV6

- A principios de la década de 1990, los problemas con IPv4 preocuparon al Grupo de trabajo de ingeniería de Internet (IETF) que, en consecuencia, comenzó a buscar un reemplazo.
- Esto tuvo como resultado el desarrollo de IP versión 6 (IPv6).
- IPv6 supera las limitaciones de IPv4 y representa una mejora importante con características que se adaptan mejor a las demandas de red actuales y previsibles.



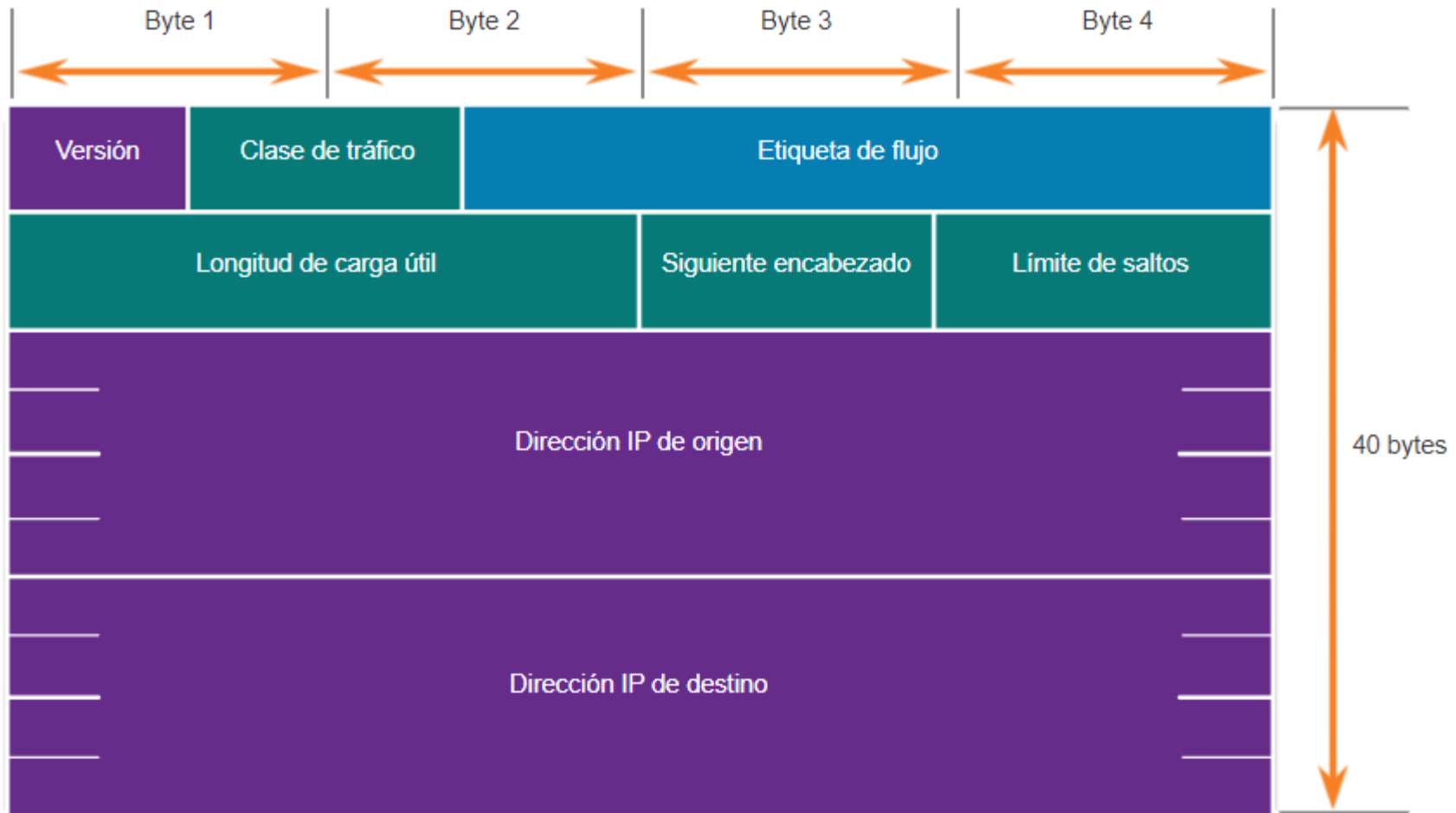


# PAQUETE IPV6


- Las mejoras que ofrece IPv6 incluyen las siguientes:
  - Manejo de paquetes mejorado:
    - las direcciones IPv6 se basan en el direccionamiento de 128 bits en lugar de IPv4 con 32 bits.
    - el encabezado IPv6 se ha simplificado con menos campos.
  - Elimina la necesidad de NAT:
    - Elimina la necesidad de NAT: con una cantidad tan grande de direcciones IPv6 públicas, no se necesita NAT entre una dirección IPv4 privada y una IPv4 pública.
    - Esto evita algunos de los problemas inducidos por NAT que experimentan las aplicaciones que requieren conectividad de extremo a extremo.





# PAQUETE IPV6



## Leyenda

 - Nombre de los campos guardados de IPv4 a IPv6

 - Cambian el nombre y la posición en IPv6

 - Nuevo campo en IPv6



# PAQUETE IPV6: FORMATO

Los campos más significativos son:

- **Versión:** contiene un valor binario de 4 bits establecido en 0110 que identifica como paquete IPv6
- **Clase de tráfico:** campo de 8 bits equivalente al campo de Tipo de servicios
- **Etiquetas de flujo:** campo de 20 bits sugiere que todos los paquetes con la misma etiqueta de flujo reciben el mismo tipo de manejo de routers
- **Longitud de carga útil:** campo de 16 bits indica la longitud de la porción de datos o carga útil del paquete IPv6. Esto no incluye la longitud del encabezado del paquete (que es de un tamaño fijo de 40 bytes)
- **Encabezado siguiente:** campo de 8 bits que es equivalente al campo de Protocolo en el paquete IPv4. Indica el tipo de datos que lleva el paquete.
- **Límite de salto:** campo de 8 bits que reemplaza al campo TTL del paquete IPv4
- **Dirección IPv6 de origen:** valor binario de 128 bits con la dirección origen.
- **Dirección IPv6 de destino:** valor binario de 128 bits con la dirección destino del paquete.



# EJEMPLO DIRECCIÓN IPV6

## Video – Sample IPv6 Headers in Wireshark

This video will cover the following:

- IPv6 Ethernet packets in Wireshark
- The control information
- The difference between packets



# DIRECCIONAMIENTO IPV4



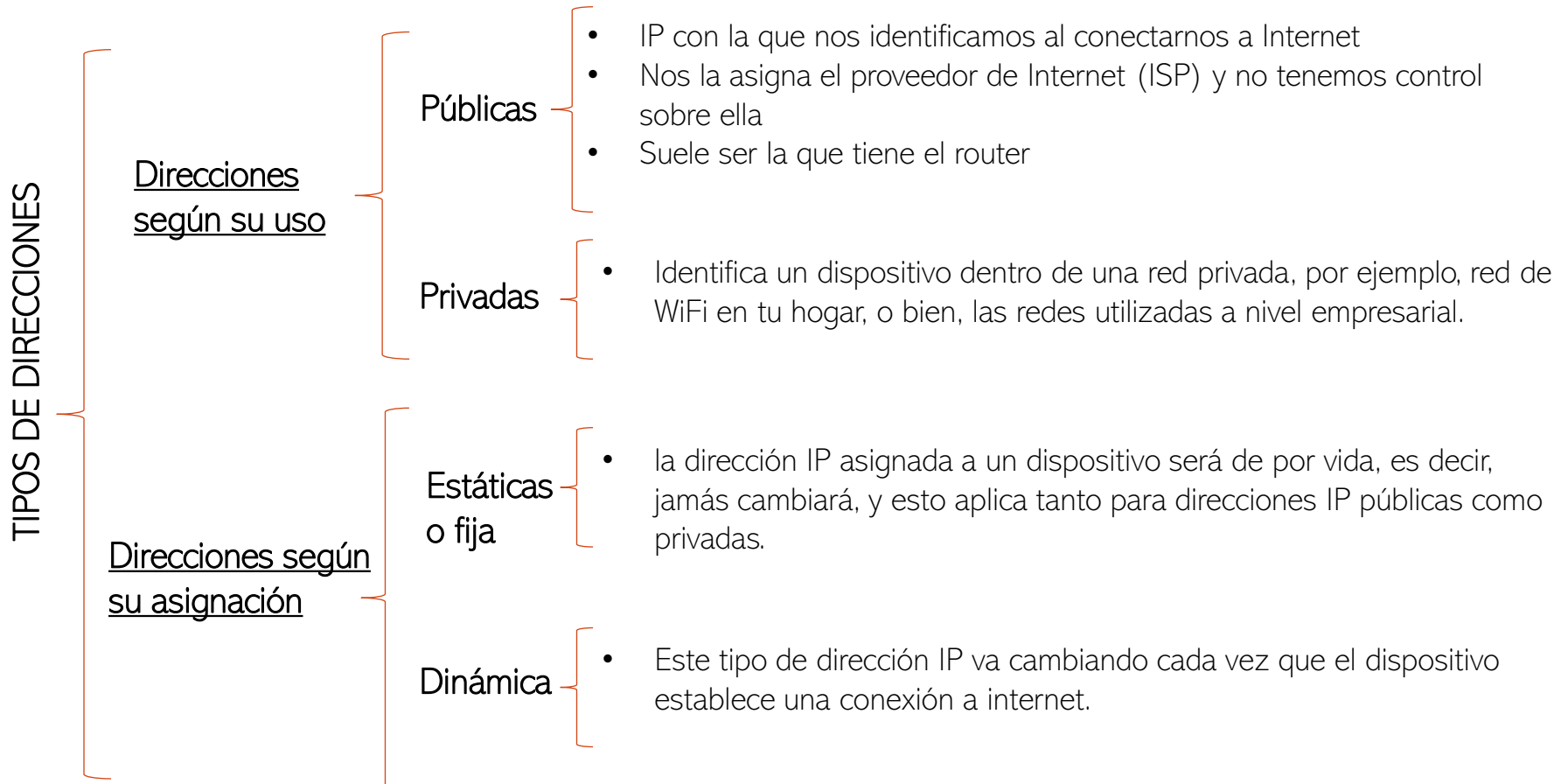
# DIRECCIONES IPV4

- La dirección lógica o dirección IPv4, identifica de forma única la conexión de un equipo a la red.
- Direcciones de 4 bytes -> 32 bits que se escriben en notación decimal con punto
- Ejemplo: 192.168.1.10



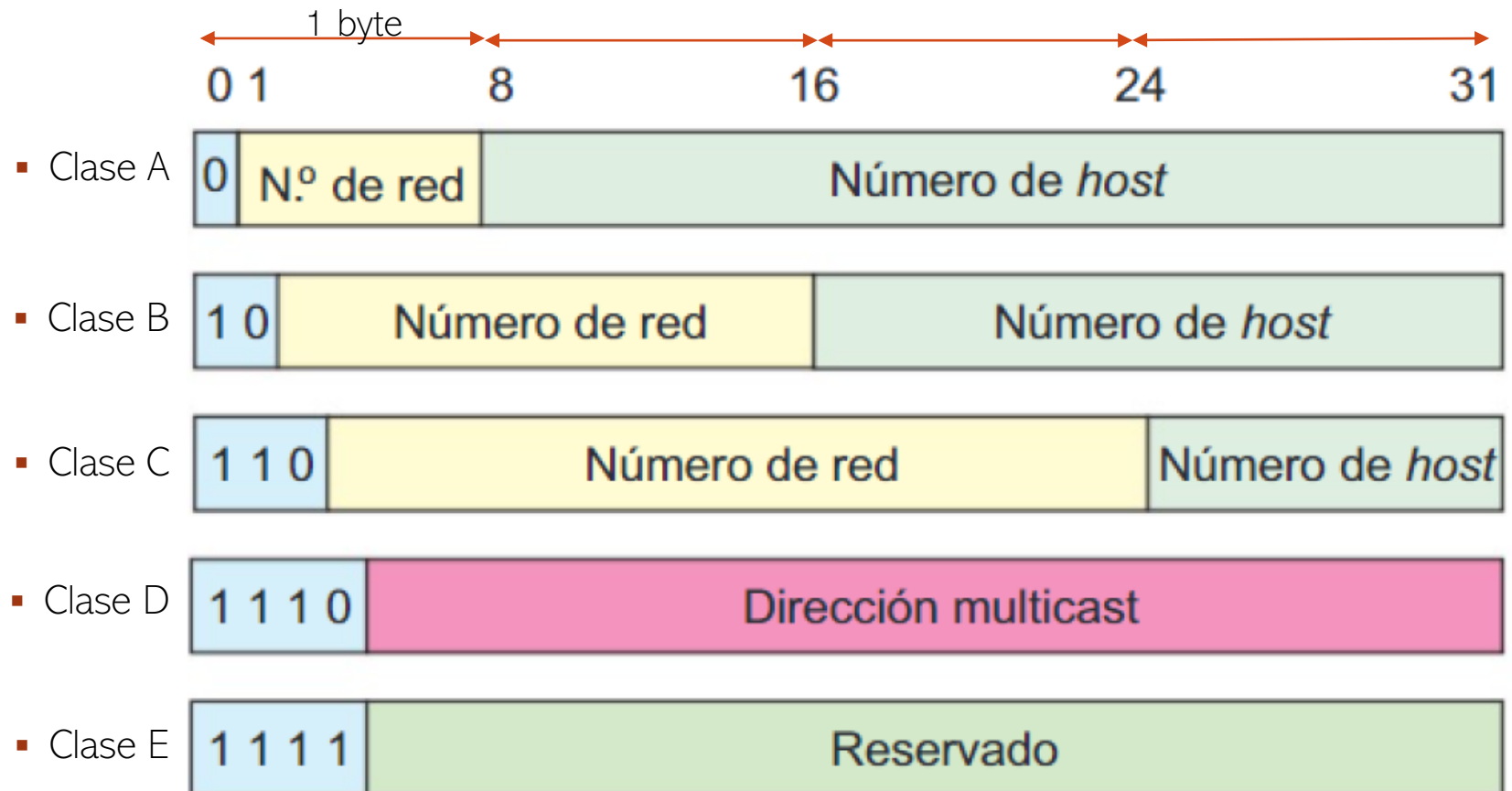
# TIPOS DIRECCIONES SEGÚN SU USO

Las direcciones IP pueden ser:



# CLASES

- Las direcciones IPv4 constan de cuatro bytes que determinan:
  - La clase
  - El identificador de la red
  - El identificador de host





# CLASE A

- Utiliza un byte (8 bits) para indicar la red.
  - El primer bit tiene valor fijo 0. Por tanto, quedarán libres 7 bits. Además, hay que descartar las direcciones 0 y 127 que están reservadas
  - $N^{\circ}$  de redes =  $2^7 - 2 = 126$  redes
- Utiliza tres bytes (24 bits) para indicar el host dentro de cada red
  - $N^{\circ}$  de host por red =  $2^{24} - 2 = 16.777.214$  hosts
- $N^{\circ}$  total de direcciones =  $2^{31}$  lo que supone el 50% del espacio direccionamiento total

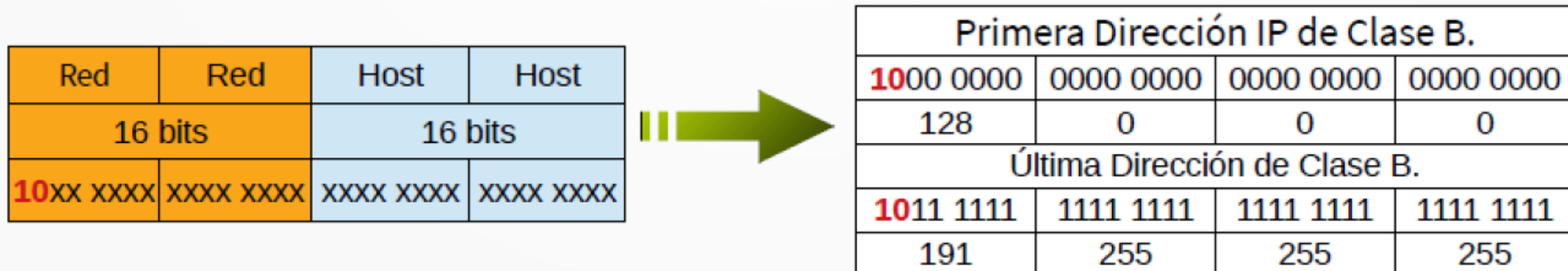
| Red       | Host      | Host      | Host      |
|-----------|-----------|-----------|-----------|
| 8 bits    | 24 bits   |           |           |
| 0xxx xxxx | xxxx xxxx | xxxx xxxx | xxxx xxxx |



| Primera Dirección IP de Clase A. |           |           |           |
|----------------------------------|-----------|-----------|-----------|
| 0000 0000                        | 0000 0000 | 0000 0000 | 0000 0000 |
| 0                                | 0         | 0         | 0         |
| Última Dirección de Clase A.     |           |           |           |
| 0111 1111                        | 1111 1111 | 1111 1111 | 1111 1111 |
| 127                              | 255       | 255       | 255       |

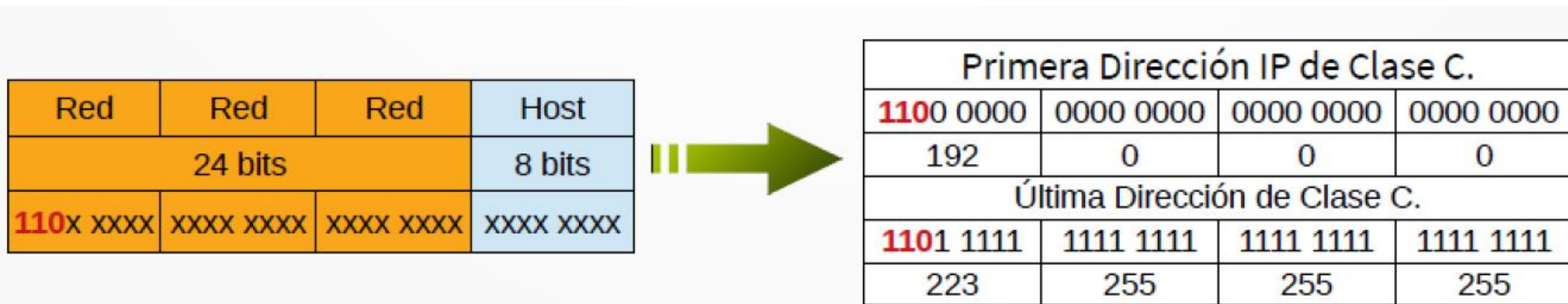
# CLASE B

- Utiliza dos bytes (16 bits) para indicar la red.
  - Los dos primeros bit tiene valor fijo 10. Por tanto, quedarán libres 14 bits.
  - N° de redes =  $2^{14}=16.384$  redes
- Utiliza dos bytes (16 bits) para indicar el host dentro de cada red
  - N° de host por red =  $2^{16}-2=65.534$  hosts
- N° total de direcciones =  $2^{30}$  lo que supone el 25% del espacio direccionamiento total



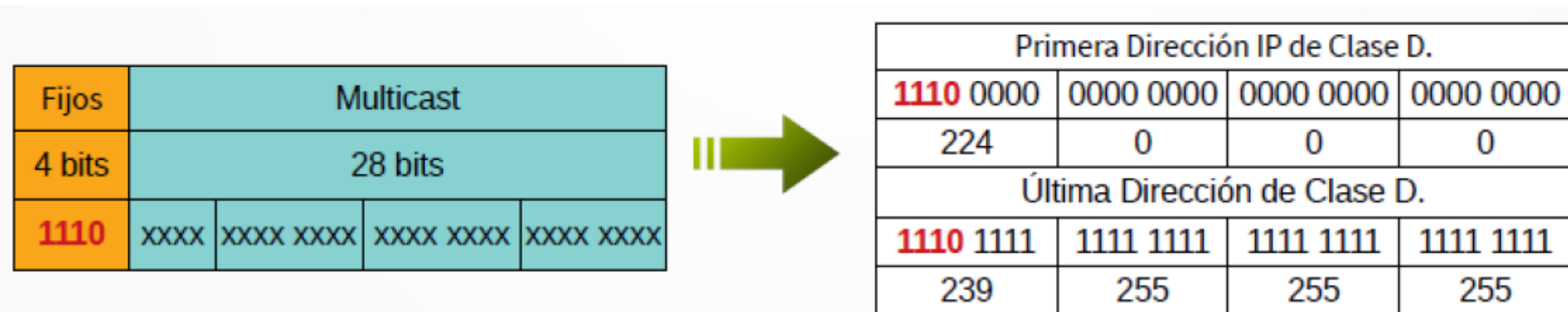
# CLASE C

- Utiliza tres bytes (24 bits) para indicar la red.
  - Los tres primeros bit tiene valor fijo 1 1 0. Por tanto, quedarán libres 21 bits.
  - N° de redes =  $2^{21}=2.097.152$  redes
- Utiliza un byte (8 bits) para indicar el host dentro de cada red
  - N° de host por red =  $2^8-2=254$  hosts
- N° total de direcciones =  $2^{29}$  lo que supone el 12,5% del espacio direccionamiento total



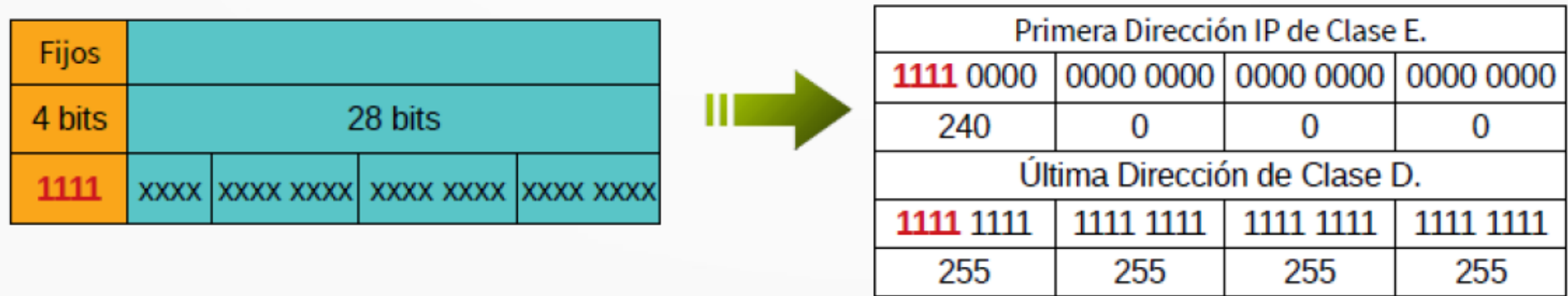
# CLASE D

- Se llaman direcciones multicast
- Los 4 primeros bits tienen valor fijo 1 1 1 0
- Este tipo de dirección permite enviar un datagrama a un grupo concreto del host dentro de una subred.
- Se usan direcciones multicast cuando el destinatario de la información no sea una única máquina, pero tampoco se quiere hacer un broadcast a toda la red.
- N° direcciones total:  $2^{28}$  lo que representa 6,25% del espacio total de IPv4



# CLASE E

- Son direcciones reservadas para uso experimental.
- Los cuatro primeros bits tiene el valor fijo 1 1 1 1
- Número de direcciones total =  $2^{28}$  lo que representa un 6,25% del espacio total



# CLASES

- La clase de una dirección IP podemos averiguarla visualizando el primer octeto y el rango al que pertenece:

| Clase | Desde | A   | Clase usada para redes |
|-------|-------|-----|------------------------|
| A     | 1     | 126 | Si                     |
| B     | 128   | 191 | Si                     |
| C     | 192   | 223 | Si                     |
| D     | 224   | 239 | Multidifusión          |
| E     | 240   | 255 | Reservado              |



# DIRECCIONES RESERVADAS

- Se trata de direcciones que no puede tomar un host
  - Dirección de red:
    - dirección que identifica a toda la red
    - Ej: 192.168.1.0
  - Dirección de difusión (broadcast)
    - Sirve para enviar mensajes a todos los hosts de una red
    - Ej: 192.168.1.255
- El rango válido de la ip de un host está comprendido entre esas dos direcciones



# DIRECCIONES ESPECIALES

- Se trata de direcciones que sí puede tomar un host pero tienen un significado específico

| Nombre                 | Dirección de red            | Significado   |
|------------------------|-----------------------------|---|
| Mi propio host         | 0.0.0.0                     | Es la dirección de un equipo antes de recibir configuración. También se utiliza en routers como ruta por defecto cuando no se conoce otro mejor |
| Bucle local o loopback | 127.0.0.1-127.255.255.255   | Es una dirección local de prueba. Los paquetes enviados a esta dirección no salen al cable y se tratan como paquetes de entrada                 |
| Enlace local           | 169.254.0.0-169.254.255.255 | Cuando la configuración IP dinámica falla, el sistema operativo puede asignar una dirección de este tipo.                                       |





# DIRECCIONES PÚBLICAS

- Las direcciones IP públicas se configuran manualmente en las estaciones de red, y el ICANN es la institución internacional, encargada de asignar las direcciones de Internet a cada organización, para impedir duplicados.



# DIRECCIONES PRIVADAS

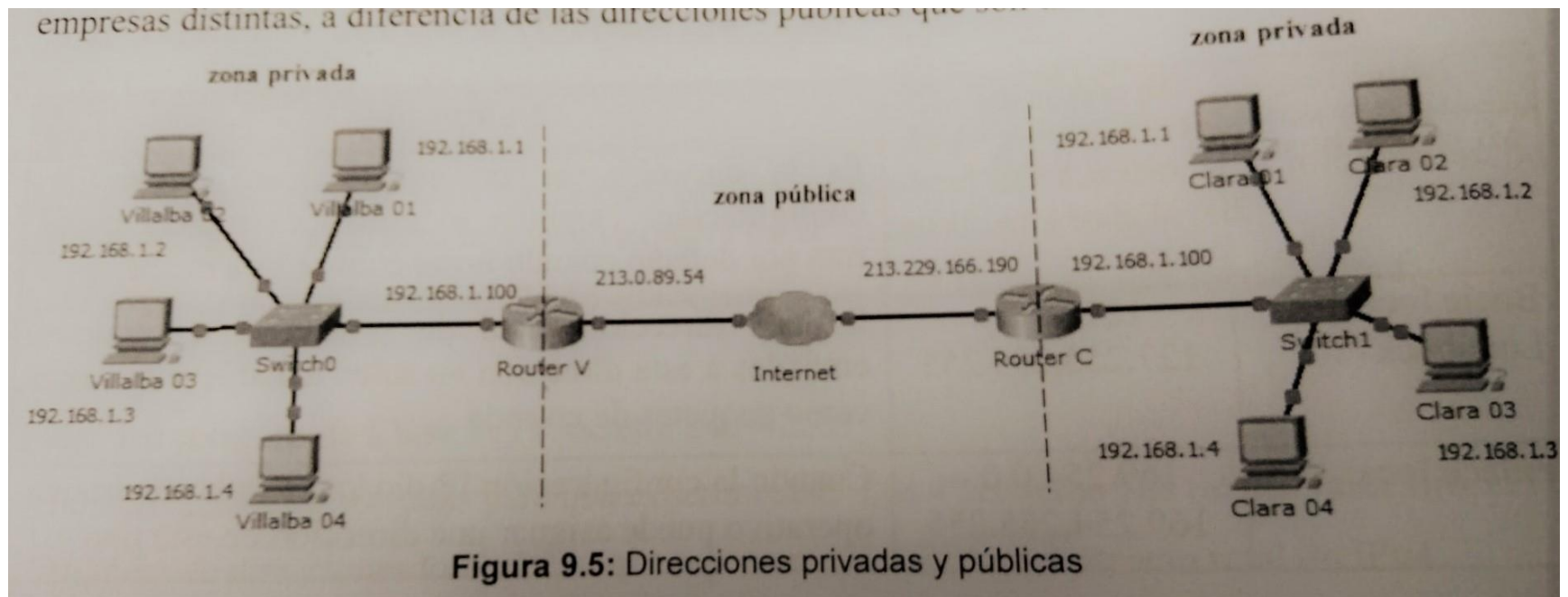
- Dentro de la intranet de una empresa los equipos necesitan conexión a Internet, pero no es necesario (ni conveniente) que sean visibles desde Internet.
- Para estos equipos se utilizan direcciones privadas sin coste alguno para la empresa
- Estas direcciones privadas se convierten en direcciones públicas por el router mediante un mecanismo llamado NAT

| Clase | Red                                   | Nº de redes | Rango direcciones           |
|-------|---------------------------------------|-------------|-----------------------------|
| A     | 10.0.0.0                              | 1           | 10.0.0.0-10.255.255.255     |
| B     | Desde 172.16.0.0 hasta 172.31.0.0     | 16          | 172.16.0.0-172.31.255.255   |
| C     | Desde 192.168.0.0 hasta 192.168.255.0 | 256         | 192.168.0.0-192.168.255.255 |



# DIRECCIONES PRIVADAS

- Las direcciones privadas son únicas dentro de cada empresa, pero pueden repetirse en empresas distintas, a diferencia de las direcciones públicas que son únicas en todo Internet.



# MÁSCARA DE SUBRED

- Una máscara de subred es aquella dirección que enmascara nuestra dirección IP, para indicarnos si otra dirección IP pertenece a nuestra red.

| Clase | Máscara de subred<br>(sistema decimal con puntos) | Máscara de subred<br>(sistema binario) |
|-------|---|--|
| A     | 255.0.0.0   | 11111111 00000000 00000000 00000000    |
| B     | 255.255.0.0                                       | 11111111 11111111 00000000 00000000    |
| C     | 255.255.255.0                                     | 11111111 11111111 11111111 00000000    |

Máscara de subred de cada clase

- Los unos indican los bits de la dirección correspondientes a la red y los ceros al host



# MÁSCARA DE SUBRED

- Para saber si una dirección pertenece a nuestra red, cada máquina realiza la operación and binaria de la dirección IP y la máscara de subred.

**Dirección de red = (Dirección IP) AND (Máscara de subred)**



# MÁSCARA DE SUBRED

**EJEMPLO:** Averiguar si las direcciones 148.120.33.110 y 148.120.45.110 pertenecen a la misma red.

- Son direcciones de Clase B. Por tanto, la máscara es 255.255.0.0
- Pasamos a binario y hacemos la operación AND

|             |                |     |                                     |
|-------------|----------------|-----|-------------------------------------|
| ■ Dirección | 148.120.33.110 |     | 10010100.01111000.00100001.01101110 |
| ■ Máscara   | 255.255.0.0    | AND | 11111111.11111111.00000000.00000000 |
| ■ Subred    | 148.120.0.0    |     | 10010100.01111000.00000000.00000000 |

|             |                |     |                                     |
|-------------|----------------|-----|-------------------------------------|
| ■ Dirección | 148.120.45.110 |     | 10010100.01111000.00101101.01101110 |
| ■ Máscara   | 255.255.0.0    | AND | 11111111.11111111.00000000.00000000 |
| ■ Subred    | 148.120.0.0    |     | 10010100.01111000.00000000.00000000 |

- La dirección de red es en ambos casos 148.120.0.0, por tanto, pertenecen a la misma red.



# MÁSCARA DE SUBRED

- Para calcular la dirección de difusión de una determinada subred

**Dirección de difusión = (Dirección IP) OR (NOT (Máscara de subred))**



# MÁSCARA DE SUBRED

EJEMPLO: Calcular la dirección de difusión de 148.120.33.110

- Son direcciones de Clase B. Por tanto, la máscara es 255.255.0.0
- Pasamos a binario y hacemos la operación OR

|             |                        |    |  |
|-------------|------------------------|----|--|
| ▪ Dirección | 148.120.33.110         |    | 10010100.01111000.00100001.01101110        |
| ▪ Máscara   | 255.255.0.0            | OR |  |
| ▪ NOT másc  | 0.0.255.255            |    | 00000000.00000000.11111111.11111111        |
| ▪ Difusión  | <u>148.120.255,255</u> |    | <u>10010100.01111000.11111111.11111111</u> |





# MÁSCARA DE SUBRED: NOTACION CIDR

- Actualmente, las direcciones IP y su máscara de subred suelen expresarse a través de una barra seguida por el número de unos de la máscara.
- Ejemplos:
  - Clase A: 118.6.24.86/255.0.0.0 => 118.6.24.86/8
  - Clase B: 129.0.37.63/255.255.0.0 => 129.0.37.63/16
  - Clase C: 213.37.2.6/255.255.255.0 => 213.37.2.6/24



# SUBREDES



# NECESIDAD DE SUBREDES

- La división en subredes disminuye el tráfico de red general y mejora su rendimiento.
- A su vez, le permite a un administrador implementar políticas de seguridad, por ejemplo, qué subredes están habilitadas para comunicarse entre sí y cuáles no lo están.
- Otra razón es que reduce el número de dispositivos afectados por el tráfico de difusión anormal debido a configuraciones incorrectas, problemas de hardware o software o intenciones malintencionadas.
- Existen diversas maneras de usar las subredes para contribuir a administrar los dispositivos de red.



# NECESIDAD DE SUBREDES

- Existen diversas maneras de usar las subredes para contribuir a administrar los dispositivos de red.

División en subredes  
por ubicación

División en subredes  
por grupo o función

División en subredes  
por tipo de dispositivo



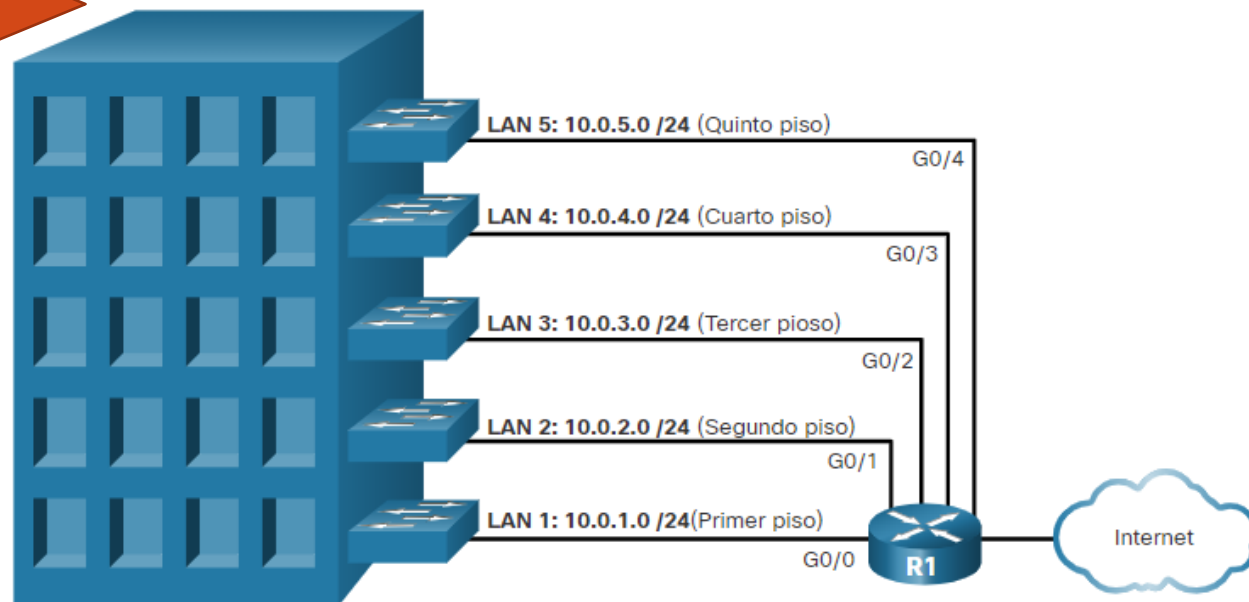
# NECESIDAD DE SUBREDES

- Existen diversas maneras de usar las subredes para contribuir a administrar los dispositivos de red.

División en subredes  
por ubicación

División en subredes  
por grupo o función

División en subredes  
por tipo de dispositivo



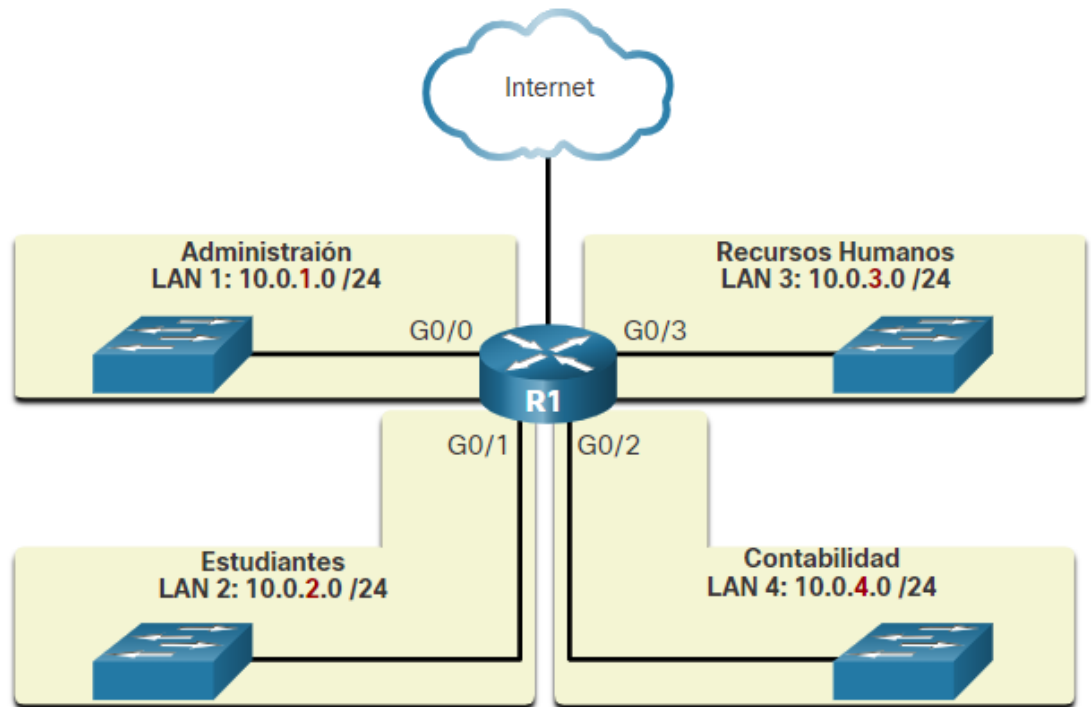
# NECESIDAD DE SUBREDES

- Existen diversas maneras de usar las subredes para contribuir a administrar los dispositivos de red.

División en subredes  
por ubicación

División en subredes  
por grupo o función

División en subredes  
por tipo de dispositivo



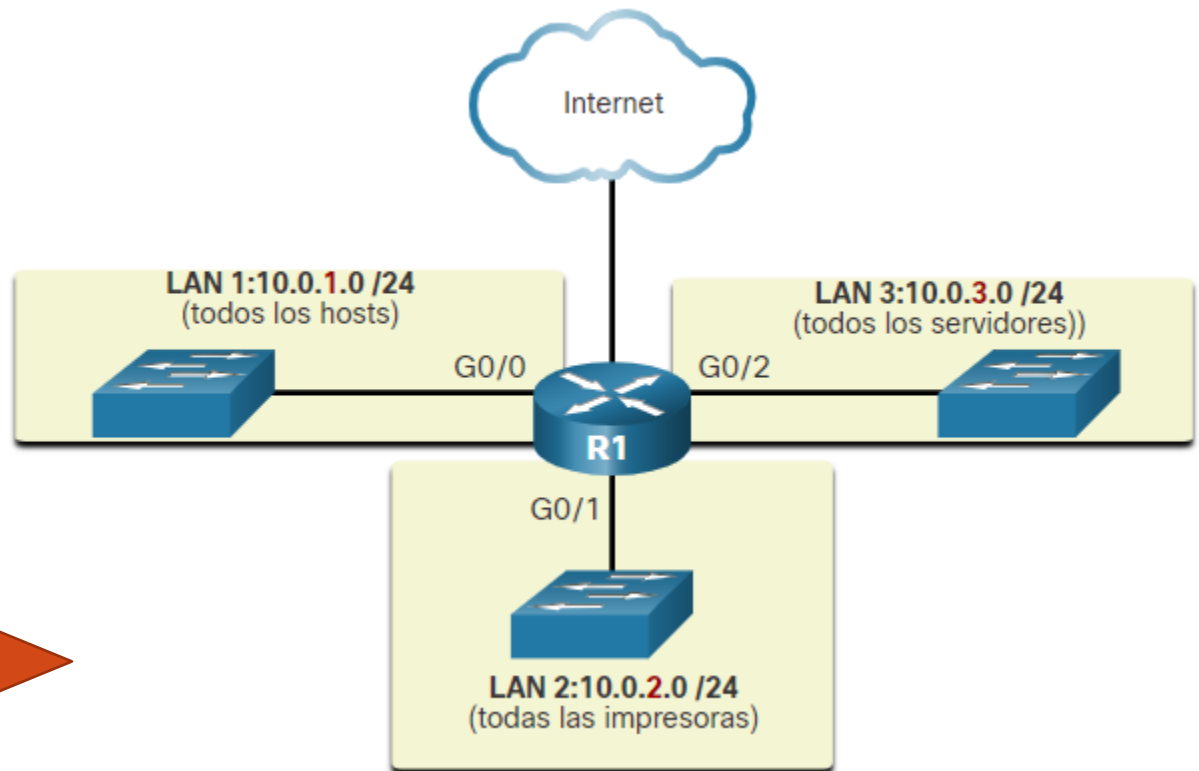
# NECESIDAD DE SUBREDES

- Existen diversas maneras de usar las subredes para contribuir a administrar los dispositivos de red.

División en subredes  
por ubicación


División en subredes  
por grupo o función

División en subredes  
por tipo de dispositivo



# MÉTODO PARA CREACIÓN SUBREDES (SUBNETTING)

1. Cálculo del número de subred
  - El n° de bits (a) necesarios para el n° de subredes queremos dividir subredes  $2^a$
  - El n° de bits (b) necesarios para host
2. Cálculo del número de host por subred
  - Cada una de las subredes tendrá  $2^b - 2$  hosts
3. Nueva máscara de red
  - La máscara de cada una de las subredes será la máscara inicial mas el número de bits de subred
4. Dirección de red de cada una de las subredes
  - Se obtienen dando valores a cada uno de los bits de subred en la IP. Los valores irán desde 0 hasta  $2^a - 1$

|         |   |      |      |      |                               |         |
|---------|---|------|------|------|-------------------------------|---------|
|         | byte  |      |      |      |                               |         |
|         |  |      |      |      |                               |         |
| CLASE A | RED   | HOST | HOST | HOST | 8 bits para red 24 para host  | 0-127   |
| CLASE B | RED   | RED  | HOST | HOST | 16 bits para red 16 para host | 128-191 |
| CLASE C | RED   | RED  | RED  | HOST | 24 bits para red 8 para host  | 192-223 |





# SUBNETTING: EJEMPLO (I)

- La red 192.168.34.0/24 se desea dividir en dos subredes.

## Paso 1 ¿Cuántos bits necesitamos para el n° de subredes necesarias?

Tenemos que buscar un número  $n$  tal que  $2^n$  iguale o supere al n° de subredes.

En este caso  $2^1=2$ . Por tanto, “se roba” un bit a la parte de host que identificará a las dos subredes.

## Paso 2 ¿A qué clase pertenece la IP?

La dirección 192.168.34.0 es de la Clase C.

|     |     |     |      |
|-----|-----|-----|------|
| RED | RED | RED | HOST |
|-----|-----|-----|------|

Un bit de host pasa a ser bit de subred. La máscara de red pasa /24 a  $/24+1 = /25$

## Paso 3 ¿Cuántos host tenemos en cada subred?

Hemos tenido que “robar” 1 bit para identificar la subred. Por tanto, tenemos 7 bits para representar a cada host. Además, se reservan otras dos para la dirección de red y de difusión. Por tanto,  $N^{\circ}$  de host =  $2^7 - 2 = 126$  host para cada subred



# SUBNETTING: EJEMPLO (I)

- La red 192.168.34.0/24 se desea dividir en dos subredes.

Después del subnetting

|          | Red |     |    | SR | Host     | DIRECCIÓN IP   |                         |
|----------|-----|-----|----|----|----------|----------------|-------------------------|
| SUBRED 0 | 192 | 168 | 34 | 0  | 000 0000 | 192.168.34.0   | Dirección de red        |
|          | 192 | 168 | 34 | 0  | 000 0001 | 192.168.34.1   | 126 host en la subred 0 |
|          | 192 | 168 | 34 | 0  | 000 0010 | 192.168.34.2   |                         |
|          | 192 | 168 | 34 | 0  | ...      | ...            |                         |
|          | 192 | 168 | 34 | 0  | 111 1111 | 192.160.34.127 |                         |
| SUBRED 1 | 192 | 168 | 34 | 1  | 000 0000 | 192.168.34.128 | 126 host en la subred 1 |
|          | 192 | 168 | 34 | 1  | 000 0001 | 192.168.34.129 |                         |
|          | 192 | 168 | 34 | 1  | 000 0010 | 192.168.34.130 |                         |
|          | 192 | 168 | 34 | 1  | ...      | ...            |                         |
|          | 192 | 168 | 34 | 1  | 111 1110 | 192.168.34.254 |                         |
|          | 192 | 168 | 34 | 1  | 111 1111 | 192.168.34.255 | Dirección de difusión   |

# SUBNETTING: EJEMPLO (II)

- La red 192.168.15.0/24 se desea dividir en cuatro subredes

## Paso 1 ¿Cuántos bits necesitamos para el n° de subredes necesarias?

Tenemos que buscar un número  $n$  tal que  $2^n$  iguale o supere al n° de subredes.

En este caso  $2^2=4$ . Por tanto, “se roban” 2 bits a la parte de host que identificará a las 4 subredes.

## Paso 2 ¿A qué clase pertenece la IP?

La dirección 192.168.15.0 es de la Clase C.

Dos bits de host pasas a ser bit de subred. La máscara de red pasa /24 a  $/24+2= /26$

## Paso 3 ¿Cuántos host tenemos en cada subred?

Hemos tenido que “robar” 2 bits para identificar la subred.

Por tanto, tenemos 6 bits para representar a cada host. Además, se reservan otras dos para la dirección de red y de difusión.

Por tanto,  $N^{\circ}$  de host =  $2^6 - 2 = 62$  hosts para cada subred



# SUBNETTING: EJEMPLO (II)

- La red 192.168.15.0/24 se desea dividir en cuatro subredes  
Después del subnetting

|          | Red |     |    | SR | Host    | DIRECCIÓN IP   |
|----------|-----|-----|----|----|---------|----------------|
| SUBRED 0 | 192 | 168 | 15 | 00 | 00 0000 | 192.168.15.0   |
|          | 192 | 168 | 15 | 00 | 00 0001 | 192.168.15.1   |
|          | 192 | 168 | 15 | 00 | 00 0010 | 192.168.15.2   |
|          | 192 | 168 | 15 | 00 | ...     | ...            |
|          | 192 | 168 | 15 | 00 | 11 1111 | 192.160.15.63  |
| SUBRED 1 | 192 | 168 | 15 | 01 | 00 0000 | 192.168.15.64  |
|          | 192 | 168 | 15 | 01 | 00 0001 | 192.168.15.65  |
|          | 192 | 168 | 15 | 01 | 00 0010 | 192.168.15.66  |
|          | 192 | 168 | 15 | 01 | ...     | ...            |
|          | 192 | 168 | 15 | 01 | 11 1110 | 192.168.15.126 |
|          | 192 | 168 | 15 | 01 | 11 1111 | 192.168.15.127 |

Dirección de red

62 host en la subred 0

62 host en la subred 1



# SUBNETTING: EJEMPLO (II)

- La red 192.168.15.0/24 se desea dividir en cuatro subredes  
Después del subnetting

|          | Red |     |    | SR | Host    | DIRECCIÓN IP   |
|----------|-----|-----|----|----|---------|----------------|
| SUBRED 2 | 192 | 168 | 15 | 10 | 00 0000 | 192.168.15.128 |
|          | 192 | 168 | 15 | 10 | 00 0001 | 192.168.15.129 |
|          | 192 | 168 | 15 | 10 | 00 0010 | 192.168.15.130 |
|          | 192 | 168 | 15 | 10 | ...     | ...            |
|          | 192 | 168 | 15 | 10 | 11 1111 | 192.160.15.191 |
| SUBRED 3 | 192 | 168 | 15 | 11 | 00 0000 | 192.168.15.192 |
|          | 192 | 168 | 15 | 11 | 00 0001 | 192.168.15.193 |
|          | 192 | 168 | 15 | 11 | 00 0010 | 192.168.15.194 |
|          | 192 | 168 | 15 | 11 | ...     | ...            |
|          | 192 | 168 | 15 | 11 | 11 1110 | 192.168.15.254 |
|          | 192 | 168 | 15 | 11 | 11 1111 | 192.168.15.255 |

62 host en la subred 2

62 host en la subred 3

Dirección de difusión

# HERRAMIENTAS PARA SUBNETTING

- Existen calculadoras de redes IPv4 online para comprobar que tus cálculos son correctos:
  - <http://www.subnet-calculator.com>
- Para IPv6: <https://www.calculator.net/ip-subnet-calculator.html>



# PROTOCOLLO ARP



# INTRODUCCIÓN

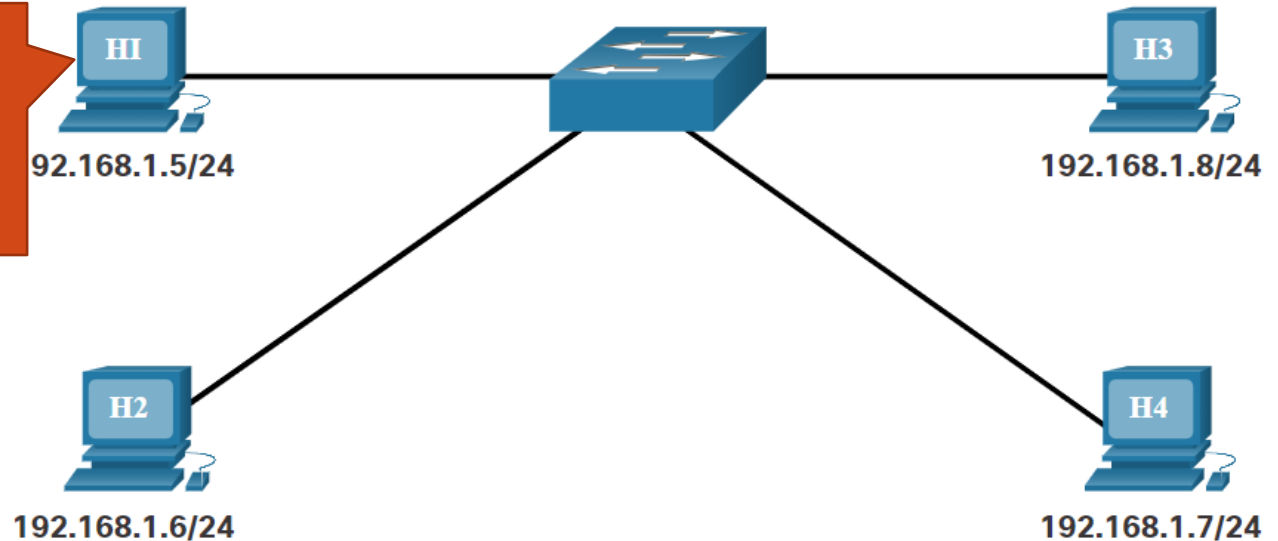
- Address Resolution Protocol (ARP) asocia una dirección IP con una dirección física.
- ARP proporciona dos funciones básicas:
  - Resolución de direcciones IPv4 a direcciones MAC
  - Mantener una tabla de asignaciones de direcciones IPv4 a MAC





# INTRODUCCIÓN

Debo enviar información a la dirección 192.168.1.7 pero solamente tengo la dirección IP, no sé cuál es su dirección MAC

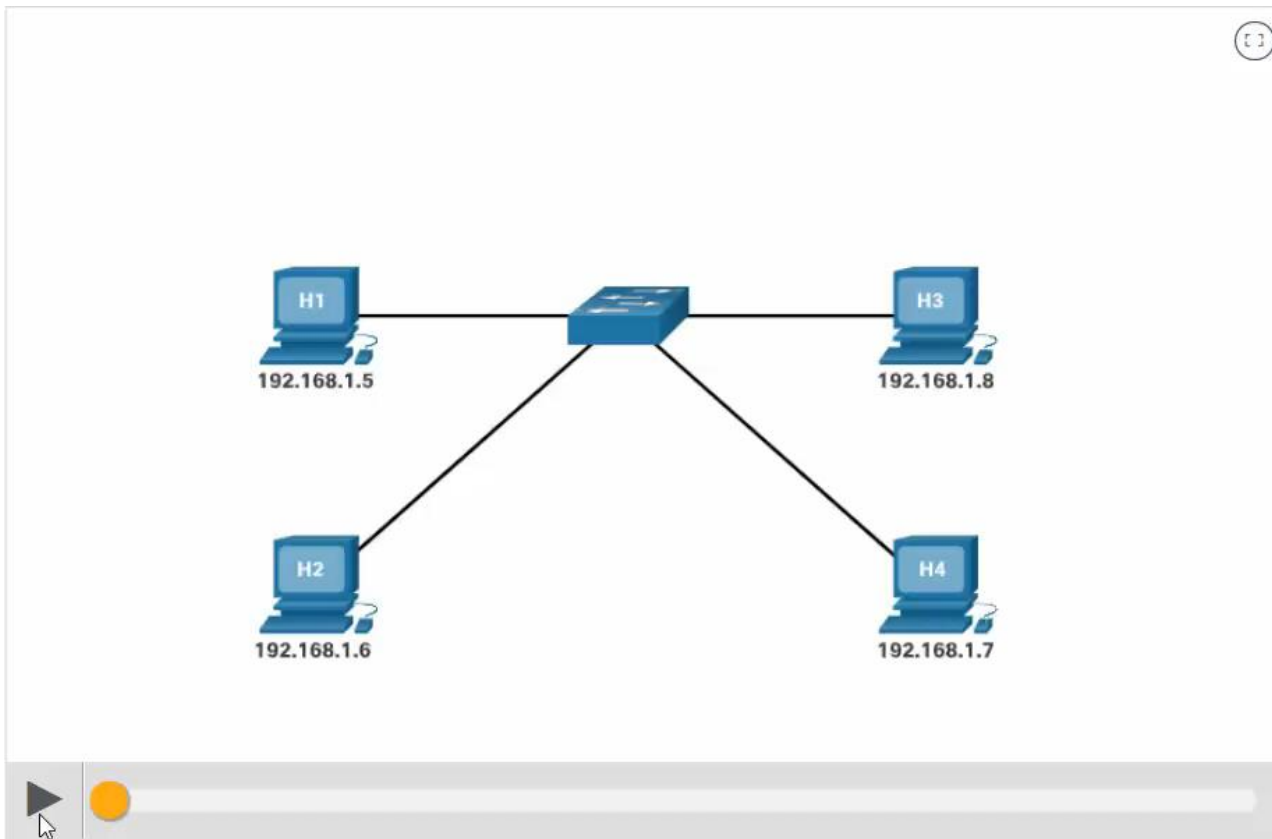


- Cada dispositivo IP de una red Ethernet tiene una dirección MAC Ethernet única. Cuando un dispositivo envía una trama de capa 2 de Ethernet, contiene estas dos direcciones:
  - Dirección MAC de destino - La dirección MAC Ethernet del dispositivo de destino en el mismo segmento de red local. Si el host de destino está en otra red, entonces la dirección de destino en el trama sería la del gateway predeterminado (es decir, router).
  - Dirección MAC de origen - La dirección MAC de la NIC de Ethernet en el host de origen.



# FUNCIONES ARP

- Cuando un equipo o router necesitan conocer la dirección física de otro host envían una petición ARP con la dirección IP destino a todos los hosts de la red.
- Solo el equipo destino responde a la petición, de esta forma el emisor conoce la dirección física asociada a la IP destino a la añade a su tabla ARP



# SOLICITUD ARP

- Se envía una solicitud ARP cuando un dispositivo necesita determinar la dirección MAC que está asociada con una dirección IPv4, y no tiene una entrada para la dirección IPv4 en su tabla ARP.
- La **solicitud de ARP** se encapsula en una trama de Ethernet con la siguiente información de encabezado:
  - **Dirección MAC de destino** – esta es una dirección broadcast que requiere que todas las NIC Ethernet de la LAN acepten y procesen la solicitud de ARP.
  - **Dirección MAC de origen** – Esta es la dirección MAC del remitente de la solicitud ARP.
  - **Tipo** - Los mensajes ARP tienen un campo de tipo de 0x806. Esto informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP.
- Como **las solicitudes de ARP son de broadcast**, el switch las envía por todos los puertos, excepto el de recepción. Todas las NIC Ethernet de la LAN procesan transmisiones y deben entregar la solicitud ARP a su sistema operativo para su procesamiento. Cada dispositivo debe procesar la solicitud de ARP para ver si la dirección IPv4 objetivo coincide con la suya.
- Solo un dispositivo de la LAN tiene la dirección IPv4 que coincide con la dirección IPv4 objetivo de la solicitud de ARP. Todos los demás dispositivos no envían una respuesta.



# SOLICITUD ARP

## Video – ARP Operation – ARP Request

This video will cover an ARP request for a MAC address.



# RESPUESTA ARP

- Solo el dispositivo con la dirección IPv4 de destino asociada con la solicitud ARP responderá con una respuesta ARP. La **respuesta de ARP se encapsula** en una trama de Ethernet con la siguiente información de encabezado:
  - **Dirección MAC de destino** – Es la dirección MAC del remitente de la solicitud de ARP.
  - **Dirección MAC de origen** – Esta es la dirección MAC del remitente de la respuesta ARP.
  - **Tipo** - Los mensajes ARP tienen un campo de tipo de 0x806. Esto informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP.
- Solamente el dispositivo que envió inicialmente la solicitud de ARP recibe la respuesta de ARP de unicast. Una vez que recibe la respuesta de ARP, el dispositivo agrega la dirección IPv4 y la dirección MAC correspondiente a su tabla ARP. A partir de ese momento, los paquetes destinados para esa dirección IPv4 se pueden encapsular en las tramas con su dirección MAC correspondiente.
- Si ningún dispositivo responde a la solicitud de ARP, el paquete se descarta porque no se puede crear una trama.



# RESPUESTA ARP

## Video - ARP Operation - ARP Reply

This video will cover an ARP reply in response to an ARP request.



# PARA IPV6

- IPv6 utiliza un proceso similar a ARP para IPv4, conocido como ICMPv6 Neighbour Discovery (ND).
- IPv6 utiliza mensajes de solicitud de vecino y de anuncio de vecino similares a las solicitudes y respuestas de ARP de IPv4.



# TABLAS ARP

- Se almacena en la RAM del dispositivo
- Cada entrada o fila de la tabla ARP vincula una dirección IP con una dirección MAC
- Para cada dispositivo, un temporizador de memoria caché ARP elimina las entradas de ARP que no se hayan utilizado durante un período especificado. Los tiempos varían según el sistema operativo del dispositivo.





# COMANDOS ARP

- El comando `arp` nos muestra la tabla ARP
  - `arp -a` muestra la tabla ARP de cada interfaz
  - `arp -s dirección_IP dirección_MAC` Añade entrada a la tabla ARP
  - `arp -d dirección_IP` Elimina entrada a la tabla ARP

```
Símbolo del sistema
C:\Users\Usuario>arp -a

Interfaz: 192.168.0.20 --- 0xe
Dirección de Internet      Dirección física      Tipo
192.168.0.1                48-29-52-3a-c3-8c    dinámico
192.168.0.10               d8-8c-79-44-fb-5b    dinámico
192.168.0.11               00-00-c0-01-d5-24    dinámico
192.168.0.16               48-29-52-3a-c3-8d    dinámico
192.168.0.22               70-8b-cd-8a-88-6e    dinámico
192.168.0.24               54-8c-a0-ca-49-47    dinámico
192.168.0.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.250                01-00-5e-00-00-fa    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
239.255.255.251            01-00-5e-7f-ff-fb    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

Interfaz: 192.168.56.1 --- 0x19
Dirección de Internet      Dirección física      Tipo
192.168.56.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.250                01-00-5e-00-00-fa    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
239.255.255.251            01-00-5e-7f-ff-fb    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático

C:\Users\Usuario>
```



# COMANDOS ARP

- En un router Cisco, el **show ip arp** comando se utiliza para mostrar la tabla ARP

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr  Type   Interface
Internet  192.168.10.1      -          a0e0.af0d.e140 ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225   -          a0e0.af0d.e141 ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226   1          a03d.6fe1.9d91 ARPA   GigabitEthernet0/0/1
R1#
```



# PROTOCOLLO ICMP



# INTRODUCCIÓN

- Debido a que el protocolo IP no es fiable, los datagramas pueden perderse o llegar defectuosos a su destino.
- El protocolo Internet Control Message Protocol (ICMP) se encarga de informar al origen si se ha producido algún error durante la entrega del mensaje.
- El protocolo ICMP únicamente informa de incidencias en la red, no realiza ninguna acción (esto es tarea de capas superiores)
- El protocolo ICMP está disponible tanto para IPv4 como para IPv6.



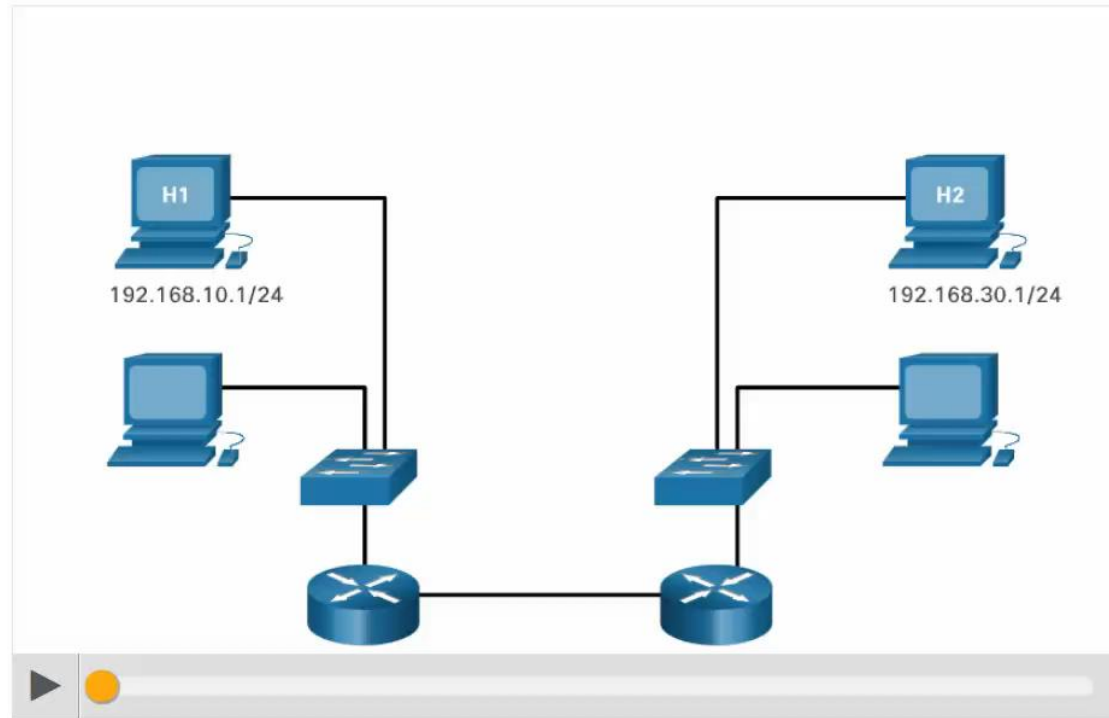
# MENSAJES ICMP

- Además de notificar errores, también transporta distintos tipos de mensajes de control.
- Los mensajes ICMP comunes a ICMPv4 e ICMPv6 son:
  - Accesibilidad al host
  - Destino o servicio inaccesible
  - Tiempo superado



# MENSAJES ICMP: ACCESIBILIDAD AL HOST

- Se puede utilizar un mensaje de eco ICMP para probar la accesibilidad de un host en una red IP.
- El host local envía una solicitud de eco ICMP a un host.
- Si el host se encuentra disponible, el host de destino responde con una respuesta de eco.



# MENSAJES ICMP: DESTINO O SERVICIO INACCESIBLE

- Cuando un host o gateway recibe un paquete que no puede entregar, puede utilizar un mensaje ICMP de destino inalcanzable para notificar al origen que el destino o el servicio son inalcanzables. El mensaje incluye un código que indica el motivo por el cual no se pudo entregar el paquete.
- Algunos de los códigos de destino inalcanzable para ICMPv4 son los siguientes:
  - 0: red inalcanzable
  - 1: host inalcanzable
  - 2: protocolo inalcanzable
  - 3: puerto inalcanzable
- Algunos de los códigos de destino inalcanzable para ICMPv6 son los siguientes:
  - 0 - No hay ruta para el destino
  - 1 - La comunicación con el destino está prohibida administrativamente (por ejemplo, firewall)
  - 2 — Más allá del alcance de la dirección de origen
  - 3 - No se puede alcanzar la dirección
  - 4 – Puerto inalcanzable



# MENSAJES ICMP: TIEMPO EXCEDIDO

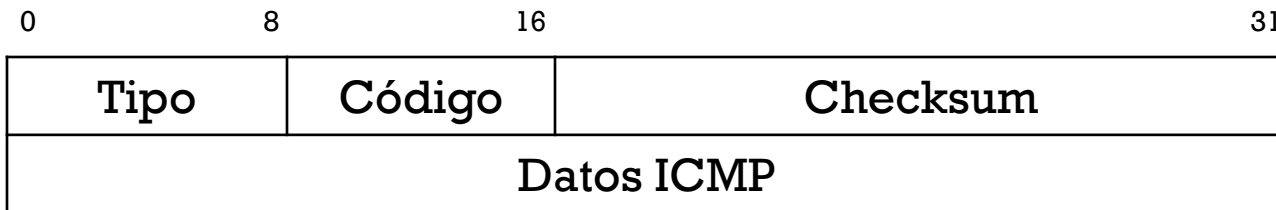
- Los routers utilizan los mensajes de tiempo superado de ICMPv4 para indicar que un paquete no puede reenviarse debido a que el campo de tiempo de duración (TTL) del paquete se disminuyó a 0.
- Si un router recibe un paquete y disminuye el campo TTL en el paquete IPV4 a cero, descarta el paquete y envía un mensaje de tiempo superado al host de origen.
- ICMPv6 también envía un mensaje de tiempo superado si el router no puede reenviar un paquete IPv6 debido a que el paquete caducó. En lugar del campo TTL de IPv4, ICMPv6 usa el campo Límite de salto de IPv6 para determinar si el paquete ha expirado.





# FORMATO MENSAJE

- Los mensajes tanto en ICMPv4 como en ICMPv6 tienen una cabecera de tres campos:
  - Tipo
  - Código
  - Checksum



Formato de un mensaje ICMP



# TIPOS DE MENSAJE ICMPV4

- Algunos tipos de mensajes ICMPv4 son los siguientes:

| Tipo | Significado                                       |   |
|------|---|---|
| 0    | Echo Reply (Respuesta de Eco)                     |   |
| 3    | Destination Unreachable<br>(Destino inalcanzable) | Código<br>0: red inaccesible<br>1: host inaccesible<br>2: protocolo inaccesible |
| 8    | Echo Request (Solicitud de eco)                   |   |
| 11   | Time Exceeded (Tiempo excedido)                   |   |



# MENSAJES DE SOLICITUD Y RESPUESTA (ECHO Y ECHO REPLY)

- Los mensajes de solicitud (8) y respuesta eco (0), se utilizan para **comprobar si existe una comunicación entre dos hosts a nivel de la capa de red.**
- Estos mensajes comprueban que las capas: físicas (cableado), acceso al medio (tarjeta red) y de red (configuración ip) están correctas
- Sin embargo, no dicen nada de las capas de transporte y aplicación. Por ejemplo, la visualización de una web puede fallar pero sí existe comunicación IP con el servidor web.
- Para **diagnosticar errores** en la red el comando **ping** es la utilidad básica



# MENSAJES DE SOLICITUD Y RESPUESTA (ECHO Y ECHO REPLY)

## Paso 1. Ping a localhost

- Si se produce un error es porque los protocolos TCP/IP están dañados.
  - Medidas: reinstalar.
- Si funciona correctamente ir al paso 2

```
C:\> Símbolo del sistema

Microsoft Windows [Versión 10.0.19044.1566]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>ping 127.0.0.1

Haciendo ping a 127.0.0.1 con 32 bytes de datos:
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 127.0.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Usuario>
```



# MENSAJES DE SOLICITUD Y RESPUESTA (ECHO Y ECHO REPLY)

## Paso 2. Ping a la IP del equipo

- Si se produce un error es porque seguramente hay problemas con el controlador de la tarjeta de red o el cable de red.
  - Medidas: testear el cable, reinstalar controlador de tarjeta de red, probar en otro equipo, etc.
- Si funciona correctamente ir la paso 3



# MENSAJES DE SOLICITUD Y RESPUESTA (ECHO Y ECHO REPLY)

## Paso 3. Ping a la puerta de enlace predeterminada

- Si se produce error puede que esté mal configurada o exista algún problema con el router o cableado con algún dispositivo de interconexión como un switch.
  - Medidas: comprobar puerta enlace en la configuración del adaptador de red, testear el cableado de red y dispositivos intermedios hasta el router.
- Si funciona ir al paso 4 o 5



# MENSAJES DE SOLICITUD Y RESPUESTA (ECHO Y ECHO REPLY)

## Paso 4. Ping a otro host de la red

- Si se produce error, el otro equipo no responde. Puede haber problema con cableado o dispositivos de red entre los equipos.
  - Medidas: testear cableado y dispositivos de red entre los dos equipos, comprobar que el otro host está encendido y tiene conectividad (pasos 1 a 3), comprobar el firewall
- Si funciona ir paso 5



# MENSAJES DE SOLICITUD Y RESPUESTA (ECHO Y ECHO REPLY)

## Paso 5. Ping a un host remoto

- Si se produce error, es posible que el equipo no responda. También puede ser que el equipo esté saturado o tenga bloqueada la respuesta echo
  - Medidas: probar otro host remoto, comprobar configuración router.
- Si funciona correctamente ir paso 6





# MENSAJES DE SOLICITUD Y RESPUESTA (ECHO Y ECHO REPLY)

## Paso 5. Ping a un nombre de host remoto

- Si se produce error, los servidores DNS estarán mal configurados.
  - Medidas: comprobar servidor DNS, hacer ping a los servidores DNS



# MENSAJES DE TIEMPO EXCEDIDO

- Los datagramas IP tienen un campo TTL (tiempo de vida) que impide que un mensaje esté dando vueltas indefinidamente en Internet.
- El n° contenido en este campo disminuye una unidad cada vez que el datagrama atraviesa un router.
- Cuando el TTL llega a 0 este no se retransmite y el router envía un ICMP tipo 11 (Time Exceed) para informar al origen.



# MENSAJES DE TIEMPO EXCEDIDO

- Estos mensajes se pueden utilizar para hacer una traza del camino que siguen los datagramas hasta llegar al destino.
- El comando **tracert** tiene implementado un bucle para envío de mensajes ICMP tipo 8 (Echo) con TTL progresivo de 1 a 30.



# DIRECCIONAMIENTO IPV6



# INTRODUCCIÓN

- IPv6 es la última versión del protocolo IPv4
- La necesidad de v6 ha sido provocada por el agotamiento de las direcciones IPv4
- En IPv4 las direcciones IP disponibles son  $2^{32} = 4.294.967.296$
- Mecanismos desarrollados para ralentizar el agotamiento de IPs han sido:
  - Uso de redes privadas combinadas con NAT, que permite a toda una intranet salir con la misma dirección IP pública.
  - DHCP
  - Control exhaustivo en la asignación de direcciones a los registros regionales de Internet



# COEXISTENCIA IPV4 E IPV6

- A pesar del agotamiento de direcciones IPv4 este protocolo seguirá vigente durante años existiendo redes IPv4 coexistiendo con redes IPv6
- Ambos protocolos son incompatibles entre sí, por ello existen diversas técnicas que permiten la interoperabilidad IPv4-IPv6 y con conocidos como mecanismos de transición

Dual-stack

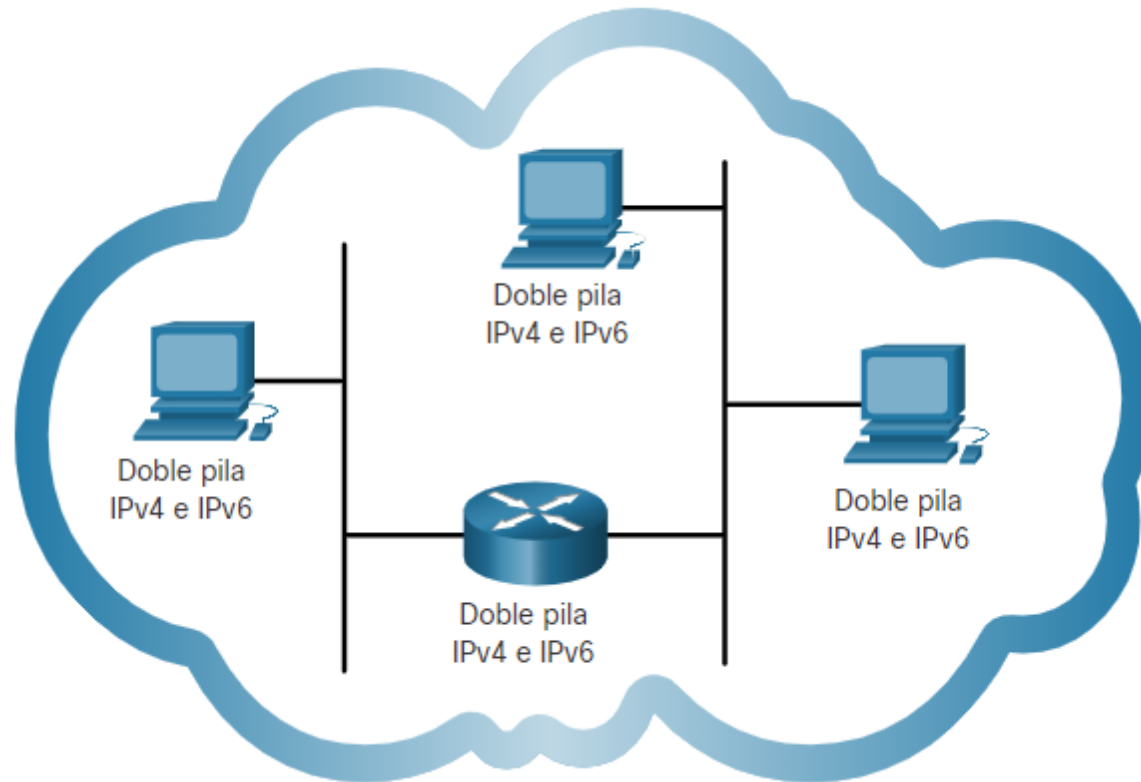
Tunelización

Traducción



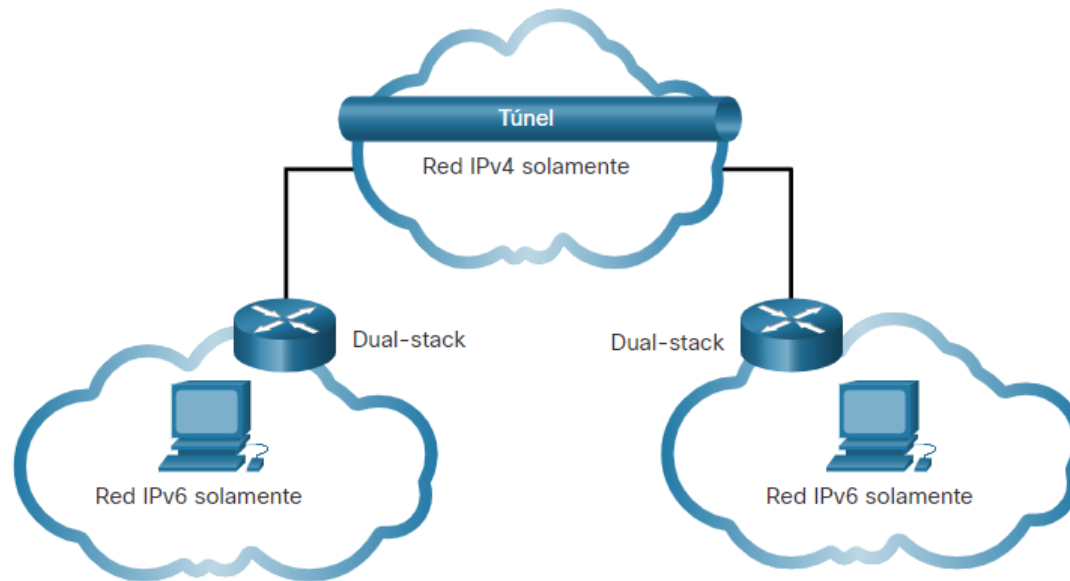
# PILA DUAL (DUAL STACK)

- Ejemplo: topología física que muestra tres PC de doble pila y un enrutador de doble pila



# TUNELIZACIÓN

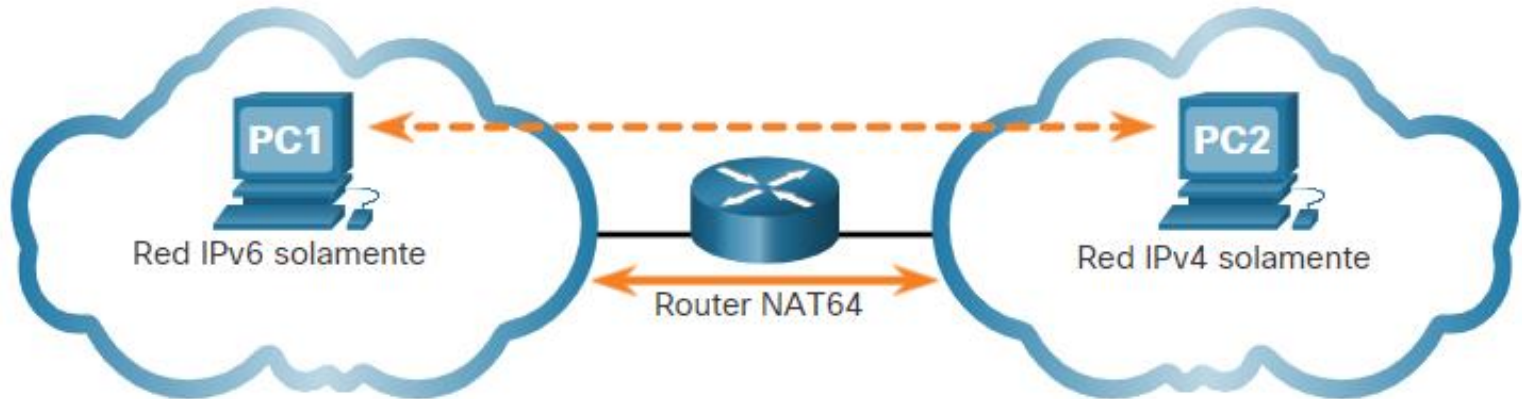
- La tunelización es un método para transportar un paquete IPv6 a través de una red IPv4. El paquete IPv6 se encapsula dentro de un paquete IPv4, de manera similar a lo que sucede con otros tipos de datos.
- Ejemplo:





# TRADUCCIÓN

- La traducción de direcciones de redes 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. Un paquete IPv6 se traduce a un paquete IPv4 y un paquete IPv4 se traduce a un paquete IPv6.



# FORMATOS DIRECCIÓN IPV6

- El primer paso para aprender acerca de IPv6 en las redes es comprender la forma en que se escribe y se formatea una dirección IPv6.
- Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales.
- Cada cuatro bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales. Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas, y pueden escribirse en minúsculas o en mayúsculas.



# FORMATO PREFERIDO

- Las direcciones IPv6 tienen 128 bits de longitud, que se escriben como 8 grupos de 4 dígitos hexadecimales separados por dos puntos.
- Ejemplos:

|              |              |              |              |              |              |              |             |
|--------------|--------------|--------------|--------------|--------------|--------------|--------------|-------------|
| <b>0000:</b> | <b>0000:</b> | <b>0000:</b> | <b>0000:</b> | <b>0000:</b> | <b>0000:</b> | <b>0000:</b> | <b>0001</b> |
| <b>fe80:</b> | <b>0000:</b> | <b>0000:</b> | <b>0000:</b> | <b>25dd:</b> | <b>ce6e:</b> | <b>0000:</b> | <b>ca71</b> |
| <b>2001:</b> | <b>0000:</b> | <b>7ef5:</b> | <b>09fd:</b> | <b>1c87:</b> | <b>0dd8:</b> | <b>aec2:</b> | <b>13a3</b> |



# FORMATO COMPRIMIDO

término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales

## REGLA 1. OMITIR LOS CEROS INICIALES

- La primera regla para ayudar a reducir la notación de las direcciones IPv6 es omitir los ceros (ceros) iniciales en cualquier **hexteto**. Aquí hay cuatro ejemplos de formas de omitir ceros a la izquierda:
  - 01ab se puede representar como 1ab
  - 09f0 se puede representar como 9f0
  - 0a00 se puede representar como a00
  - 00ab se puede representar como ab
- Esta regla solo es válida para los ceros iniciales, y NO para los ceros finales; de lo contrario, la dirección sería ambigua.
  - Por ejemplo, el hexteto "abc" podría ser "0abc" o "abc0", pero no representan el mismo valor.



# FORMATO COMPRIMIDO

## REGLA 2. DOS PUNTOS DOBLES

- Los grupos de cuatro ceros "0000" consecutivos se pueden comprimir con el símbolo "::"
- Los ceros a la izquierda de un grupo también se pueden eliminar.
- Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión solo se permite en uno de ellos, porque no queda claro cuántos grupos nulos hay en cada lado.
- Ejemplo

| Dirección IPv6 preferida                | Dirección IPv6 comprimida           |
|---|-------------------------------------|
| 0000:0000:0000:0000:0000:0000:0000:0001 | ::1                                 |
| fe80:0000:0000:0000:25dd:ce6e:0000:ca71 | fe80::25dd:ce6e:0000:ca71           |
| 2001:0000:7ef5:09fd:1c87:0dd8:aec2:13a3 | 2001::7ef5:09fd:1c87:0dd8:aec2:13a3 |



# FORMATO COMPRIMIDO

## REGLA 2. DOS PUNTOS DOBLES

| Tipo                  | Formato   |
|-----------------------|---|
| Recomendado           | 2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200 |
| Comprimido/espacios   | 2001 : db8 : 0 : 1111 : : 200                         |
| Comprimido            | 2001:db8:0:1111::200                                  |
| Recomendado           | 2001 : 0db8 : 0000 : 0000 : ab00 : 0000 : 0000 : 0000 |
| Comprimido / espacios | 2001 : db8 : 0 : 0 : ab00 ::                          |
| Comprimido            | 2001:db8:0:0:ab00::                                   |
| Recomendado           | 2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000 |
| Comprimido / espacios | 2001 : db8 : aaaa : 1 ::                              |
| Comprimido            | 2001:db8:aaaa:1::                                     |
| Recomendado           | fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdef |
| Comprimido / espacios | fe80 : : 123 : 4567 : 89ab : cdef                     |
| Comprimido            | fe80::123:4567:89ab:cdef                              |

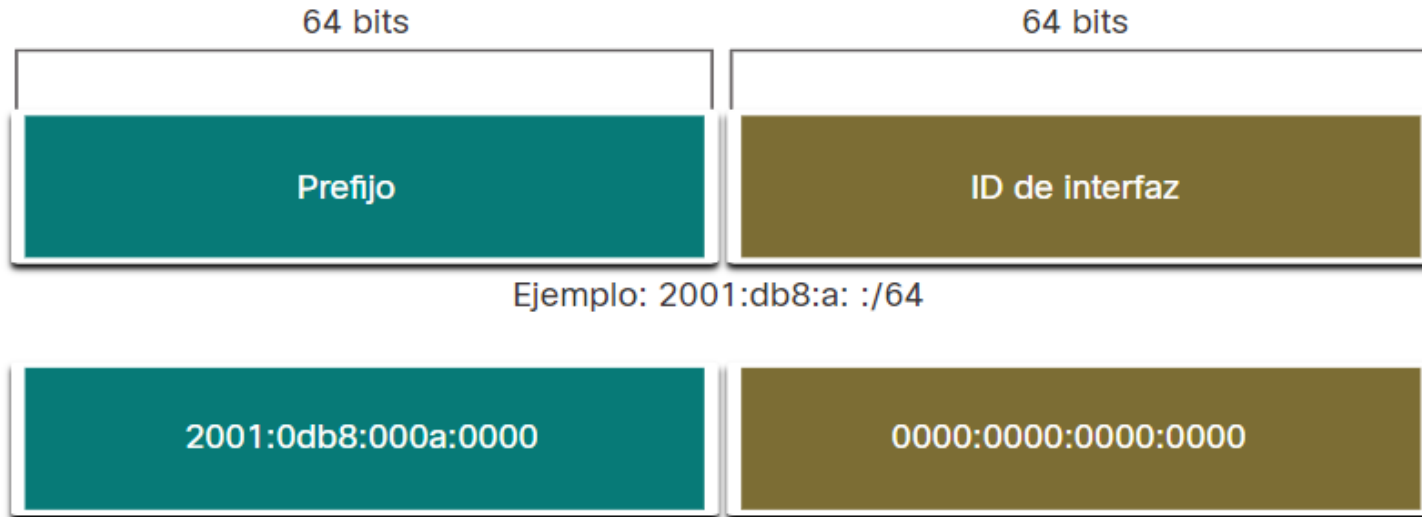


# LONGITUD PREFIJO

- El prefijo, o porción de red, de una dirección IPv4 se puede identificar mediante una máscara de subred decimal decimal o longitud de prefijo (notación de barra).
  - Por ejemplo, la dirección IPv4 192.168.1.10 con la máscara de subred decimal punteada 255.255.255.0 equivale a 192.168.1.10/24.
- En IPv4 el /24 se llama prefijo. En IPv6 se llama longitud de prefijo.
- IPv6 no utiliza la notación decimal punteada de máscara de subred. Al igual que IPv4, la longitud del prefijo se representa en notación de barra inclinada 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 recomendada del prefijo IPv6 para las LAN y la mayoría de los otros tipos de redes es / 64, como se muestra en la figura.



# LONGITUD PREFIJO



- El prefijo o porción de red de la dirección tiene 64 bits de longitud, dejando otros 64 bits para la ID de interfaz (porción de host) de la dirección





# TIPOS DE DIRECCIONES IPV6

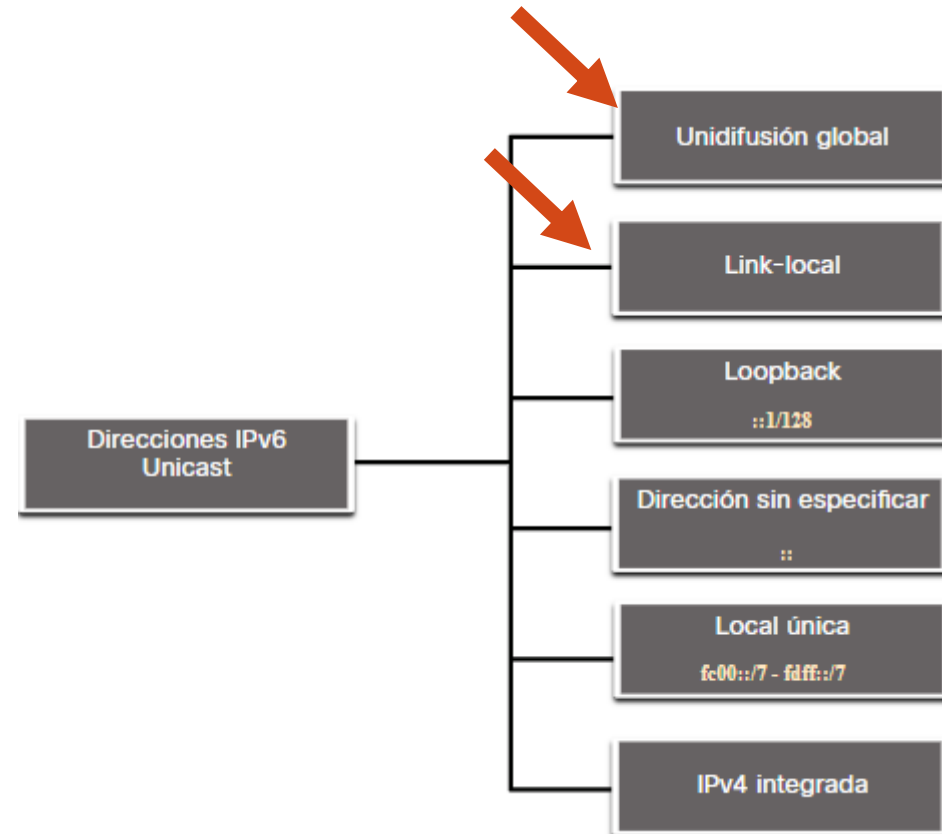
- Una dirección IPv6 puede ser clasificada en alguno de los tres tipos creados:
  - **Unicast (unidifusión):** una dirección de unidifusión IPv6 identifica de forma exclusiva una interfaz en un dispositivo habilitado para IPv6.
  - **Multicast (multidifusión):** una dirección de multidifusión IPv6 se usa para enviar un único paquete IPv6 a múltiples destinos.
  - **Anycast (difusión por proximidad).** Se asigna a múltiples interfaces (usualmente en múltiples nodos). Un paquete enviado a una dirección anycast es entregado a una de estas interfaces, usualmente la más cercana.

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



# UNICAST (UNO A UNO)

- Las direcciones IPv6 de unidifusión identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado.
- La interfaz a la que se le asigna esa dirección recibe un paquete enviado a una dirección de unidifusión.
- Como sucede con IPv4, las direcciones IPv6 de origen deben ser direcciones de unidifusión. Las direcciones IPv6 de destino pueden ser direcciones de unidifusión o de multidifusión.
- La figura muestra los diferentes tipos de direcciones de unidifusión IPv6.



Las direcciones locales únicas (rango fc00::/7 a fdff::/7) aún no se implementan comúnmente. Por lo tanto, este módulo sólo cubre la configuración GUA y LLA. Sin embargo, se pueden usar direcciones locales únicas para dirigir dispositivos a los que no se debe acceder desde el exterior, como servidores internos e impresoras.



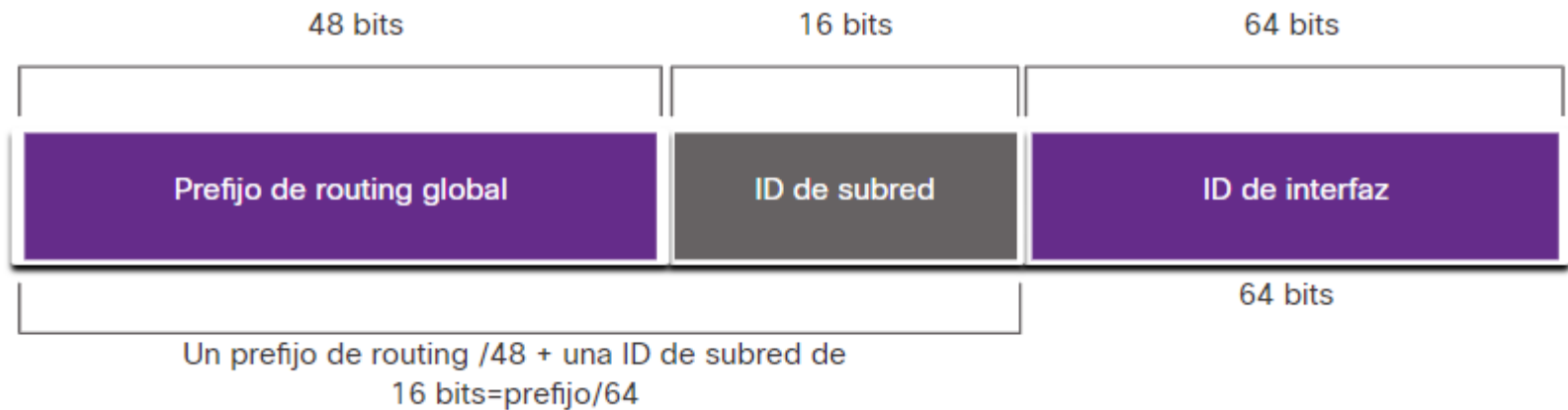
# UNICAST (UNO A UNO)

- A diferencia de los dispositivos IPv4 que tienen una sola dirección, las direcciones IPv6 suelen tener dos direcciones de unidifusión:
  - **Dirección de unidifusión global (GUA):** es similar a una dirección IPv4 pública. Estas son direcciones enrutables de Internet globalmente exclusivas. Las GUA pueden configurarse estáticamente o asignarse dinámicamente.
  - **Dirección local de enlace (LLA):** se requiere para cada dispositivo habilitado para IPv6. Los LLA se utilizan para comunicarse con otros dispositivos en el mismo enlace local. Con IPv6, el término “enlace” hace referencia a una subred. Las LLA se limitan a un único enlace. Su exclusividad se debe confirmar solo para ese enlace, ya que no se pueden enrutar más allá del enlace. En otras palabras, los routers no reenvían paquetes con una dirección de origen o de destino link-local.



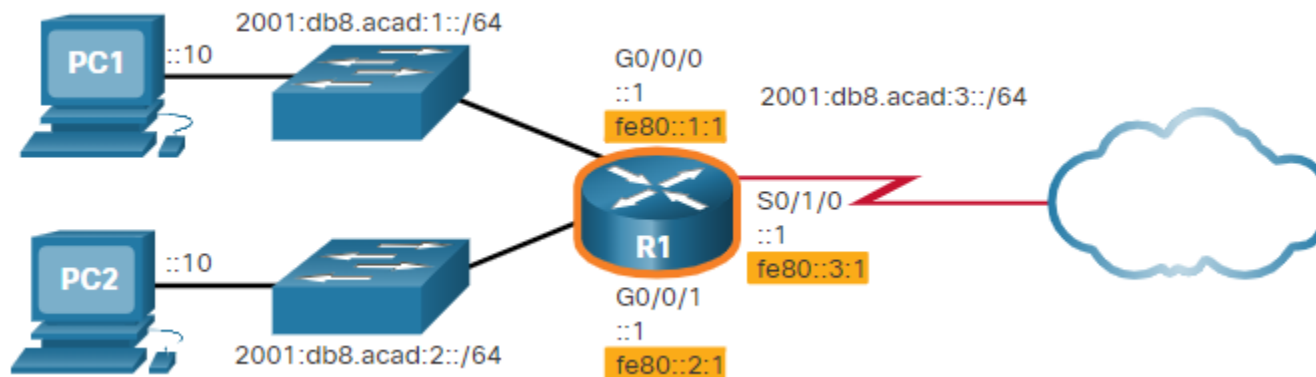
# UNICAST (UNO A UNO)

- Formato dirección IPv6 unicast:



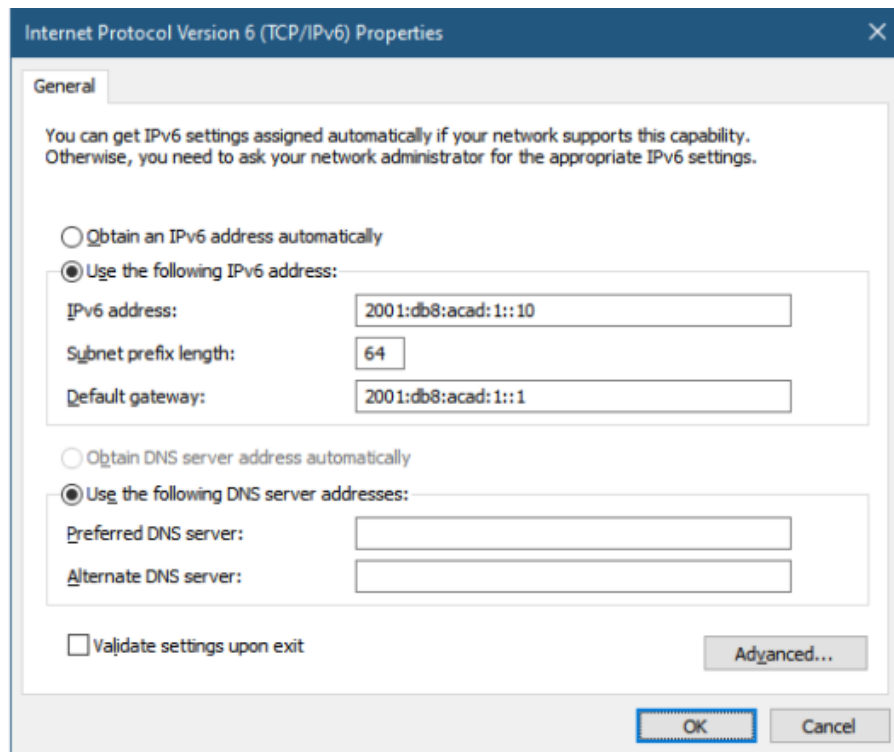
# CONFIGURACIÓN DE CUA ESTÁTICA EN UN HOST DE WINDOWS

- Configurar la dirección IPv6 en un host de forma manual es similar a configurar una dirección IPv4.



# CONFIGURACIÓN DE GUA ESTÁTICA EN UN HOST DE WINDOWS

- Configurar la dirección IPv6 en un host de forma manual es similar a configurar una dirección IPv4.



Como se muestra en la figura, la dirección de puerta de enlace predeterminada configurada para PC1 es 2001:db8:acad:1::1. Esta es la GUA de la interfaz R1 GigabitEthernet en la misma red.

Alternativamente, la dirección de puerta de enlace predeterminada se puede configurar para que coincida con el LLA de la interfaz GigabitEthernet.

El uso de la LLA del enrutador como dirección de puerta de enlace predeterminada se considera una práctica recomendada. Cualquiera de las dos configuraciones funciona.



# CONFIGURACIÓN DINÁMICA PARA GUA

- La mayoría de los dispositivos obtienen sus GUA IPv6 de forma dinámica.
- Este punto se vuelve bastante técnico, por lo que no se profundizará mas.
- Únicamente conocer que este proceso funciona mediante mensajes de anuncio de enrutador (RA) y solicitud de enrutador (RS).



# MULTICAST (UNO A MUCHOS)

- Se utiliza para identificar un grupo de interfaces IPv6.
- Un paquete enviado una dirección multicast es aceptado por todos los miembros del grupo multicast
- Las direcciones de multidifusión solo pueden ser direcciones de destino y no direcciones de origen.
- Existen dos tipos de direcciones IPv6 de multidifusión:
  - Direcciones de multidifusión conocidas
  - Direcciones de multidifusión de nodo solicitadas





# MULTICAST (UNO A MUCHOS)

## Direcciones de multidifusión conocidas

- Se asignan direcciones de multidifusión IPv6 conocidas.
- Las direcciones de multidifusión asignadas son direcciones de multidifusión reservadas para grupos predefinidos de dispositivos.
- Una dirección de multidifusión asignada es una única dirección que se utiliza para llegar a un grupo de dispositivos que ejecutan un protocolo o servicio común. Las direcciones de multidifusión asignadas se utilizan en contexto con protocolos específicos, como DHCPv6.



# MULTICAST (UNO A MUCHOS)

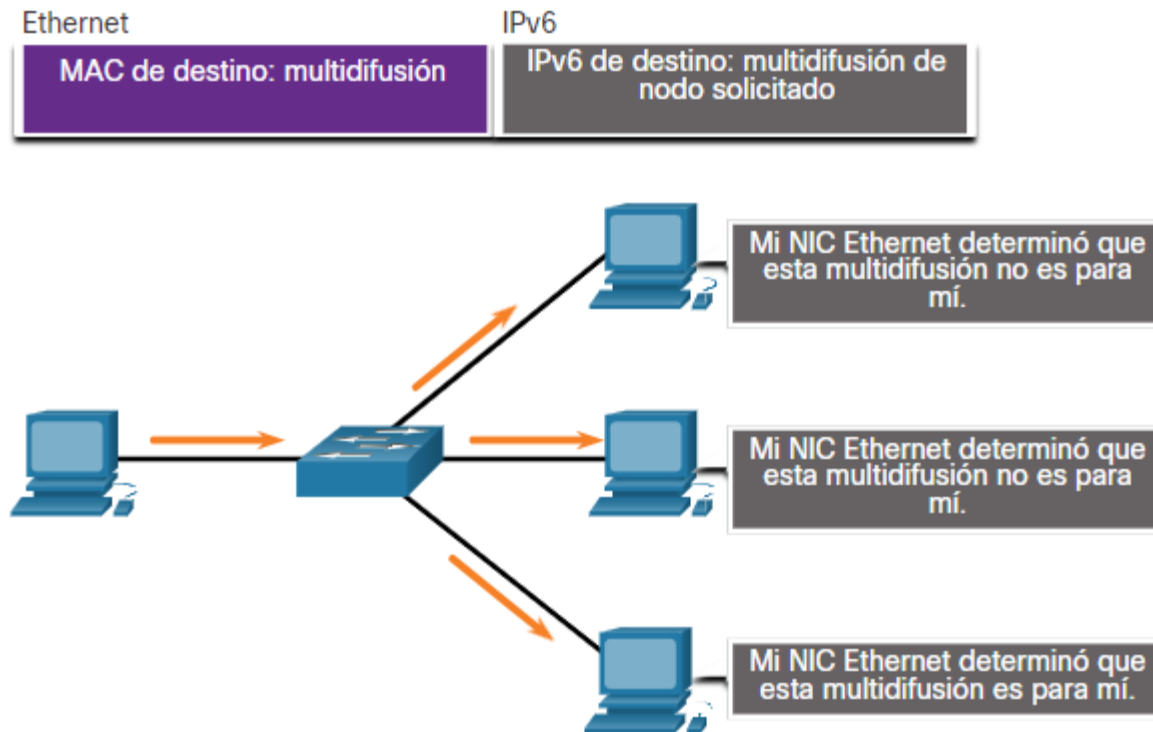
## Direcciones de multidifusión de nodo solicitado

- Una dirección de multidifusión de nodo solicitado es similar a una dirección de multidifusión de todos los nodos.
- La ventaja de una dirección de multidifusión de nodo solicitado es que se asigna a una dirección especial de multidifusión de Ethernet. Esto permite que la NIC Ethernet filtre el marco 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.



# MULTICAST (UNO A MUCHOS)

## Direcciones de multidifusión de nodo solicitado



# MULTICAST (UNO A MUCHOS)

- Formato de dirección IPv6 multicast:



# MULTICAST (UNO A MUCHOS)



- Prefijo: siempre vale 1111 1111 = FF
- Flags. Los tres primeros bits O, R y P están reservados. El último bit T, si vale 0 indica que el grupo multicast es una dirección permanente asignada y bien conocida. Si el valor es 1, indica que es una dirección temporal.
- Scope. Indica el ámbito de la red donde el paquete multicast debe ser propagado
- Group ID. Identificador de grupo. Identifica el grupo multicast concreto al que nos referimos dentro de un determinado ámbito.



# ANYCAST (UNO A LA MAS CERCANA)

- Una dirección anycast identifica a múltiples interfaces IPv6.
- Un paquete enviado a una dirección anycast es entregado solamente a una de estas interfaces, normalmente la más cercana



# ÍNDICE DE ZONA

- Cuando un equipo dispone de varios adaptadores de red, suelen pertenecer a distintos enlaces locales.
- La dirección de enlace local utiliza un índice de zona si el equipo está compuesto por varias interfaces. Este identificador permite determinar la tarjeta de red que se utiliza para enviar la trama.
- La sintaxis del índice de zona depende del sistema operativo
  - En Windows se utiliza el símbolo “%” y un valor numérico.  
Ejemplo: fe80::25dd:ce6e:a0cc:ca71%10



# **DIVISIÓN SUBREDES EN UNA RED IPV6**



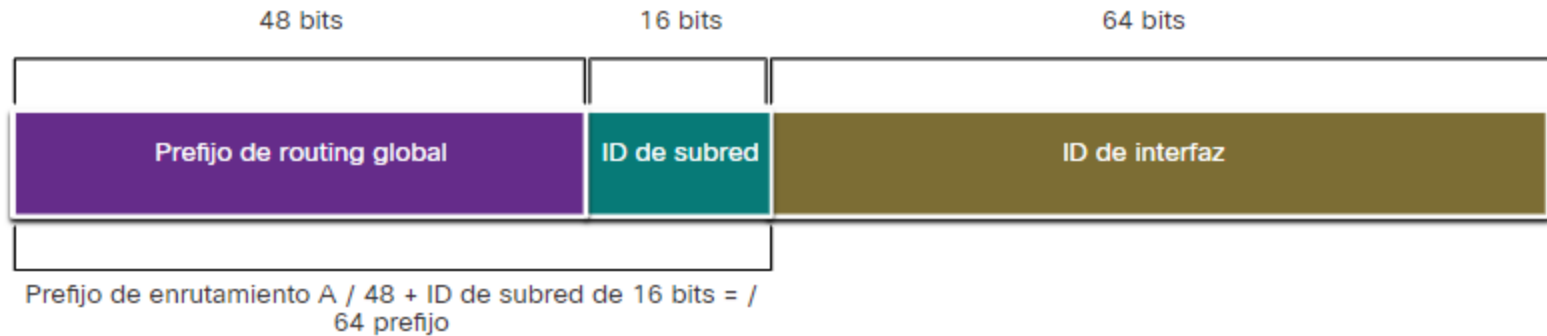


# INTRODUCCIÓN

- Recordemos que con IPv4, debemos tomar prestados bits de la parte del host para crear subredes. Esto se debe a que la subred fue una idea tardía con IPv4.
- Sin embargo, IPv6 se diseñó teniendo en cuenta las subredes.
- Se utiliza un campo ID de subred independiente en IPv6 GUA para crear subredes. Como se muestra en la figura, el campo Id. de subred es el área entre el Prefijo de enrutamiento global y el Id. de interfaz.



# INTRODUCCIÓN



- La ventaja de una dirección de 128 bits es que puede admitir más que suficientes subredes y hosts por subred, para cada red. La conservación de direcciones no es un problema. Por ejemplo, si el prefijo de enrutamiento global es /48, y utilizando un típico 64 bits para el ID de interfaz, esto creará un ID de subred de 16 bits:
  - ID de subred de 16 bits - crea hasta 65.536 subredes.
  - ID de interfaz de 64 bits - admite hasta 18 quintillones de direcciones IPv6 de host por subred (es decir, 18,000,000,000,000,000,000).
- Nota: La división en subredes en la ID de interfaz de 64 bits (o porción de host) también es posible, pero rara vez se requiere.



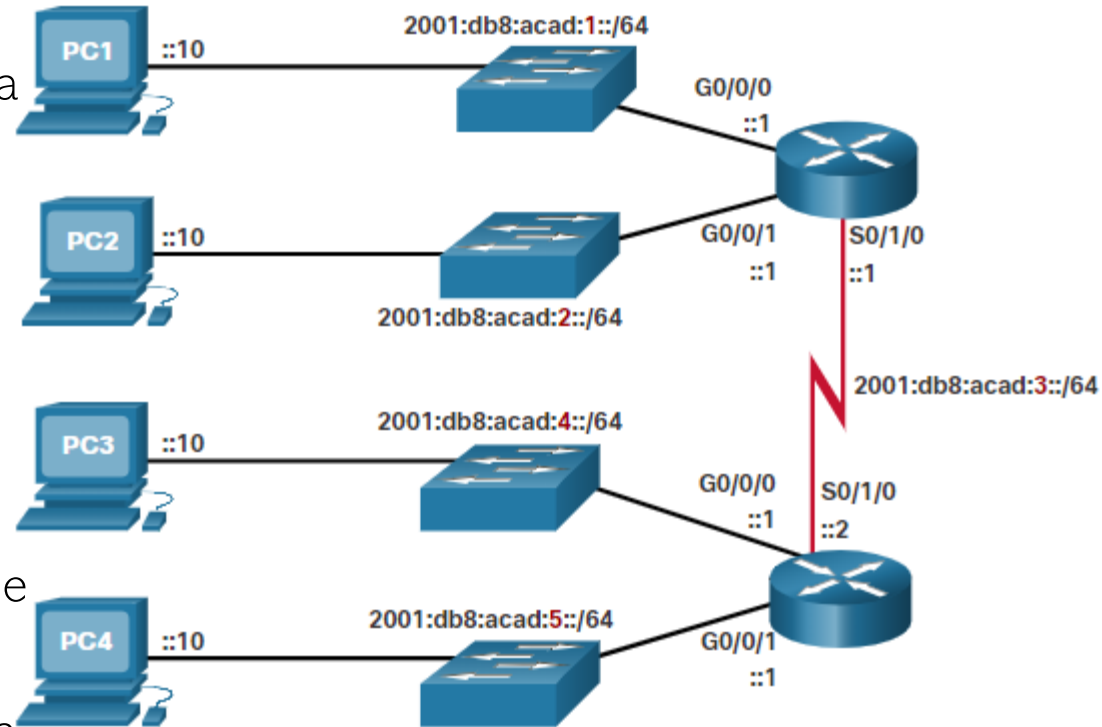
# EJEMPLO

- Suponga que a una organización se le ha asignado el prefijo de enrutamiento global 2001:db8:acad::/48 con una ID de subred de 16 bits. Esto permitiría a la organización crear 65.536 / 64 subredes, como se muestra en la figura. Observe que el prefijo de routing global es igual para todas las subredes. Solo se incrementa el hexteto de la ID de subred en sistema hexadecimal para cada subred.



# EJEMPLO

- Con más de 65.536 subredes para elegir, la tarea del administrador de la red es diseñar un esquema lógico para abordar la red.
- Como se muestra en la figura, la topología de ejemplo requiere cinco subredes, una para cada LAN, así como para el enlace serie entre R1 y R2. A diferencia del ejemplo de IPv4, con IPv6 la subred de enlace serie tendrá la misma longitud de prefijo que las LAN. Aunque esto puede parecer "desperdiciar" direcciones, la conservación de direcciones no es una preocupación cuando se utiliza IPv6.



# RECURSOS BIBLIOGRÁFICOS

- Capítulo 9. Nivel de Red. Direccionamiento IP  
Libro Planificación y Administración de Redes 2ªEd. Editorial Garceta
- Capítulos 8, 9, 11 y 12 de Introduction to NetWorks (CISCO)



# **NIVEL DE RED DIRECCIONAMIENTO IP**

