

# Capítulo 4

## La Capa de Red IP y NAT

Application
Transport
Network
Link
Physical

# La capa de red de internet

- Protocolo de CR **IP** (**protocolo de internet**).
  - Su **propósito**:
    - Explicar formato de datagramas.
    - Definición de direcciones IP.
    - Definición de redes.
    - Definición y uso de tablas de reenvío.
    - Manejo de fragmentación de paquetes.

# La capa de red de internet

- ¿Por qué estudiar IP?

1. Para entender cómo se hacen asignaciones de direcciones de red a máquinas en una red local, a instituciones varias.
  - Para entender cómo designar o identificar a las redes.
2. Para comprender cómo se hace el reenvío en internet.
3. Para comprender cómo se hace la fragmentación y reensamblado de mensajes.
4. IP da la base conceptual para entender otros protocolos de capa de red en internet.
  - P. ej. protocolos de enrutamiento.

# La capa de red de internet

- IP tiene dos versiones:
  - IPv4: trabaja con direcciones IP de 32 bits.
  - IPv6: trabaja con direcciones IP de 128 bits.
  - Los formatos de datagrama de las dos versiones son diferentes.
- En este archivo estudiamos IPv4.
- En los complementos de IP se resume IPv6.

# Aprenderemos

- **La capa de red de internet – Metas:**

1. **Datagramas IPv4**

- Para poder comprender cómo los enrutadores/hosts hacen el procesamiento de paquetes.

2. Direcciones IPv4

3. Conceptos fundamentales en los que nos basamos

4. Asignación de redes a organizaciones

5. Tablas de enrutamiento

- Uso de enfoque CIDR

6. Control de tamaño de tablas de enrutamiento

- Uso de enfoque agregación de prefijos

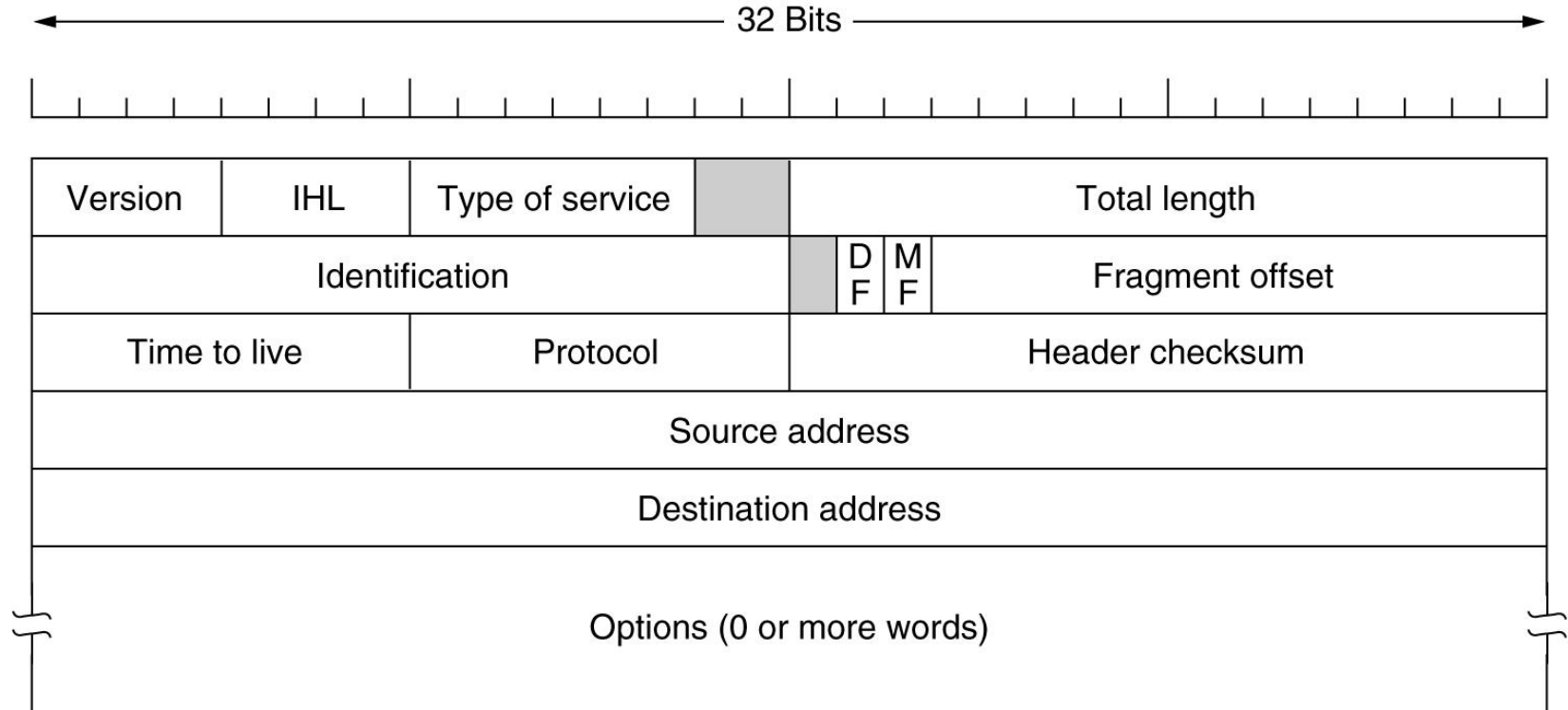
7. Racionamiento de uso de direcciones IPv4

- Uso del enfoque NAT

# Datagrama IP

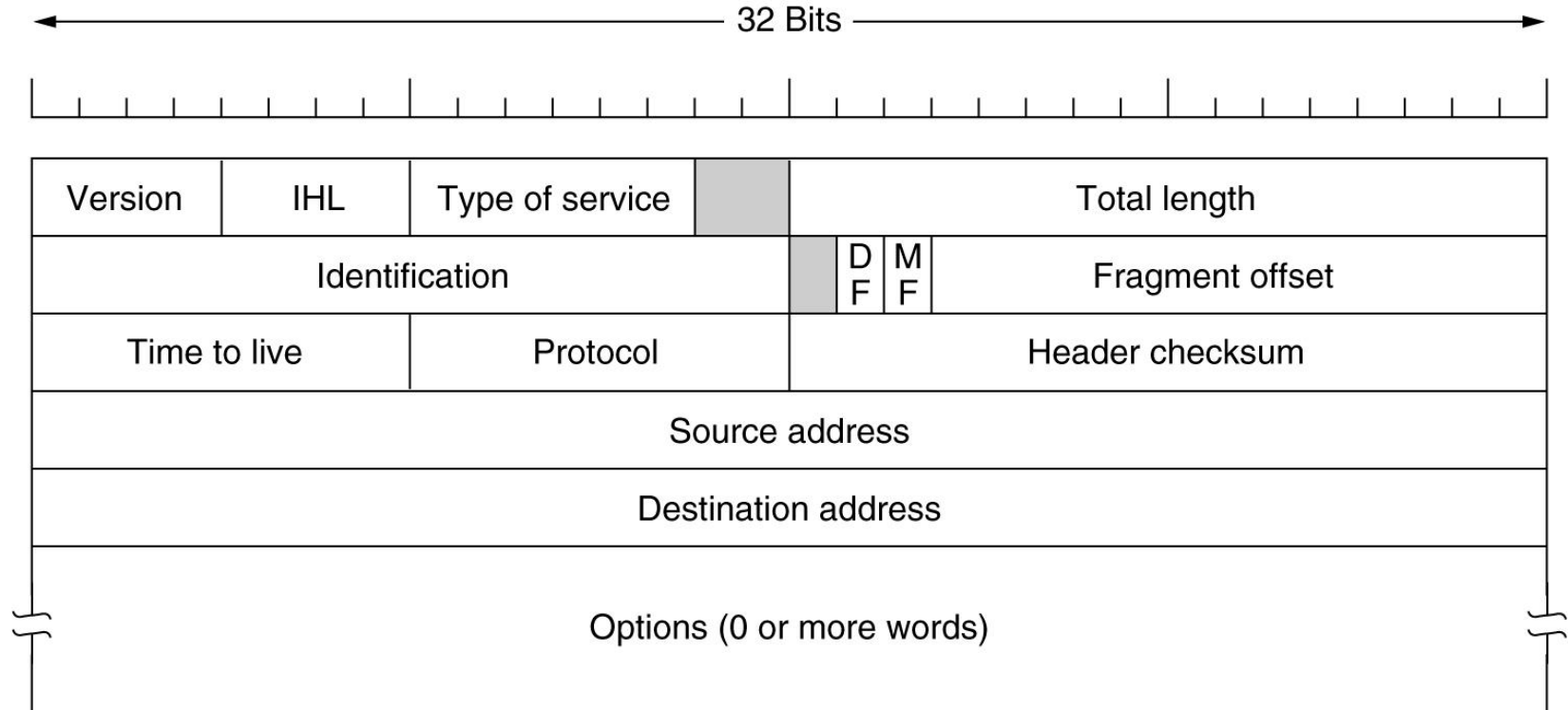
- **datagrama IP** = encabezado + texto
- **encabezado** = parte fija de 20 bytes + parte opcional
  - ❑ Un encabezado tiene varios **campos**.
  - ❑ Cada *tipo de información* que necesito va en uno o más campos
  - ❑ La parte opcional tiene longitud variable
- ¿Cómo puedo hacer para saber dónde termina el encabezado?
- ¿Cómo puedo hacer para saber dónde termina un datagrama?

# Datagrama IP



- campo **IHL** (4b):
  - ❑ longitud del encabezado en palabras de 32b ( $5 \leq \text{valor} \leq 15$ ).
  - ❑ 5 cuando no hay opciones.
- Campo **longitud total**: (2B) de encabezado + datos  $\leq 65535$  B

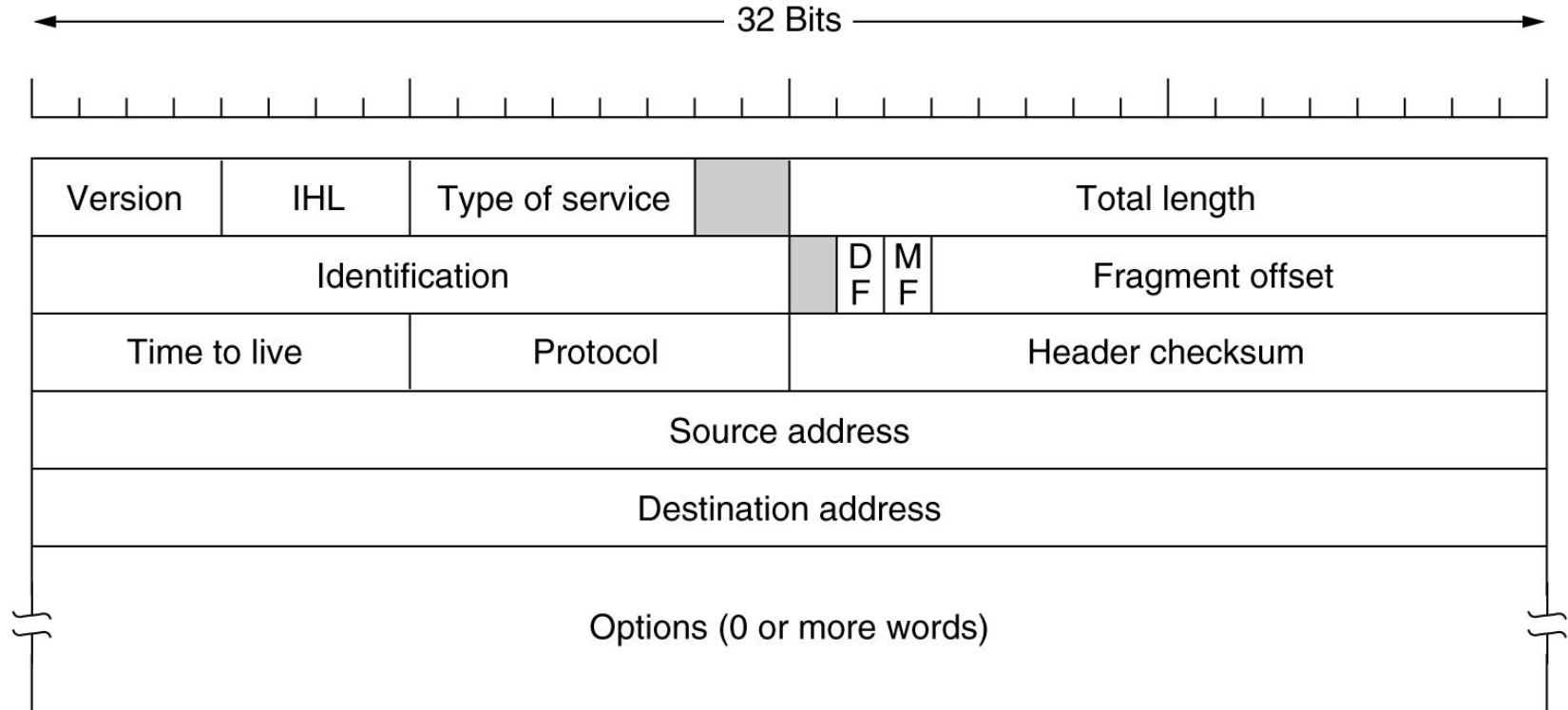
# Datagrama IP



- Campo **tipo de servicio**:
  - ☐ los 2 últimos bits se usan para información de notificación de congestión (para ECN).
  - ☐ Los 6 primeros bits se usan para indicar clase de servicio (p.ej. entrega rápida, transmisión libre de errores, etc.)

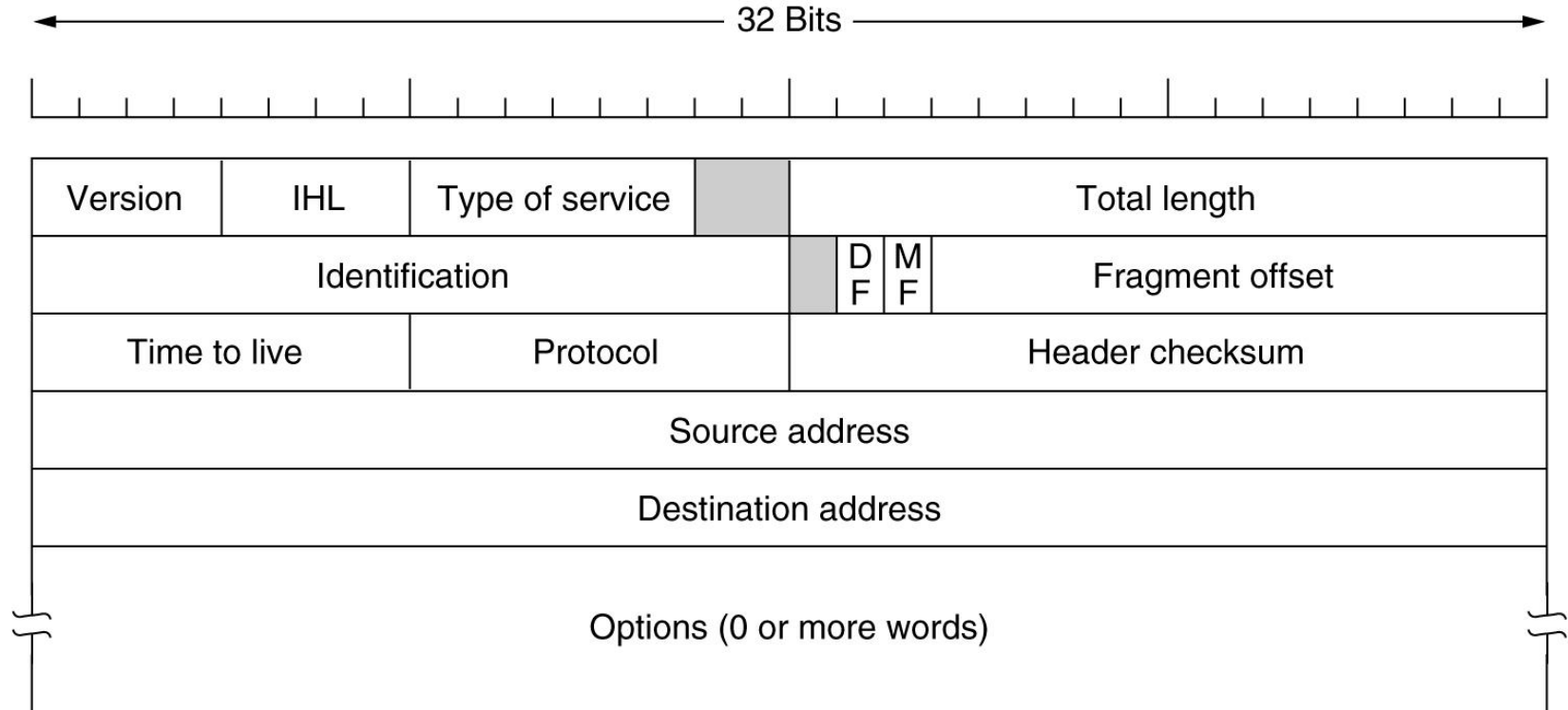


# Datagrama IP



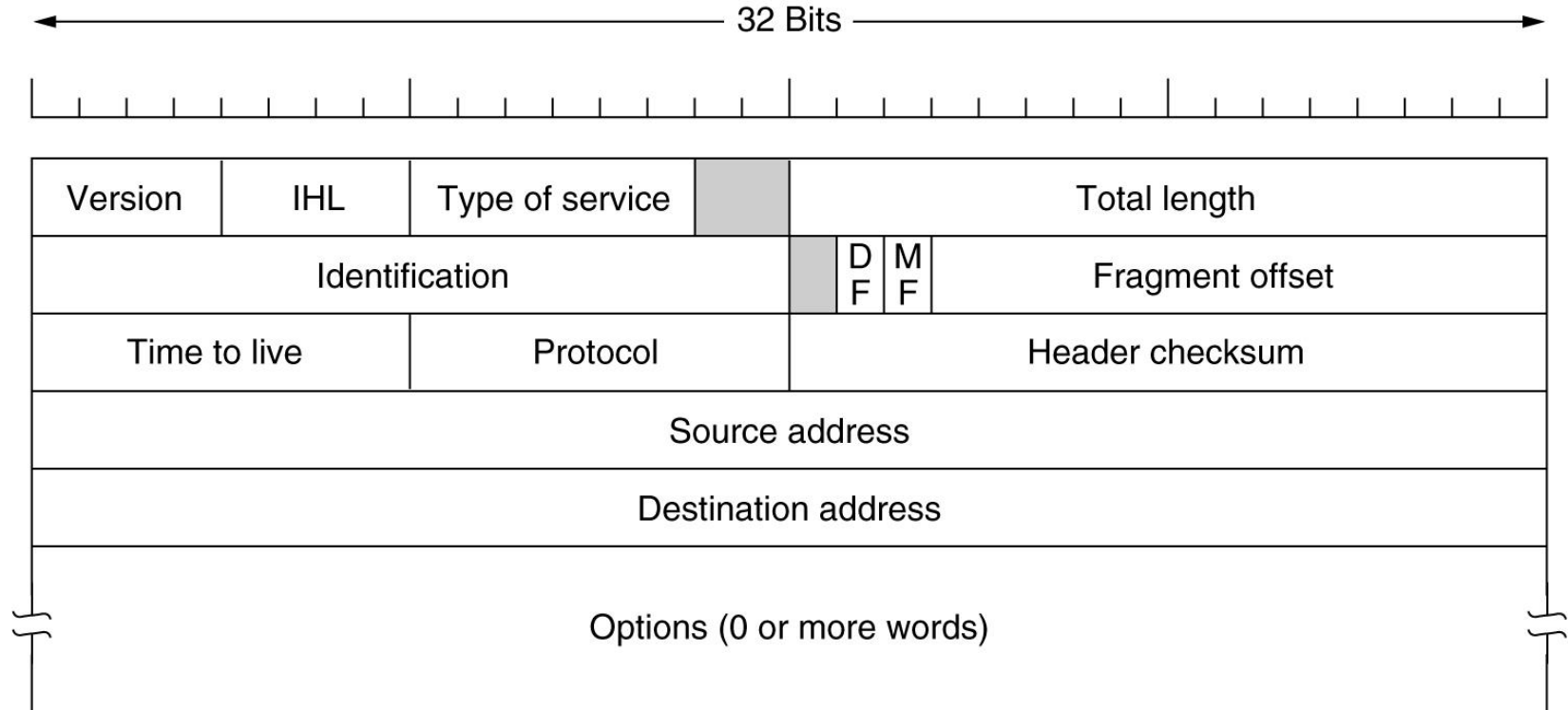
- El campo **protocolo** (8 b) dice a cuál proceso de transporte (p.ej. TCP, UDP, etc.) entregar el paquete.
- El campo **identificación** se usa para que el host de destino determine a qué paquete un fragmento pertenece.

# Datagrama IP



- El **campo tiempo de vida** se usa para limitar el tiempo de vida de un paquete.
  - ☐ Debe decrementarse en cada salto.
  - ☐ Cuando llega a cero el paquete es descartado y se manda un paquete de advertencia al host de origen.
  - ☐ Esto evita que los paquetes anden dando vueltas demasiado tiempo.

# Datagrama IP



- El **campo suma de verificación**: se usa para detectar errores cuando el paquete viaja a lo largo de la red.
  - ☐ Debe recalcularse en cada salto, porque el campo tiempo de vida siempre cambia.

# Aprenderemos

- **La capa de red de internet – Metas:**
  1. Datagramas IPv4
  2. **Direcciones IPv4**
    - Para entender su significado y a quiénes son asignadas estas direcciones.
  3. Conceptos fundamentales en los que nos basamos
  4. Asignación de redes a organizaciones
  5. Tablas de enrutamiento
    - Uso de enfoque CIDR
  6. Control de tamaño de tablas de enrutamiento
    - Uso de enfoque agregación de prefijos
  7. Racionamiento de uso de direcciones IPv4
    - Uso del enfoque NAT

# Datagrama IP

- En un datagrama IP los campos **direcciones de origen y de destino**
  - Cada una tiene 32 b.
  - indican el *número de red* y el *número de máquina*.
  - **Consecuencias:**
    - uso números IP diferentes para distinguir las máquinas de una red.
    - Las direcciones IP son ***jerárquicas***.

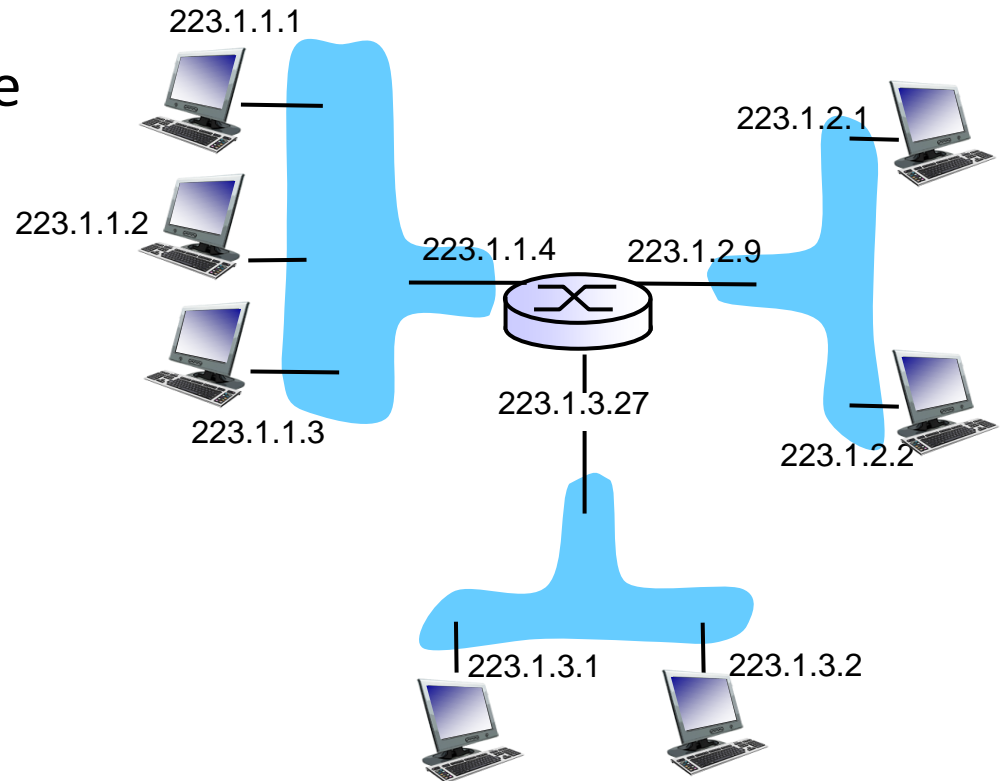
# Direcciones IP

- Cada host y enrutador *en la internet* tiene una **dirección IP**.
  - **Notación para las direcciones IP**
    - La dirección IP más baja es 0.0.0.0 y la más alta es: 255.255.255.255.
  - **Una máquina puede tener más de un IP**
    - Una máquina tiene un IP por cada red a la que está conectada
    - Pero el asunto es más complejo como vemos a continuación.

# Direcciones IP

- *interfaz*: conexión entre host/enrutador y enlace físico.

- Un enrutador tiene muchas interfaces, una por cada línea de salida.
- Un host tiene una o dos interfaces:
  - con Ethernet cableada,
  - con inalámbrica 802.11



- *Cada interfaz tiene asociada una dirección IP*

$$223.1.1.1 = \underbrace{11011111}_{223} \underbrace{00000001}_1 \underbrace{00000001}_1 \underbrace{00000001}_1$$

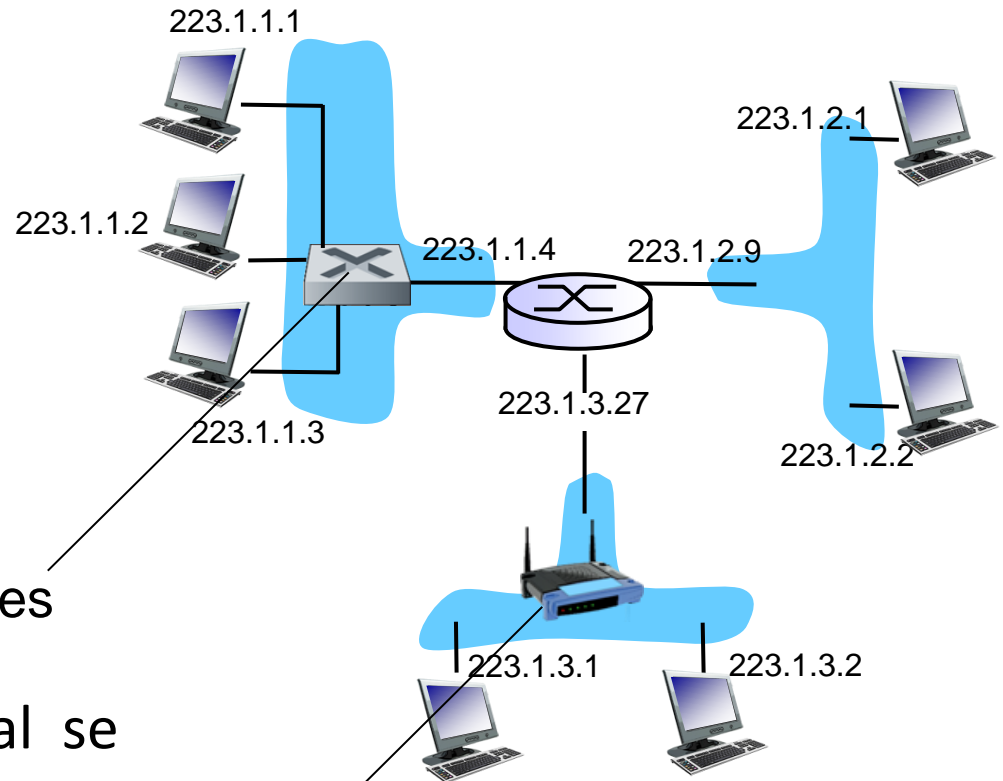
# Direcciones IP

**Repaso:** ¿Cómo están las interfaces actualmente conectadas entre sí?

Se usan conmutadores y estaciones base.

**A:** wired Ethernet interfaces connected by Ethernet switches

Fijarse que en cada red local se Usa la misma dirección de red.



**A:** wireless WiFi interfaces connected by WiFi base station





# Aprenderemos

- **La capa de red de internet – Metas:**
  1. Datagramas IPv4
  2. Direcciones IPv4
  3. **Conceptos fundamentales en los que nos basamos**
    - Para entender cómo asignar nombre a redes y cómo describir ciertos parámetros de las mismas.
  4. Asignación de redes a organizaciones
  5. Tablas de enrutamiento
    - Uso de enfoque CIDR
  6. Control de tamaño de tablas de enrutamiento
    - Uso de enfoque agregación de prefijos
  7. Racionamiento de uso de direcciones IPv4
    - Uso del enfoque NAT

# Conceptos Básicos

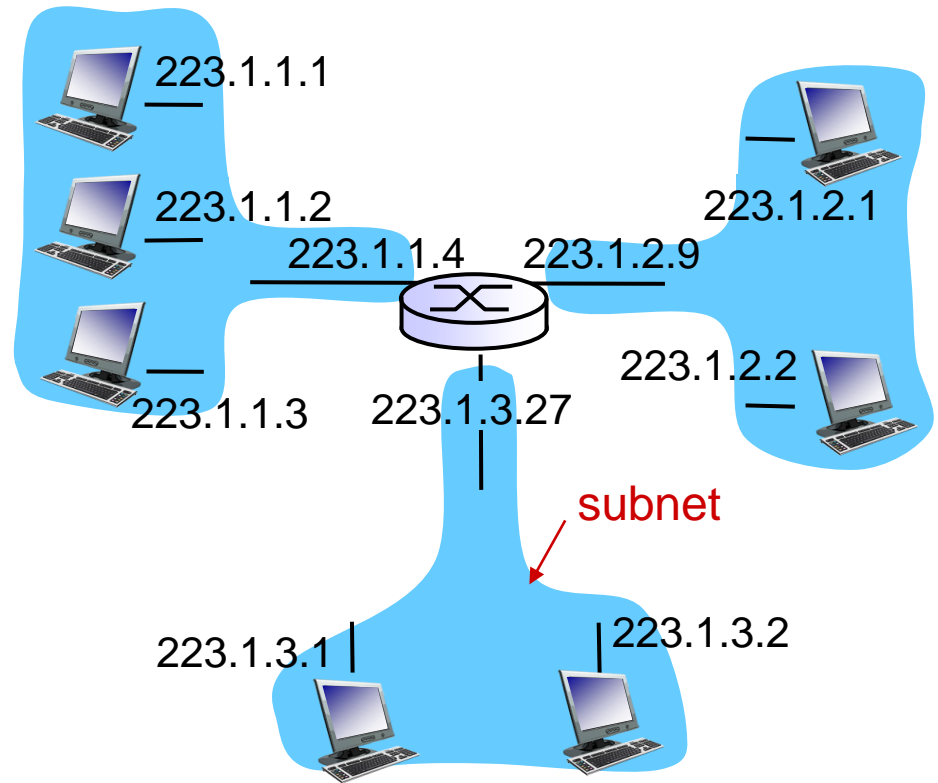
- Una red corresponde a un **bloque contiguo** del espacio de direcciones IP llamado **prefijo**.
  - Prefijos se escriben dando la dirección IP más baja en el bloque y la cantidad de bits usadas para la dirección de la red.
  - **Ejemplo: ¿Qué significa el prefijo 128.208.0.0/24?**
    - la porción de la red es de 24 bits,
    - que tengo  $2^8$  máquinas en la red y
    - la dirección IP más baja en el bloque es 128.208.0.0.

# Conceptos Básicos

- **Nomenclatura:** una red de /xx significa que la  **porción** de la red tiene xx bits.
  - P. ej. : una red de /20.
- Una **máscara** está formada de 1s para identificar la red seguido de 0s para identificar las máquinas.
- **¿Cuál es la máscara de 128.208.0.0/24?**
- 11111111 11111111 11111111 00000000 
- Otra forma de expresarla es: 255.255.255.0

# Subredes

- **Concepto de subred (libro de Kurose):**
  - conjunto de interfaces de dispositivos con la **misma** parte de red de la dirección IP
  - **Otra definición:** máquinas que se pueden alcanzar físicamente entre sí **sin la necesidad de un enrutador interviniente**.

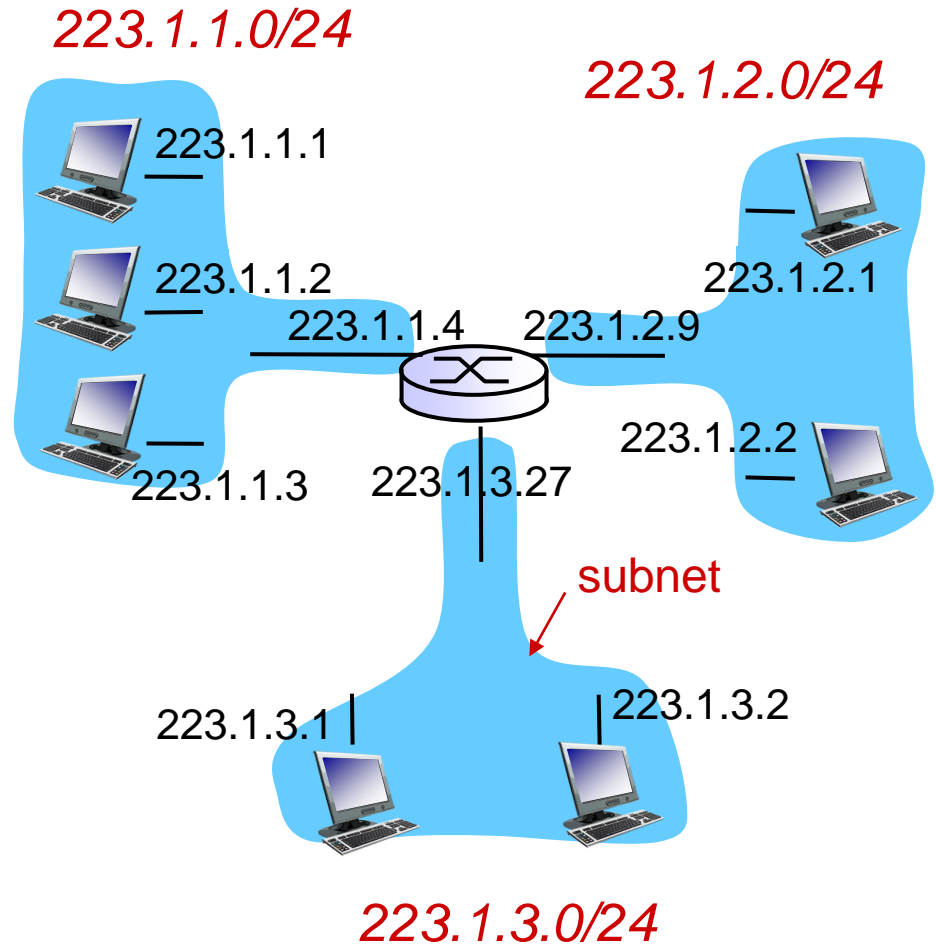


Red consistente de 3 subredes

# Subredes

## Receta:

- ❖ Para determinar las subredes, desacoplar cada interfaz de su host o enrutador, creando islas de redes aisladas
- ❖ Cada red aislada se llama una **subred**
- ❖ Las subredes se indican usando prefijos



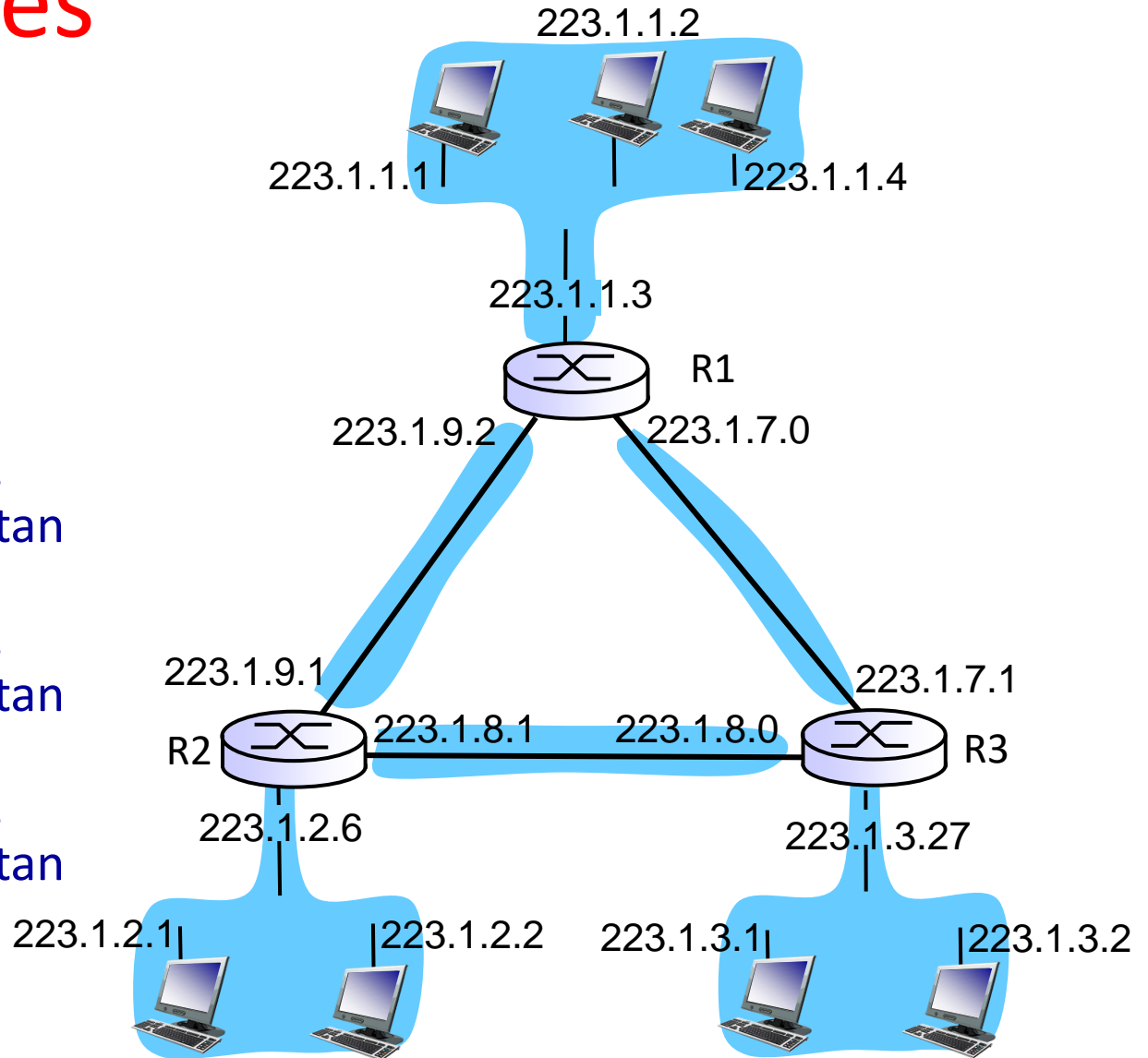
subnet mask: /24

# Subredes

## Ejemplo:

Hay 6 subredes:

- 223.1.1.0/24
- 223.1.2.0/24
- 223.1.3.0/24
- 223.1.9.0/24 para las interfaces que conectan R1 y R2
- 223.1.8.0/24 para las interfaces que conectan R2 y R3
- 223.1.7.0/24 para las interfaces que conectan R3 y R1



# Aprenderemos

- **La capa de red de internet – Metas:**
  1. Datagramas IPv4
  2. Direcciones IPv4
  3. Conceptos fundamentales en los que nos basamos
  4. **Asignación de redes a organizaciones**
    - Para entender cómo se hace la asignación de redes a organizaciones teniendo en cuenta los conceptos y problemas mencionados.
  5. Tablas de enrutamiento
    - Uso de enfoque CIDR
  6. Control de tamaño de tablas de enrutamiento
    - Uso de enfoque agregación de prefijos
  7. Racionamiento de uso de direcciones IPv4
    - Uso del enfoque NAT

# CIDR

- **Efecto sobre el reenvío de paquetes de tener una tabla grande:**
  - Los enrutadores deben buscar en esa tabla para enviar cada paquete y enrutadores en un ISP grande pueden tener que enviar millones de paquetes por segundo.
    - Para esto hace falta hardware especial y una computadora de propósito general no alcanza.
- **Efecto sobre el algoritmo de enrutamiento de tener una tabla grande:**
  - El costo de actualizar las tablas de enrutamiento es grande.
- **Conclusión:** evitar tablas de reenvío demasiado grandes.



# CIDR

- **Problema:** ¿Cómo asignar a una organización una red sin que se desperdicien demasiadas direcciones y sin que las tablas de enrutamiento crezcan demasiado?
  - Si se le da una red demasiado chica a una organización, esta puede expandirse y terminar con más de un prefijo, lo cual aumentaría el tamaño de algunas tablas de enrutamiento.
  - Si se le da una red demasiado grande a una organización, entonces se pueden desperdiciar muchas direcciones IP.
  - Colocar todas las subredes del mundo en una tabla de reenvío hace que la tabla sea demasiado grande.
  - Después veremos que un enrutador en una región no necesita saber de subredes en regiones muy alejadas de ella.

# CIDR

- **Idea de solución para la primera parte de la pregunta:** Alojar las direcciones IP de una red en un bloque contiguo que permite  $2^k$  máquinas.
  - **Ejemplo:** Si un sitio necesita 2000 direcciones, se le da un bloque de 2048 direcciones.
- **Implementación de la solución: CIDR (Classless Inter Domain Routing).**
  - En todas las máquinas de la red, la parte de la dirección IP para identificar la red es la misma.
  - Se representa la red asignada con un único prefijo.

# CIDR

- **Ejercicio:**

- Un bloque de 8192 direcciones IP está disponible comenzando en 194.24.0.0.
- Primero pide Cambridge 2048, luego Oxford 4096, y por último Edinburgh 1024.
- Asignar *adecuadamente* redes a esas universidades por medio de bloques de direcciones de los tamaños pedidos.
- Expresar cada red como un prefijo.

# CIDR

**Solución:** bloques de direcciones IP asignados:

University	First address	Last address	How many	Written as
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

# Aprenderemos

- **La capa de red de internet – Metas:**
  1. Datagramas IPv4
  2. Direcciones IPv4
  3. Conceptos fundamentales en los que nos basamos
  4. Asignación de redes a organizaciones
  5. **Tablas de enrutamiento**
    - **Para entender cómo se construyen las tablas de enrutamiento y cómo se hace el reenvío de datagramas.**
  6. Control de tamaño de tablas de enrutamiento
    - Uso de enfoque agregación de prefijos
  7. Racionamiento de uso de direcciones IPv4
    - Uso del enfoque NAT

# CIDR

- **Problema:** ¿Cómo podría definirse la tabla de enrutamiento?
- **Solución:** el enrutamiento es jerárquico y solo se representan redes - de organismos.
  - Cada entrada de tabla de enrutamiento se extiende para darle una **máscara** de 32 bits.
  - **Tabla de enrutamiento** para todas las redes tiene entradas:  
(dirección IP inicio subred, máscara, línea de salida.)

# CIDR

- **Ejercicio:** Para la figura:

University	First address	Last address	How many	Written as
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

- Definir las entradas de la tabla de enrutamiento
- Omitir la línea de salida

# CIDR

University	First address	Last address	How many	Written as
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

- **Solución:**

- Cambridge 194.24.0.0 -> 194.24.7.255

- Para 7 necesito 3 bits (se usan junto con los 8 primeros para n° de host)

- Máscara: 255.255.248.0 (248=1111 1000)



- Max: 2048 hosts

- las entradas son:

- **Dirección**

- Máscara**

- C: 11000010 00011000 00000000 00000000

- 11111111 11111111 11111000 00000000

- E: 11000010 00011000 00001000 00000000

- 11111111 11111111 11111100 00000000

- O: 11000010 00011000 00010000 00000000

- 11111111 11111111 11110000 00000000



# CIDR

- **Problema: ¿Cómo se usa la tabla de enrutamiento cuando llega un paquete?**
  1. Extraer dirección de destino IP.
  2. Luego analizar la tabla entrada por entrada,
    - Hacer AND de la máscara de la entrada con la dirección de destino y comparar el resultado con la dirección IP de inicio de la subred de la entrada.
    - **¿Qué produce ese AND?**
  3. Si coinciden entradas múltiples se usa la máscara más larga (la red más pequeña).

# CIDR

- **Ejercicio:** Un paquete viene con la dirección 194.24.17.4.
  - Si se usa la tabla de enrutamiento anterior, ¿qué entrada se va a usar para enrutar?

- Dirección

## Máscara

- C: 11000010 00011000 00000000 00000000    11111111 11111111 11111000 00000000
- E: 11000010 00011000 00001000 00000000    11111111 11111111 11111100 00000000
- O: 11000010 00011000 00010000 00000000    11111111 11111111 11110000 00000000

## Solución

- Un paquete viene con la dirección 194.24.17.4, el cual en binario es:
  - 11000010 00011000 00010001 00000100
- Se hace AND con la máscara de Cambridge obteniendo:

## • Dirección

## Máscara

- C: 11000010 00011000 00000000 00000000    11111111 11111111 11111000 00000000
- E: 11000010 00011000 00001000 00000000    11111111 11111111 11111100 00000000
- O: 11000010 00011000 00010000 00000000    11111111 11111111 11110000 00000000

## Solución

- Un paquete viene con la dirección 194.24.17.4, el cual en binario es:
  - 11000010 00011000 00010001 00000100
- Se hace AND con la máscara de Cambridge obteniendo:
  - 11000010 00011000 00010000 00000000
  - Este valor no concuerda con la dirección base de Cambridge.
- Se hace AND con la máscara de Edinburgh obteniendo:

- Dirección

## Máscara

- C: 11000010 00011000 00000000 00000000    11111111 11111111 11111000 00000000
- E: 11000010 00011000 00001000 00000000    11111111 11111111 11111100 00000000
- O: 11000010 00011000 00010000 00000000    11111111 11111111 11110000 00000000

## Solución

- Un paquete viene con la dirección 194.24.17.4, el cual en binario es:
  - 11000010 00011000 00010001 00000100
- Se hace AND con la máscara de Cambridge obteniendo:
  - 11000010 00011000 00010000 00000000
  - Este valor no concuerda con la dirección base de Cambridge.
- Se hace AND con la máscara de Edinburgh obteniendo:
  - 11000010 00011000 00010000 00000000
  - Este valor no concuerda con la dirección base de Edinburgh.
- Luego se prueba con Oxford obteniendo:

## • Dirección

## Máscara

- C: 11000010 00011000 00000000 00000000    11111111 11111111 11111000 00000000
- E: 11000010 00011000 00001000 00000000    11111111 11111111 11111100 00000000
- O: 11000010 00011000 00010000 00000000    11111111 11111111 11110000 00000000

## Solución

- Un paquete viene con la dirección 194.24.17.4, el cual en binario es:
  - 11000010 00011000 00010001 00000100
- Se hace AND con la máscara de Cambridge obteniendo:
  - 11000010 00011000 00010000 00000000
  - Este valor no concuerda con la dirección base de Cambridge.
- Se hace AND con la máscara de Edinburgh obteniendo:
  - 11000010 00011000 00010000 00000000
  - Este valor no concuerda con la dirección base de Edinburgh.
- Luego se prueba con Oxford obteniendo:
  - 11000010 00011000 00010000 00000000
  - Este valor concuerda con la base de Oxford.
- Si no se encuentran más correspondencias a continuación, la entrada de Oxford es usada.

# Aprenderemos

- **La capa de red de internet – Metas:**
  1. Datagramas IPv4
  2. Direcciones IPv4
  3. Conceptos fundamentales en los que nos basamos
  4. Asignación de redes a organizaciones
  5. Tablas de enrutamiento
    - Uso de enfoque CIDR
  6. **Control de tamaño de tablas de enrutamiento**
    - Para controlar el tamaño de las tablas de enrutamiento
    - Uso de enfoque de agregación de prefijos
  7. Racionamiento de uso de direcciones IPv4
    - Uso del enfoque NAT

# CIDR

- **Solución: CIDR (Classless Inter Domain Routing) Cont.**
  - Para evitar que las tablas de enrutamiento crezcan demasiado
  - se combinan varios prefijos en un prefijo único más grande (conocido como **superred**).
    - A esto se le llama **agregación de prefijos**.
  - **Ejemplo:** la misma dirección IP que un enrutador trata como parte de un /22 puede ser tratada por otro enrutador como parte de un /20 más grande.



# CIDR

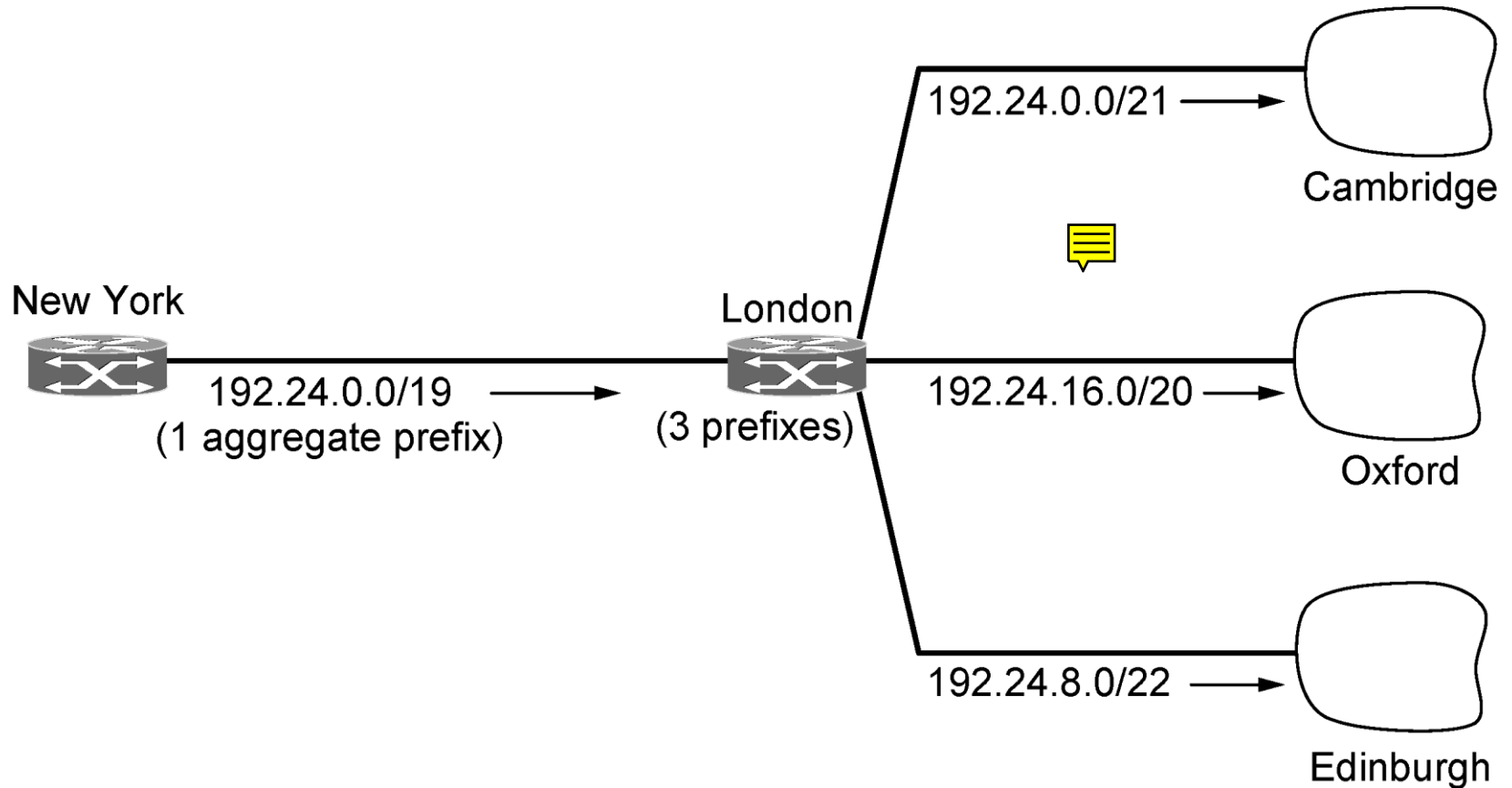
- A distintas regiones geográficas se asignan distintos espacios de direcciones. ¿Cómo aprovechar esto en la agregación de prefijos?
- **Idea:** combinar prefijos de varias redes que están ***en una misma región geográfica*** en un prefijo para un enrutador que está en otra ***región alejada***.
- **Ejemplo:** prefijos de varias redes de Inglaterra pueden combinarse en un prefijo para un enrutador de Estados Unidos.

# CIDR con agregación de prefijos

- **Ejercicio:** aplicar agregación de prefijos a las 3 redes de universidades de Inglaterra (**ayuda:** ellas entran en bloque de 8192 direcciones).

University	First address	Last address	How many	Written as
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

El proceso de enrutamiento en Londres combina los 3 prefijos en una entrada agregada para el prefijo 192.24.0.0/19 que es pasado al enrutador de New York. Este prefijo contiene 8K direcciones y cubre las 3 universidades.



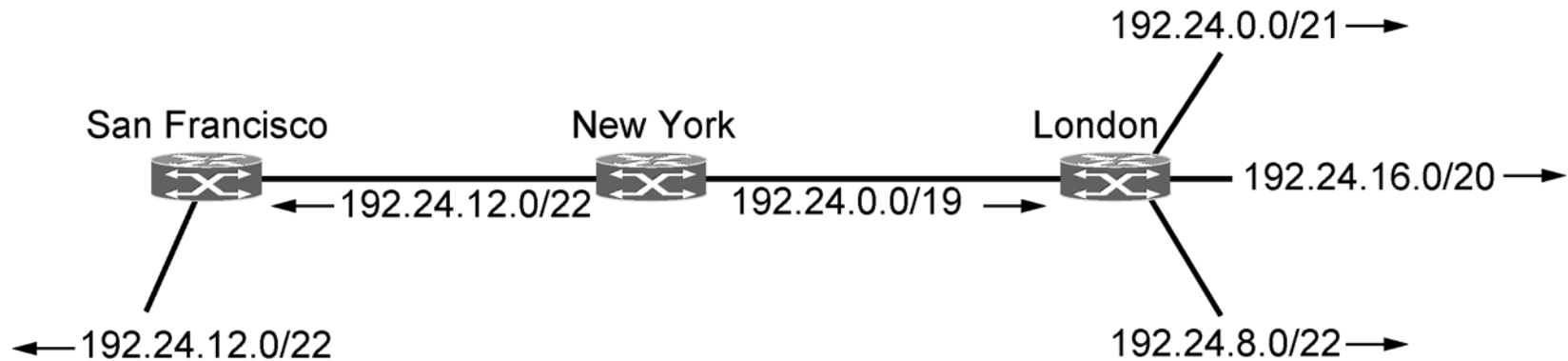
Aggregation of IP prefixes.

Usando agregación de prefijos, los 3 prefijos anteriores fueron combinados en uno

# CIDR con agregación de prefijos

- Cuándo se prende agregación de prefijos, es un ***proceso automático***.
- La agregación de prefijos es fuertemente usada en la Internet y puede reducir el tamaño de las tablas de los enrutadores en alrededor de 200.000 prefijos.
- ¿Pero esta idea de agregación de prefijos no interfiere con redes más chicas que no fueron agregadas y que caen en bloques agregados?
- No, porque los paquetes son enviados en la dirección de la ruta más específica o el **prefijo más largo a cazar (longest matching prefix)**.
  - El trabajar de ese modo provee flexibilidad,

# CIDR con agregación de prefijos



Longest matching prefix routing at the New York router.

**Ejemplo:** el bloque de 1024 que no se asignó a las 3 universidades de Inglaterra se asocia a una red de San Francisco.

- Entonces se usa un prefijo más general para enviar a Londres y un prefijo más específico para mandar a San Francisco.

# Aprenderemos

- **La capa de red de internet – Metas:**
  1. Datagramas IPv4
  2. Direcciones IPv4
  3. Conceptos fundamentales en los que nos basamos
  4. Asignación de redes a organizaciones
  5. Tablas de enrutamiento
    - Uso de enfoque CIDR
  6. Control de tamaño de tablas de enrutamiento
    - Uso de enfoque agregación de prefijos
  7. **Racionamiento de uso de direcciones IPv4**
    - **Para prolongar el uso de IPv4 a pesar de la escasez de direcciones IPv4.**
    - **Uso del enfoque NAT**

# NAT

- **Situación:** Un ISP tiene una red de  $/c$ ; esto quiere decir que se le dan  $2^{(32 - c)}$  números IP para máquinas.
  - Con el esquema actual los clientes no pueden tener más de  $2^{(32 - c)}$  máquinas usando el servicio del ISP en un momento dado.
- **Problema:** ¿Cómo aumentar la cantidad máquinas que usan el servicio del ISP bien por arriba de las  $2^{(32 - c)}$  a pesar de tener una red de  $/c$ ?
- **Consecuencia:** Resolverlo aumentaría drásticamente la cantidad de máquinas que pueden acceder a internet.

# NAT

- **Solución:** **traducción de dirección de red (NAT)**.  
Asignar un solo N° de IP a cada organización para el tráfico de internet.
  1. Dentro de la organización cada computadora tiene una dirección IP única que se usa para el tráfico interno. (o sea, estos números IP no se usan en internet – solo adentro de la organización y pueden repetirse en distintas organizaciones)
  2. Cuando un paquete sale de la organización y va al ISP, se presenta una **traducción de dirección** (de la dirección de la computadora en la organización a la dirección IP usada por la organización en internet).



# NAT

- **Implementación:** Para hacer posible este esquema los 3 rangos de direcciones IP se han declarado como privados.
  - Las organizaciones pueden usarlos internamente cuando deseen.
  - La única regla es que **ningún paquete que contiene estas direcciones pueda aparecer en la internet.** Los 3 rangos reservados son:
    - 10.0.0.0 – 10.255.255.255/8 (16,777,216 hosts)
    - 172.16.0.0 – 172.31.255.255/12 (1,048,576 hosts)
    - 192.168.0.0 – 192.168.255.255/16 (65,536 hosts)

# NAT

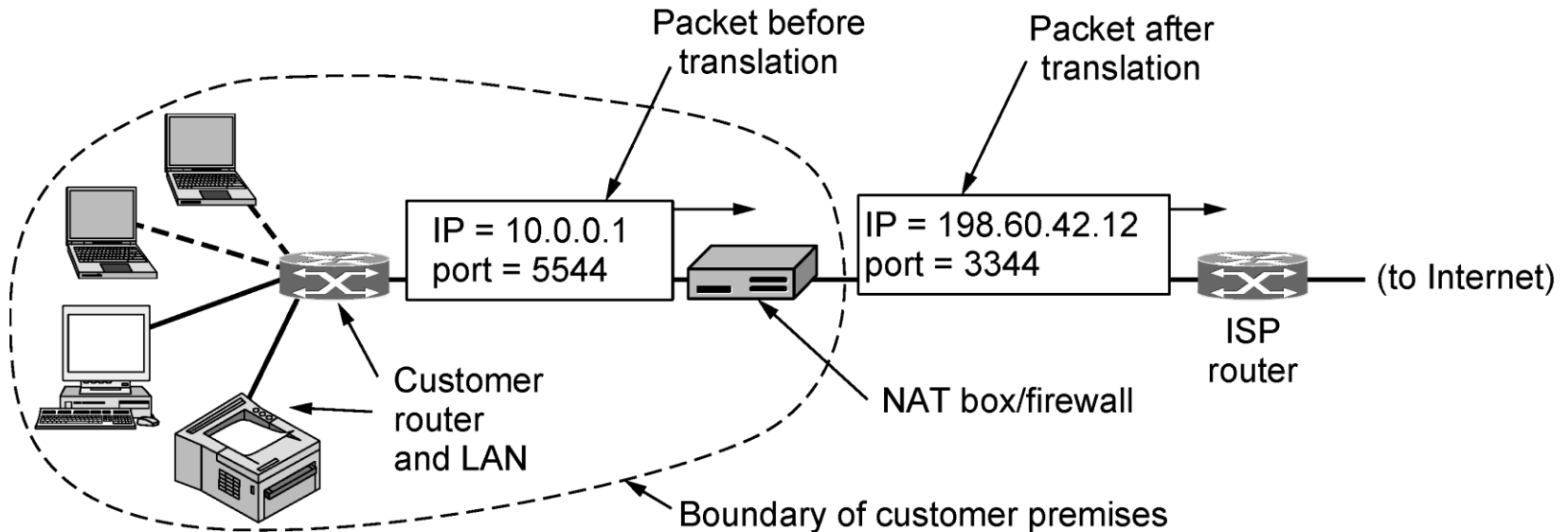


Fig. 60: Colocación y operación de la caja NAT

- Supongamos que en una organización cada máquina tiene una dirección 10.x.y.z.
- **¿Cómo hacer cuando un paquete sale de las instalaciones de la organización?**
- El paquete pasa a través de una **caja NAT** que convierte la dirección interna de origen de IP a la dirección IP de la organización.

# Puertos

- Cada **mensaje TCP saliente** contiene puertos de origen y de destino que sirven para identificar los procesos que usan la conexión en ambos extremos.
- **¿Qué pasa con el uso de puertos cuando un proceso quiere establecer una conexión TCP con un proceso remoto?**
  - se asocia a un puerto TCP sin usar en su máquina conocido como **puerto de origen** (indica dónde enviar mensajes entrantes de esta conexión).
  - El proceso proporciona también un **puerto de destino** para decir a quién dar los mensajes en el lado remoto.

# NAT

- **Problema:** Cuando la respuesta vuelve, por ejemplo de un servidor web, se dirige naturalmente a dirección IP de la compañía, **¿cómo sabe ahora la caja NAT con qué dirección se reemplaza?** (ayuda: usar puerto de origen)
- **Solución 1:** Guardar asociación en la caja NAT de número IP al puerto de origen que viene en el mensaje TCP/UDP dentro del paquete.
  - Estas asociaciones se pueden guardar en una **tabla** en la caja NAT.
- **¿Qué les parece esta solución?**

# NAT

- **Evaluación:** podría ocurrir que dos conexiones de las máquinas 10.0.0.1 y 10.0.0.2 usaran el puerto de origen 5000 por ejemplo.
  - Luego el puerto de origen no sirve para identificar el N° de IP.
- **Solución 2:** distinguir entre el N° de puerto usado para identificar la máquina (o sea IPs en la red interna) y el N° de puerto usado por TCP/UDP para identificar la conexión.
  - Cuando llega un paquete con puerto de origen, se busca en la tabla el IP del nodo y el N° del puerto que se usa para la conexión.

# NAT

## – Tabla de traducción de la caja NAT.

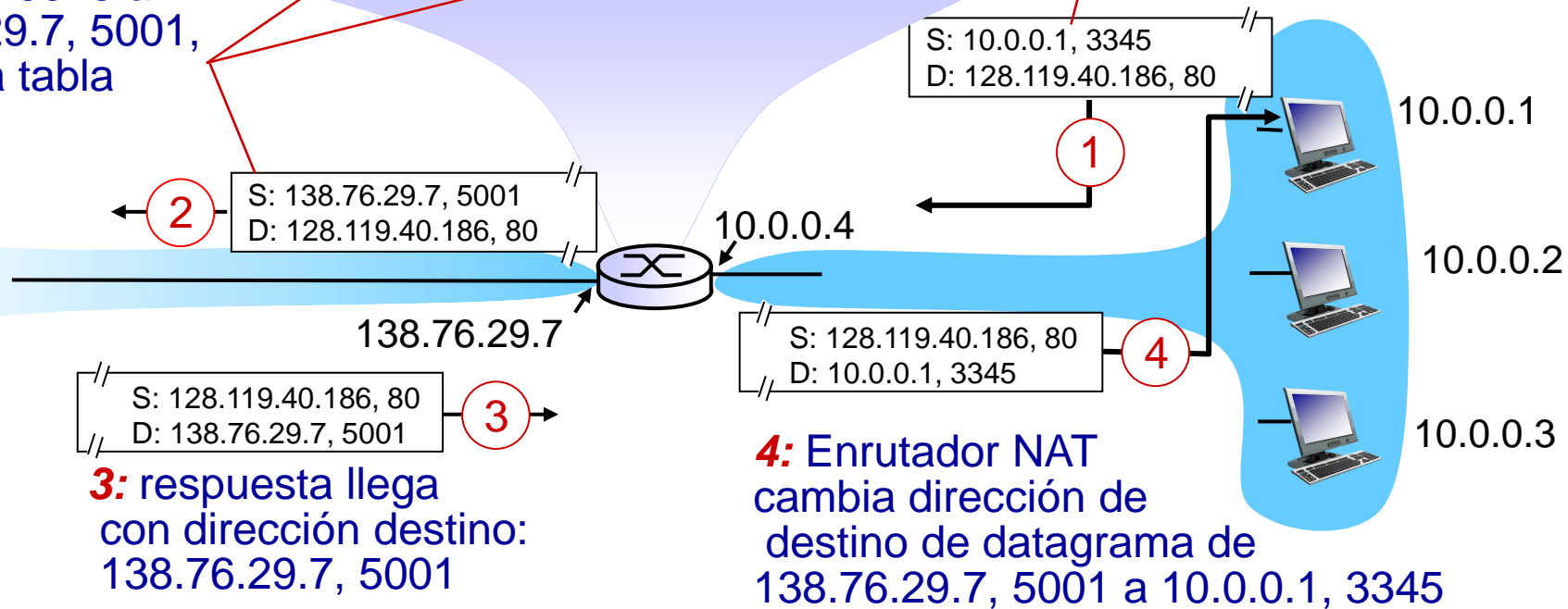
- Los **índices** en la tabla son *números de puerto para identificar la máquina*.
- Una entrada de la tabla contiene:  
(número de puerto para identificar la conexión, dirección IP)

# NAT

Tabla de traducción NAT	
WAN side addr	LAN side addr
138.76.29.7, 5001	10.0.0.1, 3345
.....	.....

**2:** Enrutador NAT cambia dirección de origen de datagrama de 10.0.0.1, 3345 a 138.76.29.7, 5001, actualiza tabla

**1:** host 10.0.0.1 envia datagrama a 128.119.40.186, 80



# NAT

- ¿Cómo tratar un paquete que llega a la caja NAT desde el ISP?
  - El puerto de origen en el encabezado TCP se extrae y usa como un índice en la tabla de traducción de la caja NAT.
    - Desde la entrada localizada, la dirección IP interna y el puerto TCP se extraen e insertan en el paquete.
    - Entonces el paquete se pasa al enrutador de la compañía para su entrega normal usando la dirección 10.x.y.z.



# NAT

- ¿Cómo tratar un paquete saliente que entra en la caja NAT?
- La dirección de origen 10.x.y.z se reemplaza por la verdadera dirección IP de la compañía y el campo puerto de origen TCP se reemplaza por un índice en la tabla de traducción de la caja NAT.

# NAT

- **Críticas a NAT**

- Viola el modelo de IP que dice que cada dirección IP identifica una sola máquina globalmente.
- Si la caja NAT se cae y se pierde su tabla de traducción, todas sus conexiones TCP se destruyen.
- Atrasa la adopción de IPv6.