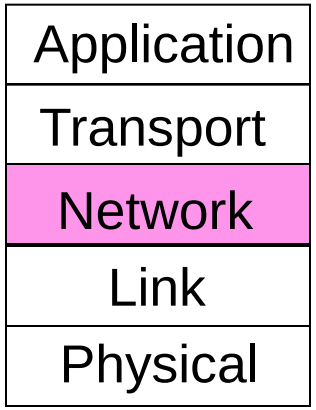
Capítulo 4

La Capa de Red
IP y NAT



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

- **Razones para 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 de paquetes en internet.
3. Para comprender cómo se hace la fragmentación y re-ensamblado de paquetes.
4. IP da la base conceptual para entender otros protocolos de capa de red en internet.
   - P. ej. protocolos de enrutamiento como OSPF y BGP.

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.
- Primero estudiamos IPv4.

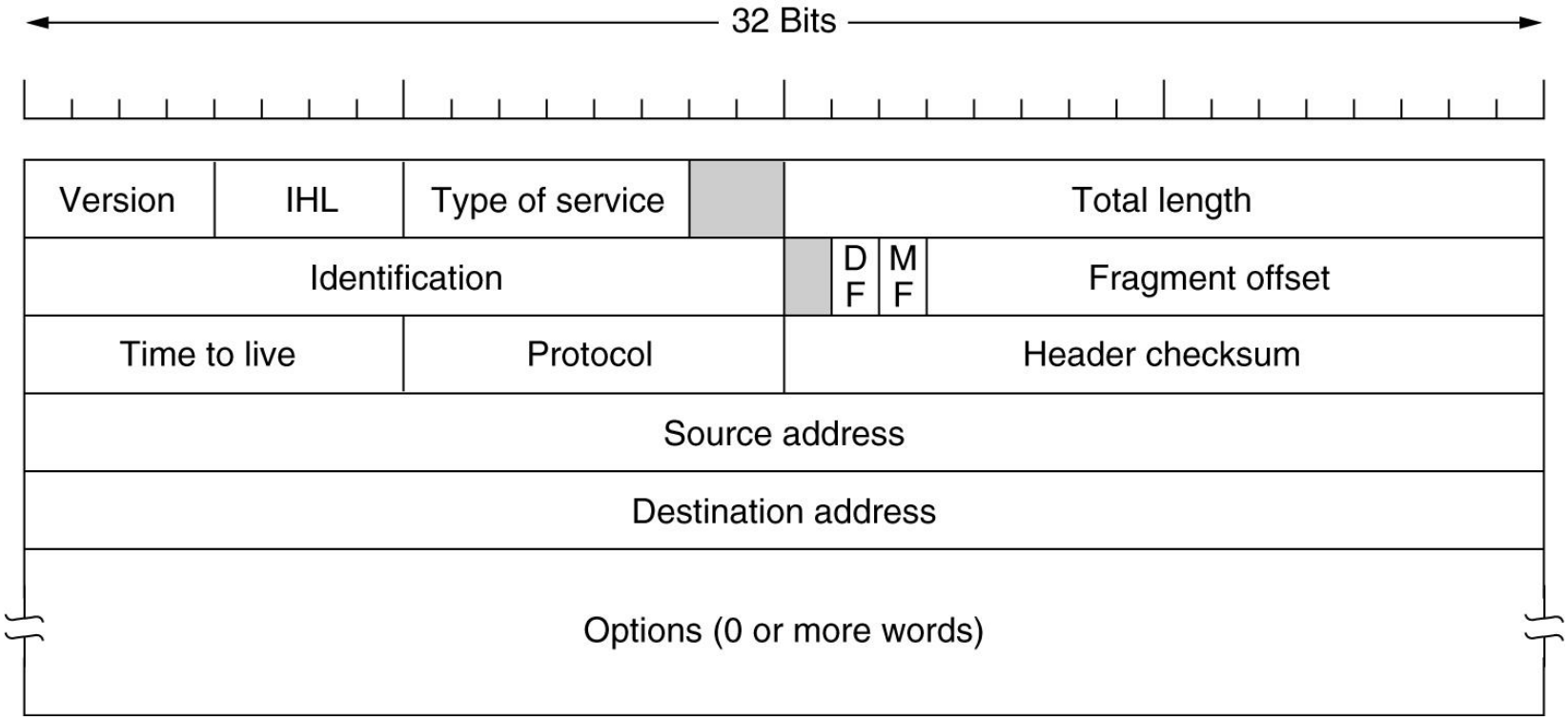
Aprenderemos

- **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

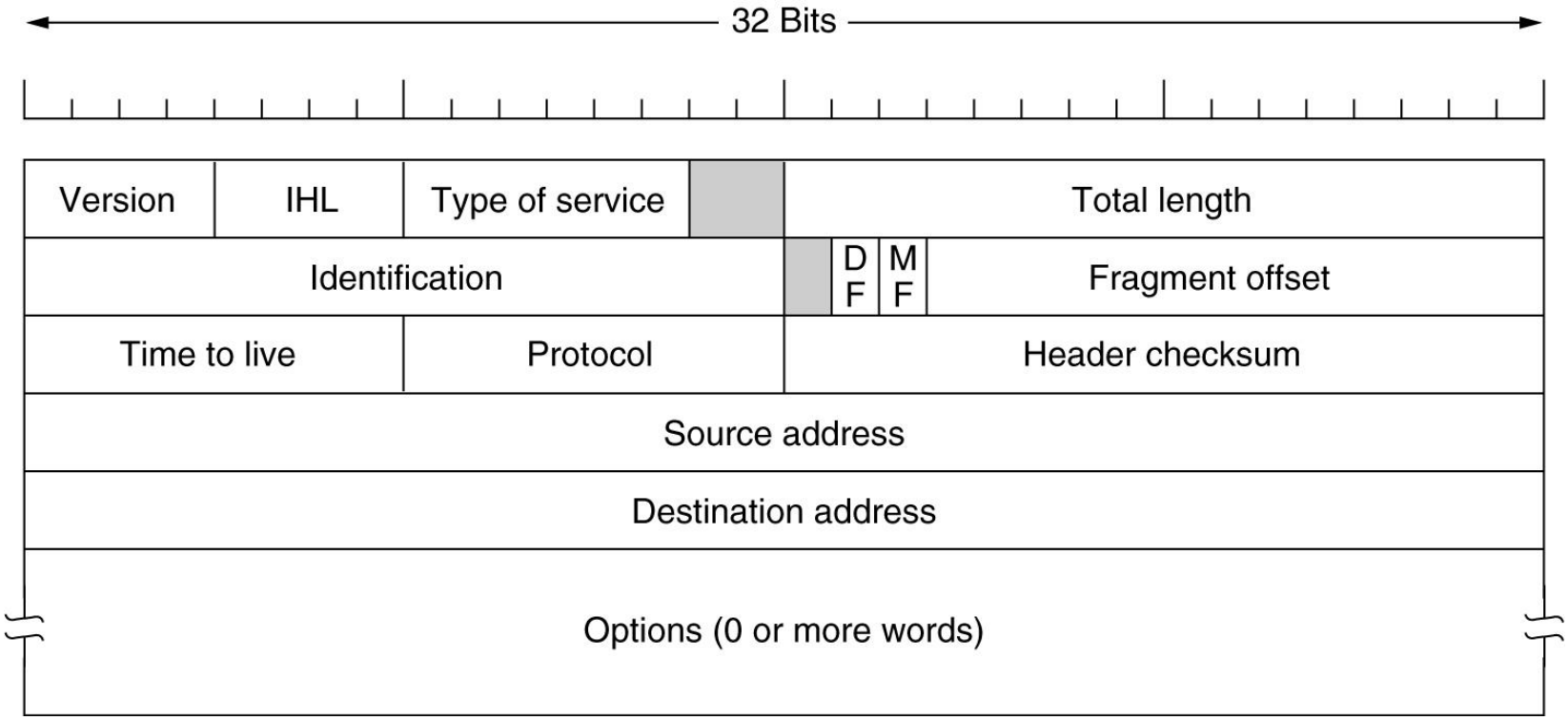
- **datagrama IP** = encabezado + texto
- **encabezado** = parte fija de 20 bytes + parte opcional
  - Un encabezado tiene varios **campos.**
  - Cada *tipo de información* que necesito va en uno o más campos
  - La parte opcional tiene longitud variable

Datagrama IP



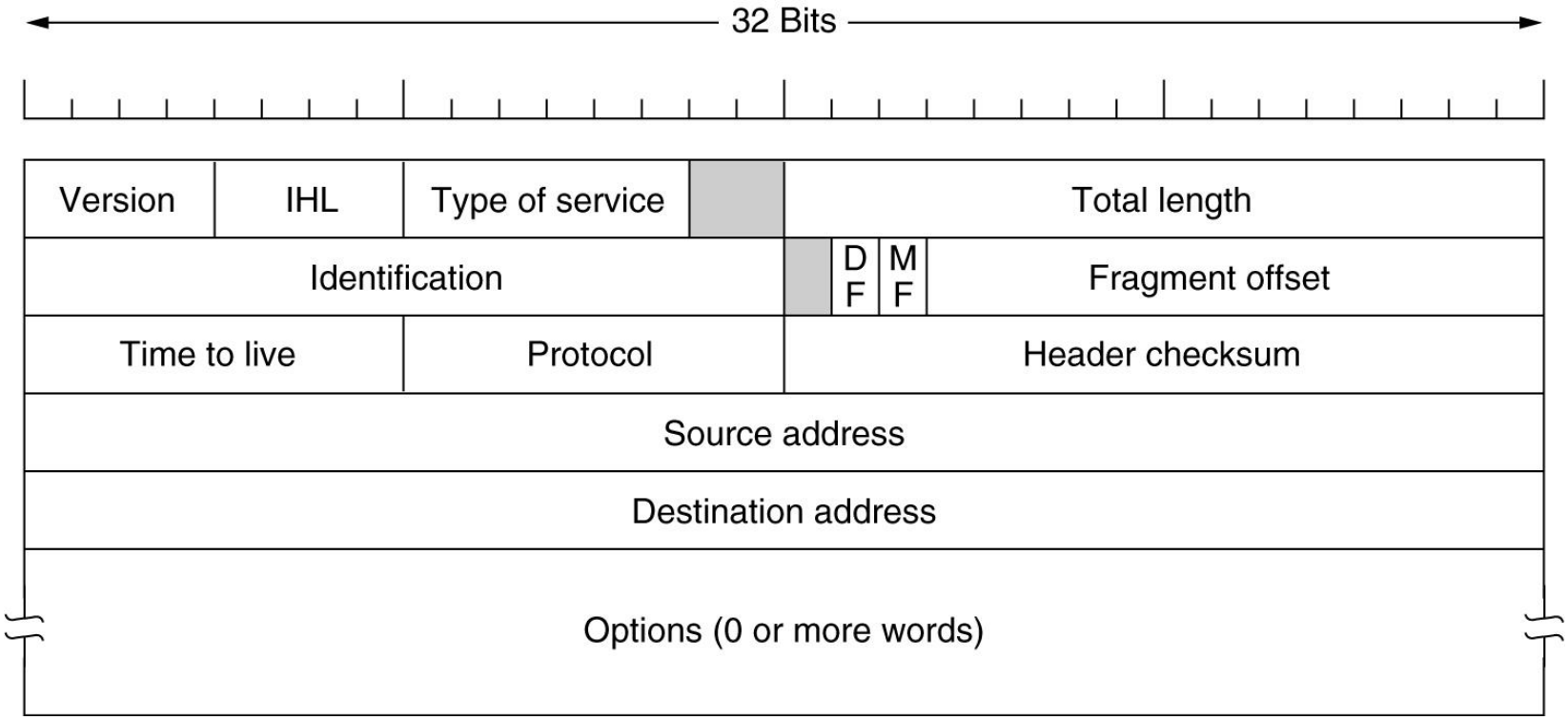
- campo **IHL** (4b):
  - ❑ Se maneja igual que el mismo campo en TCP
  - ❑ longitud del encabezado en palabras de 32b (5 ≤ valor ≤ 15).
  - ❑ 5 cuando no hay opciones.
- Campo **longitud total:** (2B) de encabezado + datos ≤ 65535 B

Datagrama IP



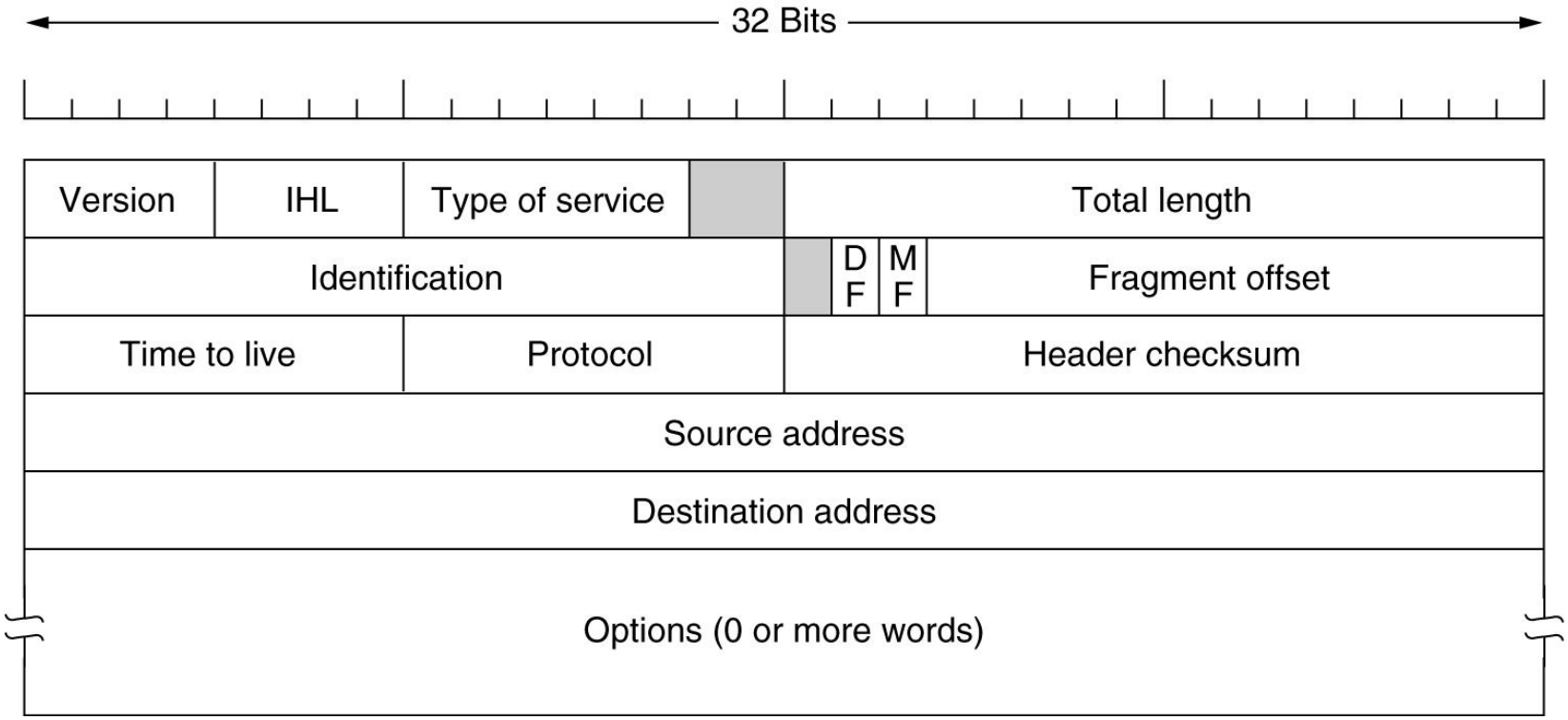
- Campo **tipo de servicio**:
  - los 2 últimos bits se usan para información de notificación de congestión (para ECN – ver filminas de control de congestión).
  - Los 6 primeros bits se usan para indicar clase de servicio (p.ej. entrega rápida, transmisión libre de errores, etc.)

Datagrama IP



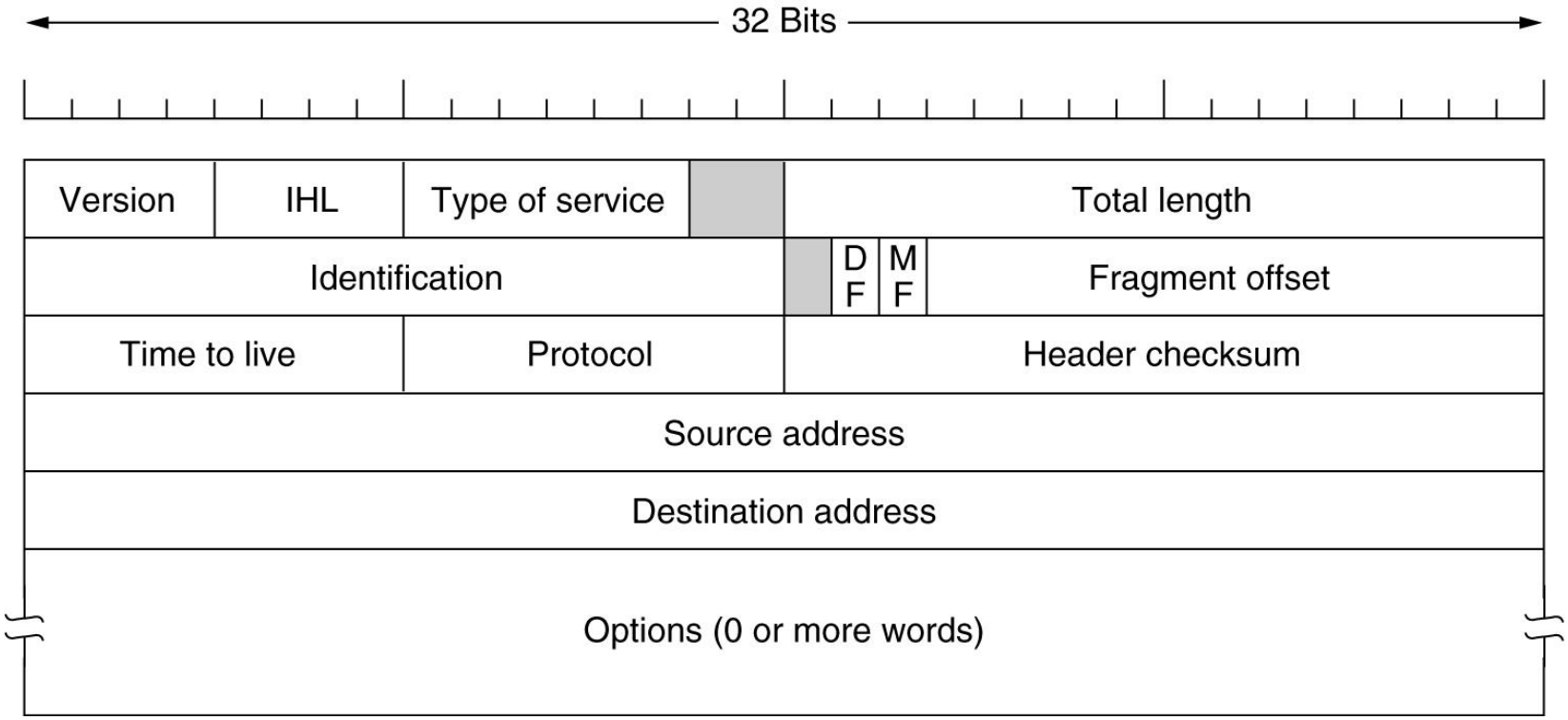
- El campo **protocolo** (8 b) dice a cuál proceso de transporte (p.ej. TCP, UDP, etc.) entregar el paquete.
- El campo **identificación** se usa para que el host de destino determine a qué paquete un fragmento pertenece (un datagrama puede ser un fragmento).

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 en el encabezado cuando el paquete viaja a lo largo de la red.
  - ❑ Debe recalcularse en cada salto, porque el campo tiempo de vida siempre cambia.
  - ❑ Es solo sobre el encabezado porque en capa de transporte se chequea el segmento entero con otro campo checksum.

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

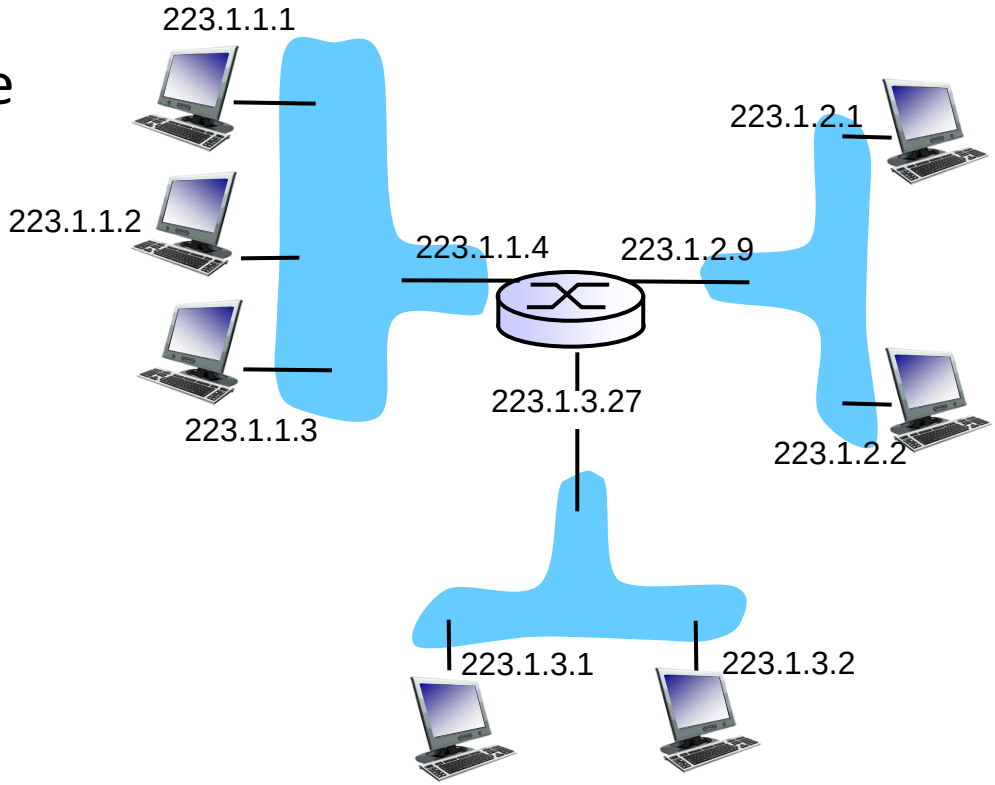
- En un datagrama IP los campos **direcciones de origen y de destino**
  - Cada una tiene 32 b.
  - indican el *número de red* y el *número de máquina*.
  - **Consecuencias**:
    - uso números IP diferentes para distinguir las máquinas de una red.
    - Las direcciones IP son ***jerárquicas***.

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 red inalámbrica 802.11
- *Cada interfaz tiene asociada una dirección IP*



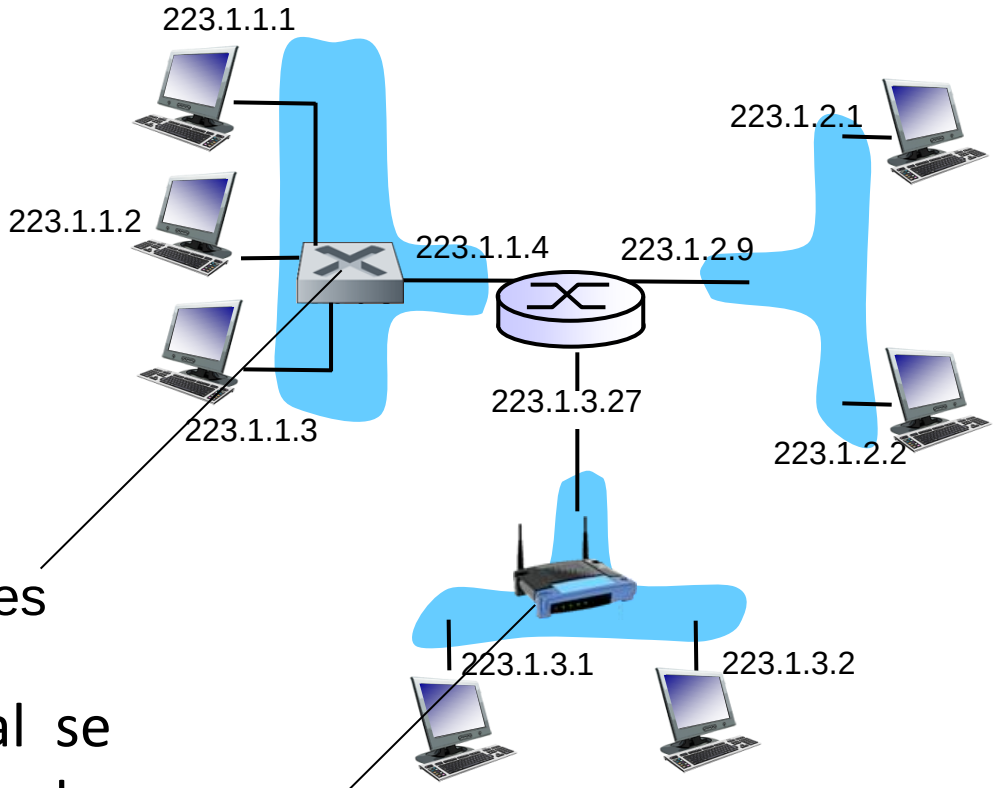
223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Direcciones IP

Las interfaces están conectadas entre sí por medio de:

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

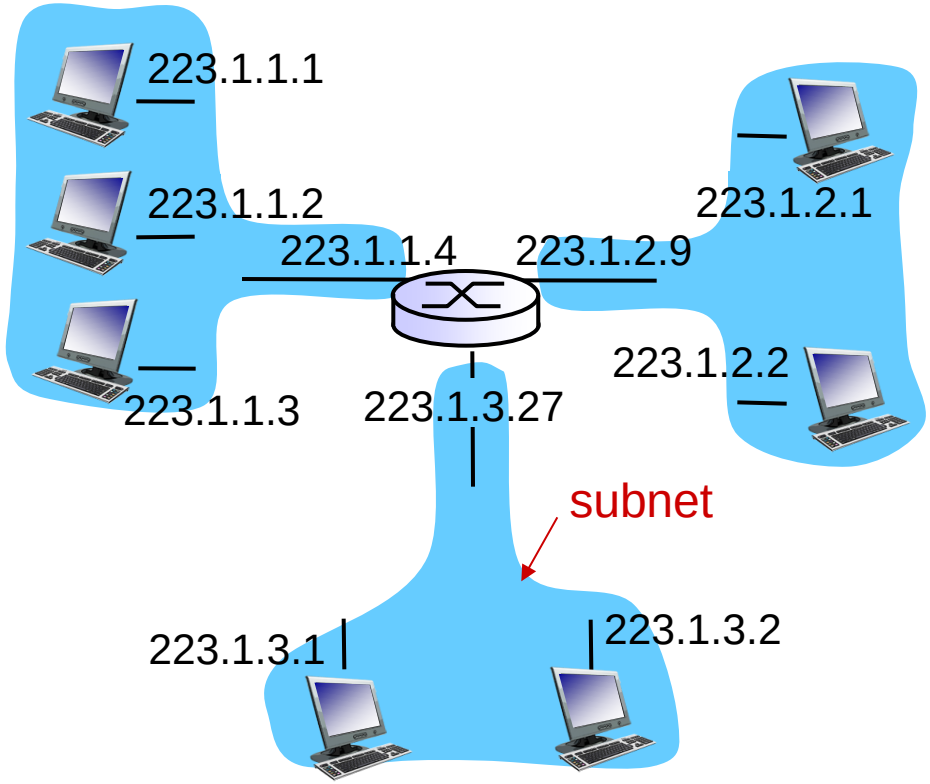
- **La capa de red de internet – Metas:**
  1. Datagramas IPv4
  2. Direcciones IPv4
  3. **Conceptos fundamentales en los que nos basamos**
     - **Para entender cómo asignar nombre a redes y cómo describir ciertos parámetros de las mismas.**
  4. Asignación de redes a organizaciones
  5. Tablas de 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**: **Significado del prefijo128.208.0.0/24:**
    - la dirección IP más baja en el bloque es 128.208.0.0;
    - la porción de la red es de 24 bits.
    - Tengo 2^8 máquinas en la red.

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.

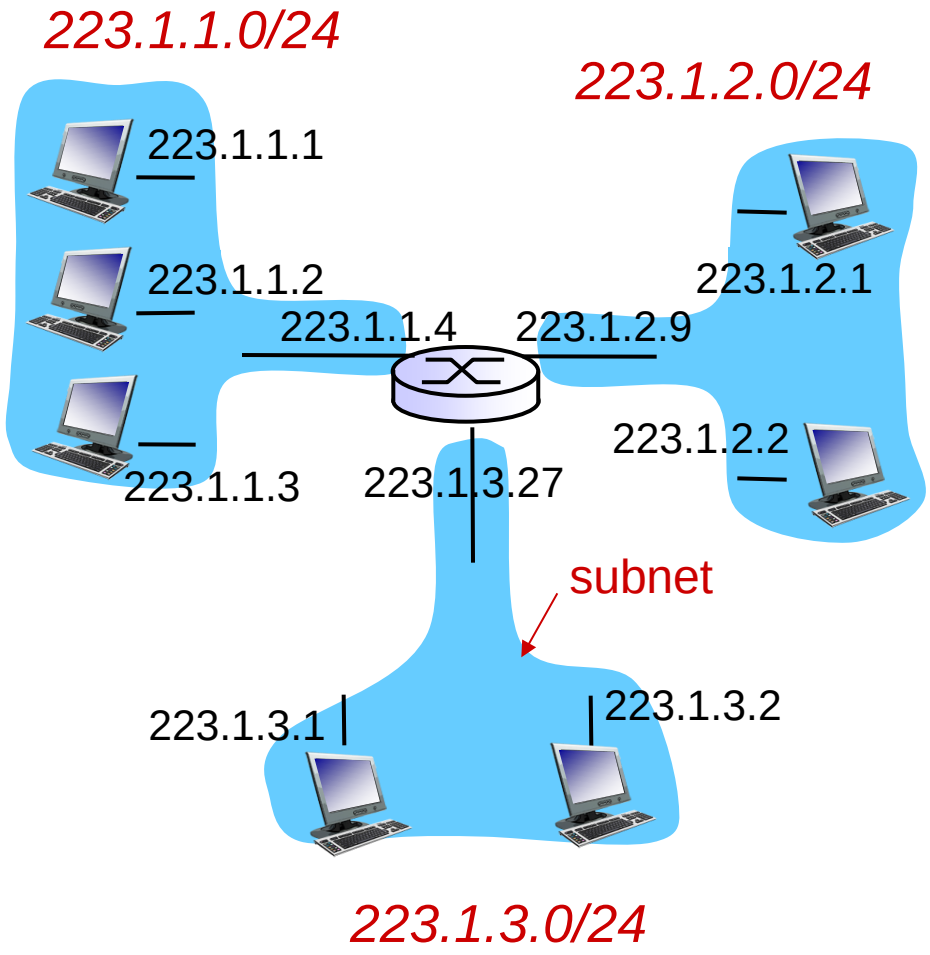


Red consistente de 3 subredes

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



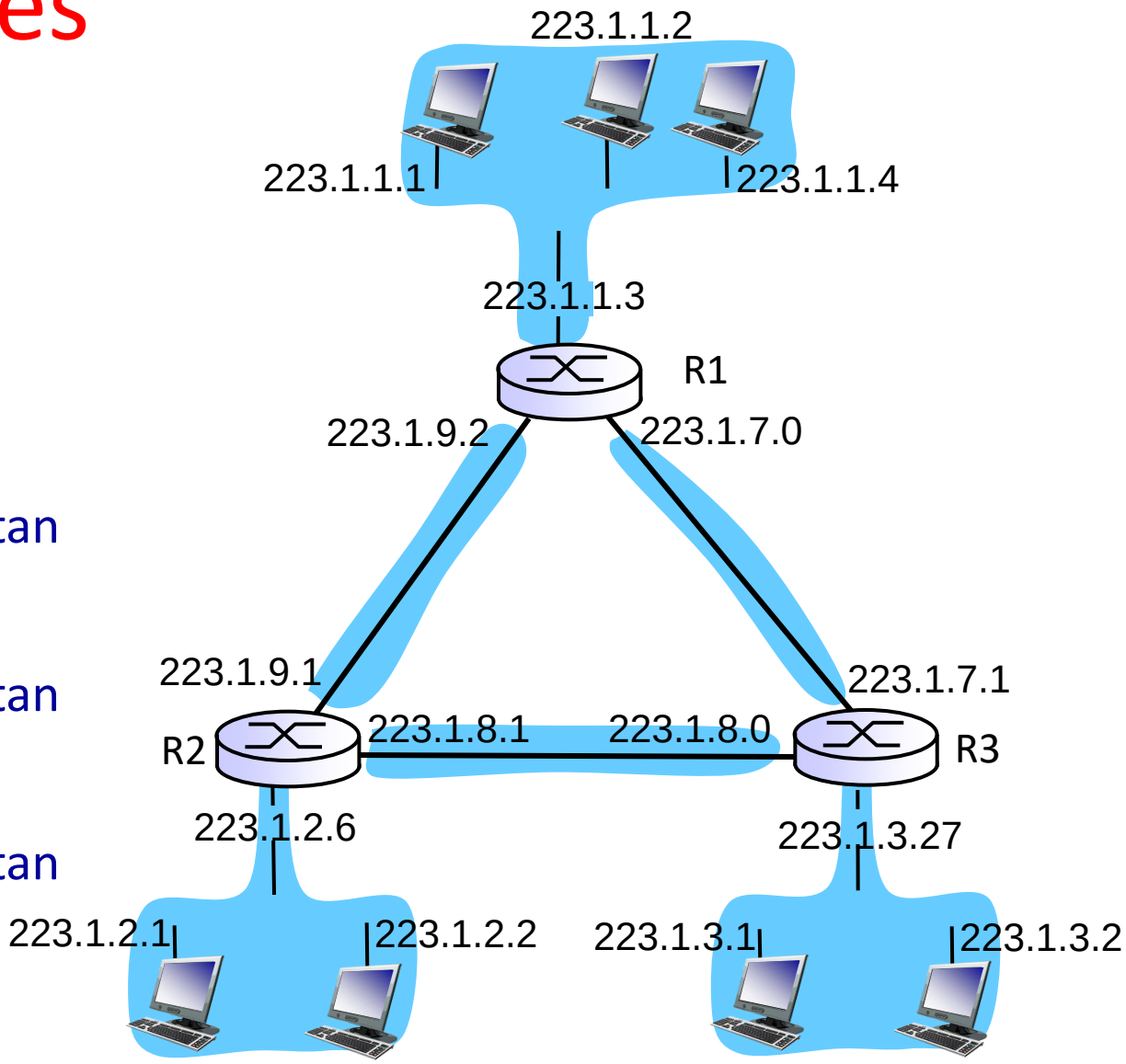
subnet mask: /24

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 de reenvío grande:**
  - Los enrutadores deben buscar en la tabla de reenvío grande para enviar cada paquete; la eficiencia de esta búsqueda es afectada.
  - Los enrutadores en un proveedor de servicios de internet (PSI) grande pueden tener que enviar millones de paquetes por segundo.
    - Este gran volumen de paquetes a enviar empeora aun más las cosas.
    - 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**: hay que evitar tablas de reenvío demasiado grandes.

CIDR

- **Problema**: ¿Cómo asignar una red a una organización 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 aumentará el tamaño de algunas tablas de reenvío.
    - Por lo tanto, cada organización debe tener un solo prefijo de red.
  - 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 las tabla sea demasiado grande.
    - Esto no es necesario, porque veremos que un enrutador en una región no necesita saber de subredes en regiones muy alejadas de ella.

CIDR

- **Subproblema**: ¿Cómo asignar una red a una organización sin que se desperdicien demasiadas direcciones?
- **Idea de solución**: 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

Conceptos Básicos

- Una **máscara de una red** está formada de 1s para identificar la red seguido de 0s para identificar las máquinas.
- **¿Cuál es la máscara de la red de prefijo 128.208.0.0/24?**
- 11111111 11111111 11111111 00000000
- Otra forma de expresarla es: 255.255.255.0

CIDR

- **Problema: ¿Cómo podría definirse la tabla de enrutamiento?**
- **Solución**: el enrutamiento es jerárquico y solo se representan redes de organismos – las llamadas subredes.
  - Cada entrada de tabla de enrutamiento se extiende para darle una **máscara** de 32 bits.
  - **Tabla de enrutamiento** paras 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 com 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

- **Uso de 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.
  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

- **Situación:** Hasta aquí se ponen los prefijos de todas las subredes en tablas de reenvío.
  - Esta situación hace que las tablas de reenvio crezcan demasiado.
- **Problema: ¿Como evitar que las tablas de reenvío crezcan demasiado?**
- **Solución**: forma parte de **CIDR**
  - 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 prefijo con dirección de red de 22 bits puede ser tratada por otro enrutador como parte de un de un prefijo más grande con parte de red de 20 bits.

CIDR

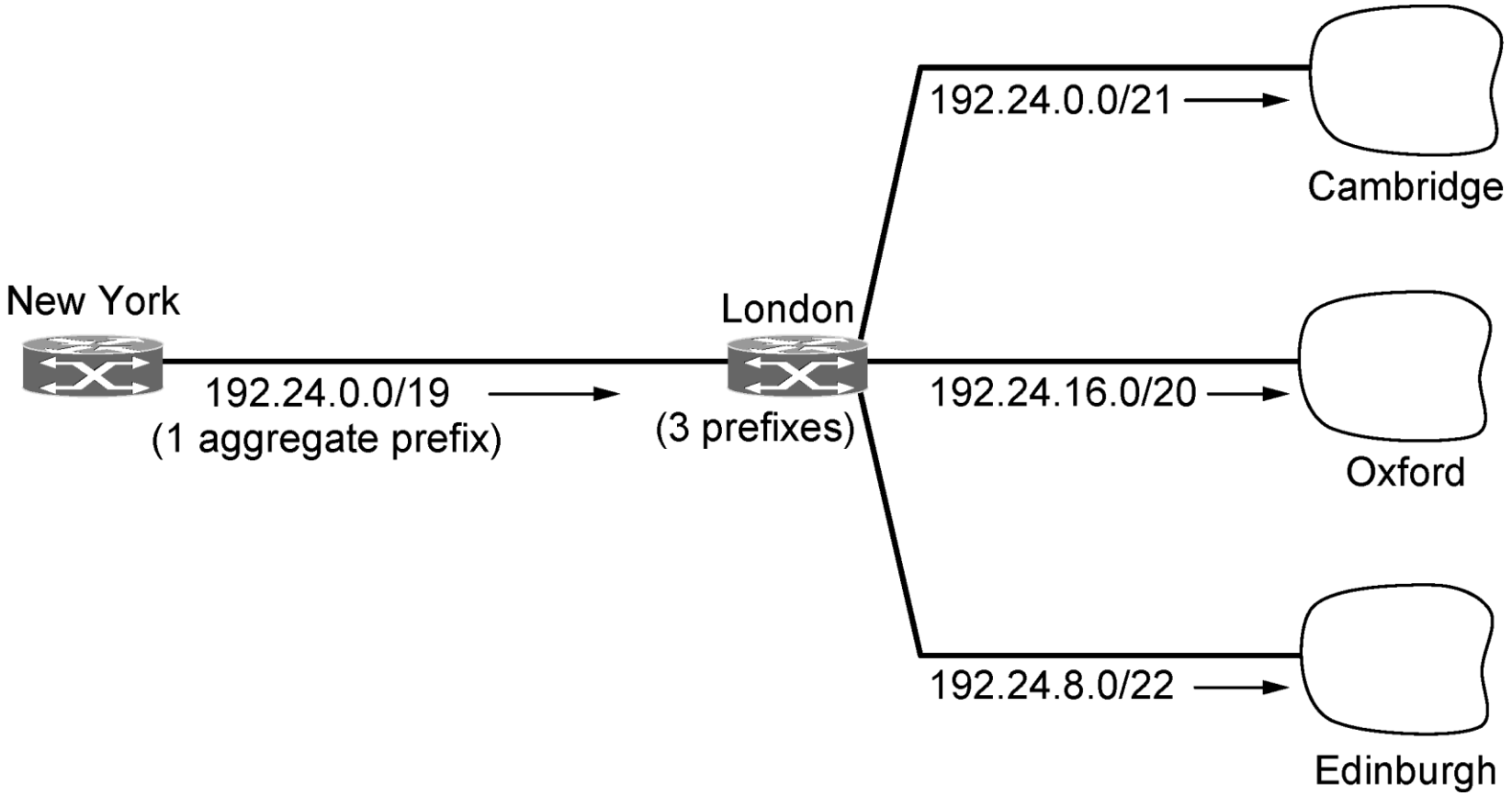
- **A distintas regiones geográficas se asignan distintos espacios de direcciones. Esto se puede aprovechar en la agregación de prefijos:**
- **Idea**: combinar prefijos de varias redes que están ***en una misma región geográfica*** en un prefijo para un enrutador que está en otra ***región alejada.***
- **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 194.24.0.0/19 que es pasado al enrutador de New York. Este prefijo contiene 8K direcciones y cubre las 3 universidades .



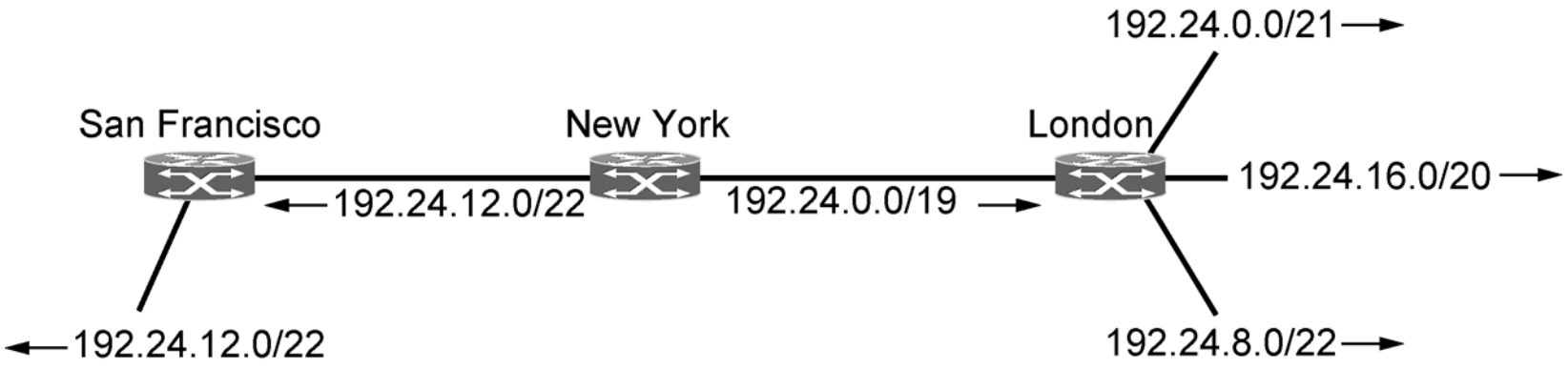
Aggregation of IP prefixes.

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

CIDR con agregación de prefijos

- Cuando se usa agregación de prefijos, éste 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.
- **Esta idea de agregación de prefijos no interfiere con redes más chicas que no fueron agregadas y que caen en bloques agregados.**
  - La razón de ello es que 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



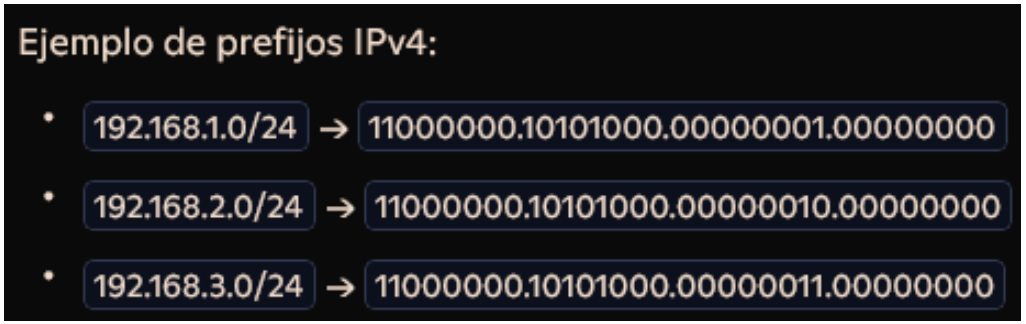
Longest matching prefix routing at the New York router.

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.

Agregación de prefijos

- Ejemplo de agregación de prefijos.



- Buscar la mayor cantidad de bits iguales desde la izquierda. En este caso los primeros 22 bits coinciden.

```
11000000.10101000.000000XX.XXXXXXXX
```

- Representar la nueva agregación: 192.168.0.0/22

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 escacéz de direcciones IPv4.**
     - **Uso del enfoque NAT**

NAT

- **Situación**: Un proveedor de servicios de internet (PSI) tiene una red de c bits (de dirección); 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 PSI en un momento dado.
- **Problema**: **¿Cómo aumentar la cantidad máquinas que usan el servicio del PSI bien por arriba de las 2^(32 - c) a pesar de tener una red de c bits?**
- **Consecuencia:** Resolverlo aumentaría drásticamente la cantidad de máquinas que pueden acceder a internet IPv4.

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 PSI, 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

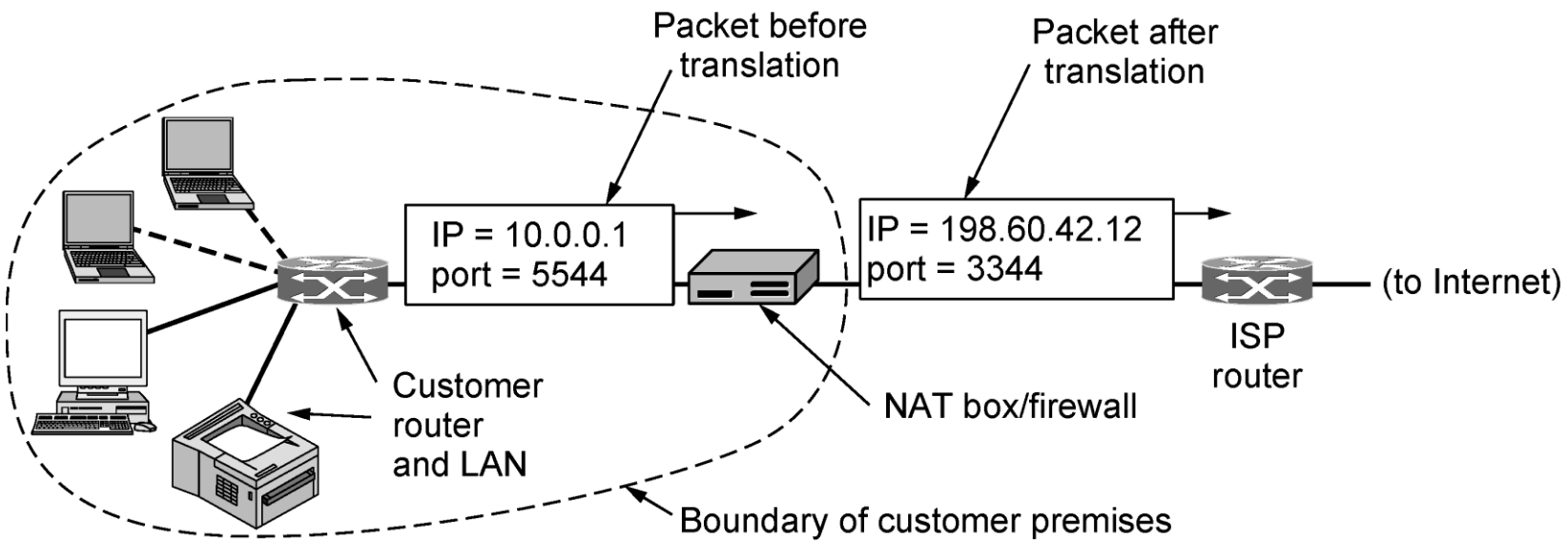


Fig. 60: Colocación y operación de la caja NAT

- 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?**
- **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.
- **Esta idea no siempre funciona.**

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 (la adoptada en la práctica)**: 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

- **Tratamiento de 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

- **Tratamiento de 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.

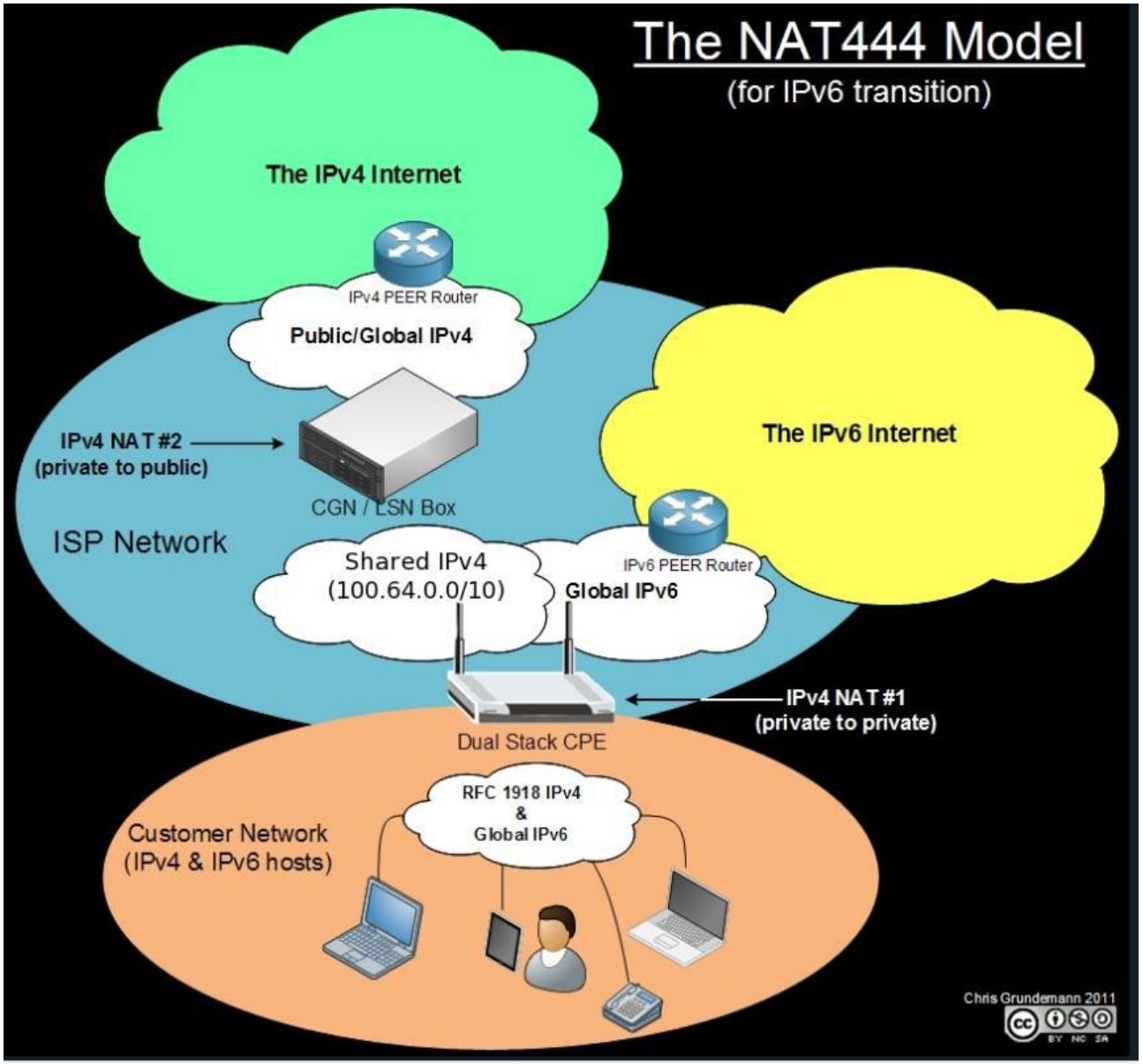
NAT

- **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.

NAT

- **NAT 444**:
  - Los proveedores de servicio de internet (PSI) también pueden tener NAT.
    - Esto hace que las direcciones IPv4 puedan racionarse más aun y durar aun más tiempo.
  - Se llama NAT 444.
  - El espacio de direcciones IP reservado para NAT 444 es 100.64.0.0/10 (o sea alrededor de 4000.000 de IP para ser usadas por la red del PSI)

NAT 444


The NAT444 Model
(for IPv6 transition)
The IPv4 Internet
IPv4 PEER Router
Public/Global IPv4
IPv4 NAT #2
(private to public)
CGN / LSN Box
ISP Network
Shared IPv4
(100.64.0.0/10)
The IPv6 Internet
IPv6 PEER Router
Global IPv6
IPv4 NAT #1
(private to private)
Dual Stack CPE
RFC 1918 IPv4
&
Global IPv6
Customer Network
(IPv4 & IPv6 hosts)
Chris Grundemann 2011

IPv6

- **Problema:** el espacio de direcciones de 32-bit ya ha sido agotado en varias regiones del mundo (incluyendo Latinoamérica, Europa, Norteamérica).
- **Solución**: Considerar un espacio de direcciones mucho más grande.
- **Problema**: con IPv4 algunos campos del encabezado hacen que el procesamiento de datagramas en los enrutadores lleve tiempo:
  - p.ej: campos para fragmentación, procesamiento de suma de verificación, etc.

IPv6

- **Requisitos:**
  - Que el formato de encabezado ayude a aumentar la velocidad de procesamiento y reenvío
  - Cambios en el encabezado para facilitar la calidad de servicio.
- **Hace falta que el procesamiento de encabezados sea más rápido.**
  - Porque las redes cada vez son más rápidas, en cambio la velocidad de los procesadores se está estabilizando.
  - Entonces para compensar hay que agilizar el procesamiento de los datagramas.

IPv6

- **Formato de datagrama IPv6:**
  - **Encabezado de longitud fija** de 40 bytes para procesamiento más rápido de datagramas
  - **Capacidad de direccionamiento expandida**: direcciones de 128 bits.
  - **Etiquetado de flujos**: se etiquetan paquetes que pertenecen a un mismo flujo para los cuales el emisor requiere manejo especial.

IPv6

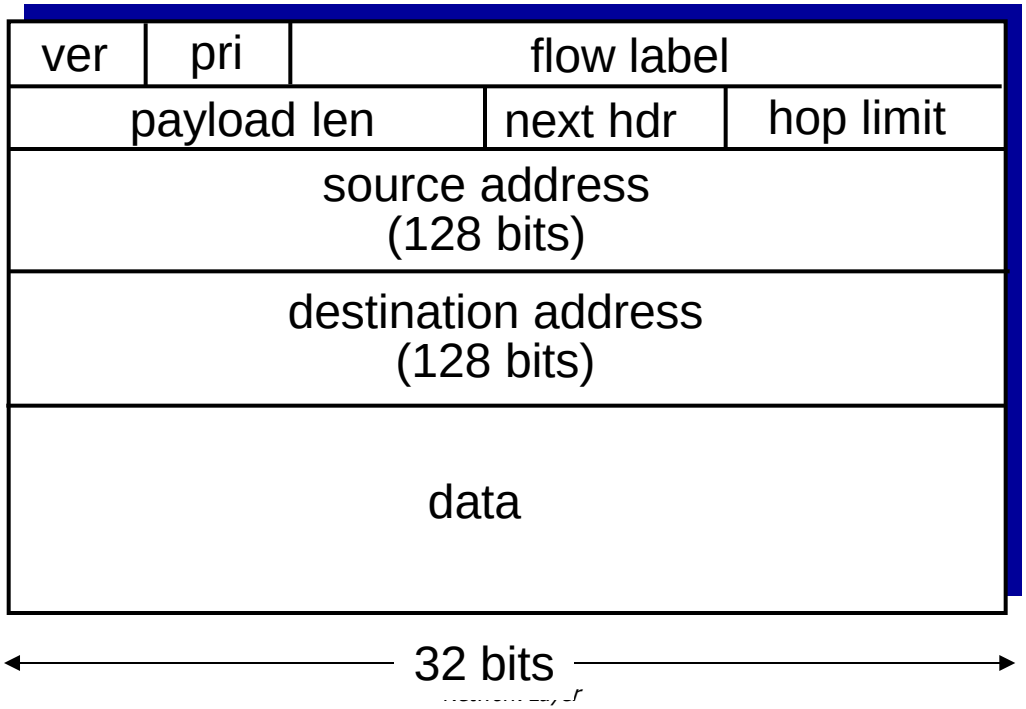
- Ejemplos de flujo o no flujo:
  - P.ej. Transmisión de audio y video pueden ser tratados como un flujo.
  - P.ej. Transferencia de archivos y e-mail pueden no ser tratados como flujos.
  - P.ej. El tráfico de un usuario de alta prioridad puede ser tratado como un flujo.
- **Consecuencia del etiquetado de flujos:**
  - Cuando un paquete con una etiqueta de flujo distinta de cero aparece, los enrutadores pueden ver en tablas internas para ver qué tipo de tratamiento especial requiere.

IPv6

Etiqueta de flujo: (20 b) para identificar datagramas en el mismo "flujo".

Prioridad tiene dos usos:

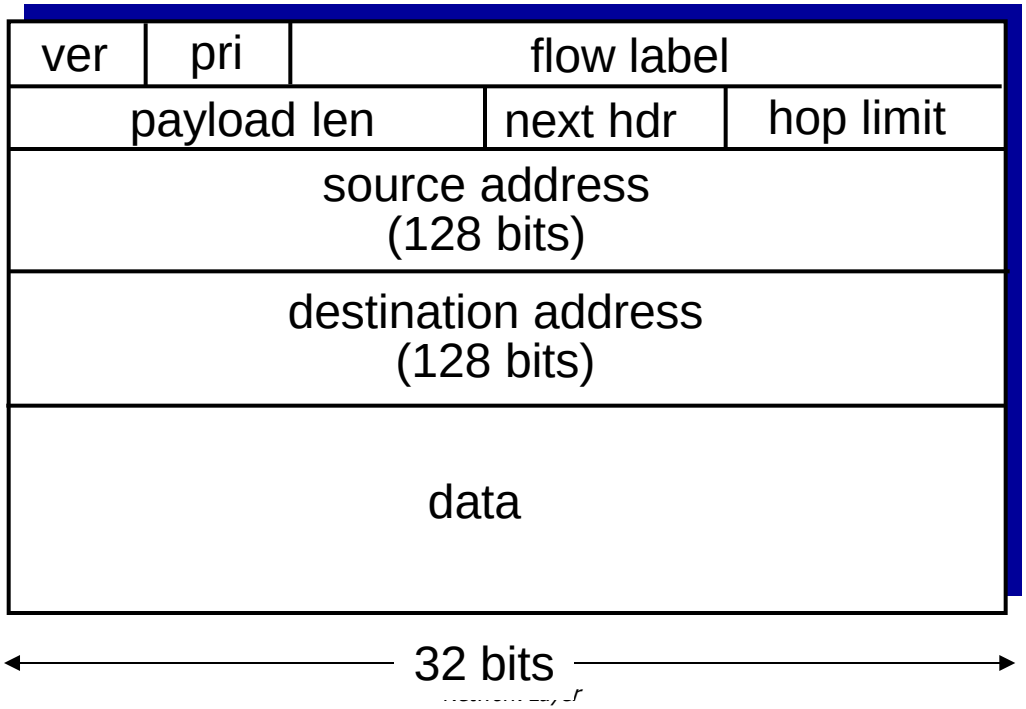
- para dar prioridad a ciertos datagramas dentro de un flujo.
- para dar prioridad a datagramas de ciertas aplicaciones sobre datagramas de otras aplicaciones.



IPv6

Longitud de carga útil: (16 b) número de bytes en el datagrama IPv6 luego del encabezado (de 40 B).

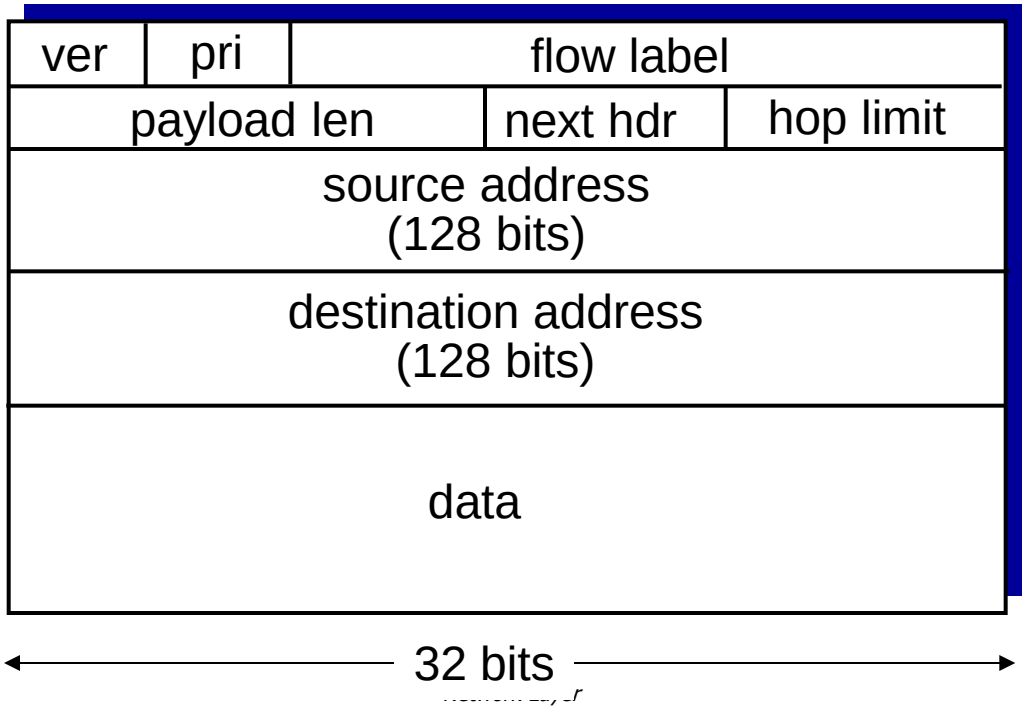
Límite de saltos: (8 bits) el contenido de este campo se decrementa en 1 por cada enrutador que entrega el datagrama. Si el contador alcanza 0, el datagrama se descarta.



IPv6

Próximo encabezado: (8 bits) significa:

- Cuál de los 6 encabezados extensión de opciones actuales le sigue al encabezado.
- Si este encabezado es el último encabezado IP, el campo dice a cuál protocolo de transporte entregar el datagrama.
- Los encabezados de opciones también tienen este campo.



IPv6

- **Direcciones IPv6:**
  - Son escritas como 8 grupos de 4 dígitos hexadecimales.
  - Para separar los grupos se usa “:”.
  - P.ej: 8000:0000:0000:0000:0123:4567:89AB:CDEF
  - **Optimización**:
    - Ceros a la izquierda de grupos pueden ser omitidos
    - Grupos con 16 bits iguales a 0 pueden reemplazarse con dos “:”.
  - P.ej. la dirección anterior: 8000::123:4567:89AB:CDEF

IPv6

- ***Otros cambios en relación a IPv4***
  - No se permite fragmentación ni re-ensamblado en enrutadores intermedios.
    - Esto solo puede hacerse por el origen y el destino.
  - ***Suma de verificación***: removido para reducir el tiempo de procesamiento en cada salto (ya la capa de transporte y de enlace de datos usan suma de verificación).
    - Trabajar con este campo era costoso en IPv4.
  - ***Opciones:*** están permitidas, pero fuera del encabezado, indicado por el campo de próximo encabezado.

IPv6

- **Problema: ¿Qué se puede hacer si un datagrama es demasiado grande para pasar por una línea de salida de un enrutador?**
  - Un enrutador descarta paquetes que son demasiado grandes para la línea de salida;
  - y manda al emisor un ***mensaje de paquete demasiado grande***.
  - Luego el emisor puede reenviar los datos usando datagramas IP más chicos.

IPv6

- Una dirección IPv6 la podemos dividir en:
  - **Identificador de red**: identifica la red principal en la que se encuentra el dispositivo.
  - **Identificador de subred**: ayuda a dividir la red principal en subredes mas pequeñas.
  - **Identificador de interfaz**: identifica de manera única al dispositivo dentro de la subred.
  - **Ejemplo**: dada la dirección: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
    - identificador de red: 2001:0db8:85a3
    - Identificador de subred: 0000:0000
    - Identificador de interfaz: 8a2e:0370:7334

IPv6

- **Esquema lógico de una red IPv6**:
  - **Nivel de red global**:
    - El ISP asigna un prefijo global a una organización.
    - Por ejemplo: 2001:db8::/32
  - **Nivel de red interna**:
    - La organización asigna subredes dentro de ese espacio.
    - Por ejemplo: 2001:db8:1::/48
  - **Nivel de subred**:
    - Son subredes divididas a partir del prefijo interno.
    - Pueden usarse para departamentos.
    - Por ejemplo: para el departamento A usa 2001:db8:1:1::/64. Un dispositivo final del departamento A tiene una dirección 2001:db8:1:1::100.
- Una organización recibe un **prefijo global**. El mismo también puede ser de /48.
  - Un prefijo global de /48 puede ser dividido en subredes más pequeñas de /64 para uso interno.

IPv6

- En IPv6 no se usan prefijos para enlaces entre enrutadores.
- En lugar de eso se usan **direcciones link-local**.
  - Todas ellas comienzan con el prefijo fe80::/10.
  - Los primeros 10 bits son: 1111111010.
  - El resto puede completarse para crear una dirección única dentro del enlace.
  - **Ejemplo de dirección link-local**: fe80::1a2b:3c4de:5e6f:7g8h%eth0. Aquí %eth0 indica la interfaz específica en la que se está usando la dirección.
- Además, si dos dispositivos están conectados al mismo enrutador, pueden comunicarse entre sí usando direcciones link local.
- Las direcciones link local se configuran automáticamente.
- Los 64 bits menos significativos suelen derivarse de la dirección MAC de la interfaz de red usando el método EUI-64.

IPv6

- Los **enrutadores de un ISP** manejan prefijos globales asignados a sus clientes u otras redes conectadas.
- Los **enrutadores de una organización** (nivel interno y subred) manejan prefijo global asignado por el ISP (p.ej. 2001:db8:1::/48) y lo dividen en subprefijos mas pequeños (p.ej. 2001:db8:1:1::/64) .
  - Sus tablas incluyen rutas para estos subprefijos.
  - Los enrutadores distribuyen el trafico entre sus subredes internas (de /64).
  - Estos enrutadores tienen rutas hacia el Gateway del ISP representadas por el prefijo global (p.ej: 2001:db8::/32)

IPv6

- Las **direcciones ULA** están diseñadas para proporcionar conectividad privada dentro de una organización.
- Una dirección ULA siempre comienza con FC o FD en los bits mas significativos.
- Estas direcciones no pueden salir hacia la internet ni ser vistas fuera de la red interna.
- Estas direcciones son unicas dentro de la red local.
- Las direcciones ULA se usan para redes locales o aisladas que no necesitan conectar la internet.
- También se pueden usar como respaldo de las direcciones globales. Si la conexión a internet falla, ULA permite que la conexión interna siga funcionando.

IPv6

- **Ejemplo**: supongamos que tienes un prefijo ULA generado automáticamente como FD00:1234:5678::/48.Puedes dividirlo en redes internas:
  - subred A: FD00:1234:5678:1::/64
  - Subred B: FD00:1234:5678:2::/64
- Un mismo dispositivo puede tener una dirección ULA para comunicación interna y una dirección global unicast para acceso externo.
- Los dispositivos usan automáticamente la dirección adecuada según el tipo de comunicación (para recursos internos la dirección ULA y para acceso externo la dirección global)
- Los recursos internos pueden estar protegidos y aislados mediante direcciones ULA.

IPv6

- **Asignación de redes globales en IPv6:**
  - **IANA** (Internet Assigned Numbers Authority): asigna bloques enormes de direcciones IPv6 a los registros regionales.
  - **RIR** (Registros Regionales de Internet): distribuyen bloques mas pequeños a los ISP, típicamente de /32.
  - **ISPs**: dividen estos bloques y asignan prefijos más pequeños a sus clientes (por ejemplo: /48)
  - **Organizaciones**: divide el prefijo recibido en subredes (por ejemplo, de /64)

IPv6

- En IPv6 las tablas de reenvío son diferentes que en IPv4.
- En IPv6 se usan los siguientes valores en una fila de la tabla de reenvío:
  - **El prefijo de destino** (por ejemplo: 2001:db8:1::/64),
  - **la interfaz de salida** (por ejemplo, eth0),
  - La **dirección del siguiente salto hacia el destino** que puede ser un enrutador adyacente,
  - **Métrica**: medida del costo asociado con la ruta usada para elegir la mejor ruta disponible si hay mas de una.
- Se pueden usar prefijos global, link-local, ULA, etc. en una misma interfaz.

IPv6

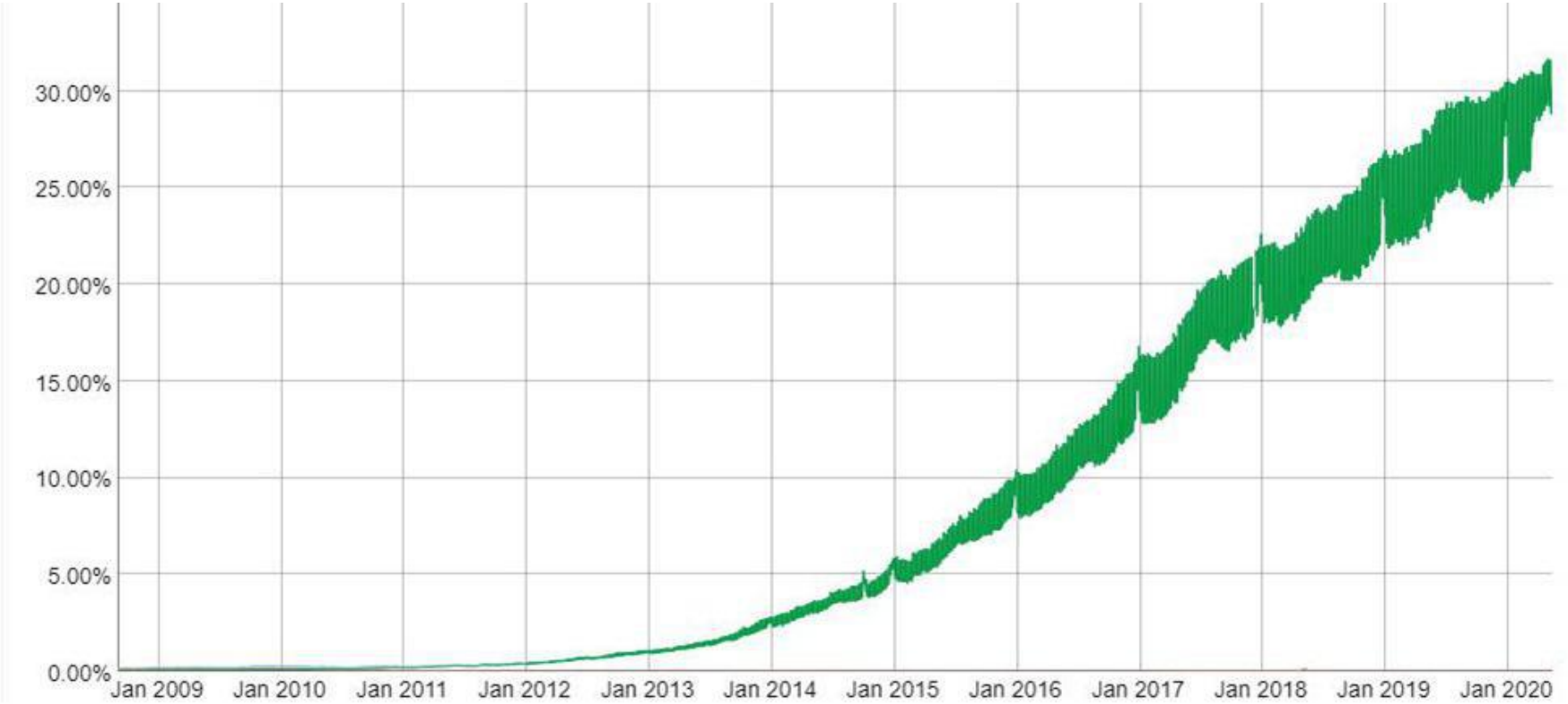
- En IPv6 las subredes suelen usar prefijos estándar de /64 lo que simplifica las búsquedas en las tablas de enrutamiento.
- En IPv6, los prefijos globales, regionales, y locales están organizados jerárquicamente. Esto permite una mayor agregación de rutas, reduciendo la cantidad total de entradas en las tablas.
- En IPv6, las búsquedas en las tablas de reenvío suelen ser bastante eficientes y pueden lograrse en **orden logarítmico** del tamaño de la tabla en muchas implementaciones modernas.
- Los routers de alto rendimiento usan memoria **TCAM (Ternary Content Addressable Memory)** que permite realizar búsquedas en paralelo en múltiples entradas de la tabla, alcanzando velocidades aún mayores.

IPv6

- **Adopción de IPv6:**
  - En enero del 2020 el 30 % de los usuarios acceden a Google usando IPv6.
  - En esa época en Argentina la adopción de IPv6 es del 11%, en Brasil del 34%, en USA es del 43%.

IPv6

- Según la figura de abajo se está acelerando la adopción de IPv6.



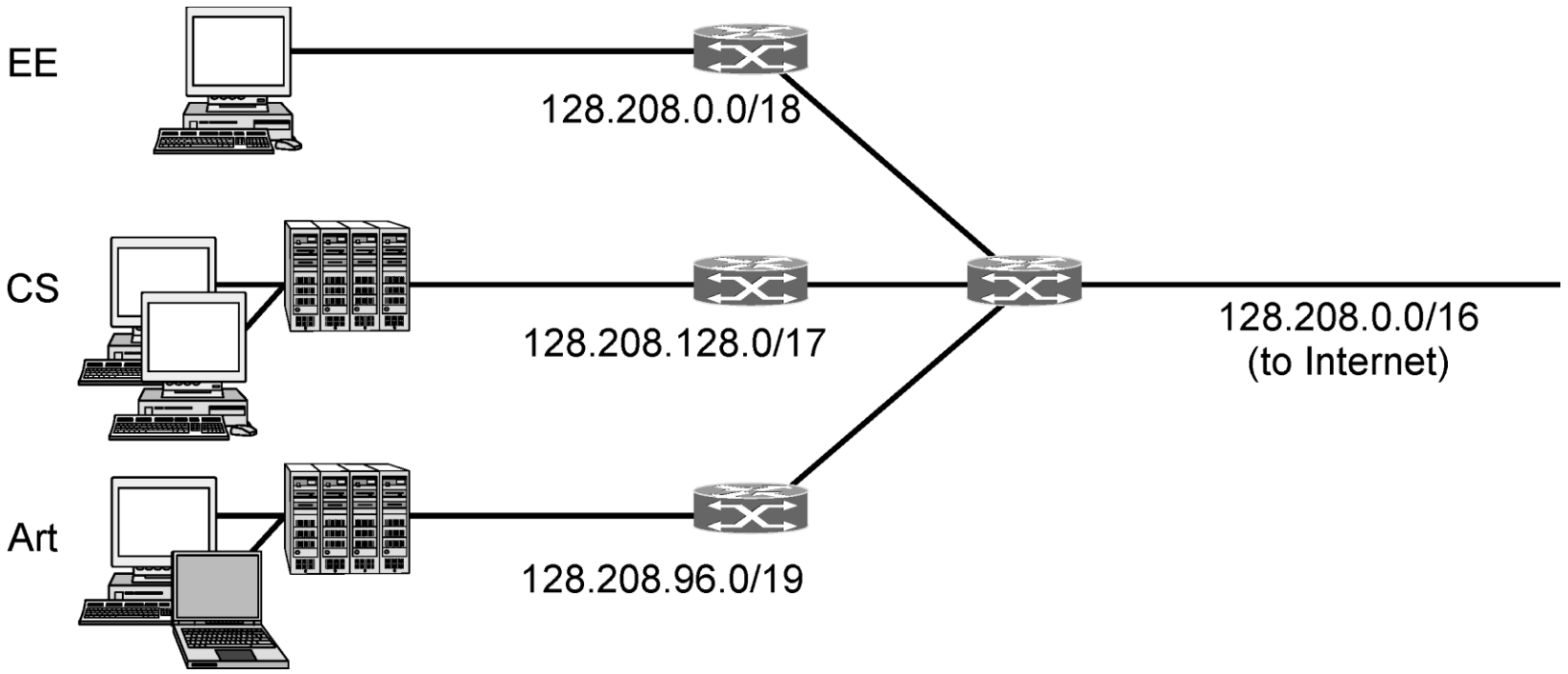
Subredes (Tanenbaum)

- **Uso de subredes**: permitir una red que sea dividida en varias partes para uso interno pero que todavía actúe como una red simple para el mundo externo.
  - Cada subred puede ser una LAN que tiene un **enrutador**.
  - Los enrutadores de una subred conectados a un **enrutador principal**.
  - Fuera de la red, una subred no es visible.

Subredes

- Una subred típica de un campus universitario podría lucir como en la Fig. 57 con un enrutador principal conectado a un ISP o a una red regional, y numerosas Ethernet dispersas en diferentes departamentos.
  - Cada una de las Ethernet tiene su propio enrutador conectado al enrutador principal, posiblemente mediante una LAN de red dorsal.
- En la literatura sobre internet a estas partes de la red (en el ejemplo Ethernets) se les llama **subredes**.

Subredes



Splitting an IP prefix into separate networks with subnetting.

Subredes

- **Problema**: Cuando un paquete entra en el enrutador principal, ¿cómo sabe a cuál subred pasarlo?
- **Solución 1**: tener una tabla en el enrutador principal (con tantas entradas como el tamaño de su red) que indique cuál enrutador usar para cada host.
  - **Evaluación**: se requeriría una tabla muy grande en el enrutador principal y mucho mantenimiento manual conforme se agregan, movieran o eliminaran hosts.
- **Solución 2**: algunos bits se eliminan del N° de host para crear un número de subred
  - P.ej. si la universidad tiene 35 departamentos, se usa 6 bits para el número de subred y 10 bits para el número de host; lo que permite hasta 64 Ethernets, cada una con a lo más 1022 hosts.

Subredes

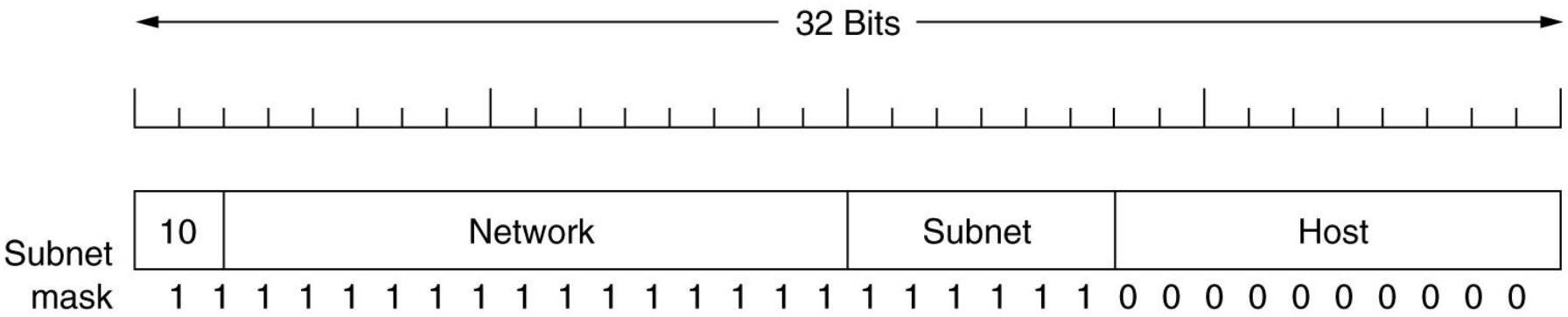


Fig. 58: Una red sub-dividida en 64 subredes.

Subredes

- **Problema**: ¿Cómo expresar subredes?
- **Solución**: el enrutador principal usa una **máscara de subred** que indique la división entre el número de red + número de subred y el host, como se ve en la Fig. 58.
  - Las máscaras de subred también se pueden escribir en notación decimal con puntos, o agregando a la dirección IP una diagonal seguida del número de bits usado para los números de red y subred.
- Para el ejemplo de la Fig. 58 la máscara de subred puede escribirse como:

  1111 1111. 1111 1111. 1111 1100. 0000 0000

  255. 255 . 252 . 0.
  - Esta máscara permite 1024 hosts
  - Una notación alternativa es /22 para indicar que la máscara de subred tiene una longitud de 22 bits.

Subredes

- Fuera de la red, la subred no es visible, por lo que la asignación de una subred nueva no requiere comunicación con el ICANN (Corporación de Internet para la Asignación de Nombres y Números) ni la modificación de bases de datos externas.

Subredes

- **Ejemplo**: Red de universidad
  - Computer Science: 10000000 11010000 1|xxxxxxx xxxxxxxx
  - Electrical Eng.: 10000000 11010000 00|xxxxxx xxxxxxxx
  - Art: 10000000 11010000 011|xxxxx xxxxxxxx
- La barra vertical (|) muestra el límite entre el N° de subred y el N° de host. A su izquierda se encuentra el número de subred, a su derecha el número de host.
  - Computer Science: Comenzando en 128.208.128.0
  - Electrical Eng. : Comenzando en 128.208.0.0
  - Art: Comenzando en 128.208.96.0

Subredes

- **¿Cómo serían las tablas de enrutamiento para el enrutador principal (i. e. cuando hay subredes)?**
- Se tienen entradas con forma de
  - (dirección IP inicio subred, máscara).
  - Cuando un paquete llega al enrutador principal, el enrutador hace un AND booleano de la dirección de destino con la máscara de subred para deshacerse del número de host y buscar la dirección resultante en sus tablas (hay que ver si coincide con la dirección de inicio de subred o prefijo).

Subredes

- **Ejemplo**: un paquete dirigido a 128.208.2.151 que llega al enrutador principal.
  - Para ver si es para el departamento de Computer Science se hace AND de 128.208.2.151 con la máscara de subred 255.255.128.0, para dar la dirección 128.208.0.0.
  - Hay que ver si esto concuerda con la dirección de inicio de subred (prefijo) que es 128.208.128.0. No concuerdan.
  - Para ver si es para el departamento de Electrical Engineering se hace AND de 128.208.2.151 con la máscara de subred 255.255.192.0, para dar la dirección 128.208.0.0.
  - Esto concuerda con el prefijo. Así que el paquete se envía a la línea que va a la red de Electrical Engineering.

Subredes

- **Observación**: El origen de una subred denota el tamaño máximo de hosts que puede albergar.
- Por ejemplo, supongamos que inicia en 130.50.8.0:

  1000 0010 . 0011 0010 . 0000 1000 . 0000 0000

  - Esta red puede crecer hasta 2^11 hosts = 2048. Dicha mascara es:
  - 255 . 255 . 248 . 0

Subredes

- Tenemos la subred que inicia en 130.50.8.0:

  1000 0010 . 0011 0010 . 0000 1000 . 0000 0000
- **Problema**: queremos hacer la red mas grande,
- **Idea**: deberíamos elegir otra máscara,
  - por ejemplo: 255. 255. 128. 0 que albergaría 2^15= 32 K hosts.
  - Esto haría que la red llegue hasta la 130.50.135.255.
  - Pero escribamos la mascara en binario:

    1111 1111. 1111 1111. 1000 0000 . 0000 0000
  - ¡Ningún paquete que se haga AND con esta máscara me da la IP de origen de la subred! (130.50.8.0)
  - **Moraleja**: la cantidad máxima de hosts se da por la cantidad de 0 a la derecha del ultimo 1 en la dirección de origen:

    1000 0010 . 0011 0010 . 0000 1000 . 0000 0000