Redes de computadoras

Capa de Red - IP

Las diapositivas están basadas en en libro:
“Redes de Computadoras – Un enfoque descendente”
de James F. Kurose & Keith W. Ross

Capa de red

La tarea de la capa de red es:

- Descubrír la topología de la red
- Manejar el enrutamiento
- preparar los datos para la transmisión
- Se debe comunicar con la capa de transporte
- Encapsular los datos de la capa de transporte dentro de unidades de datos de la capa de red (datagramas)
- Manejar la conectividad y el ruteo entre hosts y redes
- Se debe comunicar con la capa de enlace

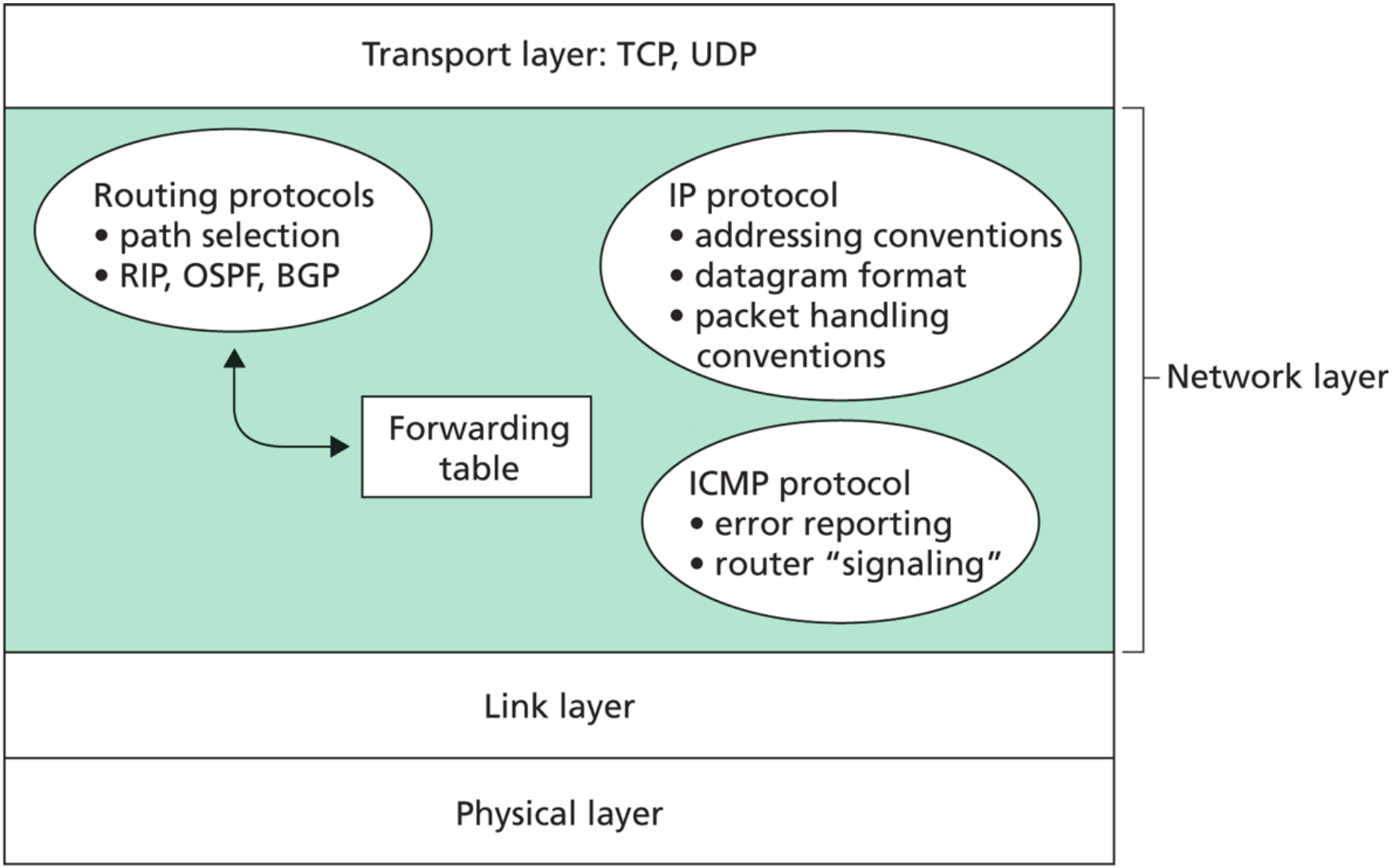
Capa de red

- Los routers deben poder realizar un reenvío de los datos que reciben, basándose en lo definido por el algoritmo de enrutamiento.

- Para cumplir con esta tarea los routers cuentan con tablas de reenvío que les permiten procesar los datos que ingresan por un enlace de entrada hacia uno de salida.

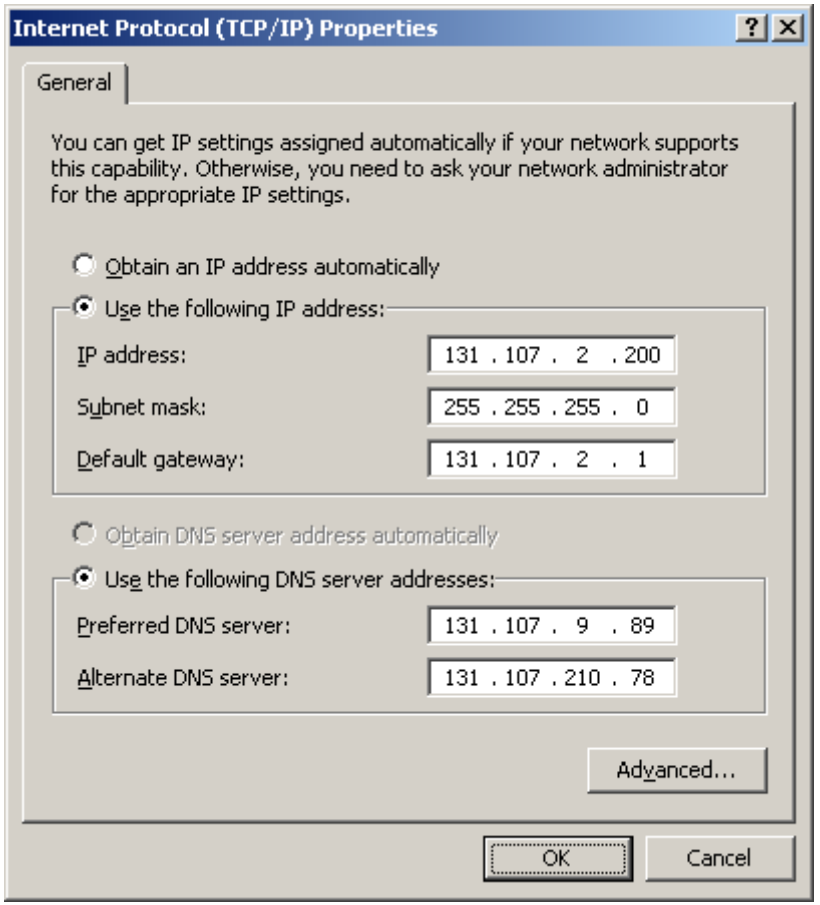
- Dos grandes arquitecturas de la capa de red son los circuitos virtuales, que brindan un servicio de conexión, y por otro lado las redes de datagramas.

Capa de red


Transport layer: TCP, UDP
Routing protocols
• path selection
• RIP, OSPF, BGP
IP protocol
• addressing conventions
• datagram format
• packet handling conventions
Forwarding table
ICMP protocol
• error reporting
• router "signaling"
Network layer
Link layer
Physical layer

Internet Protocol

IP es parte de un conjunto de protocolos de comunicación que proveen identificación global única.



IPv4

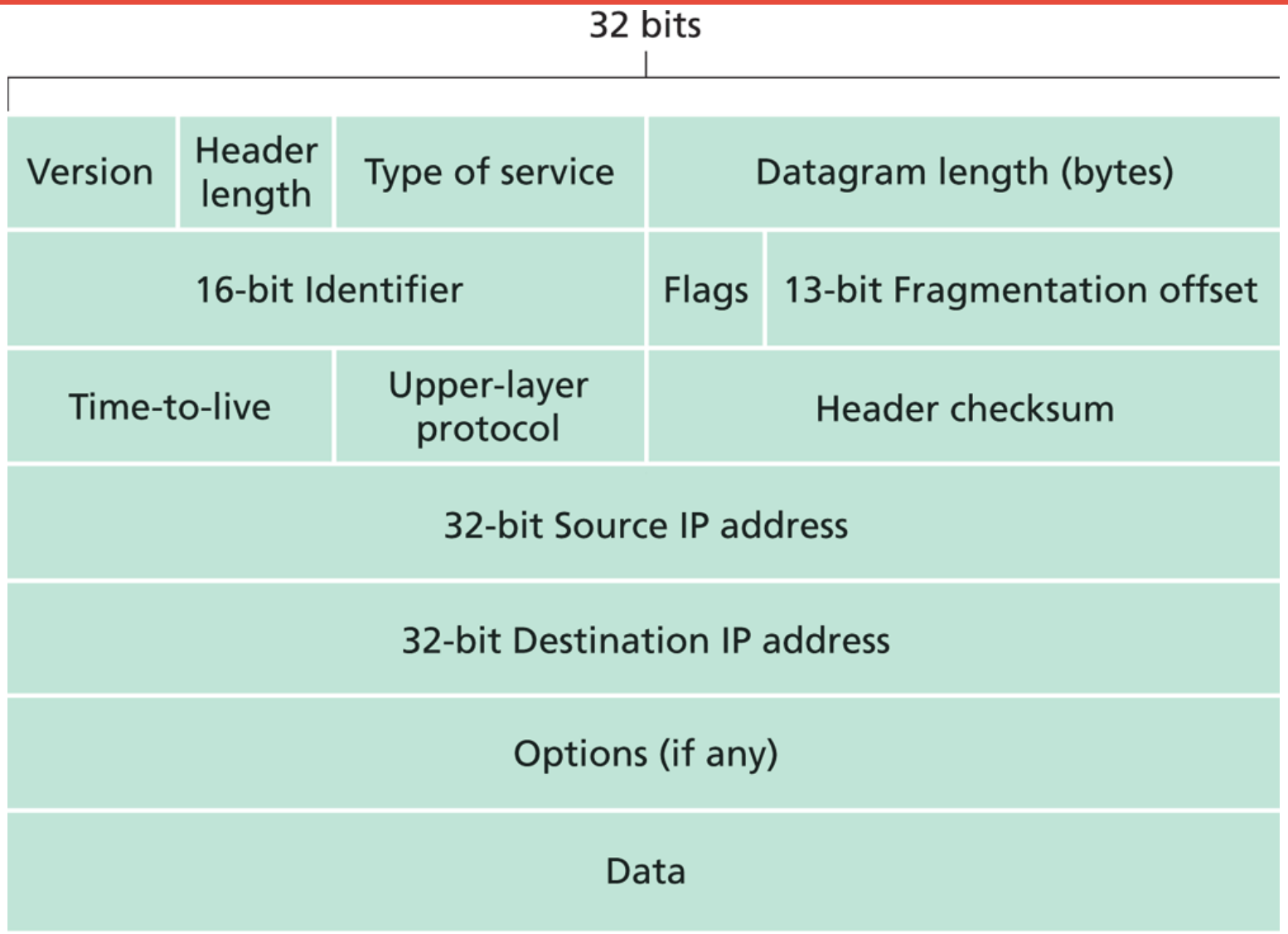
IP v4 es la primer versión implementada en producción en ARPANET y es la que funciona en la mayor parte de los sistemas al día de hoy.

Utiliza direcciones de 32 bits (2^{32} = 4.294.967.296) de las cuales muchas son reservadas a propósitos específicos.

- redes LAN
- broadcast
- autoreferencia

La gran cantidad de dispositivos conectados a Internet han agotado las reservas de direcciones provistas
por la IANA (Internet Assigned Numbers Authority) por lo que se ha impulsado la implementación de su remplazo IP v6

Datagramas IP v4

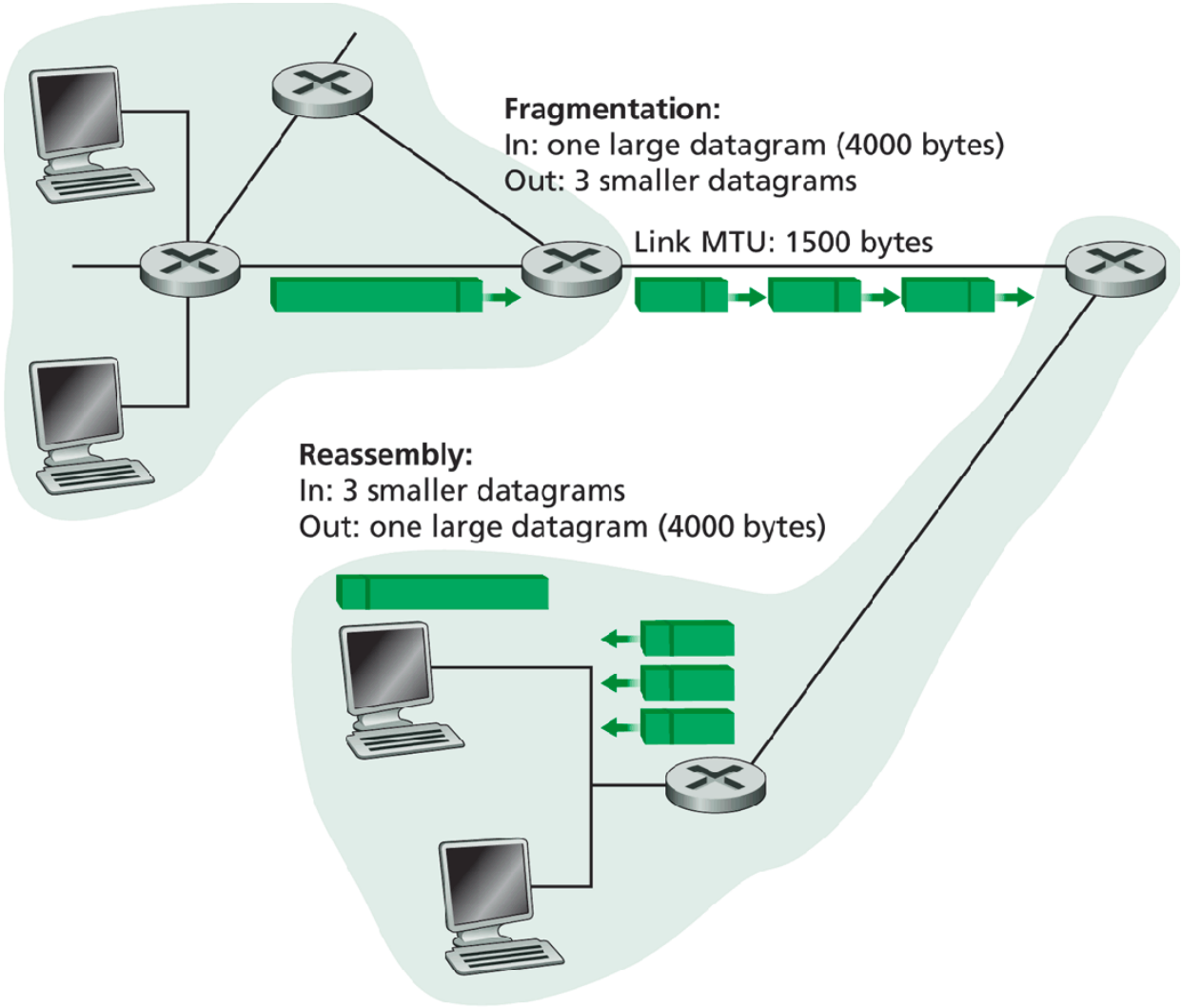


Fragmentación y rearmado IP

Los enlaces de la red pueden tener diferente MTU

En caso de que al llegar a un enlace un datagrama sea más largo que el MTU deberá ser fraccionado.

Al llegar al destino se re-ensamblará



Fragmentación y rearmado IP

Ejemplo:

Datagrama de 4000 bytes

MTU de 1500 bytes

El datagrama original de 4000Kb se fragmentará en 3

...	length	ID	fragflag	offset	...
	4000	408	000	0	

Las banderas indican que es un fragmento y el tercer bit que hay más.

...	length	ID	flags	offset	...
	1500	408	011	0	
...	length	ID	flags	offset	...
	1500	408	011	185	
...	length	ID	flags	offset	...
	1040	408	010	370	

Fragmentación y rearmado IP

Consideraciones:

- Si bien el reensablado de los datagramas esta pensado para llevarse a cabo en el destino, en algunos casos hay routers que lo podrían realizar.

- La fragmentación añade complejidad a los routers y sistemas terminales.

- Se ha utilizado para generar ataques DoS (**D**enial **O**f **S**ervice) caso en el que el atacante envía una serie de fragmentos extraños e inesperados.

  - **Jolt2** Muchos fragmentos pequeños sin ningún fragmento con offset 0.
  - **IP Fragment Overlap** numerosos fragmentos con offset solapados.

- IP v6 **no** admite la fragmentación

Direccionamiento IP

- Generalmente un host tiene un único enlace hacia la red, cuando IP desea comunicarse lo hace a través de este enlace.

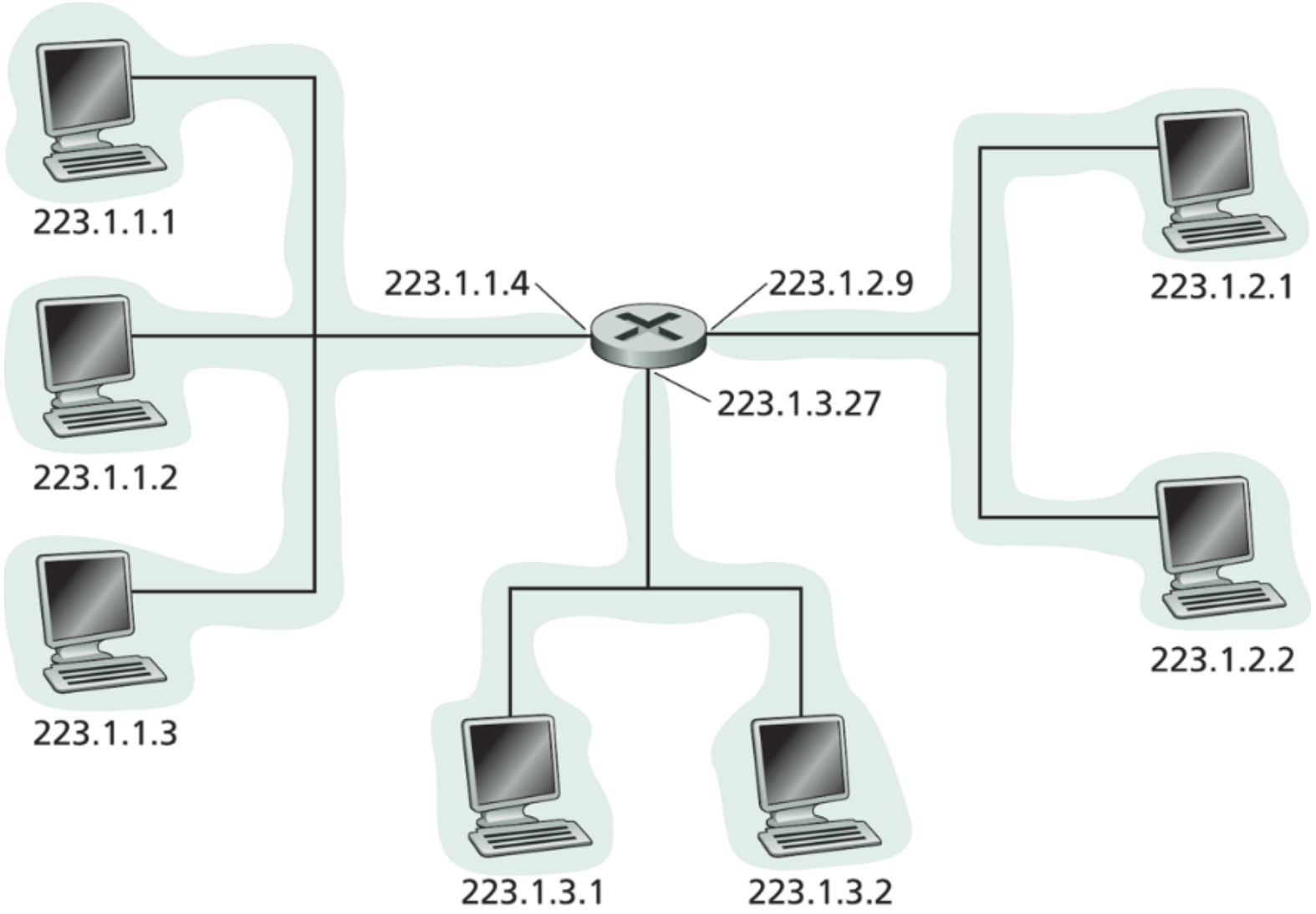
El límite entre el host y el enlace físico se denomina interfaz.

- Un router tendrá 2 o más enlaces, ya que su función así lo requiere.

Cada interfaz de host y de router debe tener su propia dirección IP.

La dirección IP se asocia a una interfaz.

Direccionamiento IP



Direccionamiento IP

Las direcciones IP tienen una longitud de 32 bits

32 bits = 4bytes

Se expresan utilizando notación decimal separando los números formados por los bytes con puntos.

Así por ejemplo:

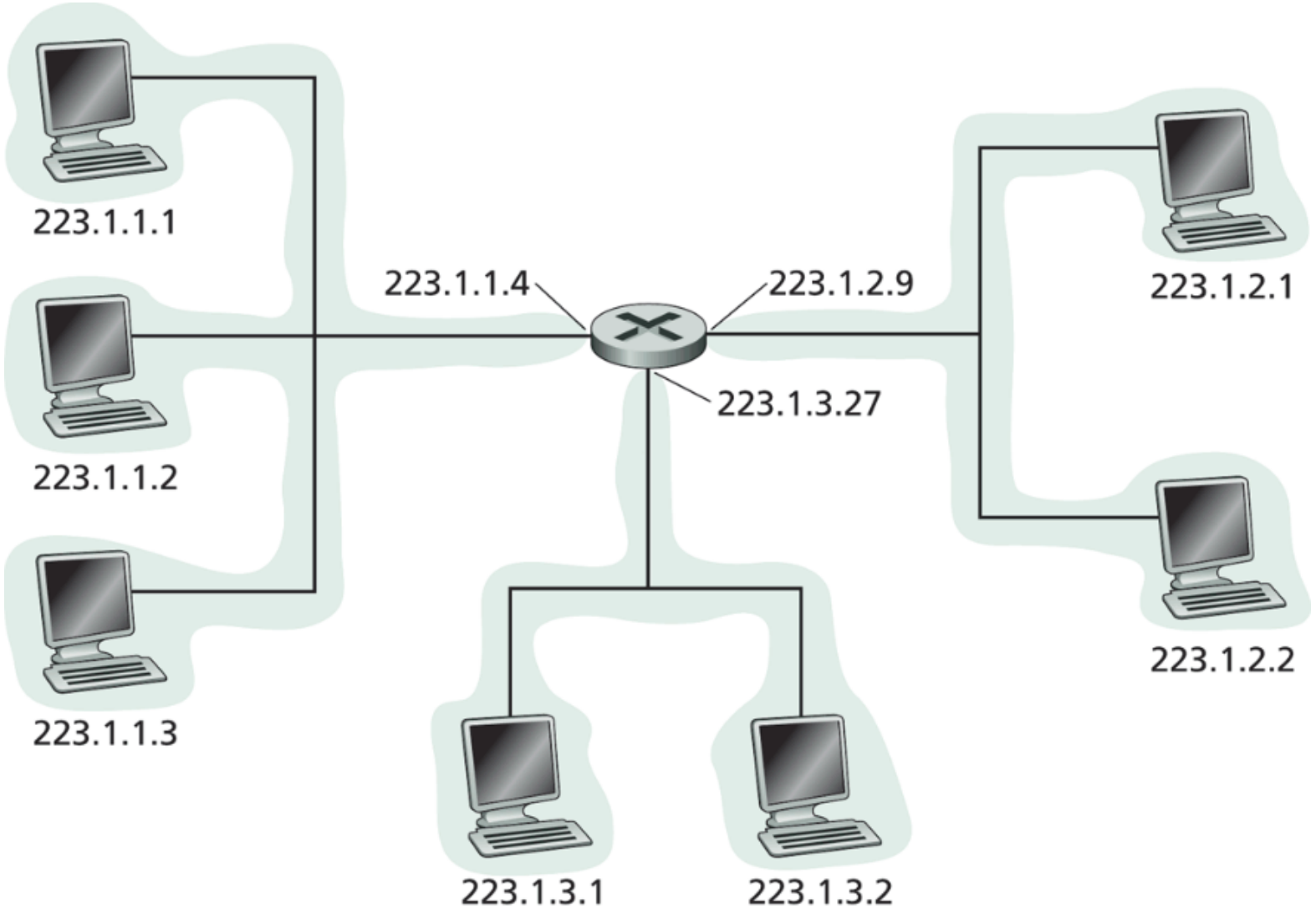
193.32.216.9

Equivale a la IP

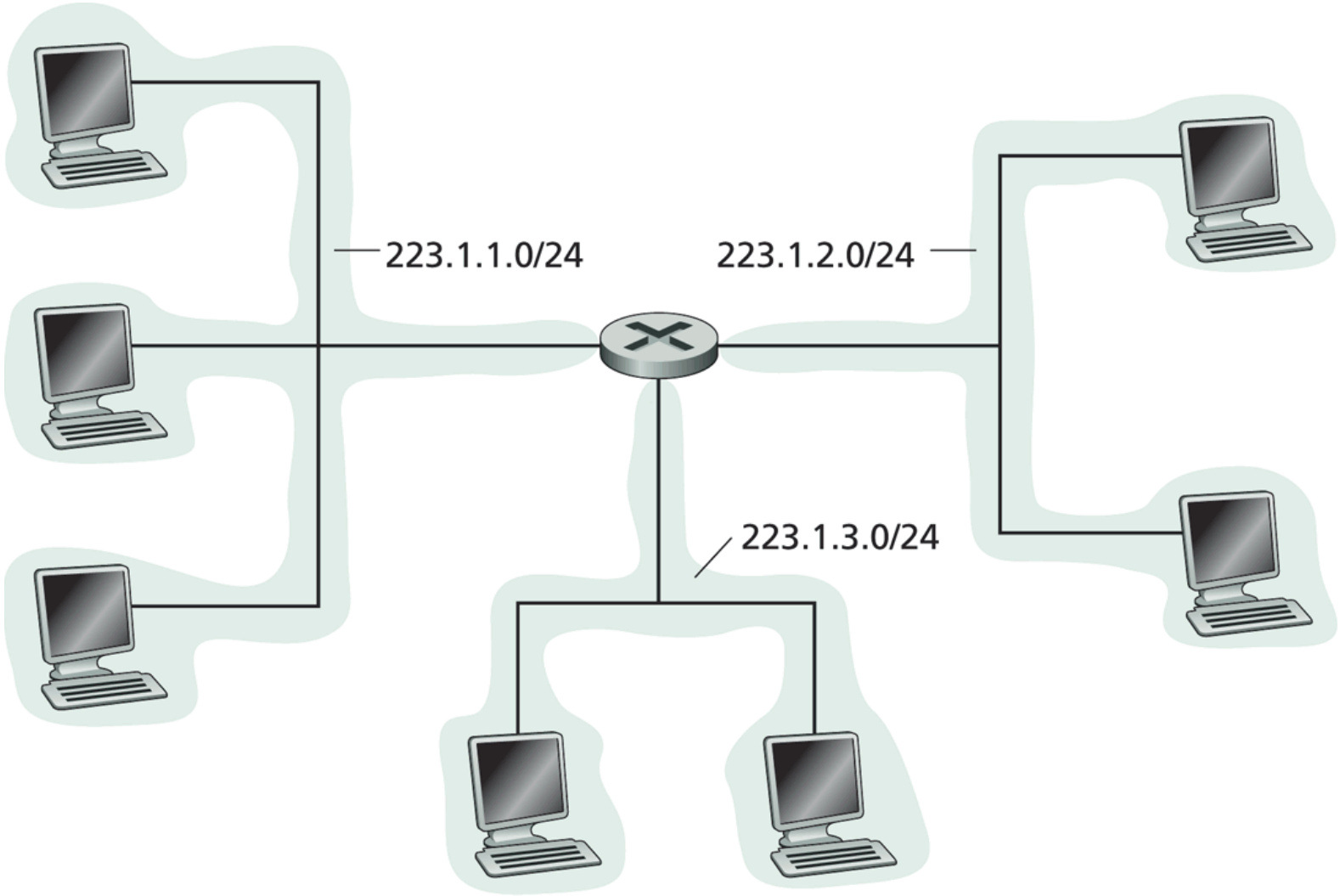
11000001 00100000 11011000 00001001

Cada interfaz conectada a Internet tiene asignada una IP globalmente única. (excepción de NAT)

Direccionamiento IP



Direccionamiento IP



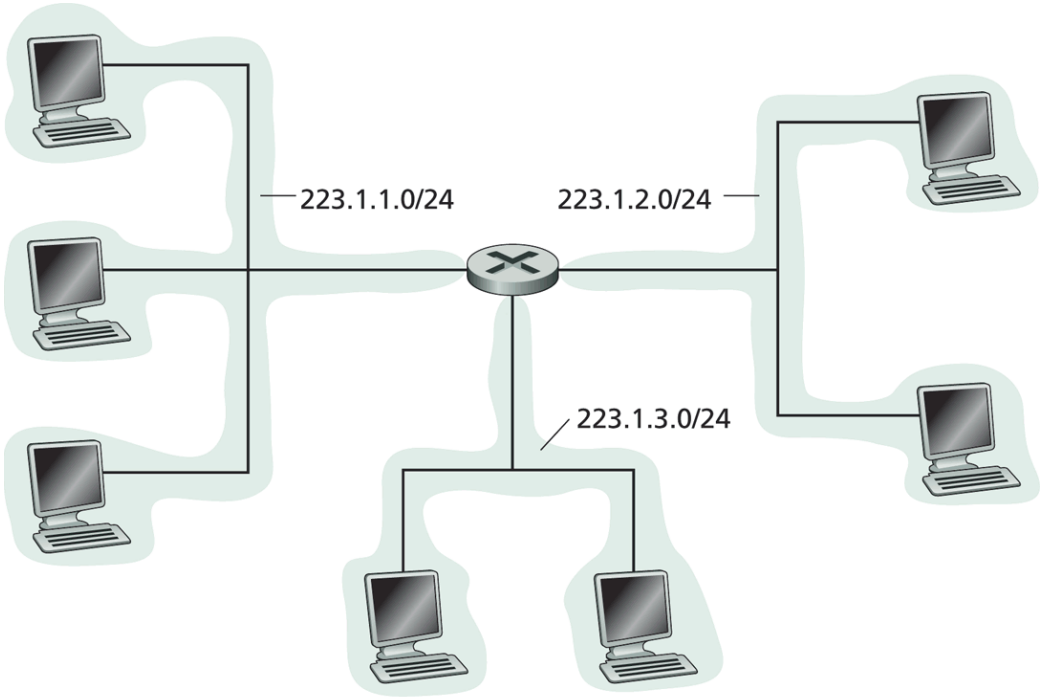
Subredes

La dirección IP se divide

- Parte de la subred (bits más altos)
- Parte del host (bits más bajos)

¿Qué es una subred?

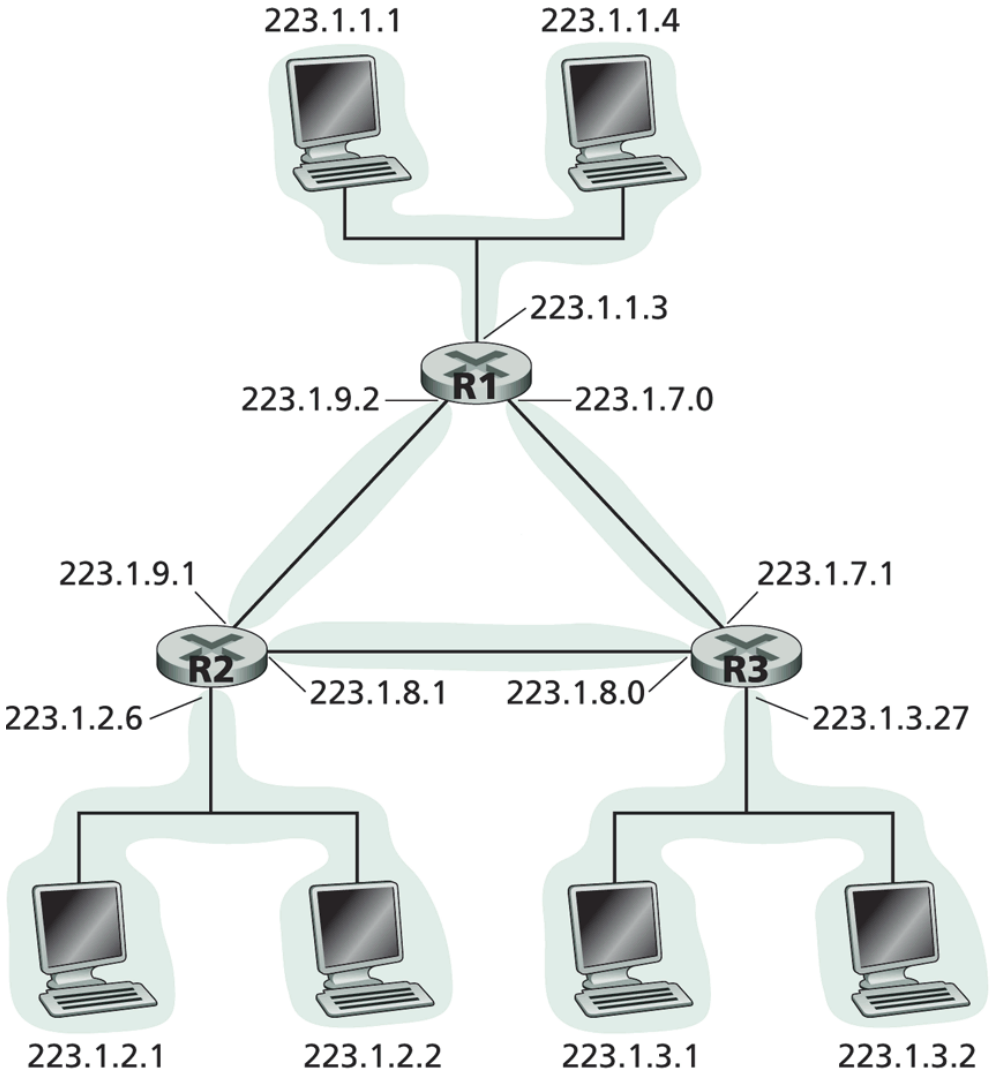
- Interfaces de dispositivos con la misma sección de subred en sus IPs
- Pueden alcanzarse físicamente sin la intervención de un router



Máscara de subred: /24

los 24 bits más a la izquierda de la dirección IP son iguales

Subredes


223.1.1.1
223.1.1.4
223.1.1.3
R1
223.1.9.2
223.1.7.0
223.1.9.1
223.1.7.1
R2
R3
223.1.8.1
223.1.8.0
223.1.2.6
223.1.3.27
223.1.2.1
223.1.2.2
223.1.3.1
223.1.3.2

Subredes
Máscara de sub red

Se utiliza para delimitar el ámbito de una red y así un host saber si debe enviar paquetes dentro de la red o fuera

Indica que parte de la IP:

- hace referencia a la red
- y que parte hace referencia al host.

Considerando un rango de direcciones
desde 223.0.0.0 hasta 223.255.255.255
siendo parte todas ellas de la misma red se podría expresar:

255.0.0.0

223.0.0.0/8

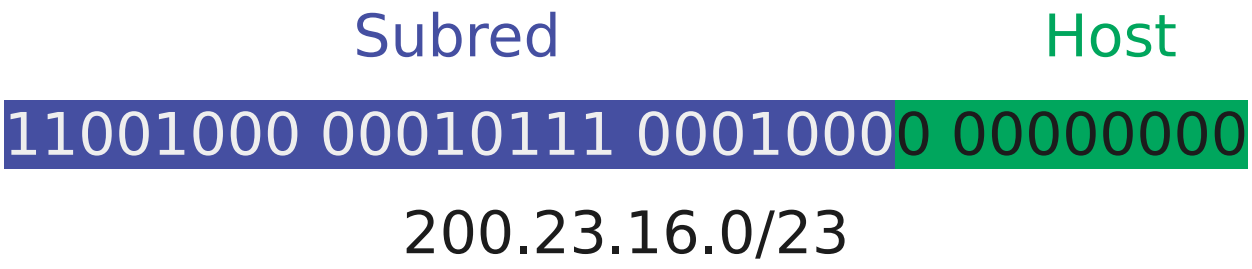
11111111 00000000 00000000 00000000

Direccionamiento IP

CIDR: Classless InterDomain Routing

- Porción de subred de la dirección de un largo arbitrario

- Formato de la dirección: a.b.c.d/x, donde x indica el número de bits que conforman la subred.



Direccionamiento IP
ISP

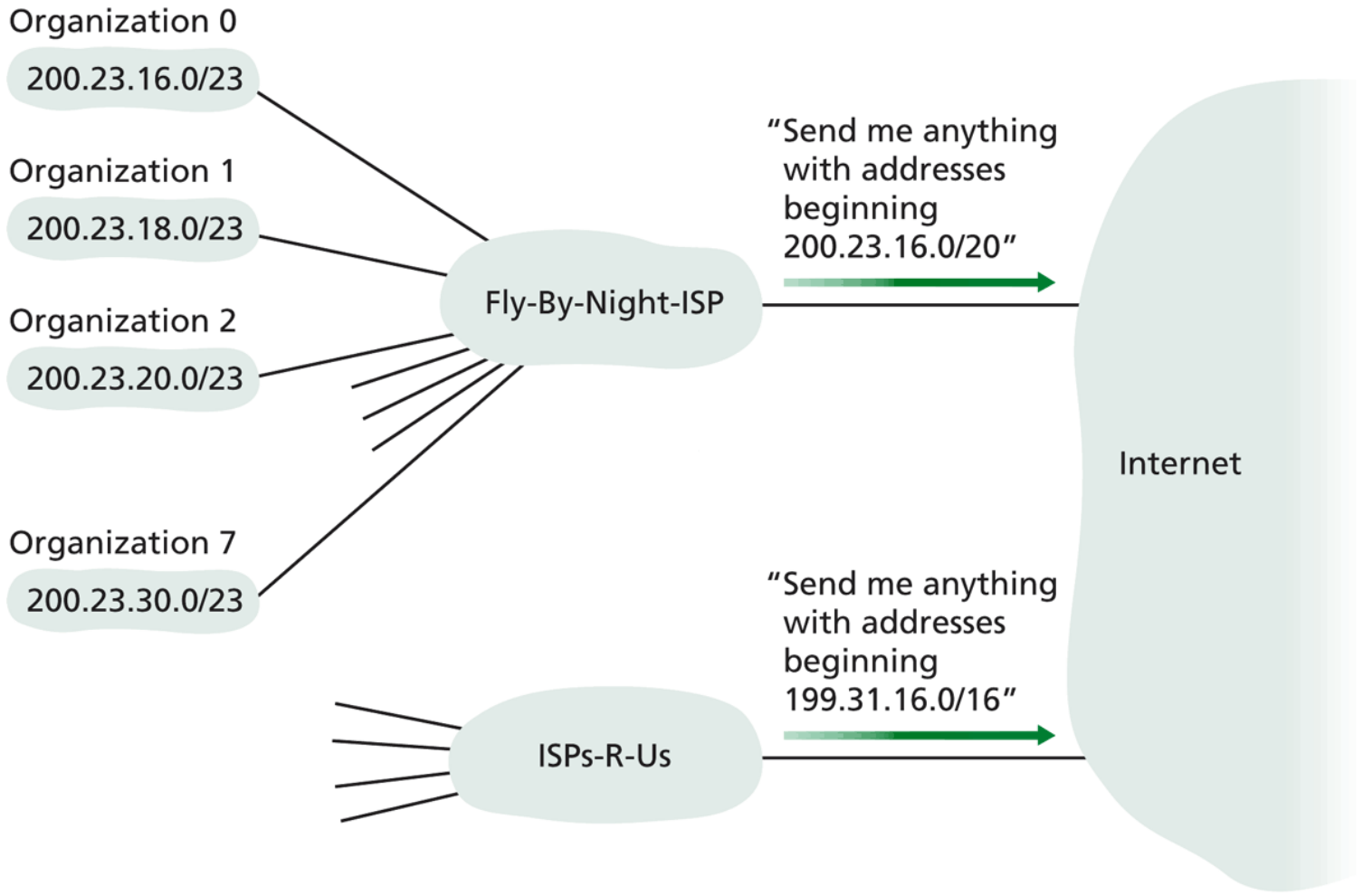


Figure 4.18 ♦ Hierarchical addressing and route aggregation

Direccionamiento IP
ISP

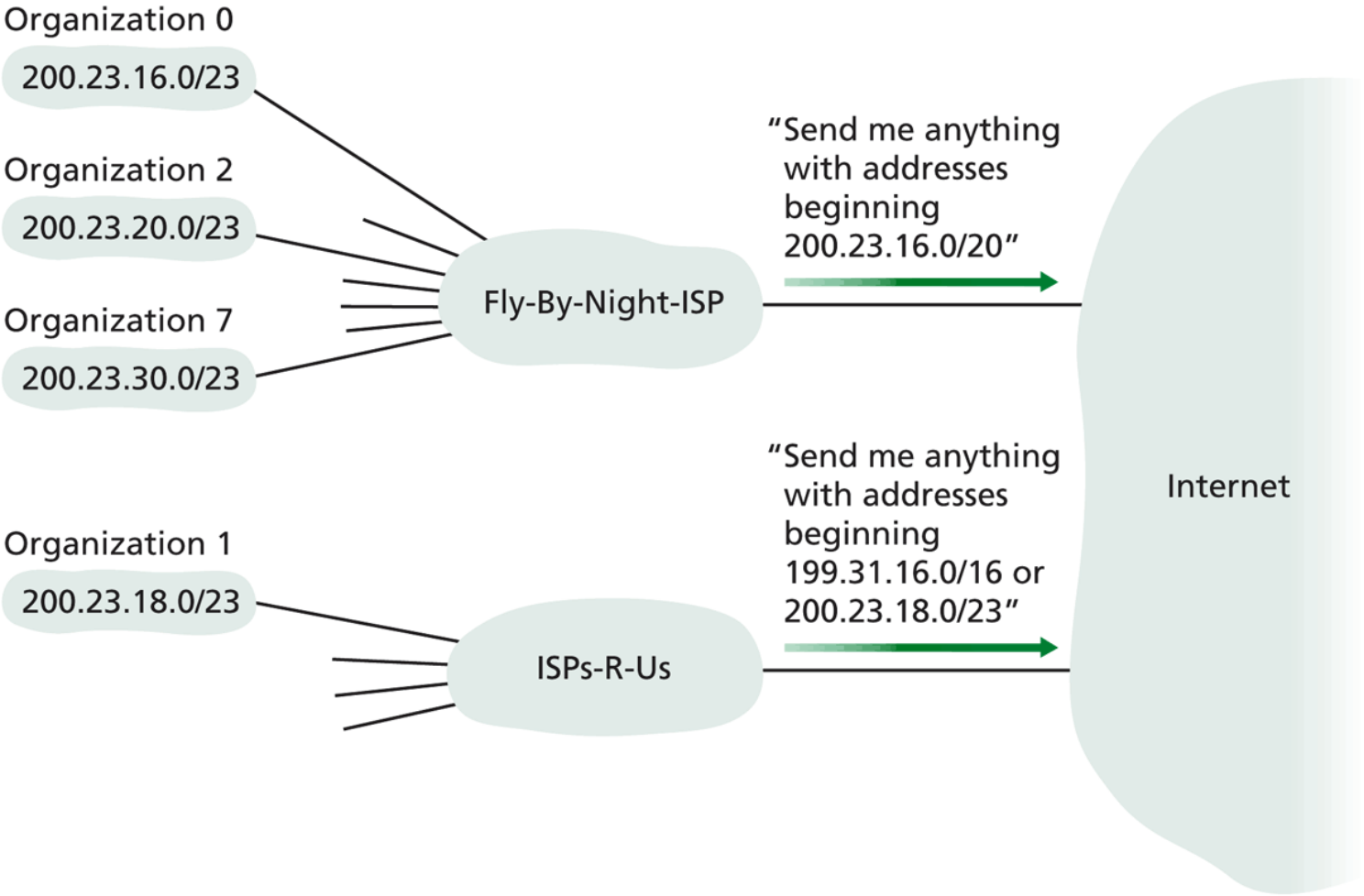


Figure 4.19 ♦ ISPs-R-Us has a more specific route to Organization 1

Direccionamiento IP

¿Cómo se obtiene la dirección IP?

- Asignada directamente por un administrador del equipo
  - En windows:

  Panel de control /Redes /Configuración /TCP-IP /Propiedades

  - UNIX:

  /etc/rc.config o

  /etc/network/interfaces

- DHCP (Dynamic Host Configuration Protocol)

  Protocolo para obtener dirección IP de forma dinámica

DHCP
Dynamic Host Configuration Protocol

Permite a los hosts obtener sus direcciones IP de forma dinámica de un servidor de red cuando se conecta a la red.

- Permite la reutilización de direcciones

Descripción de DHCP

- El host manda un mensaje de difusión (broadcast)
  DHCPDISCOVER
- El servidor DHCP responde con mensaje de
  DHCPOFFER
- El host solicita dirección IP mediante un mensaje
  DHCP request
- El servidor DHCP envía la dirección de regreso en un mensaje
  DHCP ACK

DHCP
Dynamic Host Configuration Protocol

DHCPDISCOVER

Un host recién conectado a la red enviará un paquete UDP dirigido al puerto 67 a la dirección IP de difusión 255.255.255.255 y la dirección IP de origen será 0.0.0.0

DHCPOFFER

El servidor DHCP responde con un mensaje de oferta también a la dirección de difusión donde se ofrece una dirección IP así como la mascara de red y el tiempo válido para la IP.

DHCPREQUEST

El nuevo host acepta una solicitud enviando nuevamente los parametros de configuración

DHCPACK

El servidor confirma la solicitud y desde entonces se puede utilizar la IP

DHCP
Dynamic Host Configuration Protocol

Se puede realizar una configuración mediante DHCP de tal modo que un host

- Siempre reciba la misma IP
- Reciba una IP temporal

A través de DHCP un host también recibirá información útil como:

- Máscara de subred
- Dirección del gateway predeterminado
- dirección de servidor DNS local

Se le denomina como un protocolo plug-and-play

Network Address Translation

NAT

El proveedor de internet no será el encargado de asignar direcciones IP a una LAN.

Para las direcciones privadas existen tres rangos reservados y el protocolo NAT será el encargado de traducir las direcciones incompatibles de dos redes (la LAN e Internet)

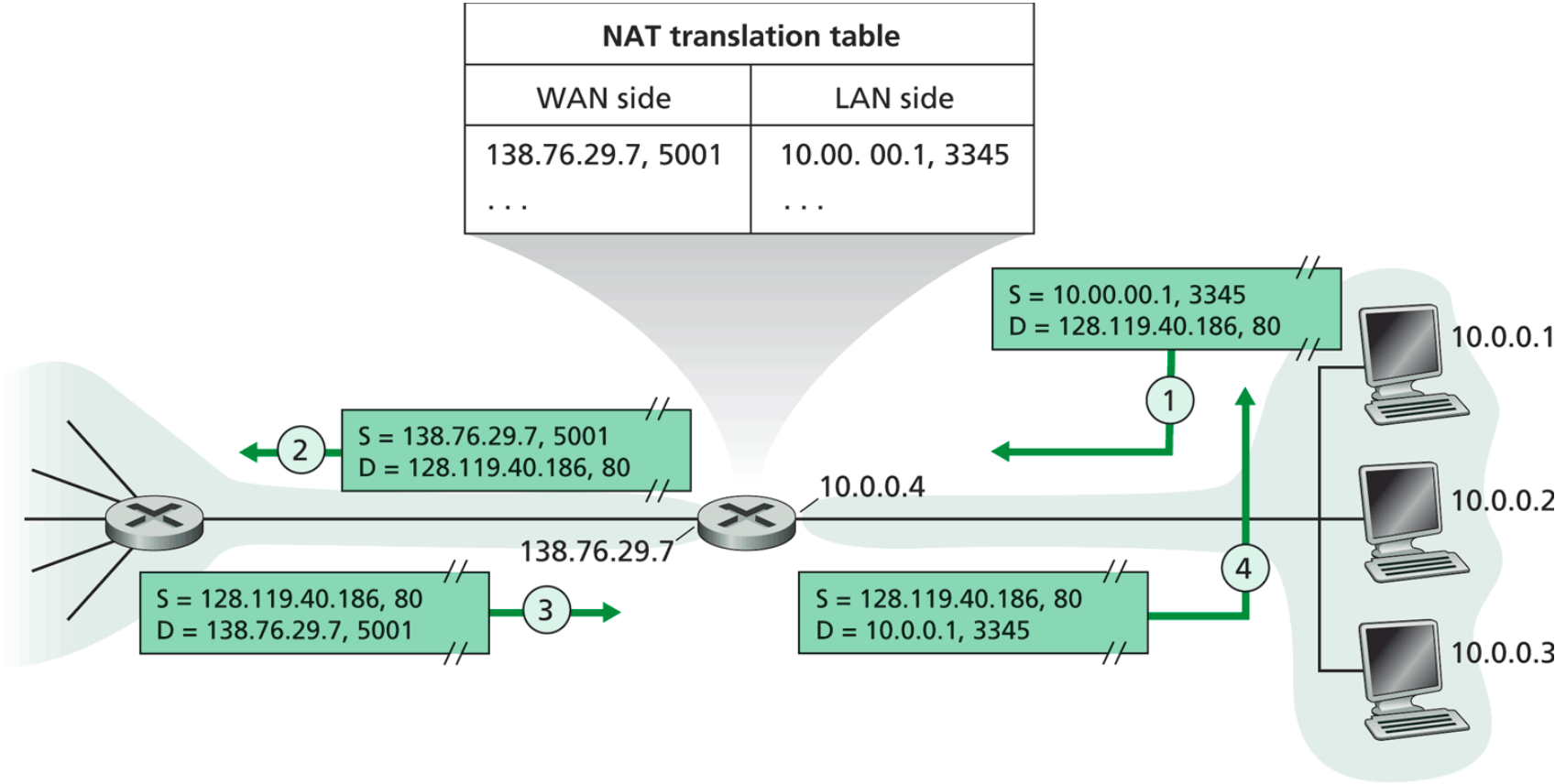
Network Address Translation

Redes privadas IPv4

Nombre	Rango	# de IPs	# de redes	# IPs por red	mask
Clase A 24bits	10.0.0.0 10.255.255.255	16.777.214	1	16.777.214	10.0.0.0/8 (255.0.0.0)
Clase B 20bits	172.16.0.0 172.31.255.255	1.048.574	16	65.534	172.16.0.0/12 (255.240.0.0)
Clase C 16bits	192.168.0.0 192.168.255.255	65.534	256	254	192.168.0.0/16 (255.255.0.0)

Network Address Translation

Al mundo exterior el router NAT se verá como un único dispositivo con una dirección IP única.



Network Address Translation

- Todos los datagramas que dejan la red local tienen la misma dirección, con diferente número de puerto.

- Los datagramas con origen o destino dentro de la red se comportarán de forma “normal”.

- Se puede modificar las direcciones de los dispositivos en la red interna sin notificar al mundo exterior.

- Los dispositivos dentro de la red local no son direccionables explícitamente, ni visibles para el resto del mundo.

Network Address Translation

Implementación:

Para los datagramas Salientes:

Se reemplaza la IP origen y el número de puerto de cada datagrama por la dirección IP NAT y un nuevo número de puerto.

Los clientes y servidores remotos responderán con la dirección destino NAT y el número de puerto determinado.

Tabla NAT:

Se debe mantener una tabla donde se realice la traducción
IP origen y número de puerto con su correspondiente NAT

Para los datagramas entrantes:

Se debe reemplazar la dirección NAT y el puerto ahí establecido por el original, guardado en la tabla.

Network Address Translation

Número de puerto de 16 bits:

Se soportan más de 60.000 conexiones simultaneas con una misma dirección IP.

Problemas:

Complica las aplicaciones

- El cambio NAT debe ser tenido en cuenta por los diseñadores de aplicaciones. (Por ejemplo de aplicaciones P2P)
- La falta de direcciones debería ser resuelta con la implantación de IPv6

Network Address Translation

Problema de atravesamiento

Un cliente desea conectarse con un servidor dirección 10.0.0.1

La dirección del servidor 10.0.0.1 es local a la LAN
(El cliente no la puede usar como dirección destino)

- Sólo hay una dirección externa visible

Posible solución:

Configurar NAT de forma estática para redirigir conexiones a un determinado puerto hacia el servidor.

Ejemplo:

Todas las peticiones al puerto 2500 serán redirigidas al 10.0.0.1:80

Network Address Translation

Problema de atravesamiento

Universal Plug and Play Internet Gateway Device (UPnP **IDG**)

- Le permite al host nateado aprender la IP pública
- Manipular la tabla NAT para agregar o remover mapeos.

ConectionReversal

Relaying

- El cliente Nateado se conecta al relay
- El cliente externo se conecta al relay
- El relay redirige los mensajes en la conexión