Bloque III
Redes Multimedia

Arquitecturas de redes de computadores
2012-2013

Rafael Sebastian
Departamento de Informática
Escuela Técnica Superior de Ingenierías
Universitat de València
Adaptado de Rogelio Montañana

Índice de contenido

- Introducción y conceptos
- Protocolos y aplicaciones en Internet
- Tecnologías avanzadas
- **Redes multimedia**
  - **IP Multicast**
- Seguridad en redes

Objetivos sección

- ☑ Diferenciar entre direccionamiento unicast y multicast
- ☑ Describir como circula el tráfico multicast a través de una red
- ☑ Entender el funcionamiento del protocolo IGMP

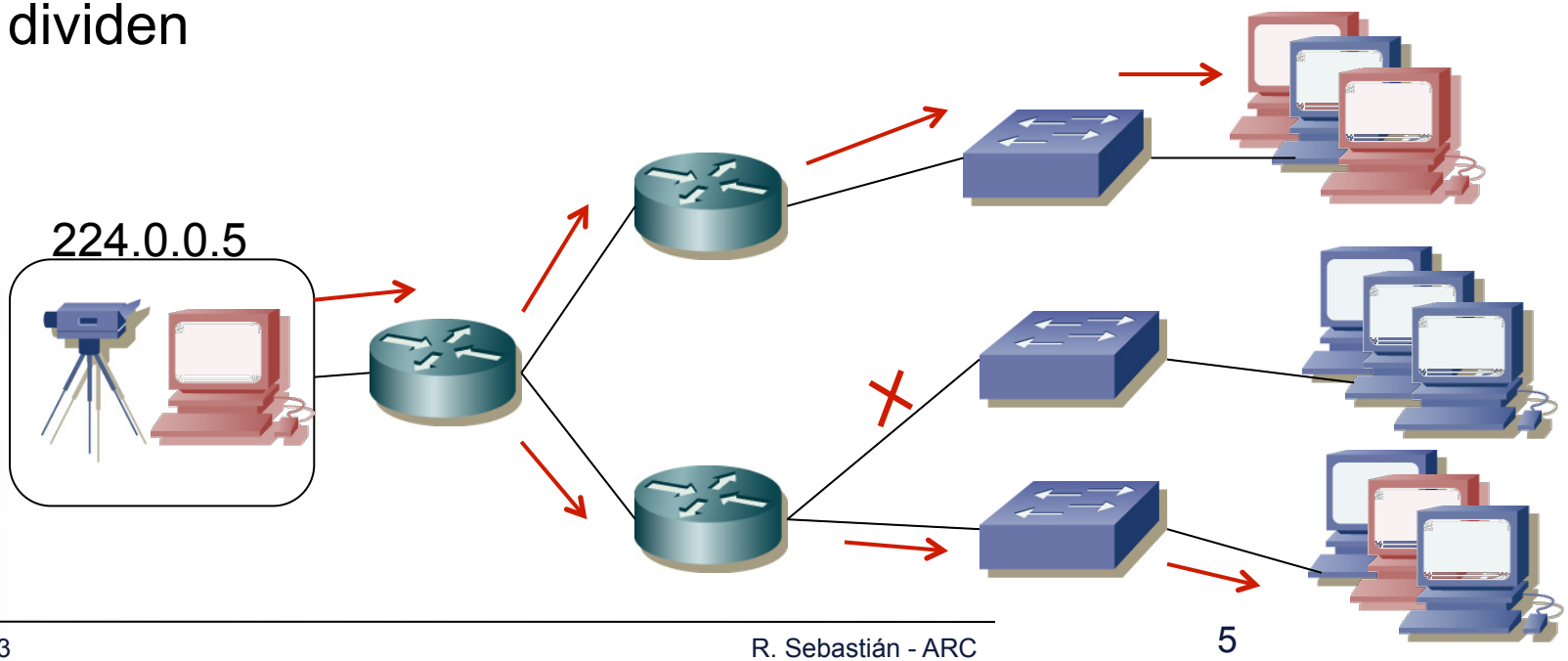
Redes Multimedia

IP Multicast

- **Introducción**
- IGMP

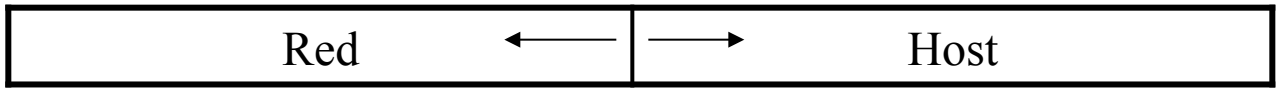
Multicast

- IP Multicast es un método para transmitir datagramas IP a un grupo de receptores interesados
  - usa la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red (sólo una vez)
  - crea copias cuando los enlaces en los destinos se dividen



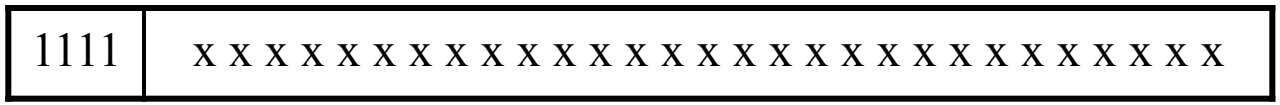
Tipos de direcciones IPv4

Unicast (A, B o C): 0.0.0.0 – 223.255.255.255

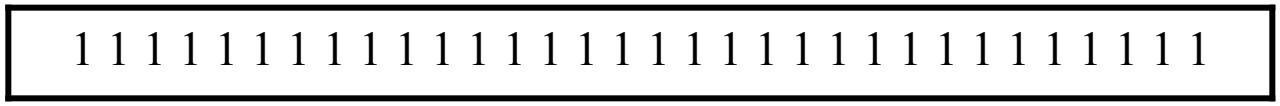


Multicast (D): 224.0.0.0- 239.255.255.255

Reservado (E): 240.0.0.0 – 255.255.255.254

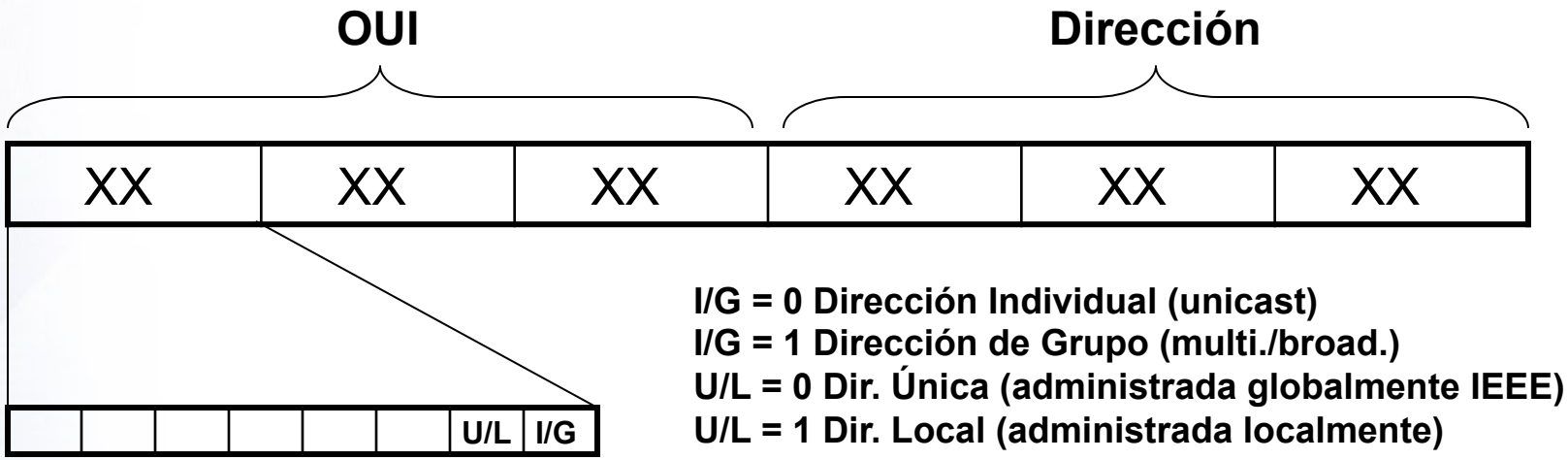


Broadcast (en la red actual): 255.255.255.255



Broadcast en una red (remota):

Direcciones multicast en Ethernet



- Por tanto el bit I/G es el último del primer byte.
- Regla:

  En Ethernet una dirección es multicast si y solo si el segundo dígito hexadecimal es impar.

  Ej.: la dirección AB-00-03-00-00-00 es multicast.

Multicast en LAN

- El tráfico multicast no es aislado normalmente por los conmutadores
- Muchos protocolos utilizan multicast en la LAN:
  - Spanning tree (dirección 01-80-C2-00-00-00)
  - Protocolos de routing: OSPF, IS-IS, RIP, etc.
  - Protocolos propietarios: Appletalk, IPX, CDP, etc.
- El tráfico multicast en una LAN puede ser importante aun cuando a nivel 3 (los routers) no esté habilitado el multicast

Multicast en una LAN broadcast compartida

0000.102C.D832

Grupo Multicast 0100.5E00.0001

Dir.Origen: 0000.102C.D832
Dir.Destino: 0100.5E00.0001

M

M

M

M

Join 0100.5E00.0001

Join 0100.5E00.0001

Juan

Rosa

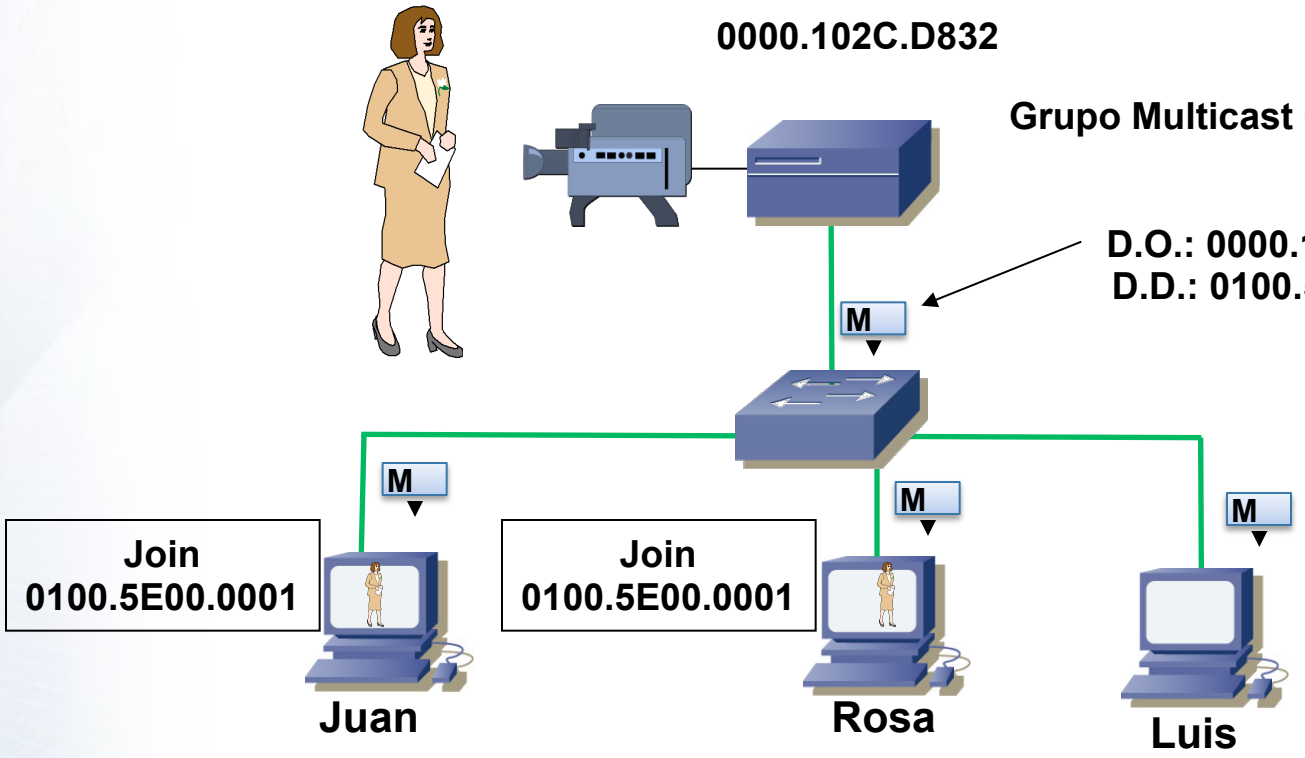
Luis

Direcciones capturadas por la tarjeta de red	Juan	Rosa	Luis
	0000.E85A.CA6D	0001.02CD.8397	0001.02CC.4DD5
	FFFF.FFFF.FFFF	FFFF.FFFF.FFFF	FFFF.FFFF.FFFF
	0100.5E00.0001	0100.5E00.0001	

En la LAN todos los equipos reciben todo el tráfico multicast, estén o no interesados

Afortunadamente la tarjeta de red descarta el que no nos interesa

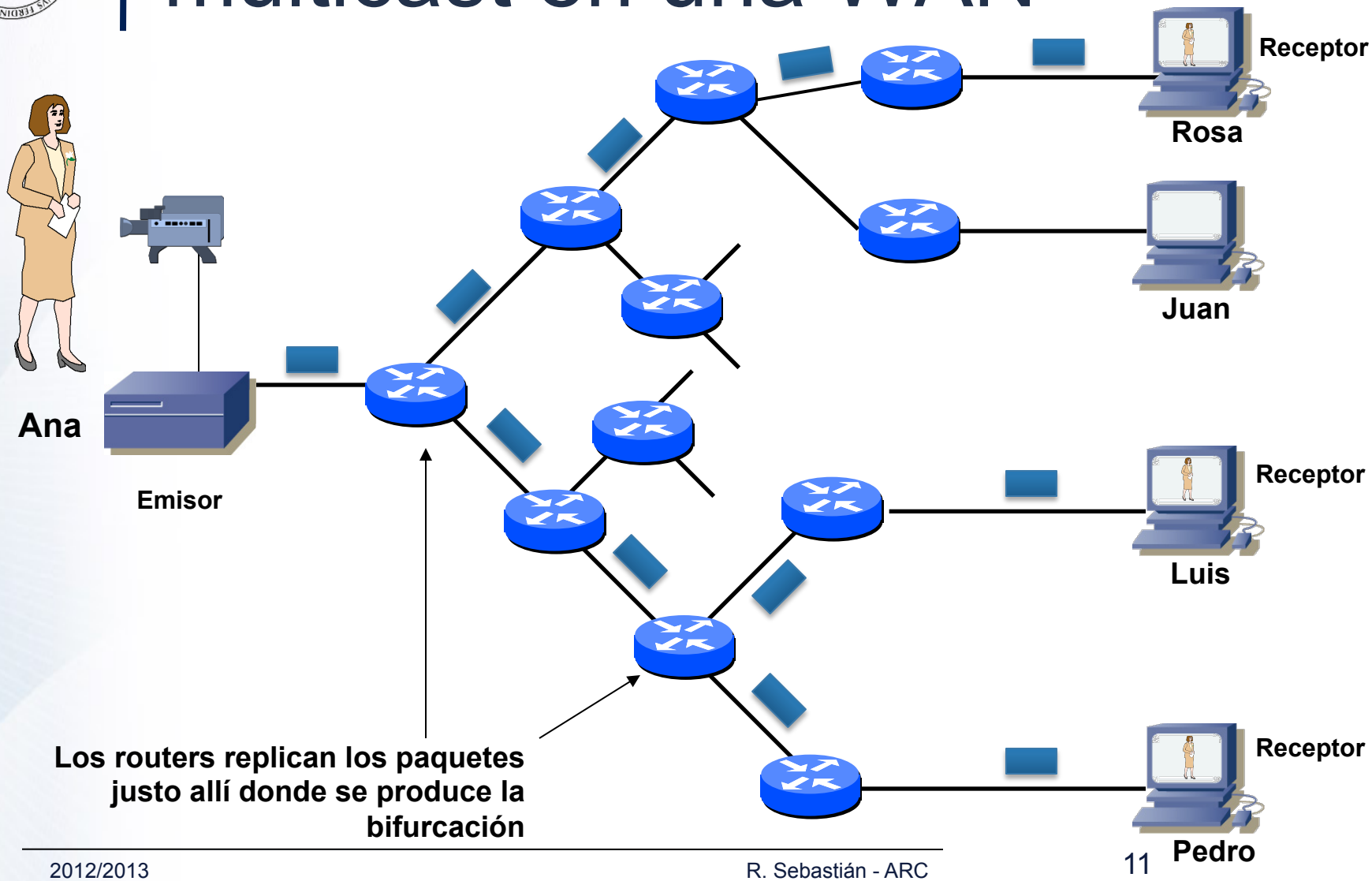
Multicast en una LAN broadcast conmutada



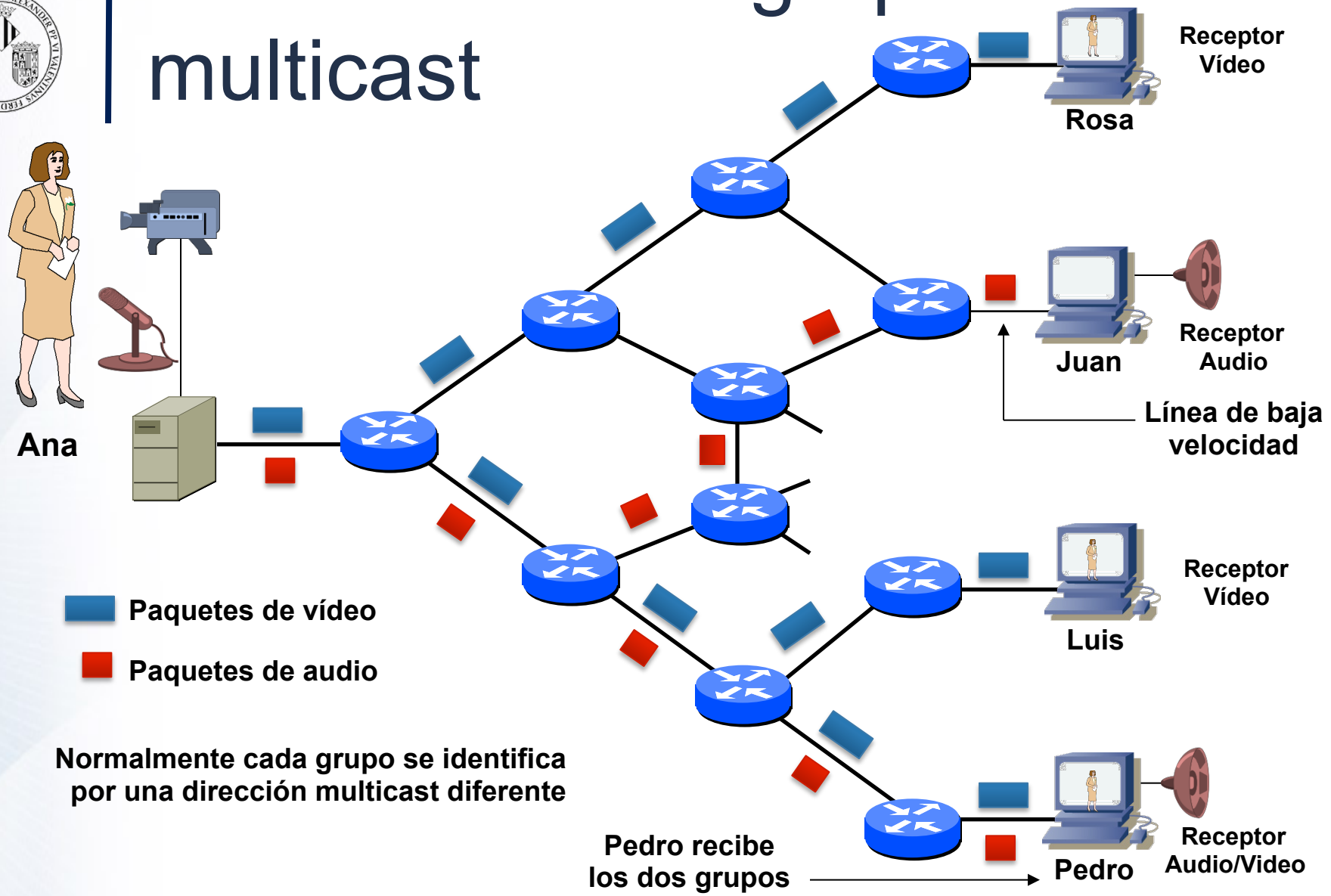
El uso de un conmutador no mejora la situación en lo que a tráfico multicast se refiere. El tráfico sigue llegando a todos los hosts

Direcciones capturadas por la tarjeta de red			
	0000.E85A.CA6D	0001.02CD.8397	0001.02CC.4DD5
	FFFF.FFFF.FFFF	FFFF.FFFF.FFFF	FFFF.FFFF.FFFF
	0100.5E00.0001	0100.5E00.0001	

Emisión de un grupo multicast en una WAN



Emisión de dos grupos multicast



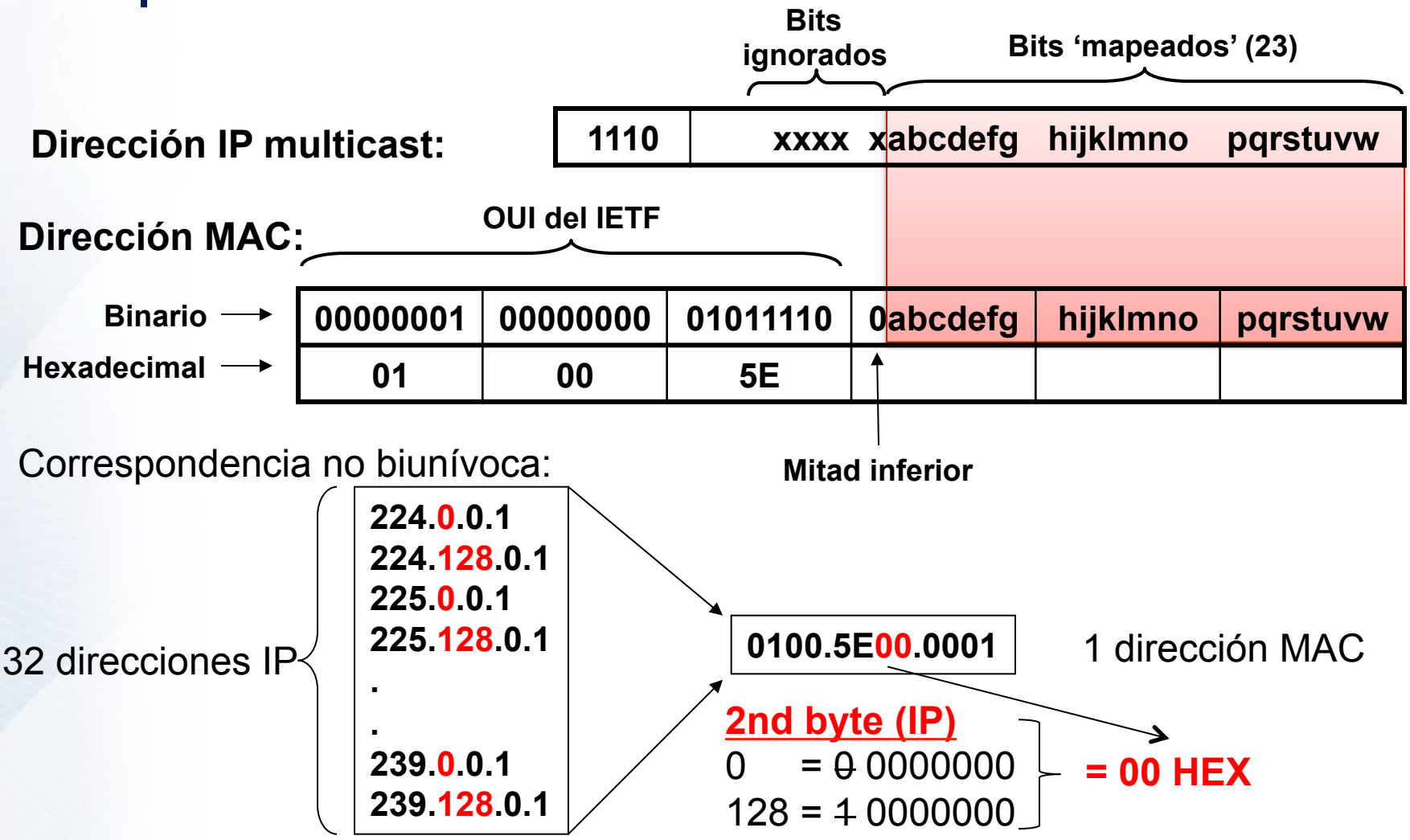
Direcciones Multicast en IP

- Las direcciones multicast tienen estructura plana (no jerárquica)
- Las direcciones multicast solo pueden aparecer como direcciones de destino, nunca de origen
- ICMP y multicast:
  - Los datagramas multicast no pueden dar lugar a mensajes ICMP DESTINATION UNREACHABLE
  - Tampoco pueden dar lugar a mensajes ICMP TIME EXCEEDED. Sin embargo el TTL se decrementa normalmente y cuando vale cero el datagrama se destruye
  - Los mensajes multicast ICMP ECHO REQUEST generan respuestas unicast de todos los miembros del grupo. Las respuestas, unicast, llevan como dirección de origen la del emisor y destino la del host que envió el ICMP multicast

Resolución de direcciones multicast IP-Ethernet

- Se realiza por mapeo de la dirección IP en la dirección MAC. No se utiliza ARP.
- Para hacer un mapeo exacto de la IP en la MAC harían falta 28 bits, es decir los 4 últimos bits de la OUI y los 24 siguientes. Esto requeriría reservar 2^4 = 16 OUIs contiguos, que habrían costado $16.000 dólares
- El IETF decidió comprar solo un OUI (01-00-5E) y dedicar solo la mitad inferior a multicast, reservando la otra para otros fines. Por tanto se dispone solo de 23 bits
- Por tanto en el mapeo se ignoran los cinco primeros bits de la dirección IP

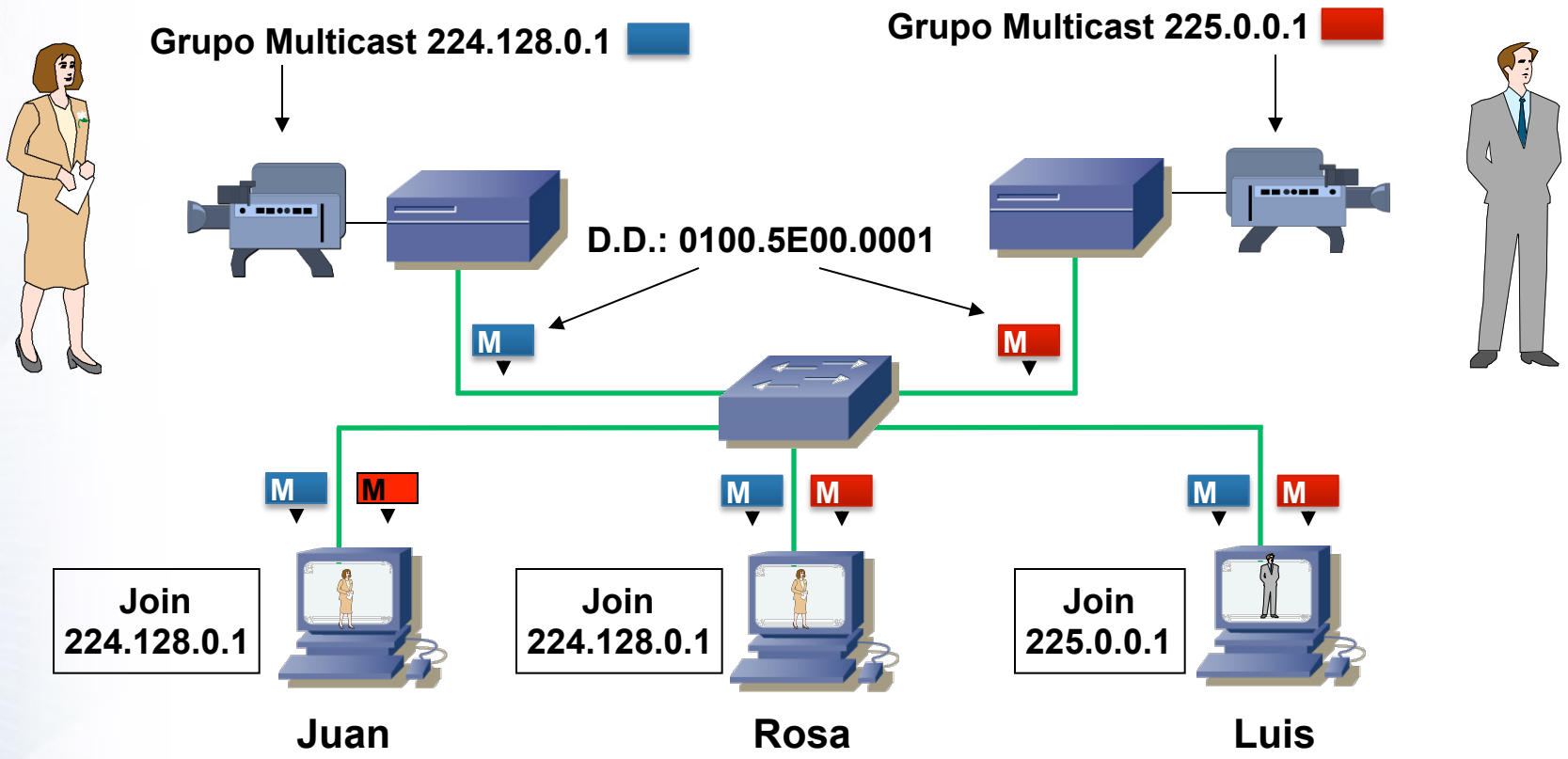
Resolución direcciones multicast IP-Ethernet



Resolución direcciones multicast

- Cuando en una LAN corresponde la misma MAC a dos direcciones IP multicast la tarjeta LAN pasa los dos grupos al nivel de red
- El nivel de red filtra los paquetes que no son suyos. El protocolo funciona pero el trabajo extra del nivel de red produce un consumo adicional de CPU
- Algunas tarjetas de red aceptan un número muy limitado de grupos multicast; cuando se supera este límite se ponen en modo 'aceptar todo el multicast'. El nivel de red ha de realizar el filtrado. Es como un modo promiscuo para el tráfico multicast

Resolución de direcciones multicast



Direcciones capturadas por la tarjeta de red	Juan	Rosa	Luis
	0000.E85A.CA6D	0001.02CD.8397	0001.02CC.4DD5
	FFFF.FFFF.FFFF	FFFF.FFFF.FFFF	FFFF.FFFF.FFFF
	0100.5E00.0001	0100.5E00.0001	0100.5E00.0001

Rangos de direcciones multicast IPv4 reservadas o especiales

Rango	Uso
224.0.0.0/24	Direcciones locales asignadas por la IANA. No propagadas por los routers.
224.0.1.0/24	Direcciones globales asignadas por la IANA. Propagadas por los routers
224.0.2.0/24 – 224.0.255.0/24	Bloque para asignaciones ad-hoc. Probablemente el más utilizado
224.1.0.0/16	Grupos multicast para Stream Protocol
224.2.0.0/16	Bloque SAP/SDP (MBone)
232.0.0.0/8	Multicast específico de la fuente (SSM)
233.0.0.0/8	Reservado para 'glop addressing'
239.0.0.0/8	Multicast con ámbito limitado por la dirección
255.255.255.255/32	Broadcast confinado a la LAN

Los rangos no incluidos en esta tabla están reservados por la IANA (Internet Assignment Numbers Authority) y no deberían utilizarse

Algunas direcciones IPv4 multicast reservadas

Locales

Dirección	Uso
224.0.0.0	Reservada
224.0.0.1	Hosts con soporte multicast
224.0.0.2	Routers con soporte multicast
224.0.0.4	Routers DVMRP (routing multicast)
224.0.0.5	Routers OSPF
224.0.0.6	Routers OSPF designados
224.0.0.9	Routers RIP v2
224.0.0.10	Routers IGRP
224.0.0.11	Agentes móviles
224.0.0.12	Agentes DHCP server/relay
224.0.0.13	Routers PIMv2 (routing multicast)
224.0.0.15	Routers CBT (routing multicast)
224.0.0.22	Routers IGMP v3 (Memb. Report)
255.255.255.255	Todos los hosts

Globales

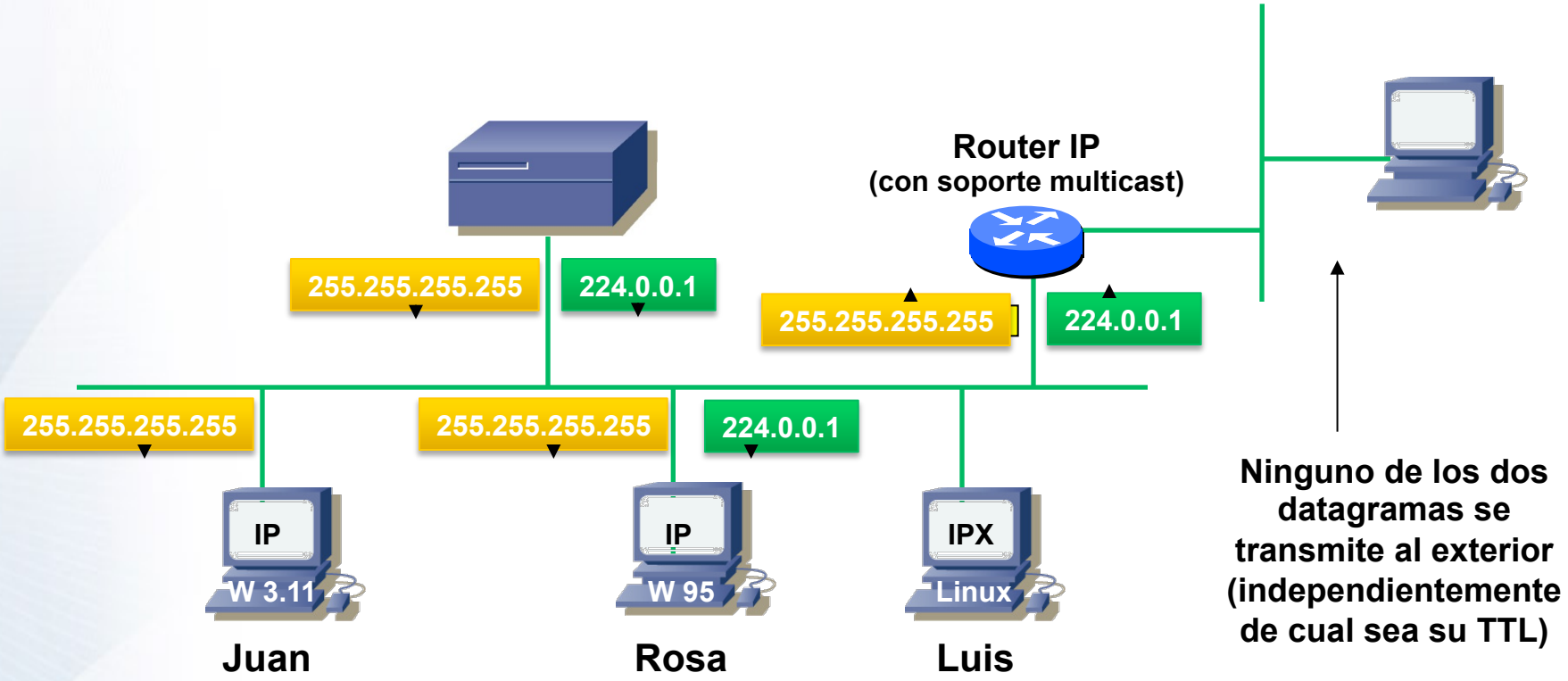
Dirección	Uso
224.0.1.1	NTP–Network Time Protocol
224.0.1.7	Audio News
224.0.1.12	IETF-1-Video
224.0.1.16	Music-Service
224.0.1.39	RP Announce (PIM)
224.0.1.40	RP Discovery (PIM)
224.0.1.41	Gatekeepers (H.323)
224.0.1.52	Directorio VCR de MBone
224.0.1.68	Protocolo MADCAP
224.2.127.254	Anuncio de sesiones SAP (SDR)

Las direcciones multicast reservadas se resuelven al nombre correspondiente en el dominio mcast.net, p. ej. 224.0.1.7 es *audionews.mcast.net*

Envíos broadcast en Internet

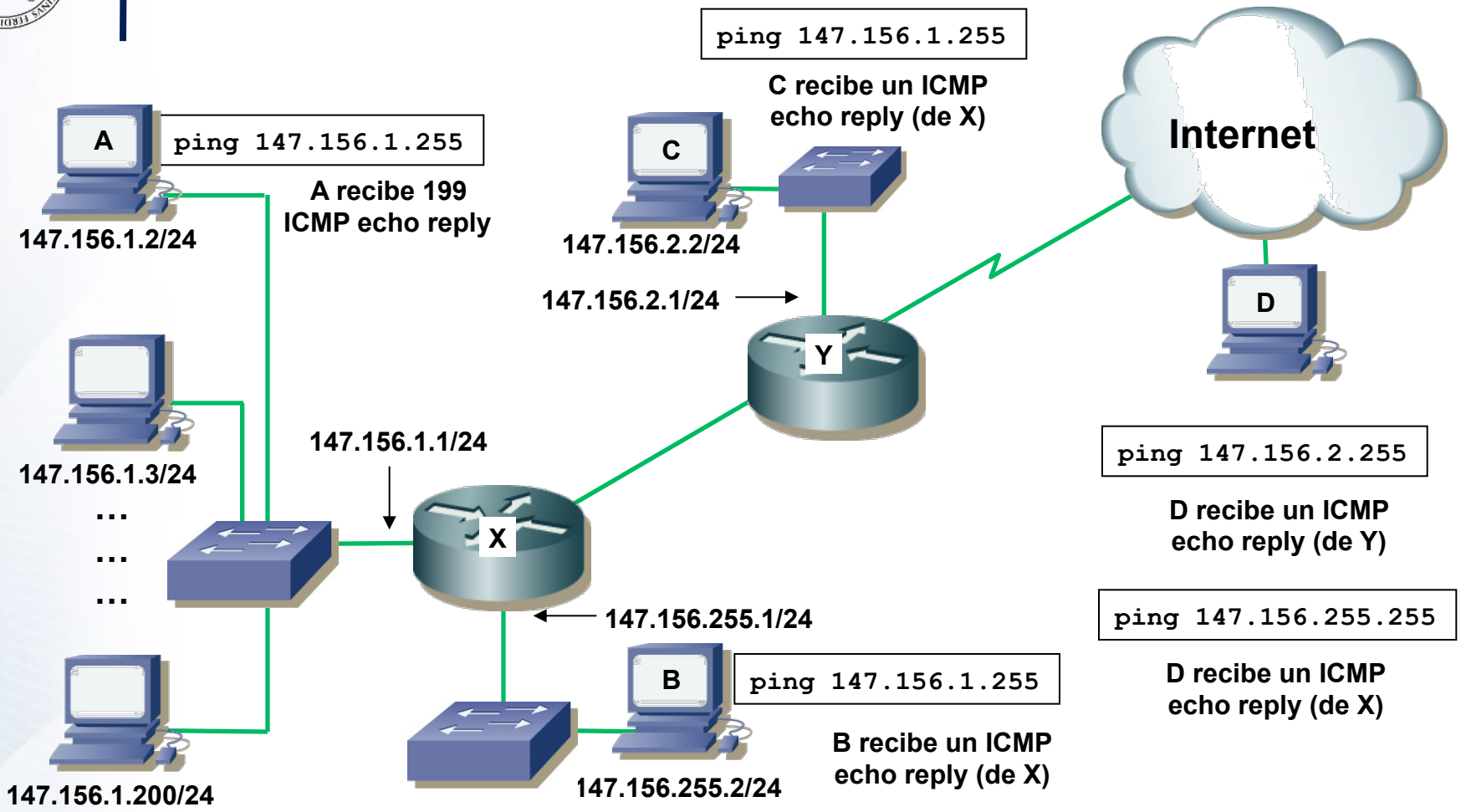
- En Internet no es posible hacer un envío broadcast. Si utilizamos la dirección 255.255.255.255 el envío se difunde en la red local únicamente, no pasa más allá.
- Dicho de otro modo, el paquete broadcast es tratado como si tuviera TTL=1, cualquiera que sea el valor de TTL que realmente tenga
- Esto se hace para preservar la 'salud' de la red. De lo contrario cualquier usuario desaprensivo o despistado podría saturar la red

Diferencia entre envíos a 255.255.255.255 y a 224.0.0.1



El kernel de Windows 3.11 no tiene soporte multicast

Broadcast en IP



Se supone que los routers X e Y tienen todas sus interfaces con la configuración por defecto, es decir con `'no ip directed-broadcast'`

Ámbito de una emisión multicast

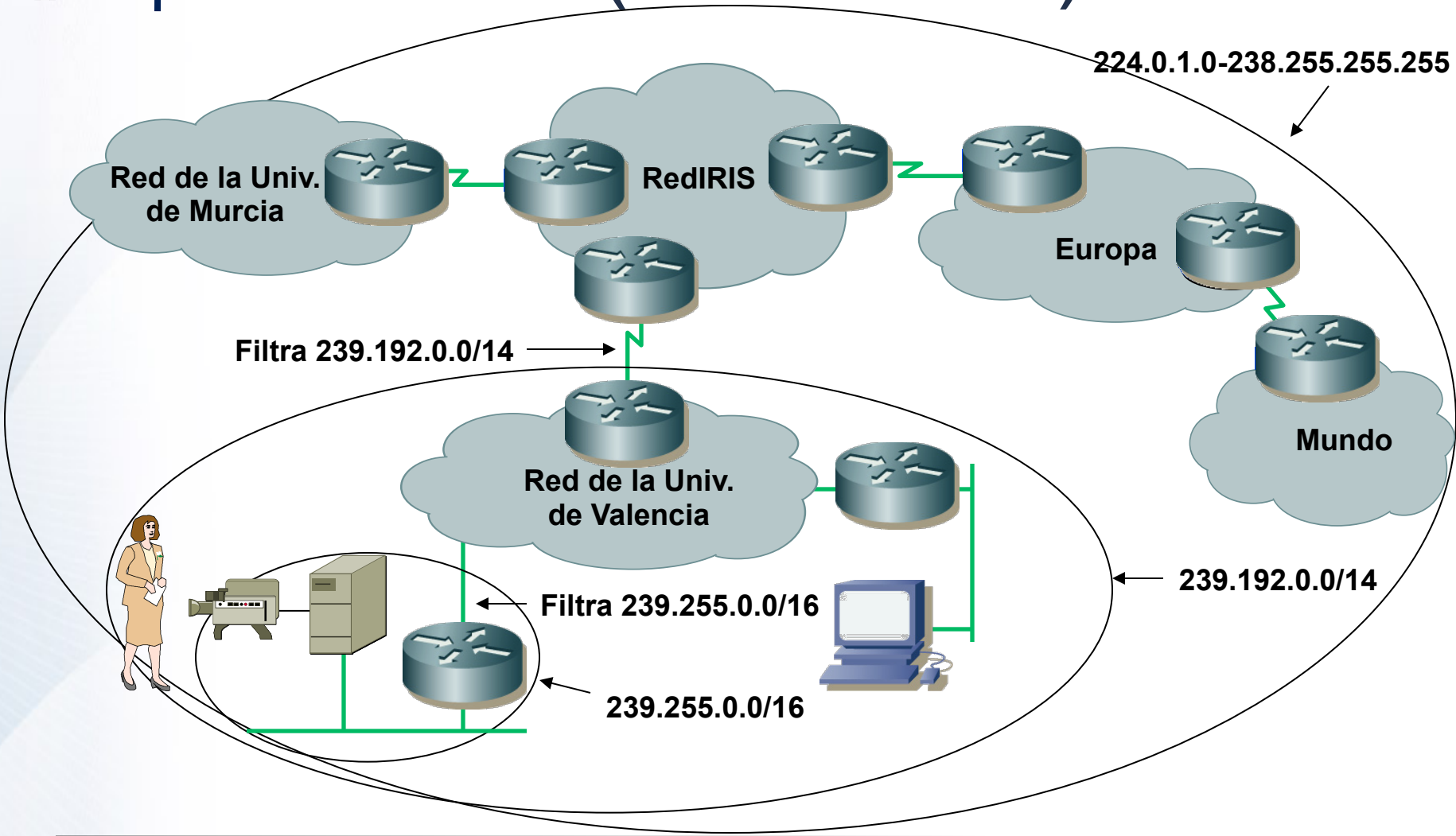
- En multicast es fundamental disponer de mecanismos que permitan limitar el ámbito de difusión de los grupos multicast. Esto puede conseguirse de tres formas:
  - Ajustando el valor del TTL (obsoleto)
  - Asignando rangos de direcciones a determinados ámbitos
  - Utilizando el protocolo de anuncio de ámbitos MZAP (Multicast Zone Announcement Protocol, RFC 2776). Poco extendido

Delimitación de Ámbito por dirección (RFC 2365)

- Se asigna un significado especial a determinados rangos de direcciones multicast
- El router, mediante ACLs, realiza un filtrado de los paquetes multicast que no deben salir (este filtrado es independiente del descarte por TTL=0

Rango	Ámbito
224.0.0.0/24 (224.0.0.0-224.0.0.255)	Nivel de enlace (LAN)
224.0.1.0-238.255.255.255	Global.
239.0.0.0 – 239.191.255.255	Reservado para usos futuros
239.192.0.0/14 (239.192.0.0-239.195.255.255)	Organización
239.196.0.0 – 239.254.255.255	Reservado para usos futuros
239.255.0.0/16 (239.255.0.0-239.255.255.255)	Nivel de enlace (LAN)

Delimitación del ámbito por dirección (RFC 2365)



Asignación de direcciones multicast

- Actualmente en Internet las direcciones multicast se asignan normalmente mediante el protocolo SAP (Session Announcement Protocol, RFC 2974, 10/2000). El rango de direcciones que utiliza SAP es el 224.2.0.0/16.
- El SAP presenta varios inconvenientes:
  - Tiene una estructura plana, no jerárquica. Por tanto no es escalable
  - Esta pensado específicamente para aplicaciones multimedia
  - La asignación se realiza dinámicamente. No es posible efectuar asignaciones estáticas (permanentes)
- Se han propuesto otros protocolos más avanzados pero hasta la fecha no han tenido éxito

‘Glop addressing’

- Para asignar direcciones IP multicast estáticas se utiliza actualmente el denominado ‘Glop addressing’ (RFC 3180, 9/2001), que funciona así:
  - Se utiliza el rango 233.0.0.0/8 (233.0.0.0 – 233.255.255.255)
  - Se asigna a los dos bytes centrales el valor del AS correspondiente. Ej.: a RedIRIS (AS 766) le corresponde el rango 233.2.254/24 (2.254 equivale a 766 expresado en dos bytes)
  - Dentro de cada AS el ISP asigna las direcciones como le parece

Redes Multimedia

IP Multicast

- Introducción
- **IGMP**

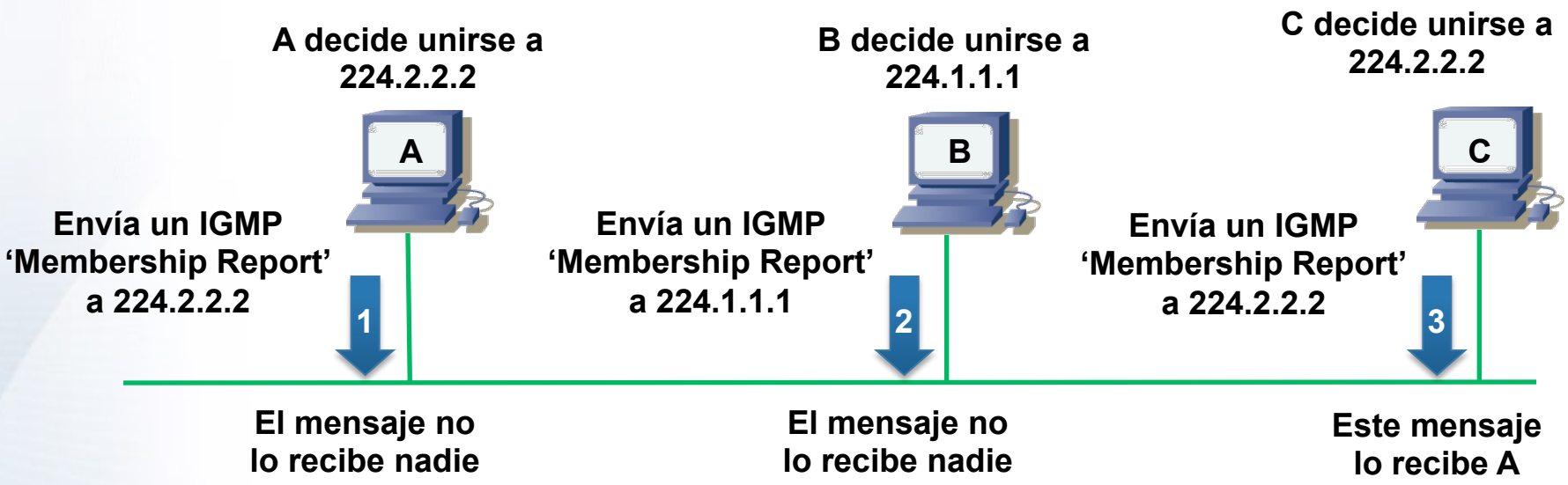
IGMP = Internet Group Management Protocol

- Objetivo: permite a los routers averiguar los grupos multicast presentes en sus interfaces LAN
- Utiliza el valor 2 del campo ‘protocolo’ en la cabecera IP
- Todos los mensajes IGMP se emiten con TTL=1, por lo que solo son recibidos en la LAN correspondiente a la interfaz por la que se emiten
- Existen tres versiones de IGMP:
  - V1: RFC 1112 (8/1989): Ej. W95, NT 4.0 SP3
  - V2: RFC 2236 (11/1997): W98, NT 4.0 SP 4, W2000
  - V3: RFC 3376 (10/2002): XP Prof., W2003

Tipos de mensajes en IGMPv1

Tipo	Emitido por	Función	Dirección de destino
Consulta de miembros (Membership Query)	Routers	Preguntar a los hosts si están interesados en algún grupo multicast	224.0.0.1
Informe de Pertenencia (Membership Report)	Hosts	Informar a los routers que el host está interesado en un determinado grupo multicast	La del grupo en cuestión

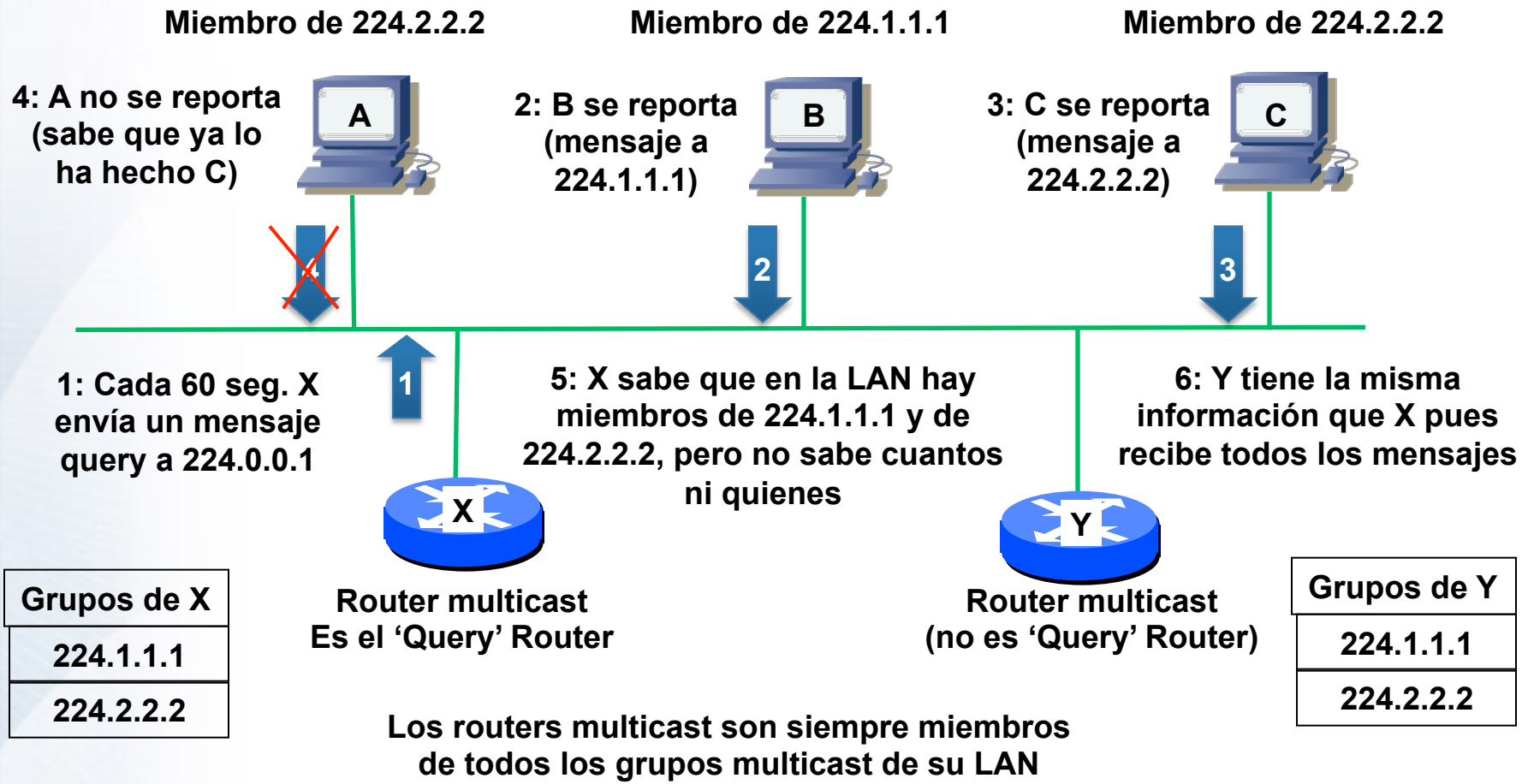
Proceso ‘presentarse’ de IGMPv1



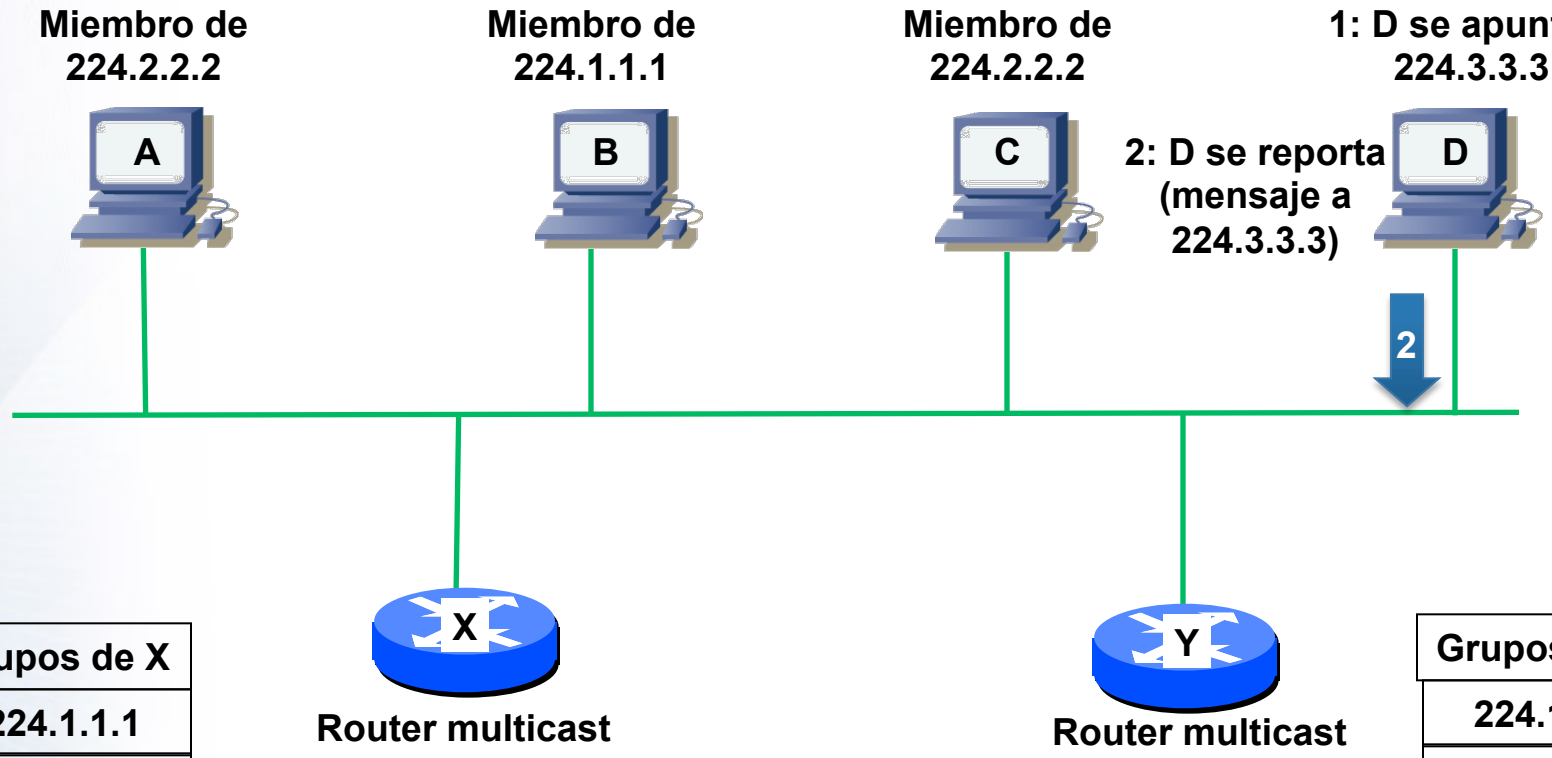
Cuando un host quiere entrar a formar parte de un grupo multicast envía un mensaje IGMP de ‘saludo’ llamado Membership Report.

Estos mensajes se envían al mismo grupo multicast al que se quiere unir el host

Proceso pregunta-respuesta de IGMPv1



Proceso apuntarse (join) de IGMPv1

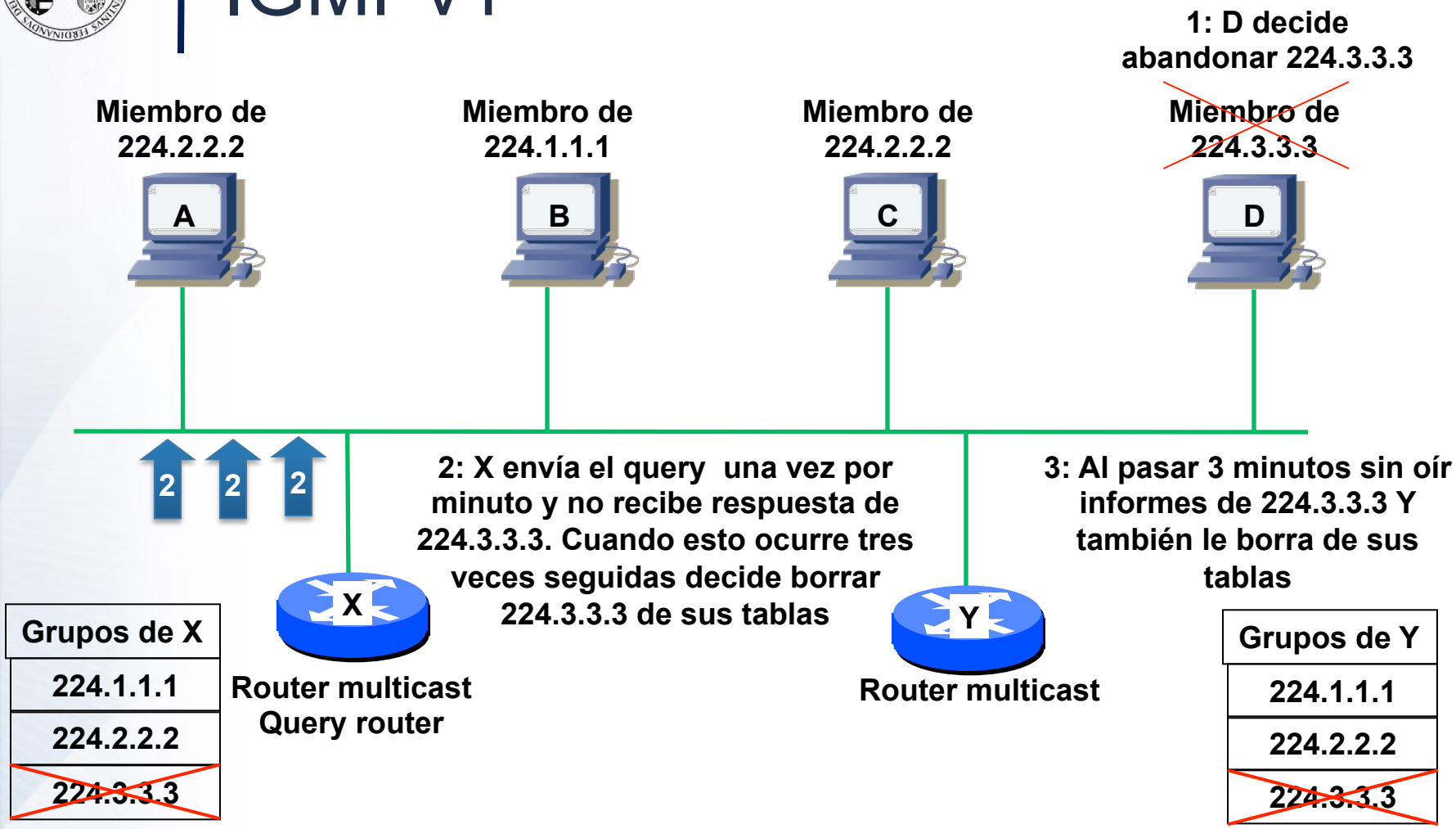


Grupos de X
224.1.1.1
224.2.2.2
224.3.3.3

Grupos de Y
224.1.1.1
224.2.2.2
224.3.3.3

3: Los routers toman nota de que hay presente un miembro de un nuevo grupo multicast, el 224.3.3.3

Proceso abandonar (leave) de IGMPv1



Problemas de IGMP v1

- Cuando un host abandona un grupo el tráfico multicast puede seguir inundando esa LAN durante un tiempo largo (tres minutos). Si el usuario hace ‘zapping’ esto consume mucho ancho de banda inútilmente y puede suponer un problema en la red.
- No se especifica por que mecanismo se elige al ‘Query router’. Se supone que se utilizará el router elegido como designado por el protocolo de routing.
- Los timeouts para la recepción de informes no se pueden configurar dinámicamente

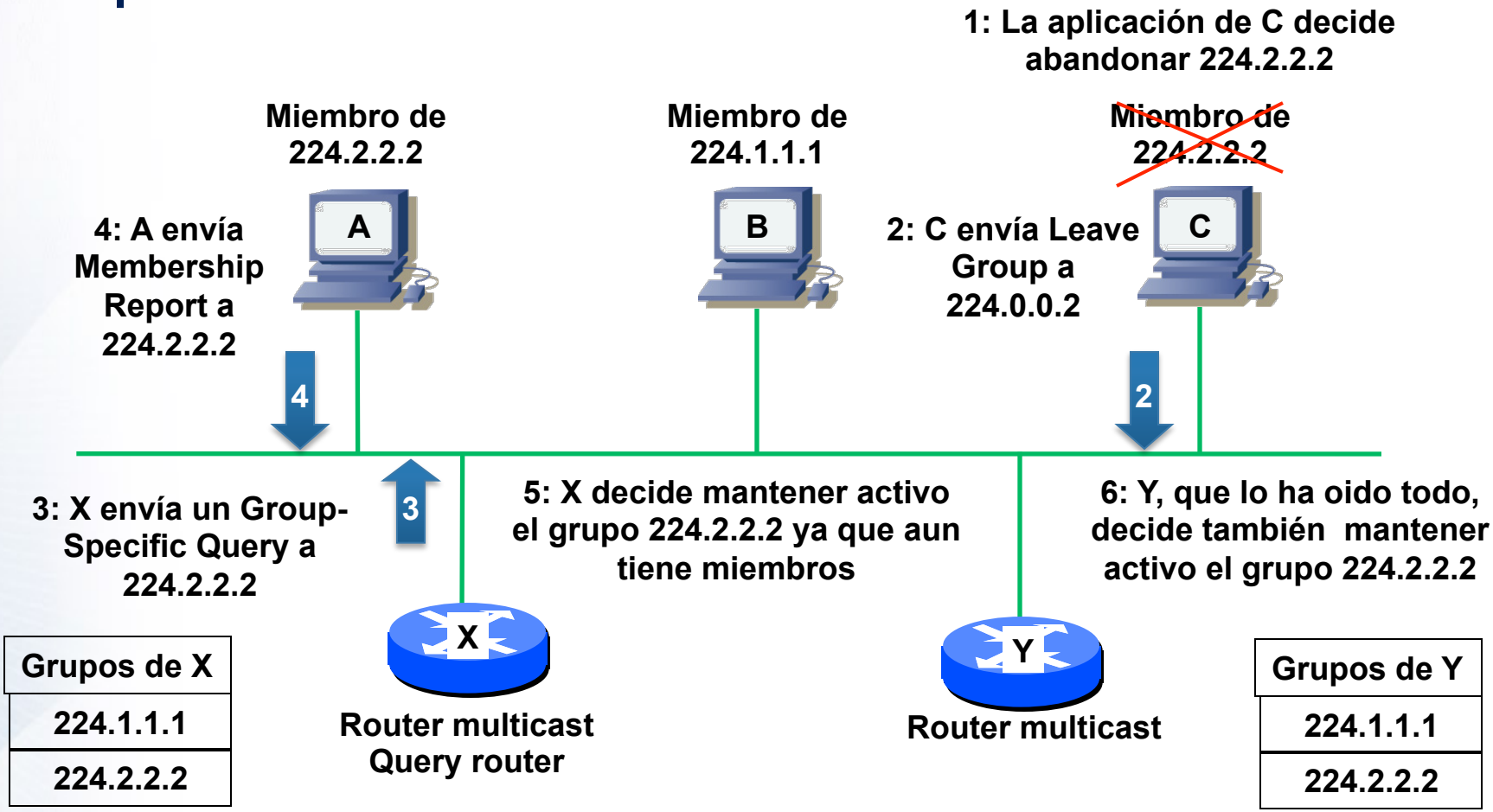
Mejoras introducidas por IGMPv2

- Hay un mensaje ‘Leave Group’ que permite a los hosts notificar al router de forma explícita cuando abandonan un grupo
- Existen dos tipos de Query:
  - Query General
  - Query específico de grupo
- La elección del Query router se realiza de forma independiente al protocolo de routing. Se elige el de dirección IP más baja.
- Los timeouts para la recepción de informes se pueden modificar dinámicamente y anunciarse en los mensajes IGMP de Query

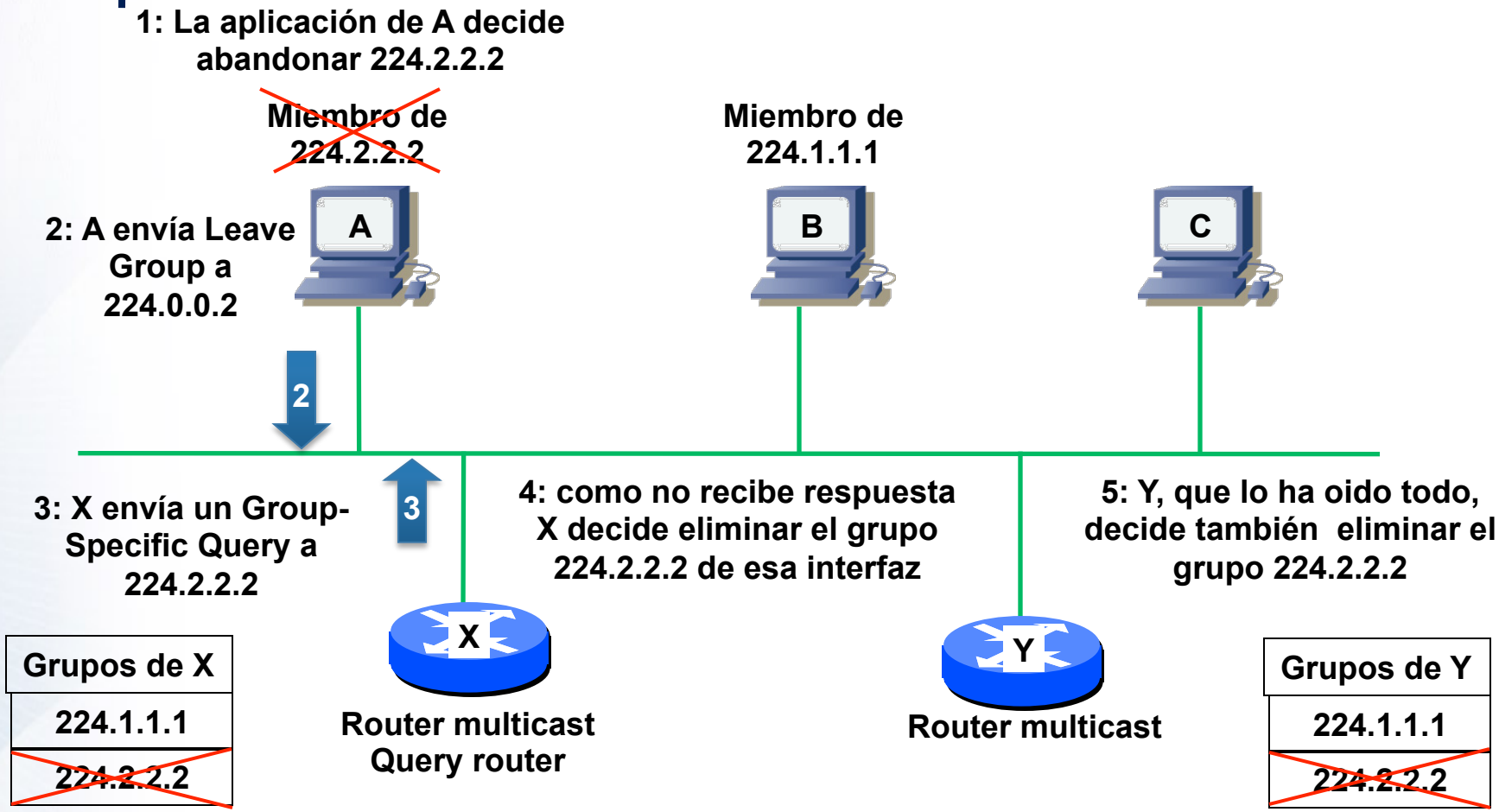
Tipos de mensajes en IGMPv2

	Tipo	Emitido por	Función	Dirección de destino
	Consulta General (General Query)	Routers	Preguntar a los hosts si están interesados en algún grupo multicast	224.0.0.1
Nuevo →	Consulta específica de grupo (Group-Specific Query)	Routers	Preguntar a los hosts si están interesados en un determinado grupo multicast	La del grupo en cuestión
	Informe de Pertenencia (Membership Report)	Hosts	Informar a los routers que el host está interesado en un determinado grupo multicast	La del grupo en cuestión
Nuevo →	Abandono de Grupo (Leave Group)	Hosts	Informar a los routers que el host deja de estar interesado en un grupo multicast	224.0.0.2

Proceso abandonar (leave) de IGMPv2 (I)



Proceso abandonar (leave) de IGMPv2 (II)



Compatibilidad IGMP v1-v2

- En general cuando en una red hay algún router o algún host que utiliza IGMP v1 todo el conjunto funciona como IGMP v1
- A menudo en estos casos los routers han de configurarse manualmente para que funcionen con IGMP v1 (para que sepan que no deben enviar los mensajes ‘Group Specific Query’)

Mejoras introducidas por IGMP v3

- La aportación de IGMPv3 es que la elección de los flujos multicast ya no se limita solo a la dirección de destino; también se puede especificar la dirección de origen
- Esto permite aislar a ‘saboteadores’ o ‘indeseables’. Evita que se puedan producir ataques de denegación de servicio en emisiones multicast.
- A la funcionalidad aportada por IGMPv3 se la denomina SSM, Source Specific Multicast.

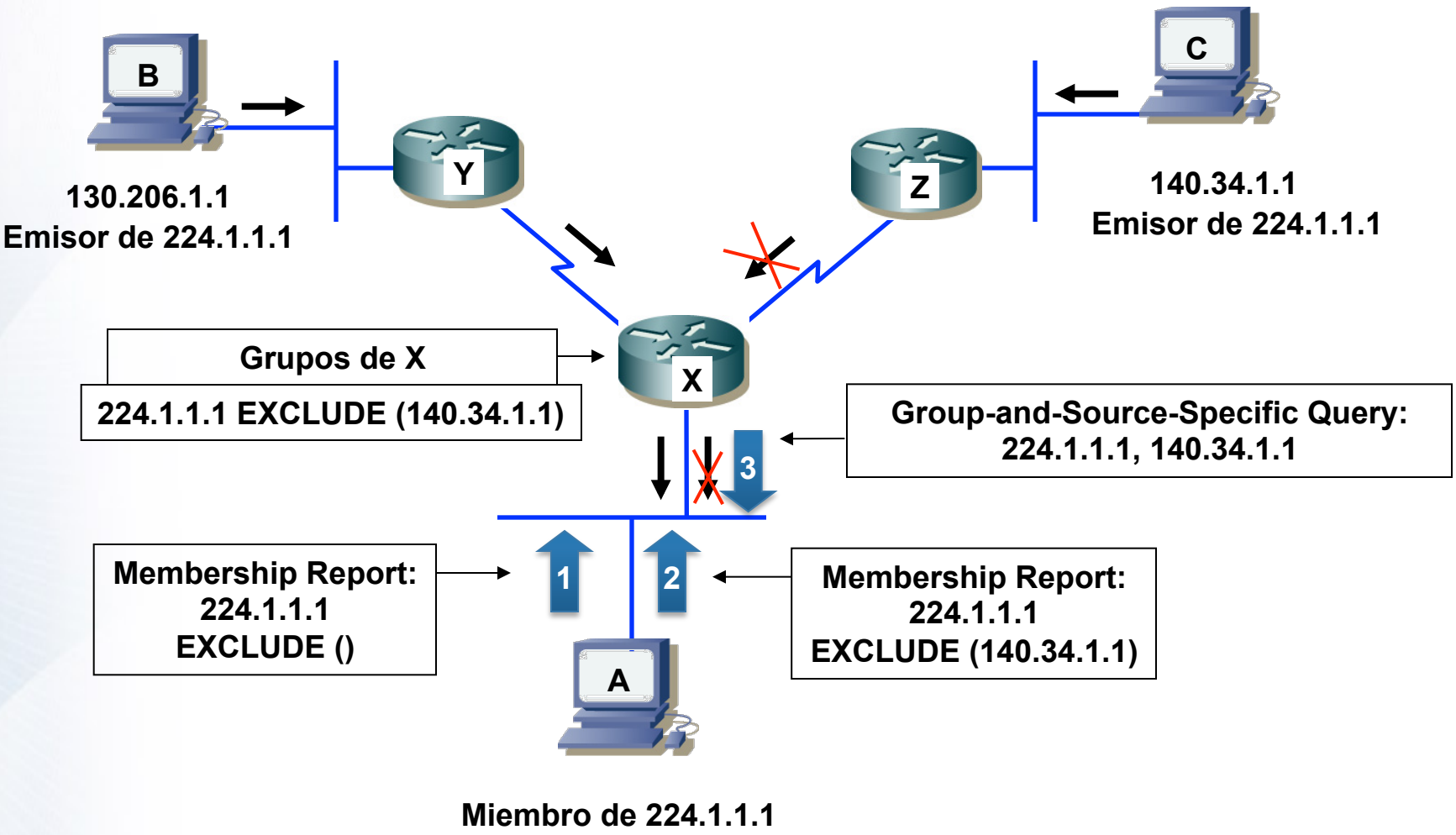
Mensajes nuevos de IGMP v3

- El Membership Report puede indicar una serie de fuentes a incluir, o a excluir, ej.:
  - Unirse (Join):
    ‘Membership Report 224.1.1.1 EXCLUDE ()’
  - Abandonar (Leave):
    ‘Membership Report 224.1.1.1 INCLUDE ()’
- El comando Query tiene ahora tres modalidades:
  - General Query (v1)
  - Group-Specific Query (v2)
  - Group-and-Source-Specific Query (v3)

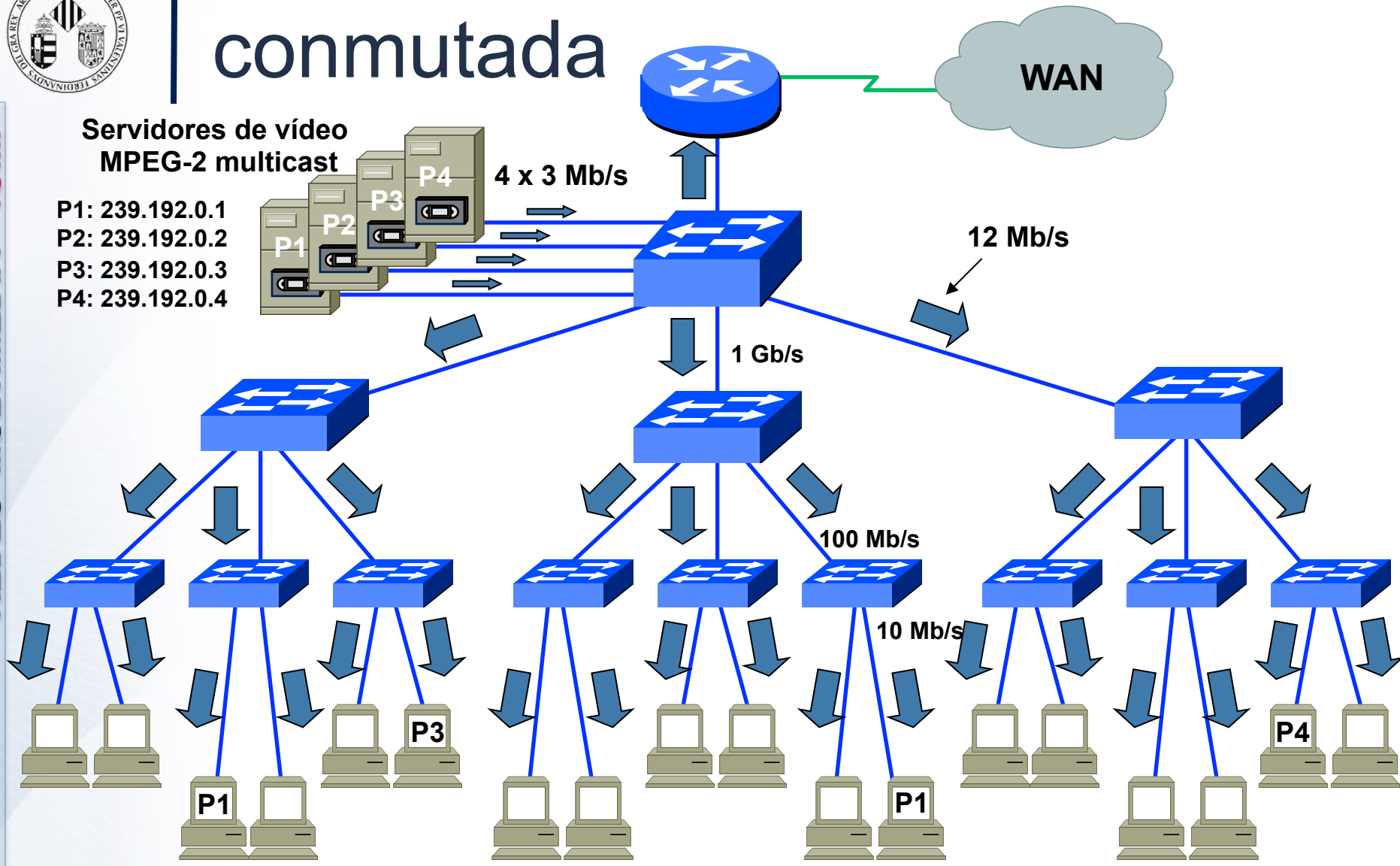
Tipos de mensajes en IGMPv3

	Tipo	Emitido por	Función	Dirección de destino
	Consulta General (General Query)	Routers	Preguntar a los hosts si están interesados en algún grupo multicast	224.0.0.1
	Consulta específica de grupo (Group-Specific Query)	Routers	Preguntar a los hosts si están interesados en un determinado grupo multicast	La del grupo en cuestión
Nuevo →	Consulta específica de grupo y fuente (Group-and-Source-Specific Query)	Routers	Preguntar a los hosts si están interesados en un determinado grupo multicast de una serie de fuentes determinada	La del grupo en cuestión
Modificado →	Informe de Pertenencia (Membership Report)	Hosts	Informar a los routers que el host está interesado en un determinado grupo multicast (indicando una serie de fuentes a incluir o a excluir)	224.0.0.22

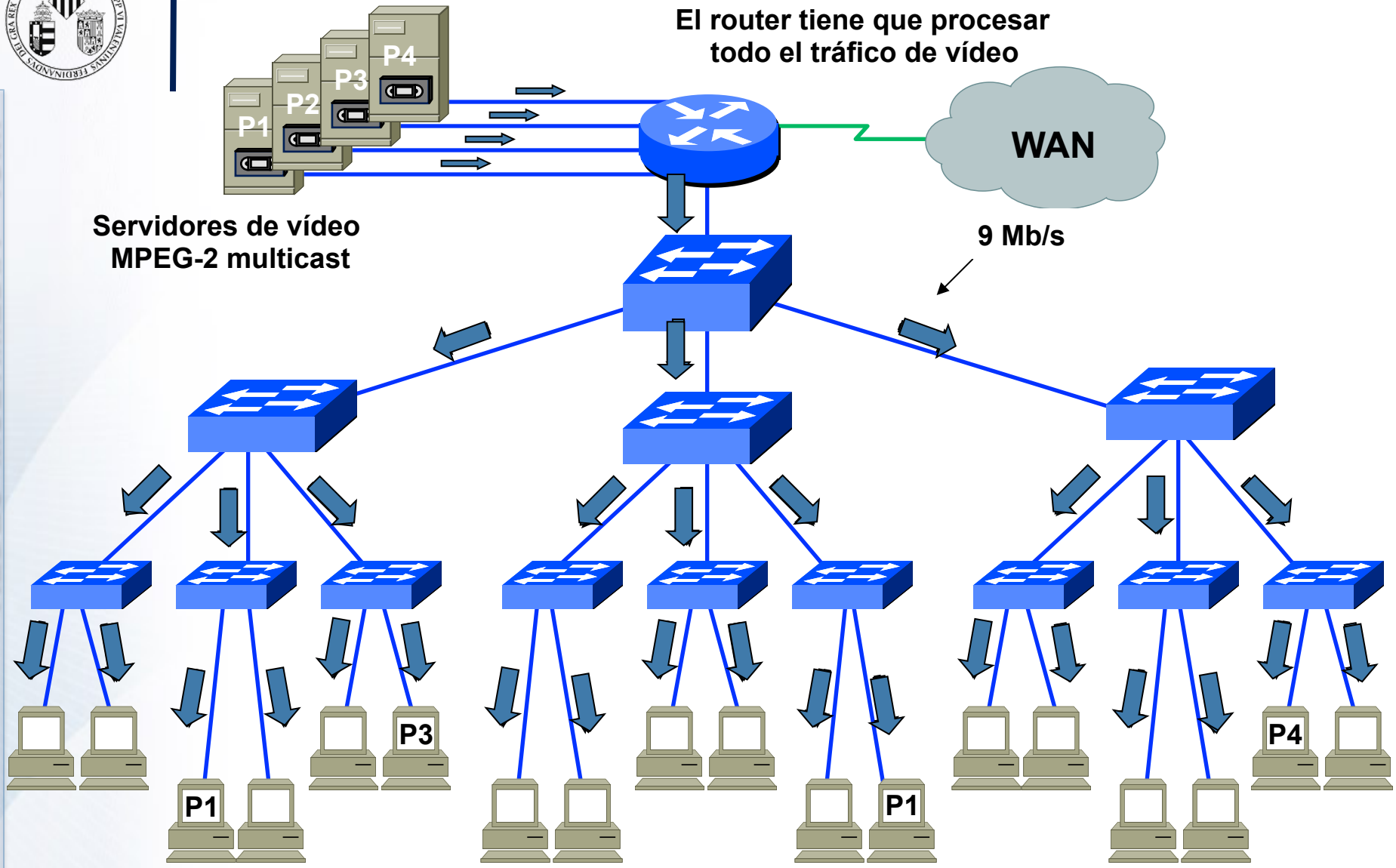
Suscripción 'selectiva' de IGMP v3



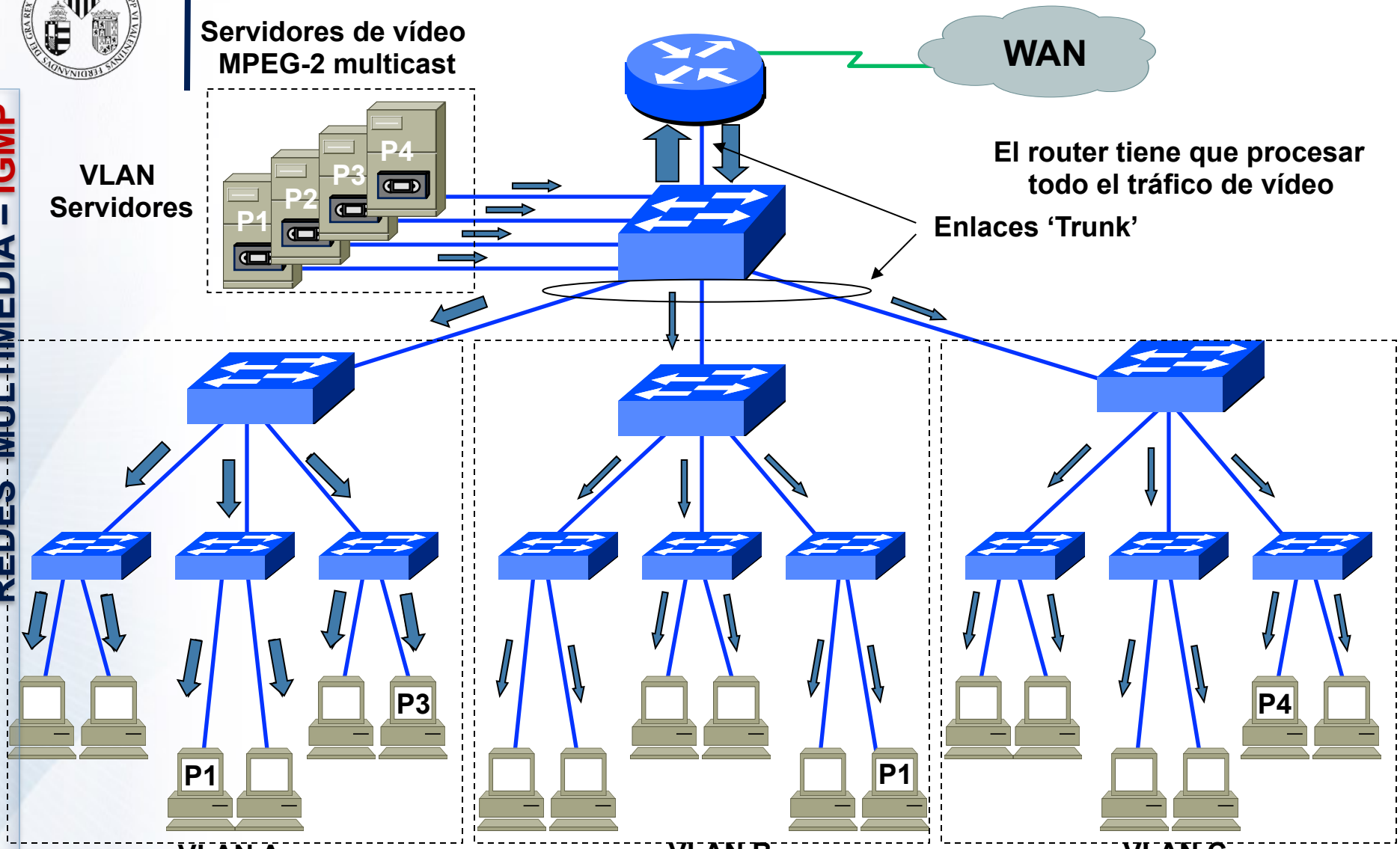
Multicast en una LAN conmutada



Multicast con router en medio



Multicast con VLANs



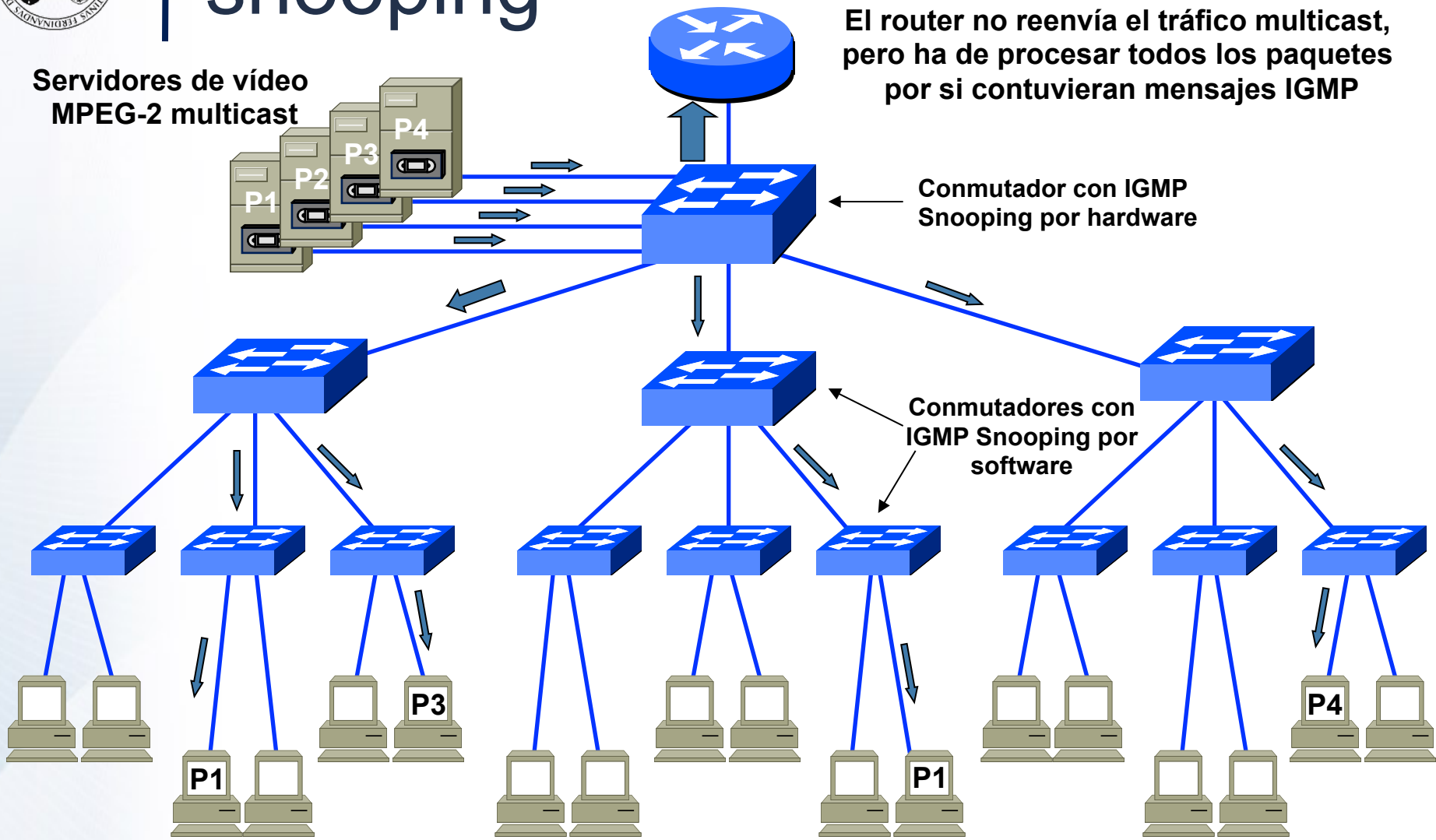
Multicast en LAN conmutada

- Cuando un host desea recibir un grupo multicast tiene que emitir un IGMP Membership Report
- Analizando los mensajes IGMP que pasan por él un conmutador podría saber por que puertos debe distribuir cada grupo multicast, y filtrar el tráfico innecesario
- Esto se conoce como 'IGMP snooping' (snooping = husmear)

IGMP Snooping

- Para realizar el IGMP snooping los conmutadores han de realizar el siguiente proceso:
  - Ver si se trata de una trama multicast
  - Ver si se trata de un paquete IP (por ejemplo campo Ethertype = x'0800)
  - Ver si se trata de un mensaje IGMP (valor 2 en el campo protocolo de la cabecera IP)
  - Una vez comprobado todo el conmutador ha de interpretar el mensaje IGMP y actuar en consecuencia
- Este proceso puede hacerse de dos formas:
  - Por hardware: se incorporan ASICs adicionales al conmutador para que no intervenga la CPU. Normalmente esto solo se hace en conmutadores de gama alta
  - Por software: la CPU realiza el IGMP snooping. Normalmente esto limita el rendimiento del equipo en tráfico multicast

Multicast en LAN con IGMP snooping



Supresión de informes con IGMP Snooping

- La supresión de informes permite que un host omita el envío del ‘Membership Report’ si otro ya lo ha enviado. Esto da al traste con el IGMP Snooping, los conmutadores ya no saben exactamente en que puertos están los receptores multicast
- Una solución es que los conmutadores propaguen los ‘Membership Report’ solo por los puertos por donde recibieron los ‘Membership Query’ (que es donde está el router que preguntó)

Supresión de informes con IGMP Snooping

- Pero los 'Membership Report' también se han de enviar a los demás routers, aunque no hayan lanzado la pregunta. Los conmutadores pueden 'descubrir' a los routers por algunos mensajes característicos, o se puede indicar en la configuración del conmutador
- Todo esto complica el funcionamiento de IGMP Snooping.
- En IGMP v3 los 'Membership Report' se envían a la dirección 224.0.0.22, que solo es recibida por los routers IGMP v.3 y no por los hosts. Por tanto en IGMPv3 no existe la supresión de informes, lo cual simplifica el IGMP Snooping