

# IP multicast

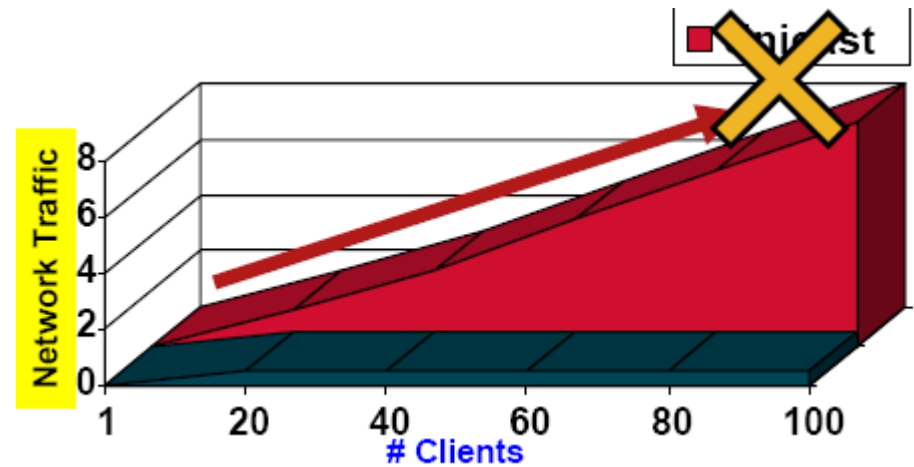
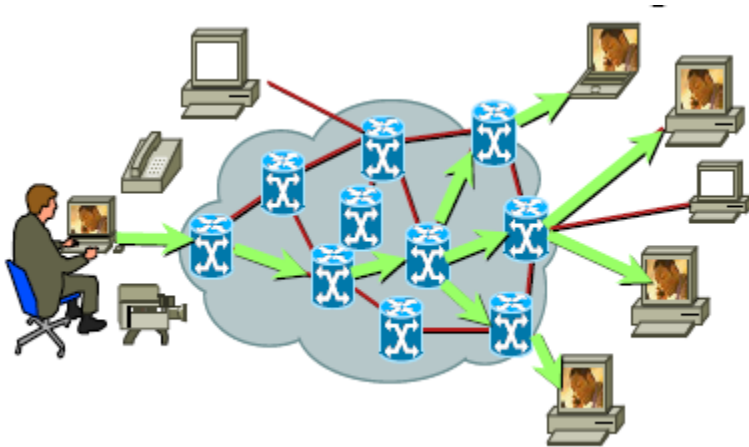
Hyogon Kim  
Korea University

# Agenda

- Introduction
  - Background
  - DVMRP, PIM-DM, PIM-SM
  - RPF
- IP Multicast Services
  - ASM vs. SSM
- IP Multicast Protocols
  - IGMP v1, 2, 3
  - PIM-SM/SSM
- Application to IPTV

# Multicast benefits

- Makes multipoint applications possible
- Reduces server loads in CPU and bandwidth
- Eliminates traffic redundancy in the network
- It's a **GREEN IT**
  - C.f.: It requires 838 pounds of coal to power 1 PC for one year



출처:

Cisco의 NANOG 발표 자료

"[http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride\\_ip\\_tv\\_N44.pdf](http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride_ip_tv_N44.pdf)"

# Multicast uses

- Live video distribution
  - Seminars, conferences, workshops, e-learning ....
- Collaborative groupware
- Periodic data delivery – “push” technology
  - Stock quotes, sports scores, magazines, newspapers, advertisements
- Resource discovery
- Etc. etc. etc.

# Start of history

- In 1995 the first multicast network was born: MBone
- **DVMRP** (Distance Vector Multicast Routing Protocol) was the protocol used
  - DVMRP subnetworks was interconnected through the unicast Internet infrastructure with **tunnels**
  - **Flood-and-prune (or, Reverse Path Multicast; RPM)** technology
    - **Using RPF check**
  - Very successful in academic circles (MBone)
  - Used IGMP, packet Type=0x13

# DVMRP issues

- DVMRP relies on RIP and carries over many of RIP's issues
  - Hop count used as metric, poisoned reverse
- Scalability issues
  - Each source performs periodic flooding to receivers widely dispersed across Internet
  - Maintains its own routing table – substantial routing traffic
- Mbone is being phased out
- In 1997, Protocol Independent Multicast (PIM) was developed
  - Uses unicast routing information, **but does not depend on particular unicast routing protocol**
    - C.f. DVMRP on RIP, MOSPF on OSPF
  - Focus is on Sparse Mode

# Evolution

- PIM Dense Mode (**PIM-DM**)
  - Similar to DVMRP, but not dependent on any single unicast routing protocol
  - For topologies where receivers are densely populated
  - **Does not have separate routing table** for RPF check
  - Not really recommended

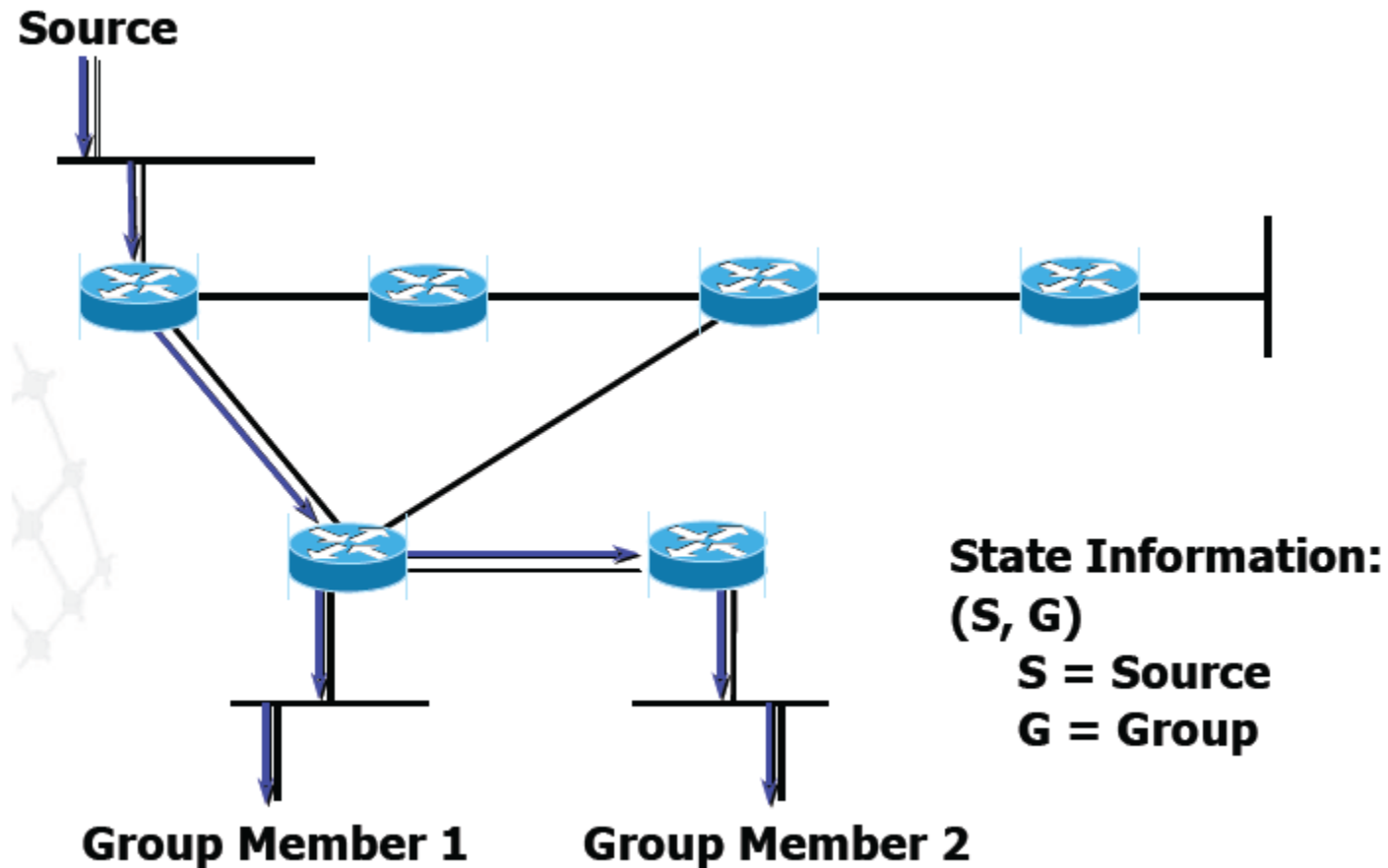
# Multicast distribution trees

- Source or Shortest Path Trees (SPT)
  - More resource intensive; requires more states:  $O(SG)$
  - You get optimal paths from source to all receivers, minimizes delay
  - Best for one-to-many distribution
- Shared or Core Based Trees
  - Uses less resources; less memory:  $O(G)$
  - You may get suboptimal paths from source to all receivers, depending on topology
  - The RP (core) itself and its location may affect performance
  - Best for many-to-many distribution
  - May be necessary for source discovery (PIM-SM)



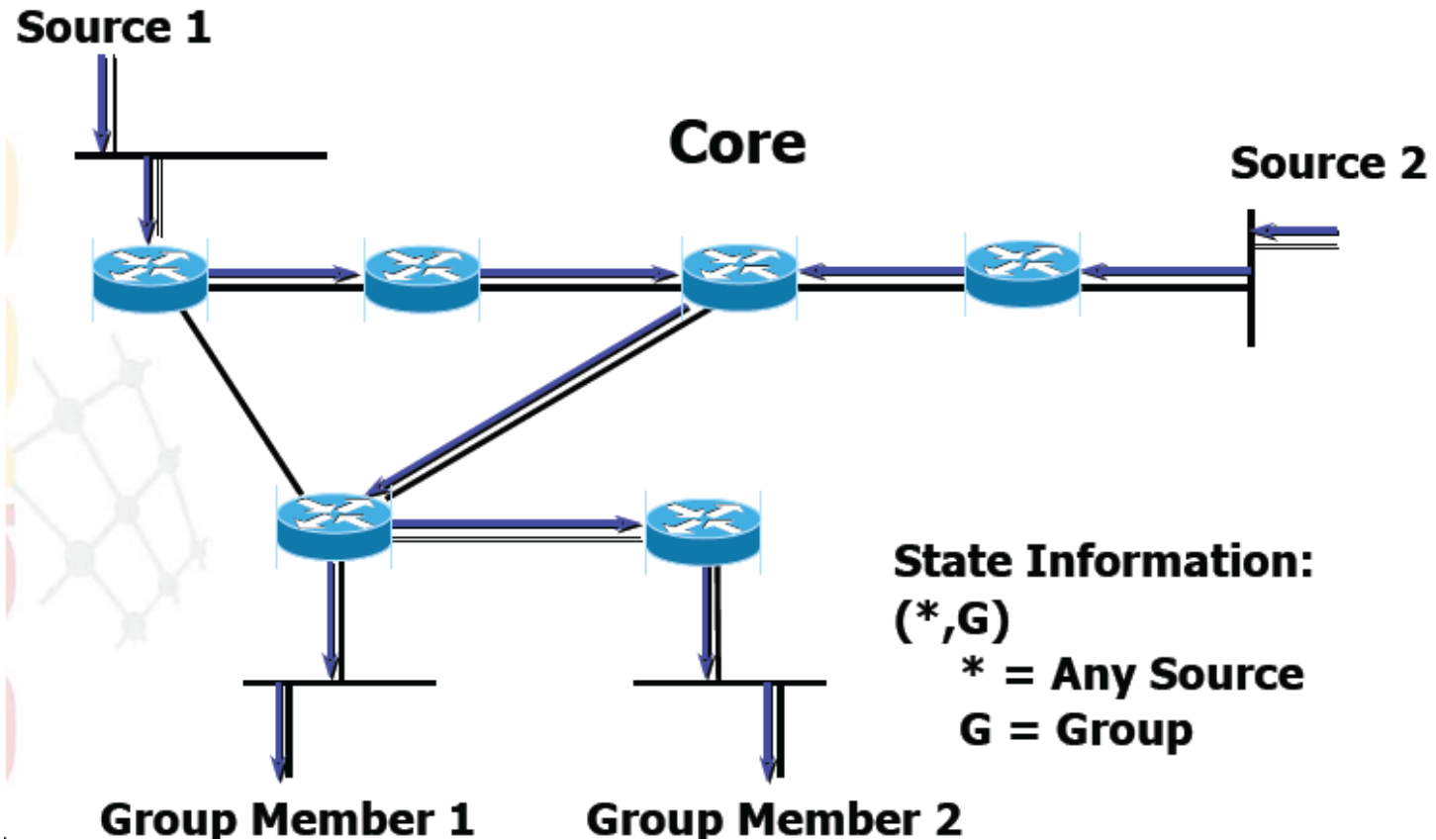
# Multicast distribution trees

- Source Tree or Shortest Path Tree (SPT)
  - Actually, it is **reverse** SPT



# Multicast distribution trees

- Shared Tree

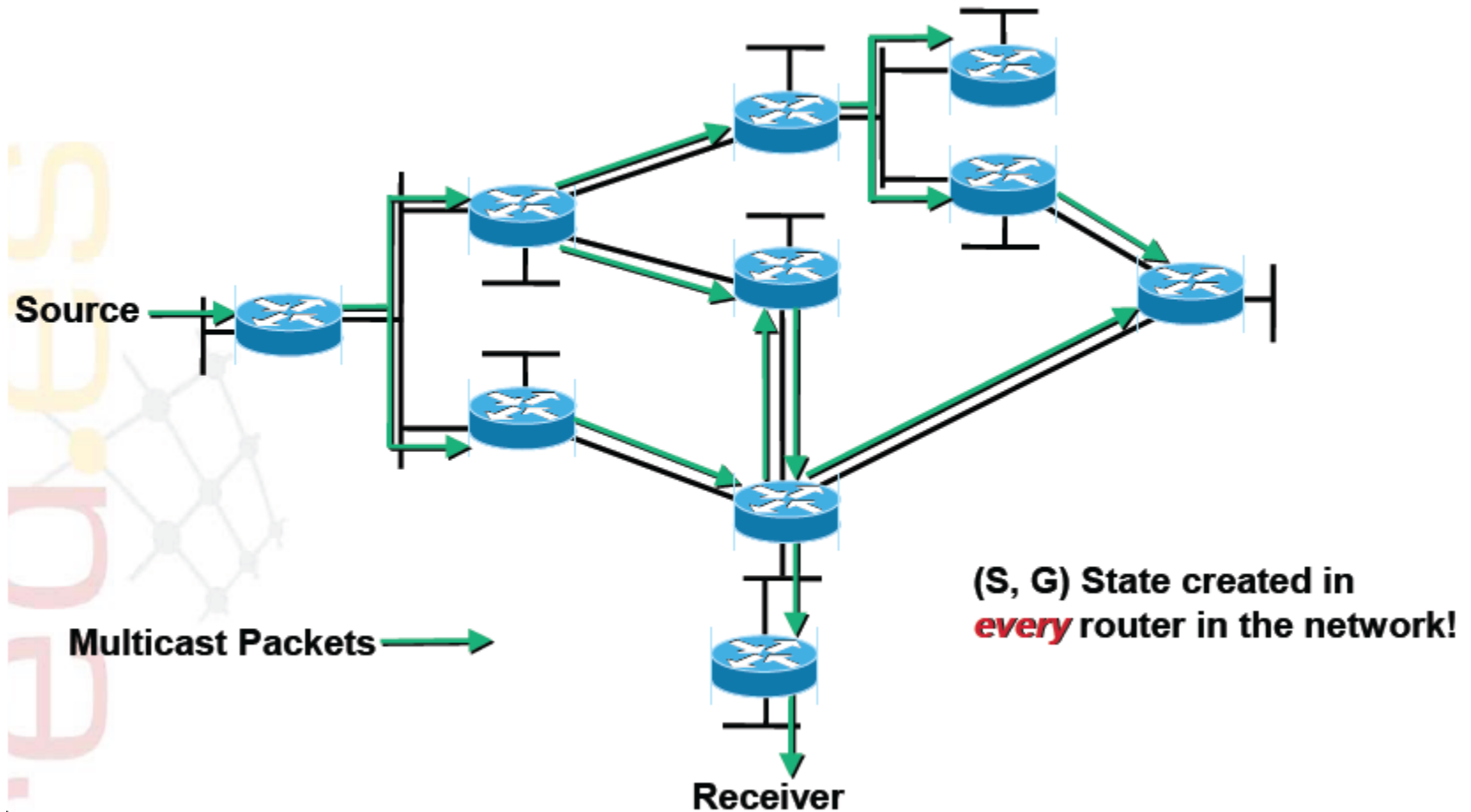


출처: Cisco의 NANOG 발표 자료

"[www.garr.it/eventiGARR/.../doc/sotos\\_rediris\\_mcast\\_eumedconnect.ppt?](http://www.garr.it/eventiGARR/.../doc/sotos_rediris_mcast_eumedconnect.ppt?)"

# PIM-DM overview

- Initial flooding

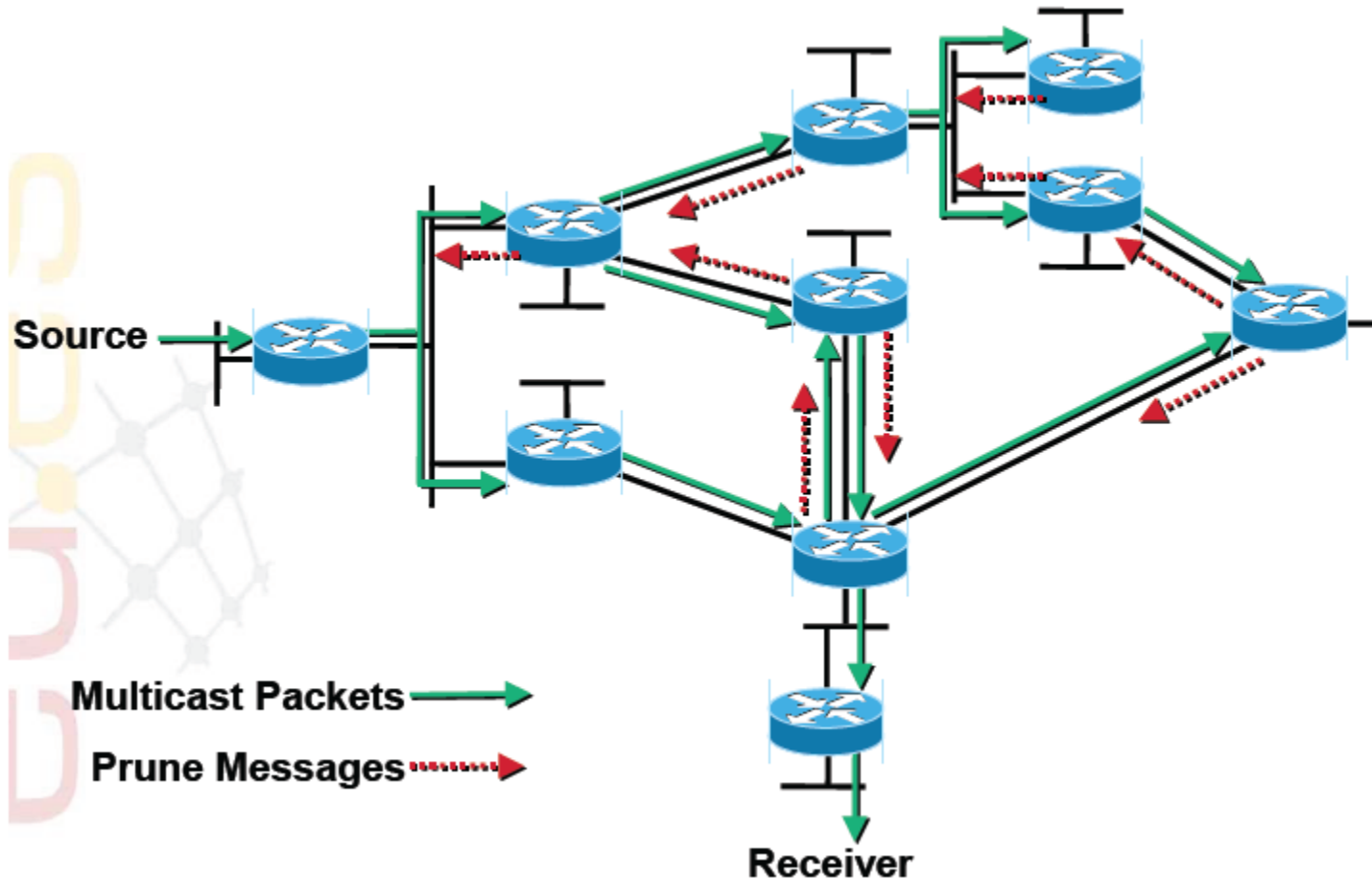


출처: Cisco의 NANOG 발표 자료

"[www.garr.it/eventiGARR/.../doc/sotos\\_rediris\\_mcast\\_eumedconnect.ppt?](http://www.garr.it/eventiGARR/.../doc/sotos_rediris_mcast_eumedconnect.ppt?)"

# PIM-DM overview

- Pruning unwanted traffic

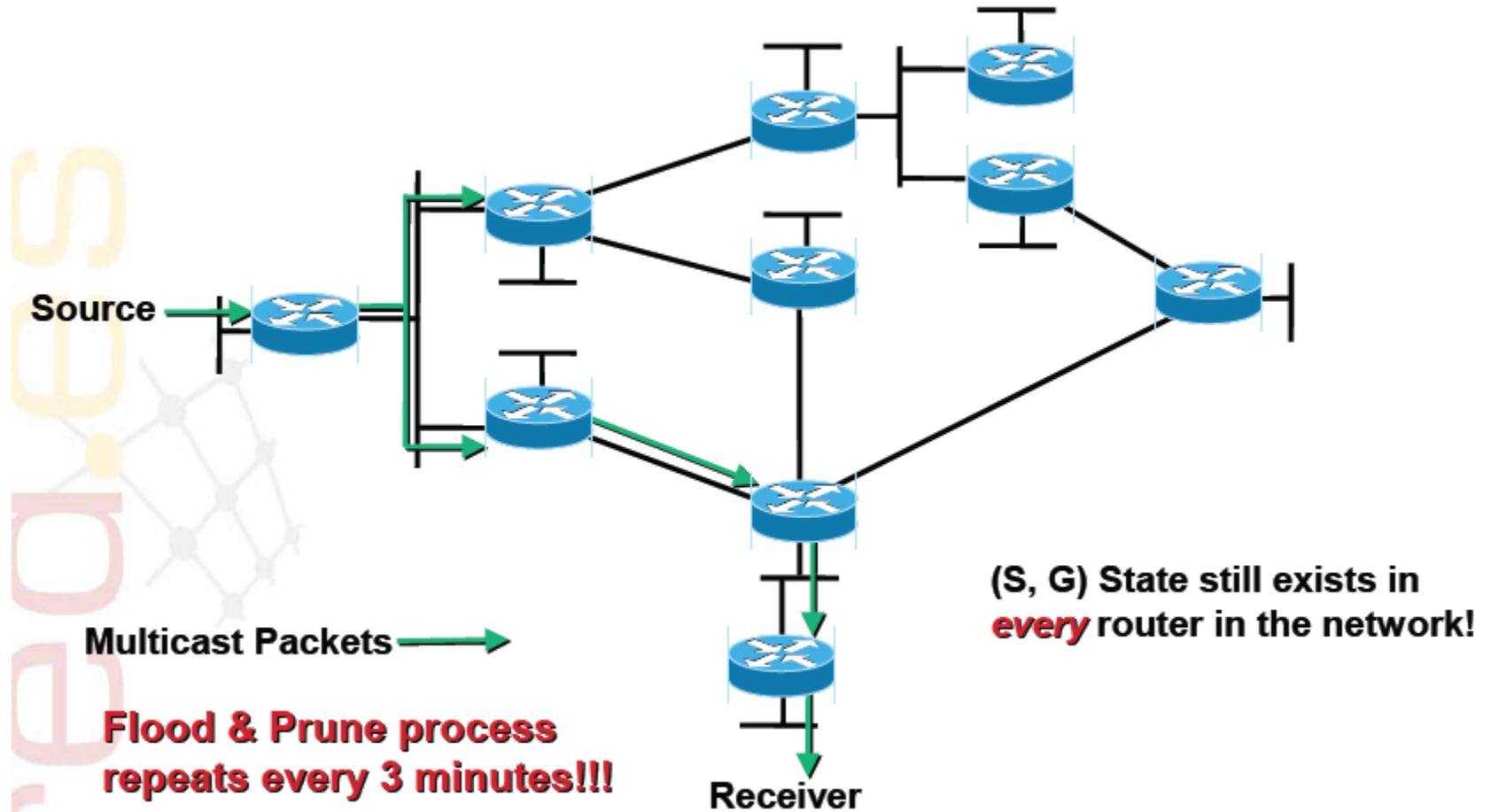


출처: Cisco의 NANOG 발표 자료

"[www.garr.it/eventiGARR/.../doc/sotos\\_rediris\\_mcast\\_eumedconnect.ppt?](http://www.garr.it/eventiGARR/.../doc/sotos_rediris_mcast_eumedconnect.ppt?)"

# PIM-DM overview

- Results after pruning



# PIM-DM problems

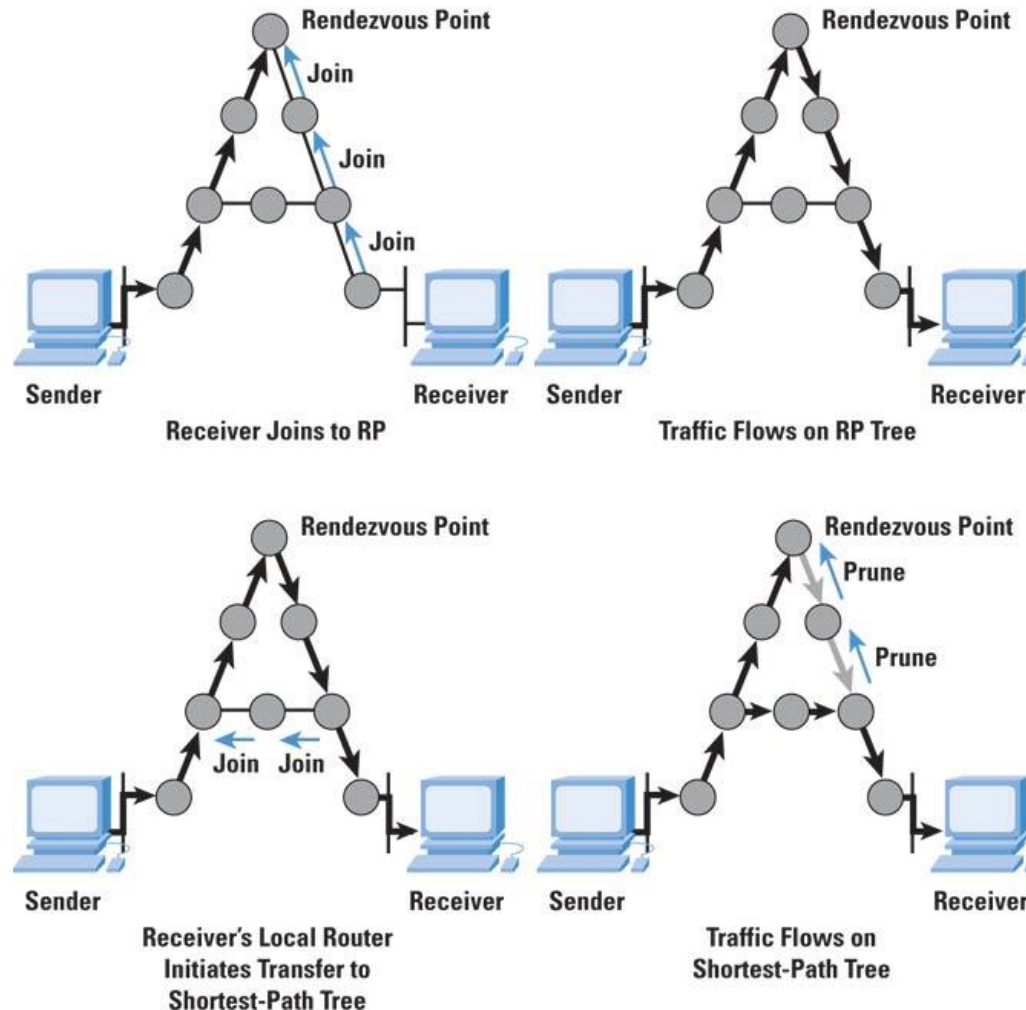
- Flood-and-prune behavior very inefficient
  - Like DVMRP
- Creates (S, G) state in every router
  - Even when there are no receivers for the traffic
    - Called the prune states
  - Like DVMRP
- No support for shared trees
  - Like DVMRP
- Complex assert mechanism
  - To determine which router in a LAN will forward the traffic

# Evolution

- PIM Sparse mode (**PIM-SM**)
  - Must configure a **Rendezvous Point (RP)**
    - Statically (on every Router)
    - Using Auto-RP or BSR (Routers learn RP automatically)
    - PIM-SM redistributes a list of candidates to be RPs to all routers
  - RP is the root of the **shared tree**
    - Each group maps to a RP
    - Senders “register” with RP
    - Receivers join towards the RP
  - Can still use source tree in addition to shared tree
    - Transition to source tree possible after shared tree formation
    - Performance becomes less dependent on RP location
  - Very efficient due to **explicit join** model
    - Traffic only flows to where it’s needed
    - Router state only created along flow paths
  - Scales better than dense mode
    - But still best be used intra-domain: RPs will be overloaded otherwise

# Transition from shared tree to source tree

- By Source-specific join + Prune towards RP

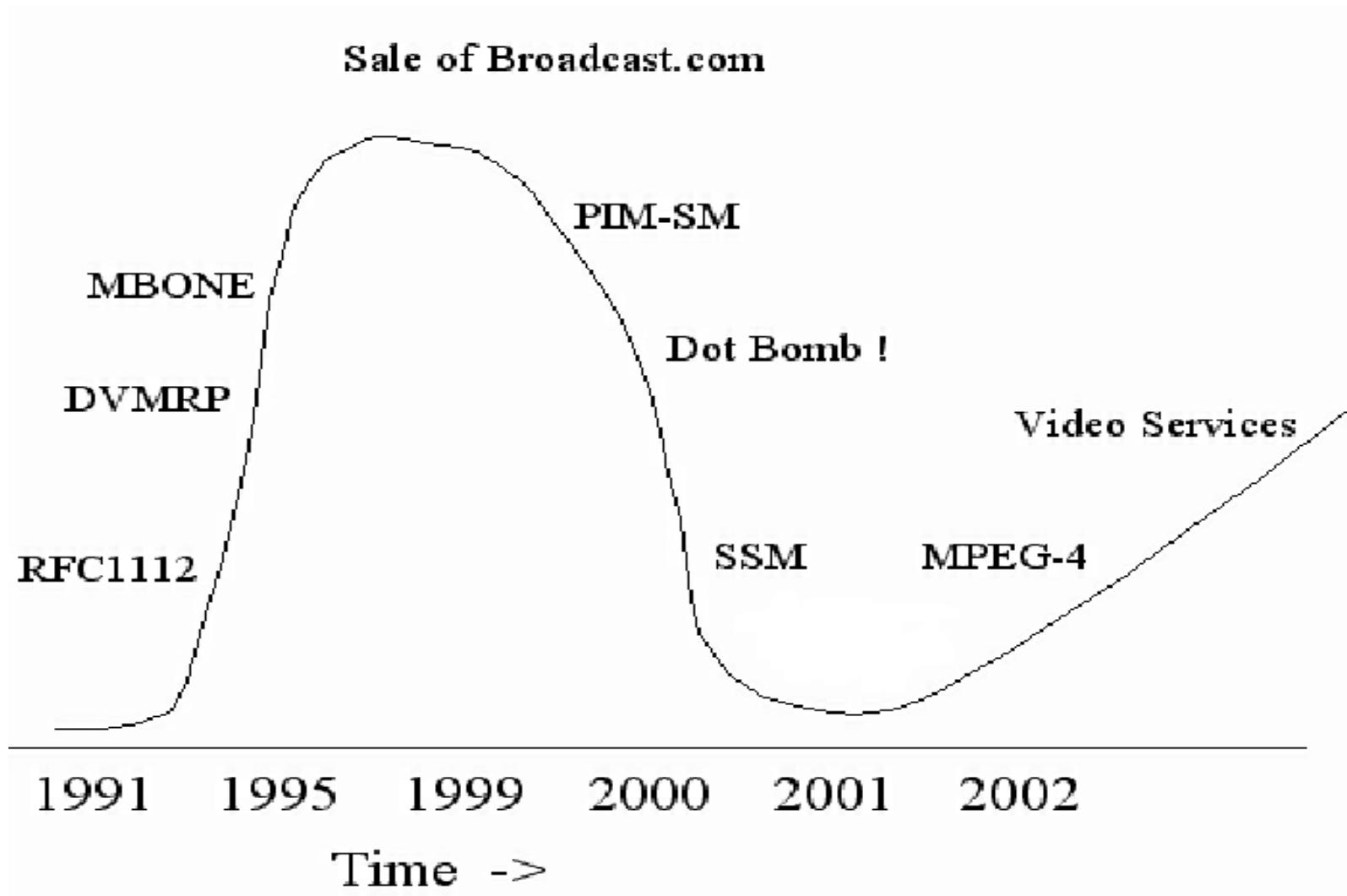




# Evolution

- **Interdomain** use of the above protocols has scalability problems of one kind or another
  - DVMRP, PIM-DM
    - Initially send data everywhere
    - Require routers to hold prune state to prevent this flooding from persisting
  - MOSPF
    - Requires all routers to know where all receivers are
  - PIM-SM
    - Needs redistribution of information about the set of RPs.
    - An RP cannot handle too many groups simultaneously, so many RPs are needed globally
- **Multiprotocol BGP (MBGP)** and **Multicast Source Discovery Protocol (MSDP)** can be used
  - MBGP helps detouring around network parts that do not support multicast
  - MSDP to glue PIM-SM domains together

# Adoption of multicast technology



출처:

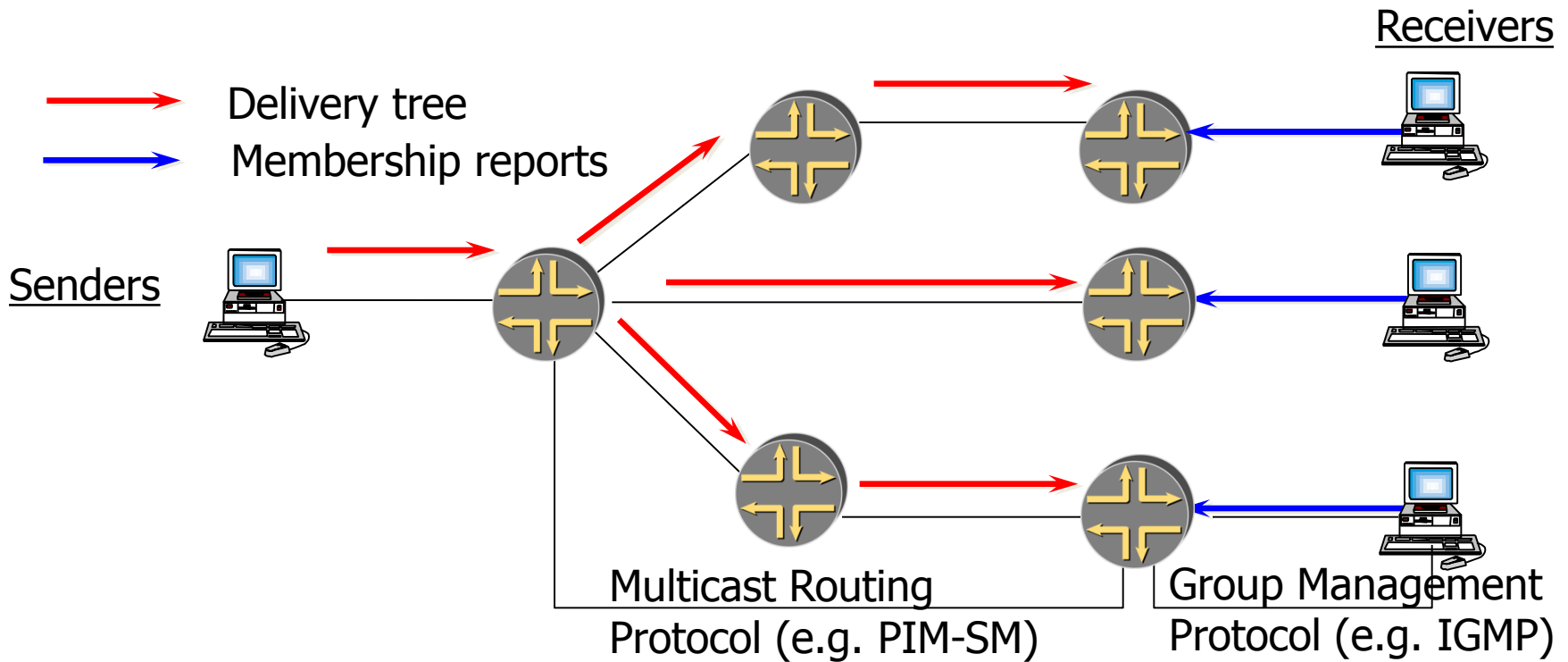
Internet2 Engineering workshop

"<http://people.inf.elte.hu/toke/halozatokII-jegyzet/el%C5%91ad%C3%A1sok/Multicast/ajanlott/I2multicast.pdf>"

# IP multicast building blocks

- The **senders** send to
  - Multicast addresses (RFC1700)
    - Class D (224.0.0.0 - 239.255.255.255)
- The **receivers** inform the routers what they want to receive
  - **Internet Group Management Protocol (IGMP)**
    - RFC2236: version 2
    - RFC3376: version 3
- The **multicast routers** make sure the streams make it to the correct receiving nets
  - Multicast routing protocols (*e.g.* PIM)
  - RPF

# IP multicast building blocks



출처:

Internet2 Engineering workshop

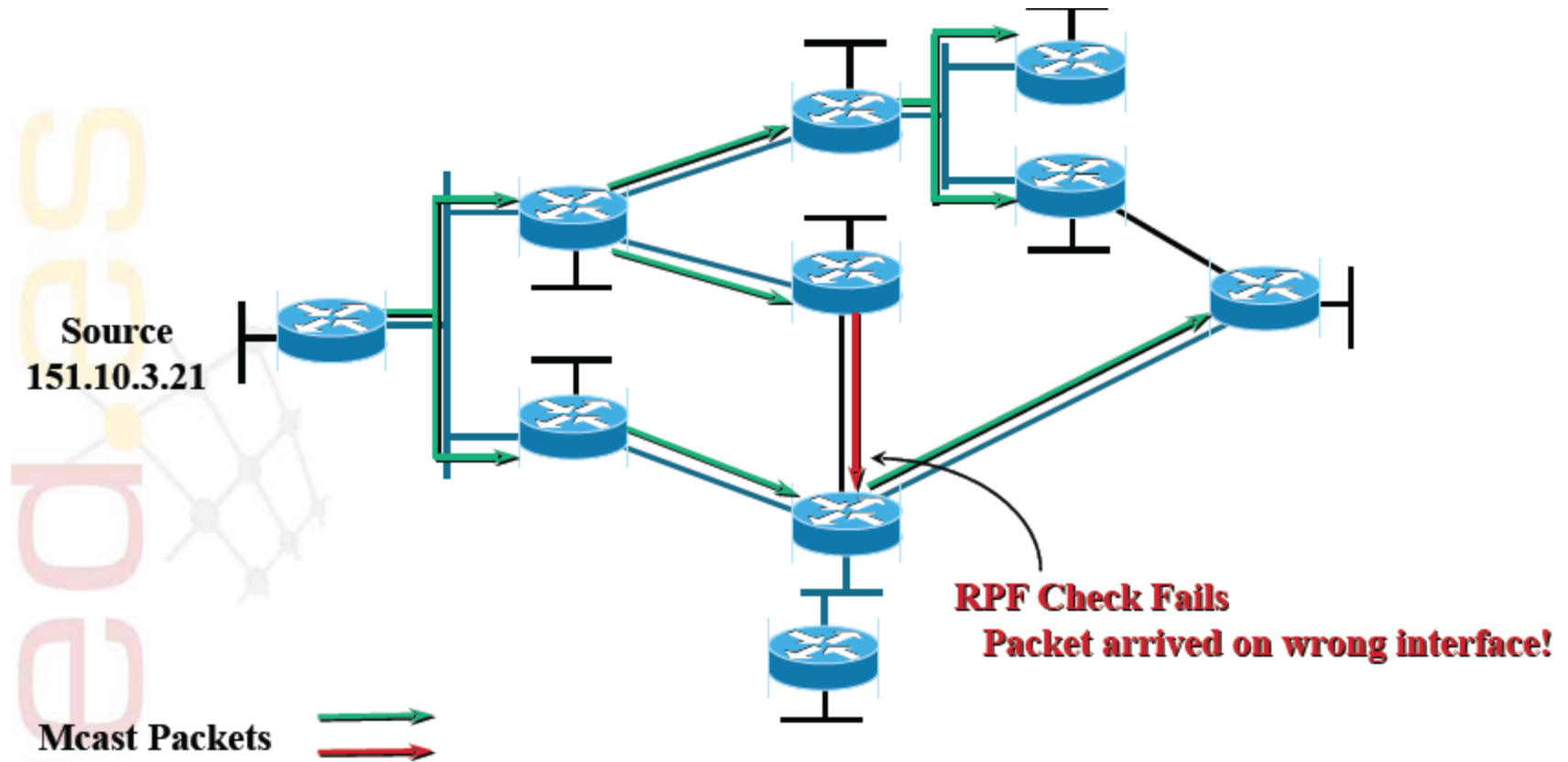
"<http://people.inf.elte.hu/toke/halozatokII-jegyzet/el%C5%91ad%C3%A1sok/Multicast/ajanlott/I2multicast.pdf>"

# Reverse Path Forwarding (RPF)

- What is RPF?
  - A router forwards a multicast datagram only if received on the upstream interface to the source (*i.e.*, it follows the distribution tree)
    - Kind of backwards from unicast routing
- Why RPF?
  - Loop prevention
- The RPF check
  - The source IP address of incoming multicast packets are checked against a unicast routing table
  - If the datagram arrived on the **interface** specified in the routing table for the source address; then the RPF check succeeds
  - Otherwise, the RPF check fails : refuse the packet
- If multicast path is different from unicast path, then a multicast table will exist
  - It will be used for RPF check

# Multicast forwarding

- Example: RPF check



출처: Cisco의 NANOG 발표 자료

"[www.garr.it/eventiGARR/.../doc/sotos\\_rediris\\_mcast\\_eumedconnect.ppt?](http://www.garr.it/eventiGARR/.../doc/sotos_rediris_mcast_eumedconnect.ppt?)"

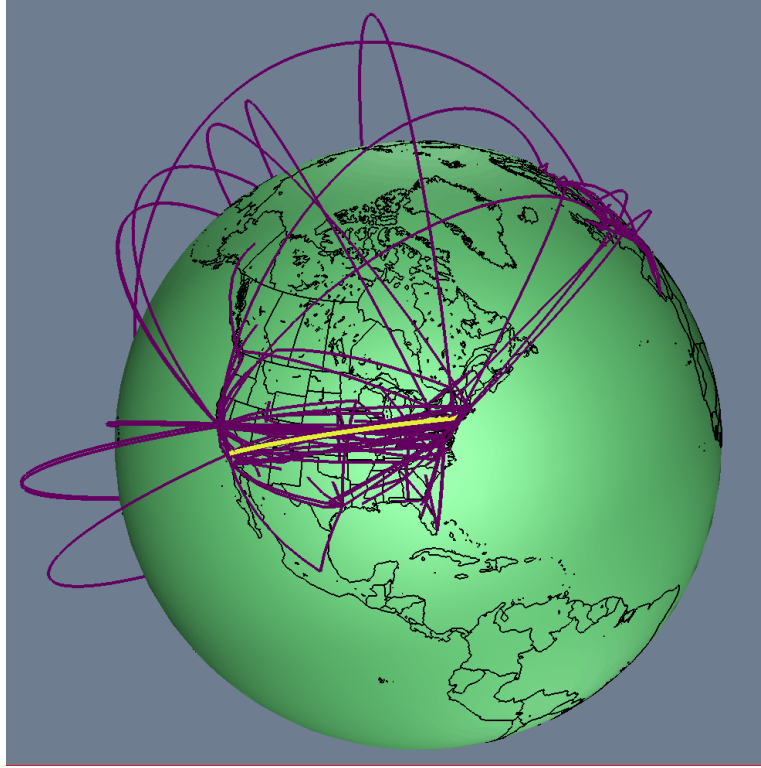
# Forwarding process

1. Check administrative scope
  - Two types of scoping: administrative and TTL
    - TTL scoping is more popular, but awkward in some situations
    - Administrative scoped group addresses: 239/8 (like RFC1918 unicast private addresses)
    - E.g. Site-local 239.253.0.0/16, organizatio-local 239.192.0.0/14
  - Facilitates group address reuse
2. Check RPF (to source)
  - Check RPF to RP if SM
3. Check output interface list (OIL) number
4. Adjust TTL; check against TTL threshold
  - TTL 0 : node-local
  - TTL 1 : link-local
  - TTL < 32 : site-local
  - TTL < 64 : region-local
  - TTL < 128 : continent-local
  - TTL < 256 : global-local
5. Replicate using OIL

# IP Multicast Standards

- RFC 1112, *Host Extensions for IP Multicasting* (defines IGMP Version 1)
- RFC 2236, *Internet Group Management Protocol, Version 2*
- RFC 2327, *SDP: Session Description Protocol*
- RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*
- RFC 2365, *Administratively Scoped IP Multicast*
- RFC 2547, *BGP/MPLS VPNs*
- RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 3376, *Internet Group Management Protocol, Version 3* (SSM include mode only)
- *Anycast Rendezvous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*, Internet draft draft-ietf-mboned-anycast-rp-08.txt
- *Bootstrap Router (BSR) Mechanism for PIM Sparse Mode*, Internet draft draft-ietf-pim-sm-bsr-03.txt
- *Distance Vector Multicast Routing Protocol*, Internet draft draft-ietf-idmr-dvmrp-v3-10.txt
- *Multicast in MPLS/BGP VPNs*, Internet draft draft-rosen-vpn-mcast-05.txt
- *Multicast Source Discovery Protocol (MSDP)*, Internet draft draft-ietf-msdp-spec-13.txt
- *Protocol Independent Multicast—Sparse Mode (PIM-SM): Protocol Specification (Revised)*, Internet draft draft-ietf-pim-sm-v2-new-06.txt
- *Protocol Independent Multicast Version 2 Dense Mode Specification*, Internet draft draft-ietf-pim-dm-new-v2-03.txt
- *SAP: Session Announcement Protocol*, Internet draft draft-ietf-mmusic-sap-00.txt
- *Source Address Selection for Multicast Listener Discovery Protocol*, Internet draft draft-ietf-magma-ml-d-source-05.txt (SSM include mode only)
- *An Overview of Source-Specific Multicast (SSM) Deployment*, Internet draft draft-ietf-ssm-overview-02.txt
- *Source-Specific Multicast for IP*, Internet draft draft-holbrook-ssm-arch-02.txt
- *Source-Specific Protocol Independent Multicast in 232/8*, Internet draft draft-ietf-mboned-ssm232-02.txt
- *Using IGMPv3 and MLDv2 for Source-Specific Multicast*, Internet draft draft-holbrook-idmr-igmpv3-ssm-04.txt





# MULTICAST SERVICES

# Protocols and services

- Multicast/multipoint protocols
  - Between routers, switches, ...
  - Of interest to network operator
  - PIM-SM, MSDP, (M)BGP, AutoRP, BSR, mLDP, RSVP-TE, ...
- Multicast services
  - How end-devices can use IP multicast
  - Of interest to network and service operator
  - ASM, SSM (and protocols IGMP/MLD)

# IP multicast services

- Any Source Multicast (ASM)
  - Since 1990, RFC1112
  - Sources send packets to multicast groups
  - Receivers join groups, receive from any source
- Source Specific Multicast (SSM)
  - Since 2000, RFC4607
  - Sources send packets to multicast groups (no change)
  - Receivers subscribe (S, G) channels, receive only traffic from S to G
  - Primarily introduced by IETF for IPTV type services because of limitations of standard protocol model for ASM
  - DoS attack is difficult (spoofing both S and G)
  - Unwanted broadcast traffic can be blocked
  - There should be out-of-band mechanism for receivers to find S, though

# Standard protocol model for ASM

- Historic
  - Mbone and DVMRP (up to 1994)
- Native multicast with PIM-SM (up to 2000)
  - AutoRP, BSR or MSDP/Anycast-RP redundancy
  - MSDP for interdomain support
  - Multiprotocol BGP for interdomain RPF selection
  - Best available general purpose ASM protocol suite (but with issues)

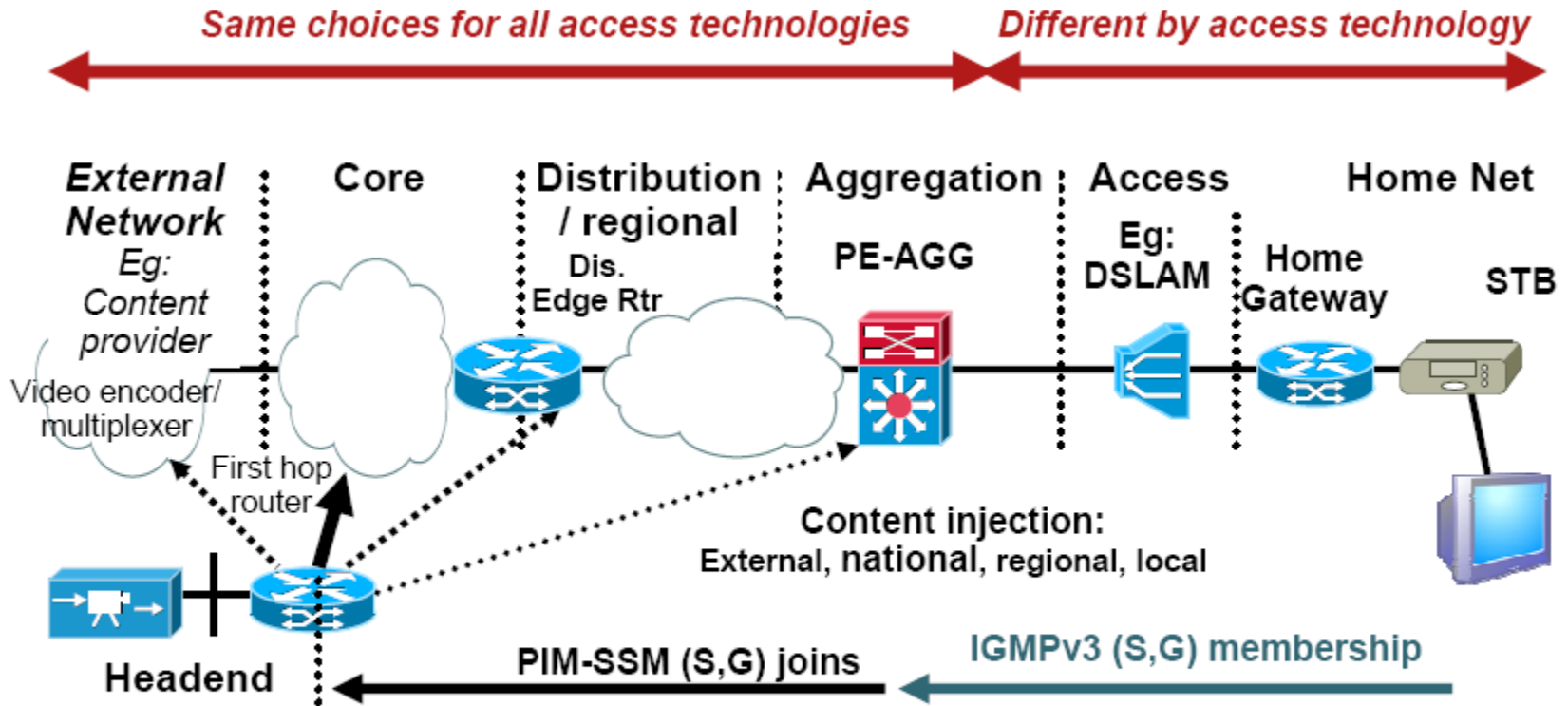
# Issues with ASM

- ASM issues
  - Traffic from unwanted sources
  - Address allocation (IPv4 only, not IPv6)
    - One group address, one channel
- Standard protocol suite
  - Complexity of protocol operations required
    - PIM-SM (RPT + SPT + Switchover), RP mapping (all routers), RP redundancy, MSDP (RPF), MBGP, interactions with MPLS cores, bandwidth reservation, protection
  - Scalability, speed of protocol operations (convergence)
    - RPT + SPT operations needed

# Standard protocol model for SSM

- IETF
  - Receiver host to router (*e.g.*: IP-STB)
    - IGMPv3(IPv4) / MLDv2(IPv6) with (S,G) signaling
    - Must be supported in host stack
  - Between routers
    - PIM-SSM: subset of PIM-SM for SSM
    - IGMPv3 proxy routing / (snooping) on HAG, L2 access
    - Simple point to multipoint tree building: (S,G) SPTs only
- Misc.
  - Anycast/Prioritycast source addresses for source redundancy

# End-to-end protocol view



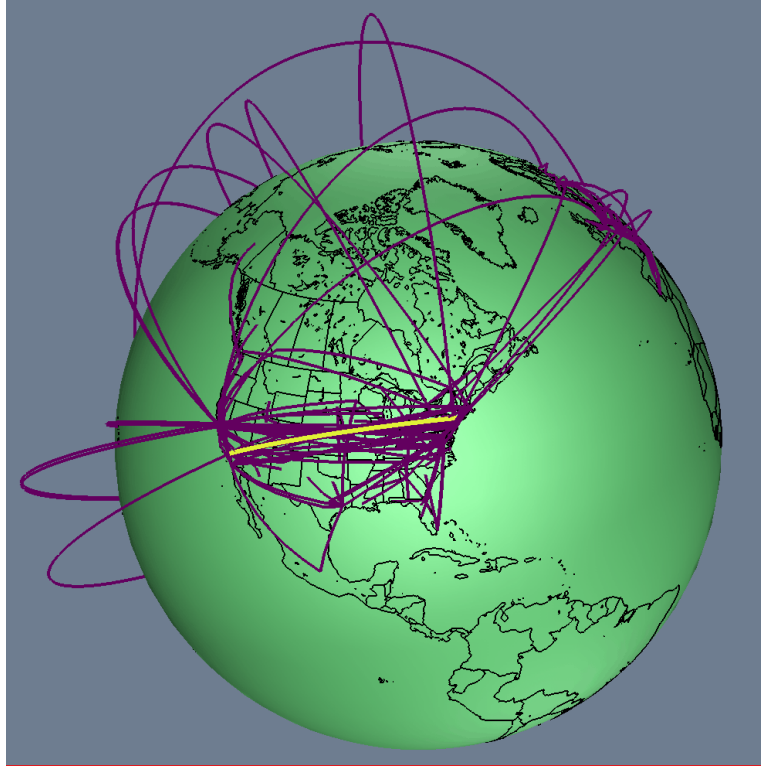
## L3 Transport Options in clouds:

Opt. Source Redundancy	Native: PIM-SSM or MVPN/SSM MPLS: LSM / mLDP RSVP-TE	IGMP: {Limits} {Static-fwd} PIM-SSM	IGMPv3 snooping	IGMPv3 proxy routing	IGMPv3 SSM
	PIM-SSM	PIM-SSM			

출처:

Cisco의 NANOG 발표 자료

"[http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride\\_ipvtv\\_N44.pdf](http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride_ipvtv_N44.pdf)"



# MULTICAST ADDRESSING



# Multicast addressing

- IP multicast group addresses
  - 224.0.0.0–239.255.255.255
    - Class “D” Address Space
    - High order bits of 1st Octet = “1110”
- TTL value defines scope and limits distribution
  - IP multicast packet must have TTL > interface TTL or it is discarded
    - TTL 0 : node-local
    - TTL 1 : link-local
    - TTL 32 : site-local
    - TTL 64 : region-local
    - TTL 128 : continent-local
    - TTL 256 : global-local
  - No longer recommended as a reliable scoping mechanism

# Multicast addressing

- Administratively scoped addresses (RFC 2365)
  - 239.0.0.0–239.255.255.255
  - Private address space
    - Similar to RFC 1918 unicast addresses
    - Not used for global Internet traffic
    - Used to limit “scope” of multicast traffic
    - Same addresses may be in use at different locations for different multicast sessions
  - Examples
    - Site-local scope: 239.253.0.0/16
    - Organization-local scope: 239.192.0.0/14

# Multicast addressing

- <http://www.iana.org/assignments/multicast-addresses>
- Examples of Reserved & Link-local Addresses

224.0.0.0 - 224.0.0.255 reserved & not forwarded

224.0.0.1 - All local hosts

224.0.0.2 - All local routers

224.0.0.4 – DVMRP

224.0.0.5 – OSPF

224.0.0.9 - RIP2

224.0.0.13 – PIM

224.0.0.15 – CBT

224.0.1.0 – 238.255.255.255 : Globally scoped addresses

224.0.0.1 - NTP

232.0.0.0 - 232.255.255.255: Source-Specific Multicast

233.0.0.0 – 233.255.255.255: GLOP

239.0.0.0 - 239.255.255.255: Administratively Limited Scope

# Multicast address allocation

- For a long time, this was a sore spot
- There was no way to claim or register a Class D address like unicast address blocks can be registered
  - For temporary teleconferences, this is not such a problem, but it does not fit well into a broadcast model.
- **Now, there are two solutions :**
  - For SSM, addresses don't matter, as the broadcast address is really unique as long as the (S,G) pair is unique
  - For ASM, there is "GLOP"

# GLOP

- GLOP addresses
  - Provides globally available private Class D space
  - 233.x.x.0/24 per AS number : globally unique
  - RFC2770
- How?
  - AS number = 16 bits
  - Insert the 16 ASN into the middle two octets of 233/8

Online Glop Calculator:

[www.shepfarm.com/multicast/glop.html](http://www.shepfarm.com/multicast/glop.html)

# Example: KT

- KT AS Number: 4766 = x.18.158.x

출처: 본인 작성

13	0.013381	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destinat
14	0.014499	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destinat
15	0.015621	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destinat
16	0.016750	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destinat

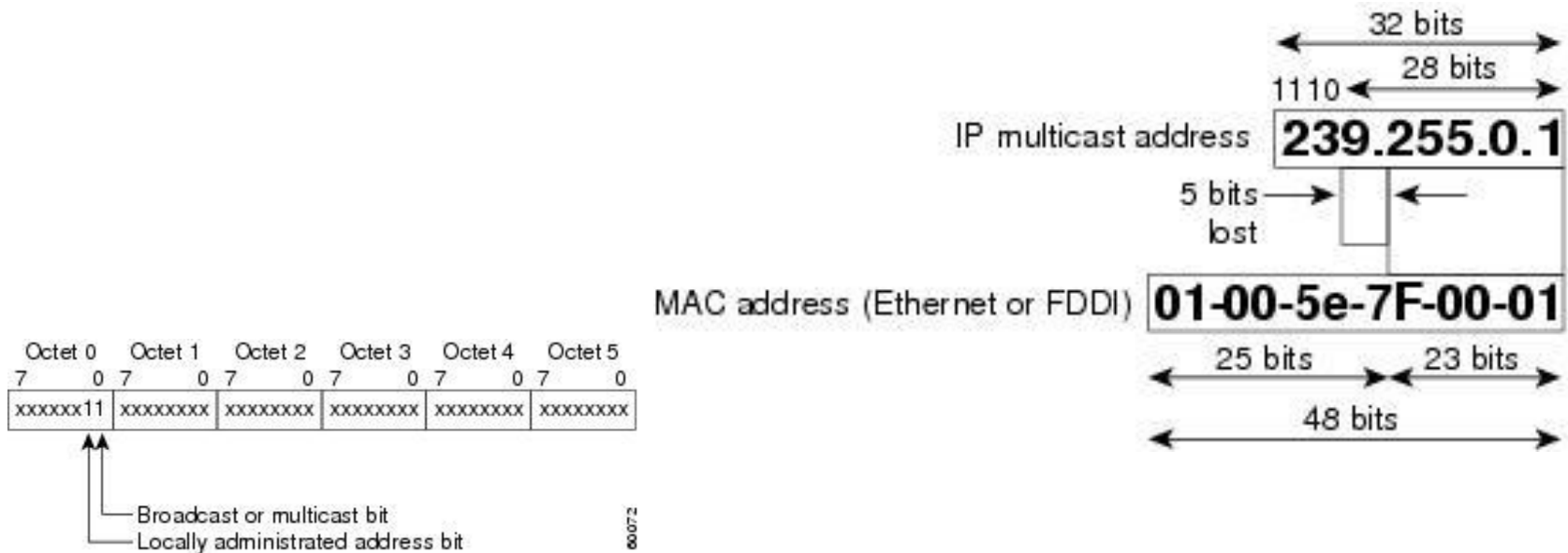
  

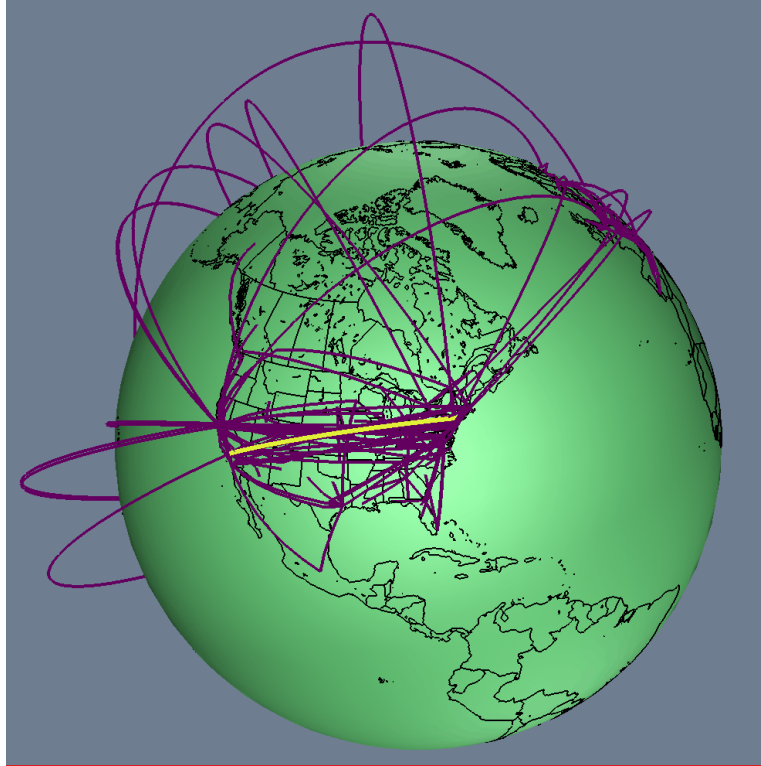
+	Frame 1 (1370 bytes on wire, 1370 bytes captured)
+	Ethernet II, Src: Dasan_79:06:57 (00:d0:cb:79:06:57), Dst: IPv4mcast_12:9e:71 (01:00:5e:12:9e:71)
+	Internet Protocol, Src: 125.159.0.53 (125.159.0.53), Dst: 233.18.158.113 (233.18.158.113)
+	User Datagram Protocol, Src Port: 50000 (50000), Dst Port: complex-main (5000)
+	Data (1328 bytes)

- With PIM-SSM, every sender (server) would have > 250 channels
  - No shortage of group addresses
  - No address coordination problem (with SSM only)
  - What if you exhaust your 233/8 space?

# Ethernet MAC address mapping

- The IANA owns a block of Ethernet MAC addresses
  - Starts with 01:00:5E in hex
  - Half of this block is allocated for multicast addresses.
    - 0100.5e00.0000 - 0100.5e7f.ffff for IP multicast
- The lower 23 bits of the IP multicast group address into these available 23 bits in the Ethernet address





# MULTICAST PROTOCOLS – IGMP



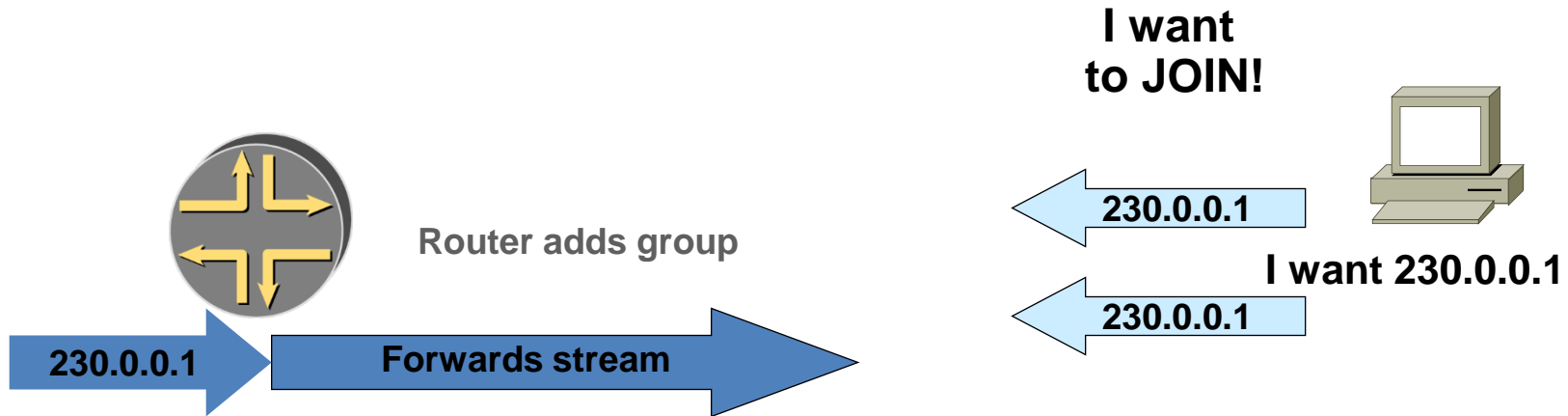
# Internet Group Management Protocol

- How hosts tell routers about group membership
- Routers solicit group membership from directly connected hosts
  - For each attached network, a multicast router can be either a **querier** or a nonquerier.
    - The querier router periodically sends general query messages to solicit group membership information.
- RFC 2236 specifies IGMPv2
  - Supported on every OS
- IGMPv3 is the latest version (RFC 3376)
  - Provides source include-list capabilities (SSM!)
  - Interoperates with versions 1 and 2
    - IGMPv3 routers must also implement versions 1 and 2 of the protocol

# IGMP overview

- IGMPv3 supports **inclusion lists**
  - Provide the ability to specify which sources can send to a multicast group
  - Source-Specific Multicast (SSM) group
- IGMPv3 provides support for source filtering
  - For example, a router can specify particular routers from which it will, or will not, receive traffic
- Exclusion mode works like an inclusion list, allowing any source but the ones listed to send to the SSM group

# IGMPv2 protocol flow – Join a Group

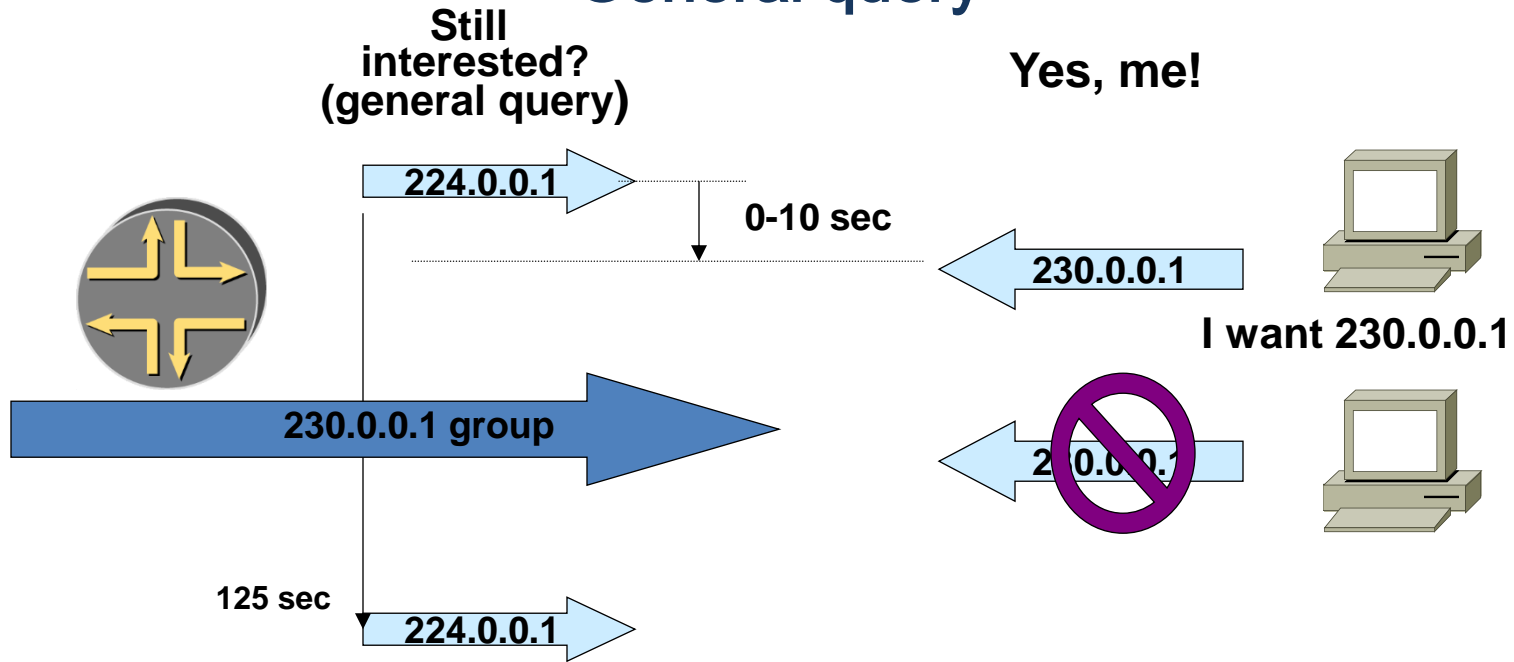


- Router triggers group membership request to PIM
- Hosts can send unsolicited join membership messages – called reports in the RFC
- Or hosts can join by responding to periodic query from router

출처: Internet2 workshop

"[https://www.google.co.kr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fpeople.inf.elte.hu%2Ftoke%2FhalozatokII-jegyzet%2Fel%25C5%2591ad%25C3%25A1sok%2FMulticast%2Fajanlott%2Finternet2-multicast-workshop-july-2004-2-LAN-SSM-2.ppt&ei=ko7nUbudPIWdiAf\\_poDICw&usg=AFQjCNFOO0KFI2zFz8hhQhLQEHdTEd1-A&sig2=2CIK45NDpd7-\\_KUBwc0xQw&bvm=bv.49478099,d.aGc&cad=rjt](https://www.google.co.kr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fpeople.inf.elte.hu%2Ftoke%2FhalozatokII-jegyzet%2Fel%25C5%2591ad%25C3%25A1sok%2FMulticast%2Fajanlott%2Finternet2-multicast-workshop-july-2004-2-LAN-SSM-2.ppt&ei=ko7nUbudPIWdiAf_poDICw&usg=AFQjCNFOO0KFI2zFz8hhQhLQEHdTEd1-A&sig2=2CIK45NDpd7-_KUBwc0xQw&bvm=bv.49478099,d.aGc&cad=rjt)"

# IGMPv2 protocol flow - General query

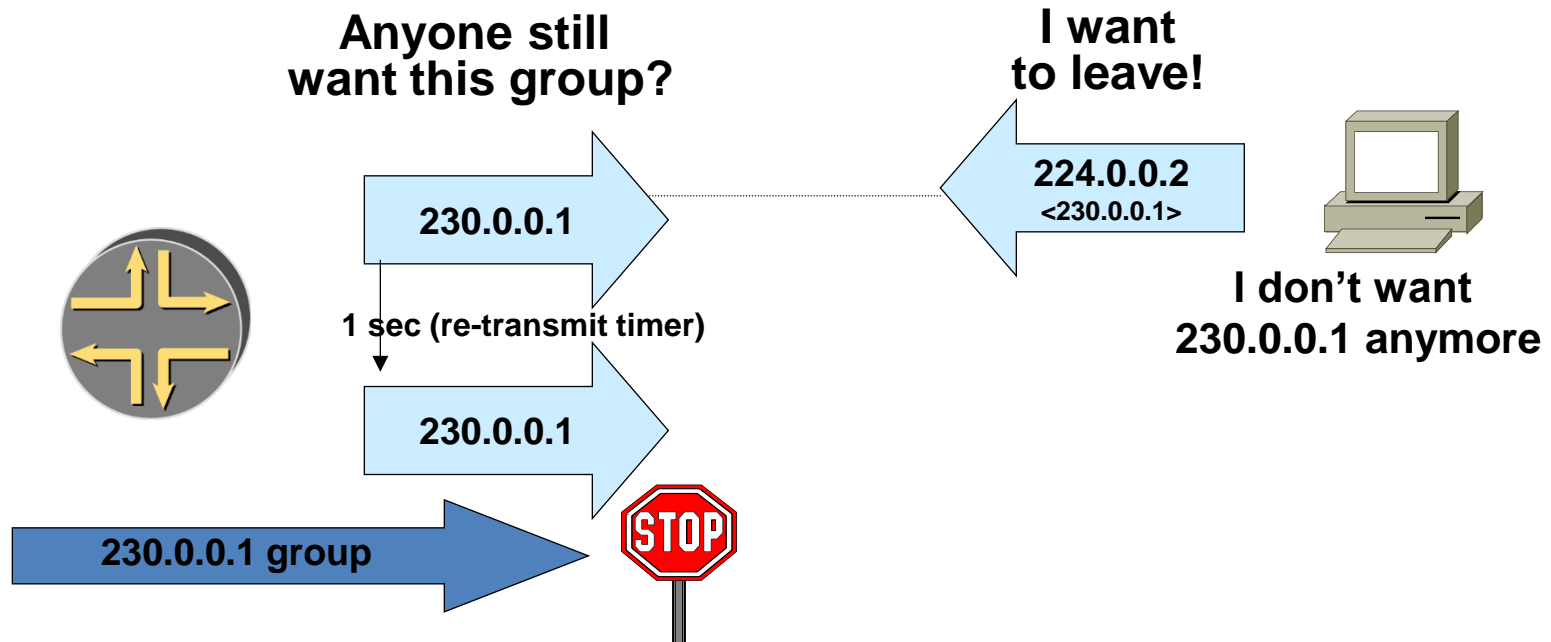


- Hosts respond to query to indicate (new or continued) interest in group(s)
  - Only 1 host should respond per group
    - Hosts fall into idle-member state when same-group report is heard
- After 260 sec with no response, router times out group

출처: Internet2 workshop

"[https://www.google.co.kr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fpeople.inf.elte.hu%2Ftoke%2FhalozatokII-jegyzet%2Fel%25C5%2591ad%25C3%25A1sok%2FMulticast%2Fajanlott%2Finternet2-multicast-workshop-july-2004-2-LAN-SSM-2.ppt&ei=ko7nUbudPIWdiAf\\_poDICw&usg=AFQjCNFOO0KFI2zFz8hhQhLQEHdTEd1-A&sig2=2CIK45NDpd7-\\_KUBwc0xQw&bvm=bv.49478099,d.aGc&cad=rjt](https://www.google.co.kr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fpeople.inf.elte.hu%2Ftoke%2FhalozatokII-jegyzet%2Fel%25C5%2591ad%25C3%25A1sok%2FMulticast%2Fajanlott%2Finternet2-multicast-workshop-july-2004-2-LAN-SSM-2.ppt&ei=ko7nUbudPIWdiAf_poDICw&usg=AFQjCNFOO0KFI2zFz8hhQhLQEHdTEd1-A&sig2=2CIK45NDpd7-_KUBwc0xQw&bvm=bv.49478099,d.aGc&cad=rjt)"

# IGMPv2 protocol flow – Leave a group



- Hosts send leave messages to all routers group indicating group they are leaving
  - Router follows up with 2 group-specific queries messages

출처: Internet2 workshop

"[https://www.google.co.kr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fpeople.inf.elte.hu%2Ftoke%2FhalozatokII-jegyzet%2Fel%25C5%2591ad%25C3%25A1sok%2FMulticast%2Fajanlott%2Finternet2-multicast-workshop-july-2004-2-LAN-SSM-2.ppt&ei=ko7nUbudPIWdiAf\\_poDICw&usg=AFQjCNFOO0KFI2zFz8hhQhLQEHFdTEd1-A&sig2=2CIK45NDpd7-\\_KUBwc0xQw&bvm=bv.49478099,d.aGc&cad=rjt](https://www.google.co.kr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fpeople.inf.elte.hu%2Ftoke%2FhalozatokII-jegyzet%2Fel%25C5%2591ad%25C3%25A1sok%2FMulticast%2Fajanlott%2Finternet2-multicast-workshop-july-2004-2-LAN-SSM-2.ppt&ei=ko7nUbudPIWdiAf_poDICw&usg=AFQjCNFOO0KFI2zFz8hhQhLQEHFdTEd1-A&sig2=2CIK45NDpd7-_KUBwc0xQw&bvm=bv.49478099,d.aGc&cad=rjt)"

# Example: KT IPTV

- Traffic almost immediately stops

출처: 본인 작성

7520	8.488730	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-main
7521	8.491038	118.48.34.143	233.18.158.113	IGMP	V2 Membership Report / Join group 233.18.158.113	
7522	8.498868	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-main
7523	8.499986	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-main
7524	8.502262	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-main
7525	8.504535	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-main
7526	8.505653	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-main
7527	8.506856	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-main
7528	8.508065	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-main
7529	8.508187	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.113	
7530	8.508192	118.48.34.143	233.18.158.68	IGMP	V2 Membership Report / Join group 233.18.158.68	
7531	8.516087	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-main
7534	8.518970	61.72.223.167	233.18.158.113	IGMP	V2 Membership Query / Join group 233.18.158.113	
7537	8.532345	125.159.0.26	233.18.158.253	UDP	Source port: 50000	Destination port: complex-main
7539	8.543089	125.159.0.26	233.18.158.253	UDP	Source port: 50000	Destination port: complex-main
7540	8.544208	125.159.0.26	233.18.158.253	UDP	Source port: 50000	Destination port: complex-main

# Example: KT IPTV

- Channel zapping

출처: 본인 작성

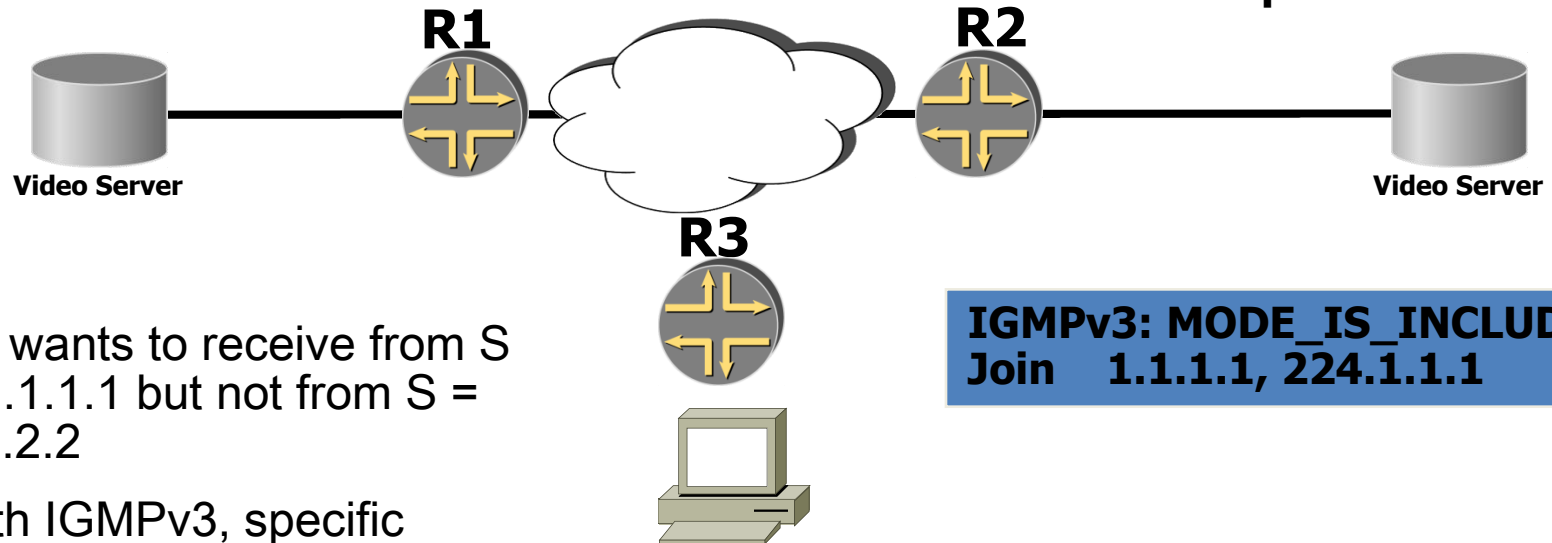
6701	7.540178	118.48.34.143	224.0.0.251	IGMP	V2 Membership Report / Join group 224.0.0.251
7521	8.491038	118.48.34.143	233.18.158.113	IGMP	V2 Membership Report / Join group 233.18.158.113
7529	8.508187	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.113
7530	8.508192	118.48.34.143	233.18.158.68	IGMP	V2 Membership Report / Join group 233.18.158.68
7534	8.518970	61.72.223.167	233.18.158.113	IGMP	V2 Membership Query / Join group 233.18.158.113
8333	9.523908	61.72.223.167	233.18.158.113	IGMP	V2 Membership Query / Join group 233.18.158.113
9644	11.138496	118.48.34.143	233.18.158.68	IGMP	V2 Membership Report / Join group 233.18.158.68
9904	11.455507	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.68
9905	11.455723	118.48.34.143	233.18.158.104	IGMP	V2 Membership Report / Join group 233.18.158.104
9916	11.466568	61.72.223.167	233.18.158.68	IGMP	V2 Membership Query / Join group 233.18.158.68
10357	12.474439	61.72.223.167	233.18.158.68	IGMP	V2 Membership Query / Join group 233.18.158.68
10682	13.221827	118.48.34.143	233.18.158.104	IGMP	V2 Membership Report / Join group 233.18.158.104
10972	13.867681	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.104
10985	13.896457	61.72.223.167	233.18.158.104	IGMP	V2 Membership Query / Join group 233.18.158.104
11068	14.902093	61.72.223.167	233.18.158.104	IGMP	V2 Membership Query / Join group 233.18.158.104
11105	15.399882	118.48.34.143	233.18.158.61	IGMP	V2 Membership Report / Join group 233.18.158.61
14653	19.411122	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.61
14662	19.423398	61.72.223.167	233.18.158.61	IGMP	V2 Membership Query / Join group 233.18.158.61
14707	20.060688	118.48.34.143	233.18.158.74	IGMP	V2 Membership Report / Join group 233.18.158.74
14971	20.431701	61.72.223.167	233.18.158.61	IGMP	V2 Membership Query / Join group 233.18.158.61
17825	23.924929	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.74
17832	23.932779	118.48.34.143	233.18.158.11	IGMP	V2 Membership Report / Join group 233.18.158.11
17835	23.939345	61.72.223.167	233.18.158.74	IGMP	V2 Membership Query / Join group 233.18.158.74
18147	24.940892	61.72.223.167	233.18.158.74	IGMP	V2 Membership Query / Join group 233.18.158.74
19024	27.374108	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.11
19027	27.379813	118.48.34.143	233.18.158.71	IGMP	V2 Membership Report / Join group 233.18.158.71
19032	27.394116	61.72.223.167	233.18.158.11	IGMP	V2 Membership Query / Join group 233.18.158.11
19863	28.401358	61.72.223.167	233.18.158.11	IGMP	V2 Membership Query / Join group 233.18.158.11
23298	32.385571	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.71
23307	32.399289	61.72.223.167	233.18.158.71	IGMP	V2 Membership Query / Join group 233.18.158.71
23309	32.408249	118.48.34.143	233.18.158.66	IGMP	V2 Membership Report / Join group 233.18.158.66
23999	33.305541	118.48.34.143	233.18.158.66	IGMP	V2 Membership Report / Join group 233.18.158.66
24085	33.409989	61.72.223.167	233.18.158.71	IGMP	V2 Membership Query / Join group 233.18.158.71
25966	35.741680	118.48.34.143	233.18.158.66	IGMP	V2 Membership Report / Join group 233.18.158.66
26162	35.985431	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.66
26163	35.985648	118.48.34.143	233.18.158.69	IGMP	V2 Membership Report / Join group 233.18.158.69
26172	36.001910	61.72.223.167	233.18.158.66	IGMP	V2 Membership Query / Join group 233.18.158.66
26549	36.467483	118.48.34.143	233.18.158.69	IGMP	V2 Membership Report / Join group 233.18.158.69
27002	37.009989	61.72.223.167	233.18.158.66	IGMP	V2 Membership Query / Join group 233.18.158.66
28734	39.155445	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.69
28739	39.161007	118.48.34.143	233.18.158.159	IGMP	V2 Membership Report / Join group 233.18.158.159
28742	39.166266	61.72.223.167	233.18.158.69	IGMP	V2 Membership Query / Join group 233.18.158.69
29158	40.184535	61.72.223.167	233.18.158.69	IGMP	V2 Membership Query / Join group 233.18.158.69
30043	42.149710	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.159

# IGMPv3

- RFC 3376
- Enables hosts to listen only to a specified subset of the hosts sending to the group

**Source = 1.1.1.1**  
**Group = 224.1.1.1**

**Source = 2.2.2.2**  
**Group = 224.1.1.1**



- H1 wants to receive from S = 1.1.1.1 but not from S = 2.2.2.2
- With IGMPv3, specific sources can be pruned back - S = 2.2.2.2 in this case

**H1 - Member of 224.1.1.1**

출처: Internet2 workshop

"[https://www.google.co.kr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fpeople.inf.elte.hu%2Ftoke%2FhalozatokII-jegyzet%2Fel%25C5%2591ad%25C3%25A1sok%2FMulticast%2Fajanlott%2Finternet2-multicast-workshop-july-2004-2-LAN-SSM-2.ppt&ei=ko7nUbudPIWdiAf\\_poDICw&usg=AFQjCNFOO0KFI2zFz8hhQhLQEHdTEd1-A&sig2=2CIK45NDpd7-\\_KUBwc0xQw&bvm=bv.49478099,d.aGc&cad=rjt](https://www.google.co.kr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fpeople.inf.elte.hu%2Ftoke%2FhalozatokII-jegyzet%2Fel%25C5%2591ad%25C3%25A1sok%2FMulticast%2Fajanlott%2Finternet2-multicast-workshop-july-2004-2-LAN-SSM-2.ppt&ei=ko7nUbudPIWdiAf_poDICw&usg=AFQjCNFOO0KFI2zFz8hhQhLQEHdTEd1-A&sig2=2CIK45NDpd7-_KUBwc0xQw&bvm=bv.49478099,d.aGc&cad=rjt)"



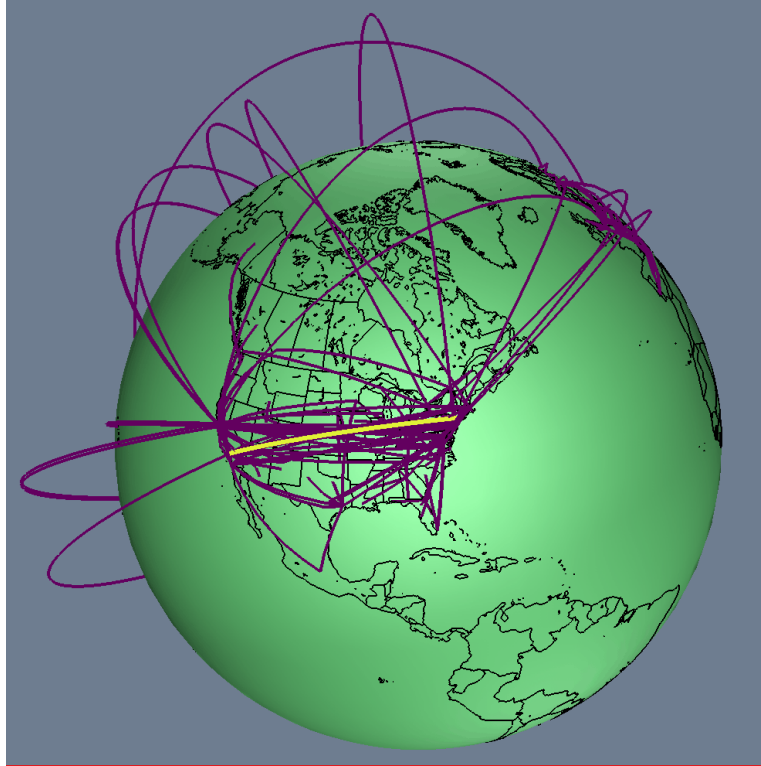
# IGMP enhancements

- IGMPv2

- Multicast router with lowest IP address is elected querier
- Group-Specific Query message is defined
  - Enables router to transmit query to specific multicast address rather than to the "all-hosts" address of 224.0.0.1
- Leave Group message is defined
  - Last host in group wishes to leave, it sends Leave Group message to the "all-routers" address of 224.0.0.2
- Router then transmits Group-Specific query and if no reports come in, then the router removes that group from the list of group memberships for that interface

- IGMPv3

- Group-Source Report message is defined
  - Enables hosts to specify which senders it can receive or not receive data from
- Group-Source Leave message is defined
  - Enables host to specify the specific IP addresses of a (S, G) that it wishes to leave



# MULTICAST PROTOCOLS – PIM-SM

# Protocol Independent Multicast – Sparse Mode

- Explicit join: assumes not everyone wants the data
- Uses unicast routing table for RPF checking
- Data and joins are forwarded to RP for initial rendezvous
- All routers in a PIM domain must have RP mapping
  - When load exceeds threshold forwarding swaps to shortest path tree (default is first packet)
- State increases as number of sources and number of groups increase
- Source-tree state is refreshed when data is forwarded and with Join/Prune control messages

# PIM-SM :RP

- Shared tree Rendezvous Point (RP)
  - Matches senders with receivers
  - Provides network source discovery
  - Root of shared tree
- Typically use shared tree to bootstrap source tree
- RP's can be learned via:
  - Static configuration
  - Auto-RP (V1 & V2)
  - Bootstrap Router (V2)

# RP mapping options

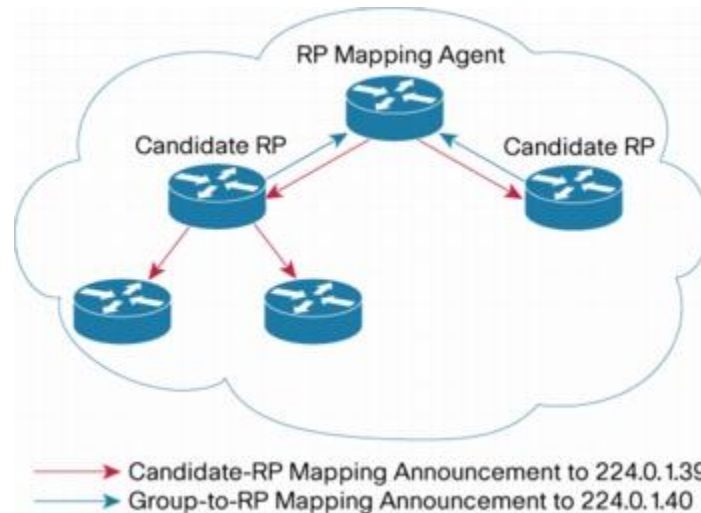
- Static RP
  - All leaf routers manually configured with the IP address of RP
  - Easy transition to Anycast-RP
  - Allows for a hierarchy of RPs
- Auto-RP
  - A router designated as an **RP mapping agent** receives the RP announcement messages from the RPs and arbitrates conflicts
  - Must flood RP mapping traffic to all routers by dense mode flooding
- Bootstrap router (BSR)
  - RFC5059
  - Allows for a hierarchy of RPs

# Static RP

- The address of the RP must be configured on every router in the domain
  - Good with small networks / infrequent mapping changes
- Static RP can co-exist with dynamic RP mechanisms (*i.e.*: Auto-RP).
  - Dynamically learned RP takes precedence over manually configured RPs
    - If a router receives Auto-RP information for a multicast group that has manually configured RP information, then the Auto-RP information will be used

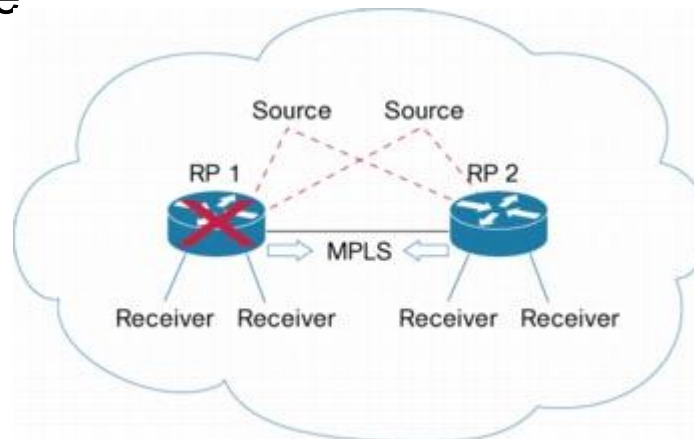
# Auto-RP

- Candidate RPs advertize their willingness to be an RP via "RP-announcement" messages.
  - Periodically sent to a reserved well-known group **224.0.1.39**
- **RP mapping agents** join group 224.0.1.39 and map the RPs to the associated groups
- The agents advertise the authoritative RP-mappings to 224.0.1.40
- All PIM routers join 224.0.1.40 and store the RP-mappings in their private cache



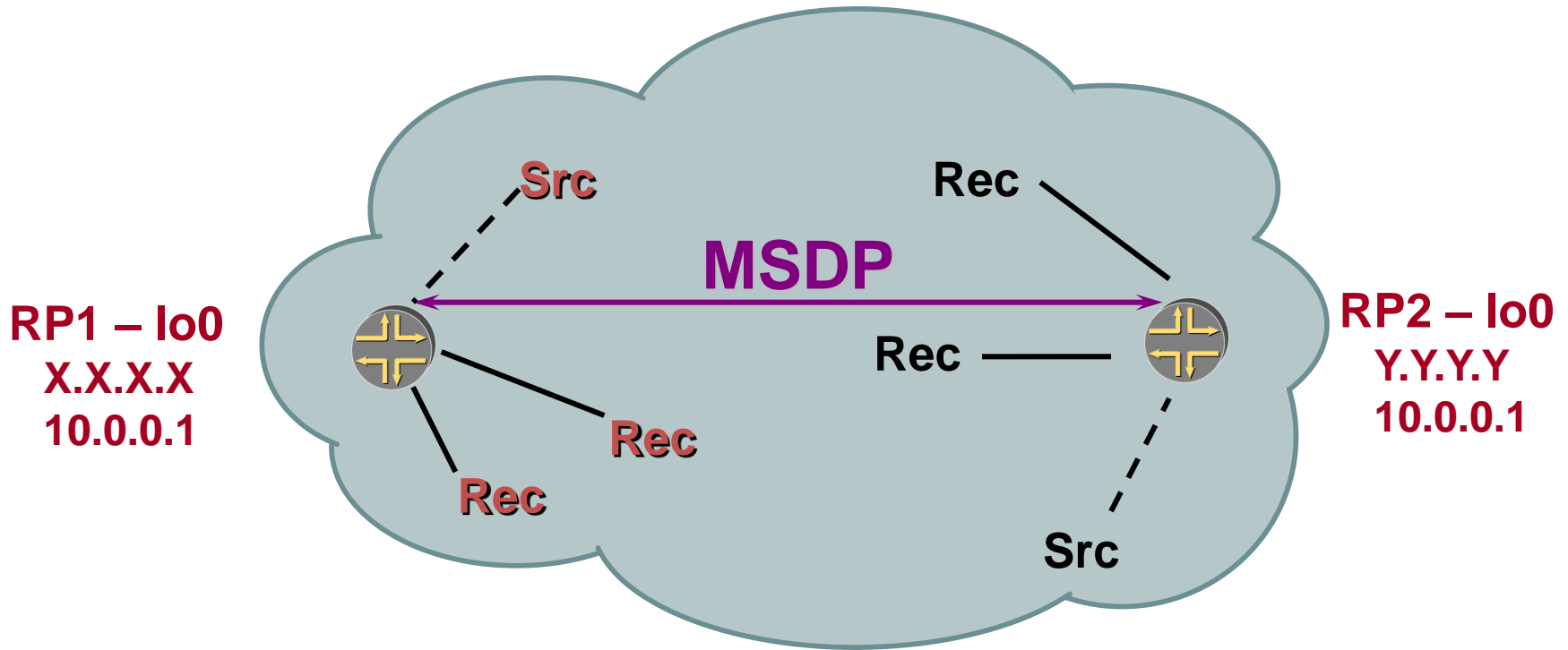
# Anycast RP

- Used to define redundant and load-balanced RPs
  - 2 or more RPs are configured with the **same IP address on loopback interfaces**
  - Can be used with Static RP or Auto-RP
- Two implementations:
  - Using Multicast Source Discovery Protocol (MSDP) described in RFC3446
    - RPs are configured to establish MSDP peering sessions using a TCP connection
  - Using Protocol Independent Multicast (PIM) described in RFC4610
    - PIM register and PIM join-prune messages are sent to the closest RP as determined by the unicast routing protocols
    - If one of the RPs goes down, unicast routing ensures these messages will be sent in the direction of the next-closest RP
- Group participants use the closest RP that is favored by the IP unicast route table





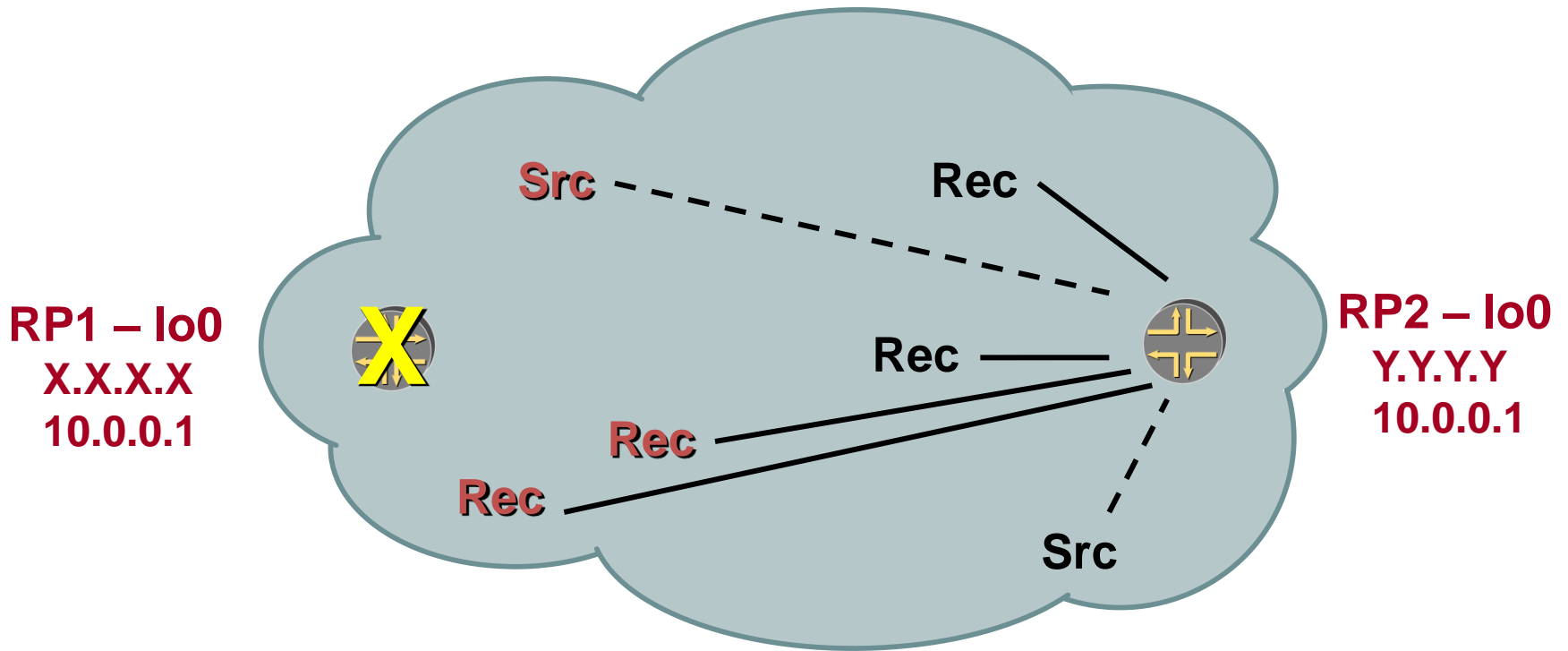
# Anycast RP with MSDP



출처: Cisco의 NANOG 발표 자료

"[www.garr.it/eventiGARR/.../doc/sotos\\_rediris\\_mcast\\_eumedconnect.ppt?](http://www.garr.it/eventiGARR/.../doc/sotos_rediris_mcast_eumedconnect.ppt?)"

# Anycast RP with MSDP

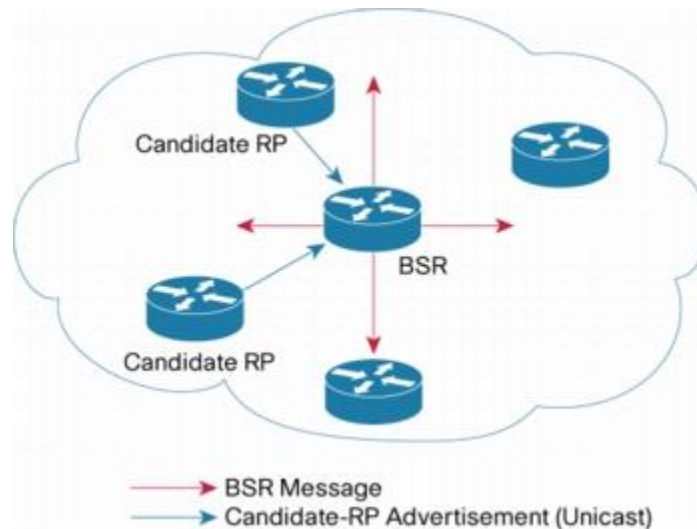


출처: Cisco의 NANOG 발표 자료

"[www.garr.it/eventiGARR/.../doc/sotos\\_rediris\\_mcast\\_eumedconnect.ppt?](http://www.garr.it/eventiGARR/.../doc/sotos_rediris_mcast_eumedconnect.ppt?)"

# BSR

- Candidate-RPs send advertisements directly to the elected BSR
- RP information flooded hop-by-hop to all routers
- Each router uses a common algorithm to select the same RP address for a given multicast group
- Cannot be used with Auto-RP



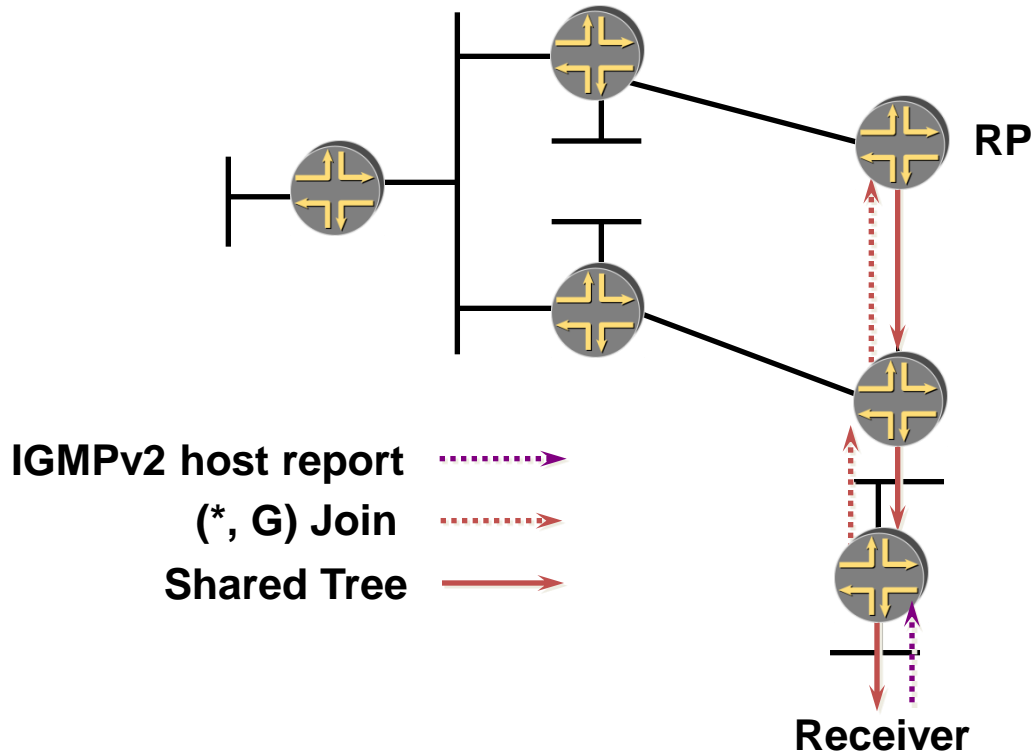
# PIM-SM group-to-RP mapping with BSR

1. Perform longest match on group-range to obtain a list of RPs
2. From this list of matching RPs, find the one with highest priority
  - Eliminate any RPs from the list that have lower priorities
3. If only one RP remains in the list, use that RP
4. If multiple RPs are in the list, use the PIM hash function to choose the highest-value one for the RP:

$$\text{Value}(G,M,C(i)) = (1103515245 * ((1103515245 * (G \& M) + 12345) \text{ XOR } C(i)) + 12345) \text{ mod } 2^{31}$$

- C(i) is the RP; Hash mask M is given in Bootstrap messages

# PIM-SM shared tree join

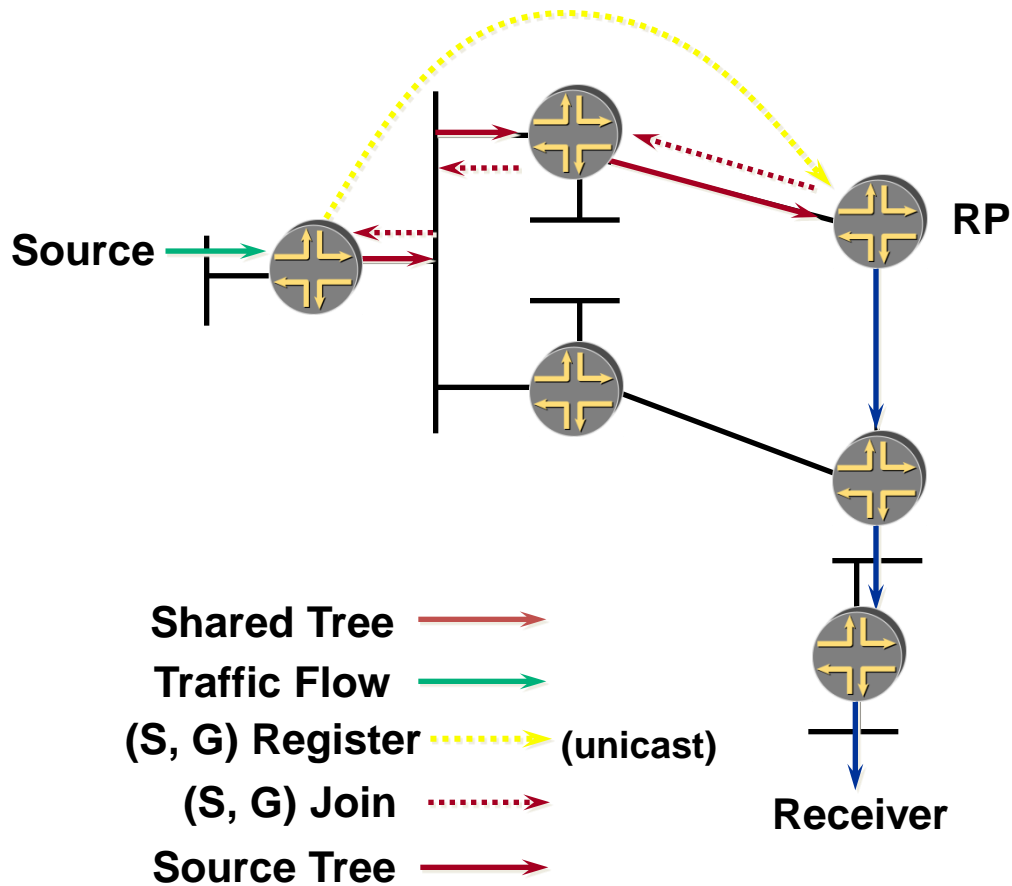


Receiver announces desire to join group G with igmpv2 host report – (\*,G).

First hop router sends PIM (\*,G) join toward the RP; subsequent routers do likewise.

(\* , G) State created from the RP to the receiver.

# PIM-SM sender registration

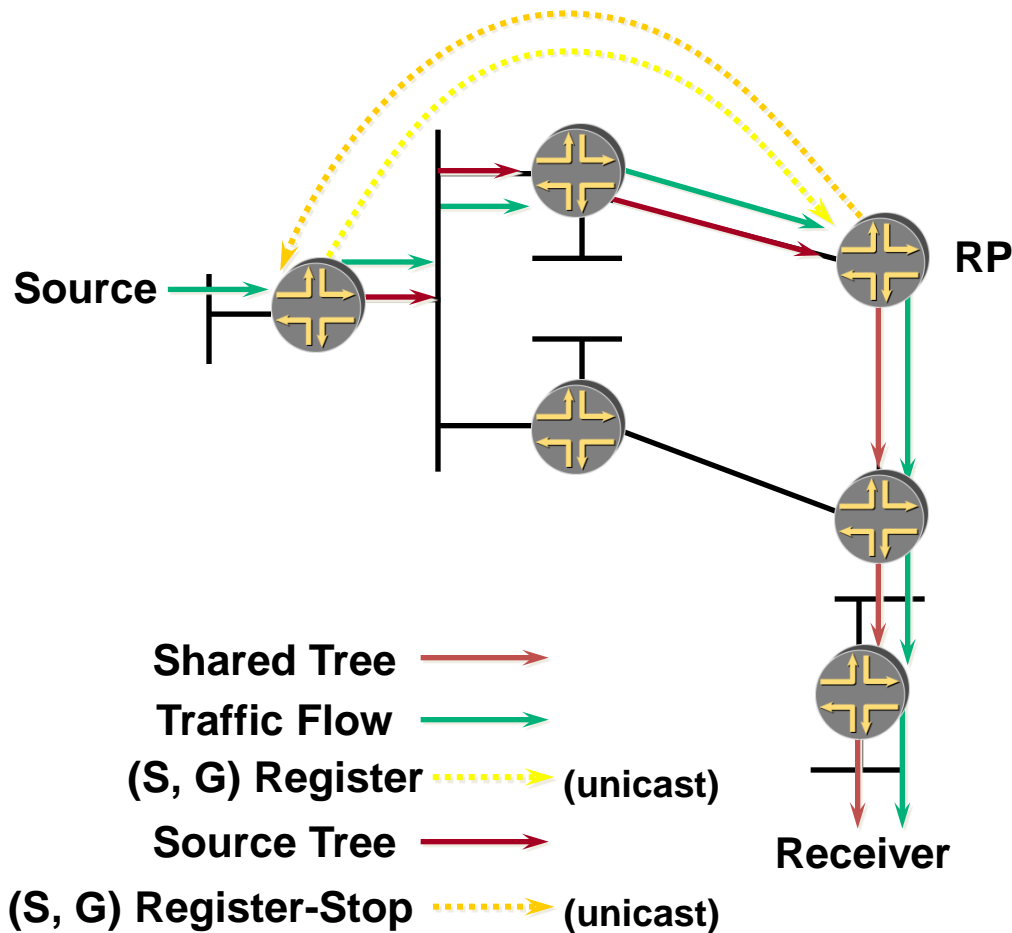


Active source triggers first-hop router (S,G) Register message to RP.

RP sends (S,G) Join to source.

(S, G) State created only along the Source Tree.

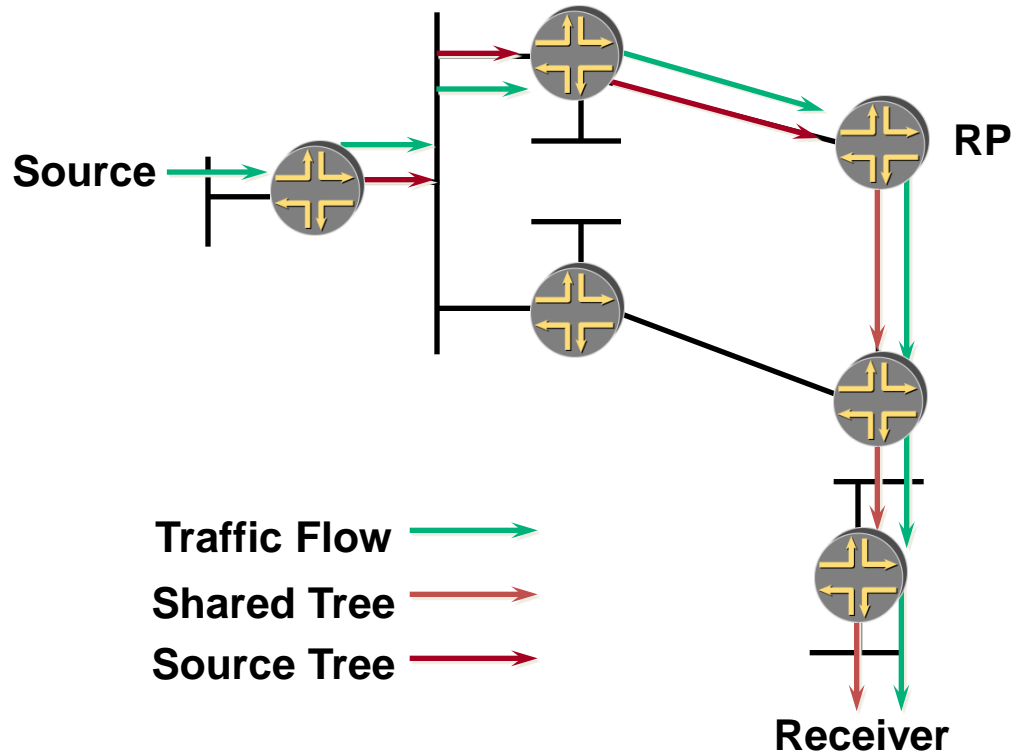
# PIM-SM sender registration



(S, G) traffic begins arriving at the RP via the Source tree.

RP sends a Register-Stop back to the first-hop router to stop the Register process.

# PIM-SM sender registration

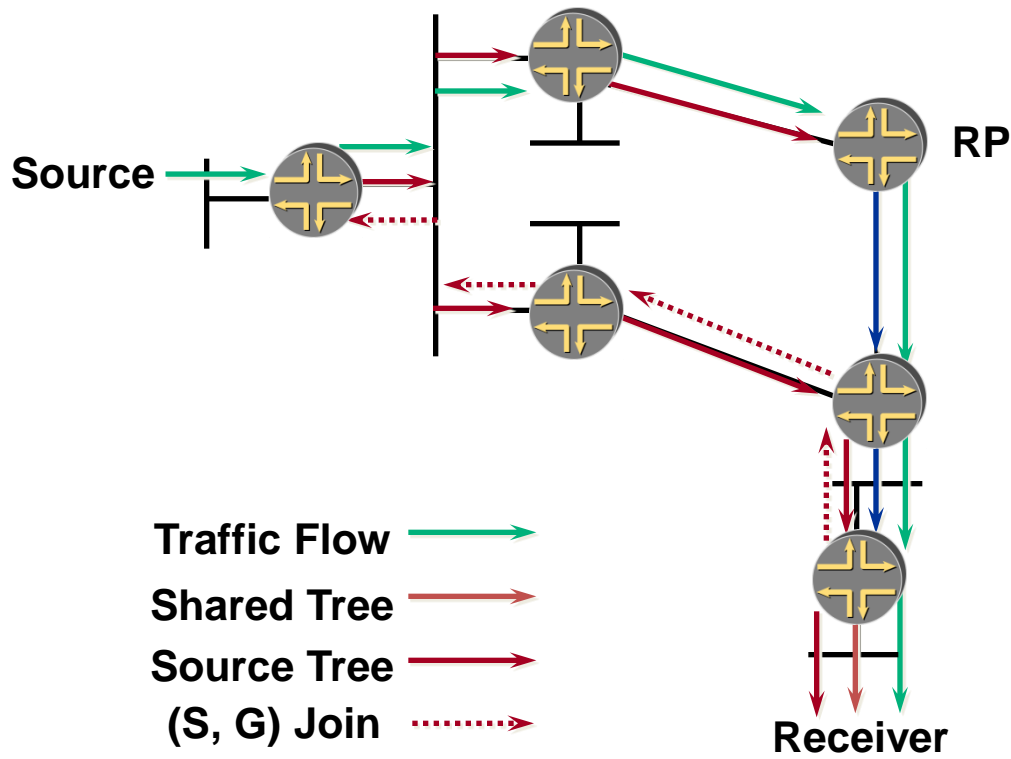


Source traffic flows natively along SPT to RP.

From RP, traffic flows down the Shared Tree to Receivers.



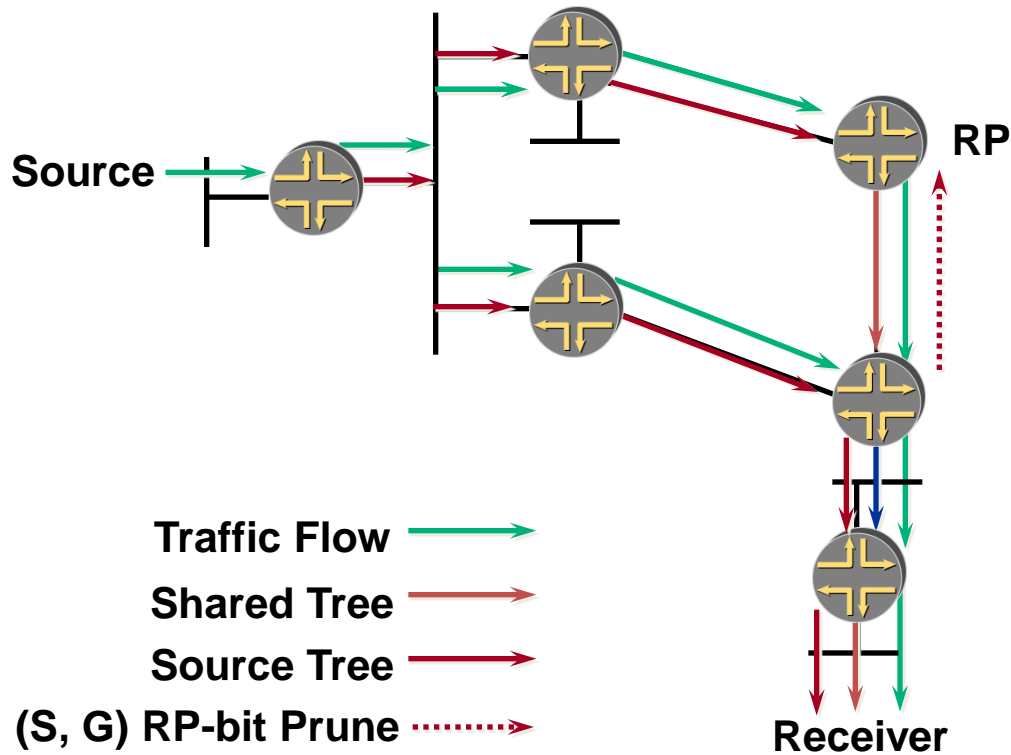
# PIM-SM SPT switchover



Last-hop router joins the Source Tree.

Additional (S, G) State is created along new part of the Source Tree.

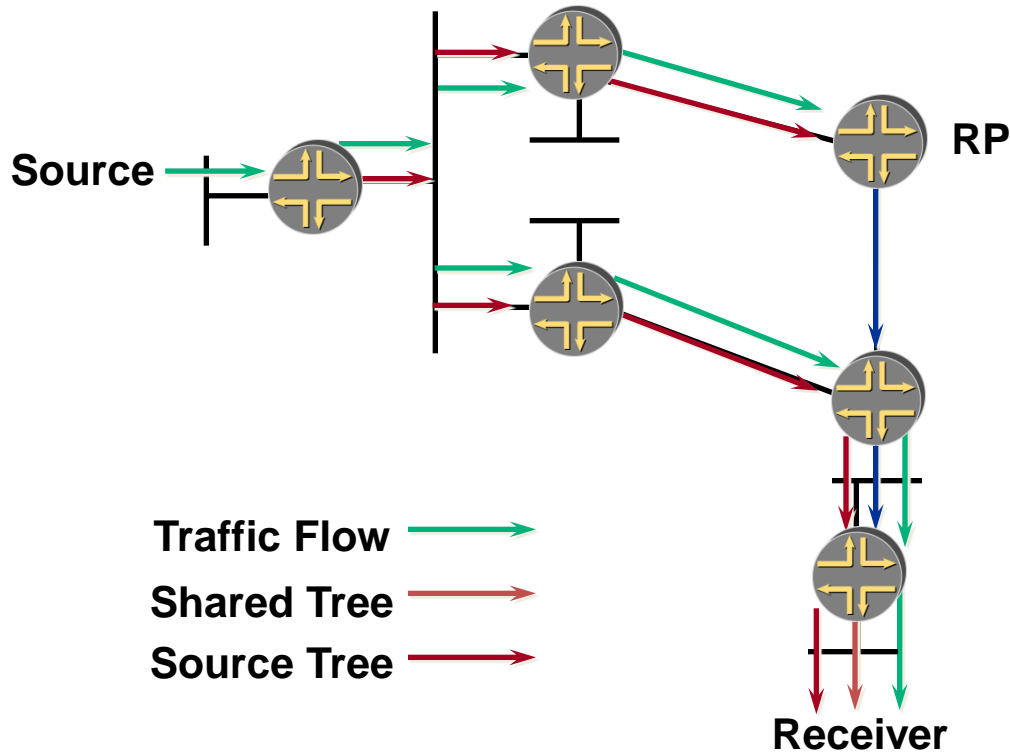
# PIM-SM SPT switchover



Traffic begins flowing down the new branch of the Source Tree.

Additional (S, G) State is created along the Shared Tree to prune off (S, G) traffic.

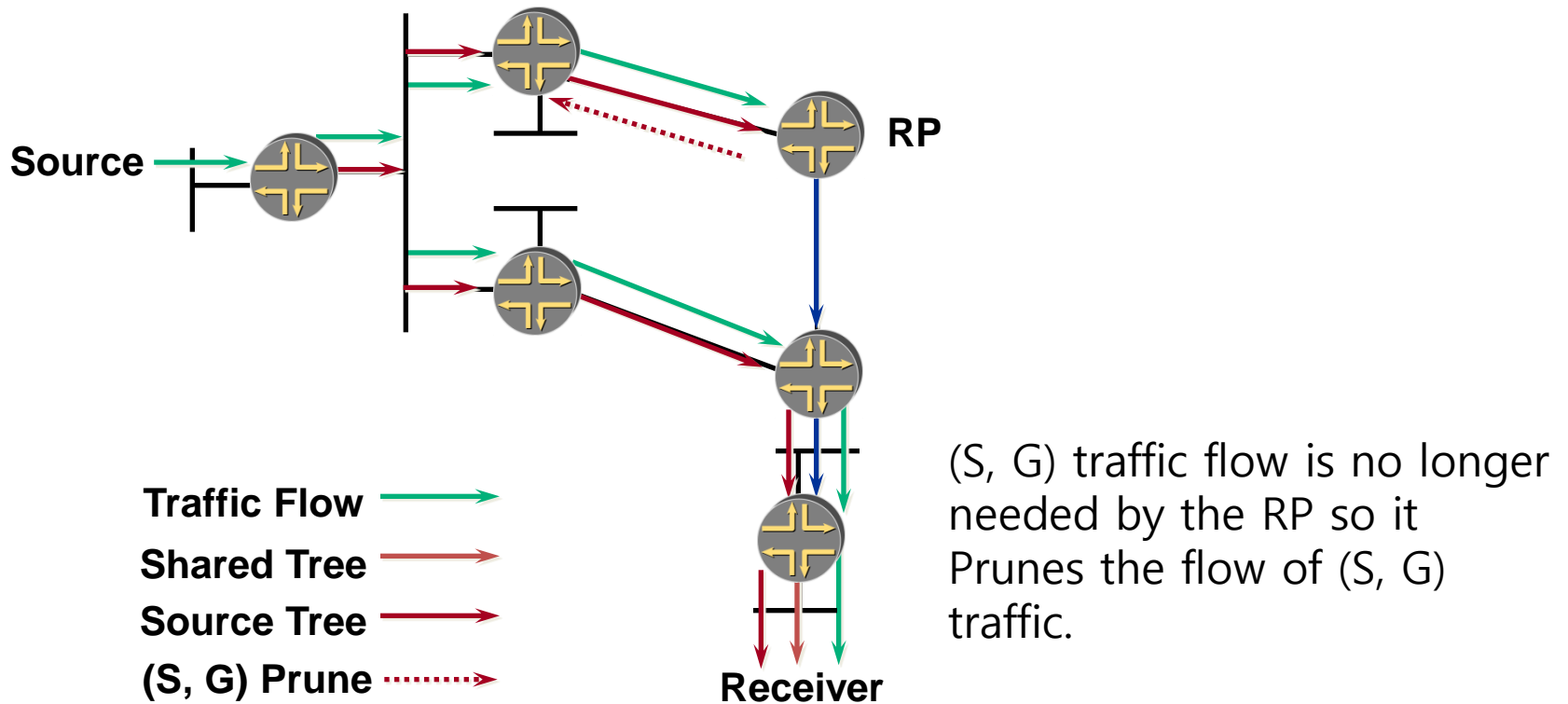
# PIM-SM SPT switchover



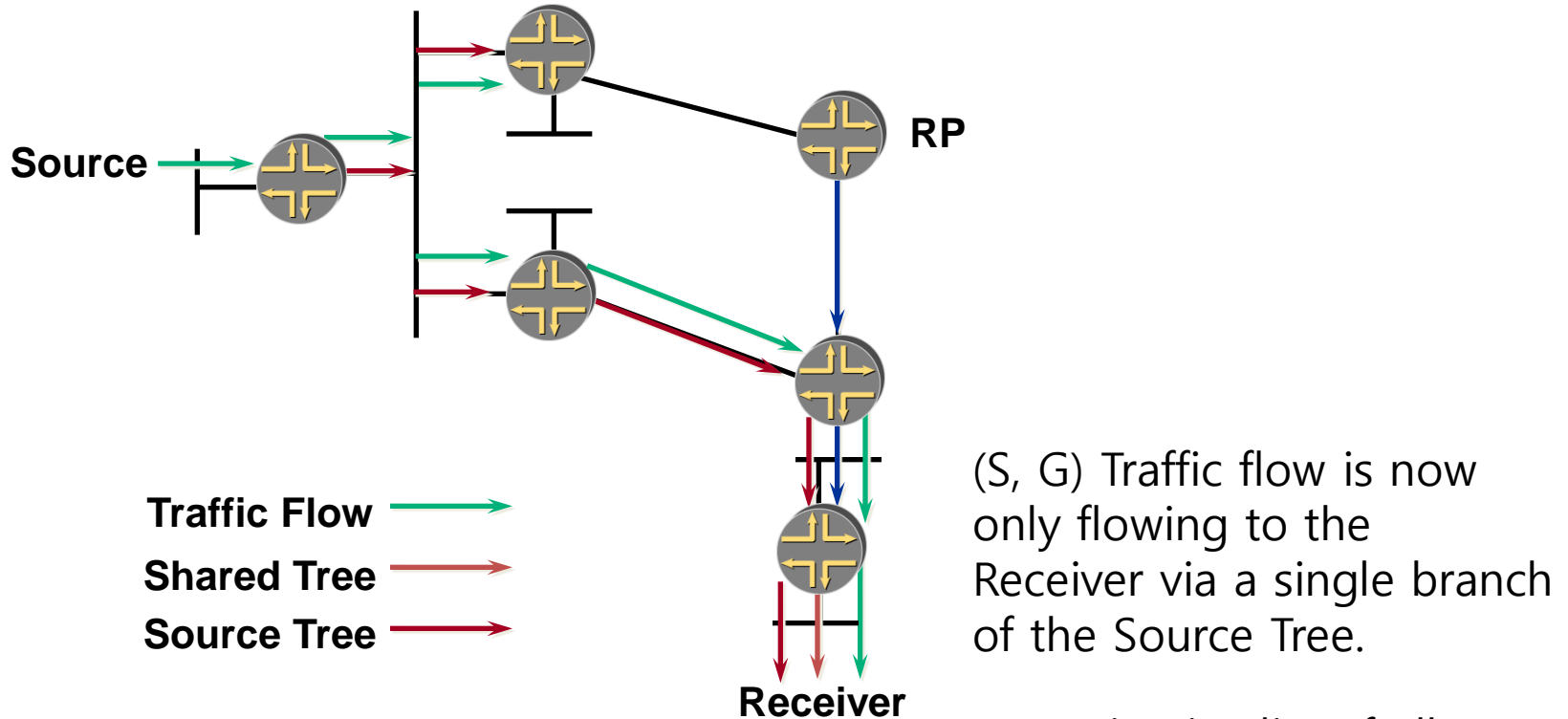
(S,G) Traffic flow is now pruned off of this branch of the Shared Tree and is flowing to the Receiver via the Source Tree.

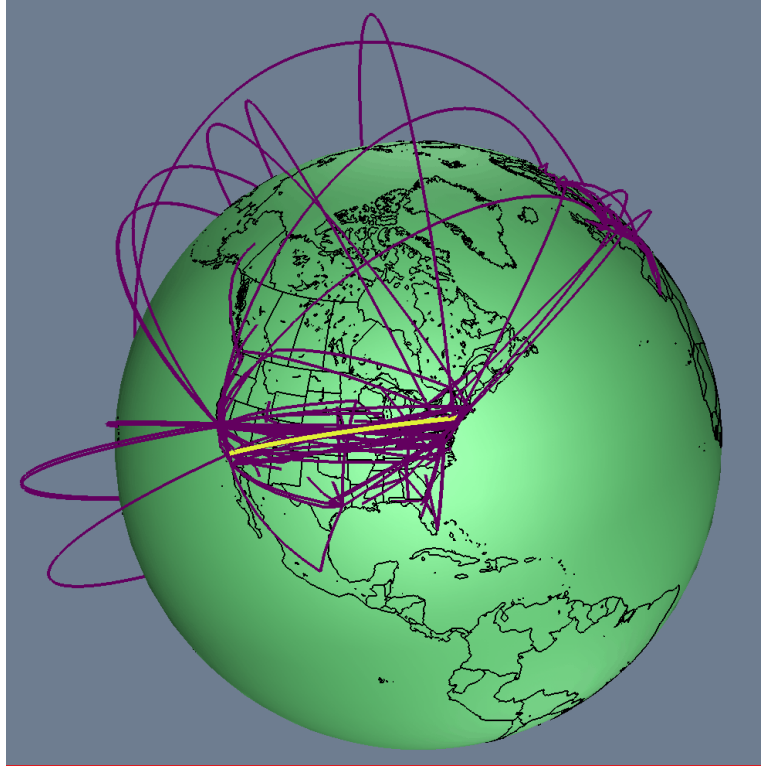
Traffic for other sources may still be flowing down the Shared Tree.

# PIM-SM SPT switchover



# PIM-SM SPT switchover





# **IP MULTICAST PROTOCOLS – PIM-SSM**

# PIM-Source Specific Multicast (SSM)

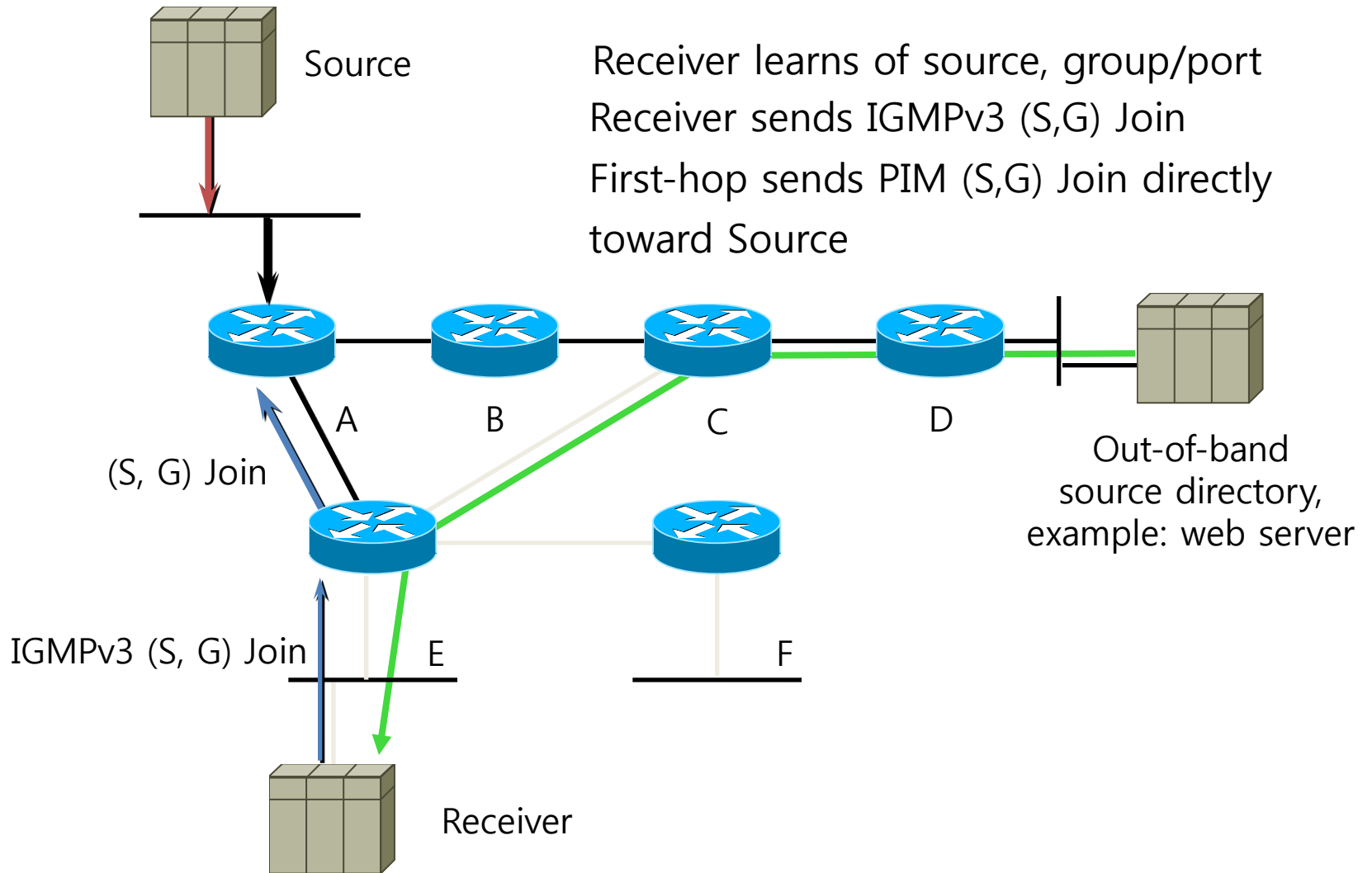
- No shared trees
  - Uses source trees only
- No register packets
- No RP required
- No RP-to-RP source discovery (MSDP)
- Assumes one-to-many model
  - Cf. many-to-many
- Hosts responsible for source discovery
  - Typically via some out-of-band mechanism
    - Web page, Content Server, etc.
- Requires IGMP include-source list – IGMPv3
  - Host must learn of source address out-of-band (web page)
  - Requires host-to-router (source + group) request

# SSM overview

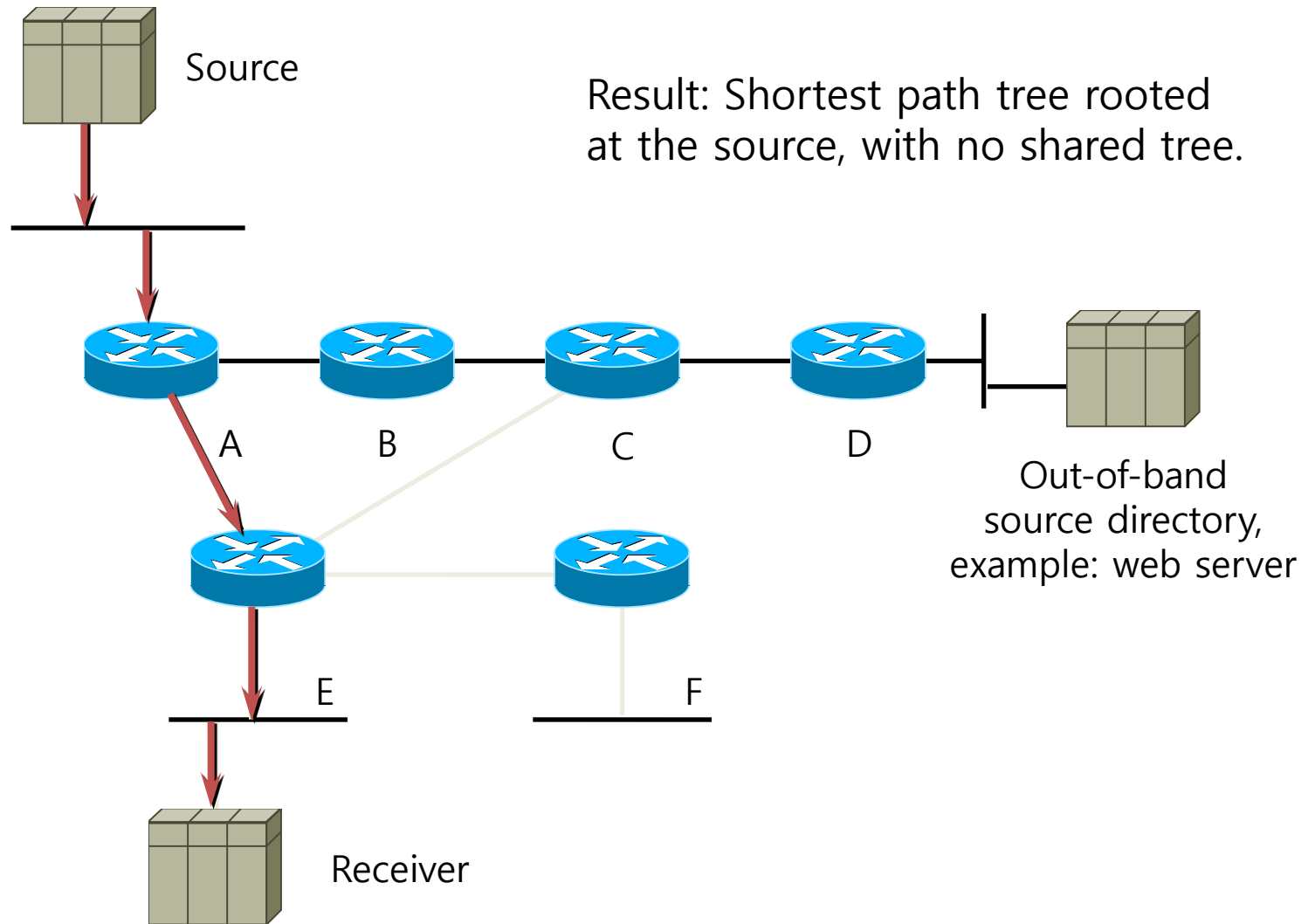
- Hosts join a specific source within a group
  - Content identified by specific (S,G) instead of (\*,G).
  - Hosts responsible for learning (S,G) information
- Last-hop router sends (S,G) join toward source
  - Shared Tree is never joined or used
  - Eliminates possibility of content jammers
  - Only specified (S,G) flow is delivered to host
- Simplifies address allocation
  - Dissimilar content sources can use same group without fear of interfering with each other



# PIM-SSM

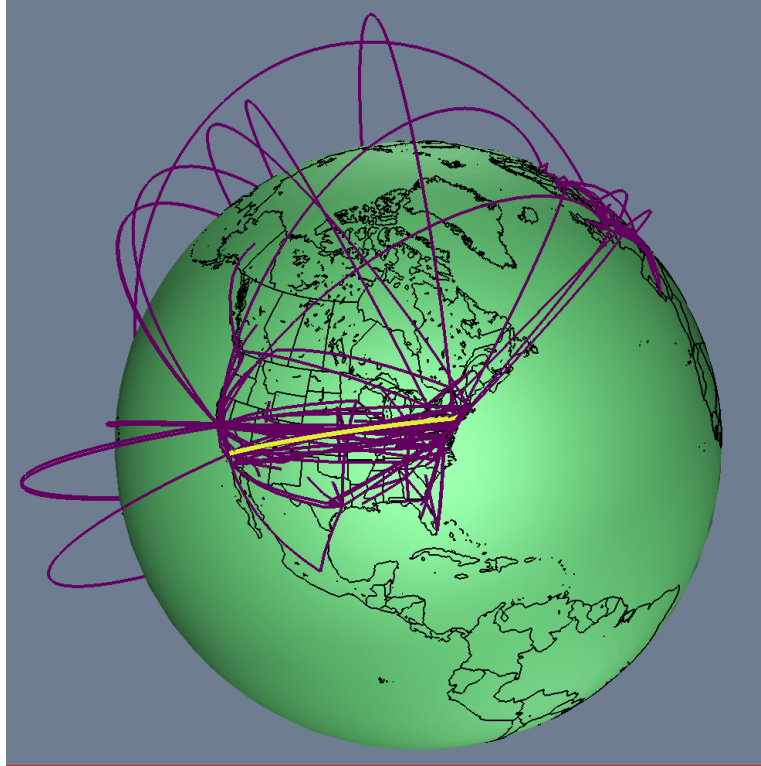


# PIM-SSM



# Where Is SSM?

- Framework
  - draft-holbrook-idmr-igmpv3-ssm-04.txt
  - draft-ietf-ssm-arch-03.txt
- BCP proposal
  - draft-ietf-mboned-ssm232-04.txt
  - draft-ietf-ssm-overview-04.txt
- Supported in:
  - Various router vendor OS
  - Windows XP, FreeBSD, Linux
  - <ftp://ftpeng.cisco.com/ipmulticast/ssm/index.html#Stacks>



# IP MULTICAST AND IPTV

# Multicast and IPTV

- Design IP multicast WITH SSM as generic infrastructure service – for IPTV and beyond
- Select transport design
  - Native IP multicast or mLDP (MPLS core) for most networks
  - RSVP-TE P2MP for eg: contribution network
- Understand your L2 broadband edge specifics
  - IGMPv3 snooping and SSM + lots of options
- Determine appropriate resilience support
- Path selection
  - ECMP and multicast or multiple topologies
- Admission control
  - Router local and broadband specific
- Channel changing
  - GOP size, total performance

# Join latency

- Static forwarding (to PE-AGG, or DSLAM) often done to avoid join latency
  - But other reasons too (policy, ...)
- Bogus ?
  - Join latency (PIM/IGMP) very low, e.g.: individual < 100 msec
    - Relevant: worst-case zapping performance
  - Joins stop at first router/switch in tree that already forwards tree
  - Probability for joins to go beyond PE-AGG very low !

*If you zap to a channel and it takes ¼ sec more:*

*You are the first guy watching this channel in a vicinity of eg: 50,000 people.*

*Are you sure you want to watch this lame program ?*

# Example: KT IPTV

- Join latency less than 50ms

출처: 본인 작성

7526	8.505653	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-m.
7527	8.506856	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-m.
7528	8.508065	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-m.
7529	8.508187	118.48.34.143	224.0.0.2	IGMP	v2 Leave Group 233.18.158.113	
7530	8.508192	118.48.34.143	233.18.158.68	IGMP	v2 Membership Report / Join group 233.18.158.68	
7531	8.516087	125.159.0.53	233.18.158.113	UDP	Source port: 50000	Destination port: complex-m.
7534	8.518970	61.72.223.167	233.18.158.113	IGMP	v2 Membership query / Join group 233.18.158.113	
7537	8.532345	125.159.0.26	233.18.158.253	UDP	Source port: 50000	Destination port: complex-m.
7539	8.543089	125.159.0.26	233.18.158.253	UDP	Source port: 50000	Destination port: complex-m.
7540	8.544208	125.159.0.26	233.18.158.253	UDP	Source port: 50000	Destination port: complex-m.
7542	8.554941	125.159.0.26	233.18.158.253	UDP	Source port: 50000	Destination port: complex-m.
7543	8.556059	125.159.0.26	233.18.158.253	UDP	Source port: 50000	Destination port: complex-m.
7544	8.557841	125.159.1.170	233.18.158.68	UDP	Source port: 50000	Destination port: complex-m.
7545	8.559147	125.159.1.170	233.18.158.68	UDP	Source port: 50000	Destination port: complex-m.
7546	8.560599	125.159.1.170	233.18.158.68	UDP	Source port: 50000	Destination port: complex-m.

# Channel changing

- IGMPv2 leave latency
  - RFC2236
    - 8.8. Last Member Query Interval The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. Default: 10 (1 second) This value may be tuned to modify the "leave latency" of the network. A reduced value results in reduced time to detect the loss of the last member of a group.
- Resolved with IGMPv3/MLDv2
  - Ability for **explicit tracking** (RFC3376) and zero leave latency
  - Can immediately stop forwarding upon leaves



# Example: KT IPTV

- Traffic stops almost immediately, although the 2<sup>nd</sup> IGMP group specific query has not been sent

출처: 본인 작성

7529	8.508187	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.113
7530	8.508192	118.48.34.143	233.18.158.68	IGMP	V2 Membership Report / Join group 233.18.158.68
7534	8.518970	61.72.223.167	233.18.158.113	IGMP	V2 Membership Query / Join group 233.18.158.113
8333	9.523908	61.72.223.167	233.18.158.113	IGMP	V2 Membership Query / Join group 233.18.158.113

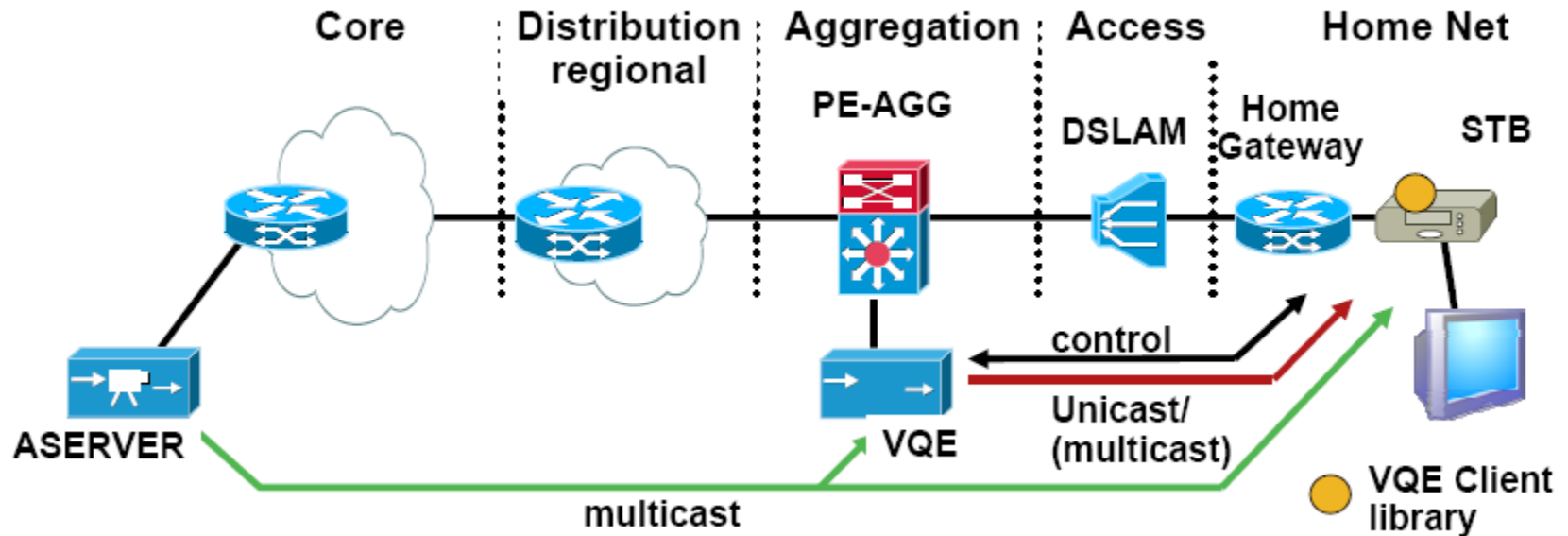
출처: 본인 작성

7520	8.488730	125.159.0.53	233.18.158.113	UDP	source port: 50000 destination port: complex-main
7521	8.491038	118.48.34.143	233.18.158.113	IGMP	V2 Membership Report / Join group 233.18.158.113
7522	8.498868	125.159.0.53	233.18.158.113	UDP	source port: 50000 destination port: complex-main
7523	8.499986	125.159.0.53	233.18.158.113	UDP	source port: 50000 destination port: complex-main
7524	8.502262	125.159.0.53	233.18.158.113	UDP	source port: 50000 destination port: complex-main
7525	8.504535	125.159.0.53	233.18.158.113	UDP	source port: 50000 destination port: complex-main
7526	8.505653	125.159.0.53	233.18.158.113	UDP	source port: 50000 destination port: complex-main
7527	8.506856	125.159.0.53	233.18.158.113	UDP	source port: 50000 destination port: complex-main
7528	8.508065	125.159.0.53	233.18.158.113	UDP	source port: 50000 destination port: complex-main
7529	8.508187	118.48.34.143	224.0.0.2	IGMP	V2 Leave Group 233.18.158.113
7530	8.508192	118.48.34.143	233.18.158.68	IGMP	V2 Membership Report / Join group 233.18.158.68
7531	8.516087	125.159.0.53	233.18.158.113	UDP	source port: 50000 destination port: complex-main
7534	8.518970	61.72.223.167	233.18.158.113	IGMP	V2 Membership Query / Join group 233.18.158.113
7537	8.532345	125.159.0.26	233.18.158.253	UDP	source port: 50000 destination port: complex-main
7539	8.543089	125.159.0.26	233.18.158.253	UDP	source port: 50000 destination port: complex-main
7540	8.544208	125.159.0.26	233.18.158.253	UDP	source port: 50000 destination port: complex-main

# GOP size and channel changing

- GOP size of N seconds causes channel change latency  $\geq N$  seconds
  - Can not start decoding before next I-frame
- Need/should-have channel change acceleration for GOP sizes  $> 0.5$  sec ?
- Unclear
  - How much bandwidth is saved in different codecs by raising GOP size (same quality)
  - Eg: WM9/AV  $\sim 2.5$  Mbps  $\rightarrow$  GOP size 3 sec
    - What bandwidth with 0.5 sec GOP size ?? Really 4 Mbps ?

# Video quality experience



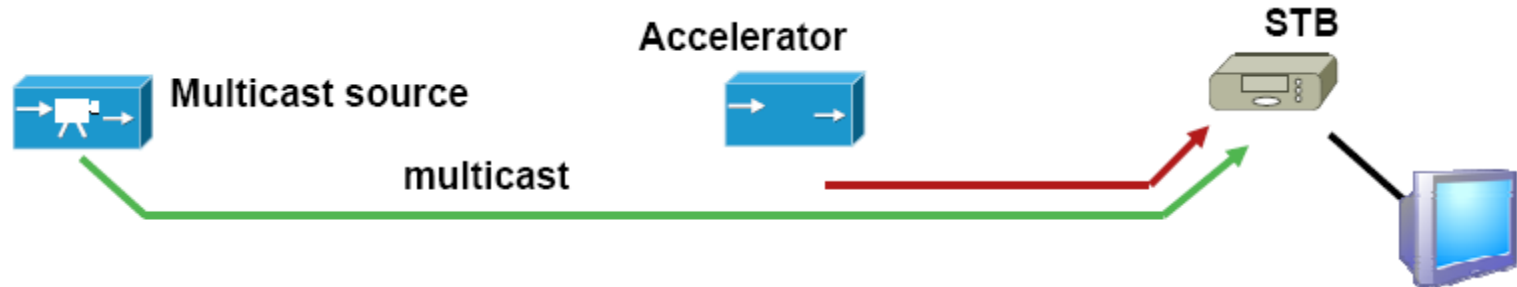
- Three functions (currently): Video Quality monitoring, FEC/ARQ support for DSL links, Fast Channel change
- Uses standards RTP/RTCP, FEC extensions
- Fast channel change by RTCP “retransmission” triggered resend of missing GOP packets from VQE (cached on VQE)

출처:

Cisco의 NANOG 발표 자료

"[http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride\\_ip\\_tv\\_N44.pdf](http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride_ip_tv_N44.pdf)"

# Channel change acceleration



- Idea: add an IPTV channel change acceleration element
  - Eg: “Instant Channel Change” in Microsoft TV IPTV edition
- Takeaway
  - MPEG broadcast/multicast alone can not provide fast channel change
    - IGMP join latency irrelevantly small compared to MPEG
  - With IP network at least flexible solutions are possible
    - As opposed to non-IP (eg: digital cable/satellite)
  - Value vs. cost ? (just small gop-size ?)
  - Acceleration could even hide whatever small IGMP join latency exists

출처:

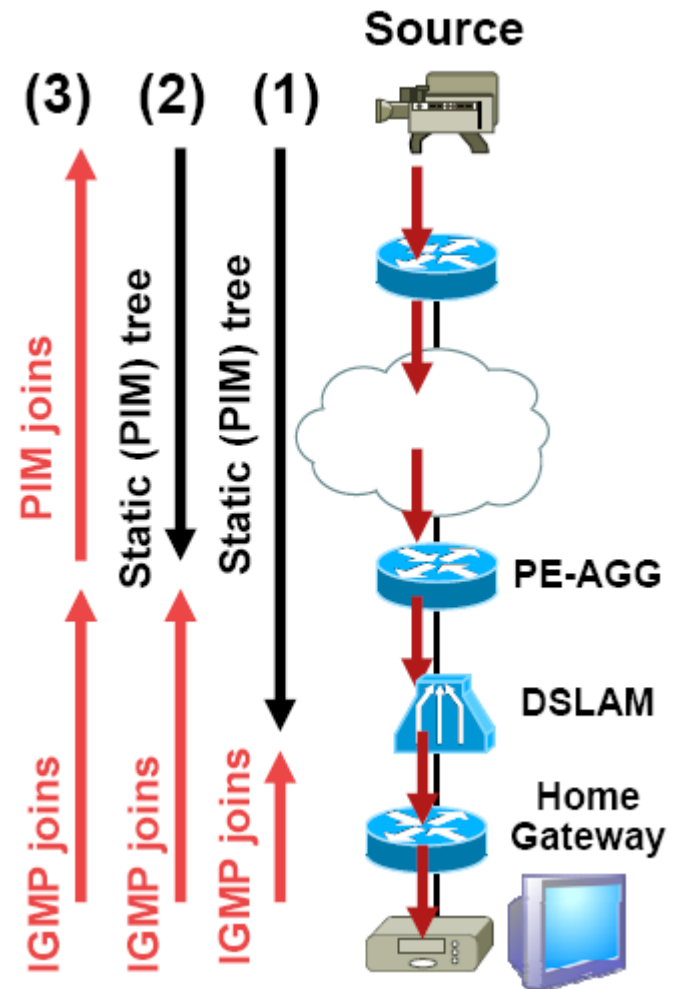
Cisco의 NANOG 발표 자료

"[http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride\\_iptv\\_N44.pdf](http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride_iptv_N44.pdf)"

# Join-latency

## Static vs. dynamic trees

1. “Broadcast Video”
  - Static forwarding into DSLAM
  - Fear of join latency
  - History (ATM-DSLAM)
2. “Switched Digital Video”
  - Allow oversubscription of PEAGG/DSLAM link
3. “Real Multicast”
  - Dynamic tree building full path



출처:

Cisco의 NANOG 발표 자료

"[http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride\\_ip\\_tv\\_N44.pdf](http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride_ip_tv_N44.pdf)"

# Switched digital video

- Consider 500...1000 users on DSLAM
  - Consider 300 available TV programs
- Run statistic how many TV programs are actually viewed in parallel
  - Numbers show often only 1/4 ... 1/3 programs maximum needed (eg: from Cable networks)
  - Dynamic joining between DSLAM/PE-AGG can allow to fit traffic into typical 1Gbps budget
- Dynamic joining towards core ?
  - Today's offered content  $\ll$  #users aggregated  $\rightarrow$  worst case traffic will always flow.
  - More a provisioning issue – and when content expands well beyond current cable-TV models

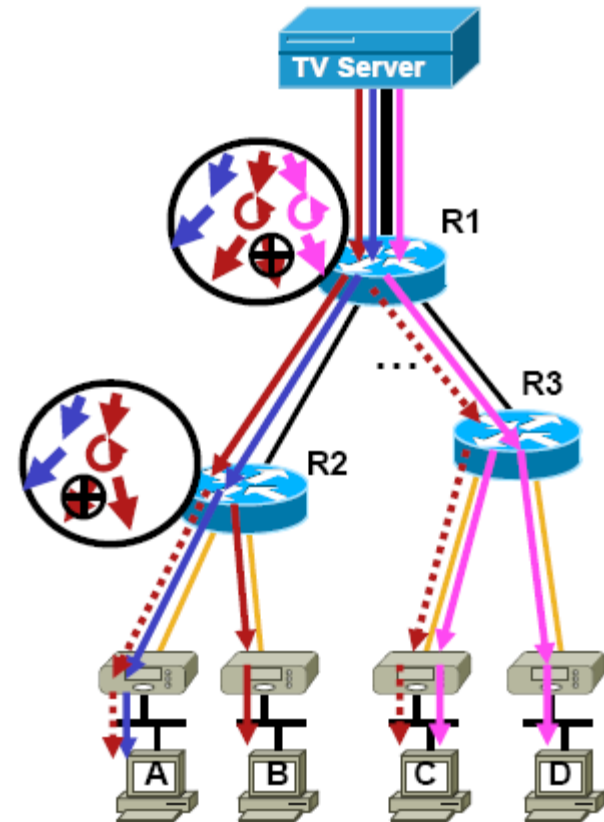
# Admission control

- Oversubscription (eg: PE-AGG/DSLAM link) raises question of admission control
  - Real-time !
  - One flow too many messes up everything
  - Vendor-specific: Router/L2-Device local config for per interface maximum# multicast flows
  - With more varying bandwidth (2.. 20Mbps) of TV programming, this may need to become bandwidth aware
    - Vendor specific: Local router CLI
  - Revive RSVP for multicast admission control, please !?!

# Multicast vs. Unicast

## Application side difference – Intserv admission control

- Intserv:
  - per flow (admission) control
- Unicast:
  - Source side enforcement!
  - No need for network enforcement
- Multicast:
  - Network enforcement!
  - Need to block forwarding at replication points to individual branches!
- Mechanisms:
  - Vendor specific..
  - RSVP only standardized common unicast/multicast solution eg: limit VoD+Bcast



출처:

Cisco의 NANOG 발표 자료

"[http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride\\_ipvtv\\_N44.pdf](http://www.nanog.org/meetings/nanog44/presentations/Sunday/McBride_ipvtv_N44.pdf)"



# IGMP snooping

- Performed by L2 switch
- A switch that does not IGMP snoop will, by default, flood multicast traffic to all the ports in a broadcast domain
- Passive mode: intended to be transparent
  - No messages suppressed
- Active mode: report suppression
  - Guess which IGMP reports are redundant at router (can break explicit tracking, fast leaves)

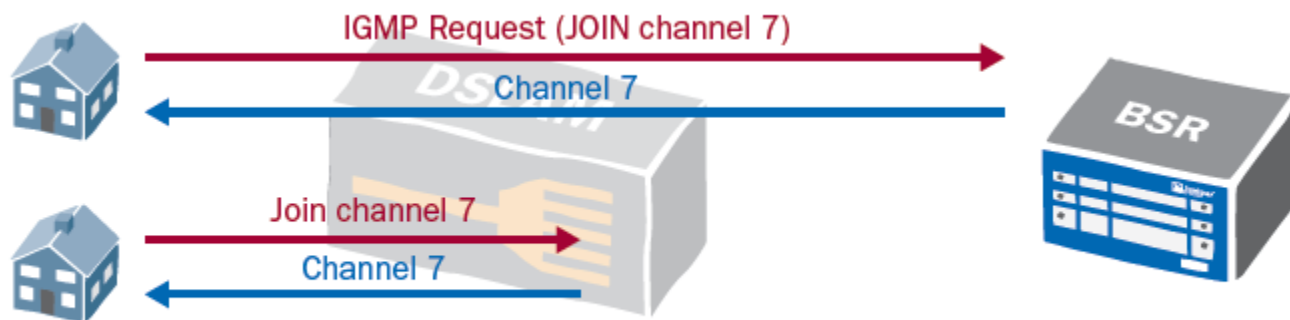


Figure 2: DSLAM with IGMP Snooping

# IGMP proxy routing

- IGMP proxy router need to act exactly like a single host on its upstream interface
  - Scalability is the key word

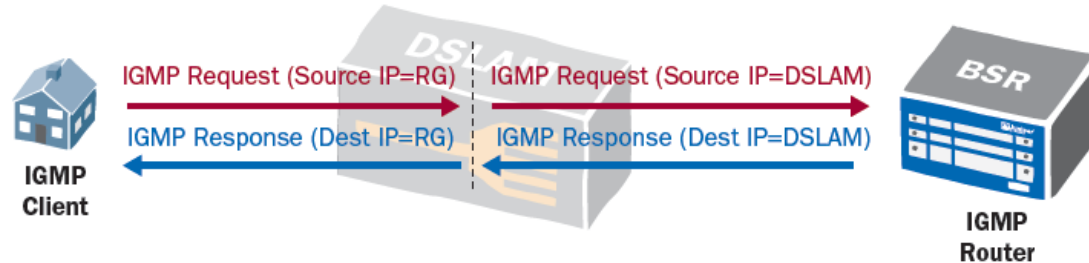


Figure 3: IGMP Proxy Routing

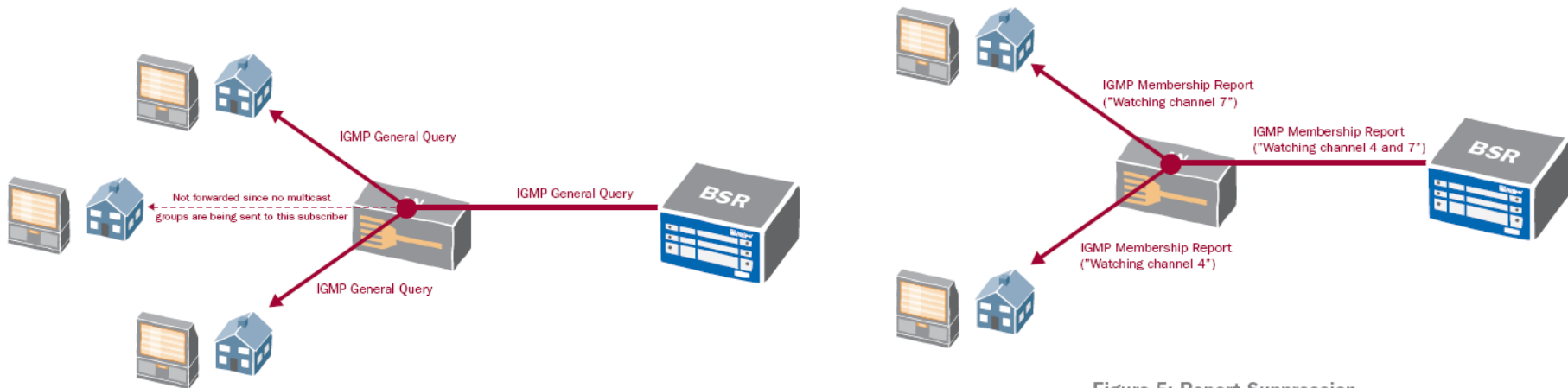
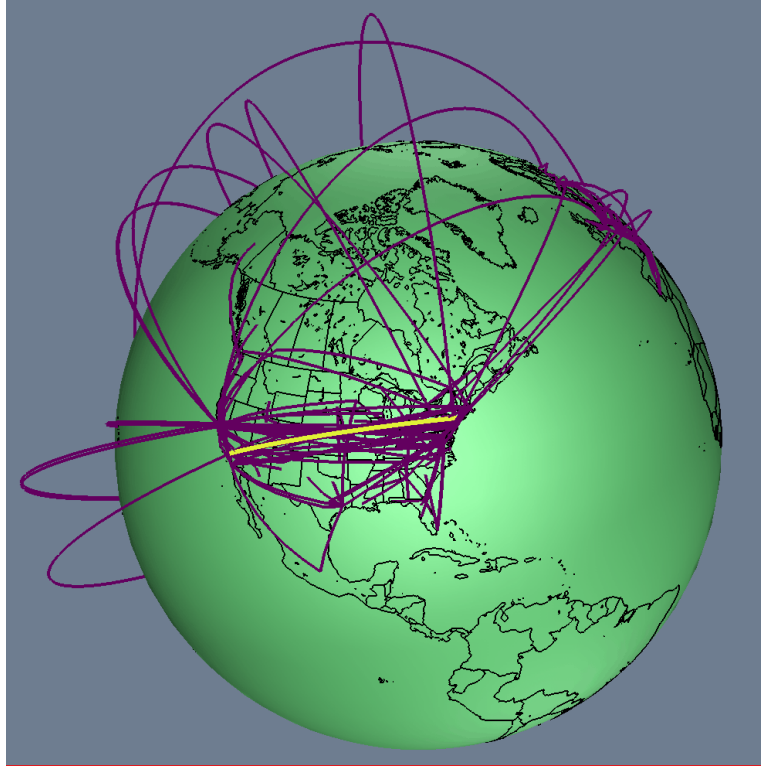


Figure 4: Query Suppression

Figure 5: Report Suppression

# Interdomain multicast

- MSDP
- MBGP
- Not presented here because they are not relevant to IPTV business model (for now at least)



**Q&A**