IGMP Snooping

Fulvio Risso

Politecnico di Torino

Based on chapter 8 of M. Baldi, P. Nicoletti, "Switched LAN", McGraw-Hill, 2002, ISBN 88-386-3426-2 and on an existing presentation of Mario Baldi and Piero Nicoletti

Copyright notice

Transmitting packets on a switched LAN

- Unicast
  - Only on the port toward the destination
- Broadcast
  - Flooding (Forward on every interface but receiving one)
  - Limited amount of traffic anyway
  - No other solutions
- Multicast
  - Flooding
  - What about delivering 50 courses in HDTV in real-time (20Mbps each)?
  - Scalability problems
  - Possible alternative: knowing member's location for each group

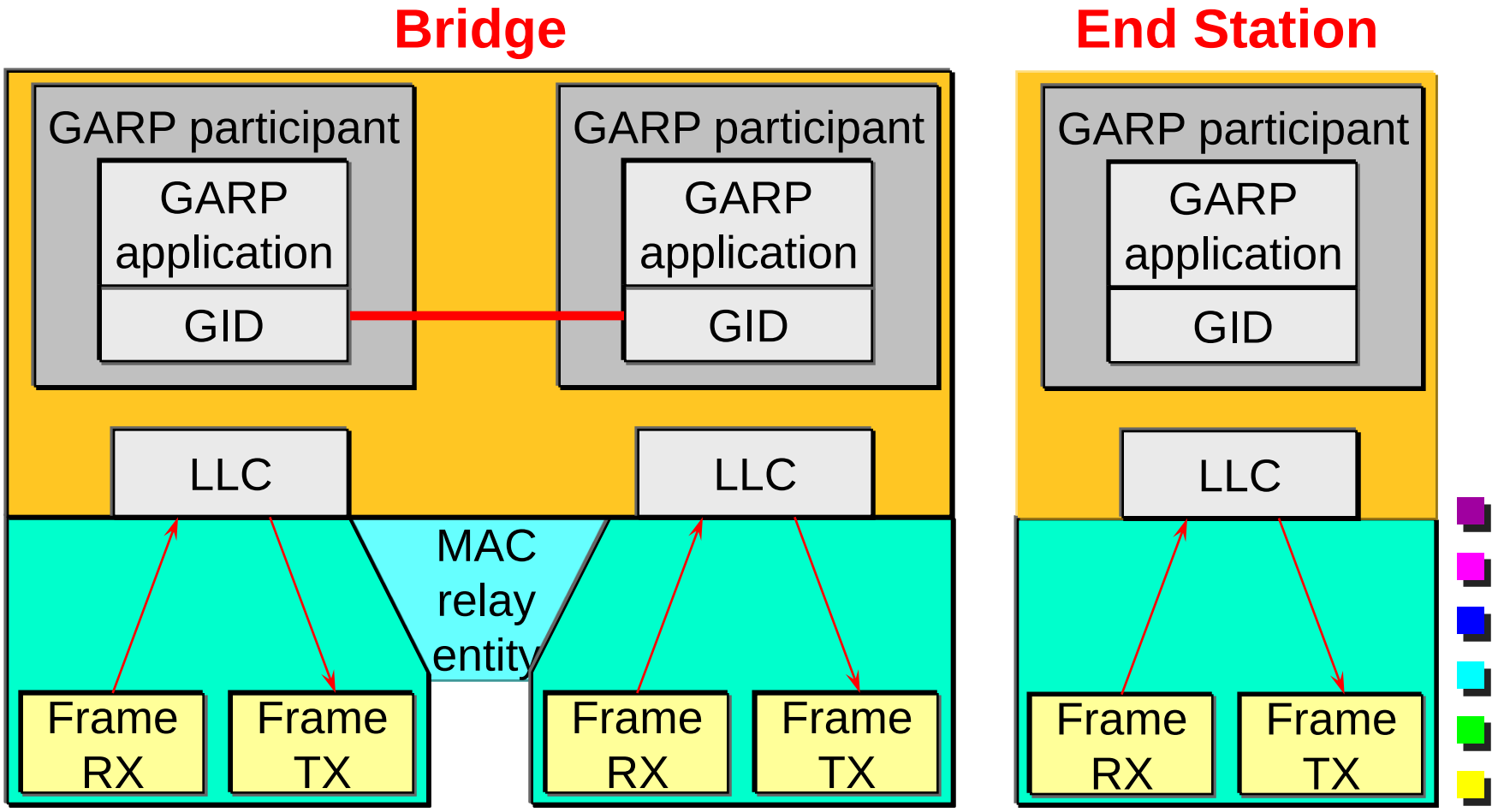
GMRP: GARP Multicast Registration Protocol

- GARP instantiation (Generic Attribute Registration Protocol)
  - GARP: meta-protocol that allows to register generic per-PC attributes in a VLAN
- Defined in IEEE 802.1D
- Allow
  - Station to communicate their membership group to the switch
  - Switch to communicate to adjacent switches from which group they must collect frames

GARP: details

- Insert or delete miscellaneous attributes in the internal entity of the device called GID
  - GID (GARP Information Distribution) is a finite state machine that defines the registration and declaration current state for each attribute's value
  - Attribute's registration or deletion takes place only in the port receiving the GARP PDU helding the declaration
    - Registration can take place in the ports that STP has Blocked
- GIP (GARP Information Propagation)
  - Entity responsible for information propagation between GARP Participant
    - internally in a single bridge
    - between different bridges (based on type 1 LLC)

GARP: entities and architecture

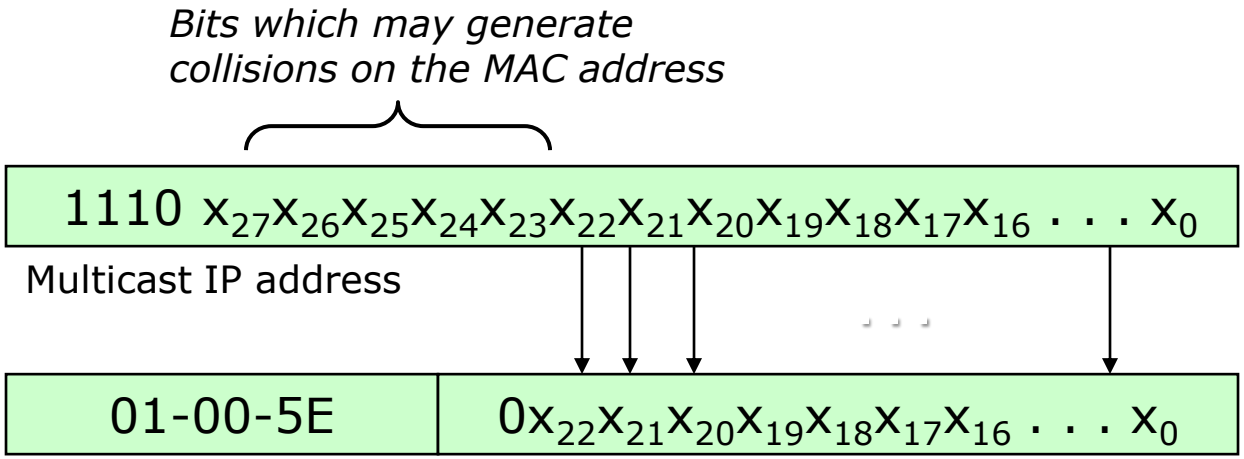


IGMP snooping: prelude

- GMRP barely used
  - Defined years ago, supported by most of switches
  - Not supported by applications/OS
  - Why should we complicate network operativeness and management with an additional protocol?
- The problem has already been solved in multicast IP
  - IGMP (Internet Group Management Protocol)
  - Multicast routing protocols
- Why should we define another mechanism?
  - Assuming that all the traffic is IPv4
  - IGMP is not a standard, but a commonly used technology

Mapping IP– MAC multicast on Ethernet

- A single multicast MAC address corresponds to 2^5 IP addresses

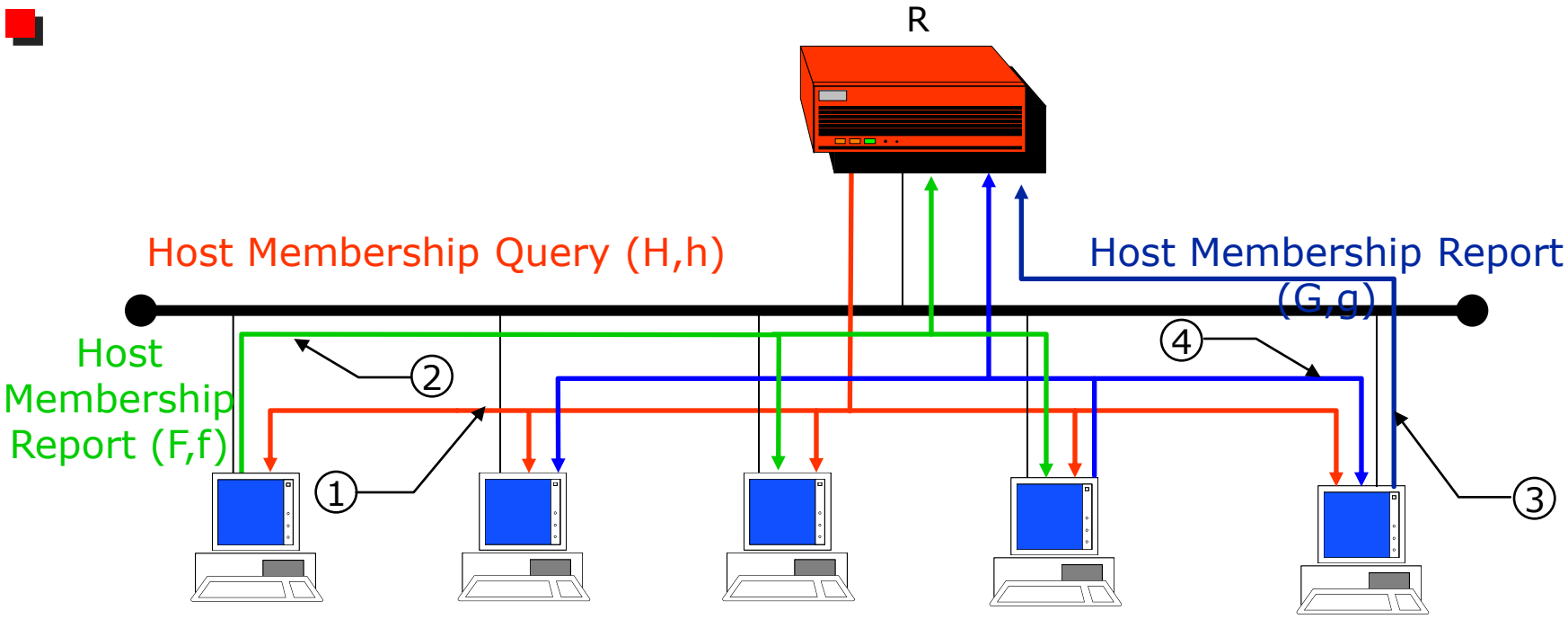


MAC addresses reserved by IEEE for IP multicast:
01-00-5E-00-00-00 - 01-00-5E-7F-FF-FF (addresses Global – Group)

IP multicast addresses

- Do not require IGMP
  - 224.0.0.0 - 224.0.0.255: Reserved for special “well-known” multicast addresses
- Do require IGMP
  - 224.0.1.0 - 238.255.255.255: Globally-scoped (Internet-wide) multicast addresses
  - 239.0.0.0 - 239.255.255.255: Administratively-scoped (local) multicast addresses

IGMP on traditional LAN



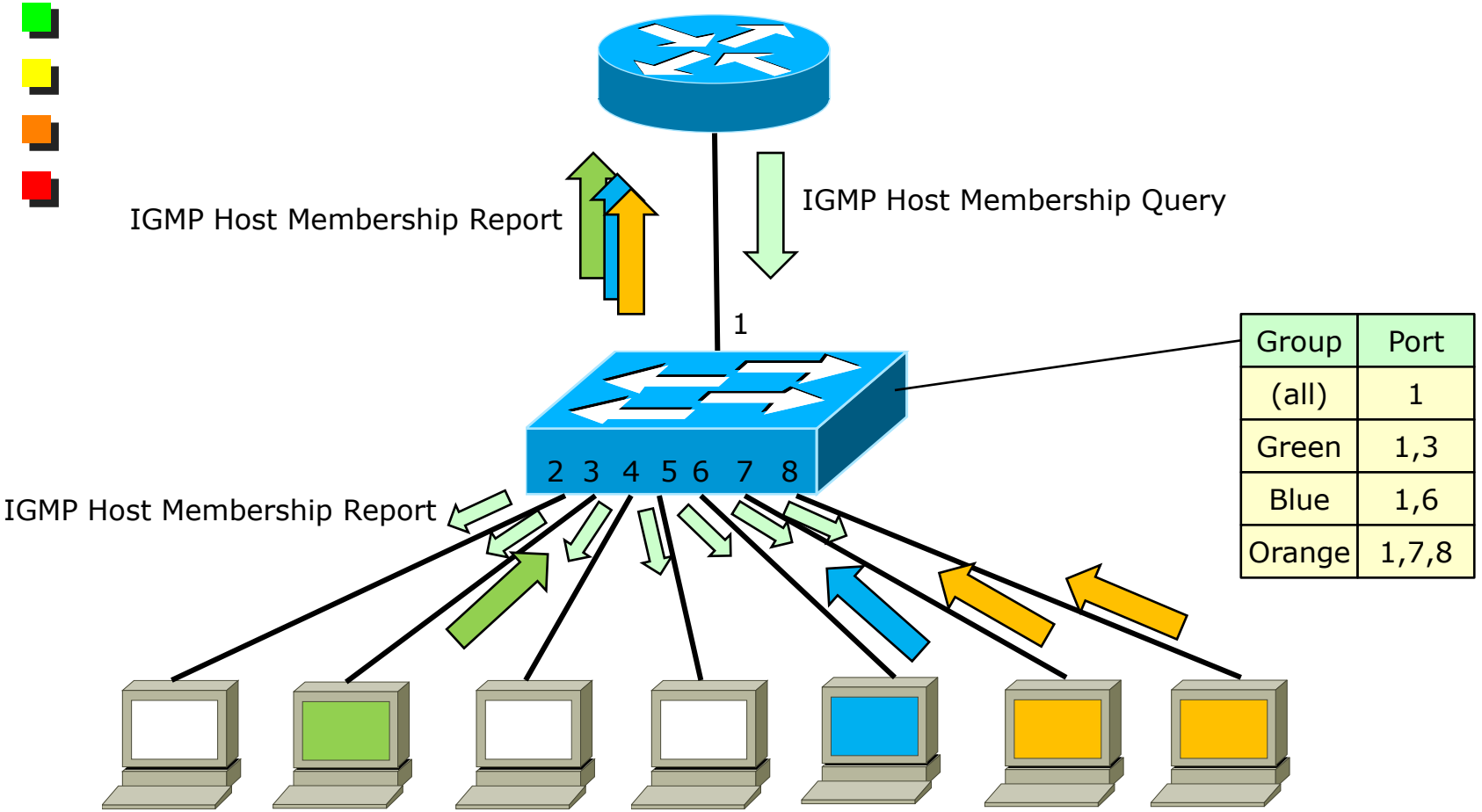
IGMP snooping: mechanisms (1)

- Switches must be able to distinguish between “well-known” multicast addresses and dynamic addresses
  - The first ones do not require IGMP
- Sending and receiving multicast packet must be preceded by
  - A message coming from the mrouter
  - The registration to the group identified by its IP address *G*
    - Send IGMP host membership report message
    - Transmitted in level 2 multicast frame addressed to multicast MAC *g* of IP address *G*

IGMP snooping: mechanisms (2)

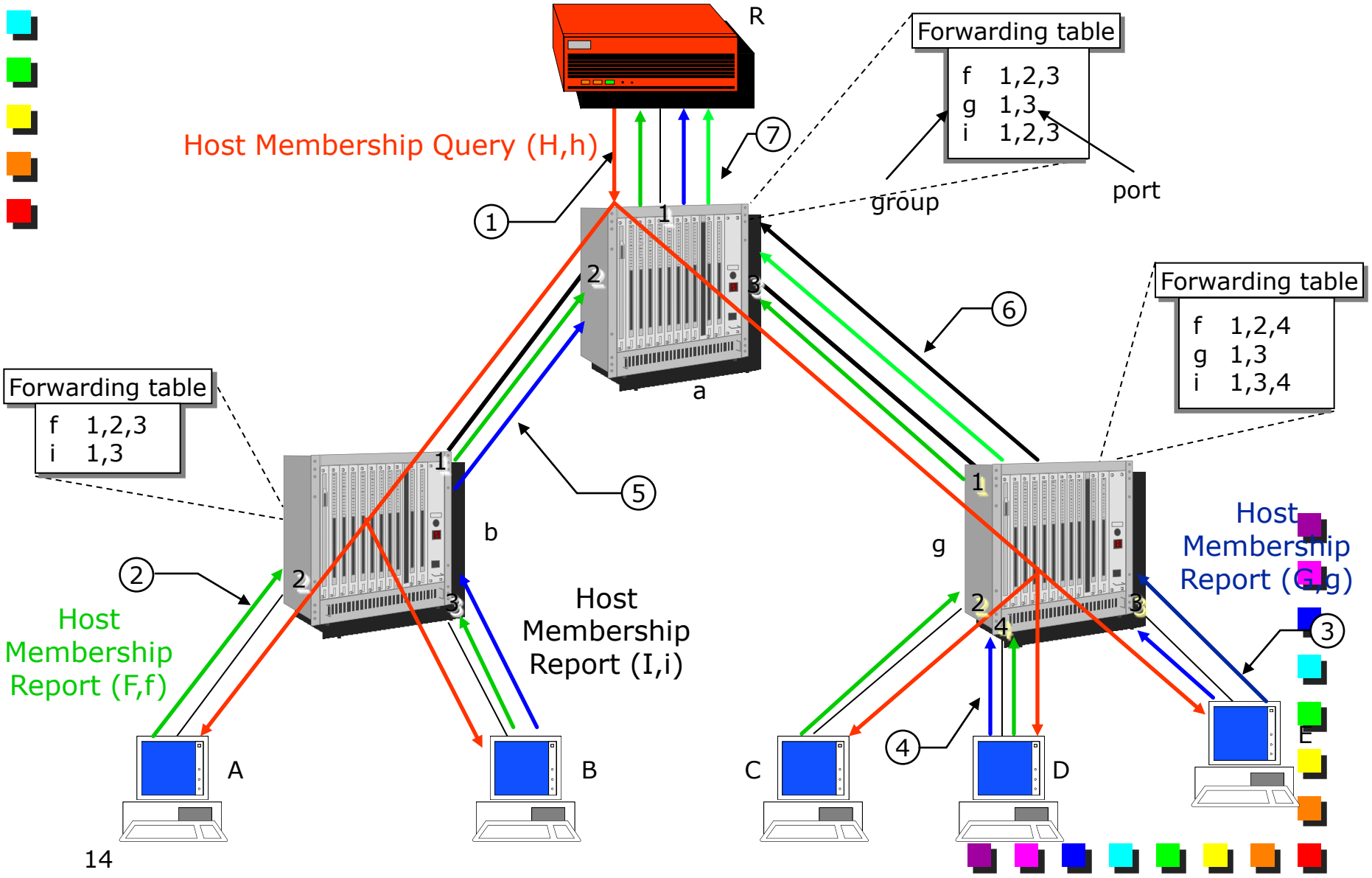
- Switches snoop
  - *Host membership query* messages
    - Learn which interface is toward the mrouter
  - *Host membership report* messages
    - Learn on which interfaces are currently members of group *g*
- Update their multicast forwarding tables
- Send one HMR message on the "uplink" toward the mrouter
  - This message is not propagated on other interfaces in order to be able to discover all the listeners

IGMP snooping on a switch



Group	Port
(all)	1
Green	1,3
Blue	1,6
Orange	1,7,8

IGMP snooping on a switched LAN



Forwarding of multicast packets

- Well-known addresses
  - Forwarded on all the ports (flooding)
- Dynamic addresses
  - Forwarded only to the ports set in the multicast table

Conclusions

- Not a standard, but works smoothly
  - Although it is a violation of the OSI model
    - Switches are required to recognize also part of the IP
- Be careful to IPv6 and other L3 protocols
  - In this case, the only option is to disable IGMP snooping