IGMP v2/3 & IGMP Snooping
analysis of messages and hands-on

Clement Duval
Senior Field Application Engineer
IGMP & IGMP Snooping Agenda

- IGMPv2: where, why and how?
- IGMPv2 messages explained with drawings
  - Hands On labs
- IGMP snooping and proxy reporting explained with drawings
  - Hands On labs
- IGMPv3 theory and hands-on
IGMP messages

• Stands for **Internet Group Management Protocol**

• Is the standard for joining, maintaining & leaving groups, between a Multicast Router (Source) and hosts on the network.

• IGMP is a transport layer (Layer 4) inside IP (Layer 3), alongside UDP, TCP and ICMP.
  • Like UDP and ICMP, it is not reliable transport, can be lost and not recovered
  • IGMP is only a receiver concept, sender are never involved in IGMP
IGMP Messages

- IGMP is activated on a router by activating PIM protocol on the interface:
  - (config-if)#ip pim sparse-mode

- The end hosts joining the groups must speak and understand IGMP.
  - Windows: RegEdit to support IGMPv2 or v3 (by default)
  - Linux: /proc/net/dev_mcast, /proc/sys/net/ipv4/, netstat –ng4
IGMPv2 Membership Reports (aka Join)

- Sent from host to Router, using Multicast (MC) address to be joined (ex. 239.1.1.1)
  - The IP packet carries IGMP (transport layer 4)
  - Not reliable transport (packet can be lost)

```
• Command on router to join a group: intf# ip igmp join-group 239.1.1.1
```
IGMPv2 Leave Message

• Host notifies the “upstream router” that it no longer wishes to receive the group.

• Such a message is generated when you:
  • Close VLC or TSReader Pro
  • Remove IP Input settings in DR5000 or TITAN LIVE (probe ends)

• The “upstream router” just wants to know that at least one host was interested in a group, he doesn’t care how many.

• The Switch uses “leave” messages to remove entries in the IGMP Snooping table.

• Uses 224.0.0.2: “all Routers” group address
IGMPv2 Leave and Group Specific Queries (GSQ)

- Multicast Router doesn’t keep track of who and how many hosts are interested in group 239.1.1.1

- Once “last member” has sent a leave, he makes sure that no one else is interested in 239.1.1 in the LAN

- The command “ip igmp immediate-leave” allows to bypass this leave process
IGMPv2 General Queries (GQ)

• A “Querier” device sends periodic Queries to all hosts on (V)LAN asking the what they are interested in.
  • This ensure to maintain groups and detects those host that silently crashed (i.e w/o sending leave)

• In response to GQ Hosts should respond within predefined time with a “solicited join”

• If not, the host’s LAN segment may be discarded from MC forwarding.

No Querier on the (V)LAN = No IGMP Snooping = MC flooded everywhere!
IGMPv2 General Queries (GQ) : Querying device

• Querier can be external ( Router)
  • Most common case when stream are coming from a big networks where traffic are routed between different networks.
  • The Router sends the GQ to all host inside the LAN
  • IGMP querier settings are made on the Router’s interface connected to LAN
    • Ip PIM Sparse-mode activated in the interface
    • Ip multicast-routing enabled globally.

• Querier can be internal to the switch ( “Snooping Querier”)
  • Small lab environment where sources and receivers are in the same “layer2 network”
  • The Switch sends the GQ to all hosts inside each LAN or VLAN.
  • Querier must be activated globally , per VLAN and with an IP source address :
    • IP igmp snooping querier
    • IP igmp snooping querier vlan 1 address 172.16.1.1
IGMPv2 General Queries (GQ) and solicited Joins

- GQ sent to 224.0.0.1 (all system address)
- Hosts respond with Group Specific message within max_response_time

Host’s random timer fell to 0.23sec

```
ip igmp query-interval 30
ip igmp query-max-response-time 2
```
IGMPv2 General Query: Max Response Time

- With many hosts interested in many groups, having all hosts responding to GQ at the same time would induce traffic peak and packet loss.

- The Querier indicates to the hosts the **maximum time they can take to respond to a GQ**

- Host send their response back after expiring a **random timer** (default 10sec)

- The Max Response time being in response to Solicited queries, it therefore doesn’t **impact the initial “Join latency”**.

- However a high “**max response time**” will increase the time between when a host dies and when it will be removed from the snooping table or Router’s forwarding table.
IGMPv2 General Query: Report suppression

• Scenario:
  • HOST 1 is interested in 239.1.1.1 and has joined this group
    • It receives a GQ and his random timer expires at 2 sec
  • Host2 is also interested in 239.1.1.1 and has joined this group
    • It receives a GQ and his random timer expires at 3 sec

• If HOST 1 and HOST 2 are on the same segment, (with no Snooping Switch in between them), then Host 2 will see the Join coming from Host1 1 sec before Host 2 is supposed to send it

• Host 2 will suppress its Join since Host 1 already Joined on behalf of the entire network

• This feature is called Report suppression and is by default on all IGMP capable devices.

• Therefore, you may not see that your device sends a Join on the network if your host has seen a Join from someone before he is supposed to send.
IGMP Snooping

• is a **mechanism** for optimizing bandwidth utilization when a switch is placed between querier and hosts.

• The Switch “snoops” into the transport layer to read the IGMP messages

• When the switch sees that an IGMP Join has arrived from Port X for group 239.1.1.1, it will make sure to forward 239.1.1.1 to Port X.

• When the switch sees that an IGMP Leave has arrived from Port X for group 239.1.1.1, it will make sure to STOP forwarding 239.1.1.1 on Port X.

• IGMP Snooping is only **Port based** (not MAC/ or source IP based)
IGMPv2 Snooping : General Queries

• The Switch Automatically detects the presence of the Querier by “snooping” the IGMP GQ inside 224.0.0.1

Show ip igmp snooping querier

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>IGMP Version</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.1.10.254</td>
<td>v2</td>
<td>Et0/0</td>
</tr>
</tbody>
</table>

No Querier = No general Queries = No IGMP Snooping = Multicast flooded everywhere !
IGMPv2 snooping : the “Querier port”

- The Switch sniffs the GQ inbound and declares “Querier port” where these GQ are coming in.

- The switch forwards any join / leave to this port and only to this port (with snooping activated).

- If more than one Querier is present in the network, an election takes place and the Querier with the highest source IP address *(Non Designated Querier)* ceases to send QG until it stops hearing from the election winner *(designated Querier)* for a configuration timeout.

- Each Switch has only one Querier port per VLAN and at a given time.
IGMPv2 Snooping: The Multicast Router port (mrouter)

• The Switch Automatically detects the presence of the Multicast Router using the PIM packets (used for Multicast routing and which come with the IGMP packets)

• When external Querier is used, Mrouter port and Querier should be the same

• The Mrouter port will always forward all the Multicast Traffic which transits through the switch’s VLAN (except the MC data coming from the Mrouter port itself)

• This Mrouter port is used since Multicast Data generated locally will are likely to be forwarded upstream to the Multicast Router and to the outside world.
  • Could be considered as the “default gateway port” for MC

• In a “snooping querier config” you may not see a Mrouter port or it is set as “switch”
**IGMPv2 Snooping : what is it ?**

- The switch usually operates at Layer 2 reading source MAC addresses coming into its port and populate its Mac address table to appropriately forward future frames.

- An “IGMP snooping” capable (layer3) switch will “snoop” into the IGMP transport Layer 4 in order to read the IGMP “type” field:
  - General Query
  - Membership Report
  - Leave

- Based on this, it will populate its “multicast Snooping table” and ensure future Multicast data streams are forwarded on the ports where interested receivers have sent their joins.

- Turn on IGMP snooping globally on a Cisco Switch (by default, it is enabled globally and for all VLANs)
  - `(config)#ip igmp snooping vlan 10 (for VLAN 10 only)`
  - `or (config)#ip igmp snooping (for all VLAN)`
IGMPv2 Snooping: Membership Reports

- Membership reports tell the switch **what ports** the MC traffic should be forwarded on
- They populate the **IGMP snooping table**
- `#Show ip igmp snooping groups`

```
<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group</th>
<th>Version</th>
<th>Port List</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>224.0.1.40</td>
<td>v2</td>
<td>Et0/0</td>
</tr>
<tr>
<td>1</td>
<td>225.1.1.1</td>
<td>v2</td>
<td>Et1/2</td>
</tr>
<tr>
<td>1</td>
<td>225.1.1.2</td>
<td>v2</td>
<td>Et1/2, Et1/3</td>
</tr>
<tr>
<td>1</td>
<td>225.1.1.3</td>
<td>v2</td>
<td>Et1/2</td>
</tr>
</tbody>
</table>
```

- Possible to statically join a port for troubleshooting or interop purposes:
  - `(config)#ip igmp snooping vlan 1 static 239.1.1.1 interface e1/3`
IGMPv2 Snooping : proxy reporting

• The Multicast Router only needs a single Join and/or leave to decide to continue or stop forward the stream inside the LAN.

• Having this goal in mind, the “snooping Switch” will make sure to filter out IGMP report/Leave so that only the necessary messages are transmitted to the Multicast Router. (thus the name “proxy”)

• If two hosts join a group: only the first one will be forwarded to the Querier port.
• If one host leaves a group but the Switch knows that some others hosts in the LAN are still interested in this group, the Switch doesn’t forward the leave to the Querier port.
• If one host leave a group on a port, the Switch will take over on the role of “last-member-querier” previously performed by Router (e.g. when a HUB was used instead of a Snooping Switch)
  • In that case, the Switch will use GSQ with source address as 0.0.0.0.

Proxy reporting implementation may depend on vendors and FW versions.
Interaction between IGMP Snooping and Spanning Tree

By default IGMP Snooping forwards MC stream only to ports where there are interested receivers.

- In a network with spanning tree activated, any switch port that don’t have the Portfast feature activated will generate a Topology Change notification (TCN) when the port goes UP or DOWN at layer 1
  - It tells the network that “something has happened somewhere” and that they should temporarily flood their traffic on their ports to avoid that anyone in the network miss an important and unidirectional data (ex. UDP)

- Like in Unicast Flooding, when a switch running IGMP Snooping receives such a TCN from other switches, it will also **temporarily flood** the multicast traffic into of all of its ports.

- This may cause interface overload, packet loss and other unexpected results due to overload.

**To solve this:**

- Make sure all your edge ports are set to “port fast”, including trunk ports to Servers (not trunk port to Switches!)
- Try to find out who in the network is originating these TCN (port flapping)
- Set “no ip igmp snooping tcn flood” on all your interfaces, which instruct the switch port to not flood traffic when it receives a TCN.
IGMPv2 versus IGMPv3

- **IGMPv2**:
  - Any Source Multicast (ASM)
  - It joins \((*,G)\) = Groups
  - Switch forwards \((*,G)\) from any source
  - If two senders sending multicast on the same group
    - Collision = contiguous CC errors in Video
  - Advantages:
    - Everybody support it

- **IGMPv3**:
  - Source Specific Multicast (SSM)
  - It joins \((S,G)\) = Channels
  - Advantages:
    - Provides stream protection:
      - Two sources can send on same group, but from on different channels
      - Receivers needs to know the source address (out-of-band directory)
    - Greatly simplifies Multicast routing
    - Good for “MC source redundancy” along with OSPF / PIM
IGMPv3: (S,G) Join message (SSM)

- All joins are sent on 224.0.0.22 (Well-Known MC reserved for IGMPv3)
  - No more one destination addressee per group like in IGMPv2

- One IGMP message can carry multiple channels

- “Group Record” Field = Destination group
  - Each Group Record can contains 0 or more Sources

- Source + Group = Channel = (S,G) state
IGMPv3: Group Record Type

• It is the mode that tells the Router (or Snooping Switch?) **how to read** the “Membership report” group records.
• The mode is **per Group Record** (per Multicast destination)
• **MODE_IS_INCLUDE**:  
  • I request the group but only for the list of sources provided, usually from solicited Join
• **MODE_IS_EXCLUDE**:  
  • I request the group for all source except the sources listed, usually from solicited Join
• Change the filter mode:  
  • **CHANGE_TO_INCLUDE_MODE**:  
    • I change the mode to Include to reset the current state, usually from unsolicited Join
  • **CHANGE_TO_EXCLUDE_MODE**:  
    • I change the mode to Include to reset the current state, usually from unsolicited Join
• **Operations on Source list**:  
  • **ALLOW_NEW_SOURCES**:  
    • I add new sources to the group records
  • **EXCLUDE_NEW_SOURCES**:  
    • I exclude new sources from the group records
  • **BLOCK_OLD_SOURCES**:  
    • I block the previous sources I was interested to add new ones
IGMPv3: (S,G) Join message (SSM)

- Joins are sent on 224.0.0.22 (Well-Known MC reserved for IGMPv3)

Mode is “Include” for the group record 239.1.1.1, it will therefore ask to receive the two channels below:

(S1,G) = (192.168.1.1,239.1.1.1)
(S2,G) = (192.168.1.2,239.1.1.1)
IGMPv3: Join (*,G) message (ASM)

- Joining group 239.1.1.1 from any source = excluding Zero Sources from this Group
IGMPv3: Query message

- Also sent on All system Multicast 224.0.0.1

Same as IGMPv2

Query Robustness variable:
how long before router considers a host leaving the group
IGMPv3: Record Type on solicited Join

- In response to Solicited Join, host sends join in “Mode is Include”
- “Mode is Include” since solicited join is made to preserve the current state
IGMPv3: Record Type on unsolicited Join

- When host first joins a channel (at bootup?), join’s record Type set to “change to include mode”
  - Because unsolicited joins are made to reset the current state (in case the router was in an exclude mode before)
IGMPv3: Record Type Block Old Sources

- Removing 192.168.2.2 from to an existing source list within Group Record 239.1.1.1

**Host sends “blocks all sources” from Group record**

**Router sends GSQ + “Group-source-Specific query to make sure no other host is interested in this Group Record”**

**Host joins new Group Record With new source list**

**Router verifies that no other host was interested in the removed channel**
IGMP Snooping Misc

- **IGMP snooping** not being a standard (RFC Informational), it may varies from vendors and from platform versions.

- The IP allocated to the devices’ interfaces joining multicast group don’t matter, they can be in completely different subnets: IGMP and IGMP Snooping isn't based on Unicast addressing.

- IGMPv3 snooping hasn’t proven to work in a very limited way on common Cisco switches, it seems most of them on the market only do snooping based on (*,G) and not on (S,G).

- A host receiving IGMPv3 GQ, will respond with IGMPv3 Join.

- If the host doesn’t support IGMPv3, it should understand the GQ and respond with IGMPv2.

- “Show run all | inc IGMP” to show all the default settings not displayed in regular “show run”
IGMP & IGMP Snooping Misconceptions

• IGMP & IGMP Snooping have nothing to do with UDP or TCP (Layer 4 transport)

• IGMP Snooping has nothing to do with ARP and MAC address

• “Generating an IGMPv3 video stream” doesn’t mean anything
  • Spoofing the Multicast source may only indicate that SSM may be chosen for source redundancy

• IGMP and Multicast don’t travel across different VLAN
  • Querier/join/leave and Multicast Data stay on their VLAN.

• Multicast senders don’t have anything to do with the IGMP mechanisms

• It is not (easily) possible to see a Multicast source on a Snooping switch, we only see interested receivers. On networks other than local labs, assume the MC are coming from the Mrouter port.
Ressources

- IGMPv2:
  - https://www.youtube.com/watch?v=GGqcwDW1a8
  - https://www.youtube.com/watch?v=BC8MfzMSRhY
  - https://www.youtube.com/watch?v=5-h5LNT6DqM&t=894s

- IGMPv3:
  - https://www.youtube.com/watch?v=Sgppv6HRFSs

- IGMP snooping :