Introduction to IGMP Snooping

IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. If the switch does not run IGMP snooping, it broadcasts multicast packets at Layer 2. However, if IGMP snooping is enabled, switch forwards multicast packets only to specified host ports based on the Layer 2 multicast forwarding table.

IGMP snooping is a basic Layer 2 multicast function that forwards and controls the link layer multicast data. IGMP snooping runs on a Layer 2 multicast device and analyzes IGMP messages exchanged between a Layer 3 device and hosts to set up and maintain a Layer 2 multicast forwarding table. The Layer 2 multicast device forwards multicast packets based on this Layer 2 multicast forwarding table.

After a Layer 2 multicast forwarding table is set up, the Layer 2 multicast device searches the multicast forwarding table for outbound ports of multicast data packets according to the VLAN IDs and destination addresses (group addresses) of the packets. If there is an outbound port for the multicast data packet, the Layer 2 multicast device forwards the packet to the corresponding multicast group member port. If no outbound port is found, the multicast data packet will be dropped by the Layer 2 multicast device. However, the Layer 2 multicast device will forward the unknown multicast packet to the other router ports if there are other router ports other than the one on which it is received.

For more information about IGMP snooping, please refer to RFC 4541.

NOTE:

- PICOS supports IGMP snooping of IGMPv1, IGMPv2 and part of IGMPv3. However, PICOS supports IGMPv3 snooping without considering the additional "include source" or "exclude source" filtering in the packets. For example,
  - When receiving an IGMPv3 snooping report message, the switch parses the packet and records the member port and the multicast group as a Layer 2 forwarding entry without parsing and recording the particular source information.
  - When receiving an IGMPv3 snooping general query packet, the switch parses the packet and records the corresponding router port information. The original packet is then forwarded.
- The report message from the downstream hosts will be treated as IGMPv3 message only when the destination address is 224.0.0.22.
- If the report message from the downstream hosts is IGMPv3 message (Type value is 0x22), but the destination address in the message is not 224.0.0.22, PICOS will not record this member port to the Layer 2 forwarding table.
- In L2/L3, IGMPv2/IGMPv3 Snooping and IGMPv2 Snooping Querier are both supported.
- When the switch receives an unknown multicast, it will forward the data packet to the router port. The unknown multicast data packet refers to multicast data packets that do not exist in the IGMP snooping forwarding table.