Multicast

Maria Pais
up202308322@up.pt
MERSI
Faculdade de Ciências (FCUP)
Universidade do Porto

Mónica Araújo
up202005209@up.pt
MERSI
Faculdade de Ciências (FCUP)
Universidade do Porto

Patrícia Miranda
up202007675@up.pt
MERSI
Faculdade de Ciências (FCUP)
Universidade do Porto

***Abstract*—In contemporary network communications, multicast technology emerges as a pivotal mechanism for the efficient broadcast of data from a single source to a plurality of recipients. Using GNS3 for network topology and Wireshark for traffic analysis, this study delves into the configuration and functionality of multicast routing protocols such as PIM, and IGMP. The network setup, consisting of two routers and a PC, demonstrates the effective dissemination of multicast traffic, with a focus on the establishment of PIM Sparse Mode and the configuration of Rendezvous Points. This abstract synthesizes the methodology, results, and prospective scope, highlighting multicast's significant yet intricate role in network resource optimization and scalability.**

***Index Terms*—Multicast, IGMP, PIM, GNS3, Wireshark, OSPF**

I. Introduction

In the ever-evolving landscape of network communications, *Multicast technology* stands out as a cornerstone for efficiently disseminating information from a single source to multiple destinations. Contrary to *unicast* transmission, where a direct connection is formed between the sender and the receiver, *multicast* allows for the simultaneous delivery of data packets to a collective group of recipients.

This method proves indispensable in applications requiring real-time data distribution across diverse sectors, including video conferencing, live content streaming, and high-frequency trading platforms.

However, there are certain difficulties in putting multicast technology into practice. The complexity of multicast protocols, coupled with issues of scalability and dynamic group management, requires a deeper examination to unlock their full potential.

This report delves into the intricacies of multicast technology, beginning with a comprehensive overview of the multicast protocols that facilitate its implementation. The discussion is organized into two main sections: Layer 3 and Layer 2 multicast protocols. At Layer 3, we examine pivotal protocols such as the Multiprotocol Border Gateway Protocol (MBGP), Protocol Independent Multicast (PIM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), and Source Specific Multicast (SSM). The exploration extends to Layer 2 protocols, including IGMP snooping, MLD snooping, PIM snooping, and Multicast VLANs, outlining each protocol's functionality and its role in enhancing multicast routing efficiency.

Beyond the technical descriptions, the report highlights the numerous advantages multicast technology offers, from enhanced network efficiency to the economization of bandwidth and resources, which are essential for supporting distributed applications at scale. Alongside the benefits, the document does not shy away from addressing the significant challenges associated with multicast routing, providing a critical analysis of the hurdles faced in deploying multicast technology effectively.

The objectives of this project are outlined to set the stage for a detailed exploration of multicast protocols through practical experimentation and simulation. Essential tools and components, including the GNS3 network simulator and the Wireshark packet analyzer, are introduced as the foundational elements of our demonstration setup. The subsequent demonstration section offers a practical perspective on configuring and observing multicast traffic flows, providing tangible evidence of the concepts discussed.

This research culminates in Section VI, establishing the foundation for forthcoming explorations and potential advancements in our ongoing investigation into multicast technology.

II. Description of the technology

Multicasting refers to a communication network's ability to accept a single message from an application and deliver copies of that message to many recipients in different places. One of the issues is reducing the amount of network resources used by multicasting.

During a Multicast transmission, the transmitter sends the data packets only once, leaving it up to the receivers to pick up this transmission and reproduce it. This technique considerably reduces traffic in various situations, such as when several clients are watching a soccer match being broadcast by a server.

A. Multicast Protocols Overview

1) ***Layer 3 Multicast Protocols****:* Layer 3 Multicast refers to IP multicast operating at the network layer.
Before introducing the protocols, there are some concepts we need to know.

Multicast group management protocols run between hosts and Layer 3 multicast devices that directly connect to the hosts to establish and maintain multicast group memberships.

Multicast routing protocols are used on Layer 3 devices to construct and maintain multicast routes and efficiently forward multicast packets. Multicast routes are loop-free data transmission paths connecting a data source to numerous receivers. Multicast routes in the Any Source Multicast (ASM) model are classified as intra-domain or inter-domain.

An intra-domain multicast routing protocol identifies multicast sources and creates multicast distribution trees within an Autonomous System (AS) to distribute multicast data to recipients.

An inter-domain multicast routing protocol is used to transfer multicast data between two ASs.

In figure 5 we can see where each protocol works.
The following protocols will be discussed:

- **Multiprotocol Border Gateway Protocol (MBGP)**: Multicast routing protocol MBGP is an extension of the Border Gateway Protocol (BGP) that allows multiple types of addresses to be distributed in parallel. Unlike BGP, MBGP supports IPv4 and IPv6 addresses, and it supports unicast and multicast variants of each.
  For a network, the topology for multicast may differ from that for unicast. To distinguish between them, the MBGP protocol allows BGP to convey both unicast and multicast Network Layer Reachability Information (NLRI) separately. The multicast NLRI only supports reverse path forwarding (RPF). As a result, route selection for a destination via the unicast routing table and the multicast routing table produces distinct results, ensuring consistent unicast forwarding and normal multicast between domains. [15] [16]
- **Protocol Independent Multicast (PIM)**: Multicast routing protocol PIM is a protocol that facilitates one-to-many and many-to-many distribution of data over the local multicast routers and sender routers. The term "protocol-independent" refers to its ability to operate without its own topology database, relying instead on routing information given by other unicast routing protocols. This design allows PIM to work alongside any existing unicast routing protocol in use on the network, as it doesn't have direct dependencies and can adapt to the network's routing environment seamlessly. There are four variants of PIM: PIM Dense Mode (PIM-DM), PIM Sparse Mode(PIM-SM), Bidirectional PIM (Bidir-PIM) and PIM Source-Specific Multicast (PIM-SMM):

  – PIM-DM is considered an implicit join, it's based on a "flood and prune" behavior for building the shortest path trees. It operates by flooding the multicast traffic for all the enabled interfaces. Routers that do not have receivers send PIM Prune messages to remove themselves from the trees. PIM-DM is relative straightforward to implement, but has poor scaling properties.

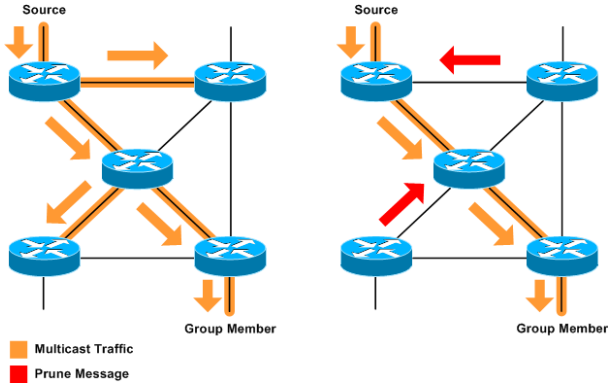

Fig. 1. PIM Dense Mode [18]

  – PIM-SM operates on an explicit join principle, meaning multicast traffic isn't forwarded unless explicitly requested. It works via the use of a Rendezvous Point (RP) to manage join requests efficiently. The RP acts as a central meeting point, coordinating communication between senders and receivers. When a sender initiates multicast traffic, it first reaches the RP, which then forwards the data to interested receivers via the shortest paths. On the other hand, receivers don't directly join the source; rather, they express their interest to receive multicast traffic. Their local router then communicates this interest with the RP, which facilitates the establishment of the necessary multicast distribution tree.PIM-SM's design ensures scalability, making it suitable for wide-area networks. By only forwarding traffic where needed, it conserves network resources while efficiently delivering multicast content.

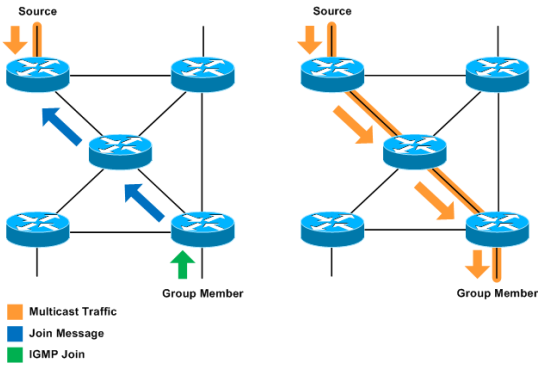

Fig. 2. PIM Sparse Mode [19]

  – Bidir-PIM extends the PIM sparse mode by enabling bidirectional flow on multicasting traffic, as the protocol name suggests. In this model, all sources can potentially function as receivers as well.

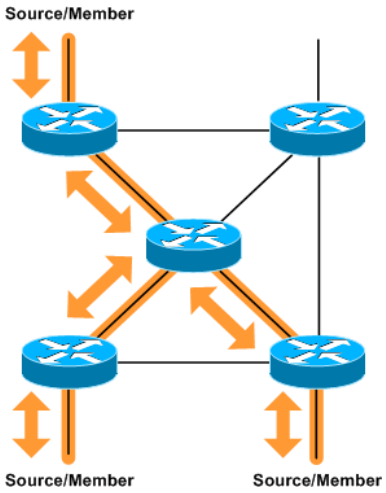

Fig. 3. Bidirectional PIM [19]

– PIM-SSM operates by builds trees that are rooted in just one source, offering a more secure and scalable model, particularly for specific applications like broadcasting. In SSM, an IP datagram is transmitted by a source to a destination address, and receivers can receive this datagram by subscribing to a specific channel identified by both the source and destination address. This targeted approach efficiently delivers multicast traffic to only those receivers interested in the specific source.

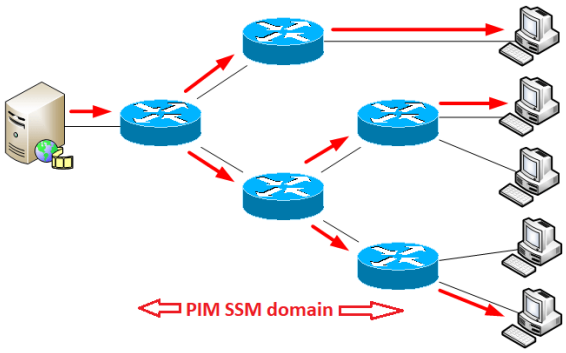

Fig. 4. PIM Source-Specific Multicast [19]

[17] [18] [19] [20]

Multicast Source Discovery Protocol (MSDP): Multicast routing protocol MSDP is a protocol that enables the linking of several PIM-SM multicast domains. The purpose of this protocol is to assist a multicast domain in discovering information about multicast sources located in other PIM-SM multicast domains.

MSDP is a critical component in an inter-domain multicast system. MSDP is only applicable to the Any Source Multicast (ASM) model, which uses PIM-SM as the intra-domain multicast routing protocol. Another essential issue to remember is that MSDP is intended to work with IPv4, and there is no IPv6 version. [5]

- **Internet Group Management Protocol (IGMP)**: The Internet Group Management Protocol (IGMP) is an essential component of the TCP/IP protocol suite, primarily concerned with monitoring multicast group memberships. It facilitates communication between hosts and adjacent multicast routers on IPv4 networks, enabling the establishment and maintenance of host memberships within specific multicast groups. This mechanism ensures that multicast traffic is strategically routed only to networks with hosts that have indicated an interest in receiving such traffic, thereby enhancing network efficiency and minimizing redundant data transmission.

  – **Different Types of IGMP Messages**: As previously stated, IGMP facilitates communication between hosts and routers on an IPv4 network through the exchange of specific messages, aimed at efficiently managing multicast group memberships.
  - **IGMP Queries:** Routers periodically broadcast queries to identify hosts that are interested in joining multicast groups. These can be general queries (asking about all groups) or group-specific queries.
  - **IGMP Reports:** Sent by hosts to signal their intention in receiving multicast traffic for a group. This action prompts routers to update their routing tables to ensure the multicast traffic is accurately directed.
  - **IGMP Leave Group Messages:** Hosts send this message to withdraw from a multicast group, leading routers to conduct a verification process to verify if any other members still require the multicast stream before discontinuing it.

  Multicast management on IPv4 networks has advanced significantly with the introduction of IGMPv1 and IGMPv3. When IGMPv1 first came out, hosts could join multicast groups but could not exit them directly; timeouts were used instead. The Leave Group message was added to IGMPv2 to allow for more dynamic group membership management through explicit departure alerts. In IGMPv3, source-specific multicasting (SSM) is added, allowing hosts to indicate which sources they are interested in receiving traffic from in addition to their group membership. This evolution demonstrates an emphasis on optimizing network resource utilization, precise traffic delivery, and protocol efficiency.
  [21] [22] [23]
- **Multicast Listener Discovery (MLD)**: Multicast group management protocol MLD is an IPv6 Multicast Group Membership Protocol. It communicates between Multicast Routers and Multicast hosts using Query, Report, and Leave Messages. MLD communicates between the MLD Querier router and the hosts. It manages Multicast members joining and leaving.
  There are two versions of MLD: MLDv1 and MLDv2. MLDv1 is the default MLD version. MLDv1 allows Multicast receivers to receive multicast traffic from any

Multicast Source. They have no choice in selecting a Multicast Source. There are three message types in MLDv1: Listener Query (Type 130), Listener Report (Type 131), and Listener Leave (Type 132).
MLDv2 is an improved version of MLDv1. With MLDv2, certain Multicast Sources can be chosen as the source of Multicast traffic. In order to use MLDv2, the router must be set to version 2. There are two types of messages in MLDv2: Listener Query (Type 130), and New MLDv2 Listener Report (Type 143). [6]

- **Source Specific Multicast (SSM)**: SSM is a Multicast routing protocol that extends the PIM protocol to provide efficient data delivery in one-to-many connections. Multicast routes are not separated into intra-domain and inter-domain routes since receivers know where the multicast sources are, and channels established by PIM-SM are adequate for multicast information transfer.

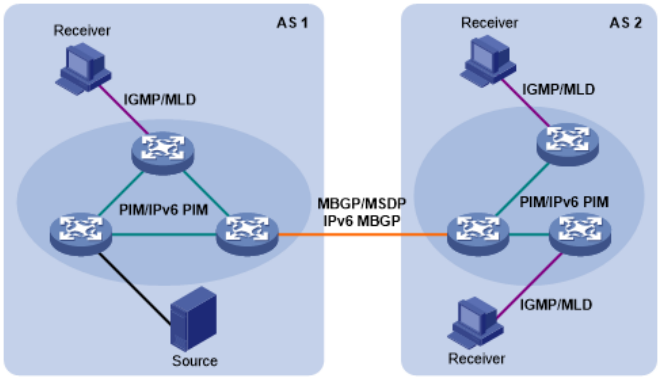

Fig. 5. Positions of Layer 3 multicast protocols [2]

*2) **Layer 2 Multicast Protocols**:* Layer 2 multicast refers to IP multicast operating at the data link layer.
In figure 8 we can see where each protocol works.
We'll discuss the following protocols:

- **IGMP snooping**: IGMP Snooping is an IPv4 method utilized by network switches to identify multicast groups and constrain the flooding of ipv4 multicast traffic on VLANs. Through monitoring IGMP traffic, switches learn which devices are interested in the multicast traffic, selectively forwarding packets to LAN devices, thus conserving bandwidth. By implementing IGMP Snooping, network bandwidth is optimized, ensuring multicast traffic is directed solely to interested receivers, preventing unnecessary flooding across all VLAN interfaces. [9] [10]
- **MLD snooping**: MLD snooping limits the flooding of IPv6 multicast traffic on VLANs. When MLD snooping is enabled on a VLAN, a Switch device examines MLD messages sent between hosts and multicast routers to determine which hosts are interested in receiving traffic from a multicast group. Based on what it learns, the device only sends multicast traffic to interfaces in the VLAN that are linked to interested receivers, rather than flooding all interfaces. MLD snooping supports both MLDv1 and MLDv2. [7] [8]

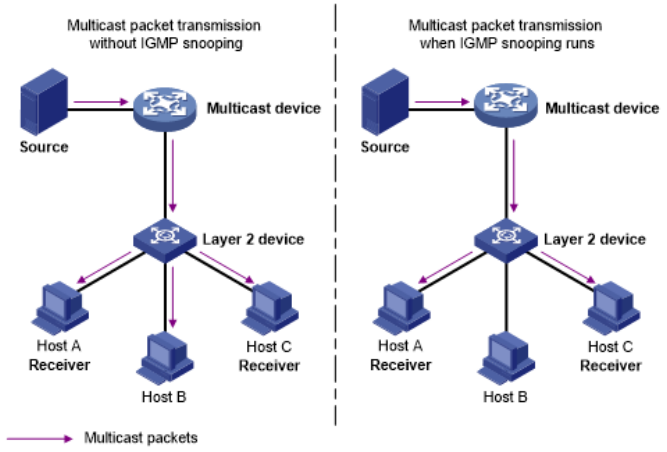

Fig. 6. Multicast packet transmission without and with IGMP snooping [13]

- **PIM snooping**: In networks with several routers connected by a Layer 2 switch, the switch automatically floods IP multicast packets on all multicast router ports, even if there are no multicast receivers downstream. When PIM snooping is enabled, the switch confines multicast packets for each IP multicast group to just the multicast router ports that have downstream receivers associated with that group. PIM Snooping uses IGMP snooping to evaluate incoming PIM messages and adds ports that are interested in specific multicast data to a PIM snooping route entry. This allows the multicast data to be forwarded only to ports that are interested in it. [11] [12]

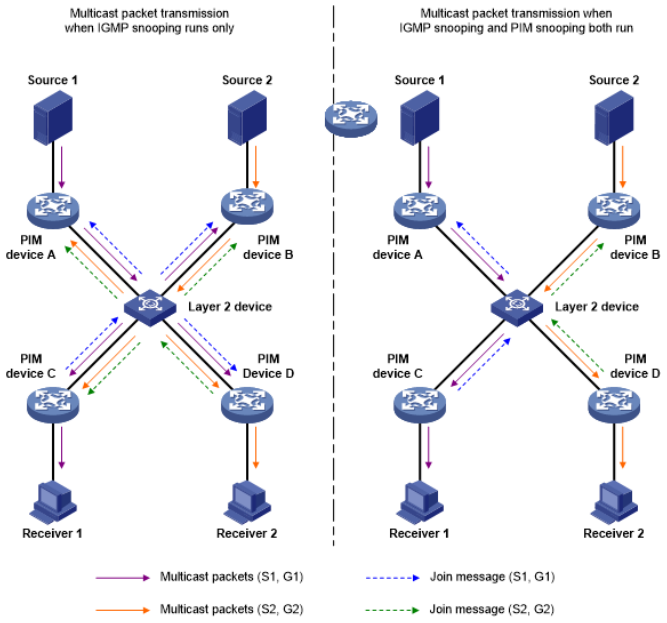

Fig. 7. Multicast packet transmission without or with PIM snooping [12]

- **Multicast VLAN**: When hosts from distinct VLANs request multicast programs-on-demand service, the Layer 3 device (Router) must forward a separate copy of the multicast traffic in each user VLAN to the Layer 2 device (Switch). This not only wastes network capacity but also places additional stress on the Layer 3 device. The multicast VLAN feature requires the Layer 3 device to replicate multicast traffic exclusively in the multicast VLAN, rather than producing a separate copy in each user's VLAN. This saves network traffic and reduces the load on the Layer 3 device. [14]

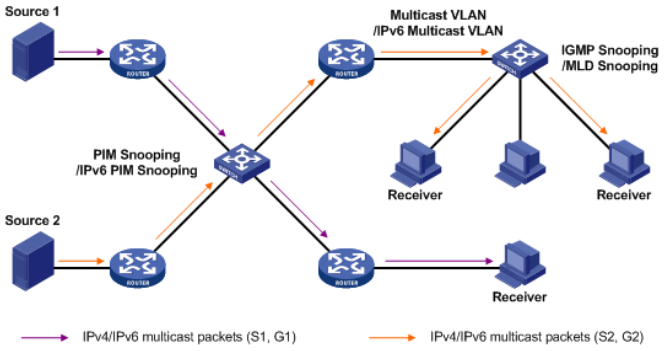

Fig. 8. Positions of Layer 2 multicast protocols [2]

[1] [2]

B. Advantages of Multicast

Multicast technology provides significant advantages for the success of some advanced applications. Some of these advantages are listed below.

- **Optimized network performance**: The thoughtful utilization of network resources prevents excessive flow repetition. In this method, an economy in terms of passing band is realized by using a better data distribution architecture.
- **Support for distributed applications**: Multicast technology has been designed for distributed applications. Multimedia applications, such as distant learning and videoconferencing, can be used in the network in measurable and successful ways.
- **Resource economy**: The passing band economy in links, as well as the processing economy in servers and network equipment, minimize the cost of network resources. New apps and services can be implemented without the need to renovate network resources.
- **Scalability**: A large number of participants can access services and applications thanks to effective network use and reduced pressure on traffic sources. As a result, multicast services can be simply dimensioned, sending packets to a small or large number of receivers.
- **Availability**: The economy of network resources linked with the reduction of load in applications and servers makes the network less prone to jams and thus more available for use.

[3]

C. Challenges in Multicast Routing

In this subsection, we will discuss numerous issues in Multicast Routing. The migration of a group member (receiver or transmitter) causes the following multicast routing issues.

*1) **Network Inactivity**:* The foreign network contacted by mobile receivers may be inactive, with multicast service restricted. Thus, mobile receivers will not receive multicast traffic.

*2) **Multicast Encapsulation/Decapsulation**:* Several implementations use tunneling to enable multicast for mobile hosts. Using IP tunnels necessitates several encapsulation and decapsulation procedures, which incur additional CPU and memory costs. Furthermore, numerous encapsulations increase the multicast packet size, which might result in fragmentation and high bandwidth consumption.

*3) **Routing State Maintenance**:* The routing of multicast packets destined for mobile receivers may vary frequently. Thus, the branches of the multicast distribution tree should be dynamically renewed and rebuilt. The cost of reconstructing a multicast tree is substantial due to the routing overhead involved. To maintain a multicast tree, two ways can be used: the soft state approach, in which branches are removed if they are not refreshed within a delay, and the hard state approach, in which members must explicitly request to leave or relocate. The soft tree maintenance method appears to be better suited for mobile situations than the hard state scheme, particularly when shared trees are used.

*4) **Core Placement**:* Existing multicast protocols make the implicit assumption that group members are topologically stationary while constructing a multicast tree. However, in Mobile IP networks, the members (receivers or senders) are mobile and can migrate from one IP subnet to another. Some core routers are statically configured prior to multicast tree formation, so frequent handovers can cause these critical multicast routers to be off-center. This condition further contributes to the non-optimality of multicast routing pathways. The principal proposed solutions to this problem are relocation, anycast routing schemes, tree migration, and evolution techniques.

[4]

III. Project Objectives

Study/experiments with different Multicast protocols.

- **Design Network Topology**: Design a network topology using GNS3 that accurately reflects a real-world multicast network.
- **Implement Multicast Protocols**: Configure IGMP and PIM protocols on routers and/or switches to enable multicast communication within the network.
- **Generate Multicast Traffic**: Simulate multicast traffic within the network to observe how multicast packets are forwarded and delivered to the intended recipients.
- **Verify Functionality**: Test the multicast network to verify its functionality, ensuring that multicast groups can communicate effectively and troubleshoot any issues encountered during simulation.

To accomplish successfully this study, we orchestrated a simple setup consisting of two routers and one PC configured to manage multicast traffic, as shown in figure 9. Router *Server* was configured as the multicast source, *R1* as the *Rendezvous Point (RP)*, and *Receiver* as the intended multicast receiver.

IV. Tools/components

A. GNS3

GNS3 is a popular open-source network simulation platform for simulating, configuring, testing, and troubleshooting virtual and physical networks. GNS3 enables you to operate a simple topology with only a few devices on your laptop, as well as large topologies with many devices hosted on numerous servers or in the cloud. In this project, we used GNS3 to implement the topology.

In this project, we utilized GNS3 to implement and configure our specific network topology. We tailored network parameters including IP addresses, routers, OSPF, multicast routing, IGMP, PIM and Loopback to align with project goals. By using GNS3, we were able to simulate the network scenario required for showcasing the multicast technology, enabling a deeper understanding of such technology in the real-world.

B. Wireshark

Wireshark is a popular open-source packet analyzer and network protocol analyzer. It is notable for its ability to capture, analyze, and debug network traffic in real-time.
The Wireshark was used to capture the IGMP and PIM messages to understand the path of the packets.

V. Demonstration

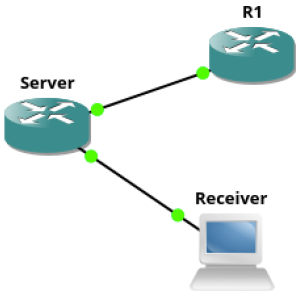

Fig. 9. Setup of a Multicast Network

- **Configuring OSPF:** OSPF was configured on all devices to ensure there was a unicast routing foundation, which is necessary for multicast routing to function properly.

```
# router ospf 1
# network 0.0.0.0 255.255.255.255 area 0
```

- **Enabling Multicast Routing**: We enabled multicast routing on all routers using the command below to handle the PIM protocol's routing of multicast packets.

```
# ip multicast-routing
```

- **Configuring PIM**: we configured PIM in sparse mode on the relevant interfaces of each router to facilitate the routing of multicast traffic.

```
# ip pim sparse-mode
```

- **Defining Loopback on RP**: On *R1*, we defined a loopback interface (Loopback0) with the IP address 3.3.3.3/24, which was used as the RP address for the multicast network.

```
# interface Loopback 0
# ip address 3.3.3.3 255.255.255.0
```

- **Setting the RP**: We statically designated R1 as the RP for the multicast group *224.0.1.40*.

```
# ip pim rp-address 3.3.3.3
```

- **Join the multicast group**: Configure the *Receiver* to join the multicast group 224.0.1.40 on it's FastEthernet interface.

```
# ip igmp join-group 224.0.1.40
```

- **Capturing Traffic on the Receiver**: Wireshark was used on the *Receiver* to capture incoming packets, checking for the reception of the multicast traffic.

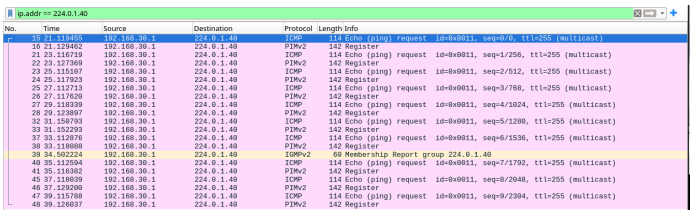

Fig. 10. **Inspecting Multicast Traffic Flow:** ICMP Echo Requests and PIM register messages captured on the network Receiver.

Evidently, the image reflects a successful culmination of the multicast network test scenario within the GNS3 environment. It verifies that the multicast source is actively transmitting pings to the group address 224.0.1.40, and the network infrastructure, including the designated Rendezvous Point, is operational and properly handling multicast PIM registrations.

Additionally, IGMP Membership Reports sent by the receiver signal that it is an active member of the group and prepared to receive multicast traffic. The observation of numerous sequence numbers with progressive values and uniform TTLs underscores the multicast distribution's stability and dependability in the simulated environment.

To conclude, this test underlines the network's proficiency in enabling multicast communication, affirming the accuracy of the multicast routing setups and the operational integrity of PIM across the participating routers and PC.

VI. Future Work

Moving forward, the plan is to enhance the complexity and functionality of our current network topology. This will involve a deliberate selection of advanced routing and transport

protocols that align with our specific objectives, potentially incorporating both established and cutting-edge technologies. Emphasis will be placed on analyzing the dynamics of packet flow within this expanded topology, including the examination of packet behavior under various network conditions and load scenarios. Additionally, the study will aim to understand the impact of different protocol interactions on network performance, reliability, and resilience, with a particular focus on optimizing multicast traffic efficiency and robustness.

REFERENCES

[1] Cisco, IP Multicast Technology Overview, accessed March 26, 2024, https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html

[2] Hewlett Packard Enterprise, Multicast Protocols, accessed March 27, 2024. https://techhub.hpe.com/eginfolib/networking/docs/switches/5710/5200-4986_ip-multi_cg/content/517702718.htm

[3] Rede Nacional de Ensino e Pesquisa, Benefits of the multicast technology, accessed March 29, 2024. https://memoria.rnp.br/en/multicast/benefits.html

[4] I. Romdhani, M. Kellil, H. -Y. Lach, A. Bouabdallah and H. Bettahar, "IP mobile multicast: Challenges and solutions," in IEEE Communications Surveys & Tutorials, vol. 6, no. 1, pp. 18-41, First Quarter 2004, doi: 10.1109/COMST.2004.5342232. https://ieeexplore.ieee.org/abstract/document/5342232?casa_token=lGKU0NfNQAQAAAAA:H1R8ZFOvUWOfxSJ2faV5eq0fWG_XAJgsN-qXhJ0hqenZ6CVcYAnvyMiiUNTCoLVBJw1vv28I-w

[5] The Cisco Learning Network, Multicast Source Discovery Protocol, accessed March 30, 2024. https://learningnetwork.cisco.com/s/question/0D53i00000Ksr0ICAR/multicast-source-discovery-protocol

[6] IPCisco.com, MLD (Multicast Listener Discovery), accessed March 30, 2024. https://ipcisco.com/lesson/mld-multicast-listener-discovery/

[7] Juniper, Understanding MLD Snooping, accessed March 30, 2024. https://www.juniper.net/documentation/us/en/software/junos/multicast/topics/concept/mld-snooping-overview-l2.html

[8] Hewlett Packard Enterprise, Introduction to MLD snooping, accessed March 30, 2024. https://techhub.hpe.com/eginfolib/networking/docs/switches/WB/15-18/5998-8170_wb_2920_ipv6_config_guide/content/v33585413.html

[9] Cloudflare, What is IGMP snooping?, accessed March 31, 2024. https://www.cloudflare.com/learning/network-layer/what-is-igmp-snooping/#:~:text=IGMP%20snooping%20is%20a%20method,correct%20devices%20in%20their%20network.

[10] Jupiter, IGMP Snooping Overview, accessed March 31, 2024. https://www.juniper.net/documentation/us/en/software/junos/multicast/topics/concept/igmp-snooping-qfx-series-overview.html

[11] Cisco, Configuring PIM Snooping, accessed April 2, 2024. https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/snooppim.html

[12] Hewlett Packard Enterprise, About PIM snooping, accessed April 2, 2024. https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3944_ip-multi_cg/content/483573792.htm

[13] Hewlett Packard Enterprise, Fundamentals of IGMP snooping, accessed April 2, 2024. https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3944_ip-multi_cg/content/483573748.htm

[14] Hewlett Packard Enterprise, Introduction to multicast VLAN, accessed April 2, 2024. https://techhub.hpe.com/eginfolib/networking/docs/switches/5120si/cg/5998-8495_ip-multi_cg/content/436144271.htm

[15] Hewlett Packard Enterprise, MBGP overview, accessed April 2, 2024. https://techhub.hpe.com/eginfolib/networking/docs/routers/msrv5/cg/5200-2314_ip-multi-cg/content/index.htm

[16] Orhan Ergun, What is MP-BGP – Multiprotocol BGP, accessed April 3, 2024. https://orhanergun.net/what-is-mp-bgp-multiprotocol-bgp

[17] Wikipedia, Protocol Independent Multicast, acessed April 2, 2024 https://en.wikipedia.org/wiki/Protocol_Independent_Multicast

[18] Packet coders, What is PIM (Protocol Independent Multicast)?, acessed April 2, 2024 https://www.packetcoders.io/what-is-pim-protocol-independent-multicast/

[19] PacketLife.net, PIM crash course, acessed April 2, 2024 https://packetlife.net/blog/2008/oct/16/pim-crash-course/

[20] Wikipedia, Source-specific multicast, acessed April 2, 2024 https://en.wikipedia.org/wiki/Source-specific_multicast

[21] OmniSecu.com, Different Types of IGMP messages, acessed April 1, 2024 https://www.omnisecu.com/tcpip/igmp-message-types.php#google_vignette

[22] cloudflare, What is IGMP? — Internet Group Management Protocol, acessed April 1, 2024 https://www.cloudflare.com/learning/network-layer/what-is-igmp/

[23] geeksforgeek, What is IGMP(Internet Group Management Protocol)?, acessed April 1, 2024 https://www.geeksforgeeks.org/what-is-igmpinternet-group-management-protocol/