Qubahan Academic Journal
گوڤارا قبهان یا ئەکادیمی
مجلة قبهان الأكاديمية
Doi: 10.48161/Issn.2709-8206

Study on: Multicast Routing Protocols: MOSPF and DVMRP

Rasan I. Ali
Computer Science
Researcher
Iraq
rasan.r95@yahoo.com

Awaz A. Shaban
Computer Science
Researcher
Iraq
awz.ahmad@gmail.com

https://doi.org/10.48161/qaj.v3n1a140

Abstract *– Today's networks are designed to reliably transmit traffic such as data from point to point i.e. unicasting, or from point to multipoint i.e. broadcasting. Multimedia places further demands on the network. First of all, multimedia traffic, such as audio or video, cannot tolerate delays in delivery like those tolerable by plain data transfer applications. Multimedia requires that data packets arrive on time and in the proper order at the client side. Real-time protocols and quality of service guarantees addresses this issue. Furthermore, multimedia requires transmitting large amount of traffic over the network and thus uses far more of the network's bandwidth than in case of those basic network operations. Multicasting offers far more efficient way of transmitting such traffic over the Internet than unicasting or broadcasting ever would. The subject of this paper addresses the issue of efficient routing of such multicast traffic.*

Keywords*: MOSPF, DVMRP, Multicasting, Protocols.*

1. INTRODUCTION

The majority of IP traffic on today's networks is unicast, i.e. a separate IP packet is sent from a source to a destination participating in a connection. Networks also support broadcasting. When a packet is broadcast, the same packet is sent to all clients on the network. In case when the same packet needs to be sent only to some of the clients on the network, both of these methods unnecessary waste network bandwidth. Unicast is wasting bandwidth by sending multiple copies of the same packet through the same portion of the network from the source to the destination. Broadcast is wasting bandwidth by sending the data to the whole network no matter if there is a client that wants to receive it. Because each client must process the broadcast IP packet no matter the broadcast is of its interest or not, broadcast slows the performance of client machines needlessly.[1]

Multicasting in some way takes the advantages of both these approaches and tries to avoid their disadvantages. General idea behind multicast is to send single copy of an IP packet to all of those of clients that requested it, and not to send multiple copies of a packet over the same portion of the network, nor to send packets to clients who don't want it. Basic idea in multicasting IP packets is to construct a tree structure data delivery path through the network.[2] This tree is rooted at the source of the multicast traffic and its leaves are subnetworks containing receivers of that traffic. The multicast source sends a single copy of an IP packet through the branches of the tree. The intermediate routers are responsible for multiplication of received IP packets and for forwarding them down the correct branches to other routers and to receivers' subnetworks. Furthermore, routers have to prune off branches where client decided not to receive multicast traffic any more and graft branches back to the tree when a client in a new subnetwork wishes to join the receiver group.[3]

This way multicasting allows that deployment of multimedia applications on the network doesn't cause immediate network congestion by forcing network to do packet replication only when necessary.[4]

2. MULTICAST FUNDAMENTALS

For each IP packet relay method there is corresponding fundamental type of IP address: unicast, broadcast, and multicast. The key difference between a multicast IP packet and a unicast IP packet is the presence of a "group address" in the Destination Address field of the IP header of multicast IP packet. Instead of Class A, B, or C of IP addresses, multicasting employs Class D destination addresses which are all those IP addresses that begin with following binary sequence 1110, which in Internet standard dotted decimal notation are IP addresses ranging from 224.0.0.0 to 239.255.255.255.[5]

A multicast address is designed to enable a delivery of IP multicast packets to a set of clients that have been configured as members of a multicast group in various scattered subnetworks. Individual clients are free to join or leave multicast group at any time. A client may be a member of more than one multicast group at any given time and does not have to belong to a group to send message to members of a group.[6]

Multicast enabled router employs a group membership protocol, such as Internet Group Management Protocol (IGMP) [2], to learn about the presence of group members on their directly attached subnetworks. When a client wishes to join a multicast group, it transmits a group membership protocol message to its router for the group or groups that it wishes to join, and sets its IP process and network interface card to receive IP packets addressed to the multicast group.[7]

Most prevalent multicast routing protocols in Internet today, which implement some of the previously mentioned forwarding algorithms, are:

- Distance Vector Multicast Routing Protocol (DVMRP),
- Multicast Open Shortest Path First (MOSPF) and
- Protocol-Independent Multicast (PIM).

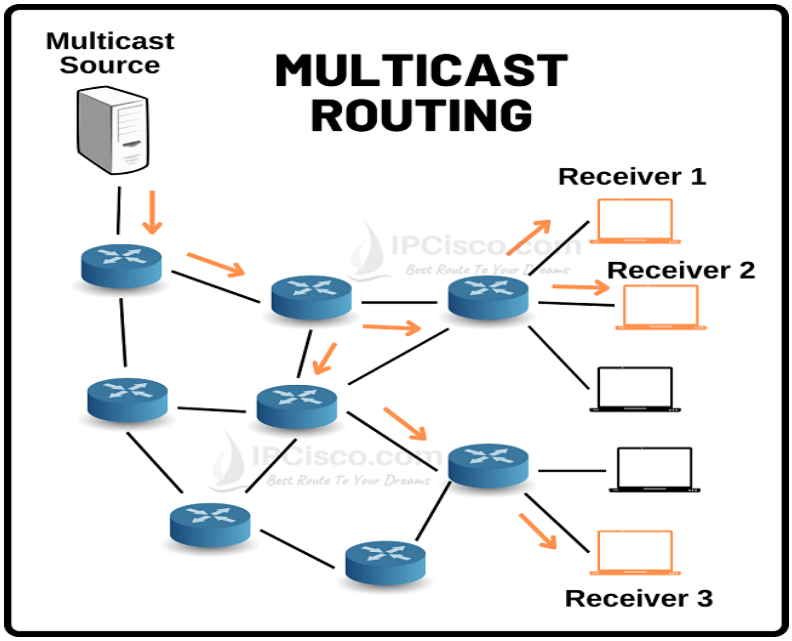

Figure 1: Multicasting Routing

Applications of Multicasting:

- Access to Distributed Databases
  - Large databases are distributed, i.e., stored in more than one location
  - Multiple requests can be sent to a distributed database
- Information Dissemination
  - Examples: sending software update to all purchasers; sending news.
- Teleconferencing
  - same information at the same time.
- Distance Learning
- Live Internet Protocol TV (IPTV)
  - A server has many TV channels (Groups)
  - A host subscribes any one of the TV channels (Becomes a group member)

To perform Multicasting, needs the following components:

- Multicast Addresses - A multicast destination address defines a group of destinations
- Forwarding Table - A router needs to know any members of a group connected to it.
  - Internet Group Management Protocol (IGMP)
- Routing Protocols - Determine the 'best' path to all destinations
  - Distance Vector Multicast Routing Protocol (DVMRP)
  - Multicast Open Shortest Path First (MOSPF)
  - Protocol Independent Multicast (PIM)

Internet Multicast Model

- Hosts addresses IP datagram to multicast group
- Routers forward multicast datagrams to hosts that have "joined" that multicast group

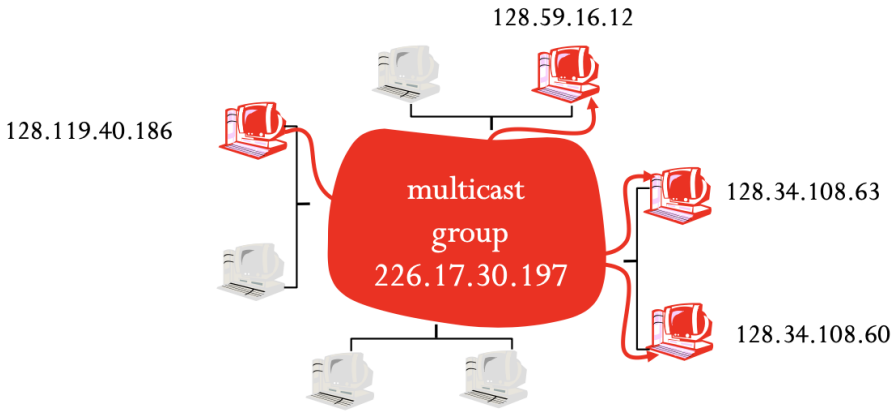

Figure 2: Internet Multicast Model

Internet Multicast Model is a two-step process.

- Local: host informs local multicast router of desire to join group: IGMP (Internet Group Management Protocol)
  - Internet Group Management Protocol (IGMP) are used by hosts and routers to manage the multicast addresses (multicast group membership information)
- Wide area: local router interacts with other routers to receive multicast datagram flow (multicast routing)
  - multicast protocols (e.g., DVMRP, MOSPF, CBT, PIM)

3. MULTICAST ROUTING PROTOCOLS

The second question that we will answer in this lesson is what is Multicast Routing? Multicats Routing is basically an efficient method for one-to-many multicast traffic. This multicast traffic can be an IPTV traffic, a video conference traffic, gaming, live streaming etc. With an efficient way, this routing provides sending only one stream of a multicast traffic to multiple receivers.

Multicast Routing has some similarities and differences with normal routing. Normally, when we check a routing table of a router, we see routing entries. These entries can be static route, OSPF, EIGRP, BGP entries etc. Each of these routes shows us the required next hop for the given destination address. But all of them are unicast entries. When a packet comes to the routers with a multicast destination address, routers do not know how to route this packet if they are not using Multicast Routing Protocols. But if a router uses a Multicast Routing Protocol, it can send this multicast packet to the interfaces that are members of the specific multicast groups. In normal routing, each router needs to know the address of the next router in the path to the destination. But in multicast routing, there is no need for this. Having only the next router address is enough for multicast routing. This reduces bandwidth usage and increases performance a lot! For multicasting routing, all routers need to have a multicast address with which they can send packets each other.

1. Distance Vector Multicast Routing Protocol (DVMRP)

DVMRP is a distance-vector routing protocol designed to support forwarding of multicast packets through an internetwork. DVMRP is widely used in the Internet Multicast Backbone (MBone) [8], multicast enabled set is of subnetworks and routers that support the delivery of IP multicast traffic to over 30 countries all over the world. [9]

DVMRP constructs source-rooted multicast delivery trees using variants of the Reverse Path Broadcasting (RPB) algorithm. DVMRP was first defined in RFC-1075 [1]. The original specification was derived from the Routing Information Protocol (RIP) and employed the Truncated Reverse Path Broadcasting (TRPB) algorithm. The major difference between RIP and DVMRP is that RIP is concerned with calculating the next hop to a destination, while DVMRP is concerned with computing the previous hop back to a source. The latest version of software multicast routing - mrouted 3.9, has extended DVMRP to employ the Reverse Path Multicasting (RPM) algorithm.[10] This means that the latest implementations of DVMRP are quite different from the original RFC specification in many ways.

The ports of a DVMRP router may be either a physical interface to a directly attached subnetwork or a virtual interface to another multicast island. These virtual interfaces are used for tunneling multicast traffic across parts of an internetwork that don't support multicast. Tunneling refers to the process of encapsulation of multicast IP packets in unicast IP packets, which then can be routed by conventional routers. The encapsulation is added on entry into a tunnel and stripped off on exit from the tunnel. [11]

All interfaces are configured with a metric that specifies the cost for the given port and a Time-To-Live (TTL) threshold that limits the scope of a multicast transmission. In addition, each tunnel interface must be explicitly configured with two additional parameters - the IP address of the local router's interface and the IP address of the remote router's interface.[12]

TABLE 1. TTL Scope control values

TTL Value	Scope
0	Restricted to the same host
1	Restricted to the same subnetwork
32	Restricted to the same site
64	Restricted to the same region
128	Restricted to the same continent
255	Unrestricted in scope

A multicast router will only forward multicast packets across an interface if the TTL field in the IP header is greater than the TTL threshold assigned to the interface. Table 1 lists the conventional TTL values used to restrict the scope of an IP multicast. [13]

Operation and Future Development

DVMRP implements the Reverse Path Multicasting (RPM) algorithm. According to RPM, the first packet for any source-group pair is forwarded across the entire internetwork, providing the packet's TTL and router interface thresholds permit it. The initial multicast packet is delivered to all leaf routers, which transmit prune messages back toward the source if there are no group members on their directly attached leaf subnetworks. The prune messages result in the removal of branches from the tree that do not lead to group members, thus creating a source-specific shortest path tree with all leaves having group members. Periodically, this initial procedure is repeated to allow the pruned branches grow back if needed. Furthermore, DVMRP implements mechanisms to quickly "graft" back a previously pruned branch of a group's delivery tree. If a router that previously sent a prune message for a (source, group) pair discovers new group members on a leaf network, it sends a graft message to the group's previous-hop router. When an upstream router receives a graft message, it cancels out the previously received prune message. Graft messages may cascade back toward the source allowing previously pruned branches to be restored as part of the multicast delivery tree.[14]

When there is more than one DVMRP router on a subnetwork, the Dominant Router has to be elected among them to be responsible for the periodic transmission of IGMP Host Membership Query messages. Upon initialization, a DVMRP router considers itself to be the Dominant Router for the

subnetwork until it receives a Host Membership Query message from a neighbour router with a lower IP address. In such case the router with lower IP address is always elected as the new Dominant Router.[15]

Since the DVMRP was developed to route only multicast and not unicast traffic, a router may be required to run multiple routing processes - one for the delivery of unicast traffic and another for the delivery of multicast traffic. The DVMRP process periodically exchanges routing table update messages with multicast-capable neighbours. [16]

DVMRP relies on the receipt of "poison reverse" updates for leaf router detection. This technique requires that a downstream neighbour advertise "infinity" for a source subnetwork to the previous hop router on its shortest-path back to that source subnetwork. If an upstream router does not receive a "poison reverse" update for the source subnetwork on a downstream interface, the upstream router assumes that the downstream subnetwork is a leaf and removes the downstream port from its list of forwarding ports.

The rapid growth of the MBone is beginning to place increasing demands on its routers. The current version of the DVMRP treats the MBone as a single, "flat" routing domain where each router is required to maintain detailed routing information to every subnetwork on the MBone. As the number of subnetworks continues to increase, the size of the routing tables and of the periodic update messages will continue to grow.

To overcome these potential threats, a hierarchical version of the DVMRP is under development. In hierarchical routing, the MBone is divided into a number of individual routing domains. Each routing domain executes its own instance of a multicast routing protocol and another protocol is used for routing between the individual domains. Hierarchical routing reduces the demand for router resources because each router only needs to know the explicit details about routing packets to destinations within its own domain, but knows nothing about the detailed topological structure of any of the other domains. The protocol running between the individual domains maintains information about the interconnection of the domains, but not about the internal topology of each domain. [17]

Hierarchical DVMRP allows the creation of non-intersecting regions, each identified by unique Region-Id, where a region can implement any multicast routing protocols such as DVMRP, MOSPF or PIM as so called "Level 1" protocol. Each region is required to have at least one "boundary router" that is responsible for providing inter-regional connectivity. The boundary routers execute a "Level 2" protocol to forward traffic between regions. When a multicast packet originates within a region, it is forwarded according to the "Level 1" protocol to all subnetworks containing group members. In addition, the packet is forwarded to each of the boundary routers for that source region. The "Level 2" routers tag the

packet with the Region-Id and place it in an encapsulation header for delivery to other regions. When the packet arrives at a remote region, the encapsulation header is removed before delivery to group members by the "Level 1" routers.

2. Multicast Open Shortest Path First (MOSPF)

The Multicast extensions to OSPF (MOSPF) are defined in RFC-1584 [4].Version 2 of the Open Shortest Path First (OSPF) routing protocol is defined in RFC-1583 [3]. It is an Interior Gateway Protocol (IGP) specifically designed to distribute unicast topology information among routers belonging to a single Autonomous System. OSPF is based on link-state algorithms that permit rapid route calculation with a minimum of routing protocol traffic. In addition to efficient route calculation, OSPF is an open standard that supports hierarchical routing, load balancing, and the import of external routing information.[18]

MOSPF routers maintain a current image of the network topology through the unicast OSPF link-state information exchange. MOSPF enhances the OSPF protocol by providing the ability to route multicast IP traffic. The enhancements that have been added are backward compatible so that routers running MOSPF will interoperate with non-multicast OSPF routers when forwarding unicast IP data traffic. MOSPF, unlike DVMRP, does not provide support for tunnels.

The OSPF link state database provides a complete description of the Autonomous System's topology. By adding a new type of link state advertisement (LSA), the group-membership LSA, the location of all multicast group members is precisely located in the database. The path of a multicast packet can then be calculated by building a shortest-path tree rooted at the packet's source. All branches not containing multicast members are pruned from the tree. The shortest path tree for each source-group pair is built "on demand" using Dijkstra's algorithm when a router receives the first multicast packet for a particular source-group pair. The results of the shortest path calculation are then cached for use by subsequent packets having the same source and destination.[19]

Properties of the basic MOSPF routing algorithm can be summarized as:

- For a given multicast packet, all routers within an OSPF area calculate the same source-rooted shortest path delivery tree. Tiebreakers have been defined to guarantee that if several equal-cost paths exist, all routers agree on a single path through the area. MOSPF does not support the concept of equal-cost multipath routing like unicast OSPF does.
- Synchronized link state databases containing Group-Membership LSAs allow an MOSPF router to effectively perform the Reverse Path Multicasting (RPM) computation "in memory". Unlike DVMRP, this means that the first multicast packet of a group transmission does not have to be forwarded to all routers in the area.
- The "on demand" construction of the shortest-path delivery tree has the benefit of spreading calculations over time, resulting in a lesser impact for participating routers.

Each MOSPF router makes its forwarding decision based on the contents of its forwarding cache. The forwarding cache is built from the source-rooted shortest-path tree for each (source, group) pair and the router's local group database. After the router discovers its position in the shortest path tree, a forwarding cache entry is created containing the (source, group) pair, the upstream node, and the downstream interfaces.[20] At this point, the Dijkstra shortest path tree processing is discarded, releasing all resources associated with the creation of the tree. From this point on, the forwarding cache entry is used to forward all subsequent multicast packet for the (source, group) pair.

The information in the forwarding cache is not aged or periodically refreshed. It is maintained as long as there are system resources (i.e. memory) available or until the next topology change.[21] In general, the contents of the forwarding cache will change when:

- The topology of the OSPF internetwork changes, forcing all of the packets shortest-path trees to be recalculated.
- There is a change in the Group-Membership LSAs indicating that the distribution of individual group members has changed.

Benefits and Shortcomings of MOSPF

MOSPF routers can be combined with non-multicast OSPF routers. This permits the gradual deployment of MOSPF and allows experimentation with multicast routing on a limited scale. When MOSPF and non-multicast OSPF routers are mixed within an Autonomous System, all routers will interoperate in the forwarding of unicast packets.[22]

The MOSPF router is required to eliminate all non-multicast OSPF routers when it builds its source-rooted shortest-path delivery tree. An MOSPF router can easily determine the multicast capability of any other router based on the setting of the multicast bit (MC-bit) in the Options field of each router's link state advertisements. The omission of non-multicast routers can create a number of potential problems when forwarding multicast traffic:[23]

- Multicast packets may be forwarded along suboptimal routes since the shortest path between two points may require traversal of a non-multicast OSPF router
- Even though there is unicast connectivity to a destination, there may not be multicast connectivity. For example, the network may partition with respect to multicast connectivity since the only path between two points requires traversal of a non-multicast OSPF router.
- The forwarding of multicast and unicast packets between two points may follow entirely different paths through the internetwork. This might make some routing problems a bit more difficult to debug.

Protocol-Independent Multicast (PIM)

The Protocol-Independent Multicast (PIM) routing protocol is the youngest of all multicast routing protocols and still under development by the Inter-Domain Multicast Routing (IDMR) working group of the IETF. PIM receives its name because it is not dependent on the mechanisms provided by any particular unicast routing protocol. However, any implementation supporting PIM requires the presence of a unicast routing protocol for providing routing table information and to adapt to topology changes.[24,25]

PIM makes a clear distinction between a multicast routing protocol that is designed for dense environments and one that is designed for sparse environments. Dense-mode refers to a protocol that is designed to operate in an environment where group members are relatively densely packed and bandwidth is plentiful. Sparse-mode refers to a protocol that is optimized for environments where group members are distributed across many regions of the Internet and bandwidth is not necessarily widely available. It is important to note that sparse-mode does not imply that the group has few members, just that they are widely dispersed across the Internet.[26]

The argument for making this distinction and therefore two different protocols is that when group members and senders are sparsely distributed across a wide area, both DVMRP and MOSPF as dense-mode protocols do not provide the most efficient multicast delivery service. DVMRP periodically sends multicast packets over many links that do not lead to group members, while MOSPF can send group membership information over links that do not lead to senders or receivers.[27]

PIM Dense Mode (PIM-DM)

While the PIM architecture was driven by the need to provide scalable sparse-mode delivery trees, it also defines a new dense-mode protocol instead of relying on existing dense-mode protocols such as DVMRP and MOSPF. It is envisioned that PIM-DM [7] will be deployed in resource-rich environments, such as a campus LAN where group membership is relatively dense and bandwidth is likely to be readily available. PIM Dense Mode (PIM-DM) is similar to DVMRP in that it employs the Reverse Path Multicasting (RPM) algorithm. However, there are several important differences between PIM-DM and DVMRP or MOSPF:[28]

- PIM-DM relies on the presence of an existing unicast routing protocol to adapt to topology changes, but it is independent of the mechanisms of the specific unicast routing protocol. In contrast, DVMRP contains an integrated routing protocol that makes use of its own RIP-like exchanges to compute the required unicast routing information. MOSPF uses the information contained in the OSPF link-state database, but MOSPF is specific to only the OSPF unicast routing protocol.
- Unlike DVMRP, which calculates a set of child interfaces for each (source, group) pair, PIM-DM simply forwards multicast traffic on all downstream interfaces until explicit prune messages are received. PIM-DM is willing to accept packet duplication to eliminate routing protocol dependencies and to avoid the overhead involved in building the parent/child database.

PIM Sparse Mode (PIM-SM)

PIM Sparse Mode (PIM-SM) [29] is being developed to provide a multicast routing protocol that provides efficient communication between members of sparsely distributed groups that are most common in wide-area internetworks. Its designers believe that a situation in which several hosts wish to participate in a multicast conference do not justify flooding the entire internetwork with periodic multicast traffic. They fear that existing multicast routing protocols will experience scaling problems if several thousand small conferences are in progress, creating large amounts of aggregate traffic that would potentially saturate most wide-area Internet connections.[30] To eliminate these potential scaling issues, PIM-SM is designed to limit multicast traffic so that only those routers interested in receiving traffic for a particular group “see” it.

When there is more than one PIM router connected to a multi-access LAN, the router with the highest IP address is selected to function as the Designated Router (DR) for the LAN. The DR is responsible for the transmission of IGMP Host Query messages, for sending Join/Prune messages toward the RP, and for maintaining the status of the active RP for local senders to multicast groups.[31]

To facilitate the differentiation between DM and SM groups, a part of the Class D multicast address space is reserved to be used by SM groups. When the DR receives an IGMP Report message for a new group, the DR determines if the group is RP-based by examining the group address. If the address indicates a SM group, the DR performs a lookup in the associated group’s RP-list to determine the primary RP for the group. After performing the lookup, the DR creates a multicast forwarding cache for the (*, group) pair and transmits a unicast PIM-Join message to the primary RP. The (*, group) notation indicates an (any source, group) pair. The intermediate routers forward the unicast PIM-Join message and create a forwarding cache entry for the (*, group) pair. Intermediate routers create the forwarding cache entry so that they will know how to forward traffic addressed to the (*, group) pair downstream to the DR originating the PIM-Join message.[32,33]

When a host first transmits a multicast packet to a group, its DR must forward the packet to the primary RP for subsequent distribution across the group’s delivery tree. The DR encapsulates the multicast packet in a PIM-SM-Register packet and unicasts it to the primary RP for the group. The PIM-SM-Register packet informs the RP of a new source, which causes the active RP to transmit PIM-Join messages back to the source station’s DR. The routers lying between the source’s DR and the RP maintain state from received PIM-Join messages so that they will know how to forward subsequent unencapsulated multicast packets from the source subnetwork to the RP.[34]

The source’s DR ceases to encapsulate data packets in PIM-SM-Registers when it receives Join/Prune messages from

the RP. From this point on, the DR forwards data traffic in its native multicast format to the RP. When the RP receives multicast packets from the source station, it resends the packet on the RP-shared tree to all downstream group members.[35]

The RP-shared tree provides connectivity for group members but does not optimize the delivery path through the internetwork. PIM-SM allows receivers to either continue to receive multicast traffic over the RP-shared tree or over a source-rooted shortest-path tree that a receiver subsequently creates thus reducing the transmission delay between itself and a particular source.[36]

A PIM router with local receivers has the option of switching to the source's shortest-path tree as soon as it starts receiving data packets from the source station. The local receiver's DR does this by sending a Join message toward the active source. At the same time, protocol mechanisms guarantee that a Prune message for the same source is transmitted to the active RP. Alternatively, the DR may be configured to continue using the RP-based tree and never switch over to the source's shortest-path tree.[37,38]

It is important to note that PIM is an Internet draft. It means it is still early in its development cycle and there are several important issues that require further research, engineering, and experimentation:

- PIM-SM still requires routers to maintain a significant amount of state information to describe sources and groups.
- Some multicast routers will be required to have both PIM interfaces and non-PIM interfaces. The interaction and sharing of multicast routing information between PIM and other multicast routing protocols is still in the early stages of definition.
- The future deployment of PIM-SM will probably require more coordination between Internet service providers to support an Internet-wide delivery service.
- Finally, PIM-SM is considerably more complex than DVMRP or the MOSPF extensions.

TABLE 2. Multicast Routing Protocols Overview

Multicast Routing Protocol	Forwarding Algorithm	Unicast Protocol Dependence	Supports Tunneling
DVMRP	TRPB	RIP	Yes
MOSPF	RPM	OSPF	No
PIM - DM	RPM	-	No
PIM – SM	Similar to CBT	-	No

4. CONCLUSION

In conclusion, the study on multicast routing protocols MOSPF and DVMRP revealed that both protocols are effective in enabling multicast communication in a network. MOSPF is a protocol that uses a modified version of the OSPF protocol and provides efficient routing in large networks with multiple multicast groups. On the other hand, DVMRP is a distance-vector multicast routing protocol that provides a simple and scalable solution for small to medium-sized networks. The study found that MOSPF is more complex to configure and maintain than DVMRP, but it provides better performance in terms of scalability and convergence time. DVMRP, on the other hand, has a simpler configuration and requires less memory and processing power than MOSPF, making it a more suitable option for smaller networks. In summary, the choice of multicast routing protocol depends on the size and complexity of the network and the specific requirements of the application. Both MOSPF and DVMRP have their strengths and weaknesses, and it is important to carefully evaluate and choose the appropriate protocol based on the network's specific needs.

REFERENCES

[1]. RFC 1075 "Distance Vector Multicast Routing Protocol", D. Waitzman, C. Partridge, and S. Deering, November 1988.

[2]. Asaad, R. R. (2021). A Study on Instruction Formats on Computer Organization and Architecture. ICONTECH INTERNATIONAL JOURNAL, 5(2), 18-24. https://doi.org/10.46291/ICONTECHvol5iss2pp18-24

[3]. RFC 1112 "Host Extensions for IP Multicasting", Steve Deering, August 1989.

[4]. Asaad, R. R., Ashqi Saeed, V., & Masud Abdulhakim, R. (2021). Smart Agent and it's effect on Artificial Intelligence: A Review Study. ICONTECH INTERNATIONAL JOURNAL, 5(4), 1-9. https://doi.org/10.46291/ICONTECHvol5iss4pp1-9

[5]. Yahya Hussien , A., Rajab Asaad, R., & Younis Masiha, R. (2022). Review on Social Media and Digital Security. Qubahan Academic Journal, 2(2), 1–4. https://doi.org/10.48161/qaj.v2n2a119

[6]. RFC 1584 "Multicast Extensions to OSPF", John Moy, March 1994.

[7]. Asaad, R. R. (2020). Implementation of a Virus with Treatment and Protection Methods. ICONTECH INTERNATIONAL JOURNAL, 4(2), 28-34. https://doi.org/10.46291/ICONTECHvol4iss2pp28-34

[8]. "Core Based Trees (CBT) Multicast Routing Architecture", <draft-ietf-idmr-cbt-arch-04.txt>, A. J. Ballardie,

June 20, 1995.
[9]. Asaad, R. R., Abdulrahman, S. M., & Hani, A. A. (2017). Advanced Encryption Standard Enhancement with Output Feedback Block Mode Operation. Academic Journal of Nawroz University, 6(3), 1–10. https://doi.org/10.25007/ajnu.v6n3a70
[10]. "Hierarchical Distance Vector Multicast Routing for the MBONE", Ajit Thyagarajan and Steve Deering, July 1995.
[11]. Abdulfattah, G. M., Ahmad, M. N., & Asaad, R. R. (2018). A reliable binarization method for offline signature system based on unique signer's profile. INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING INFORMATION AND CONTROL, 14(2), 573-586.
[12]. "Protocol-Independent Multicast (PIM), Dense-Mode Protocol Specification", <draft-ietf-idmr-PIM-DM-spec-01.txt>, D. Estrin, D. Farinacci, V. Jacobson, C. Liu, L. Wei, P. Sharma, and A. Helmy, January 17, 1996.
[13]. Asaad, R. R., Abdurahman, S. M., & Hani, A. A. (2017). Partial Image Encryption using RC4 Stream Cipher Approach and Embedded in an Image. Academic Journal of Nawroz University, 6(3), 40–45. https://doi.org/10.25007/ajnu.v6n3a76
[14]. "Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", <draft-ietf-idmr-PIM-SM-spec-02.txt>, S. Deering, D. Estrin, D. Farinacci, V. Jacobson, C. Liu, L. Wei, P. Sharma, and A Helmy, September 7, 1995.
[15]. Asaad, R. R., Ahmad, H. B., & Ali, R. I. (2020). A Review: Big Data Technologies with Hadoop Distributed Filesystem and Implementing M/R. Academic Journal of Nawroz University, 9(1), 25–33. https://doi.org/10.25007/ajnu.v9n1a530.
[16]. "Introduction to IP Multicast Routing", An IP Multicast Initiative White Paper, http://www.ipmulticast.com/community/whitepapers/introrouting.html
[17]. Rajab Asaad, R., & Masoud Abdulhakim, R. (2021). The Concept of Data Mining and Knowledge Extraction Techniques. Qubahan Academic Journal, 1(2), 17–20. https://doi.org/10.48161/qaj.v1n2a43
[18]. Asaad, R. R., & Segerey, R. I. (2018). School Management Application Using iOS. Academic Journal of Nawroz University, 7(4), 38–44. https://doi.org/10.25007/ajnu.v7n4a269.
[19]. "How IP Multicast Works", An IP Multicast Initiative White Paper, http://www.ipmulticast.com/community/whitepapers/howipmcworks.html
[20]. Asaad, R. R. (2021). Penetration Testing: Wireless Network Attacks Method on Kali Linux OS. Academic Journal of Nawroz University, 10(1), 7–12. https://doi.org/10.25007/ajnu.v10n1a998
[21]. Zhiyong Zhang, Brij B. Gupta, Social media security and trustworthiness: Overview and new direction, Future Generation Computer Systems, Volume 86, 2018, Pages 914-925, ISSN 0167-739X, https://doi.org/10.1016/j.future.2016.10.007.
[22]. Simerly, T. W., Tang, T. S. H., Dutt, A. M., Pledger, P. K., Breton, K. D., & Kay, A. (2011). U.S. Patent No. 7,952,609. Washington, DC: U.S. Patent and Trademark Office.
[23]. Redmiles, E. M., Malone, A. R., & Mazurek, M. L. (2016, May). I think they're trying to tell me something: Advice sources and selection for digital security. In 2016 IEEE Symposium on Security and Privacy (SP) (pp. 272-288). IEEE.
[24]. Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L. (2014). History of information: the case of privacy and security in social media. In Proc. of the History of Information Conference (pp. 283-310).
[25]. Kim, H. J. (2012). Online social media networking and assessing its security risks. International journal of security and its applications, 6(3), 11-18.
[26]. Li, H., Wouhaybi, R. H., & Kohlenberg, T. (2015). "Security challenge assisted password proxy." U.S. Patent No. 9,223,950. Washington, DC: U.S. Patent and Trademark Office.
[27]. Kals, S., Kirda, E., Kruegel, C., & Jovanovic, N. (2006, May). Secubat: a web vulnerability scanner. In Proceedings of the 15th international conference on World Wide Web (pp. 247-256).
[28]. Oder, I.J.D., Oder, J.D., Cronic, K.J., Sommers, S.M. and Warner, D.W., Shift4 Corp, 2011. Secure payment card transactions. U.S. Patent 7,891,563.
[29]. Data Reportal, (2020) Digital 2020: Global Digital Overview, https://datareportal.com/
[30]. Asaad, Renas Rajab. (2014). An Investigation of the Neuronal Dynamics Under Noisy Rate Functions. Thesis (M.S.), Eastern Mediterranean University, Institute of Graduate Studies and Research, Dept. of Computer Engineering, Famagusta: North Cyprus.
[31]. Asaad, R. R., Abdurahman, S. M., & Hani, A. A. (2017). Partial Image Encryption using RC4 Stream Cipher Approach and Embedded in an Image. Academic Journal of Nawroz University, 6(3), 40–45. https://doi.org/10.25007/ajnu.v6n3a76
[32]. Rajab Asaad, R., & Masoud Abdulhakim, R. (2021). The Concept of Data Mining and Knowledge Extraction Techniques. Qubahan Academic Journal, 1(2), 17–20. https://doi.org/10.48161/qaj.v1n2a43
[33]. Asaad, R. R., Ahmad, H. B., & Ali, R. I. (2020). A Review: Big Data Technologies with Hadoop Distributed Filesystem and Implementing M/R. Academic Journal of Nawroz University, 9(1), 25–33. https://doi.org/10.25007/ajnu.v9n1a530
[34]. Asaad, R. R. (2019). Güler and Linaro et al Model in an Investigation of the Neuronal Dynamics using noise Comparative Study. Academic Journal of Nawroz University, 8(3), 10–16. https://doi.org/10.25007/ajnu.v8n3a360
[35]. Asaad, R. R. (2021). Penetration Testing: Wireless Network Attacks Method on Kali Linux OS. Academic

Journal of Nawroz University, 10(1), 7–12. https://doi.org/10.25007/ajnu.v10n1a998
[36]. Almufti, S., Marqas, R., & Asaad, R. (2019). Comparative study between elephant herding optimization (EHO) and U-turning ant colony optimization (U-TACO) in solving symmetric traveling salesman problem (STSP). Journal Of Advanced Computer Science & Technology, 8(2), 32.
[37]. Asaad, R. R., & Abdulnabi, N. L. (2018). Using Local Searches Algorithms with Ant Colony Optimization for the Solution of TSP Problems. Academic Journal of Nawroz University, 7(3), 1-6. https://doi.org/10.25007/ajnu.v7n3a193
[38]. Almufti, S., Asaad, R., & Salim, B. (2018). Review on elephant herding optimization algorithm performance in solving optimization problems. International Journal of Engineering & Technology, 7, 6109-6114.
[39]. Asaad, R. R., & Ali, R. I. (2019). Back Propagation Neural Network(BPNN) and Sigmoid Activation Function in Multi-Layer Networks. Academic Journal of Nawroz University, 8(4), 216–221. https://doi.org/10.25007/ajnu.v8n4a464
[40]. Rajab Asaad, R. (2021). Review on Deep Learning and Neural Network Implementation for Emotions Recognition . Qubahan Academic Journal, 1(1), 1–4. https://doi.org/10.48161/qaj.v1n1a25
[41]. Asaad, R. R., Abdulrahman, S. M., & Hani, A. A. (2017). Advanced Encryption Standard Enhancement with Output Feedback Block Mode Operation. Academic Journal of Nawroz University, 6(3), 1–10. https://doi.org/10.25007/ajnu.v6n3a70
[42]. Abdulfattah, G. M., Ahmad, M. N., & Asaad, R. R. (2018). A reliable binarization method for offline signature system based on unique signer's profile. INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING INFORMATION AND CONTROL, 14(2), 573-586.
[43]. Almufti, S. M., Ahmad, H. B., Marqas, R. B., & Asaad, R. R. (2021). Grey wolf optimizer: Overview, modifications and applications. International Research Journal of Science, Technology, Education,and Management, 1(1),1-1.
[44]. Asaad, R. R., Sulaiman, Z. A., & Abdulmajeed, S. S. (2019). Proposed System for Education Augmented Reality Self English Learning. Academic Journal of Nawroz University, 8(3), 27–32. https://doi.org/10.25007/ajnu.v8n3a366
[45]. Asaad, R. R. (2020). Implementation of a Virus with Treatment and Protection Methods. ICONTECH INTERNATIONAL JOURNAL, 4(2), 28-34. https://doi.org/10.46291/ICONTECHvol4iss2pp28-34
[46]. Boya Marqas, R., M. Almufti, S., & Rajab Asaad, R. (2022). FIREBASE EFFICIENCY IN CSV DATA EXCHANGE THROUGH PHP-BASED WEBSITES. Academic Journal of Nawroz University, 11(3), 410–414. https://doi.org/10.25007/ajnu.v11n3a1480
[47]. Ihsan, R. R., Almufti, S. M., Ormani, B. M., Asaad, R. R., & Marqas, R. B. (2021). A survey on Cat Swarm Optimization algorithm. Asian J. Res. Comput. Sci, 10, 22-32.
[48]. Rajab Asaad, R., & Luqman Abdulnabi, N. (2022). A Review on Big Data Analytics between Security and Privacy Issue. Academic Journal of Nawroz University, 11(3), 178–184. https://doi.org/10.25007/ajnu.v11n3a1446
[49]. Yahya Hussien , A., & Rajab Asaad, R. (2022). Review on Social Media and Digital Security. Qubahan Academic Journal, 2(2), 1–4. https://doi.org/10.48161/qaj.v2n2a119
[50]. Asaad, R. R. (2022). Keras Deep Learning for Pupil Detection Method . Academic Journal of Nawroz University, 10(4), 240–250. https://doi.org/10.25007/ajnu.v10n4a1328
[51]. Asaad, R. R., & Segerey, R. I. (2018). School Management Application Using iOS. Academic Journal of Nawroz University, 7(4), 38–44. https://doi.org/10.25007/ajnu.v7n4a269
[52]. Asaad, R. R., Mustafa, R. F., & Hussien, S. I. (2020). Mortality Statistics and Cause of Death at Duhok City from The Period (2014-2019) Using R Language Data Analytics. Academic Journal of Nawroz University, 9(3), 1–7. https://doi.org/10.25007/ajnu.v9n3a699
[53]. Asaad, R. R. (2021). A Study on Instruction Formats on Computer Organization and Architecture. ICONTECH INTERNATIONAL JOURNAL, 5(2), 18-24. https://doi.org/10.46291/ICONTECHvol5iss2pp18-24
[54]. Asaad, R. R. (2021). Virtual reality and augmented reality technologies: A closer look. Virtual reality, 1(2).
[55]. Asaad, R. R. A Review: Emotion Detection and Recognition with Implementation on Deep Learning/Neural Network.
[56]. Asaad, R. R., Saeed, V. A., & Abdulhakim, R. M. (2021). Smart Agent and it's effect on Artificial Intelligence: A Review Study. ICONTECH INTERNATIONAL JOURNAL, 5(4), 1-9.
[57]. Asaad, R. R. A Asaad, R. R. A Review: Emotion Detection and Recognition with Implementation on Deep Learning/Neural Network.
[58]. Ferinia, R., Kumar, D.L.S., Kumar, B.S. et al. Factors determining customers desire to analyse supply chain management in intelligent IoT. J Comb Optim 45, 72 (2023). https://doi.org/10.1007/s10878-023-01007-8
[59]. Poornima, E., Muthu, B., Agrawal, R. et al. Fog robotics-based intelligence transportation system using line-of-sight intelligent transportation. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023-15086-6