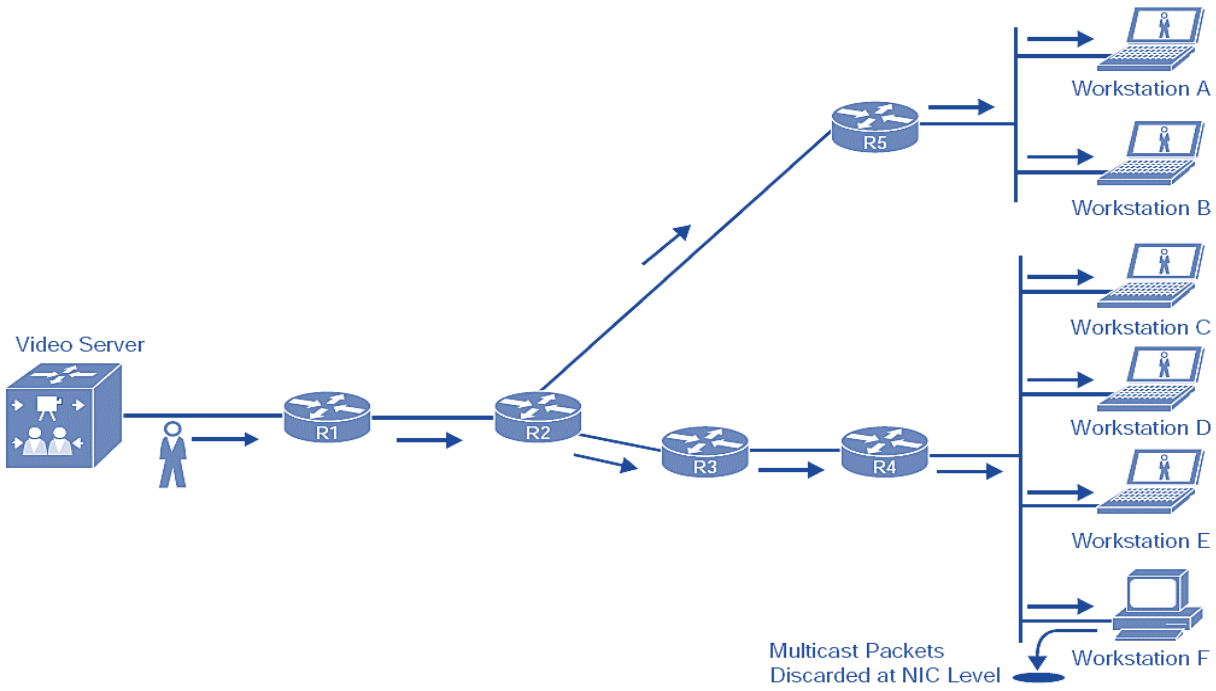
Multicast:

- There are three main types of traffic that we can choose from for our networks.
- The Three main types of traffic are the Unicast, the Broadcast and the Multicast.
- If you want to send a message from one source to one destination, we use unicast.
- If you want to send a message from one source to everyone, we use the broadcast.
- If we want to send a message from one source to a group of receivers, use multicast.
- Multicast communication is a technology that optimizes network bandwidth utilization.
- Multicast communication is a technology optimizes network conserves system resources.
- It relies on Internet Group Management Protocol (IGMP) for its operation in L2 networks.
- It relies on Protocol Independent Multicast (PIM) for its operation in OSI Layer 3 networks.
- Multicast has many advantages; main advantage is scalability compared to unicast traffic.
- Multicast protocols UDP & RTP are used to broadcast data to any number receiving devices.
- Multicast traffic provides one-to-many communication, where only one data packet is sent.
- The Data packets are stream that uses special destination IP address name group address.
- Common applications that take advantage of multicast traffic include Cisco Telepresence.
- Real-time video, IPTV, stock tickers, distance learning, video/audio conferencing, & gaming.



Multicast IP Addresses:

- Unicast IP addresses represent single device, multicast IP addresses represent a group.
- Internet Assigned Numbers Authority has reserved the class D range to use for multicast.
- Means we have from 224.0.0.0 through 239.255.255.255 range for IP multicast addresses.
- Some of the addresses are reserved and we cannot use them for our own applications.
- Make sure you don't use the 224.0.0.0 /24 and 224.0.1.0 /24 range and you will be safe.
- Like private and public IP addresses for unicast, IANA has reserved a range of IP addresses.
- We can use for the multicast on our local networks and this is the 239.0.0.0 /8 range.
- Everything between 239.0.0.0 - 239.255.255.255 is safe to use on your own networks.

Local Network Control Block:

- The 224.0.0.0 – 224.0.0.255 range has been reserved by IANA to use for network protocols.
- All multicast IP packets in this range are not forwarded by Cisco routers between subnets.
- (224.0.0/24) Addresses in local network control block are used for protocol control traffic.
- Internetwork control block (224.0.1.0/24) - Addresses in the internetwork control block.
- They are used for protocol control traffic that may be forwarded through the Internet.

Address	Usage
224.0.0.1	All Hosts
224.0.0.2	All Multicast Routers
224.0.0.3	Unassigned
224.0.0.4	DVMRP Routers
224.0.0.5	OSPF Routers
224.0.0.6	OSPF DR/BDR Router
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	RIPv2 Routers
224.0.0.10	EIGRP Routers
224.0.0.11	Mobile Agents
224.0.0.12	DHCP Server / Relay
224.0.0.13	All PIM Routers
224.0.0.14	RSVP Encapsulation
224.0.0.15	All CBT Routers
224.0.0.16	Designated SBM
224.0.0.17	All SBMS
224.0.0.18	VRRP
224.0.0.19 – 255	Unassigned

Address	Usage
224.0.1.0	VMTP Managers Group
224.0.1.1	NTP
224.0.1.2	SGI-Dogfight
224.0.1.3	Rwhod
224.0.1.6	NSS
224.0.1.8	SUN NIS+
224.0.1.20	Any Private Experiment
224.0.1.21	DVMRP on MOSPF
224.0.1.32	Mtrace
224.0.1.33	RSVP-encap-1
224.0.1.34	RSVP-encap-2
224.0.1.39	Cisco-RP-Announce
224.0.1.40	Cisco-RP-Discovery
224.0.1.52	Mbone-VCRDirectory
224.0.1.78	Tibco Multicast 1
224.0.1.79	Tibco Multicast 2
224.0.1.80 – 224.0.1.255	Unassigned

Designation	Multicast Address Range
Local network control block	224.0.0.0 to 224.0.0.255
Internetwork control block	224.0.1.0 to 224.0.1.255
Ad hoc block	224.0.2.0 to 224.0.255.255
Reserved	224.1.0.0 to 224.1.255.255
SDP/SAP block	224.2.0.0 to 224.2.255.255
Ad hoc block II	224.3.0.0 to 224.4.255.255
Reserved	224.5.0.0 to 224.255.255.255
Reserved	225.0.0.0 to 231.255.255.255
Source Specific Multicast (SSM) block	232.0.0.0 to 232.255.255.255
GLOP block	233.0.0.0 to 233.251.255.255
Ad hoc block III	233.252.0.0 to 233.255.255.255
Reserved	234.0.0.0 to 238.255.255.255
Administratively scoped block	239.0.0.0 to 239.255.255.255

IGMP Protocol:

Internet Group Management Protocol (IGMP) is the protocol that receivers use to join multicast groups. When a receiver wants to receive a specific multicast feed, it sends an IGMP join using the multicast IP group address for that feed. The receiver reprograms its interface to accept the multicast MAC group address that correlates to the group address. For example, a PC could send a join to 239.255.1.1 and would reprogram its NIC to receive 01:00:5E:7F:01:01. IGMP must be supported by receivers and the router interfaces facing the receivers. Three versions of IGMP exist. IGMPv1, which is old and rarely used. IGMPv2, which is common in most multicast networks, and IGMPv3, which is used by SSM.

IGMP Version 1:

- IGMP version 1 is the first version that hosts can use to announce to a cisco router.
- That they want to receive the multicast traffic from a specific multicast group.
- Simple protocol uses only two messages Membership report & Membership query.
- Host wants to join multicast group; it send membership report to the group address.
- When multicast-enabled router receives this message, it start forwarding requested.
- Multicast traffic on the interface where it received the IGMP membership report on.
- The router will periodically send a membership query to destination 224.0.0.1.
- After each 60 seconds each will send a membership query on enable interfaces.
- Hosts that receive this message will respond with a membership report to tell router.
- That they are still interested in receiving the multicast traffic from the given group.
- When the router receives the membership report, it's expiry timer will be refreshed.
- When no hosts respond, router knows that is interested anymore in multicast traffic.
- And it will then remove the entry from the multicast routing once the timer exceeds.
- In multicast the IGMP Version 1 is a simple protocol with only two different packets.
- Disadvantage is router will keep forwarding multicast traffic even no one interested.

R1(config)#ip multicast-routing
R1(config)#interface GigabitEthernet 0/1 R1(config-if)#ip igmp version 1 R1(config-if)#ip pim sparse-mode
R1#show ip igmp interface GigabitEthernet 0/1
R1#show ip igmp groups 239.1.1.1
R1#debug ip igmp
R2(config)#interface GigabitEthernet 0/1 R2(config-if)#ip igmp version 1 R2(config-if)#ip igmp join-group 239.1.1.1
R2#debug ip igmp

IGMP Version 2:

- In multicasting the IGMP version 2 is the enhanced version of the IGMP version 1.
- IGMP V1, hosts stop listening to multicast group address but never report to router.
- IGMP Version 2 is very similar to Version 1 but due to new features its more efficient.
- IGMP Version 2 because of new features it leaving groups has become much faster.

Leave Group Messages	When a host no longer wants to listen to a multicast group address then it will report to the router that it has stopped listening.
Group Specific Membership Query	Router is now able to send membership query for specific group address. When router receives a leave group message, it use this query to check if there are still any hosts interested in receiving multicast traffic.
MRT (Maximum Response Time) Field	A new field in query messages, it specifies how much time hosts have to respond to the query.
Querier Election Process	When there are two routers in same subnet then only one of them should send query messages. The election ensures only one router becomes the active querier. The router with the lowest IP address becomes the active querier.

R1(config)#ip multicast-routing
R1(config)#interface GigabitEthernet 0/1 R1(config-if)#ip pim sparse-mode
R1#show ip igmp interface GigabitEthernet 0/1
R1#debug ip igmp
R1#show ip igmp groups 239.1.1.1

R2(config)#interface GigabitEthernet 0/1 R2(config-if)#ip igmp join-group 239.1.1.1

IGMP Version 3:

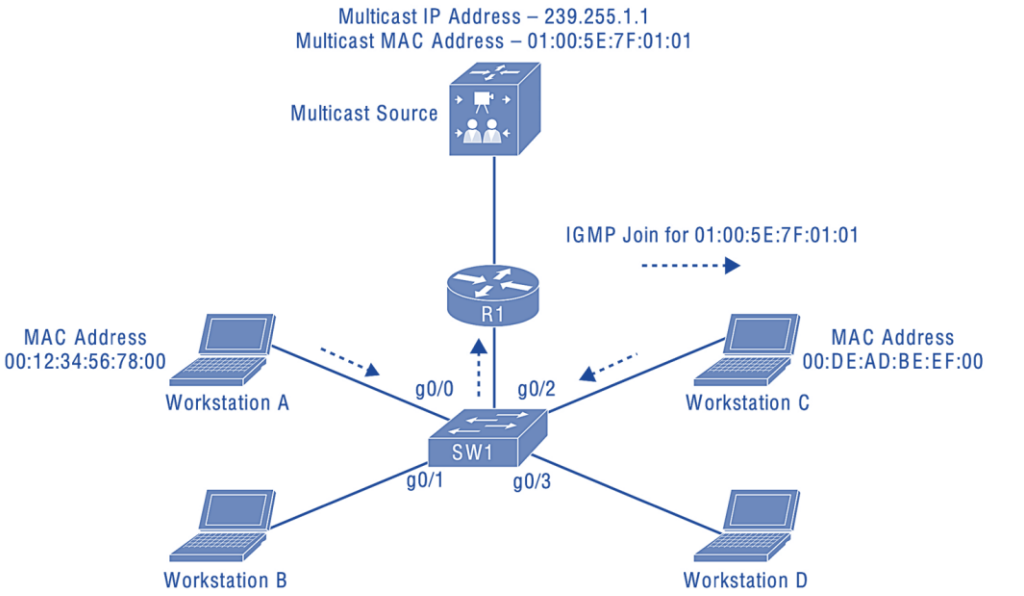
- Internet Group Management Protocol Version 3 adds support for "Source Altering".
- IGMP v1 & v2 allow hosts to join multicast groups but don't check source of the traffic.
- In IGMPv2, when a receiver sends a membership report to join the multicast group.
- IGMP V2 does not specify which source it would like to receive multicast traffic from.
- Internet Group Management Protocol V3 adds support for multicast source filtering.
- Giving receivers the capability to pick source they wish to accept multicast traffic from.
- It supports all IGMPv2's IGMP message types & is backward compatible with IGMPv2.

R1(config)#ip multicast-routing
R1(config)#interface GigabitEthernet 0/1 R1(config-if)#ip pim sparse-mode R1(config-if)#ip igmp version 3
R1#debug ip igmp

R2(config)#interface GigabitEthernet 0/1
R2(config-if)#ip igmp join-group 239.1.1.1 R2(config-if)#no ip igmp join-group 239.1.1.1 source 1.1.1.1
R1#show ip igmp groups 239.1.1.1 detail

IGMP Snooping:

In the case of multicast traffic, a multicast MAC address is never used as a source MAC address. Switches treat multicast MAC addresses as unknown frames and flood them out all ports. All workstations then process these frames. It is then up to the workstations to select interested frames for processing and select the frames that should be discarded. The flooding of multicast traffic on a switch wastes bandwidth utilization on each LAN segment. IGMP snooping allows us to constrain our multicast traffic. As the name implies, this is done by listening to IGMP traffic between the router and hosts: IGMP snooping, is the most widely used method and works by examining IGMP joins sent by receivers and maintaining a table of interfaces to IGMP joins. When the switch receives a multicast, frame destined for a multicast group, it forwards the packet only out the ports where IGMP joins were received for that specific multicast group. Switches listen to IGMP messages and learn on which interfaces they have to forward multicast traffic. Without IGMP snooping, switches will flood multicast traffic everywhere, treating like broadcast traffic. IGMP snooping works pretty well but it does require a multicast router in the network.



Switch MAC Address Table	
MAC Address	**Interface**
00:12:34:56:78:00	g0/0
00:DE:AD:BE:EF:00	g0/2
01:00:5E:7F:01:01	g0/0, g0/2

← Multicast MAC Address

Multicast Routing Protocols:

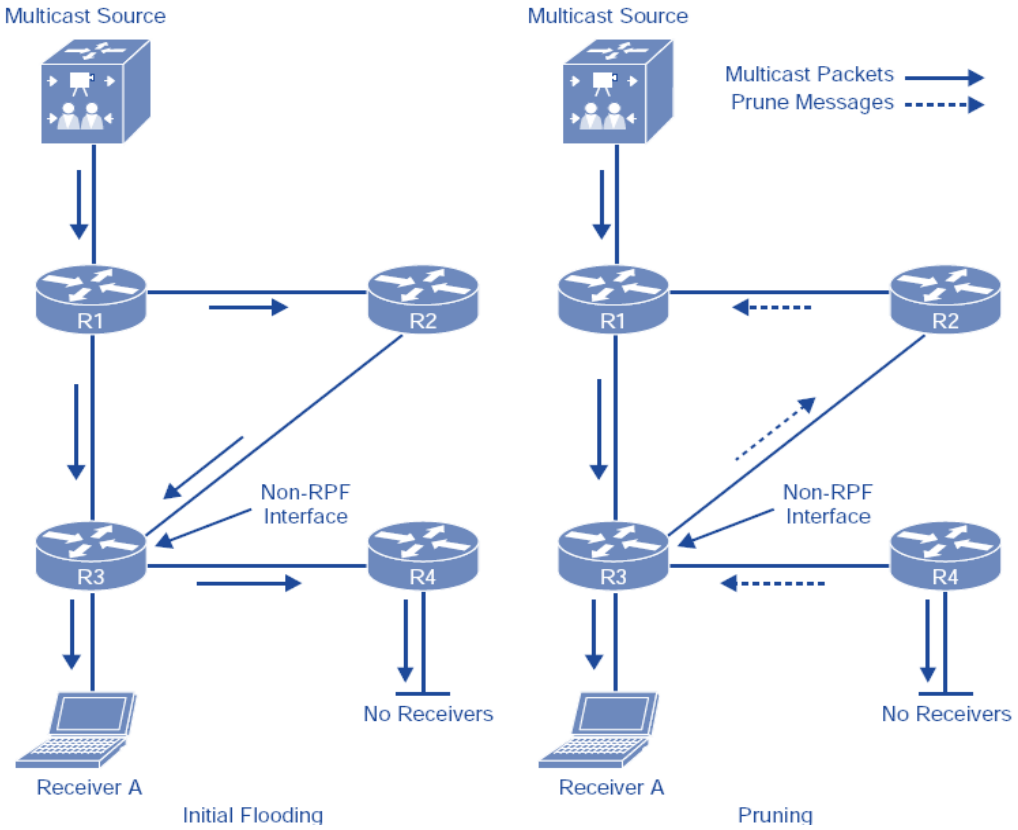
To route multicast traffic, we need to use a multicast routing protocol. There are two types of multicast routing protocols: Dense Mode and Sparse Mode. A multicast routing protocol is necessary to route the multicast traffic throughout the network so that routers can locate and request multicast streams from other routers.

PIM (Protocol Independent Multicast):

A multicast routing protocol is necessary to route the multicast traffic throughout the network so that routers can locate and request multicast streams from other routers. The only multicast routing protocol that is fully supported on Cisco IOS devices is PIM (Protocol Independent Multicast). Protocol Independent Multicast (PIM) is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs. Typically, either PIM Sparse Mode or PIM Dense Mode will be used throughout a multicast domain. PIM is a multicast routing protocol that routes multicast traffic between network segments. PIM can use any of the unicast routing protocols to identify the path between the source and receivers. Multicast routers create distribution trees that define the path that IP multicast traffic follows through the network to reach the receivers.

Dense Mode:

Dense mode multicast routing protocols are used for networks where most subnets in your network should receive the multicast traffic. When a router receives the multicast traffic, it will flood it on all of its interfaces except the interface where it received the multicast traffic on. PIM (Protocol Independent Multicast) is the most popular multicast routing protocol. Dense mode floods multicast traffic until a router asks you to stop.



Sparse Mode:

When you only have a few receivers on your network then yes, you will be wasting a lot of bandwidth and resources on your routers. The alternative is sparse mode which is far more efficient. Sparse mode multicast routing protocols only forward the multicast traffic when another router requests it. It's the complete opposite of dense mode. Sparse mode sends multicast traffic only when a router requests it.