# IP MULTICAST

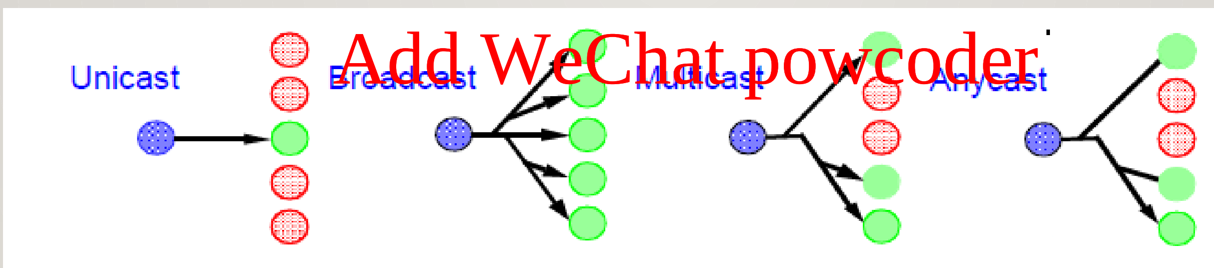


GUIDED BY: PROF. THOMAS REDDINGTON

# INTRODUCTION TO IP MULTICAST

- **IP multicast** is a method of sending **IP packets** to a group of interested receivers in a single transmission.
- It is a form of **point-to-multipoint** communication.





# ANYCAST

- In anycast, datagrams from a single sender are routed to **any one of several destination** nodes, selected on the basis of which is the nearest, lowest cost, with the least congested route, or some other distance measure.



- Used in **Google Public DNS:** It functions as a recursive name server providing domain name resolution for any host on the Internet.
- Google operates DNS name servers at the following IP addresses- **8.8.8.8** & **8.8.4.4**
- The addresses are mapped to the nearest operational server by anycast routing.

# APPLICATIONS OF MULTICAST

- Streaming continuous media (the transfer of the audio, video, and text of a live lecture to a set of distributed lecture participants)
- Shared data applications (teleconferencing application that is shared among many distributed participants)
- Interactive gaming (multiplayer games)

# OVERVIEW OF IP MULTICAST

- Process: Multiple copies of IP packet are required because there are multiple receivers.
- In multicast, **source sends the packet only once**; the **nodes** in the network **take care of replicating the packet** to reach multiple receivers.
- **UDP** is commonly used as the transport layer protocol for multicast.
- **Design issue:** how to **identify the receivers** of a multicast packet and how to **address** a packet sent to these receivers.
- The direction of interfaces and routers towards the **source** is called **upstream** and the direction towards the **receivers** is called **downstream**.

# MULTICAST GROUP ADDRESS

- MULTICAST GROUPS: A single **identifier** is used for the **group of receivers**, and a copy of the packet that is addressed to the group using this single identifier is delivered to all of the multicast receivers associated with that group. In the Internet, the single identifier that represents a group of receivers is **a class D multicast IP address** (224.0.0.0 to 239.255.255.255).
- An IP multicast group address is used by sources and the receivers to send and receive multicast messages.
- Sources use the group address as the IP destination address in their data packets.
- Receivers use this group address to inform the network that they are interested in receiving packets sent to that group.

# MULTICAST GROUP ADDRESS (EXAMPLE)

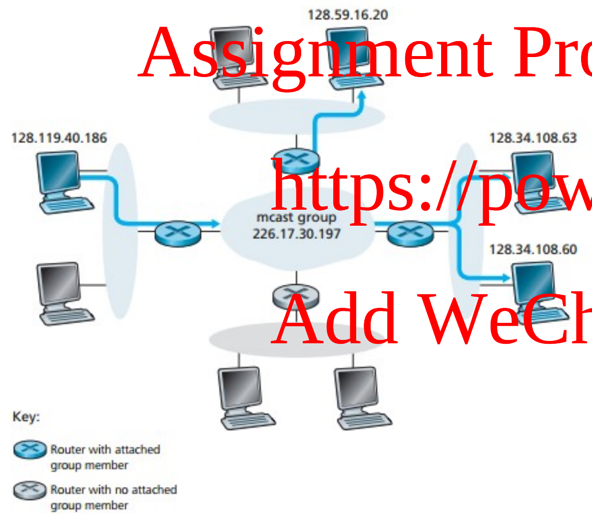



**Figure** ♦ The multicast group: A datagram addressed to the group is delivered to all members of the multicast group



- Here, four hosts (shown in shaded color) are associated with the **multicast group address of 226.17.30.197** and will receive all datagrams addressed to that multicast address.

# KEY CONCEPTS OF MULTICAST

- **Multicast addressing**
  - Define a common group IP address for all nodes in each multicast group. (layer-3)
  - Map a multicast group IP address to a MAC address for Layer-2.
- **Multicast group management**
  - A multicast group is dynamic; users may join and leave the group during the multicast session.
  - A multicast router needs to keep track of the memberships of all the multicast groups.

– **Protocol**

- **Multicast routing**
  - Find and maintain a multicast tree from one participating node to all other nodes in the group.
  - The tree should be updated when the network topology changes, or the group membership changes.

# MULTICAST GROUP (IGMP)

- **Receivers join a group** using Internet Group Management Protocol (IGMP).



- **The IGMP protocol** version 3 [RFC 3376] **operates between a host and its directly attached router** (informally, we can think of the directly attached router as the first hop router that a host would see on a path to any other host outside its own local network, or the last-hop router on any path to that host).





- IGMP provides the means for a **host to inform its attached router** that an application running on the host **wants to join a specific multicast group**.

# MULTICAST GROUP (IGMP)

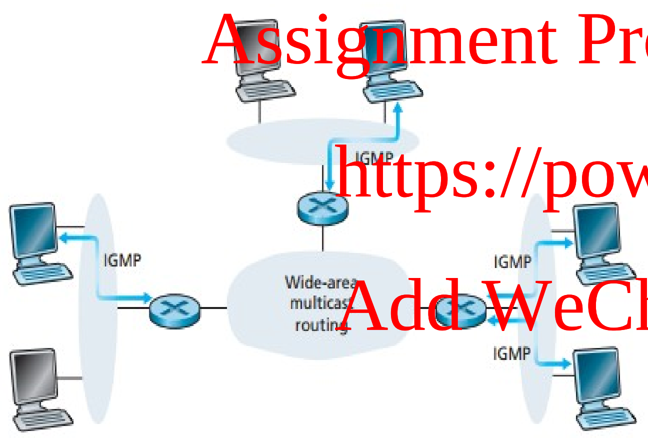



**Figure** ♦ The two components of network-layer multicast in the Internet: IGMP and multicast routing protocols

- IGMP interaction is limited to a host and its attached router, therefore another protocol **is clearly required to coordinate the multicast routers** throughout the Internet, **so that multicast datagrams are routed to their final destinations.** This latter functionality is accomplished by network-layer multicast routing algorithms.
- IP multicast thus consists of two complementary components: IGMP and multicast routing protocols.

# IGMP - OVERVIEW

- Like ICMP, IGMP messages are carried (encapsulated) within an IP datagram, with an IP protocol number of 2.
- Every IGMP message is sent with an IP Time-to-Live of 1. Exchanged between the router and attached host hence one hop only.
- IGMP has only three message types :-
  - membership_query
  - membership_report
  - leave_group

# IGMP - OVERVIEW

- The **membership_query** message is **sent by a router to all hosts on an attached interface** to determine the set of all multicast groups that have been joined by the hosts on that interface.
- Hosts respond to a membership_query message with an IGMP **membership_report message.** membership_report messages can also be generated by a host when an application first joins a multicast group without waiting for a membership_query message from the router.
- A host in a multicast group sends a **leave_group** message to the router signaling that it is leaving a multicast group.

# IGMP - OVERVIEW

- **leave_group** message is **optional**, then how does a router detect when a host leaves the multicast group?
  - The router infers that a host is no longer in the multicast group if it no longer responds to a membership_query message with the given group address.

# MULTICAST ROUTING ALGORITHMS (MULTICAST ROUTING PROBLEM)

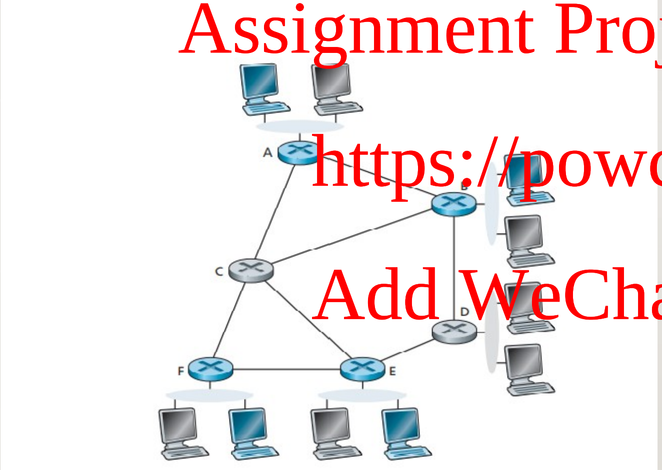



**Figure** ♦ Multicast hosts, their attached routers, and other routers



- Only a **subset of routers** (those with **attached hosts** that are joined to the **multicast group**, shaded in blue) actually needs to receive the multicast traffic.
- Neither C nor D needs to receive the multicast group traffic.

# MULTICAST ROUTING TREE

- The **goal** of multicast routing, is to **find a tree of links that connects all of the routers that have attached hosts belonging to a multicast group**.
- **The tree may contain** routers that do not have attached hosts belonging to the multicast group (for example, in previous figure it is impossible to connect routers A, B, E, and F in a tree without involving either router C or D).
- 2 approaches for determining multicast routing tree:

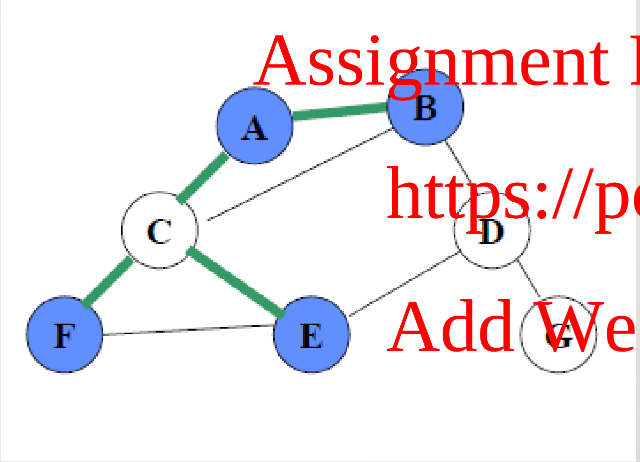
  **1) Multicast routing using a group-shared tree**

  **2) Multicast routing using a source-based tree:**

# GROUP-SHARED TREE

- A single routing tree is constructed for the entire multicast group. 
- It is **a center-based approach** in which **a central node**(rendezvous point or a core) is defined. 
- Nodes (**edge routers** attached to multicast group hosts) then unicast tree-join messages addressed to the center node. 

# GROUP SHARED TREE






- A tree-join message is forwarded using unicast routing toward the center until it either arrives at a node that already belongs to the spanning tree or arrives at the center.
- In either case, **the path that the tree-join message has followed** defines the **branch** of the spanning tree.

# SOURCE-BASED TREE

- An individual routing tree is constructed for each sender in the multicast group.

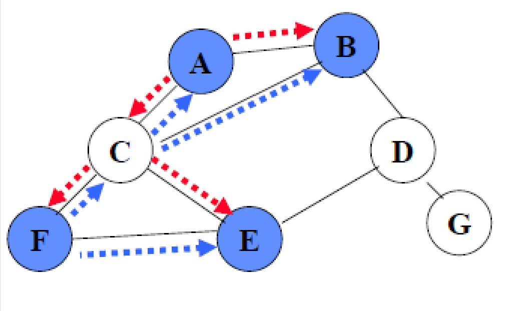


- In a multicast group with N hosts, N routing trees (which can also be identical to each other) will be constructed for each sender in the multicast group.





- Uses RPF (reverse path forwarding) algorithm.



# REVERSE PATH FORWARDING

- When a router receives a multicast packet with a given source address, **it transmits the packet on all of its outgoing links** (except the one on which it was received) **only if the packet arrived on the link that is on its own shortest unicast path back to the source.**
- Otherwise, the router simply discards the incoming packet without forwarding it on any of its outgoing links. Such a packet can be dropped because the router knows it either will receive or has already received a copy of this packet on the link that is on its own shortest path back to the sender.
- RPF does **not use unicast routing to actually deliver a packet to a destination.**

# REVERSE PATH FORWARDING

- Thick lines represent the least-cost paths from the receivers to the source (A).
- Node A initially multicasts a source-A packet to nodes C and B.
- Node B will forward the source-A packet it has received from A (since A is on its least-cost path to A) to both C and D.

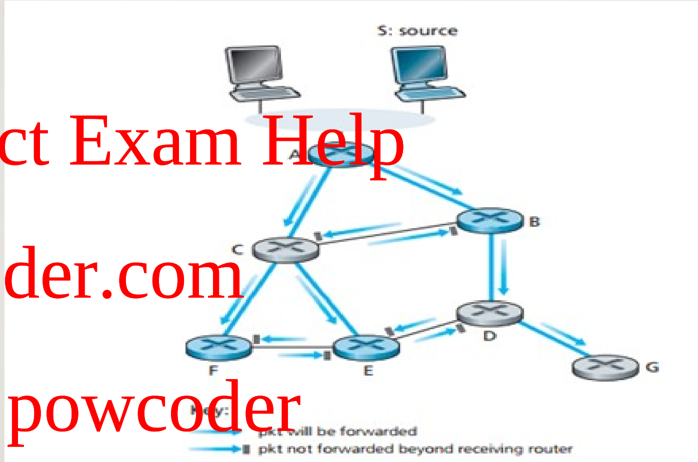



**Figure** ◆ Reverse path forwarding, the multicast case

# REVERSE PATH FORWARDING

- C will receive a source-A packet directly from A as well as from B.
- Since B is not on C's own shortest path back to A, C will ignore any source-A packets it receives from B.
- On the other hand, when C receives a source-A packet directly from A, it will forward the packet to nodes B, E, and F.

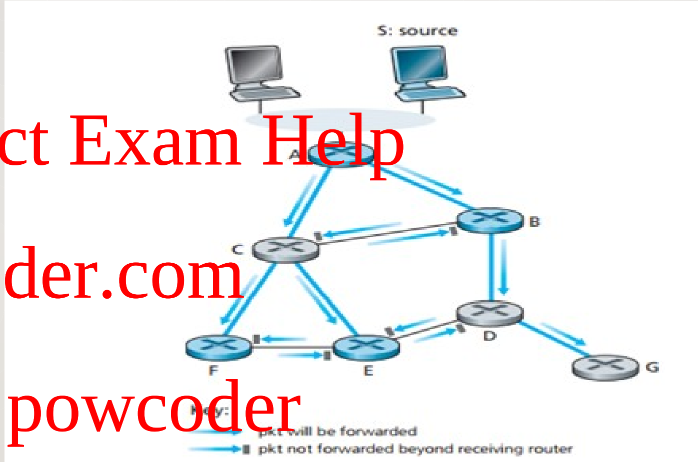



Figure ◆ Reverse path forwarding, the multicast case

# FLOODING

- The source node sends a copy of the packet to all of its neighbors. When a node receives a multicast packet, it duplicates the packet and forwards it to all of its neighbors (except the neighbor from which it received the packet).

# PRUNING

- Pruning solves the problem of receiving unwanted packets.
- Consider previous example of in which RPF would forward packets to router G, even though router G has no attached hosts that are joined to the multicast group.
- While this is not so bad for this case where D has only a single downstream router, G, imagine what would happen if there were thousands of routers downstream from D!
- A multicast **router** that receives multicast packets and has **no attached hosts joined to that group will send a prune message to its upstream router.** If a router receives prune messages **from each of its downstream routers**, then it can forward a prune message upstream.

# MULTICAST ROUTING ALGORITHM: DVMRP

- Distance-Vector Multicast Routing Protocol (DVMRP) implements **source-based trees** with **reverse path forwarding** and **pruning.**


- Hence 3 key concepts:
  - Source based trees
  - Reverse path forwarding
  - Pruning

# MULTICAST ROUTING ALGORITHM: PIM

- PIM (protocol independent multicast) is termed *protocol-independent* because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols. PIM is not dependent on a specific unicast routing protocol; it can make use of any unicast routing protocol in use on the network.

# MULTICAST ROUTING ALGORITHM: PIM

- PIM recognizes 4 multicast distribution scenarios:
  - Dense mode
  - Sparse mode
  - Bidirectional
  - Source specific multicast

# MULTICAST ROUTING ALGORITHM: PIM

- In **dense mode**, multicast group members are densely located; that is, many or most of the routers in the area need to be involved in routing multicast datagrams.
- PIM **dense mode** is a **flood-and-prune reverse path forwarding** technique similar in spirit to DVMRP.
- In **sparse mode**, the **number of routers with attached group members is small with respect to the total number of routers**; group members are widely dispersed. PIM sparse mode uses **rendezvous points (center based approach)** to set up the multicast distribution tree.
- PIM **sparse mode** builds unidirectional shared trees rooted at a *rendezvous point* (RP) per group.

# MULTICAST ROUTING ALGORITHM: PIM

- **Bidirectional PIM** explicitly builds shared bi-directional trees.
- In **PIM Source-Specific Multicast** only a **single sender is allowed to send** traffic into the multicast tree, considerably simplifying tree construction, maintenance and offering a more secure model

# LAYER-2 DELIVERY OF MULTICAST (HOW MULTICAST TRAVELS ON ETHERNET)

| Layer # | Layer Name | Protocol Data Unit |
|---|---|---|
| 5 | Application | Messages |
| 4 | Transport | Segments/ Datagrams |
| 3 | Network or Internet | Packets |
| 2 | Data Link | Frames |
| 1 | Physical | Bits |

- Comparison with delivery of unicast and broadcast packets on Ethernet:
  - **Unicast** packets are delivered to a specific recipient on an Ethernet setting a specific layer-2 **MAC** address on the Ethernet packet address.
  - **Broadcast** FF:FF:FF:FF:FF:FF

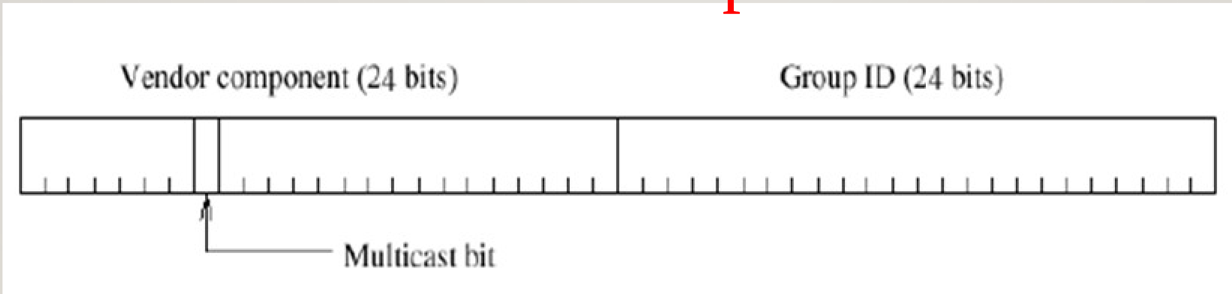
# LAYER-2 DELIVERY OF MULTICAST (HOW MULTICAST TRAVELS ON ETHERNET)

- **Multicast:** At the sender, a multicast destination IP address (used by Layer-3) is **directly mapped** to an Ethernet multicast address (Layer-2).
- This is because since receivers have **group IP address**, they also **need corresponding MAC** addresses.
- No need for ARP.

# ETHERNET MULTICAST ADDRESS

- A 48-bit long Ethernet address consists of
  - A 24-bit vendor component
  - A 24-bit group identifier: assigned by vendor
  - A multicast bit: **set** if the address is an Ethernet **multicast** address. (least significant bit of first octect).

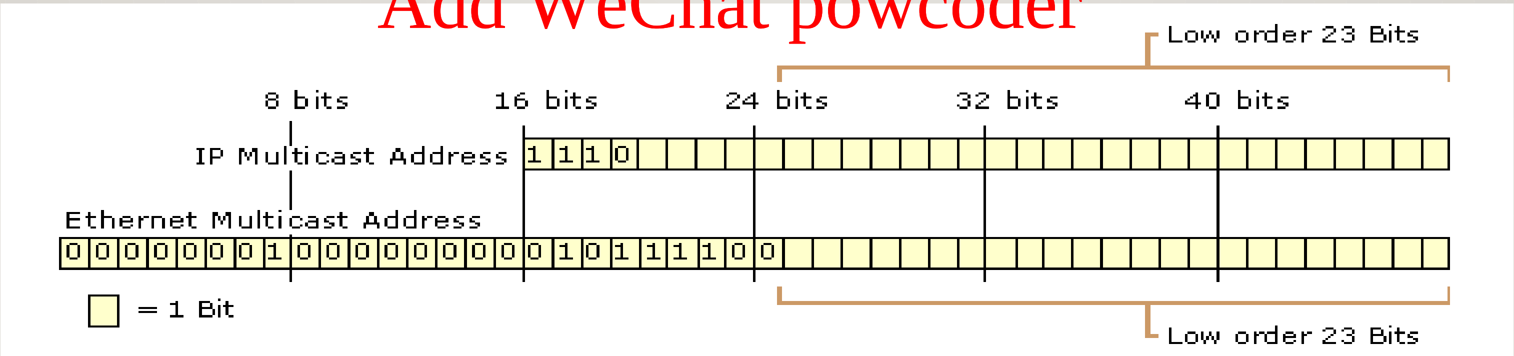




# ETHERNET MULTICAST ADDRESS (IP-MAC MAPPING)

- IP address which has 32 bits. A multicast IP address also has 32 bits **but the first 4 bits are always the same (1110)** because we use the 224.0.0.0 – 239.255.255.255 range (Class D). This means that each multicast IP address has **28 unique bits**.





# AMBIGUITY

- This means that there is **ambiguity** in delivering frames.
- If two hosts on the **same subnet** each subscribe to a different **multicast group** whose **address differs only in the first 5 bits,** Ethernet frames for both multicast groups will be delivered to both hosts.
- Network software in the hosts may need to **discard** the unrequired packets by **packet filtering.**

# MULTICAST AND SWITCHES

- If a **switch (layer-2 device) does not understand** Ethernet multicast addresses, then it will flood the frames to all the ports.
- In this case the **system's network card (NIC) or operating system has to filter** the frames sent (on layer-2) to multicast groups they are not subscribed to.
- There are switches that listen to **IGMP traffic** and maintain a **state table** that informs that which network systems are subscribed to a given multicast group. This table is then used to forward traffic destined to a given group only to a limited set of hosts (ports). This process of listening to the IGMP traffic is called **IGMP snooping.**

# IGMP SNOOPING

- IGMP snooping manages multicast traffic in switches by allowing **directed switching** of multicast traffic.
- IGMP snooping requires that the **switch examine**, or snoop, some **Layer 3 information (specifically IGMP join/leave messages)** in the **IGMP messages** that are sent between the hosts and the router. (IGMP will also require layer-2 transfer and hence they are accessible to switches).
- When the switch hears the IGMP host report from a host for a particular multicast group, **the switch adds the port number of the host to the associated multicast table entry.** When the switch hears the IGMP leave group messages from a host, the switch **removes** the table entry of the host.

# REFERENCES


- Computer Networking A Top-Down Approach 6th Edition
- TCP/IP essentials – A lab based approach
- https://en.wikipedia.org/wiki/IP_multicast
- https://learningnetwork.cisco.com/thread/39620
- https://technet.microsoft.com/en-us/library/cc957928.aspx?f=255&MSPPError=-2147217396