Multicast Routing

- Unicast: one source to one destination
- Multicast: one or more sources to many destinations
- Two main functions:
  - Efficient data distribution
  - Logical naming of a group

Multicasting

- One-to-many
  - Radio station broadcast
  - Transmitting news, stock-price
  - Software updates to multiple hosts

- Many-to-many
  - Multimedia teleconferencing
  - Online multi-player games
  - Distributed simulations
Unicast

- Without support for multicast
  - A source needs to send a separate packet with the identical data to each member of the group
    - This redundancy consumes more bandwidth
    - Redundant traffic is not evenly distributed, concentrated near the sending host
  - Source needs to keep track of the IP address of each member in the group
    - Group may be dynamic
Unicast

Multicast

- Basic IP multicast model is many-to-many based on multicast groups
  - Each group has its own IP multicast address
  - Hosts that are members of a group receive copies of any packets sent to that group’s multicast address
  - A host can be in multiple groups
  - A host can join and leave groups

Multicast

- Using IP multicast to send the identical packet to each member of the group
  - A host sends a single copy of the packet addressed to the group’s multicast address
  - The sending host does not need to know the individual unicast IP address of each member
  - Sending host does not send multiple copies of the packet
Multicast

Multicast

Multicast
Example applications

• Broadcast audio/video
• Push-based systems
• Software distribution
• Web-cache updates
• Teleconferencing (audio, video, shared whiteboard, text editor)
• Multi-player games

Multicasting Overview

• IP’s original many-to-many multicast has been supplemented with support for a form of one-to-many multicast
• One-to-many multicast
  – Source specific multicast (SSM)
  – A receiving host specifies both a multicast group and a specific sending host
• Many-to-many model
  – Any source multicast (ASM)

Multicasting Overview

• A host signals its desire to join or leave a multicast group by communicating with its local router using a special protocol
  – In IPv4, the protocol is Internet Group Management Protocol (IGMP)
  – In IPv6, the protocol is Multicast Listener Discovery (MLD)
• The router has the responsibility for making multicast behave correctly with regard to the host
Multicast Routing

- A router’s unicast forwarding tables indicate for any IP address, which link to use to forward the unicast packet.
- To support multicast, a router must additionally have multicast forwarding tables that indicate, based on multicast address, which links to use to forward the multicast packet.
- Unicast forwarding tables collectively specify a set of paths.
- Multicast forwarding tables collectively specify a set of trees:
  - Multicast distribution trees

Components of the IP Multicast Architecture

1. Service model
2. Host-to-router protocol (IGMP)
3. Multicast routing protocols (various)

IP Multicast Service Model (RFC-1112)

- Each group identified by a single IP address
  - Group members are not known explicitly
- Groups may be of any size
- Members of groups may be located anywhere in the Internet
- Members of groups can join and leave at will
- Senders need not be members
- Analogy:
  - each multicast address is like a radio frequency, on which anyone can transmit, and to which anyone can tune-in.
IP Multicast Addresses

Class D IP addresses:

```
1 1 1 0
```

in “dotted decimal” notation: 224.0.0.0 — 239.255.255.255

Two administrative categories:

– “well-known” multicast addresses, assigned by IANA/ICANN
– “transient” multicast addresses, assigned and reclaimed dynamically

Components of the IP Multicast Architecture

- service model
- host-to-router protocol (IGMP)
- multicast routing protocols (various)

Internet Group Management Protocol (IGMP)

- The protocol by which hosts report their multicast group memberships to neighboring routers
- Version 1 is specified in RFC-1112
- Operates over broadcast LANs and point-to-point links
- Occupies similar position and role as ICMP in the TCP/IP protocol stack
How IGMP Works

- On each link, one router is elected the “querier”
- Querier periodically sends a Membership Query message to the all-systems group (224.0.0.1), with TTL = 1
- On receipt, hosts start random timers (between 0 and 10 seconds) for each multicast group to which they belong

How IGMP Works (cont.)

- When a host’s timer for group G expires, it sends a Membership Report to group G, with TTL = 1
- Other members of G hear the report and stop their timers
- Routers hear all reports, and time out non-responding groups

How IGMP Works (cont.)

- In normal case, only one report message per existing group is sent in response to a query
  - routers need not know who all the members are, only that at least one member exists
- Query interval is typically 60—90 seconds
- When a host first joins a group, it sends one or two immediate reports, instead of waiting for a query
Early Routing Techniques

- **Flood and prune**
  - begin by flooding traffic to entire network
  - prune branches with no receivers
  - *unwanted state where there are no receivers*
- **Link-state multicast protocols**
  - Routers advertise groups for which they have receivers to entire network
  - compute trees on demand
  - *unwanted state where there are no senders*

Rendezvous Options

- **Broadcast initial packets from each source to entire network; non-members prune**
  - examples: DVMRP, PIM-DM
- **Broadcast membership advertisement from each edge to entire network**
  - example: MOSPF
- **Specify “meeting place” to which sources send initial packets, and receivers join; requires mapping between multicast group address and “meeting place”**
  - examples: CBT, PIM-SM

Shared v.s. Source-based Trees

- **Source-based trees**
  - separate shortest path tree for each sender
- **Shared trees:**
  - single tree shared by all members
  - data flows on same tree regardless of sender
A shared tree

Source-based trees

Shared v.s. Source-Based Trees

- Source-based trees
  - shortest path trees - low delay, better load distribution
  - more state at routers (per-source state)
  - efficient for dense-area multicast
- Shared trees
  - higher delay (bounded by factor of 2), traffic concentration
  - per-group state at routers
  - efficient for sparse-area multicast
Multicast Forwarding

- How do the forwarding entries at a router look like?
- Shared tree: 
  - (\(<\ast, G>\), list of outgoing interfaces)
- Source-based tree: 
  - (\(<\text{src}, G>\), list of outgoing interfaces)
- Compare to Unicast: 
  - (prefix, outgoing interface)

Protocol taxonomy

- **DVMRP** – Distance-Vector Multicast Routing Protocol - source-based trees
- **MOSPF** – Multicast Open Shortest Path First Protocol - source-based trees
- **PIM** – Protocol Independent Multicast - shared and source-based trees
- **CBT**: Core-Based Trees – shared tree

Distance-Vector Multicast Routing Protocol

DVMRP consists of two major components:
- a conventional distance-vector routing protocol (like RIP)
- a protocol for determining how to forward multicast packets, based on the routing table
**Multicast forwarding**

- A DVMRP router forwards a packet if
  - the packet arrived from the link used to reach the source of the packet (Reverse path forwarding - RPF)
  - similar (but not quite the same) to flooding each packet once
  - if downstream links have not pruned the tree

---

**Example Topology**

[Diagram of a network topology]

---

**Phase 1: Flood using Truncated Broadcast**

[Diagram of the flood process with truncated broadcast]

- Router with no Receivers does not broadcast
Phase 2: Prune

Phase 3: Graft

Phase 4: Steady State
Cores, centers, and rendezvous points

Protocol Independent Multicast (PIM)

Rendezvous

• With source-based trees senders and receivers meet by:
  – flooding and pruning
  – LS distribution of group and receiver state
• How do we solve the problem with shared trees?
  – establish a meeting place: center, core or rendezvous point
  – associate the meeting place with G
Using a core to construct a tree

Data flow when sender is near core

Data flow when sender away from core
Observations - Shared Trees

- Core placement affects efficiency
- Finding the optimal core location is an NP-hard problem
  - most protocols use heuristics
- For dynamic groups core location may have to be calculated frequently
- Need multiple cores for robustness

Status of IP Multicast

- IP multicast has had limited deployment
  - Even though most routers support the protocols
- Problems include, pricing, service model (not what users wanted), security, scalability
- Two ways forward:
  - Single Source Multicast (SSM)
  - Application-layer multicast: a form of overlay, also known as end-point multicast

Changing the Service Model

- What we’ve discussed so far
  - Any-source multicast
- Problems:
  - How do you charge users?
  - How do you manage the bandwidth allocation?
  - How can you ensure secure communication?
  - All of these are still research topics
- Other problems
  - Multicast state aggregation
- Is there a simpler alternative we can deploy now?
Single Source Multicast (SSM)

- ISP acceptance will be higher
  - If the multicast service model restricted the senders
  - If there was a way to figure out how many receivers there were
  - They can then have a viable billing and accounting model
  - Simplest such scheme
    - Single-source per multicast group
    - Receivers can still join and leave at will

SSM Groups

- A group in SSM is denoted by (S,G)
  - S is the source’s address
  - G is the group identifier
- Address allocation
  - Aside: we haven’t talked about multicast address allocation
  - But this immediately solves the multicast address allocation problem!
    - Unlike for any source multicast, G doesn’t have to be globally unique

SSM Details

- Receiver specifies that it wants to join source S on group G
  - Already being designed in IGMP v3
- Routers send source-specific joins towards S
  - PIM-SM already does this
- Only source S allowed to send traffic to group G
  - Routers silently drop other traffic if there is no state
- Note that we don’t need a special inter-domain multicast routing protocol
Overlay Networks

- A logical network built on top of a physical network
  - Overlay links are tunnels through the underlying network
- Many logical networks may coexist at once
  - Over the same underlying network
  - And providing its own particular service
- Nodes are often end hosts
  - Acting as intermediate nodes that forward traffic
  - Providing a service, such as access to files
- Who controls the nodes providing service?
  - The party providing the service (e.g., Akamai)
  - Distributed collection of end users (e.g., peer-to-peer)
End-System Multicast

- IP multicast still is not widely deployed
  - Technical and business challenges
  - Should multicast be a network-layer service?
- Multicast tree of end hosts
  - Allow end hosts to form their own multicast tree
  - Hosts receiving the data help forward to others
  - How to do routing?

Routing for Mobile Hosts

- Mobile IP
  - home agent
    - Router on the home network of the mobile hosts
  - home address
    - The permanent IP address of the mobile host.
    - Has a network number equal to that of the home network and thus of the home agent
  - foreign agent
    - Router on a network to which the mobile node attaches itself when it is away from its home network

- Problem of delivering a packet to the mobile node
  - How does the home agent intercept a packet that is destined for the mobile node?
    - Proxy ARP
  - How does the home agent then deliver the packet to the foreign agent?
    - IP tunnel
    - Care-of-address
  - How does the foreign agent deliver the packet to the mobile node?
Routing for Mobile Hosts

- Route optimization in Mobile IP
  - The route from the sending node to mobile node can be significantly sub-optimal
  - One extreme example
    - The mobile node and the sending node are on the same network, but the home network for the mobile node is on the far side of the Internet
      - Triangle Routing Problem
    - Solution
      - Let the sending node know the care-of-address of the mobile node.
        The sending node can create its own tunnel to the foreign agent
      - Home agent sends binding update message
      - The sending node creates an entry in the binding cache
      - The binding cache may become out-of-date
        - The mobile node moved to a different network
        - Foreign agent sends a binding warning message