Deployment Issues for the IP Multicast Service and Architecture

Outline

- What is IP Multicast
- What are the deployment challenges

IP Multicast

- Method for simultaneous data transfer to multiple hosts
- A channel only needs one stream to support all subscribers
- In contrast, unicast requires one stream for each end host
- Important: implemented at IP layer, thus involves hardware
- Myriad protocols
- Multicast is currently “open”, anyone can send/receive to/from any channel

Motivating applications

- Real time audio and video to multiple recipients
- Push applications that provide continues data updates (stock market data)
- Many-to-many group collaboration (large-scale multiplayer games)
- One-to-many file transfer (Windows update file)

Customer requirements

- Ubiquitous access to single mesh
- Deployment, management and data collection should be easy
- Group management for both senders and receivers that is secure and authenticated
- Unique addresses for providers
- Reliable transmission?

Deployment issues

- Hardware
  - Old hardware might not support multicast
  - Migration policies slow adoption
- Domain independence
  - ISPs do not have control over the streams
  - Peer agreements more complex
  - ... basically similar to what we have now...
  - Group control protocols introduce additional overhead and must be efficient

Deployment issues (cont.)

- Management
  - (as of paper writing) no deployed solution for hosts behind a NAT
  - Firewalls generally disallow multicast traffic and therefore might require a tunnel for private networks
- Cost
  - Unicast hardware is plentiful though adding a new user has a fixed network cost
  - Multicast hardware is more expensive while the marginal cost for adding an additional client is small
  - Suggests that large scale is needed for adoption

Missing functionality

- Group management
  - IP multicast lacks group access contols
  - Creates several issues
    - Flooding from malicious users
    - Session collisions destroying content
    - Unauthorized access to content
    - Malicious content replacement
- Security
  - Mainly extensions of the ACL issue
  - Scalable key-based encryption challenging
- To support, versatile routers needed

Missing functionality (cont.)

- Address allocation
  - Currently, anyone can send data on a given multicast address
  - Addresses unregulated
  - Address space is limited...
  - Router tables much more so (source address, group address entries), limiting no. of groups
  - Solutions
    - MAAA – complex dynamic allocation
    - Static assignment – considerable management overhead
    - Per-source allocation, address is a combination of source and multicast channel – addresses less common
    - IPv6

Missing functionality (cont.)

- Network management
- Billing
- ... other non-critical niceties...

Alternate Models

- Single sender
  - Alleviates many of the authorization and security issues
  - Routing simplified
- Multipeer service model
  - Not as well understood
  - Requires core rendezvous point
  - Distributed and centralized authorization tricky