draft-tarapore-mbone-multicast-cdni-05

Percy S. Tarapore, AT&T
Robert Sayko, AT&T
Greg Shepherd, Cisco
Toerless Eckert, Cisco
Ram Krishnan, Brocade

Scope of Document

- Develop ***Best Current Practice*** (BCP) for Multicast Delivery of Applications Across Peering Point Between Two Administrative Domains (AD):
  - Describe Process & Establish Guidelines for Enabling Process
  - Catalog Required Information Exchange Between AD's to Support Multicast Delivery
  - Limit Discussion to "Popular Protocols" (PIM-SSM, IGMPv3, MLD)
- Identify "Gaps" (if any) that may Hinder Such a Process
- Gap Rectification (e.g., New Protocol Extensions) is Beyond the Scope of this BCP Document

Revision History

- Vancouver 2012 - Revision 0 Proposed as a BCP for Content Delivery via Multicast Across CDN Interconnections.
- Atlanta 2012 – Revision 1 Preempted due to Hurricane Sandy
- Orlando 2013 – Revision 2 Proposed as General Case for Multicast Delivery of Any Application Across two AD's:
  - CDNi Case is One Example of this General Scenario
- Berlin 2013 – Revision 3 provides detailed text for Use Cases in section 3 ➔ ***Accepted as Working Group Draft.***
- Vancouver 2013 – Revision 4 added new use (section 3.5) & proposed guidelines for each use case in section 3.
- ***London 2014 – Revision 5 Additions in Section 4:***
  - ***Section 4.1: Interconnection Transport & Security Guidelines***
  - ***Section 4.2: Routing Aspects/Guidelines for all Use Cases***

Network Interconnection Transport Guidelines (Section 4.1)

"Network Interconnection Transport" ⇔ Peering Point between 2 Administrative Domains. Attribute list to be Exchanged between AD's to Support Multicast:

- Number of Peering Points, Addresses & Locations
- Type: Dedicated for Multicast or Shared with Other Transport
- Mode: Direct or via Another ISP
- Protocol Support (e.g., eBGP, BGMP, MBGP)
- Bandwidth Allocation/Utilization for Multicast
- QoS Requirements (per SLA)
- AD Roles & Responsibilities

Network Interconnection Security Guidelines (Section 4.1)

Assumption: "Normal" Security Procedures will be Followed by the 2 Administrative Domains to Deliver Services via Multicast to ***Registered & Authenticated End Users***.

Additional Security Aspects:

- Encryption Use: Peering Point interconnection may be encrypted if dedicated for Multicast Transport
- Security Breach Mitigation Plan:
  - Determine if Peering Point(s) is Impacted by Security Breach
  - Shut Down Impacted Peering Point & Re-route Multicast traffic to Alternate Peering Point(s)
  - Share Appropriate Information to Secure Impacted Peering Point(s)

Routing Aspects (Section 4.2)

General Considerations:

- "Optimal Source" for Multicast (Applies to Native & AMT):
  - Maximizes Multicast Portion of Transport
  - Minimizes any Unicast Portion of Transport
  - Minimizes Overall Combined Network(s) Route Distance
- Solution Must Be:
  - Scalable
  - Avoid/Minimize New Protocol Development
  - Robust & Reliable

Routing Aspects for Native (Section 4.2.1) & GRE Tunnel (Section 4.2.2)

Discussion Applies to Use Cases 3.1 (E2E Native) and 3.2 (E2E Native with GRE Tunnel Across Peering Points).

Multicast Delivery Process is the Same for Both Cases:

- AD's Advertise Source Address(es) at Their Peering Point Border Routers
- EU Client Obtains Relevant Information via File Transfer (Manifest File) Including:
  - (S, G)
  - Other Relevant Information
- Client Uses Join Message from (S, G) to Join Multicast Stream
- AD's Need to:
  - Advertise Source ID's over Peering Points
  - Exchange Peering Point Status (Capacity, Utilization, etc.)

Routing Aspects for AMT Use Cases (Section 4.2.3)

AMT Use Cases Have Two Criteria:

- Find Closest AMT Relay with Multicast Connectivity to End User
- Minimize AMT Unicast Tunnel Distance

Two AMT Components:

- AMT Relay:
  - Receives Stream Natively from Multicast Source
  - Encapsulates Multicast Packets into Unicast Packets
  - Transmits Unicast Stream to Gateway(s)
- AMT Gateway:
  - Resides on an End Point (EU Device, Set Top Box)
  - Receives Join/Leave Requests from Application
  - Allows End Point to Act Like a True Multicast End Point

Routing Aspects for AMT Use Cases (Section 4.2.3)

Use Case 3.3:

- Both AD's are Native Multicast Enabled
- Peering Point Not Multicast Enabled
- AMT Tunnel Established between Relay (AD-1) & GW (AD-2):
  - Two AD's Advertise Special AMT Relay Anycast Addresses with Each Other
  - Alternately, AD's Provision Relay Addresses (Not Optimal for Scalability)

Routing Aspects for AMT Use Cases (Section 4.2.3)

Use Cases 3.4 & 3.5 (AD-2 Not Multicast Enabled).
Multicast Delivery Process is as Follows:

- EU Client Receives Relevant Information (via Manifest File) such as (S, G)
- DNS Query Initiated to Enable EU Client/Gateway to Connect to an AMT Relay
- Query Results Return Relay Anycast Addresses which is Used to Return Specific IP Address of AMT Relay Based on Routing Rule (e.g., Closest Relay)
- AMT Tunnel Established Between GW/Relay Pair
- (S, G) Info Used to Join Multicast Stream

Routing Process Information Exchange to be Completed!!

Next Steps

- Complete Section 4.2
- Start Work on Rest of Section 4
- Request Comments on New Draft Text

Thank You