Multicasting Applications Across Inter-Domain Peering Points

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
- Identify "Gaps" (if any) that may Hinder Such a Process
- Current Status:
  - "Kitchen Sink" Approach towards BCP Development
  - Focus is on SP ⇔ SP interaction to setup service
- ***Discussion Requested (Goldilocks Rules):***
  - ***Is the BCP Draft "Too Much", "Too Little", or "Just Right"?***
  - ***What do we have to do get this ready for Last Call?***

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 case (section 3.5) & proposed guidelines for each use case in section 3.
- London 2014 – Revision 5 added sections 4.1 (Transport & Security) & 4.2 (Routing) Guidelines.
- Toronto 2014 – Revision 6 added text in section 4.3 Back-Office Functions
- Honolulu 2014 – Revision 7 added text to sections 4.4 (Operations), 4.5 (Client Reliability Models), 5 (Security) , & 7 (Conclusions

Draft Name Change??

- Draft initiated to address use of multicast for distributing CDN-I
- Initiated as:
  - draft-tarapore-mboned-multicast-cdni
- Adopted as WG document in Berlin (IETF 87) but draft indicator not changed
- Latest version: 07 of draft
- What should new name be and how can it be uploaded??

Section 2 - Overview

- Two Independent AD's Connected via Peering Point
- Peering Point is:
  - Multicast Enabled, or
  - Provisioned via a Tunnel which is Either:
    - GRE Tunnel, or
    - AMT
- Domain A is Multicast Enabled; Domain B May or May Not Be
- Application (e.g., Live Stream) Source in Domain A & End User (EU) Associated with Domain B.
- End User (One of Many EUs) Requests Application
- Application Delivered via Multicast from Source Through Peering Point to EU in Domain B

Section 3 – Use Cases

- 3.1: End-to-End Native Multicast
- 3.2:
  - Native Multicast in Both Domains
  - Peering Point Enabled with GRE
- 3.3:
  - Native Multicast in Both Domains
  - Peering Point Enabled with AMT Tunnel
- 3.4:
  - Native Multicast in Domain A
  - No Multicast in Domain B
  - "Long Tunnel" Across Peering Point to End User
- 3.5:
  - Same Scenario as 3.4
  - "Long Tunnel" broken up into chained series of shorter tunnels

Section 4 – Supporting Functions

- 4.1: Network Interconnection Transport & Security Guidelines
- 4.2: Routing Aspects:
  - 4.2.1: Native Multicast Routing
  - 4.2.2: GRE Tunnel Across Peering Point
  - 4.2.3: AMT Tunnels (Use Cases 3.3, 3.4, 3.5)
- Question: Should there be additional discussions on multicast protocols?
  - Resolve situation where the two domains may not utilize the same protocols??

Section 4 (continued)

- 4.3: Back Office Functions:
  - 4.3.1: Provisioning
  - 4.3.2: Application Accounting and Billing
  - 4.3.3: Log Management
  - 4.3.4: Settlements
- 4.4: Operations – Service Performance & Monitoring
- 4.5: Client Reliability Models & Service Assurance

Ending Sections

- 5: Security Considerations
- 6: IANA Considerations
- 7: Conclusions:
  - Identified Need to Determine Method for Finding "Optimal" AMT Gateway ⇔ Relay Pairs to Support AMT Tunnel Setup