Deploying Interdomain IP Multicast

Agenda

- ISP Solutions Overview
- MBGP (routing)
- MSDP (source discovery)
- MBGP/MSDP Examples
- SSM (Source Specific Multicast)
- IPv6
- Security
Service Providers

Business Drivers for Using Multicast

- Provide corporate enterprise customers Multicast connectivity
- Moving from offering Layer 2 to Layer 3 Services
  
  example: FR, ATM → VPN Services

Applications used

- Multicast as a Service Differentiator
- Offer separate Multicast VPN
- Be a transit provider for Internet Multicast traffic

Interdomain Multicast Solutions

- Open Access Content
  - Access Grid
  - Multicast Technologies
  - NASA
  - Berkeley Seminar Series
- Closed Access Content
  - Moving traffic from content providers to access providers
  - VPN services for Enterprise customers
Tier 1 Peering at Multicast Exchange

Peering Solution: MBGP + PIM-SM + MSDP

ISP A
ISP B
ISP C

Public Interconnect

PIM-SM
RP
iMBGP
eMSDP
eMBGP

AS 10888

Multicast VPN

Provider’s Point of View

- Each Multicast Domain consists of a Default-MDT.
- Each Default-MDT uses a separate Multicast Group inside of Provider’s Network.
Agenda

- ISP Solutions Overview
- MBGP (routing)
- MSDP (source discovery)
- MBGP/MSDP Examples
- SSM (Source Specific Multicast)
- IPv6
- Security

Multicast Components
Cisco End-to-End Architecture

Campus Multicast
- End Stations (hosts-to-routers):
  - IGMP
- Switches (Layer 2 Optimization):
  - CGMP, IGMP Snooping or RGMP
- Routers (Multicast Forwarding Protocol):
  - PIM Sparse Mode or Bidirectional PIM

Interdomain Multicast
- Multicast routing across domains
  - MBGP
- Multicast Source Discovery
  - MSDP with PIM-SM
- Source Specific Multicast
  - PIM-SSM
MBGP Overview

- MBGP: Multiprotocol BGP
  - Defined in RFC 2283 (extensions to BGP)
  - Can carry different types of routes
    - IPv4 Unicast IPv6 Unicast
    - IPv4 Multicast IPv6 Multicast
  - May be carried in same BGP session
  - Does not propagate multicast state info
    - Still need PIM to build Distribution Trees
  - Same path selection and validation rules
    - AS-Path, LocalPref, MED, ...

- Separate BGP tables maintained
  - Unicast BGP Table (U-Table)
  - Multicast BGP Table (M-Table)
  - BGP ‘nlri’ keyword specifies which BGP Table
  - Allows different unicast/multicast topologies or policies

- Unicast BGP Table (U-Table)
  - Contains unicast prefixes for unicast forwarding
  - Populated with BGP unicast NLRI

- Multicast BGP Table (M-Table)
  - Contains unicast prefixes for RPF checking
  - Populated with BGP multicast NLRI
MBGP Update Message

- **Address Family Information (AFI)**
  - Identifies Address Type (see RFC1700)
    - AFI = 1 (IPv4)
    - AFI = 2 (IPv6)

- **Sub-Address Family Information (Sub-AFI)**
  - Sub category for AFI Field
  - Address Family Information (AFI) = 1 (IPv4)
    - Sub-AFI = 1 (NLRI is used for unicast)
    - Sub-AFI = 2 (NLRI is used for multicast RPF check)

PIM RPF Calculation Details

- Static Mroute Table
  - Route/Mask, Dist. (First Match)
    - Default Dist. = 1

- MBGP Table
  - Route/Mask, Dist. (Best Path)
    - IBGP Def. Dist. = 200
    - eBGP Def. Dist. = 20

- Unicast Routing Table
  - Route/Mask, Dist. (Longest Match)

- RPF Calculation
  - (Use best Distance unless “Longest Match” is enabled. If enabled, use longest Mask.)

Global Command: *ip multicast longest-match*
MBGP—Capability Negotiation

- Keyword on neighbor command
  ```
  neighbor <foo> remote-as <asn> nlri multicast unicast
  ```
  - Configures router to negotiate either or both NLRI
  - If neighbor configures both or subset, common NRLI is used in both directions
  - If there is no match, notification is sent and peering doesn’t come up

---

**MBGP — Capability Negotiation**

![Diagram of MBGP capability negotiation between two ASes](image)
MBGP — Capability Negotiation

**AS 123**

192.168.100.0/24

**AS 321**

192.168.100.2

router bgp 321
neighbor 192.168.100.1 remote-as 123 nlrinlri unicast multicast

MBGP — Capability Negotiation

**AS 123**

MBGP Session for Unicast and Multicast NLRI

192.168.100.0/24

**AS 321**

192.192.25.0/24

BGP: 192.168.100.2 open active, local address 192.168.100.1
BGP: 192.168.100.2 sent OPEN, version 4
BGP: 192.168.100.2 rcvd OPEN, version 4
BGP: 192.168.100.2 rcvd OPEN w/option parameter type: 2, len: 6
BGP: 192.168.100.2 OPEN has CAPABILITY code: 1, length 4
BGP: 192.168.100.2 OPEN has MP_EXT CAP for afi/safi: 1/1
BGP: 192.168.100.2 OPEN has MP_EXT CAP for afi/safi: 2, len: 6
BGP: 192.168.100.2 OPEN has CAPABILITY code: 1, length 4
BGP: 192.168.100.2 OPEN has MP_EXT CAP for afi/safi: 1/2
BGP: 192.168.100.2 went from OpenSent to OpenConfirm
BGP: 192.168.100.2 went from OpenConfirm to Established
• Storage of arriving NLRI information depends on AFI/SAFI fields in the Update message
  • Unicast BGP Table only (AFI=1/SAFI=1 or old style NLRI)

• Storage of arriving NLRI information depends on AFI/SAFI fields in the Update message
  • Unicast BGP Table only (AFI=1/SAFI=1 or old style NLRI)
  • Multicast BGP Table only (AFI=1/SAFI=2)
MBGP—NLRI Information

Congruent Topologies

BGP Session for Unicast and Multicast NLRI

Router bgp 321
neighbor 192.168.100.1 remote-as 123 nlri unicast multicast
network 192.192.25.0 255.255.255.0 nlri unicast multicast
no auto-summary

MBGP—NLRI Information

Incongruent Topologies

Router bgp 321
neighbor 192.168.100.1 remote-as 123 nlri unicast multicast
neighbor 192.168.200.1 remote-as 123 nlri multicast
MBGP Syntax Change

```
router bgp 5
 network 171.69.214.0 mask 255.255.255.0 nlri unicast multicast
 neighbor 171.69.214.38 remote-as 2 nlri unicast
 neighbor 171.69.214.50 remote-as 2 nlri multicast

Address-Family Syntax
```

```
router bgp 5
 no bgp default ipv4-unicast
 neighbor 171.69.214.38 remote-as 2
 neighbor 171.69.214.50 remote-as 2

!  address-family ipv4 unicast
  neighbor 171.69.214.38 activate
  network 171.69.214.0 mask 255.255.255.0
  exit-address-family

!  address-family ipv4 multicast
  neighbor 171.69.214.50 activate
  network 171.69.214.0 mask 255.255.255.0
  exit-address-family
```

MBGP—Summary

- Solves part of inter-domain problem
  - Can exchange multicast routing information
  - Uses standard BGP configuration knobs
  - Permits separate unicast and multicast topologies if desired
- Still must use PIM to:
  - Build distribution trees
  - Actually forward multicast traffic
  - PIM-SM recommended
Agenda

- ISP Solutions Overview
- MBGP (routing)
- **MSDP (source discovery)**
- MBGP/MSDP Examples
- SSM (Source Specific Multicast)
- IPv6
- Security

MSDP Overview

MSDP Example

MSDP Peers

Source Active Messages

Join (*, 224.2.2.2)

Register

192.1.1.1, 224.2.2.2

SA Message
192.1.1.1, 224.2.2.2

Domain A

Domain B

Domain C

Domain D

Domain E
MSDP Overview

MSDP Example

MSDP Peers
Multicast Traffic

Domain A
Domain B
Domain C
Domain D
Domain E

RP

S

Join

(S, 224.2.2.2)

Multicast Traffic

MSDP Peers

Domain A
Domain B
Domain C
Domain D
Domain E

RP

RP

Join

(S, 224.2.2.2)
MSDP SA Messages

- MSDP Source Active (SA) Messages
  - Used to advertise active Sources in a domain
  - Carry 1st multicast packet from source
    - Hack for Bursty Sources (ala SDR)
  - SA Message Contents:
    - IP Address of Originator (RP address)
    - Number of (S, G)’s pairs being advertised
    - List of active (S, G)’s in the domain
    - Encapsulated Multicast packet

Receiving SA Messages

- RPF Check Rules depend on peering
  - Rule 1: Sending MSDP peer = i(m)BGP peer
  - Rule 2: Sending MSDP peer = e(m)BGP peer
  - Rule 3: Sending MSDP peer != (m)BGP peer

- Exceptions:
  - RPF check is skipped when:
    - Sending MSDP peer = Originating RP
    - Sending MSDP peer = Mesh-Group peer
    - Sending MSDP peer = only MSDP peer
      - (i.e. the ‘default-peer’ or the only ‘msdp-peer’ configured.)
RPF Check Rule 1

- When MSDP peer = i(m)BGP peer
  - Find “Best Path” to RP in BGP Tables
    - Search MRIB first then URIB
    - If no path to Originating RP found, RPF Fails
  - Note “BGP peer” that advertised path
    - (i.e. IP Address of BGP peer that sent us this path)
    - Warning:
      - This is not the same as the Next-hop of the path!!
      - i(m)BGP peers normally do not set Next-hop = Self.
      - This is also not necessarily the same as the Router-ID!
  - Rule 1 Test Condition:
    - MSDP Peer address = BGP peer address?
      - If Yes, RPF Succeeds

Rule1: MSDP peer = i(m)BGP peer
Rule 1: MSDP peer = i(m)BGP peer

Common Mistake #1: Failure to use same addresses for MSDP peers as i(m)BGP peers!

show ip mbgp 172.16.6.1
BGP routing table entry for 172.16.6.0/24, version 8745118
Paths: (1 available, best #1)
7 5, (received & used)
172.16.5.1 (metric 68096) from 172.16.3.1

SA RPF Check Fails

172.16.5.1 (metric 68096) from 172.16.3.1
**Rule 1: MSDP peer = i(m)BGP peer**

- **Common Mistake #2:**
  - Failure to follow i(m)BGP topology!
  - Can happen when RR’s are used.

- i(m)BGP Peer address = 172.16.1.1
  - Advertising best-path to RP
- MSDP Peer address = 172.16.3.1
- MSDP Peer address != i(m)BGP Peer address

- **SA RPF Check Fails**
  - Show ip mbgp 172.16.6.1
  - BGP routing table entry for 172.16.6.0/24, version 8745118
  - Paths: (1 available, best #1)
    - 7 5, (received & used)
    - 172.16.5.1 (metric 68096) from 172.16.1.1
  - i(m)BGP Peer address = 172.16.1.1
  - MSDP Peer address = 172.16.3.1

**RPF Check Rule 2**

- **When MSDP peer = e(m)BGP peer**
  - Find (m)BGP “Best Path” to RP
    - Search MRIB first then URIB
      - If no path to Originating RP found, RPF Fails
  - Rule 2 Test Condition:
    - First AS in path to the RP = MSDP peer?
      - If Yes, RPF Succeeds
**Rule2: MSDP peer = (e)mBGP peer**

**SA RPF Check Succeeds**

```
First-AS in best-path to RP = 3
AS of MSDP Peer = 3
```

**SA RPF Check Fails!**

```
First-AS in best-path to RP != AS of (e)mBGP Peer
```

---

**Rule2: MSDP peer = e(m)BGP peer**

**SA RPF Check Succeeds**

```
First-AS in best-path to RP = 3
AS of MSDP Peer = 3
```

**SA RPF Check Fails!**

```
First-AS in best-path to RP != AS of (e)mBGP Peer
```

---

*Figure 1: Network diagram showing the configurations for MSDP peer and BGP peer.*

*Figure 2: Network diagram showing the configurations for MSDP peer and BGP peer.*
RPF Check Rule 3

- When MSDP peer != (m)BGP peer
  - Find (m)BGP “Best Path” to RP
    - Search MRIB first then URIB
      - If no path to Originating RP found, RPF Fails
  - Find (m)BGP “Best Path” to MSDP peer
    - Search MRIB first then URIB
      - If no path to sending MSDP Peer found, RPF Fails
  - Note AS of sending MSDP Peer
    - Origin AS (last AS) in AS-PATH to MSDP Peer
  - Rule 3 Test Condition:
    - First AS in path to RP = Sending MSDP Peer AS ?
      - If Yes, RPF Succeeds

Rule 3: MSDP peer != BGP peer

First-AS in best-path to RP = 3
AS of MSDP Peer = 3

First-AS in best-path to RP = AS of MSDP Peer

SA RPF Check Succeeds
Rule 3: MSDP peer ≠ BGP peer

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.3.0/24</td>
<td>172.16.1.1</td>
<td>3 i</td>
</tr>
<tr>
<td>172.16.4.0/24</td>
<td>172.16.1.1</td>
<td>3 i</td>
</tr>
<tr>
<td>172.16.5.0/24</td>
<td>172.16.1.1</td>
<td>3 i</td>
</tr>
<tr>
<td>172.16.3.0/24</td>
<td>172.16.2.1</td>
<td>3 i</td>
</tr>
</tbody>
</table>

First-AS in best-path to RP = 3
AS of MSDP Peer = 1

SA RPF Check Fails

Rule 3: MSDP peer ≠ BGP peer

More flexibility with MSDP peer placement

First-AS in best-path to RP = 3
AS of MSDP Peer = 3

SA RPF Check Succeeds
MSDP Configuration

- **Configure peers**
  
  ```
  ip msdp peer <ip-address> [connect-source <i/f>]
  ```

- **Configure default peer**
  
  ```
  ip msdp default-peer <ip-address> [prefix-list acl]
  ```

- **Mesh groups**
  
  ```
  ip msdp mesh-group <name> <ip-address>
  ```

---

MSDP Mesh-Group Example

```
ip msdp peer R2
ip msdp peer R3
ip msdp peer R4
ip msdp mesh-group My-Group R2
ip msdp mesh-group My-Group R3
```

**SA not forwarded to other members of the mesh-group**

---

MSDP mesh-group peering
MSDP Configuration

- Latest draft:
  draft-ietf-msdp-spec-20.txt
- Filtering
  - Can filter SA in/out, groups, with acls or route-maps
- For configuration commands see:
  - ftp://ftpeng.cisco.com/ipmulticast/Multicast-Commands
- For MSDP BCP (Best Current Practice) Draft:
  - draft-ietf-mboned-msdp-deploy-03.txt

Agenda

- ISP Solutions Overview
- MBGP (routing)
- MSDP (source discovery)
  - MBGP/MSDP Examples
- SSM (Source Specific Multicast)
- IPv6
- Security
Anycast RP—Overview

![Diagram of Anycast RP](image)

RP1: 10.1.1.1

RP2: 10.1.1.1

Rec

Rec

Rec

Rec

Src

Src

SA

SA

MSDP
Anycast RP Configuration

```
ip pim rp-address 10.0.0.1

Interface loopback 0
 ip address 10.0.0.2 255.255.255.255

Interface loopback 1
 ip address 10.0.0.1 255.255.255.255
 !
 ip msdp peer 10.0.0.3 connect-source loopback 0
 ip msdp originator-id loopback 0

Interface loopback 0
 ip address 10.0.0.3 255.255.255.255

Interface loopback 1
 ip address 10.0.0.1 255.255.255.255
 !
 ip msdp peer 10.0.0.2 connect-source loopback 0
 ip msdp originator-id loopback 0
```

Recommended MSDP SA Filter

```
rcp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt

! domain-local applications
access-list 111 deny ip any host 224.0.2.2  ! Rwhod
access-list 111 deny ip any host 224.0.1.1  ! Microsoft-ds
access-list 111 deny ip any host 224.0.1.24 ! SVRLOC
access-list 111 deny ip any host 224.0.1.2  ! SGI-Dogfight
access-list 111 deny ip any host 224.0.1.35 ! SVRLOC-DA
access-list 111 deny ip any host 224.0.1.40 ! hp-device-disc
  !-- auto-rp groups
access-list 111 deny ip any host 224.0.1.39
access-list 111 deny ip any host 224.0.1.40
  !-- scoped groups
access-list 111 deny ip any 239.0.0.0 0.255.255.255
  !-- loopback, private addresses (RFC 1918)
access-list 111 deny ip 10.0.0.0 0.255.255.255 any
access-list 111 deny ip 127.0.0.0 0.255.255.255 any
access-list 111 deny ip 172.16.0.0 0.15.255.255 any
access-list 111 deny ip 192.168.0.0 0.0.255.255 any
access-list 111 permit ip any any
  !-- Default SSM-range. Do not do MSDP in this range
access-list 111 deny ip any 232.0.0.0 0.255.255.255
access-list 111 permit ip any any
```
Single-Homed, ISP RP, Non-MBGP

Tail-site Customer

Transit AS109

<table>
<thead>
<tr>
<th>pos 0/0 1.1.1.1</th>
<th>pos 0/0 1.1.1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>int pos 0/0</td>
<td>int pos 0/0</td>
</tr>
<tr>
<td>ip pim sparse-dense-mode</td>
<td>ip pim sparse-dense-mode</td>
</tr>
<tr>
<td>ip pim bsr-border</td>
<td>ip pim bsr-border</td>
</tr>
<tr>
<td>ip multicast-boundary 1</td>
<td>ip multicast-boundary 1</td>
</tr>
<tr>
<td>ip pim rp-address 3.3.3.7 override</td>
<td>ip pim rp-address 3.3.3.7 override</td>
</tr>
</tbody>
</table>

```
int pos 0/0
ip pim sparse-dense-mode
ip pim bsr-border
ip multicast-boundary 1
ip pim rp-address 3.3.3.7 override
```

```
tail-gw#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4, Static-Override
RP: 3.3.3.7
```
Single-Homed, ISP RP, Non-MBGP

Tail-site Customer

Transit AS109

pos0/0 1.1.1.1  pos0/0 1.1.1.2

192.168.100.0/24

Receiver

Transit-tail#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4, Static-Override
RP: 3.3.3.7

Single-Homed, ISP RP, Non-MBGP

MSDP RPF Check

Tail-site Customer

Transit AS109

pos0/0 1.1.1.1  pos0/0 1.1.1.2

192.168.100.0/24

Receiver

Transit-tail#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4, Static-Override
RP: 3.3.3.7

- no RP / no MSDP

- no downstream RP
- no downstream MSDP peering
Single-Homed, ISP RP, Non-MBGP

**Multicast RPF Check**

```
ip route 0.0.0.0 0.0.0.0 1.1.1.1
router bgp 109
   network 192.168.100.0 nrli unicast multicast
```

- Receiver
- Transit AS109
- Multicast RPF Check
- pos0/0 1.1.1.1
- pos0/0 1.1.1.2
- ip route 192.168.100.0 255.255.255.0 1.1.1.1
- router bgp 109
- network 192.168.100.0 nrl unicast multicast

Note: Access-list 111 = Recommended SA Filter

Single-Homed, Customer RP, Non-MBGP

```
int pos0/0
   ip pim sparse-mode
   ip pim bsr-border
   ip multicast boundary 1
   ip msdp sa-filter out 1.1.1.2 111
   ip msdp sa-filter in 1.1.1.2 111
```

- Receiver
- Transit AS109
- RP
- pos0/0 1.1.1.1
- pos0/0 1.1.1.2
- int pos0/0
  - ip pim sparse-mode
  - ip pim bsr-border
  - ip multicast boundary 1
  - ip msdp sa-filter out 1.1.1.2 111
  - ip msdp sa-filter in 1.1.1.2 111

Note: Access-list 111 = Recommended SA Filter
Single-Homed, Customer RP, Non-MBGP

Tail-site Customer                   Transit AS109

192.168.100.0/24                  RPs pos0/0 1.1.1.1 pos0/0 1.1.1.2

Receiver

Note: Access-list 111 = Recommended SA Filter

---

Single-Homed, Customer RP, Non-MBGP

MSDP RPF Check

Tail-site Customer                   Transit AS109

192.168.100.0/24                  RPs pos0/0 1.1.1.1 pos0/0 1.1.1.2

Receiver

ip msdp peer 1.1.1.1 connect-source pos0/0
ip msdp peer 1.1.1.2 connect-source pos0/0
**Single-Homed, Customer RP, Non-MBGP**

**Multicast RPF Check**

<table>
<thead>
<tr>
<th><strong>Tail-site Customer</strong></th>
<th><strong>Transit AS109</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RP</strong></td>
<td><strong>RP</strong></td>
</tr>
<tr>
<td>pos0/0 1.1.1.1</td>
<td>pos0/0 1.1.1.2</td>
</tr>
<tr>
<td>ip route 192.168.100.0/24</td>
<td>ip route 192.168.100.0/24</td>
</tr>
<tr>
<td>ip route 0.0.0.0 0.0.0.0 1.1.1.1</td>
<td>ip route 255.255.255.0 1.1.1.1</td>
</tr>
<tr>
<td>router bgp 109</td>
<td>...</td>
</tr>
<tr>
<td>network 192.168.100.0 nlr unicast multicast</td>
<td>...</td>
</tr>
</tbody>
</table>

**Single-Homed, Customer RP, MBGP**

<table>
<thead>
<tr>
<th><strong>NANOG SLC</strong></th>
<th><strong>Transit AS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RP</strong></td>
<td><strong>RP</strong></td>
</tr>
<tr>
<td>pos0/0 1.1.1.1</td>
<td>pos0/0 1.1.1.2</td>
</tr>
<tr>
<td>int pos0/0</td>
<td>int pos0/0</td>
</tr>
<tr>
<td>ip pim sparse-mode</td>
<td>ip pim sparse-mode</td>
</tr>
<tr>
<td>ip pim bsr-border</td>
<td>ip pim bsr-border</td>
</tr>
<tr>
<td>ip multicast boundary 1</td>
<td>ip multicast boundary 1</td>
</tr>
<tr>
<td>ip msdp sa-filter out 3.3.3.3 111</td>
<td>ip msdp sa-filter in 3.3.3.3 111</td>
</tr>
</tbody>
</table>

Note: Access-list 111 = Recommended SA Filter
Single-Homed, Customer RP, MBGP

**NANOG SLC**
- Receiver
- 192.168.100.0/24

**Transit AS**
- RP
  - pos0/0 1.1.1.1
  - MSRP
  - 4.4.4.4
- MBGP
  - pos0/0 1.1.1.2
- MSDP
  - 3.3.3.3
- RP
  - 2.2.2.2

**Commands**
- int pos0/0
- ip pim sparse-mode
- ip pim bsr-border
- ip multicast boundary 1
- ip msdp sa-filter out 4.4.4.4 111
- ip msdp sa-filter in 4.4.4.4 111

---

**Single-Homed, Customer RP, MBGP**

**MSDP RPF Check**

**Commands**
- ip msdp peer 3.3.3.3 connect-source pos0/0
- ip msdp peer 4.4.4.4 connect-source pos0/0
Single-Homed, Customer RP, MBGP

Multicast RPF Check

NANOG SLC

Router bgp 100
network 192.168.100.0 nlri unicast multicast
neighbor 1.1.1.2 remote-as 109 nlri unicast multicast
neighbor 1.1.1.1 update-source pos0/0

Transit AS

Router bgp 109
neighbor 1.1.1.1 remote-as 100 nlri unicast multicast
neighbor 1.1.1.1 update-source pos 0/0

Multicast RPF Check

Single-Homed, Customer RP, MBGP

Multicast RPF Check

NANOG SLC

Router bgp 100
network 192.168.100.0 nlri unicast multicast
neighbor 1.1.1.2 remote-as 109 nlri unicast multicast
neighbor 1.1.1.1 update-source pos0/0

Transit AS

Router bgp 109
neighbor 1.1.1.1 remote-as 100 nlri unicast multicast
neighbor 1.1.1.1 update-source pos 0/0

Dual-Homed, Customer RP, MBGP

Incongruent Multicast—Unicast

Customer AS100

Int pos0/0
ip pim sparse-mode
ip pim bsr-border
ip multicast boundary 1
int pos1/0
ip msdp sa-filter out 1.1.1.2 111
ip msdp sa-filter in 1.1.1.2 111

Transit AS109

Transit AS110

Unicast Transit
Dual-Homed, Customer RP, MBGP
Incongruent Multicast—Unicast

Customer AS100

Receiver

192.168.100.0/24

Dual-Homed, Customer RP, MBGP
Incongruent Multicast—Unicast

Customer AS100

Receiver

192.168.100.0/24

Hey, this site knows no multicast so there is no PIM to constrain.
Dual-Homed, Customer RP, MBGP
Incongruent Multicast—Unicast

MSDP RPF Check

Customer AS100
RP
pos0/0 1.1.1.1
pos1/0 1.1.2.1
192.168.100.0/24
Receiver

Transit AS109
Multicast Transit

Transit AS110
Multicast Transit

Unicast Transit

ip msdp peer 1.1.1.2 connect-source pos0/0
ip msdp peer 1.1.1.1 connect-source pos0/0

Again, no multicast clue... Then no MSDP peering.

Dual-Homed, Customer RP, MBGP
Incongruent Multicast—Unicast

Multicast RPF Check

Customer AS100
RP
pos0/0 1.1.1.1
pos1/0 1.1.2.1
192.168.100.0/24
Receiver

Transit AS109
Multicast Transit

Transit AS110
Multicast Transit

Unicast Transit

router bgp 100
network 192.168.100.0 nlri unicast multicast
neighbor 1.1.1.2 remote-as 109 nlri multicast
neighbor 1.1.1.2 update-source pos 0/0
neighbor 1.1.2.2 remote-as 110 nlri unicast
neighbor 1.1.2.2 update-source pos 1/0

Multicast
Transit
Unicast
Transit
Dual-Homed, Customer RP, MBGP Incongruent Multicast—Unicast

Multicast RPF Check

Customer AS100

pos0/0 1.1.1.1

pos1/0 1.1.2.1

192.168.100.0/24

Receiver

RP

192.168.100.0/24

Transit AS109

Transit AS110

pos0/0 1.1.2.2

pos0/0 1.1.2.1

router bgp 109
neighbor 1.1.1.1 remote-as 100 ntlri multicast
neighbor 1.1.1.1 update-source pos 0/0

Transit

Unicast

Multicast

Transit

Unicast

router bgp 110
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 update-source pos0/0

Dual-Homed, Customer RP, MBGP Incongruent Multicast—Unicast

Multicast RPF Check

Customer AS100

pos0/0 1.1.1.1

pos1/0 1.1.2.1

192.168.100.0/24

Receiver

RP

192.168.100.0/24

Transit AS109

Transit AS110

pos0/0 1.1.2.2

pos0/0 1.1.2.1

router bgp 109
neighbor 1.1.1.1 remote-as 100 ntlri multicast
neighbor 1.1.1.1 update-source pos 0/0

Transit

Unicast

Multicast

Transit

Unicast

router bgp 110
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 update-source pos0/0
Dual-Homed, Customer RP, MBGP Congruent Multicast—Unicast

```
int pos0/0
ip pim sparse-mode
ip pim bsr-border
ip multicast boundary 1
int pos1/0
ip pim sparse-mode
ip pim bsr-border
ip multicast boundary 1
ip msdp sa-filter out 1.1.1.2 111
ip msdp sa-filter in 1.1.1.2 111
ip msdp sa-filter out 1.1.2.2 111
ip msdp sa-filter in 1.1.2.2 111
```
Dual-Homed, Customer RP, MBGP Congruent Multicast—Unicast

```
ip msdp peer 1.1.1.1 connect-source pos0/0
ip msdp peer 1.1.2.2 connect-source pos0/0
```

MSDP RPF Check

```
ip msdp peer 1.1.1.2 connect-source pos0/0
ip msdp peer 1.1.2.1 connect-source pos0/0
```
Dual-Homed, Customer RP, MBGP  
Congruent Multicast—Unicast

Multicast RPF Check

Customer AS100  
RP  
192.168.100.0/24

Transit AS109
Unicast & Multicast Transit

pos0/0 1.1.1.1
pos0/0 1.1.1.2
pos1/0 1.1.2.1

Transit AS110
Unicast & Multicast Transit

pos0/0 1.1.2.1
pos0/0 1.1.2.2

Dual-Homed, Customer RP, MBGP  
Congruent Multicast—Unicast

Multicast RPF Check

Customer AS100  
RP  
192.168.100.0/24

Transit AS109
Unicast & Multicast Transit

pos0/0 1.1.1.1
pos0/0 1.1.1.2
pos1/0 1.1.2.1

Transit AS110
Unicast & Multicast Transit

pos0/0 1.1.2.1
pos0/0 1.1.2.2

router bgp 100
network 192.168.100.0 nri unicast multicast
neighbor 1.1.1.2 remote-as 109 nri unicast multicast
neighbor 1.1.1.2 update-source pos0/0
neighbor 1.1.2.2 remote-as 110 nri unicast multicast
neighbor 1.1.2.2 update-source pos1/0
GLOP—Static Allocation of 233/8

- Temporary allocation of 233/8
  - RFC 2770
- Statically assigned by mapping AS number into middle octets
  - http://gigapop.uoregon.edu/glop/index.html
- Provides each AS with /24 addresses to use while waiting another solution
Company A owns AS 5662. How do we use GLOP to come up with a multicast address range?

5662 written in binary is: 0001011000011110

Map the high order octet to the second octet of the address, and the low order octet to the third octet:

0 0 0 1 0 1 1 0 | 0 0 0 1 1 1 0

0 0 0 1 0 1 1 0 = 22     0 0 0 1 1 1 0 = 30

AS 5662 gets 233.22.30.0/24 for multicast use over the internet.

---

The hexadecimal value of 5662 is 161E. 16 hex equals 22 decimal and 1E hex equals 30 decimal. We get 233.22.30.0/24.

The lazy (smart?) way to calculate your GLOP address space is by entering it here and it will calculate if for you:

http://www.ogig.net/glop/
**Agenda**

- ISP Solutions Overview
- MBGP (routing)
- MSDP (source discovery)
- MBGP/MSDP Examples
  - SSM (Source Specific Multicast)
- IPv6
- Security

**PIM Source Specific Mode**

- Receiver learns of source, group/port
- Receiver sends IGMPv3 (S,G) Join
- First-hop sends PIM (S,G) Join directly toward Source

Diagram:
- Source
- Receiver
- (S, G) Join
- IGMPv3 (S, G) Join
- Out-of-band source directory, example: web server
PIM Source Specific Mode

Result: Shortest path tree rooted at the source, with no shared tree.

Out-of-band source directory, example: web server

SSM Mapping

- Customers want to deploy SSM
- Hosts in network don’t support IGMPv3
- Host OS is outside of network operators control
- Network operators don’t control content
  - No knowledge about S,G mapping
SSM Mapping

• Bring Source to Group mapping from host to router
• Use an external or internal database for Source to Group mapping
  – Allows content providers to provide the mapping
  – Independent from network operators
  – Database is chosen to be static or DNS
• Allows only for one source per Group

Example

Set Top Box (STB)

IGMPv2 join

PIM (S,G) join

DNS response: Group G -> Source S

Reverse DNS lookup for group G
Configuration

**Enabling SSM mapping on the router**

```
   ip igmp ssm-map enable
```

**For static mapping:**
```
   ip igmp ssm-map static <acl-1> <source-1 IP address>
   ip igmp ssm-map static <acl-2> <source-2 IP address>
```

**For DNS mapping (existing commands):**
```
   ip domain-server <ip address>
   ip domain-name <domain.com>
```

**To disable DNS mapping**
```
   no ip igmp ssm-map query dns
```

**DNS Record Format:**
```
   3.2.1.232       IN A   172.23.20.70
```

Agenda

- ISP Solutions Overview
- MBGP (routing)
- MSDP (source discovery)
- MBGP/MSDP Examples
- SSM (Source Specific Multicast)
- IPv6
- Security
IPv6 Multicast Addressing

- Multicast Addresses (RFC 2373)
  - ff::/8 is the ipv6 equivalent of 224/4
  - ff02::1 is the ipv6 equivalent of the link local address 224.0.0.1
  - SSM address range is ff3X::/32, where X represents the scope bits.

IPv6 Multicast – O.S. & Application Support

- Stacks
  - KAME host stack
  - Microsoft Windows XP
  - Mac OS 10.2
  - Linux
  - HP OpenVMS and True64

- Applications
  - Microsoft Media Player & Server 9
  - Many emerging commercial applications
  - DVTS, Videolan, etc
  - Standard MBONE Tools (vic, rat, ...) support IPv6
IPv4 versus IPv6 Multicast

<table>
<thead>
<tr>
<th>IP Service</th>
<th>IPv4 Solution</th>
<th>IPv6 Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Range</td>
<td>32-bit, class D</td>
<td>128-bit</td>
</tr>
<tr>
<td>Routing</td>
<td>Protocol Independent</td>
<td>Protocol Independent</td>
</tr>
<tr>
<td></td>
<td>All IGPs, and BGP4+</td>
<td>All IGPs, and BGP4+</td>
</tr>
<tr>
<td></td>
<td>PIM-DM, PIM-SM, PIM-SSM, PIM-bidir</td>
<td>PIM-SM, PIM-SSM, PIM-bidir</td>
</tr>
<tr>
<td>Forwarding</td>
<td>IGMPv1, v2, v3</td>
<td>MLDv1, v2</td>
</tr>
<tr>
<td>Group Management</td>
<td>Boundary/Border</td>
<td>Scope Identifier</td>
</tr>
<tr>
<td>Domain Control</td>
<td>MSDP across Independent PIM</td>
<td>Single RP within Globally Shared</td>
</tr>
<tr>
<td></td>
<td>Domains</td>
<td>Domains</td>
</tr>
</tbody>
</table>

Interdomain Solutions

IP Routing for Multicast

- RPF based on reachability to v6 source same as with v4 multicast
- RPF still protocol independent:
  - Static routes, mroutes
  - Unicast RIB: BGP, ISIS, OSPF, EIGRP, RIP, etc
  - Multi-protocol BGP (mBGP)
    - Support for v6 mcast sub-address family
    - Provide translate function for non-supporting peers
Domain Control

• Definitions:
  – A PIM domain is topology served by common RP for all sources and receivers of same group.
  – A routing domain is consistent with AS.

• It’s necessary to constrain the PIM messages, rp-mappings, and data for groups within the PIM domain:
  – In IPv4 we used multicast boundary/ BSR border
  – In IPv6 we use scopes and zones

Interdomain v6 Multicast Options

SSM, no RPs

ASM across multiple separate PIM domains, each with RP, MSDP peering

ASM across single shared PIM domain, one RP
Multicast Phase I

12.3(1)T, 12.2S RLS3, 12.0(26)S

- **PIM**
  - Source Specific Multicast (PIM-SSM)
  - Sparse-mode (PIM-SM)
    - Full support for DR functionality (registers, etc)
    - Static RP assignment with multiple RP mapping
- **Scoping support (replaces v4 boundary function)**
- **MLDv1 and v2**
  - Support INCLUDE and EXCLUDE mode reports in MLDv2
  - Full MLDv1/v2 compatibility
  - Explicit tracking in v2 mode.
- **v6-in-v4 tunneling**

Multicast Phase II, active

- **PIM**
  - Support for embedded RP mapping
  - Support for “upstream-address-detection” PIM Hello Option
- **Multicast specific Routing – mBGP**
  - ‘translate update’ for seamless migration into existing BGP peerings
    - (also in 12.0(26)S for initial GSR release)
  - static mroutes
    - (also in 12.0(26)S for initial GSR release)
Multicast Phase II, active

- BSR Forwarding support for BSR messages
  - (also in 12.0(26)S for initial GSR release)
- Security and access-control
  - MLD access-groups for receiver control
  - Register filters for source control
- Distributed Fast Switching
  - (also in 12.0(26)S for initial GSR release)
- v6-in-v6 tunneling

IOS CLI: Configure like v4, but easier

Group mode determines how to forward, compared to interface mode in v4.

By default all interfaces are PIM enabled unless explicitly disabled.

Config for PIM-SSM:
```conf
ipv6 multicast-routing
```

Config for PIM-SM:
```conf
ipv6 multicast-routing
ipv6 pim rp-address <v6_address>
```

Config for PIM-bidir:
```conf
ipv6 multicast-routing
ipv6 pim rp-address <v6_address> bidir
```

Disable PIM on an interface:
```conf
interface ethernet 0
no ipv6 pim
```
Conclusion

- Cisco IOS IPv6 Multicast in initial deployment now
- Multicast Applications can be developed and tested over an infrastructure running Cisco IOS IPv6 Multicast
- IPv6 Multicast is an IPv6 service fully integrated with other Cisco IPv6 solutions

v6 Mcast Questions?:
mcast-v6-support@cisco.com

Agenda

- ISP Solutions Overview
- MBGP (routing)
- MSDP (source discovery)
- MBGP/MSDP Examples
- SSM (Source Specific Multicast)
- IPv6
- Security
Controlling Receivers

IGMP Access-Group Approach

```
interface VLAN100
  ip igmp access-group IPMC-ACL
  ip access-list standard IPMC-ACL
    permit 239.192.244.1
    deny any
```

No filter (default)

Permit VT Stream
Deny Executive Meeting Stream

This is micro-management of IP Multicast traffic!!!

Controlling Source Registration

- Global command
  ```
  ip pim accept-register [list <acl>] | [route-map <map>]
  ```
  - Used on RP to filter incoming Register messages
  - Filter on Source address alone (Simple ACL)
  - Filter on (S, G) pair (Extended ACL)
  - May use route-map to specify what to filter
    - Filter by AS-PATH if (m)BGP is in use.
  - Helps prevents unwanted sources from sending
    - First hop router blocks traffic from reaching net
    - Note: Traffic can still flow under certain situations
Controlling Source Registration

- RP configured to only accept Registers from specific source.

```
ip pim accept-register list 10
access-list 10 permit 192.16.1.1
```

Controlling Source Registration

- Unwanted source traffic hits first-hop router.
- First-hop router creates (S,G) state and sends Register.
- RP rejects Register, sends back a Register-Stop.
Disabling Entire Group Ranges

• **Accept-Register Method**
  - `ip pim accept-register group-list 10`
  - `access-list 10 deny 224.2.0.0 0.0.255.255`
  - `access-list 10 permit any`

• **Pros**
  - Only configured on RP(s)

• **Cons**
  - Shared Trees and (*,G) state still created.
    - Results in unwanted (*,G) PIM Control Traffic.
  - Source traffic can still flow.
    - (See previous section on Accept-Register)

---

Disabling Entire Group Ranges

• **Local Loopback RP Method**

  – **Concept:**
    - Only Auto-RP-learned groups are authorized.
    - All other groups are considered *unauthorized*.

  – **Implementation:**
    - Define local Loopback as RP for unauthorized groups on each router.
      - `ip pim rp-address <local_loopback> 10`
      - `access-list 10 permit 224.2.0.0 0.0.255.255`
      - Note: The permit clause defines the unauthorized group.
Disabling Entire Group Ranges

• Local Loopback RP Method
  – Operation:
    • Each router serves as RP for unauthorized groups.
      – Collapses PIM-SM domain of unauthorized groups down to the local router.
    • Unauthorized group traffic cannot flow beyond local router.

• Local Loopback RP Method
  – Pros:
    • No PIM control traffic sent.
      – Local router is RP so no Registers/Joins are sent.
    • No additional workload on local router.
      – First-hop routers always have to create state anyway.
    • Can also serve as RP-of-last-resort
      – Solving DM Fallback problem at the same time.
  – Cons:
    • Must be configured on every router.
    • Local sources can still send to local receivers.
Disabling Entire Group Ranges

• Recommendation
  – Use Local Loopback RP Method
    • Effectively disables unauthorized group traffic.
    • Can also serve as RP-of-last-resort
      ip pim rp-address <local_loopback> 10
      access-list 10 deny 224.0.1.39
      access-list 10 deny 224.0.1.40
      access-list 10 permit any

Disabling Entire Group Ranges – Future

• New ‘no ip pim dm-fallback’ command
  – Undefined (via Auto-RP or BSR) groups default to an RP address of 0.0.0.0.
  – Effectively disables any group unlearned groups.

• Available soon.
Preventing RP-Spoofing DoS Attacks

• Global command
  
  ip pim rp-announce-filter rp-list <acl> [group-list <acl>]

  rp-list <acl>
  – Specifies from which routers C-RP Announcements are accepted.

  group-list <acl>
  – Specifies which groups in the C-RP Announcement are accepted.
  – If not specified, defaults to deny all groups

• Use on Mapping Agents to filter out bogus C-RP’s
  – Some protection from RP-Spoofing denial-of-service attacks
  – Multiple commands may be configured as needed

Use ip pim rp-announce-filter on RP

• Using this configuration allows the router to accept RP announcements from only the RP in ‘access-list 11’ for group ranges described in ‘access-list 12’

  ip pim rp-announce-filter rp-list 11 group-list 12
  access-list 11 permit 10.6.2.1 !IP address of Permitted RP
  access-list 12 permit 239.192.240.0 0.0.3.255 !Permit MoH
  access-list 12 permit 239.192.244.0 0.0.3.255 !Permit Low Stream
  access-list 12 permit 239.192.248.0 0.0.3.255 !Permit Medium Stream
  access-list 12 permit 239.255.0.0 0.0.255.255 !Permit High Stream
  access-list 12 deny 239.0.0.0 0.255.255.255 !Deny remaining Admin. Scoped range
  access-list 12 permit 224.0.0.0 15.255.255.255 !Permit Link Local/Reserved Add.