

UKERNA IP Multicast Hands-on Workshop

Lab 3: **IP Multicast, Inter-domain**

Networkshop 2006

Laboratory 3 Overview

- Inter-domain multicast
 - Goal to receive multicast from external network(s)
- Configure multicast on uplink of access router
- Set up MBGP peering to core router (7206)
- Create an MSDP peering to the core router
- Run ssm ping/asm ping to another internal Team network
 - Coordinate with another Team!
- Try external multicast sources
 - BBC Multicast trial feed (ASM)
 - ssm ping.beacon.ja.net (SSM or ASM)

In this exercise, we move from 'campus' multicast to study how you can set up inter-domain (for example inter-campus) multicast.

By the end of the session you should have established MBGP and MSDP peerings to the core router in the lab network (the Cisco 7206) and as a result be able to exchange IPv4 multicast (SSM and ASM) with other Team networks and with networks external to the lab network.

At that point we will have completed our IPv4 exercises, and for the final session move on to look at IPv6 multicast.

Current setup (after Lab session 2)

- IPv4 unicast throughout in 'provider'
 - Static routing
- IPv4 multicast on edge router
- IPv4 multicast on access router
- PIM-SM RP is configured on your access router
- Next step: configuring your access router uplink
 - Enabling PIM

At this stage it is worth remembering the lab setup as it was from the end of exercise 2.

You have multicast deployed on your 'campus' network of edge and access router.

Note that IPv4 routing in the lab is static and configured for you. We will thus first introduce MBGP to allow BGP to handle multicast routing, then add MSDP to enable discovery of sources in remote PIM domains, and to allow remote domains to learn of our sources.

You will next need to configure multicast on your uplink to the core Cisco 7206 router.

Multicast on access router uplink

- You first need to configure multicast on the uplink to the core router
 - Enable PIM
- Note Teams A-C have a Cisco 2801 access router, while Teams D-F have a Cisco 3825, so the uplink interfaces will be slightly different
 - fa0/0 (on 2801) as opposed to gi0/0 (on 3825)

Enable multicast on the access router's uplink interface:

For the 2810 (Teams A-C):

```
int fa0/0
ip pim sparse-mode
```

For the 3825 (Teams D-F):

```
int gi0/0
ip pim sparse-mode
```

Note that at this stage ssm ping should work for remote servers, e.g. `ssmping.uninett.no`, because SSM only requires multicast to be enabled, unlike ASM where MBGP and MSDP are required between domains.

The next step is to configure an MBGP peering to the core router, and to check the MBGP status.

Add an MBGP peering

- The goal is to use MBGP to exchange multicast routing information
 - Including routes for groups used by other Teams, as well as external groups
- Configure BGP peering to core router (7206)
- Configure IPv4 multicast for BGP

The first step is to configure a BGP peering to the core router

You will need to use two Autonomous System Numbers (ASNs) here, one for your Team's access router (see the topology map at the bottom), and one for the 7206 router (AS 64615). Both AS's are 'private' ASNs, i.e. they have no meaning outside the scope of the lab network.

In configure mode:

```
router bgp <your group specific ASN>
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor <ip address of connected 7206 interface> remote-as 64615
neighbor <ip address of connected 7206 interface> description nws7206
```

Configure IPv4 multicast for MBGP

- Set up MBGP to exchange IPv4 multicast routes
- Remember IPv4 unicast is statically routed.



At the configure level:

```
address-family ipv4 multicast
neighbor <ip address of connected 7206 interface> activate
no auto-summary
no synchronisation
network <group network address> mask 255.255.255.224
```

You will need to know your group network address. Each Team has a /27 prefix, and 32 possible addresses, thus the netmask is 255.255.255.224. The network address is the first address in the prefix. Your access router uplink uses the first available address in the range, e.g. Team C uses 193.61.85.65, and thus their network address is 193.61.85.64.

Checking MBGP status

- Now we check the BGP status
- You can check for example
 - Multicast routes
 - Multicast neighbours



There are some other commands you can try.

To look at MBGP routes:

```
show ip bgp ipv4 multicast summary
```

```
show ip bgp ipv4 multicast neighbors <neighbouraddr> advertised-routes
```

You should see your /27 advertised to the core router.

MSDP Peering

- The goal of deploying an MSDP peering to the core router is to be able to discover multicast sources from other PIM domains (and vice versa)
- Configure MSDP peering
- Configure an example access list to prevent 239.0.0.0/8 being exchanged over the peering
 - This prefix requires administrative scoping

Now we have MBGP up, we can move on to set up the MSDP peering.

To set up the MSDP peer, enter configure mode:

```
ip msdp peer <ip address of connected 7206 interface>  
ip msdp description <ip address of connected 7206 interface> nws7206  
ip msdp originator-id Loopback0
```

The <ip address> will depend on which team you are in; check the topology map. For example, Team D connects to ge0/1 on the 7206 which has IP address 193.61.85.241 (in the top right list on the topology map).

We'll now go on to see how to set up a filter on this peering to block 239.0.0.0/8 being propagated over it.

MSDP filters

- Here we show one example of an MSDP filter. There is fuller discussion of filters in the 'IPv4 Multicast on JANET' guide.
 - For example you would not expect to see SSM prefixes
- Create the access list
- Apply the list to the MSDP peering

The first step is to define the access list:

Enter configure mode:

```
ip access-list extended MSDP-FILTER
    deny ip any 239.0.0.0 0.255.255.255
    permit ip any any
```

The apply the filter:

```
ip msdp sa-filter in <ip address of connected 7206 interface> list MSDP-FILTER
ip msdp sa-filter out <ip address of connected 7206 interface> list MSDP-FILTER
```

At this point the MSDP peering should be up.

You may wish to look at other filters as per the 'IPv4 Multicast on JANET' guide (section A2.4.2)

Checking the MSDP peering

- We can check the peering status, e.g.
 - Overall
 - By peer
 - Counts



Try:

```
show ip msdp summary
show ip msdp peer <ip_address_of_peer>
show ip msdp count
```

This should verify that the peering is up and Source Advertisements (SAs) have been received.

Running asmping

- Try asmping (and ssm ping) in your local 'campus' network
- Try it between 'campus' (Team) networks
- Try it remotely – example servers:
 - ssm ping.uninett.no
 - ssm ping.beacon.ja.net

At this time you should be able to test asmping to hosts in your 'campus', in other Team networks, or to remote ssm ping servers (that will respond to ssm ping or asmping clients)

To run asmping, the format is:

```
asmping-0.8.1-exe <multicast_group> <server_ip>
```

We suggest you use multicast groups as follows:

```
224.<group_number>.x.234
```

Where Team A uses group_number 1, Team B uses group_number 2, etc. and 'x' is any number you like (this may be useful if running multiple tests, or when you are waiting for state to time out).

The last byte must be 234 for the ssm ping tools.

Checking router state on asmping

- As you run asmping to remote target servers, you can check the router state
 - Multicast routes
 - MSDP peers



Try to do

```
show ip mroute
```

on your RP router while running asmping. You should then see an (S,G)-entry with an A flag (A means that it's a candidate for being announced in MSDP).

Also, you can then do

```
show ip msdp peer <address> advertised-SAs
```

to see what you are advertising. If MSDP is working you should see an entry there.

You can also check by using asmping between groups. Speak to your neighbours



BBC Multicast feed

- The BBC is transmitting various channels in a multicast pilot. JANET peers with the BBC source. See:
 - <http://www.bbc.co.uk/multicast>
- Use Windows Media Player and/or VideoLAN client to receive BBC/ITV multicast test streams
- Check router states

Open a web browser (MS Internet Explorer) and visit

<http://www.bbc.co.uk/multicast>

Follow the 'Take part...' link.

Select a stream to view in Windows Media Player.

If you have the VideoLAN client (vlc) installed on your workstation, you can use that to view the H.264 multicast streams (which are sent at a higher quality).

dbeacon

- The dbeacon tool is a good way to monitor multicast connectivity longer term with a matrix view
 - Unfortunately the official release is Linux-based only
- The lab workstations are Windows XP only
 - At the time of writing the exercises, we hope to have a Windows dbeacon client available for the workshop
 - If not, we will use instructor laptops to see dbeacon running between at least some Team networks

The dbeacon package is a very useful IP (v4 and v6) multicast monitoring tool.

See <http://artemis.av.it.pt/~hsantos/dbeacon>

Each client runs the beacon, such that each client gets a view of which other clients it can see and be seen by.

Usage information is given in the wiki at the above URL.

Lab Overview

- What did we do
- What did we learn
- What would be different in the real world
- What's coming up next

