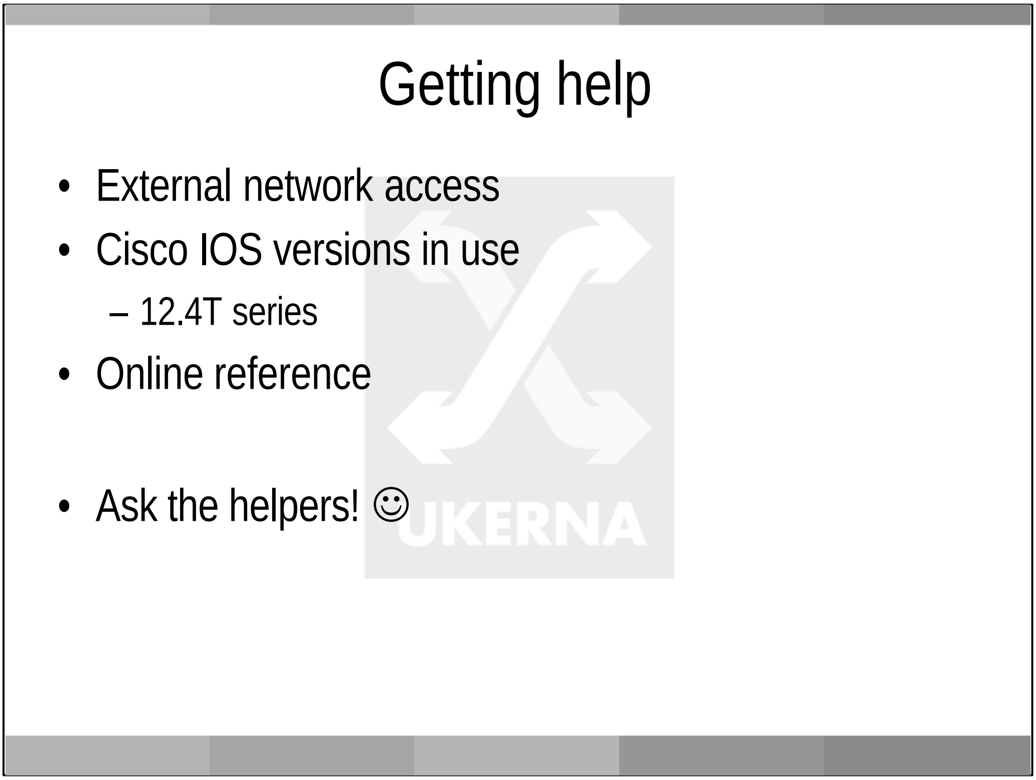
UKERNA
IP Multicast Mini Workshop
Inter-domain Multicast

Hands-on Lab Exercises

Networkshop 2006



Getting help

- External network access
- Cisco IOS versions in use
  - 12.4T series
- Online reference

- Ask the helpers! ☺

Your workstations should have external IPv4 access; thus you can access remote web resources for help. Alternatively there are lab helpers to hand who should be able to assist you.

The lab routers are Ciscos running IOS12.4T.

Places to look when seeking on-line documentation include:

* Cisco Software Release 12.4T Command References
http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/

* Cisco Software Release 12.4T Debug Commands Reference
http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cr/hdb_r/

Note that you're not expected to have to finish everything in this lab - it's designed for you to experiment at your own pace.

Cisco IOS

- Knowledge of Cisco IOS would be useful. If new…
- Most configuration is undertaken with level-15 privileges (reached by “enable” on the console)
- Commands tab out, type “?” to show possibilities, a good starting point is “show ?”, e.g. “show ip interfaces”
- Use “config terminal” to enter configuration mode.

The workgroup routers start off in a state in which you can access their CLI using telnet. The exec password you need is “nws$password”. There’s only so much you can look at in IOS without having level-15 privileges, however it is handy to familiarise oneself with the environment by playing with a few commands - it’s hard to break Ciscos without level-15 access!

“show ?” lists a set of possible command completions for the current context are displayed. Depending on your current privilege level, different options will avail themselves of you. Try “show ip interfaces” and press return, and have a look over the output.

The command that promotes an interactive session to level-15 privileged status is “enable”. The enable password for the routers is “nws$enable”.

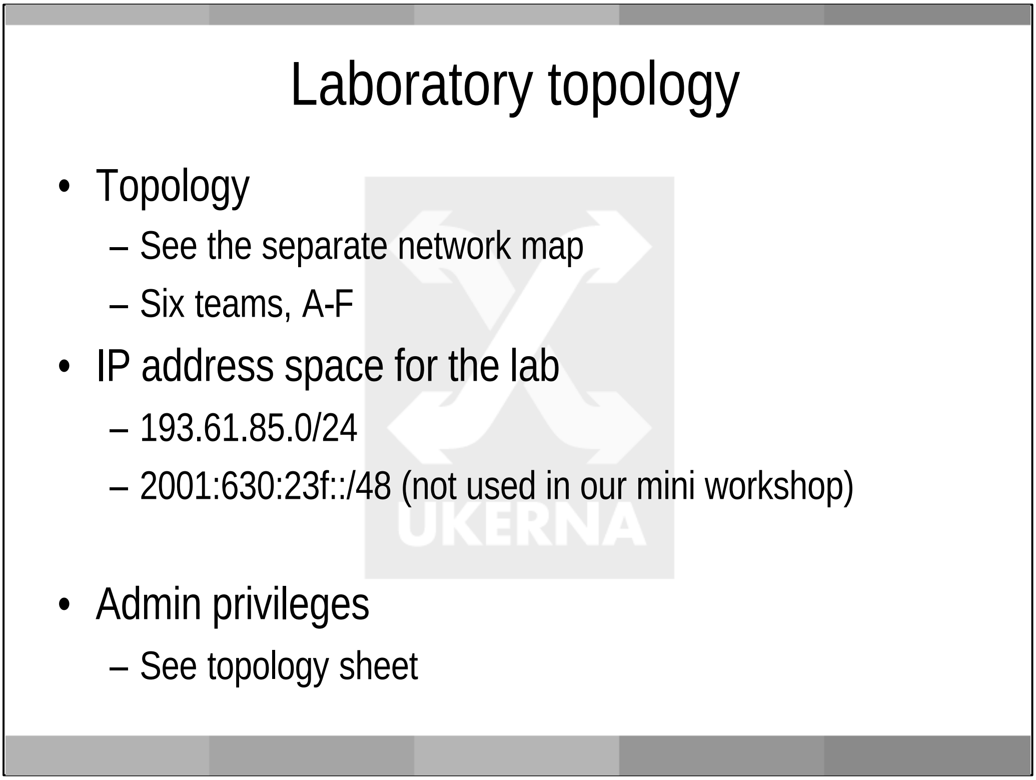
Once enabled, you can examine the running configuration, access much greater usage and debug information and, critically for this lab, configure the router.

To enter configuration mode, type “config terminal” (or just “conf t”) and press return. Note how the prompt changes to reflect the new context - currently the router’s global configuration context. Additional sub-contexts include interface definition mode where subsequent directives entered affect a particular interface; line definition mode to configure the administration and modem interfaces; etc. To step back up a level to the parent context (and from the global context back out of configuration mode and back into exec/interactive), type “exit” on a line of its own.

Once you’ve made configuration changes, the live running configuration can be dumped to console by typing “show running-config” in interactive mode. Likewise the configuration directives that will be applied post reboot is the ‘startup-config’. To make the current live config persist (I.e. become the startup-config), enter “write memory” (or just “write”) in interactive mode.

The laboratory helpers should have the base configurations on flash memory; so these can be reinstalled if you get in a knot.

A crash-course on IOS is beyond the scope of this workshop, however there are plenty of books and web articles that cover the elementary aspects of IOS configuration and use. As ever - just shout if you get stuck.



Laboratory topology

- Topology
  - See the separate network map
  - Six teams, A-F
- IP address space for the lab
  - 193.61.85.0/24
  - 2001:630:23f::/48 (not used in our mini workshop)
- Admin privileges
  - See topology sheet

The laboratory is using a /24 size IPv4 prefix and a /48 size IPv6 prefix allocated by the JANET NOSC, resulting in every workstation and router having public and globally-routable IPv4 addresses. Since this allocation is not part of Hatfield's address space, the lab network is connected to the JANET multicast service via an IPv4 unicast tunnel from the core laboratory router (a Cisco 7206).

The laboratory is split into six Teams (A through F), with each group sharing a bench comprising two workstations, split into two subnets.

Each bench has a network topology map showing the initial state of the laboratory network.

You will have full administrator privileges on the workstations and level 15 access on your local workgroup router.

The windows administrator account is called “admin”. The password is “qazwsx” (not particularly secure, admittedly, but this is a lab).

Your Team cluster

- Each group has the following:
  - – Cisco 2801 or 3825 access router
    - Two Ethernet ports (one uplink one downlink)
  - – Cisco 2801 edge router
    - One Ethernet uplink
    - One single Ethernet subnet, one QuadFE subnet
  - – Client nodes
    - Two Windows XP Service Pack 2 PCs, split into two subnets
  - – Full IPv4 unicast connectivity

Please take a moment to study the laboratory network diagram.

You will see the six teams of people, Team A through Team F, each having a similar setup.

Each team has an edge router to which two host subnets are attached. In each case this is a Cisco 2801 Your two workstations are wired such that each workstation lies in one of the two subnets. The edge router represents a departmental router in a campus environment. Each subnet has a /29 (8 host addresses) so you have the capability to plug a laptop into one of the extra ports on the edge router with the quad Fast Ethernet card if you wish to do so (if you do, you can use the next IP address up from your Client2 node. There is no DHCP on the network.

Each team also has an access router connecting to their edge router downstream and a core Cisco 7206 upstream. Teams A-C have Cisco 2801 for this purpose while Teams D-F have a Cisco 3825. This router will be used as if it were a campus access router, and will support MBGP and MSDP functions during this mini-workshop exercise set.

The 7206 is the core router, connecting downstream to each Team's access router and upstream to the JANET multicast service (via an IPv4 unicast tunnel). As the 'JANET-level' router, you will not have configuration access to this router.

The 7206 is running IOS 12.4(2)T4 with Advanced IP Services.

The 2801's and the 3825's are running IOS 12.4(4)T1 with Advanced IP Services.

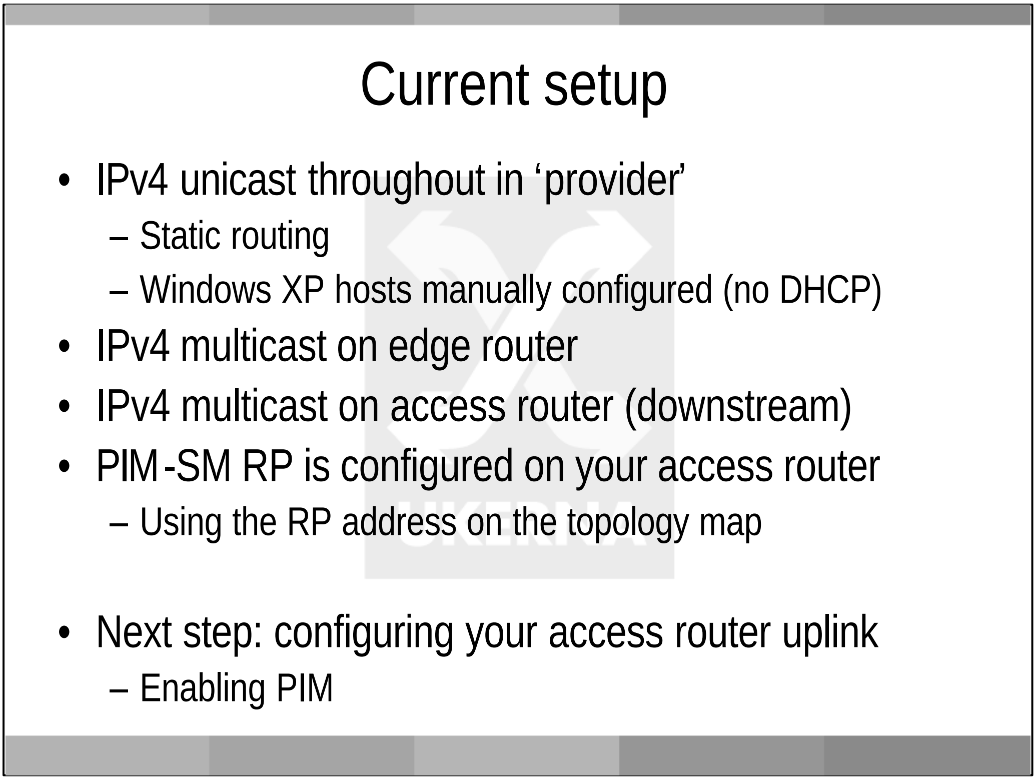
Note that there is only one edge and one access router per group, so you will need to work together and rotate responsibility for configuring the router, etc.

Laboratory 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 ssmping/asmping to another internal Team network
  - Coordinate with another Team!
- Try external multicast sources
  - BBC Multicast trial feed (ASM)
  - ssmping.beacon.ja.net (SSM or ASM)

In this exercise, we study how you can set up inter-domain (for example inter-campus) multicast, given a working intra-domain (campus) multicast network as a platform.

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.



Current setup

- IPv4 unicast throughout in ‘provider’
  - Static routing
  - Windows XP hosts manually configured (no DHCP)
- IPv4 multicast on edge router
- IPv4 multicast on access router (downstream)
- PIM-SM RP is configured on your access router
  - Using the RP address on the topology map

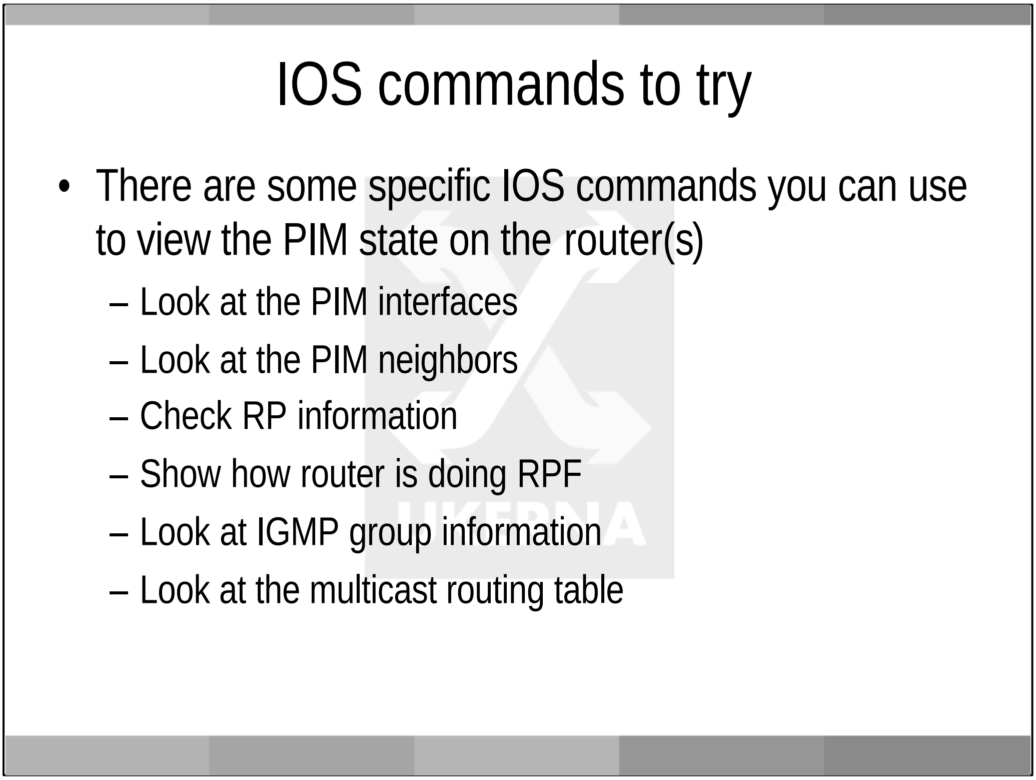
- Next step: configuring your access router uplink
  - Enabling PIM

You are entering this lab session with a working multicast PIM domain in your Team network (edge and access router). The goal of this exercise is to interconnect your PIM domain to the other team PIM domains, using MBGP and MDSP and to then run some external multicast tests.

Note that IPv4 unicast 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.

Feel free to first inspect your router states. Some example commands are listed on the next page.

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



IOS commands to try

- There are some specific IOS commands you can use to view the PIM state on the router(s)
  - Look at the PIM interfaces
  - Look at the PIM neighbors
  - Check RP information
  - Show how router is doing RPF
  - Look at IGMP group information
  - Look at the multicast routing table

Here are some commands you can try before, after or while running asmping.

Look at the PIM interfaces:

```
show ip pim interface
```

Show your PIM neighbours:

```
show ip pim neighbor
```

Look at the RP information:

```
show ip pim rp
```

For RPF information:

```
show ip rpf
```

To look at IGMP groups on the router:

```
show ip igmp groups
```

And in detail:

```
show ip igmp groups detail
```

To verify multicast is enabled

```
show ip multicast
```

To see multicast route information use

```
show ip mroute
```

To show counts on the routes

```
show ip mroute count
```

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
```

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
```

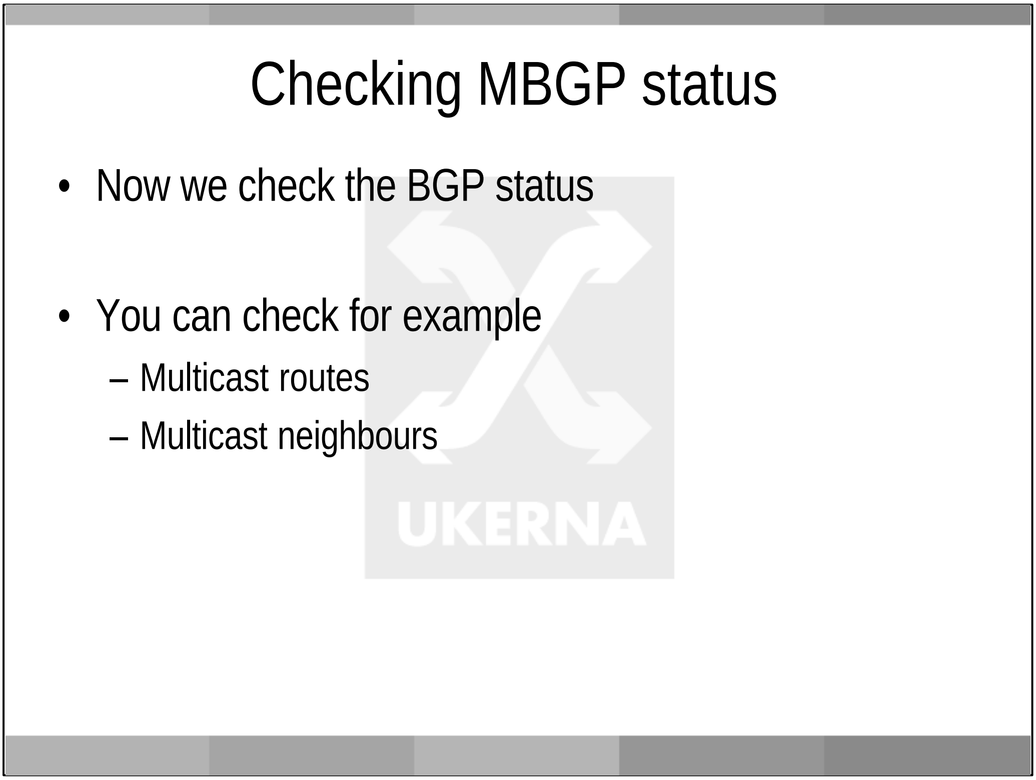
Configure IPv4 multicast for MBGP

- 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

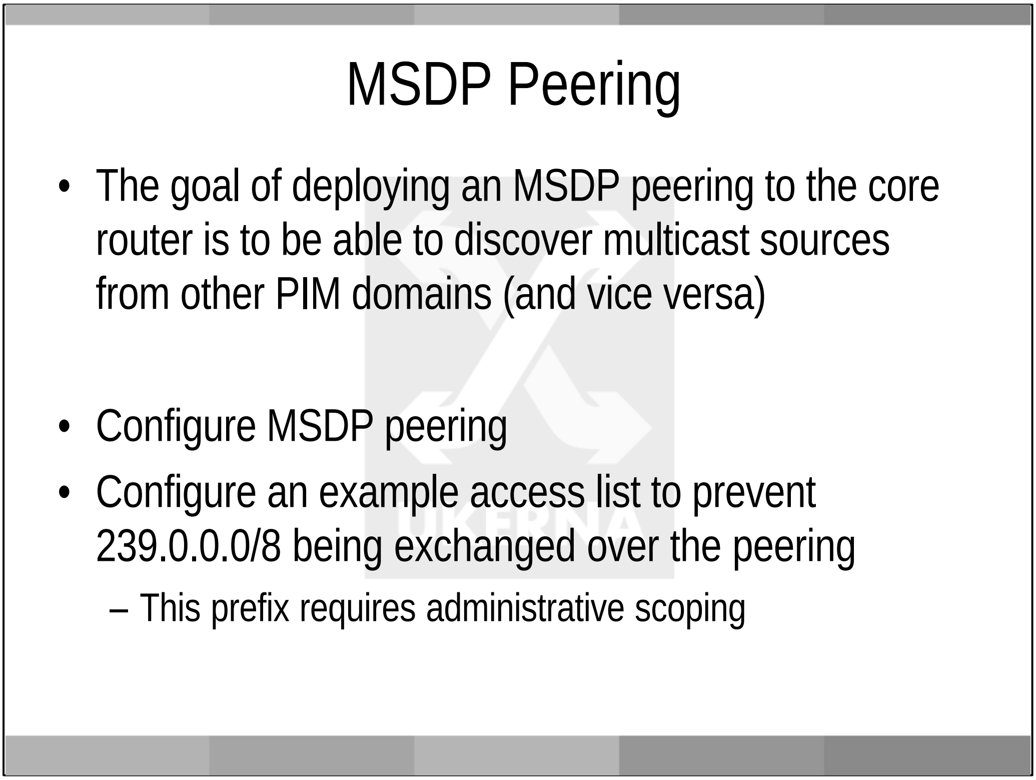
- Now we check the BGP status
- You can check for example
  - Multicast routes
  - Multicast neighbours

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

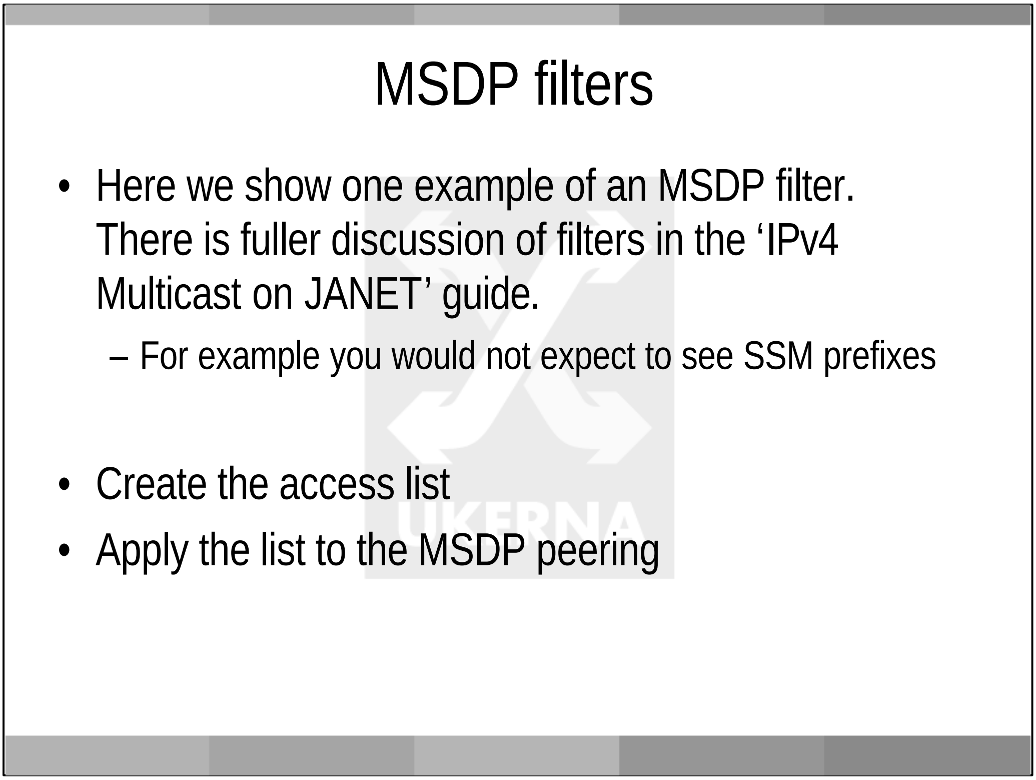
Now we have MBGP up, we can move on to set up the MSDP peering.

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)

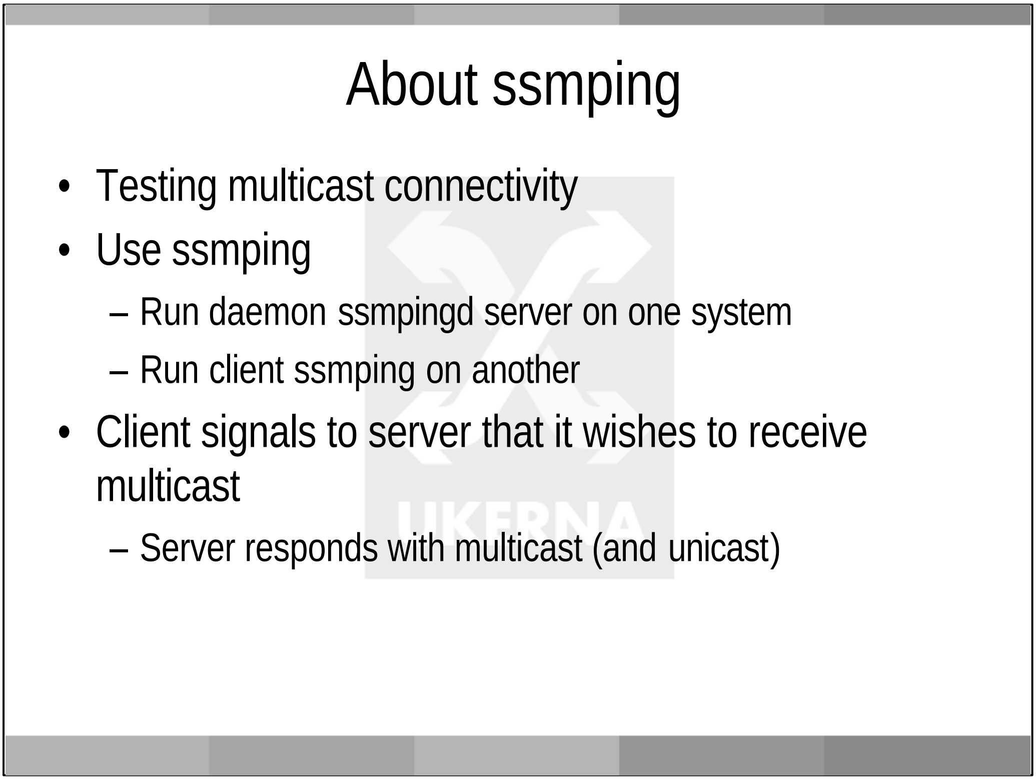
Checking the MSDP peering

- 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.



About ssmping

- Testing multicast connectivity
- Use ssmping
  - Run daemon ssmpingd server on one system
  - Run client ssmping on another
- Client signals to server that it wishes to receive multicast
  - Server responds with multicast (and unicast)

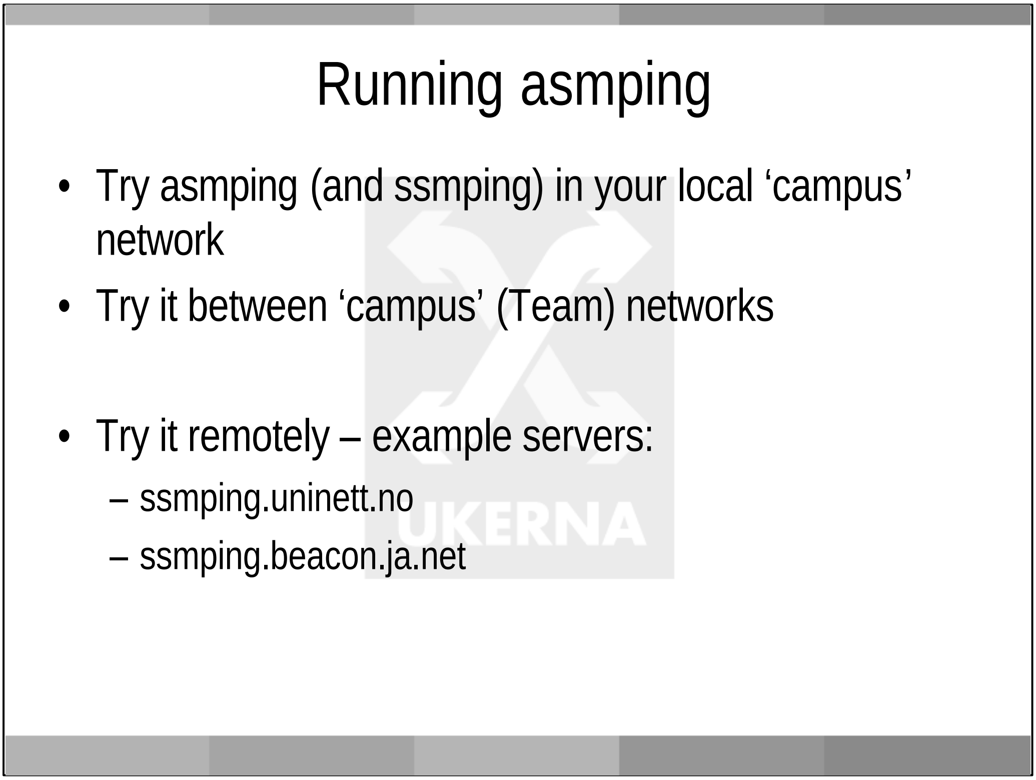
The ssmping tool (and its integral *asmping* counterpart) is very useful for testing multicast connectivity. By running these tools, one can send a message to a host on the Internet (which is running the *ssmping*/*asmping* server) and one will see whether one can receive (unicast and) multicast from the server back to the ssmping client host.

The tool thus allows us to generate a multicast flow from one host (running the daemon) to another (the client running ssmping).

The ssmping client signals to the server on UDP port 4321.

The client will join (S,G) where S is its IP address and G is set by ssmping to be 232.43.211.234.

The *ssmping* package is pre-installed for you on the lab workstations, but is also available from http://www.venaas.no/multicast/ssmping/ for Windows and Unix platforms.



Running asmping

- Try asmping (and ssmping) in your local ‘campus’ network
- Try it between ‘campus’ (Team) networks
- Try it remotely – example servers:
  - ssmping.uninett.no
  - ssmping.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 ssmping servers (that will respond to ssmping 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 ssmping 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