# UKERNA
# IP Multicast Hands-on Workshop

## Lab 1: **IP Multicast, LAN view**

Networkshop 2006

# Laboratory 1 Overview

- Study the lab network topology
- Get familiar with Windows XP workstation platform and Cisco 2801 router platform
- Run an IP multicast application between the two clients on your edge router
  - Gain familiarity with the ssmping tool
- Run ethereal to observe packets on the links
- Observe IGMPv3 packets
- Observe edge router multicast states

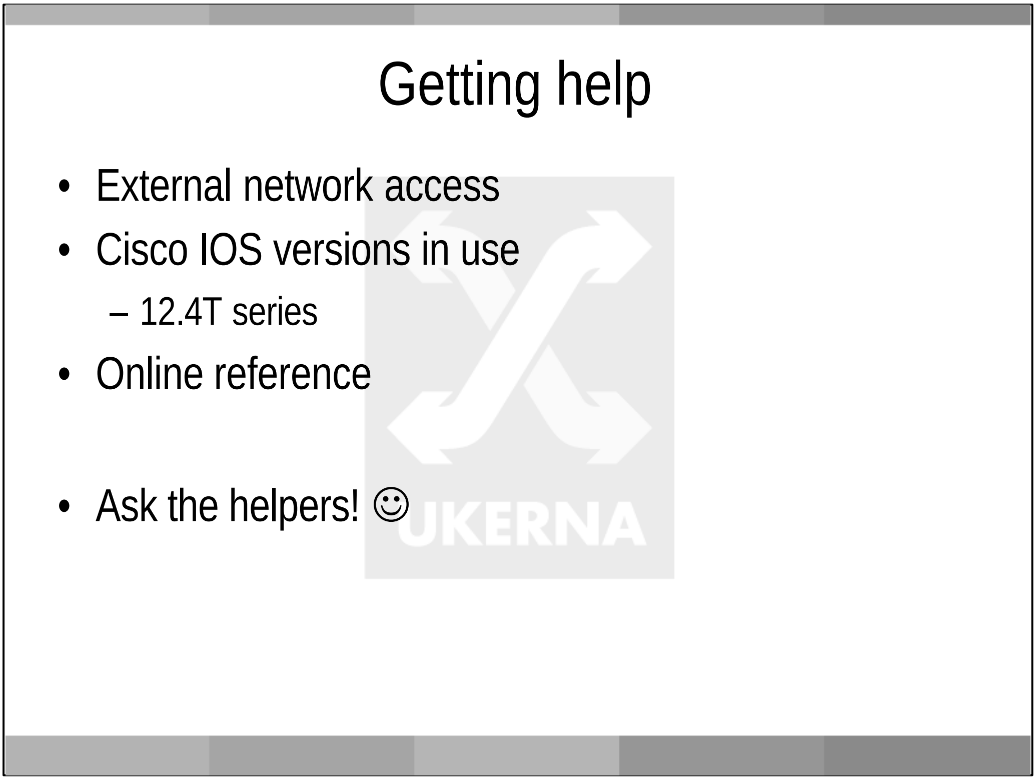
The four sets of exercises in this workshop offer an overview of IP multicast in operation from both a network operator's perspective and that of a site administrator.

Our aim in setting the exercises is to take you through the multicast perspective from the bottom up, i.e. to begin with how IP multicast works on a subnet or LAN, including the on-link router. This represents working with IP multicast at a departmental perspective on campus, understanding LAN issues, how IGMP works, and router states as multicast groups are joined.

Then in the second hands-on session we consider site (campus) wide multicast, including deployment of a PIM-SM Rendezvous Point (RP). This represents the campus access router, which may act as the central multicast router on your site. SO in this session we cover the intra-domain issues and features.

In the third set of exercises we move on to deploying multicast inter-domain, so you will be configuring MSDP and MBGP between your access router and the laboratory's core router (which you don't configure – this is conceptually a JANET-level multicast router).

Finally, in the last session, we give you a flavour of IPv6 multicast operation, allowing you to study MLD in action and to configure and test the IPv6-specific embedded-RP feature. You should get a feel from this session as to how IPv6 multicast is different from IPv4 multicast, and how it's deployment model can be more streamlined.



# 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”.

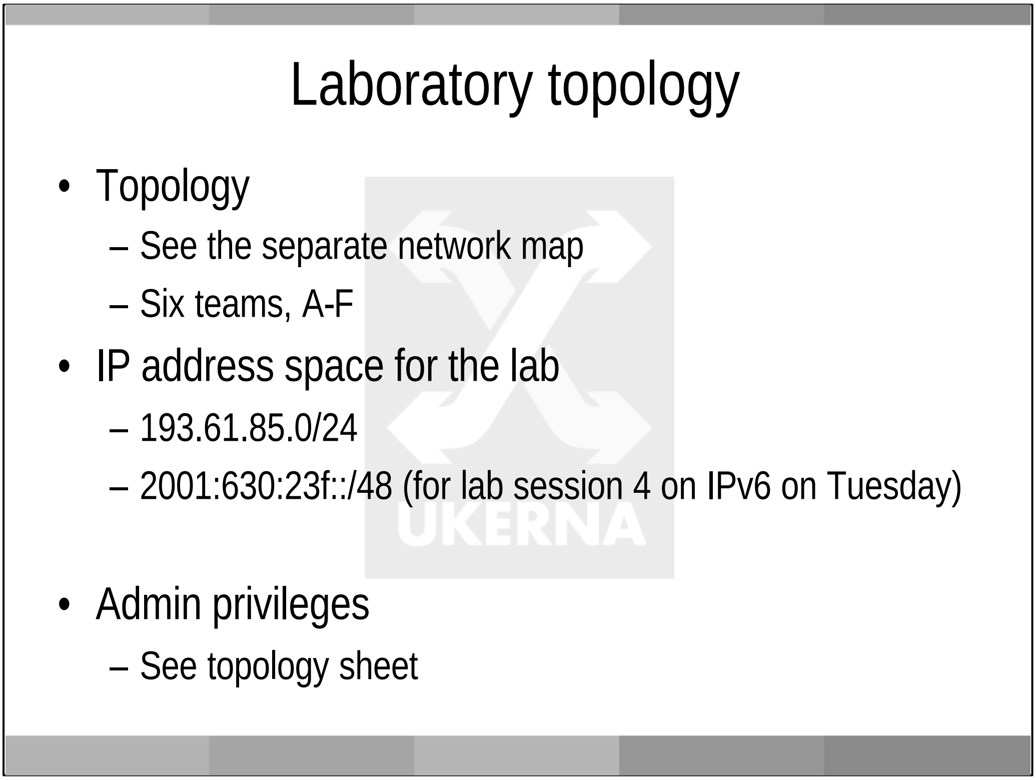
Once enabled, you can examine the running configuration, access much greater usage and debug information and, critically for this lab, configure the router.

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 (for lab session 4 on IPv6 on Tuesday)
- 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 (embedded) RP, MBGP and MSDP functions during the exercises.

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. We will use some external multicast sources in the third and fourth sessions.

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.

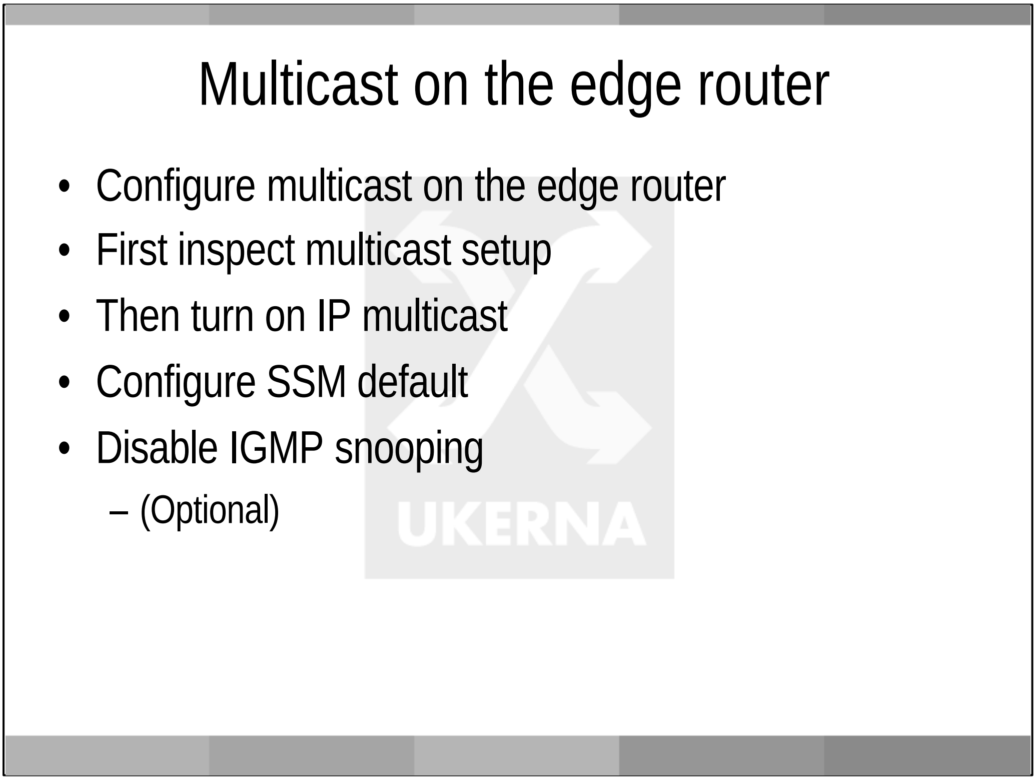
Note that there is only one edge and one access router per group, so you will need to work together and rotate responsibility for configuring the router, etc. In organising the teams, we tried to assign someone with IOS experience to each Team.

# Current setup

- IPv4 unicast in ‘provider’
  - Routing IPv4 unicast towards your access router
  - Routing IPv4 unicast from your access router to your edge router
  - Subnet routes (IPv4 unicast) for your workstation systems
- Stock IPv4 on your client subnets
  - Off-the-shelf Windows XP SP2
  - Manually configured IP settings (no DHCP)
- Next step: get the edge router ready
  - Configuring IP multicast

It is probably worth spending a little time getting familiar with the topology of the laboratory network. The groups have been allocated so that you should all have at least one experienced operator/administrator per group, so if you’re not familiar with core tools such as Ethereal, ping, tracert, etc then please do ask.

Your first task will be to turn multicast on on your edge router, then run some connectivity tests and look at packet dumps from the network to verify behaviour.



# Multicast on the edge router

- Configure multicast on the edge router
- First inspect multicast setup
- Then turn on IP multicast
- Configure SSM default
- Disable IGMP snooping
  - (Optional)

For the purposes of this laboratory, you will enable IP multicast on the edge router, then observe multicast behaviour between two Windows XP clients (on different subnets), by inspecting the traffic on the links and the routing state held by the edge router. We will use Source Specific Multicast (SSM) for these tests.

First you should check on the edge router that no multicast is configured and be confident that no multicast routes are present. This should be the default setup/status when you site down to configure the edge router for the first time.

To do this, enter enable mode and use

```
show ip mroute
```

To turn on IP multicast, enter configure mode and then use the global command

```
ip multicast-routing
```

You should also tell IOS to treat the proper default range (232.0.0.0/8) as SSM

```
ip pim ssm default
```

And to avoid any potential issues with ‘smart’ Layer 2 snooping, you can disable Internet Group Management Protocol (IGMP) snooping

```
no ip igmp snooping
```

To leave config mode, type

```
exit
```

# Quad FE cards and IGMP snooping

- Edge router interfaces
  - One FE
  - One Quad FE
- A vlan has been configured spanning the Quad FE interface
  - IOS can be configured to do IGMP snooping to be ‘smart’ about which multicast traffic is flooded to which physical interfaces
  - For the sake of the workshop, we keep the setup ‘clean’

The Cisco 2801 edge routers have a quad fast Ethernet card for one of the two workstation subnets; in principle IGMP snooping can prevent multicast flooding to switched Ethernet ports without interested hosts, but in practice use of IGMP (and MLD for IPv6) snooping needs to be considered carefully (we will discuss this more in the open session on Day 2 of the workshop).

# Multicast on the router interfaces

- You now need to enter interface-specific commands to enable multicast on the edge router subnets
- Single FE port:
  - Turn on PIM-SM
  - Turn on IGMPv3
- Quad FE port:
  - Turn on PIM-SM
  - Turn on IGMPv3

Having turned on multicast on the router, we now need to configure multicast on each workstation subnet.

First, we select the interface to apply the commands to; enter configure mode and then use

```
int fa0/1
```

will select the single FE interface. Then configure PIM SM and configure IGMPv3 (so that SSM will work; with just IGMPv2 there will be no SSM capability)

```
ip pim sparse-mode
ip igmp version 3
```

Type

```
exit
```

To then step out of the interface configuration level/mode.

Then apply the same configuration to the quad FE interface

```
int vlan1
ip pim sparse-mode
ip igmp version 3
exit
```

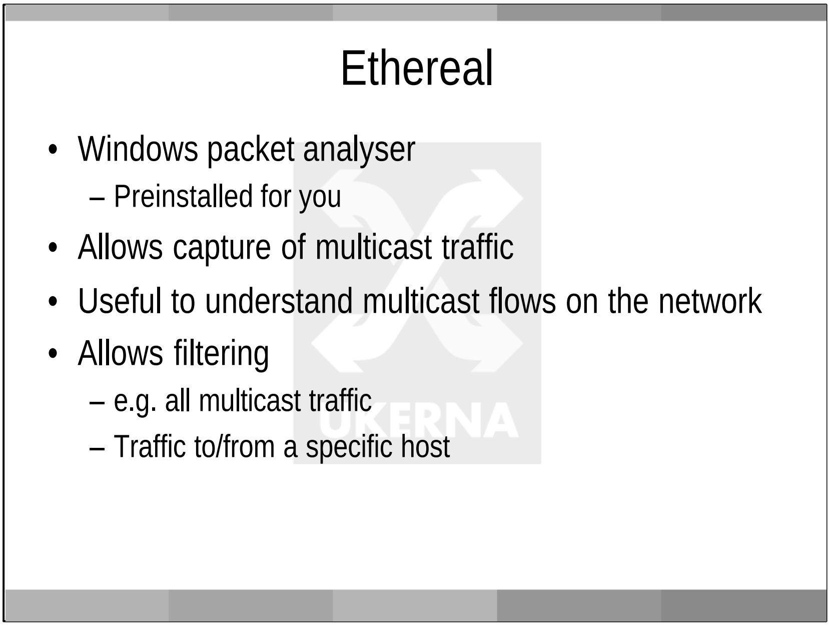
At this stage, everything should be configured on your edge router that is required to support the host-based commands that you'll use in the rest of this exercise.

You can at any time review the multicast routes that your edge router knows about with

```
show ip mroute
```

when outside of the config mode.

From any level you can use ‘end’ to exit the config mode.



# Ethereal

- Windows packet analyser
  - Preinstalled for you
- Allows capture of multicast traffic
- Useful to understand multicast flows on the network
- Allows filtering
  - e.g. all multicast traffic
  - Traffic to/from a specific host

In order to view the interesting multicast packets on the network, some packet analyser is required.

We have pre-installed Ethereal on the Team workstations.

When running Ethereal you will by default see all traffic. In our lab that will be limited; in a real environment it will be much busier.

Ethereal allows you to filter specific traffic to view. You can click on ‘Capture’ on the menu bar, then select Capture Filters, which pops up a window in which you can select the “New” button, and enter filter strings for filtering. You can experiment with these.

As a filter string

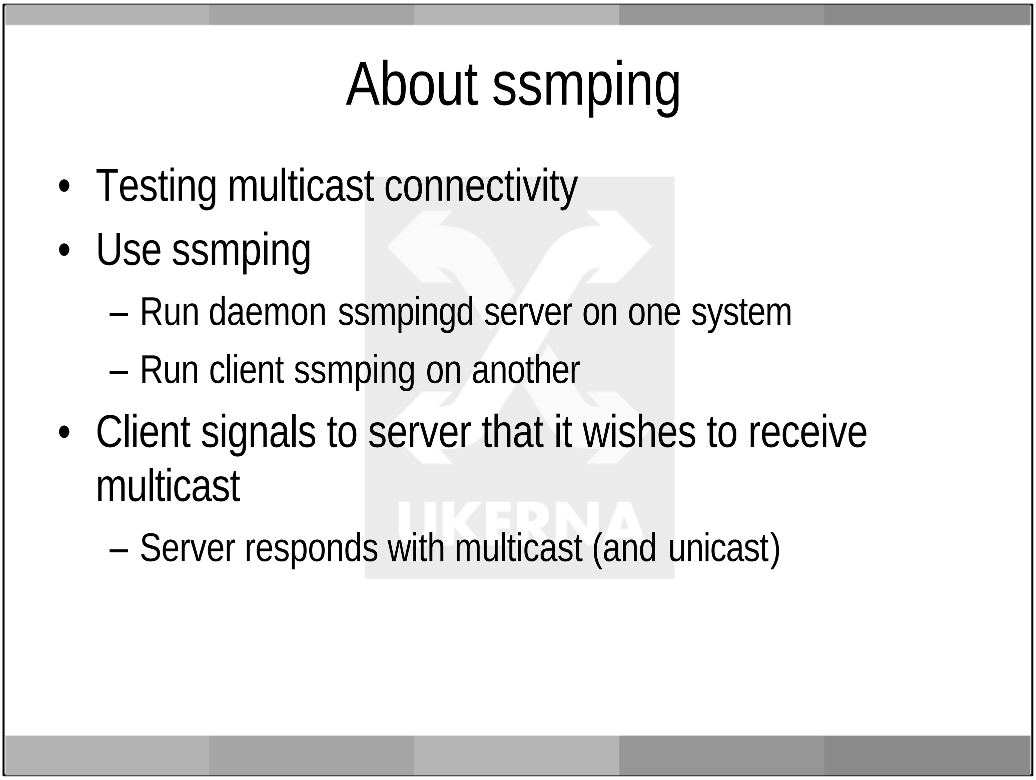
```
ip multicast
```

Should capture all multicast traffic.

To capture all traffic to or from a host, use

```
host <ipaddress>
```

(though note each workstation is in its own subnet in our lab, unless extra laptop devices are plugged in to the QuadFE ports)



# 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)

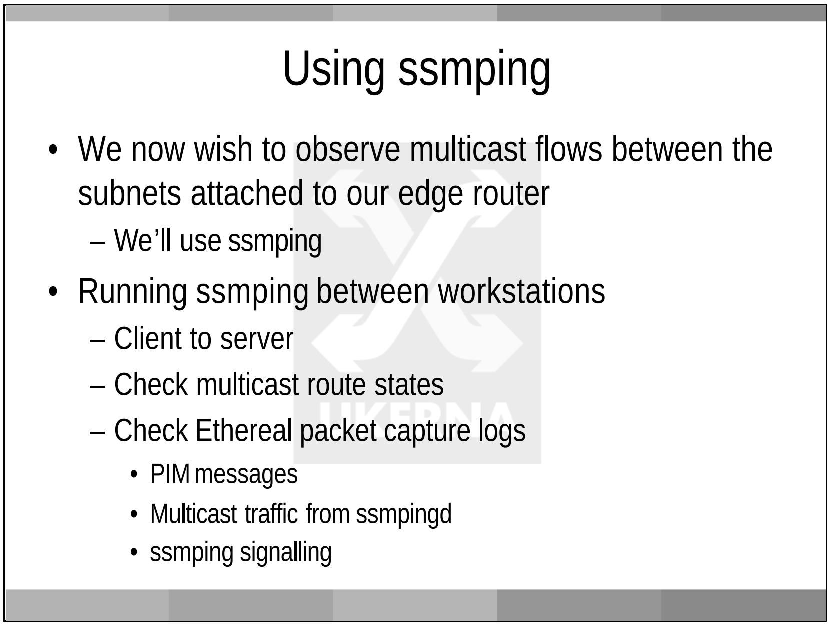
The ssmping tool (and its integral *asmping* counterpart) is very useful for testing multicast connectivity. By running these tools, one can send a message to a host on the Internet (which is running the *ssmping*/*asmping* server) and one will see whether one can receive (unicast and) multicast from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



## Using ssmping

- We now wish to observe multicast flows between the subnets attached to our edge router
  - We’ll use ssmping
- Running ssmping between workstations
  - Client to server
  - Check multicast route states
  - Check Ethereal packet capture logs
    - PIM messages
    - Multicast traffic from ssmpingd
    - ssmping signalling

Start Ethereal on both workstations, to capture the packet flows that you are about to generate.

The ssmping package should be preinstalled on your workstations.

Choose one workstation to be the server and one to be the client.

Start ssmpingd on the server

```
ssmpingd.exe
```

Then run ssmping from the client to the server

```
ssmping-0.8.1.exe <server_ipaddress>
```

You should see unicast and multicast replies.

Log in to the edge router and check the multicast routes

```
show ip mroute
```

What new route entries do you see? Can you identify them for specific (S,G) pairs?

Have a look at the host routing table on the XP workstation. At the command line use

```
route print
```

Inspect the Ethereal capture log; is the traffic what you expected to see?

Stop the ssmping client.

Inspect the Ethereal capture log, and see what multicast packets where exchanged regarding IGMP.

Check the edge router multicast route status.

# Other IOS commands

- You may also wish to try other IOS commands
  - Look at IGMP groups
  - Look at details of those groups
  - Verify multicast is enabled
  - Show counts on the routes

There are some other commands you can try.

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

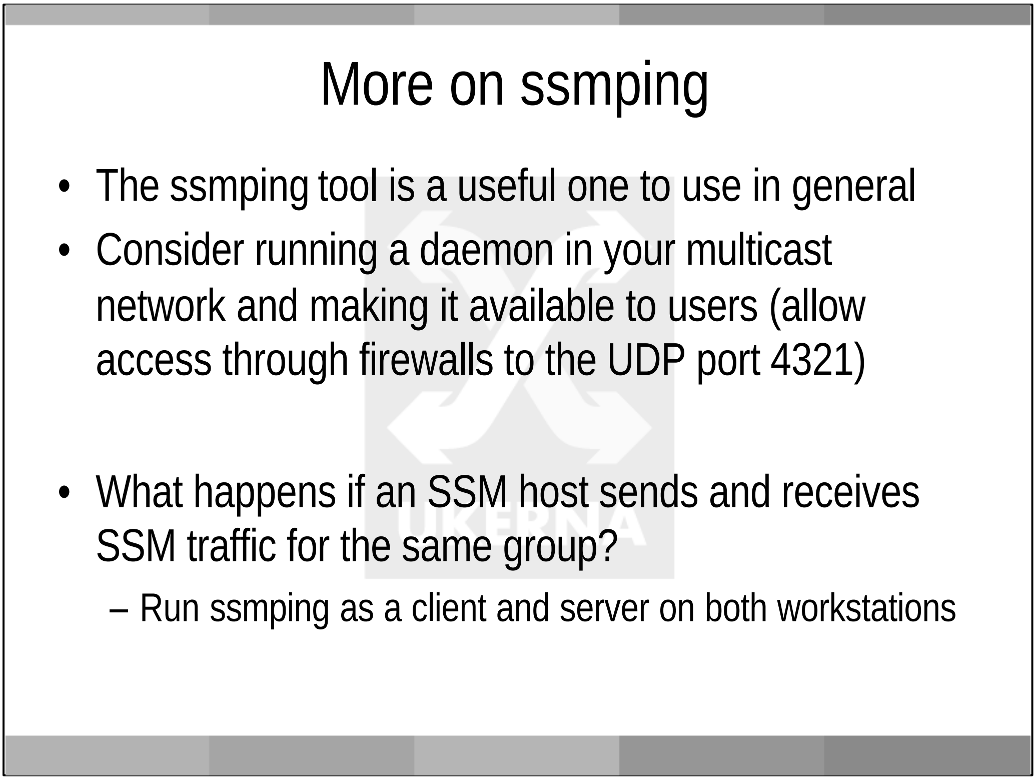
```
show ip multicast
```

To see multicast route information use

```
show ip mroute
```

To show counts on the routes

```
show ip mroute count
```



# More on ssmping

- The ssmping tool is a useful one to use in general
- Consider running a daemon in your multicast network and making it available to users (allow access through firewalls to the UDP port 4321)

- What happens if an SSM host sends and receives SSM traffic for the same group?
  - Run ssmping as a client and server on both workstations

What happens if you try to run deamons on both workstations and run the client from both workstations?

Is this what you expected?

As a site administrator or network operator it’s probably useful for you to run such a server, so that end-users in the site or those wishing to receive content, can use the *ssmping*/*asmping* to check multicast reception.

# Lab Overview

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