Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Home > Network and technology service docs > Vscene > Technical documentation > Configuring a Gatekeeper to use with Janet VideoConferencing > Cisco Multimedia Conference Manager

Cisco Multimedia Conference Manager

The test Cisco® gatekeeper was a Cisco® MCM, running on a Cisco® 3662 router, using Cisco IOS® version 12.2(17). Gatekeeper configuration should be done by persons with experience of the Cisco® Command Line Interface, if possible.

Gatekeeper configuration

Enter gatekeeper configuration mode

Before entering commands it is necessary to be at the correct administration level. This is reached by logging on to the router running the gatekeeper software, and entering the following commands:

enable

This command is used to enter the privileged EXEC mode. The prompt should now change to:

any-gk#

Next enter:

configure terminal

Note that Cisco IOS® will interpret shortened forms of commands, providing that enough letters have been used to allow the router to distinguish between similar commands – so for the above the command

conf t

would be adequate. For the sake of completeness, the full commands are used in this document.

Configuring an H.323 Gatekeeper for use with the Janet Videoconferencing Service

GD/VTAS/016 8

This command starts the configuration mode of the router. The router should then display the words:

“Enter configuration commands, one per line. End with CTRL/Z.”

and the prompt should now change to:

any-gk(config)#

Enter:

gatekeeper

This command causes the router to enter gatekeeper configuration mode. The prompt should now change to:

any-gk(config-gk)#

Set up the local zone

To set up a local zone it is necessary to use the zone local command, which has the format:

zone local gatekeeper-name domain-name

where gatekeeper-name is usually the fully domain-qualified host name of the gatekeeper, and domain-name is the domain served by this gatekeeper. The command to enter is:

```
zone local gatekeeper-name.any.ac.uk any.ac.uk
```

Substitute the gatekeeper’s host name and the local domain as appropriate. The gatekeeper cannot function without having at least one local zone defined in this way.

Specify remote zones

To specify a remote zone use the zone remote command. This takes the form:

```
zone remote other-gatekeeper-name other-domain-name other-gatekeeper-ip-address [port-number]
```

To specify the JANET directory gatekeepers, enter the following command twice, substituting the actual gatekeeper names and IP addresses (as supplied by the JVCS-MC):

```
zone remote gatekeeper-name.ja.net ja.net aaa.bbb.ccc.ddd 1719
```

With a Cisco® gatekeeper configuration it is necessary to define the remote gatekeeper at this point, in order to refer to it when using the ‘zone prefix’ command (see next section).

E.164 address definition

It is necessary to inform the gatekeeper of its own zone address, and that of the Janet directory gatekeeper. The command to do this is zone prefix, which adds a prefix to the gatekeeper zone list. The parts of this command that are used in a standard campus configuration are:

```
zone prefix <gatekeeper-name> <e164-prefix>*
```

The asterisk denotes that the number of digits available for endpoint use is undefined (i.e. any amount).

To define the Anytown college gatekeeper’s zone prefix (which is 0XXYY) the command needs to be issued thus:

```
zone prefix gk.any.ac.uk 00440XXYY *
```

In practice, substitute your own gatekeeper’s DNS (Domain Name Service) name and your own zone number (which is supplied by JVCS-IP and is of the form 0044xxxxx).

The gatekeeper has already had the remote Janet directory gatekeepers defined (see section 7.1.3 above). It now needs to be told of their zone prefix (which is 00). To do this, enter this command twice (substituting the actual DNS names of the Janet directory gatekeepers as supplied by the JVCS-MC):

```
zone prefix gatekeeper-name.ja.net 00*
```

Use the lrq forward-queries command to configure the gatekeeper to forward LRQs (location requests) from endpoints whose E.164 addresses include zone prefixes controlled by remote gatekeepers. The lrq forward-queries command will cause the gatekeeper to forward address resolution requests to the national gatekeeper, which will resolve the zone prefix for the local gatekeeper. This command has no arguments or keywords. Enter:

```
lrq forward-queries
```

Endpoint registration

The command that allows endpoints to register with this gatekeeper is zone subnet. This can allow individual endpoints, or groups of endpoints within particular subnets, to register with the gatekeeper currently being configured. When a zone subnet is configured, a gatekeeper will accept discovery and registration messages sent by endpoints within the subnets defined in the command(s).

The command takes the form:

```
zone subnet <local gk name> <IP add of EP or subnet/mask> enable
```

The subnet that is defined by this command can be limited to a single terminal, or can be a larger subnet with an appropriate net mask. So, in order to allow registration by a terminal with the IP address 192.168.6.11, the Anytown college gatekeeper will have the command in the form:

```
zone subnet gk.any.ac.uk 192.168.6.11/32 enable
```

However, in the same way that access to files is often configured by first defining no access whatever (‘DENY ALL’) and then defining the exceptions to this, the gatekeeper should be instructed to ignore discovery messages and registration attempts from all IP addresses in the college, before those that are permitted access are granted it. By default, the gatekeeper will allow and accept registration attempts from any H.323 endpoints within its local subnets. The definitions of particular addresses that are allowed to communicate with the gatekeeper are therefore meaningless without a statement which disallows all preceding them. For this reason it is necessary to issue the negative of the zone subnet command – no zone subnet – to stop the acceptance of messages from any but pre-defined addresses. Enter the following command (with the real gatekeeper host name substituted):

```
no zone subnet gk.any.ac.uk default enable
```

The zone subnet command can then be used to create a list of endpoints that are permitted to communicate with the gatekeeper. This is obviously a far more secure method of working than leaving the default situation, which could allow ‘rogue’ endpoints to register and use the services of the gatekeeper.

So the no zone subnet command is followed by a series of endpoint definitions, one by one. Enter the command for each terminal that you wish to allow to register with the gatekeeper:

```
zone subnet gk.any.ac.uk 192.168.6.11/32 enable
zone subnet gk.any.ac.uk 192.168.6.12/32 enable
zone subnet gk.any.ac.uk 192.168.7.0/24 enable
```

Enable the gatekeeper

The MCM will, by default, assume that the gatekeeper will use the H.323 proxy service (see section 7.2 below). If the intention is to use the MCM only as a gatekeeper, and not to use the H.323 proxy service, then enter the command:

```
no use-proxy any-gk.any.ac.uk default inbound-to terminal
no use-proxy any-gk.any.ac.uk default outbound-from terminal
```

The last command necessary for a Cisco® gatekeeper configuration enables the gatekeeper. The command is:

```
no shutdown
```
and it has no arguments or keywords.

Save the configuration to memory

At this point the administrator should enter CTRL -Z to exit from gatekeeper configuration mode. It will then be necessary to save the configuration. This can be done by entering

```
write mem
```
or
```
copy run start
```

which will cause the gatekeeper configuration to be saved.

Cisco® H.323 proxy configuration

The Cisco® MCM also has an H.323 proxy service. This acts as a security measure by hiding all internal addresses from the external Internet. Its logical function is that of an IP/IP gateway – a bridge between two discrete IP networks. The proxy registers with the gatekeeper as an endpoint to which the gatekeeper routes packets.
The commands necessary to configure the H.323 proxy service are detailed below. To turn on the proxy service, enter this command before configuring the physical port to which the proxy is attached:

```
proxy h323
```

Then start configuration of the physical port on which you wish to run the proxy by entering:

```
interface FastEthernet0/0
```

To ensure the current interface’s IP address will be used by the proxy to register with the gatekeeper, use the following command:

```
h323 interface
```

The next command registers an H.323 proxy alias with the gatekeeper. The command takes the form: h323 h323-id <alias>. The alias can be an IP address or email-type address: any-px@any.ac.uk [1]. The alias in this case is any-px.any.ac.uk (substitute a suitable alias of your own):

```
h323 h323-id any-px.any.ac.uk
```

Next it is necessary to specify the gatekeeper associated with the proxy. The h323 gatekeeper command (example below) specifies the IP address to which gatekeeper registration requests will be unicast. Note that the commands here and above must be issued in the correct order; i.e. the h323 interface and h323 h323-id commands must be used before using the h323 gatekeeper command. Also, the h323 gatekeeper command must be specified on your Cisco IOS® platform or the proxy will not go online. The proxy will use this interface address as its signalling address for RAS (Registration, Admission, and Status Protocol) messages. Enter (with the IP address of your gatekeeper substituted):

```
h323 gatekeeper ipaddr 192.168.7.8
```

Return to gatekeeper configuration (the prompt will end with (config-gk)#), then instruct the gatekeeper to use the proxy for incoming and outgoing calls between local and remote zones, by typing the following three commands at the command line. Substitute the gatekeeper name supplied by the JVCS for ‘gatekeepername’ and your own gatekeeper’s name for ‘any-gk.ac.uk’.

```
use-proxy any-gk.ac.uk remote-zone gatekeepername.ja.net inbound-to terminal
use-proxy any-gk.ac.uk default inbound-to terminal
use-proxy any-gk.ac.uk default outbound-from terminal
```

These commands actually reinforce the default behaviour that occurs if the simple statement ‘use-proxy’ (with no arguments) is entered here, but it is recommended that the proxy behaviour is defined explicitly, which these commands do.

Checking gatekeeper registration

It is sometimes useful to be able to check which terminals are currently registered with the gatekeeper. To do this, enter gatekeeper configuration mode (see section 7.1.1 above). Then enter this command:

```
Show gatekeeper endpoints
```

A table will be produced with various fields for each terminal, including the H323-ID of the terminal(s) currently registered.

Cisco® MCM references

Cisco® IOS Release 12.2, Command reference
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/ [2]
Cisco® Gatekeeper/Multimedia Conference Manager
http://www.cisco.com/en/US/products/sw/voicesw/ps4139/index.html

[3]

Source URL: https://community-stg.jisc.ac.uk/library/videoconferencing-booking-service/cisco-multimedia-conference-manager

Links
[1] mailto:any-px@any.ac.uk
[2] http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/
[3] http://www.cisco.com/en/US/products/sw/voicesw/ps4139/index.html