TANDBERG Gatekeeper User Manual

Software version N3

D13381.03

Trademarks and copyright

Disclaimer

The information in this document is furnished for informational purposes only, is subject to change without prior notice, and should not be construed as a commitment by TANDBERG ASA.

The information in this document is believed to be accurate and reliable, however TANDBERG ASA assumes no responsibility or liability for any errors or inaccuracies that may appear in this document, nor for any infringements of patents or other rights of third parties resulting from its use. No license is granted under any patents or patent rights of TANDBERG ASA.

Environmental Issues

Thank you for buying a product which contributes to a reduction in pollution, and thereby helps save the environment. Our products reduce the need for travel and transport and thereby reduce pollution. Our products have either none or few consumable parts (chemicals, toner, gas, paper). Our products are low energy consuming products.

TANDBERG's Environmental Policy

- TANDBERG's Research and Development is continuously improving TANDBERG's products towards less use of environmentally hazardous components and substances as well as to make the products easier to recycle.
- TANDBERG's products are Communication Solutions. The idea of these solutions is to reduce the need for expensive, time demanding and polluting transport of people. Through people's use of TANDBERG's products, the environment will benefit from less use of polluting transport.
- TANDBERG's wide use of the concepts of outsourcing makes the company itself a company with a low rate of emissions and effects on the environment.
- TANDBERG's policy is to make sure our partners produce our products with minimal influence on the environment and to demand and audit their compatibility according to applicable agreements and laws (national and international).

Environmental Considerations

Like other electronic equipment, the TANDBERG Gatekeeper contains components that may have a detrimental effect on the environment. TANDBERG works continuously towards eliminating these substances in our products.

- Printed-wiring boards made of plastic, with flame-retardants like Chloride or Bromide.
- Component soldering that contains lead.
- Smaller components containing substances with possible environmental effect.

After the product's end of life cycle, it should be returned to authorized waste handling and should be treated according to National and International Regulations for waste of electronic equipment.

Operator Safety Summary

For your protection, please read these safety instructions completely before operating the equipment and keep this manual for future reference. The information in this summary is intended for operators. Carefully observe all warnings, precautions and instructions both on the apparatus and in the operating instructions.

Warnings

- Water and moisture - Do not operate the equipment under or near water - for example near a bathtub, kitchen sink, or laundry tub, in a wet basement, or near a swimming pool or in areas with high humidity.
- Cleaning - Unplug the apparatus from the wall outlet before cleaning or polishing. Do not use liquid cleaners or aerosol cleaners. Use a lint-free cloth lightly moistened with water for cleaning the exterior of the apparatus.
- Ventilation - Do not block any of the ventilation openings of the apparatus. Install in accordance with the installation instructions. Never cover the slots and openings with a cloth or other material. Never install the apparatus near heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
- Grounding or Polarization - Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or third prong is provided for your safety. If the provided plug does not fit into your outlet, consult an electrician.
- Power-Cord Protection - Route the power cord so as to avoid it being walked on or pinched by items placed upon or against it, paying particular attention to the plugs, receptacles, and the point where the cord exits from the apparatus.
- Attachments - Only use attachments as recommended by the manufacturer.
- Accessories - Use only with a cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.
- Lightning - Unplug this apparatus during lightning storms or when unused for long periods of time.
- Servicing - Do not attempt to service the apparatus yourself as opening or removing covers may expose you to dangerous voltages or other hazards, and will void the warranty. Refer all servicing to qualified service personnel.
- Damaged Equipment - Unplug the apparatus from the outlet and refer servicing to qualified personnel under the following conditions:
    - When the power cord or plug is damaged or frayed
    - If liquid has been spilled or objects have fallen into the apparatus
    - If the apparatus has been exposed to rain or moisture
    - If the apparatus has been subjected to excessive shock by being dropped, or the cabinet has been damaged
    - If the apparatus fails to operate in accordance with the operating instructions.

Table Of Contents

1 Introduction

This User Manual is provided to help you make the best use of your TANDBERG Gatekeeper.

A Gatekeeper is a central part of an H.323 infrastructure. It provides address translation and controls access to the network for H.323 terminals, Gateways and MCUs. The Gatekeeper also provides other services to the terminals, Gateways and MCUs such as bandwidth management and locating Gateways.

A Gatekeeper is also a key component of TANDBERG's Expressway™ firewall traversal solution. Used in conjunction with a TANDBERG Border Controller it allows calls to be made into and out of a secured private network.

The main features of the TANDBERG Gatekeeper are:

- Automatic discovery and manual registrations of H.323 terminals, gateways and MCUs.
- Registration of H.323 ID, E.164 aliases and services.
- Secure traversal of any firewall or NAT.
- URI dialing.
- Supports up to 1000 registered devices and services.
- Supports up to 100 neighboring zones.
- Up to 200 active calls.
- Up to 100 traversal calls.
- Flexible zone configuration with and without prefixes.
- Can function as a leaf Gatekeeper or as a master Gatekeeper in a Gatekeeper hierarchy.
- Can be used to control the amount of bandwidth used both within a zone and to neighboring zones.
- Can limit total bandwidth usage and set maximum per call bandwidth usage with automatic down-speeding if call exceeds per-call maximum.
- Can be managed with TANDBERG Management Suite 9.0 or newer, or as a standalone system with RS-232, Telnet, SSH, HTTP and HTTPS.
- Embedded setup wizard on serial port for initial configuration.

Note that features may vary depending on software package.

1.1 TANDBERG Gatekeeper Overview

On the front of the Gatekeeper there are three LAN interfaces, a serial port (Data 1) and a Light Emitting Diode (Power). The LAN 1 interface is used for connecting the system to your local area network, LAN interface 2 and 3 are disabled. The serial port (Data 1) is for connection to a PC, and power on is indicated by the Light Emitting Diode (Power) being lit.

The back of the Gatekeeper has a power connector, a power switch, and a serial port (Data 2) for connecting to a PC.

2 Installation

Precautions:

- Never install communication equipment during a lightning storm.
- Never install jacks for communication cables in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninstalled communication wires or terminals unless the communication line has been disconnected at the network interface.
- Use caution when installing or modifying communication lines.
- Avoid using communication equipment (other than a cordless type) during an electrical storm.
- There may be a remote risk of electrical shock from lightning.
- Do not use communication equipment to report a gas leak in the vicinity of the leak.
- The socket outlet shall be installed near to the equipment and shall be easily accessible.
- Never install cables without first switching the power OFF.
- This product complies with directives: LVD 73/23/EC and EMC 89/366/EEC.
- Power must be switched off before power supplies can be removed from- or installed into the unit.

2.1 Unpacking

The TANDBERG Gatekeeper is delivered in a special shipping box which should contain the following components**:**

- Gatekeeper unit
- Installation sheet
- User manual and other documentation on CD
- Rack-ears and screws
- Kit with 4 rubber feet.
- Cables:
    - Power cables
    - One Ethernet cable
    - One null-modem RS-232 cable

Installation site preparations

- Make sure that the Gatekeeper is accessible and that all cables can be easily connected.
- For ventilation: Leave a space of at least 10cm (4 inches) behind the Gatekeeper's rear and 5cm (2 inches) on the sides.
- The room in which you install the Gatekeeper should have an ambient temperature between 0^{o}C and 35^{o}C (32^{o}F and 95^{o}F) and between 10% and 90% non-condensing relative humidity.

- Do not place heavy objects directly on top of the Gatekeeper.
- Do not place hot objects directly on top, or directly beneath the Gatekeeper.
- Use a grounded AC power outlet for the Gatekeeper.

2.2 Mounting

The Gatekeeper comes with brackets for mounting in standard 19" racks.

Before starting the rack mounting, please make sure the TANDBERG Gatekeeper is placed securely on a hard, flat surface.

1. Disconnect the AC power cable.

2. Make sure that the mounting space is according to the `Installation site preparations' in section 2.1.

3. Attach the brackets to the chassis on both sides of the unit.

4. Insert the unit into a 19" rack, and secure it with screws.

2.3 Connecting Cables

Power cable

Connect the system power cable to an electrical distribution socket.

LAN cable

Connect a LAN cable from the LAN 1 connector on the front of the unit to your local area network.

Null-modem RS-232 cable

Connect the supplied null-modem RS-232 cable between the Gatekeeper’s Data 1 connector and the COM-port on a PC.

2.4 Switching on the System

To start the TANDBERG Gatekeeper, make sure that the following has been done:

- The power cable is connected.
- The LAN cable is connected

Then switch the power switch button on the back of the unit to ’1'.

On the front of the chassis you will see the Power LED being lit.

2.5 Gatekeeper Initial Configuration

The TANDBERG Gatekeeper requires some configuration before it can be used. This must be done using a PC connected to the serial port (Data 1).

The main thing that needs to be configured is the IP settings of the Gatekeeper. This includes the IP address, the IP subnet mask, and the IP gateway. The Gatekeeper has to be configured with a static IP address. Consult your network administrator for information on which addresses to use.

To set the initial configuration, do the following:

1. Connect the supplied null-modem RS-232 cable from Data 1 to a PC running a terminal program.
2. Start the terminal program and configure it with baud rate 115200, 8 data bits, no parity, 1 stop bit, no flow control.
3. Power on the unit if it is not already on.
4. You should see the unit display start up information.
5. After approximately 1 minute you will get a login prompt.
6. Enter username 'admin' and your password. The default password is TANDBERG.
7. You will be prompted if you want to run the install wizard. Type 'Y' and press Enter.

```
(none) login: admin
Password:
Run install wizard [n]: Y
```

8. Specify the following:
    a. The password you want to use for your system. This password is used to login to the system with the Admin user account.
    b. The IP address of the system.
    c. The IP subnet mask of the system.
    d. The IP default gateway of the system.
    e. The Ethernet speed.
    f. The local zone prefix you want to use for the zone controlled by this system.
    g. Whether you want to use SSH to administer the system.
    h. Whether you want to use Telnet to administer the system.
9. You will be prompted to login again. You should see a welcome message like this.

```
Welcome to
TANDBERG Gatekeeper Release N3.0
SW Release Date: 2005-06-15
OK
```

10. Login with username 'admin' and your password.
11. Review other system settings. You may want to set the following:
    a. The name of the Gatekeeper. This is used to identify the Gatekeeper by the TANDBERG Management Suite and by the TANDBERG Border Controller. See the `xConfiguration SystemUnit` command in section 5.2 for more information on setting the name
    b. Automatic discovery. If you have multiple Gatekeepers in the same network you may want to disable automatic discovery on some of them. See the

`xConfiguration Gatekeeper AutoDiscovery` command in section 5.2 for more information.

12. Reboot the Gatekeeper by typing the command `xCommand boot` to make your new settings take effect.
13. Disconnect the serial cable.

NOTE

To secure the Gatekeeper you should disable HTTP, HTTPS, SSH and Telnet, relying on the serial interface for management. If you need IP connectivity, it is recommended that you use SSH or HTTPS.

NOTE

If you do not have an IP gateway, configure it with an unused IP address that is valid in your subnet as your IP gateway.

3 Using the Gatekeeper

The Gatekeeper is used by H.323 terminals, Gateways and MCUs. These devices register with the Gatekeeper and the Gatekeeper then provides address translation and controls access to the network.

3.1 System Administration

To configure and monitor the TANDBERG Gatekeeper you can either use the web interface or a command line interface. The command line interface is available over SSH and Telnet, or through the serial port. The interface is the same using all three access methods.

To enter commands you should start a session and login with username ‘admin’ and your password.

The interface groups information in different commands

xstatus	Provides a read only interface to determine the current status of the system. Information such as current calls and registrations is available through this command group.
xconfiguration	A read/write interface to set system configuration data such as IP address and subnet.
xcommand	A miscellaneous group of commands for setting information or obtaining it.
xhistory	Provides historical information about calls and registrations.
xfeedback	An event interface, providing information about calls and registrations.

A command reference is given in section 5, Configuring the Gatekeeper.

3.2 Registration

Before an endpoint can use the Gatekeeper it must register with the Gatekeeper. There are two ways an endpoint can register:

- Automatically.
- Manually by specifying the IP address of the Gatekeeper.

You can disable automatic registration on the Gatekeeper. See auto discovery in section 5.2 for more information.

When registering, the endpoint registers with one or more of the following:

- One or more H.323 IDs.
- One or more E.164 aliases.
- One or more services.

Users on other registered endpoints can then call the endpoint by using the H.323 ID, a URI, an E.164 alias, or one of the services.

Consult the endpoint documentation for information on how to configure it with a Gatekeeper.

The Gatekeeper can be configured to only accept registrations from particular endpoints. See section 3.7, Registration Control for details.

NOTE

Automatic discovery is a function that allows the Gatekeeper to reply to multicast Gatekeeper discovery messages from the endpoint.

NOTE

If you have problems registering the endpoint, try turning on automatic discovery. Some endpoints require automatic registration to be enabled.

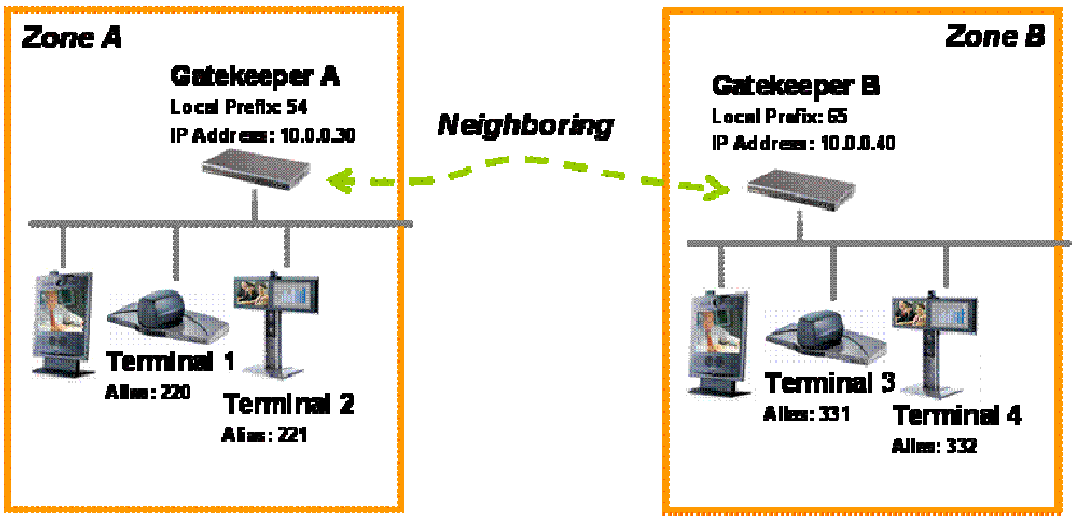
NOTE

When URI dialing is used to discover an endpoint, the URI used is based on either the H.323 ID or the E.164 alias that the endpoint registered with. The local domain is then added to this. See section 3.9, URI Dialing for more details

3.3 Neighbor Gatekeepers

You may configure several Gatekeepers to work together, each taking responsibility for part of the endpoint community. You will typically want to do this for separate geographical regions or organizational entities. You may create a list of up to 100 neighbor Gatekeepers. Each of these may be assigned a prefix, similar to an area code in telephony terms. All endpoints which register with that Gatekeeper are assigned the same number prefix. They are referred to as being in the Gatekeeper's zone. When one Gatekeeper needs to query another for a particular number, it can consult its own prefix list, find the appropriate Gatekeeper and issue the query.

The figure below shows an example with two zones, zone A with local prefix 54 and zone B with local prefix 65. A also has B configured as its neighbor.



This means that a system in zone A can call a system in zone B. If terminal 1 wants to dial terminal 3 it can do so by prefixing the number of terminal 3 with the zone prefix of zone B; the number to dial will then be 65331.

The TANDBERG Gatekeeper also supports prefixless zones. If none of the prefix zones provide a match for a dialed number, all of the prefixless zones will be queried.

In the example above, if Gatekeeper A had configured Gatekeeper B as a prefixless zone, Terminal 1 could call Terminal 3 by dialing 331. Gatekeeper A will not recognize 331 as a registered alias and because of this "forward" the request to the Gatekeeper in zone B.

Zones also play an important role in helping you to control the amount of traffic on your network. See section 3.6, Bandwidth Control for details on this.

Remote zones can be configured through the web interface of the TANDBERG Gatekeeper by navigating to *Gatekeeper Configuration* > *Gatekeeper*. See Figure 1 for a screenshot of the configuration.

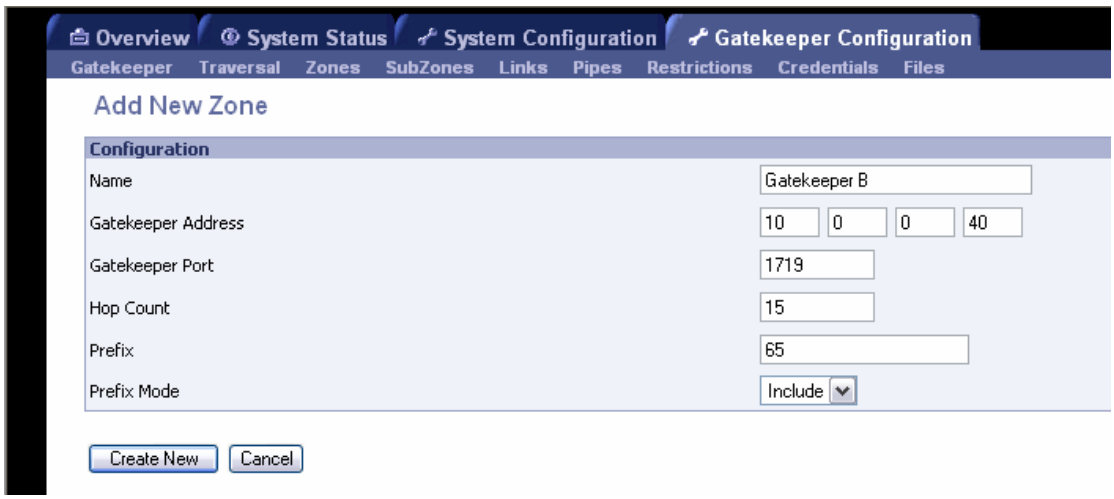


Figure 1 Screenshot of the Adding a New Zone configuration

NOTE

When using a local zone prefix do not start the E.164 aliases with the same digits as the local prefix. If you do this the Gatekeeper will strip the digits equal to the prefix from the alias thinking it is a call from another zone.

NOTE

If you want to use URI dialing (see section 3.9, URI Dialing) to neighbor Gatekeepers you should not use prefixes on your zones.

NOTE

If prefixing zones are used, all prefixes used must be unique to both the other zones as well as to any other alias or service prefixes registered to the gatekeeper.

NOTE

If prefix mode is set to “Strip” rather than “Include” the gatekeeper will not send the remote zone prefix to the far end gatekeeper in the Location Requests.

3.4 Alternate Gatekeepers

Alternate Gatekeeper support is provided to increase the reliability of your deployment. If one Gatekeeper becomes unavailable, perhaps due to a network or power outage, another will be used as an Alternate. Alternate Gatekeepers share responsibility for their endpoint community: an individual endpoint may be registered with any one of the Alternates. You should configure Alternate Gatekeepers identically for all registration and call features such as authentication, bandwidth control and policy. If you do not do this, endpoint behavior will vary unpredictably depending on which Alternate it is currently registered with. Alternate Gatekeepers should also be deployed on the same LAN as each other so that they may be configured with the same routing information such as local domain names and local domain subnet masks.

Each Gatekeeper may be configured with the IP addresses of up to five Alternates. When an endpoint registers with the Gatekeeper, it is presented with the IP addresses of all the Alternates. If the endpoint loses contact with its initial Gatekeeper, it will seek to register with one of the Alternates. This may result in your endpoint community’s registrations being spread over all the Alternates.

When a Gatekeeper receives a Location Request, if it cannot respond from its own registration database, it will query all of its Alternates before responding. This allows the pool of registrations to be treated as if they were registered with a single Gatekeeper.

The Alternate Gatekeepers can be configured within the web interface of the Gatekeeper by navigating to *Gatekeeper Configuration* > *Gatekeeper*. Up to five different alternates can be configured. Please see Figure 2 for a screenshot of a sample configuration.

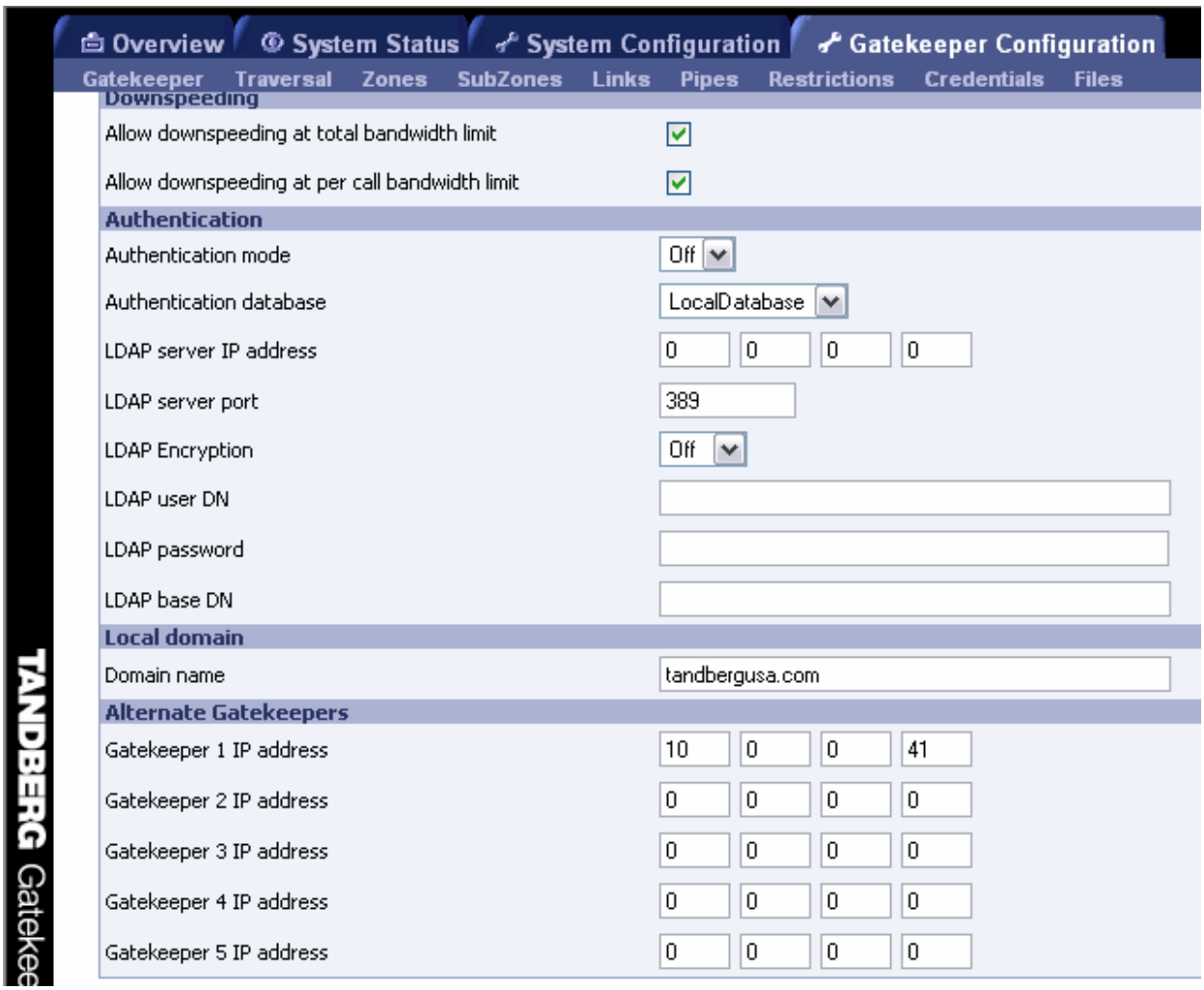


Figure 2 Screenshot of the Alternate Gatekeeper configuration

3.5 Call Control

When an end-point wants to call another endpoint it presents the address it wants to call to the Gatekeeper using a protocol knows as RAS. The Gatekeeper tries to resolve this address and supplies the calling endpoint with information about the called endpoint. The destination address can take several forms: IP address, H.323 ID, E.164 alias or a full H.323 URI.

Dialing by IP address is necessary when the destination endpoint is not registered with a Gatekeeper or Border Controller. If it is registered, then one of the other addressing schemes should be used instead as they are more flexible.

When an H.323 ID or E.164 alias is used, the Gatekeeper looks for a match between the dialed address and the aliases registered by its endpoints. If no match is found, it may query other Gatekeepers and Border Controllers.

When dialing by H.323 URI, the destination address resembles an email address. The Gatekeeper first follows the procedure for matching H.323 IDs. If that fails it looks for a Gatekeeper or Border Controller responsible for the domain (the part of the URI following the @) and queries that device.

NOTES

ARQ, Admission Request. An endpoint request to make or answer a call

LRQ, Location Request. A query between Gatekeepers or Border Controllers to determine the location of an endpoint.

RAS, Registration, Admission and Status Protocol. Used by endpoints and Gatekeepers to communicate.

The Figures 1 and 2 illustrate the process the Gatekeeper performs when receiving call requests.

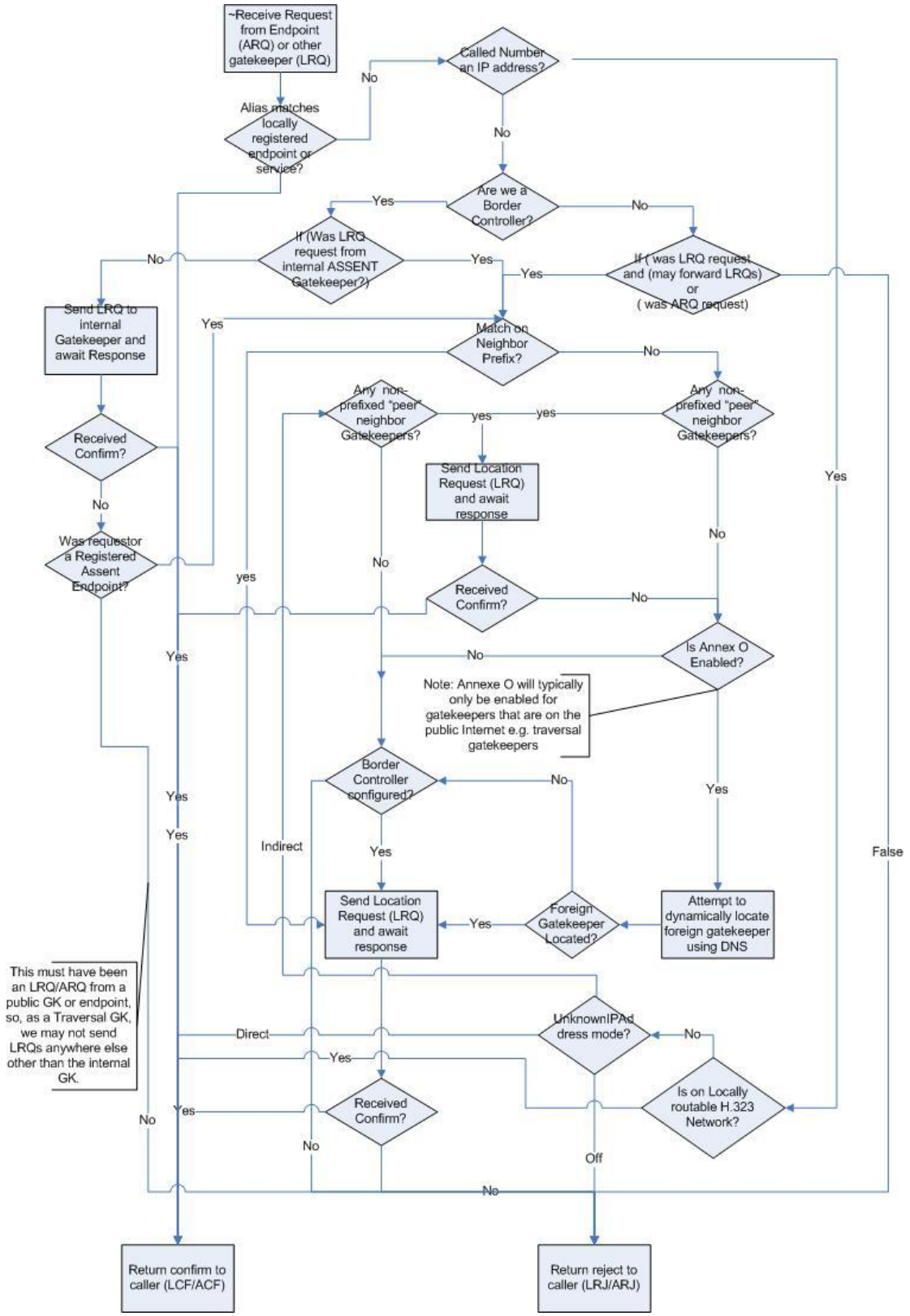


Figure 3 Admission Request Processing

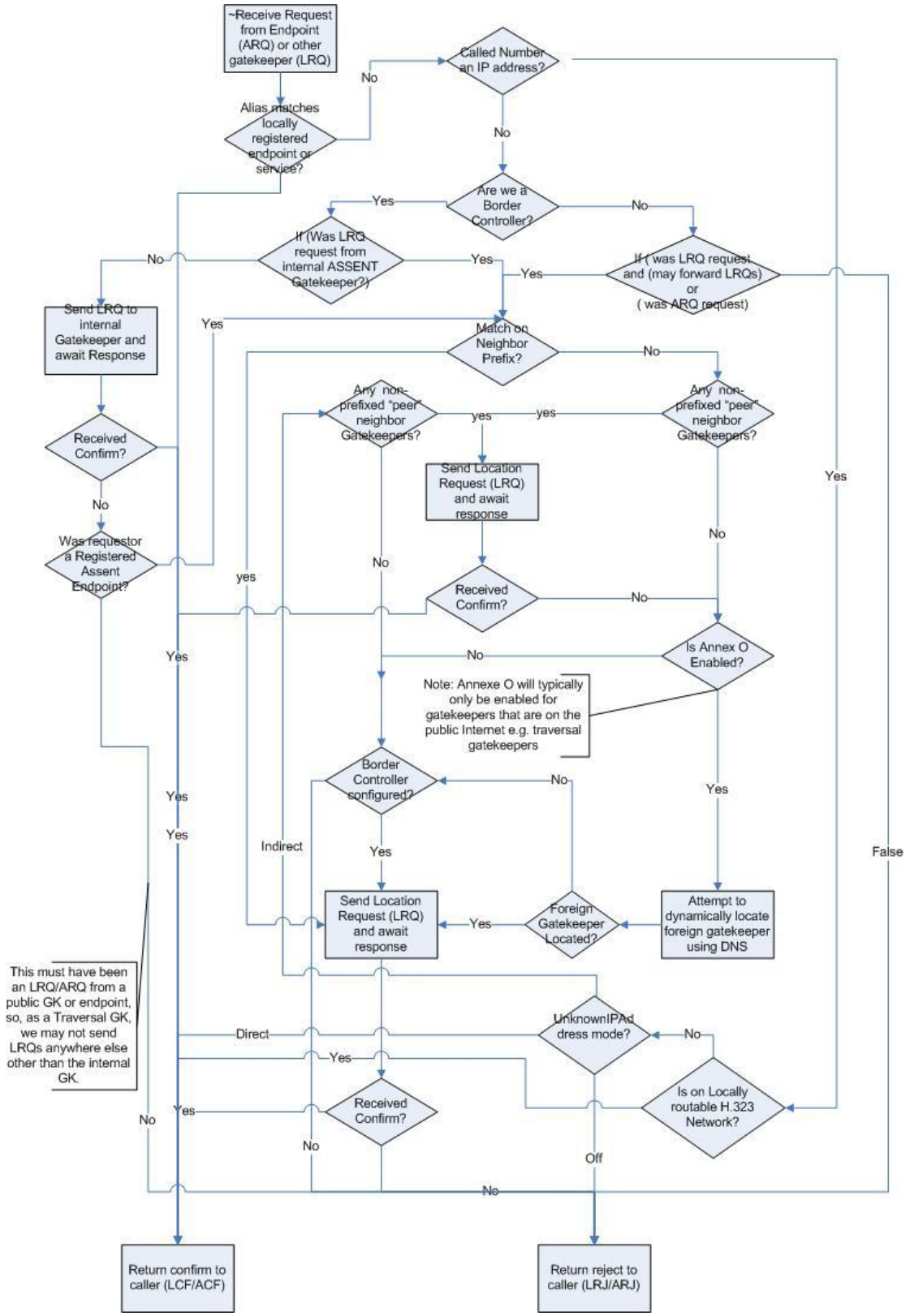


Figure 4 Location Request Processing

3.6 Bandwidth Control

The TANDBERG Gatekeeper allows you to control endpoints' use of bandwidth on your network. Figure 5 shows a typical deployment: a broadband LAN, where high bandwidth calls are acceptable, a pipe to the internet with restricted bandwidth, and two satellite offices, each with their own restricted pipes. In order to utilize the available bandwidth efficiently, the TANDBERG Gatekeeper allows you to model your network, and bandwidth controls on individual components of the network. Bandwidth controls may be set on a call by call basis and on a total concurrent usage basis.

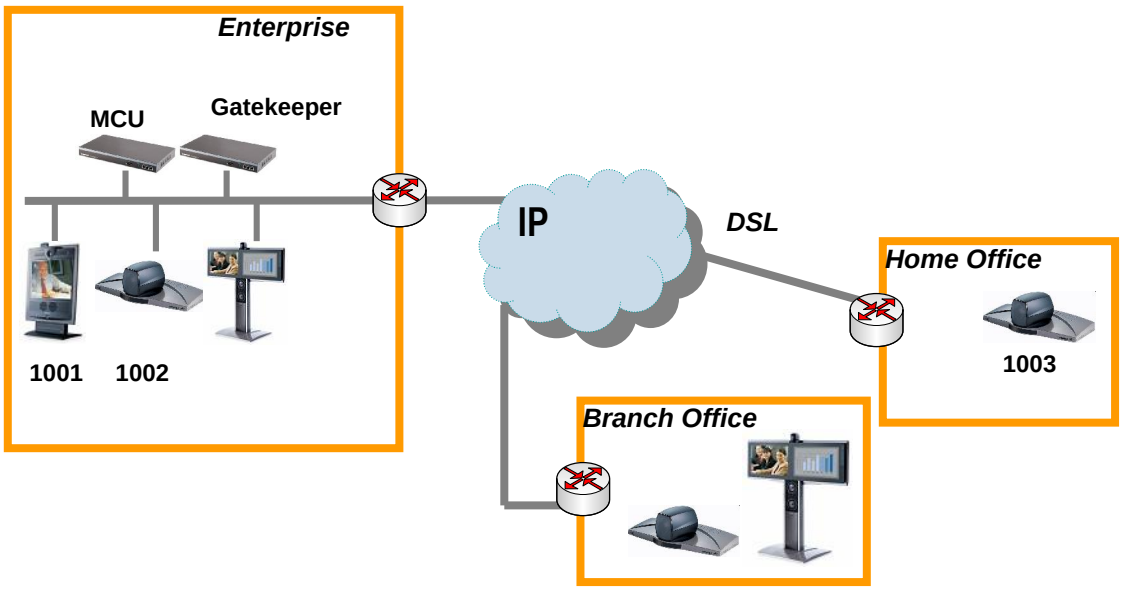


Figure 5 Typical network deployment

All endpoints registered with your Gatekeeper are part of its local zone. As shown in Figure 5, the local zone can contain many different networks with different bandwidth limitations. In order to model this, the local zone is made up of one or more subzones. When an endpoint registers with the Gatekeeper it is assigned to a subzone, based on its IP address.

By default all endpoints registering with the Gatekeeper are assigned to the default subzone. This is suitable if you have uniform bandwidth available between all your endpoints. When you have differing bandwidth provision, as in Figure 5, you should create a new subzone for each pool of endpoints.

Subzones are added and configured through the web interface on the *Gatekeeper Configuration* > *SubZones* page, or through the command line using the following commands:

```
xConfiguration SubZones SubZone [1..100] Name
xConfiguration SubZones SubZone [1..100] Subnet IP Mask
xConfiguration SubZones SubZone [1..100] Subnet IP Address
```

Subzones may be configured with links joining them to each other and to other zones. These links are used to calculate how a call is routed over the network and so which zones and subzones are involved. If multiple routes are possible, your Gatekeeper will select the one with the fewest links.

Links may be configured through the web interface on the *Gatekeeper Configuration* > *Links* page, or through the command line using the following commands:

```
xConfiguration Links Link [1..100] Name
xConfiguration Links Link [1..100] Node1 Name
xConfiguration Links Link [1..100] Node2 Name
xConfiguration Links Link [1..100] Pipe1 Name
```

```
xConfiguration Links Link [1..100] Pipe2 Name
```

Each subzone may be configured with its own bandwidth limits. Calls placed between two endpoints in the same subzone consume resource from the subzone's allocation. Subzone bandwidths are configured on the *Gatekeeper Configuration* > *SubZones* page (see Figure 6 for a screenshot of the configuration) or using the following command line commands:

```
xConfiguration SubZones SubZone [1..100] Bandwidth TotalMode
xConfiguration SubZones SubZone [1..100] Bandwidth Total Limit
xConfiguration SubZones SubZone [1..100] Bandwidth PerCall Mode
xConfiguration SubZones SubZone [1..100] Bandwidth PerCall Limit
```

When calls are placed between endpoints in different subzones, it is possible to control the bandwidth used on the link between them. To do this, create a pipe and configure it with the required bandwidth characteristics. This pipe is then assigned to a link. Calls traversing the link will now take the pipe's bandwidth allocation into consideration. Pipes are created and configured on the *Gatekeeper Configuration* > *Pipes* page (see Figure 7 for a screenshot of the Pipe Configuration) or using the following command line commands:

```
xConfiguration Pipes Pipe [1..100] Name
xConfiguration Pipes Pipe [1..100] Bandwidth Total Mode
xConfiguration Pipes Pipe [1..100] Bandwidth Total Limit
xConfiguration Pipes Pipe [1..100] Bandwidth PerCall Mode
xConfiguration Pipes Pipe [1..100] Bandwidth PerCall Limit
```

Pipes may be shared between one or more links. This is used to model the situation where a site communicates with several other sites over the same broadband connection to the Internet. Each link may have up to two pipes associated with it. This is useful for modeling two sites, each with their own broadband connection to the Internet backbone. Calls between zones or subzones consume bandwidth from each zone and any pipes on the link between them.

When a Gatekeeper is neighbored with another Gatekeeper or a Border Controller, the neighbor is placed in its own zone. This allows you to control the bandwidth used by calls to and from endpoints controlled by the other Gatekeeper. Sometimes you may place and receive calls to Gatekeepers you are not neighbored with (See section 3.9, URI Dialing). These Gatekeepers, and any unregistered endpoints reached by dialing their IP address, are placed in the Default Zone.

If bandwidth control is in use, there are two possible behaviors when a call cannot be placed at the bandwidth requested. By default the call will be connected at a reduced bandwidth (down-speeding), assuming that there is some bandwidth still available. Optionally the call may be rejected if it cannot be placed at the requested bandwidth. This option is controlled through the web interface of the Gatekeeper by navigating to *Gatekeeper Configuration* > *Gatekeeper* (for a screenshot of these settings, see Figure 8) or through the following command line instructions:

```
xConfiguration Gatekeeper Downspeed PerCall Mode: <On/Off>
xConfiguration Gatekeeper Downspeed Total Mode: <On/Off>
```

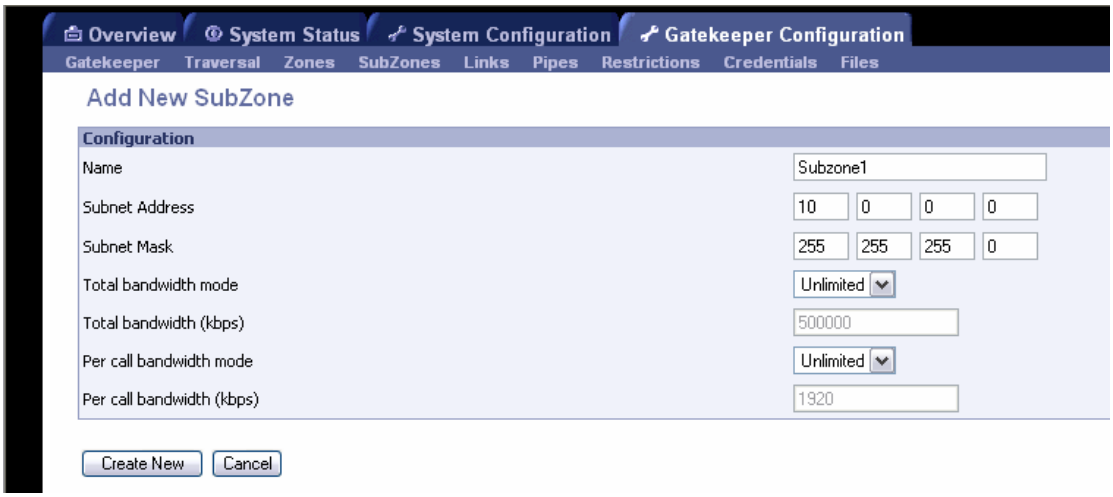


Figure 6 Configuration of a SubZone through the web interface

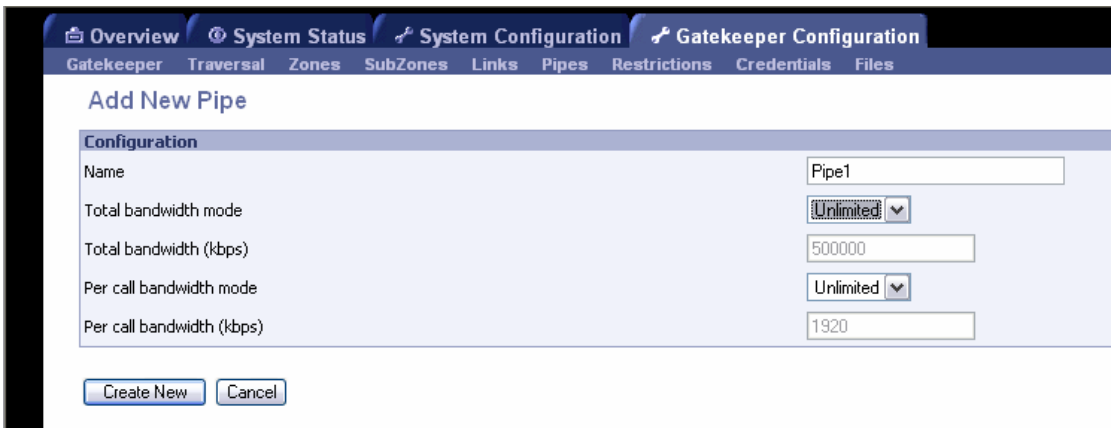


Figure 7 Adding a new Pipe through the web interface

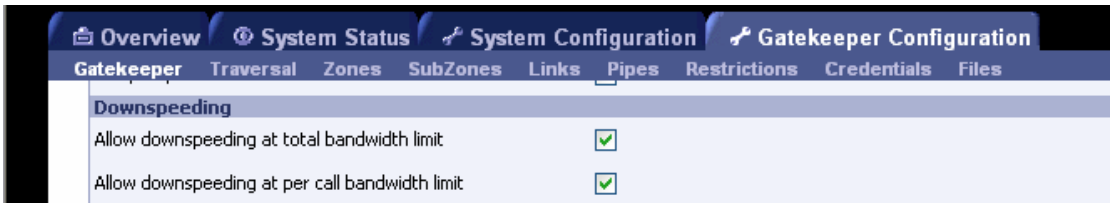


Figure 8 Configuring the downspeeding parameters of the Gatekeeper

3.6.1 Bandwidth Control and Firewall Traversal

When a Border Controller and Gatekeeper are being used to traverse a firewall, an additional zone and subzone come into use.

The traversal zone is used to represent the zone containing the Border Controller this Gatekeeper is paired with. This zone is automatically added for you. The traversal subzone represents the Gatekeeper itself. When an endpoint registers with the Gatekeeper and places a traversal call, its media will be routed through the Gatekeeper[1]. The traversal subzone allows you to control total and per call bandwidths passing through the Gatekeeper. Unlike other subzones, no endpoints will ever be registered in this subzone.

[1] TANDBERG MXP endpoints running F3 and later software can send their media directly to the Border Controller, depending on the setting of `xConfiguration Traversal Allow Media Direct`.

3.6.2 Bandwidth Control Examples

One possible configuration for the deployment in Figure 5 is shown in Figure 9. Each of the offices is represented as a separate subzone, with bandwidth configured according to local policy. The enterprise's leased line connection to the Internet, and the DSL connections to the remote offices, are modelled as separate pipes.

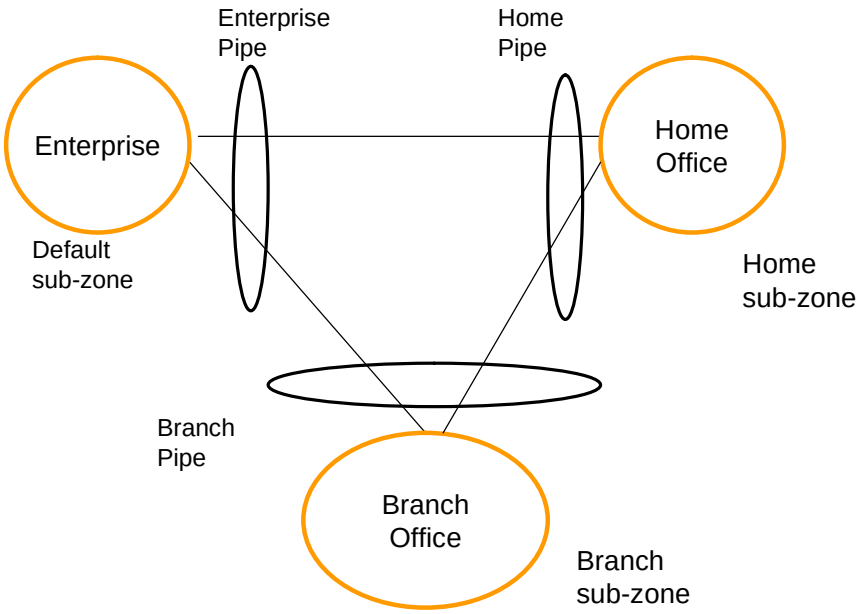


Figure 9 Bandwidth control example

There are no firewalls involved in the scenario shown in figure 1, so we can configure links between each of the offices. Each link is then assigned two pipes, representing the Internet connections of the offices at each end of the link. A call placed between the Home Office and Branch Office will consume bandwidth in the home and branch subzones and on the home and branch pipe. The enterprise's bandwidth budget will be unaffected by the call.

If we now modify our deployment to include firewalls between the offices, we can use the firewall traversal capability of the TANDBERG Gatekeeper and Border Controllers to maintain connectivity.

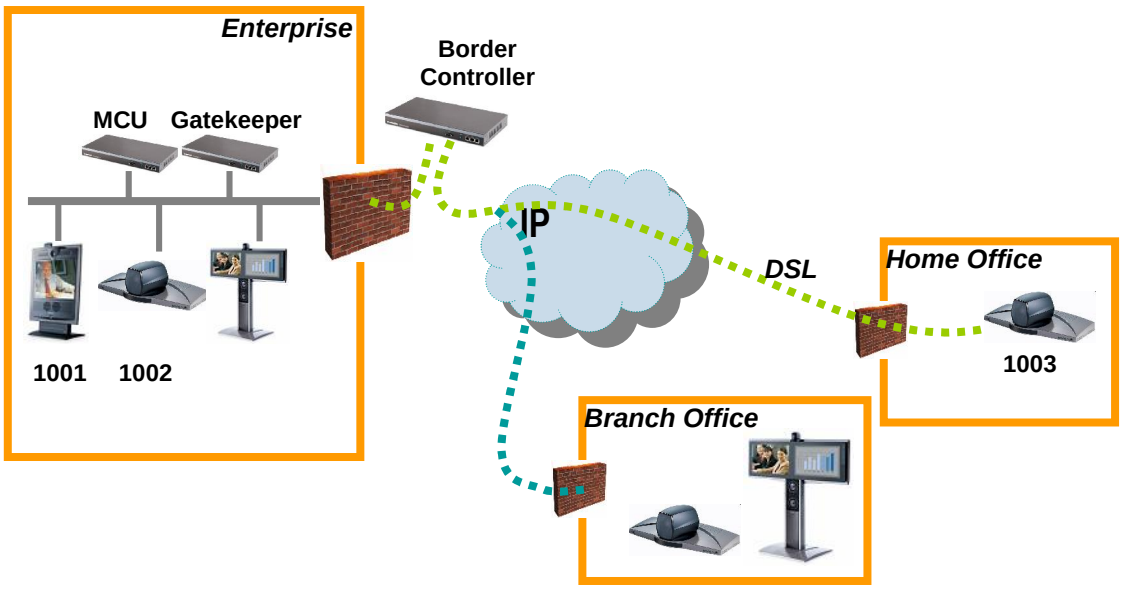


Figure 10 Network Deployment with firewalls

In Figure , the endpoints in the enterprise register with the Gatekeeper, whilst those in the branch and home office register with the Border Controller.

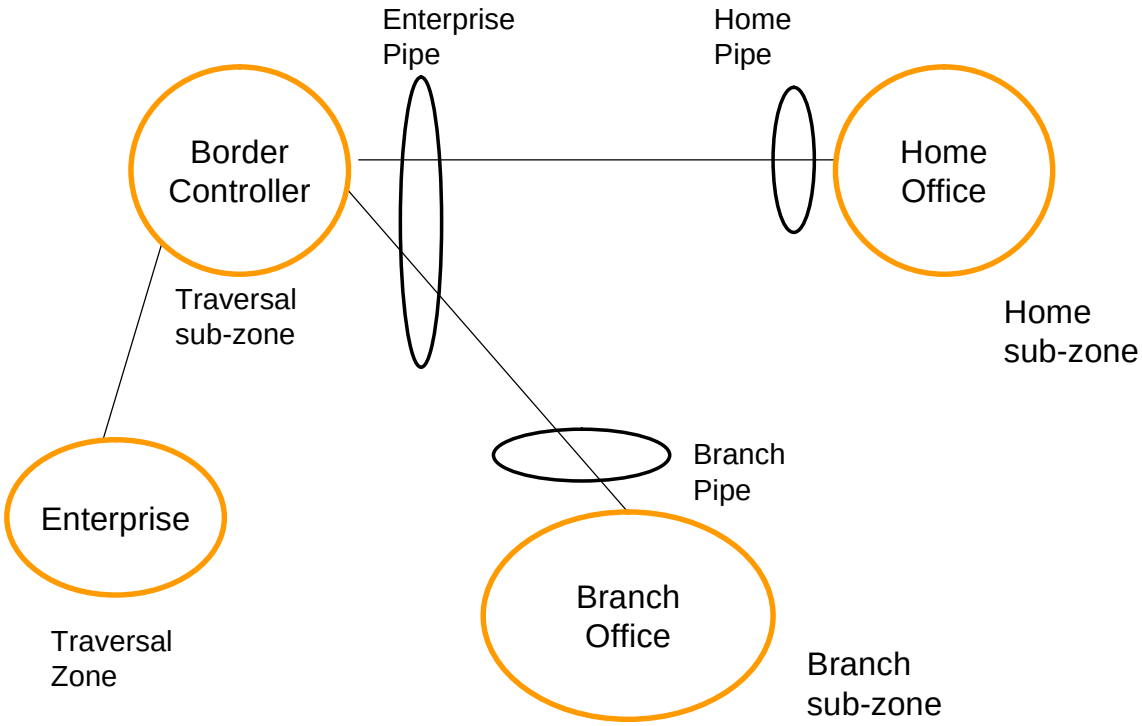


Figure 11 Border Controller example configuration

Figure 11 shows how the Border Controller could be configured for the deployment in Figure 10. The introduction of the firewalls means that there is no longer any direct connectivity between the Branch and Home offices. All traffic must be routed through the Border Controller. This is shown by the absence of a link between the Home and Branch subzones.

The Traversal Zone in Figure 11 represents the Enterprise Gatekeeper. The Border Controller will consume bandwidth from the Traversal Zone for all calls placed to endpoints managed by the Enterprise Gatekeeper. In this example we have assumed that there is no bottleneck on the link between the Border Controller and the Enterprise network, so have not placed a pipe on this link. If you want to limit the amount of traffic flowing through your firewall, you could provision a pipe on this link.

The traversal subzone in Figure 11 may be used to control the amount of traffic flowing through the Border Controller itself.

Because the Gatekeeper is only managing endpoints on the LAN, its configuration is simpler as shown in Figure 12.

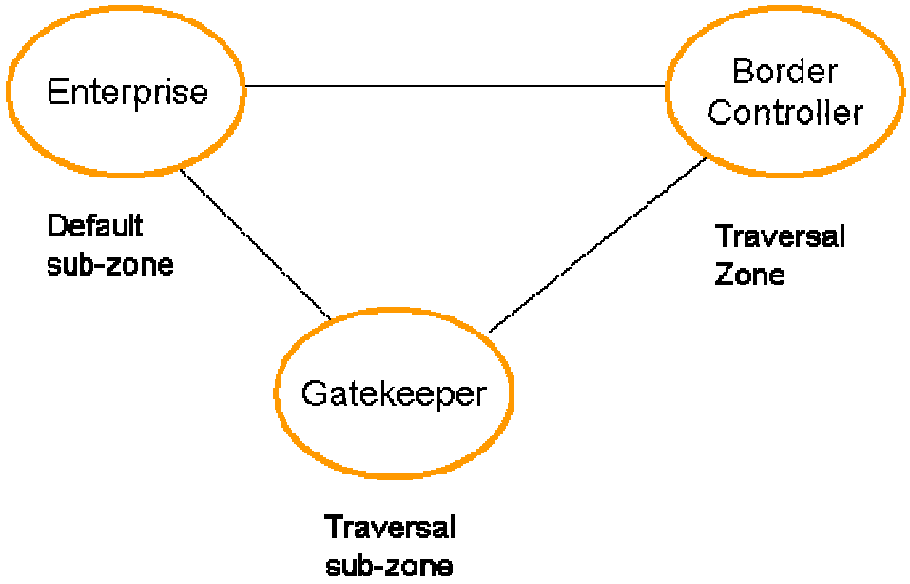


Figure 12 Gatekeeper example configuration

All of the endpoints in the enterprise will be assigned to the default subzone. The Traversal subzone controls traversal traffic flowing through the Gatekeeper, whilst the Traversal Zone controls all traffic traversing the enterprise firewall and passing on to the Border Controller. Both subzones and the Traversal zone are linked: the link between the default subzone and the Traversal zone is used by endpoints which can send media directly to the Border Controller. The other two links are used by endpoints using the Gatekeeper to traverse the firewall.

Both the Border Controller and Gatekeeper are shipped with Default and Traversal Zones and Default and Traversal subzones already configured. They are also preconfigured with the links between these zones to allow calls to be placed. You may delete or amend the default links if you need to model restrictions of your network. The default links may be restored by running the command

```
xCommand DefaultLinksAdd
```

3.7 Registration Control

The TANDBERG Gatekeeper can control which endpoints are allowed to register with it. Two separate mechanisms are provided: a simple Registration Restriction Policy and an authentication process based on user names and passwords. It is possible to use both mechanisms at once: authentication to verify an endpoint's identity from a corporate directory and registration restriction to control which of those authenticated endpoints may register with a particular Gatekeeper.

3.7.1 Registration Restriction Policy

When an endpoint registers with your Gatekeeper it presents a list of aliases. By default, registration restriction policy is set to None. In this state, any endpoint may register. The registration restriction policy can be configured using the following command:

```
xConfiguration Gatekeeper RegistrationRestrictionPolicy [None |
AllowList | DenyList ]
```

or by using the web interface, on the *Gatekeeper Configuration* > *Restrictions* page (see Figure 13 for a screenshot of the Registration Restrictions Configuration). If the policy is set to AllowList, only those endpoints with an alias which matches an entry in the AllowList may register. Conversely, if the policy is set to DenyList, all endpoints may register, unless they

match an entry on the DenyList. Allow lists and Deny lists are mutually exclusive: only one may be in use at any given time.

Matching uses a simple form of wild card expansion:

12345678	Exact match only
1234567?	First 7 characters are an exact match, last may be anything
123*	123 followed by anything
*@example.com	Any string ending with @example.com

To set entries in the Allow and Deny lists use the following commands

```
AllowListAdd, AllowListDelete, DenyListAdd, DenyListDelete
```

To view the entries in the allow and deny lists, use the following commands:

```
xConfiguration Gatekeeper Registration AllowList
xConfiguration Gatekeeper Registration DenyList
```

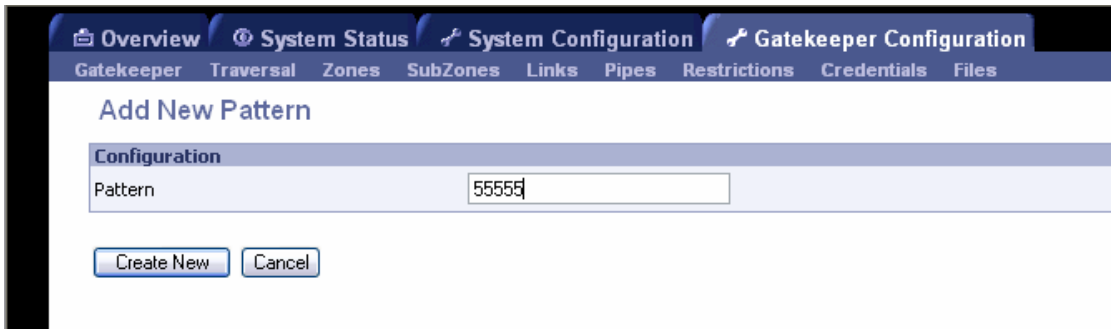


Figure 13 Configuring a pattern for the Allow/Deny List within the Registration Restrictions

3.7.2 Authentication

The TANDBERG Gatekeeper can use a user name and password based challenge-response scheme to permit registrations. For details of how to configure the Gatekeeper for authentication see section 3.8 H.235 Authentication. For details of how to configure your endpoint with the appropriate information, please consult your endpoint manual.

3.8 H.235 Authentication

The Gatekeeper supports the ITU H.235[2] specification for authenticating the identity of network devices with which the Gatekeeper communicates.

In order to verify the identity of a device, the Gatekeeper needs access to the password information. This credential information may be stored in a local database on the Gatekeeper or obtained from an LDAP Director Server.

3.8.1 Authentication using a local database

[2] ITU Specification: H.235 Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals

To configure the Gatekeeper to use the local database of credentials during authentication issue the following commands

```
xConfiguration Authentication Mode: On
xConfiguration Authentication Database: LocalDatabase
```

Each credential in the local database has a username and a password. To manage the credentials in the local database use the following commands

```
xcommand CredentialAdd <user name> <password>
xcommand CredentialDelete <credential index>
```

To show the credentials in the local database use the command

```
xConfiguration Authentication Credential
```

The credential database can also be configured via the web interface on the *Gatekeeper Configuration* > *Credentials* page(see Figure 14 for a screenshot of this configuration).

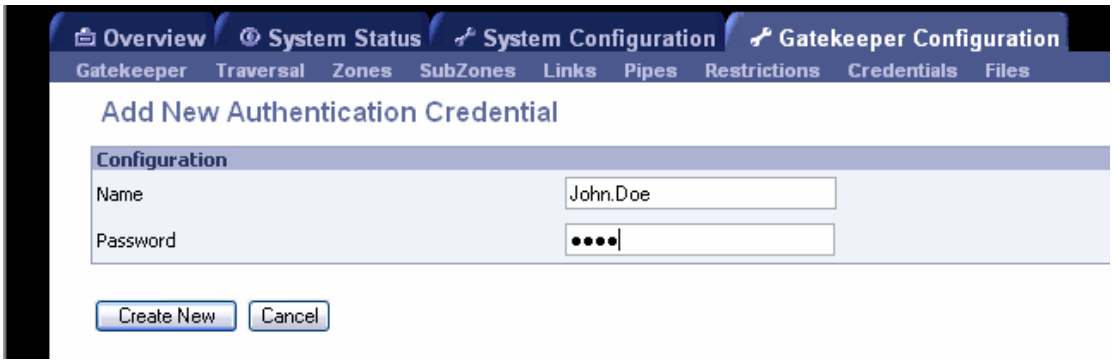


Figure 14 Adding Credentials to the local Gatekeeper database for H.235 Registrations

3.8.2 Authentication using an LDAP server

The authentication information can be obtained from an LDAP server. The directory on the LDAP server should be configured to implement the ITU H.350[3] specification to store H.235 credentials for devices that the Gatekeeper communicates with. The directory should also be configured with the H.323 aliases of endpoints that will register with the Gatekeeper.

For instructions on how to configure common third party LDAP servers, see the Appendix: Configuring LDAP Servers.

To configure the Gatekeeper to use the LDAP server directory during authentication issue the following commands

```
xConfiguration Authentication Mode: On
xConfiguration Authentication Database: LDAPDatabase
```

The Gatekeeper is required to be configured with the area of the directory which will be searched for the communication device information. This should be specified as the Distinguished Name (DN) in the directory under which the H.350 objects reside:

```
xConfiguration Authentication LDAP BaseDN: "Your base DN"
```

The Gatekeeper must also be configured with the location of the LDAP server and the security credentials required to gain access to the LDAP server. The following commands are used to configure the LDAP server details

```
xConfiguration LDAP Server Address: "ldap_server_ip"
xConfiguration LDAP Server Port: 389
```

[3] ITU Specification: H.350 Directory services architecture for multimedia conferencing

```
xConfiguration LDAP UserDN: "Your user DN"
xConfiguration LDAP Password: "password"
```

The status of the connection between the Gatekeeper and the LDAP server can be verified using the command

```
xstatus LDAP
```

The details of the LDAP server can also be configured via the web interface on the *Gatekeeper Configuration* > *Gatekeeper* page (see Figure 15 for the parameters configured to work with an LDAP server).

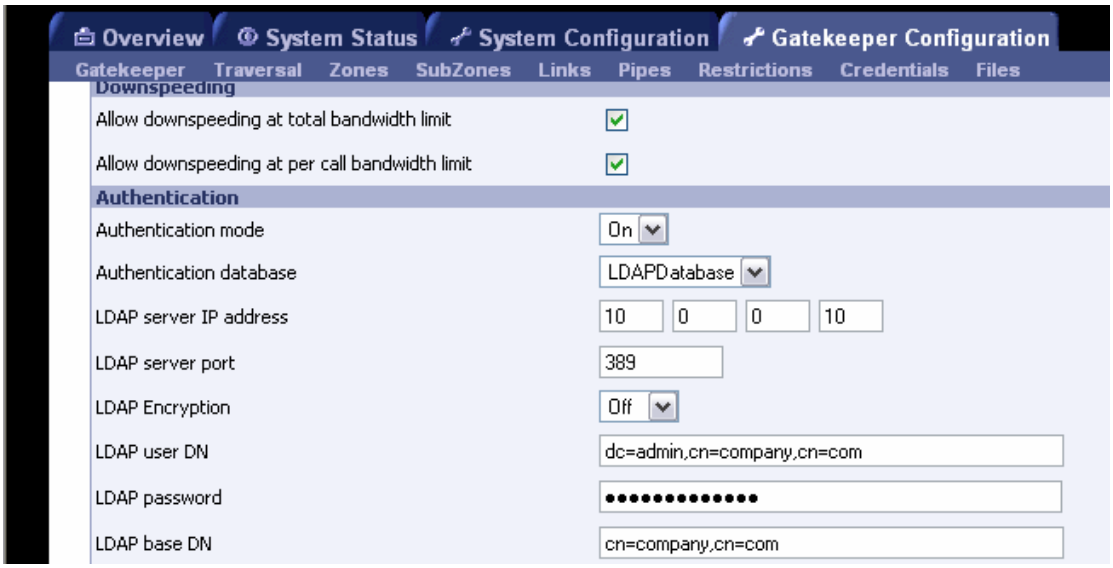


Figure 15 Configuring the Gatekeeper to authenticate with an LDAP server

Securing the LDAP connection with TLS

The traffic between the Gatekeeper and the LDAP server can be encrypted using Transport Layer Security (TLS). To use TLS, the LDAP server must have a valid certificate installed so that the Gatekeeper can verify the server's identity. For more information on setting up certificates using common LDAP servers, see the Appendix: Configuring LDAP Servers.

Using the terminal interface TLS can be enabled with the following command

```
xConfiguration LDAP Encryption: TLS
```

TLS can also be enabled via the web interface using the *Gatekeeper Configuration* > *Gatekeeper* page (see Figure 16 for the TLS LDAP Configuration).

The Gatekeeper will now only communicate with the LDAP server using TLS. To verify the identity of the LDAP server, the certificate of the Certificate Authority (CA) that issued the LDAP server with its certificate must be uploaded to the Gatekeeper. To install the CAs certificate, navigate to the *Gatekeeper Configuration* > *Files* page and upload the CA certificate as a Trusted CA certificate.

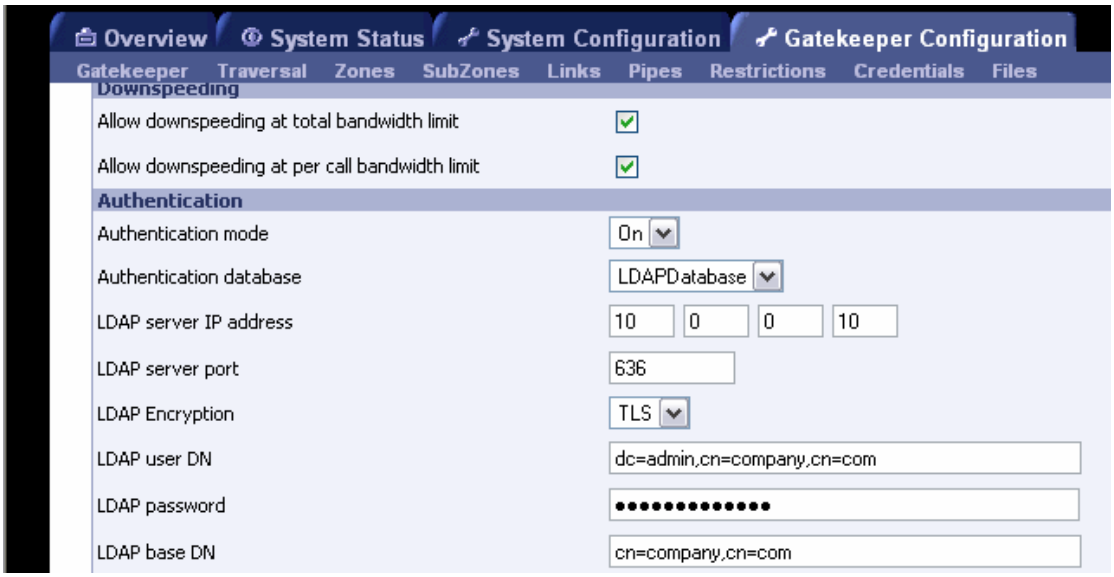


Figure 16 Configuring the Gatekeeper to authenticate with an LDAP server using TLS encryption

3.9 URI Dialing

If an alias is not located in the Gatekeeper's list of registrations, it may attempt to find an authoritative Gatekeeper through the DNS system.

URI dialing makes it easier for endpoints registered with different Gatekeepers to call each other. Without URI dialing, you need to neighbor all the Gatekeepers to each other. This does not scale well as the number of Gatekeepers grows. It is also inconvenient for making one off calls to endpoints registered with previously unknown Gatekeepers.

Using URI dialing, you call using an H.323 URI which looks like an email address. The destination Gatekeeper is found from the domain name – the part after the @ - in the same way that an email server is found.

The decision as to whether or not to do this is governed by the current state of

```
xConfiguration Gatekeeper DNSResolutionMode <On/Off>
```

You will also need to configure a DNS server for the systems to query. This is set using

```
xConfiguration DNS Server Address: <address>
```

or using the web interface on the *System Configuration* > *IP* page (see Figure 17 for the IP Configuration screen).

If you want others to be able to reach you using URI dialing, add a record to your DNS information as described in the Appendix: Configuring DNS Servers

Endpoints will typically register with the Gatekeeper without their domain name. The Gatekeeper needs to match a request for "fred@example.com" to a registration for "fred". To do this, it must be configured with the name of the domain in which its endpoints belong. This is set using

```
xConfiguration Gatekeeper LocalDomain DomainName: <name>
```

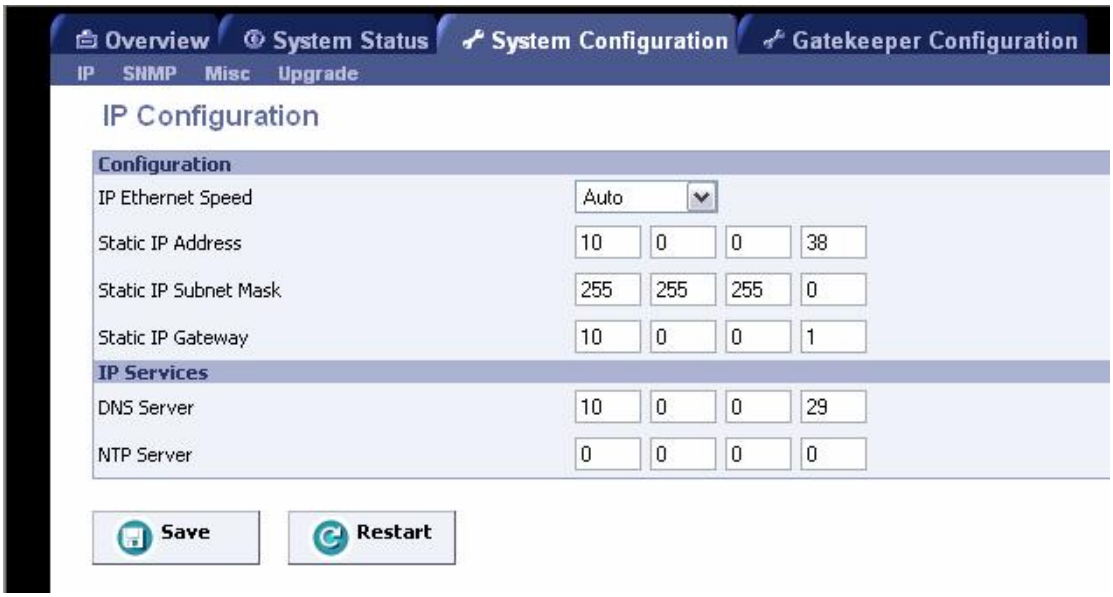


Figure 17 IP Configuration Screen

3.9.1 URI Dialing and firewall traversal

If URI dialing is being used in conjunction with firewall traversal, DNSResolutionMode should only be enabled on the Border Controller. The DNS records should be updated with the address of the Border Controller as the authoritative Gatekeeper for the enterprise. This ensures that calls placed using URI dialing enter and leave the enterprise through the Border Controller, allowing successful traversal of the firewall.

The LocalDomain DomainName should be set on both the Gatekeeper and the Border Controller. Any Alternates should also have the same LocalDomain Domain Name.

3.9.2 Creating DNS SRV records

URI dialing relies on the presence of SRV Record in the DNS information for the zone. The SRV record specifies the location of a server for a particular protocol and domain. Its format is defined by an Internet standard RFC 2782[4] as

```
_Service._Proto.Name TTL Class SRV Priority Weight Port Target
```

In our case `_Service` is defined by the H.323 protocol suite to be _h323ls and `_Proto` is `_udp`. Name corresponds to the host part of the H.323 URI.

How you add the SRV record depends on the type of DNS server you are using. Instructions for setting up two common DNS servers are given in Appendix: Configuring DNS Servers.

3.10 Firewall traversal

When used with a TANDBERG Border Controller, your Gatekeeper can assist you in making and receiving calls through firewalls and NAT devices.

Install the Gatekeeper on the private side of your firewall and the Border Controller on the public side.

[4] http://www.ietf.org/rfc/rfc2782.txt

To configure the Gatekeeper for firewall traversal, use the Web or console interface (see Figure 18 for this configuration screen on the web interface). You will need to set the IP address of the Border Controller

```
xConfiguration Traversal Server Address: <ip_address>
```

You will need to enter the name of your Gatekeeper onto the Border Controller. This name can be determined on the Gatekeeper with the command

```
xConfiguration System UnitName
```

and set on this on the Border Controller with the command

```
xConfiguration Traversal Client Name: <name>
```

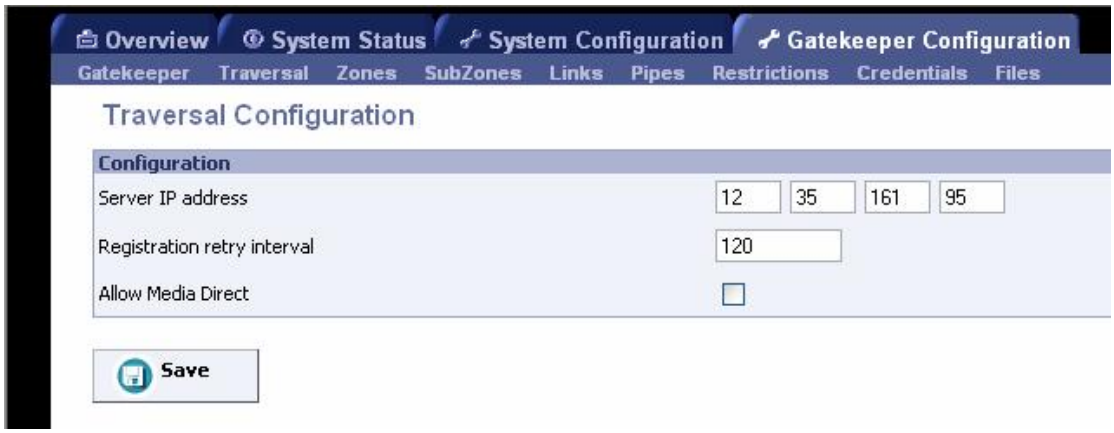


Figure 18 Traversal Configuration

3.10.1 Calling unregistered endpoints

If an endpoint is not registered with a Gatekeeper or Border Controller, calls may still be placed to it via the TANDBERG Gatekeeper. From your registered endpoint, enter the IP address of the endpoint you wish to call.

If a Border Controller and Gatekeeper are being used for firewall traversal, it is necessary to enter information that allows the Border Controller and Gatekeeper to determine which address space the destination endpoint is in. This is described in the Border Controller manual.

3.11 Call Policy

Your TANDBERG Gatekeeper allows you to set up policy to control which calls are allowed and even redirect selected calls to different destinations. You specify this policy by uploading a script written in the Call Processing Language (CPL) [5]. Each time a call is made the Gatekeeper executes the script to decide, based on the source and destination of the call, whether to

- Proxy the call to its original destination
- Redirect the call to a different destination
- Reject the call.

The CPL script is uploaded via the Web interface under the *Gatekeeper Configuration* > *Files* web page.

The execution of the CPL script is controlled by the setting

[5] http://www.ietf.org/rfc/rfc3880.txt

```
xConfiguration Gatekeeper Policy Mode <On/Off>
```

Policy interacts with authentication (section 3.7.2, Authentication). If authentication is enabled on the local Gatekeeper and a call received from a remote, unauthenticated Gatekeeper, the call's source aliases will be removed from the call request before it is passed to the policy engine. This is because the unauthenticated source aliases could be forged and so should not be used for policy decisions in a secure environment.

The following sections give details of the Gatekeeper's implementation of the CPL language and should be read on conjunction with the CPL standard (RFC 3880)[5].

3.11.1 Making Decisions Based on Addresses

address-switch

The address-switch node allows the script to run different actions based on the source or destination aliases of the call. The address-switch specifies which fields to match and then a list of address nodes contains the possible matches and their associated actions.

The supported attributes on an address-switch and their interpretation are as follows

field

"origin"	Match against the source aliases
"destination"	Match against the destination aliases
"original-destination"	Match against the destination aliases

If the selected field contains multiple aliases then the Gatekeeper will attempt to match each address node with all of the aliases before proceeding to the next address node i.e. an address node matches if it matches ANY alias.

subfield

The following table gives the definition of subfields for each alias type, if a subfield is not specified for the alias type being matched then the not-present action will be taken.

"address-type"	For all aliases types the address-type subfield is the string "h323"
"user"	For URI aliases this selects the username part. For H.323 ID's it is the entire ID and for E.164 numbers it is the entire number.
"host"	For URI aliases this selects the domain name part. If the alias is an IP address then this subfield is the complete address in dotted decimal form.
"port"	For IP addresses this is the port number in decimal.
"tel"	For E.164 numbers this selects the entire string of digits.
"alias-type"	Gives a string representation of the type of alias as follows

Alias Type	*Result*
URI	"url-ID"
H.323 ID	"h323-ID"
Dialed Digits	"dialedDigits"
IP Address	"transportID"

“display”	Not defined for any alias types

address

The address construct is used within an address-switch to specify addresses to match. Please note that all address comparisons ignore upper/lower case differences so <address is=“Fred”> will match “fred”, “freD” etc.

is=<string>	Selected field and subfield exactly match the given string.
contains=<string>	Selected field and subfield contain the given string. Note: The CPL standard only allows for this matching on the display subfield; however the Gatekeeper allows it on any type of field
subdomain-of=<string>	If the selected field is numeric (e.g. the “tel” subfield) then this matches as a prefix; so <address subdomain-of=”555”> matches “5556734” etc. If the field is not numeric then normal domain name matching is applied; so <address subdomain-of=”company.com”> matches nodeA.company.com etc.

otherwise

The otherwise node will be executed if the address specified in the address-switch was found but none of the preceding address nodes matched.

not-present

The not-present node is executed when the address specified in the address-switch was not present in the call setup message. This form is most useful when authentication is being used. With authentication enabled the gatekeeper will only use authenticated aliases when running policy so the not-present action can be used to take appropriate action when a call is received from an unauthenticated user (see example in section 3.11.4).

3.11.2 CPL Script Actions

location

As the CPL script runs it maintains a list of addresses (H.323 IDs, URLs and E.164 numbers) which will be used as the destination of the call if a proxy node is executed. The location node allows the location set to be modified so that calls can be redirected to different destinations.

At the start of script execution the location set is initialized to empty for incoming calls and to the original destination for outgoing calls.

The following attributes are supported on location nodes

Clear = "yes" | "no"	Specifies whether to clear the current location set before adding the new location. The default is to append this location to the end of the set.
url=<string>	The new location to be added to the location set. The given string can specify a URL (user@domain.com), H.323 ID or

an E.164 number.

proxy

On executing a proxy node the Gatekeeper will attempt to forward the call to the locations specified in the current location set. If multiple entries are in the location set then they are treated as different aliases for the same destination and are all placed in the destination alias field. If the current location set is empty the call will be forwarded to its original destination.

It is important to note that when a proxy node is executed script execution stops immediately i.e. there is currently no support for the proxy outputs “busy”, “noanswer” etc.

reject

If a reject node is executed the Gatekeeper stops any further script processing and rejects the current call.

3.11.3 Unsupported CPL Elements

The Gatekeeper does not currently support the following elements that are described in the CPL RFC. If an attempt is made to upload a script containing any of the following elements an error message will be generated and the Gatekeeper will continue to use its existing policy.

- time-switch
- string-switch
- language-switch
- time-switch
- priority-switch
- redirect
- mail
- log
- subaction
- lookup
- remove-location

3.11.4 CPL Examples

Call screening

Only allow calls from users with authenticated source addresses. See section 3.8 H.235 Authentication, for details on how to enable authentication.

```
<cpl>
  <incoming>
    <address-switch field=”origin”>
     <not-present>
        <reject/>
     </not-present>
    </address-switch>
  </incoming>
</cpl>
```

Selective Call Screening

User "fred" will not accept calls from anyone at "annoying.com", or from any unauthenticated users. All other users will allow any calls.

```
<cpl>
  <incoming>
    <address-switch field="destination">
      <address is="fred">
        <address-switch field="origin" subfield="host">
          <address subdomain-of="annoying.com">
            <reject/>
          </address>
          <otherwise>
            <proxy/>
          </otherwise>
          <not-present>
            <reject/>
          </not-present>
        </address-switch>
      </address>
    </address-switch>
  </incoming>
</cpl>
```

Call Redirection

Redirect all calls to user "barney" to voicemail.

```
<cpl>
  <incoming>
    <address-switch field="destination">
      <address is="barney">
         <location clear="yes" url="barney@voicemail">
           <proxy/>
         </location>
       </address>
       <otherwise>
         <proxy/>
       </otherwise>
     </address-switch>
   </incoming>
</cpl>
```

4 Software Upgrade

Software upgrade can be done in one of two ways:

- Using a web browser (HTTP/HTTPS).
- Using secure copy (SCP).

NOTE

To upgrade the Gatekeeper, a valid Release key and software file is required. Contact your TANDBERG representative for more information.

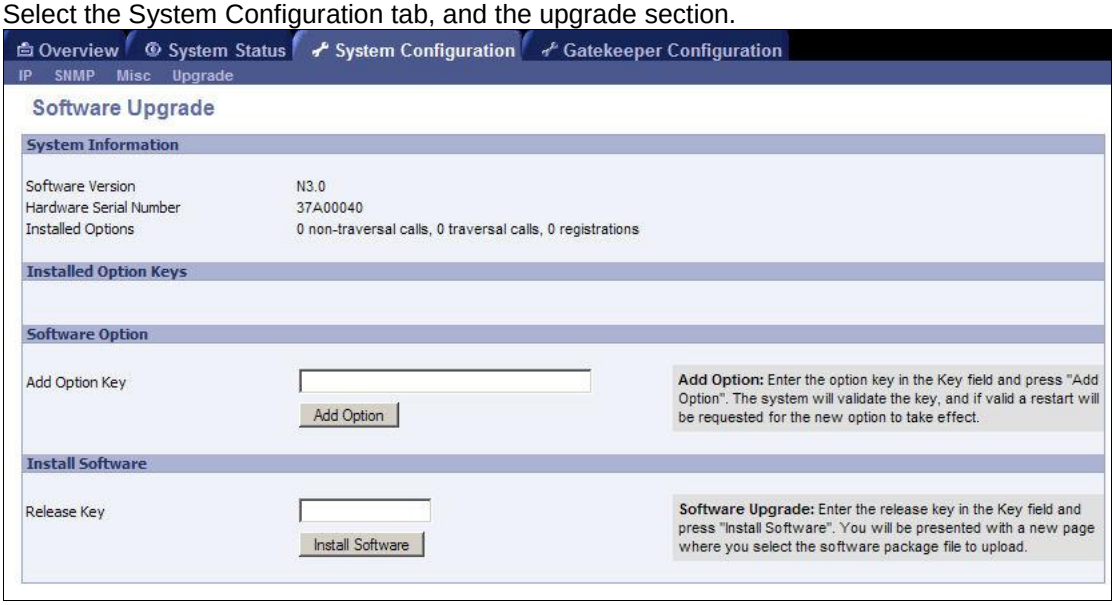
NOTE

Configuration is restored after performing an upgrade but we recommend that you make a backup of the existing configuration using the TANDBERG Management Suite before performing the upgrade.

4.1 Upgrading Using HTTP(S)

To upgrade using HTTP(S), do the following:

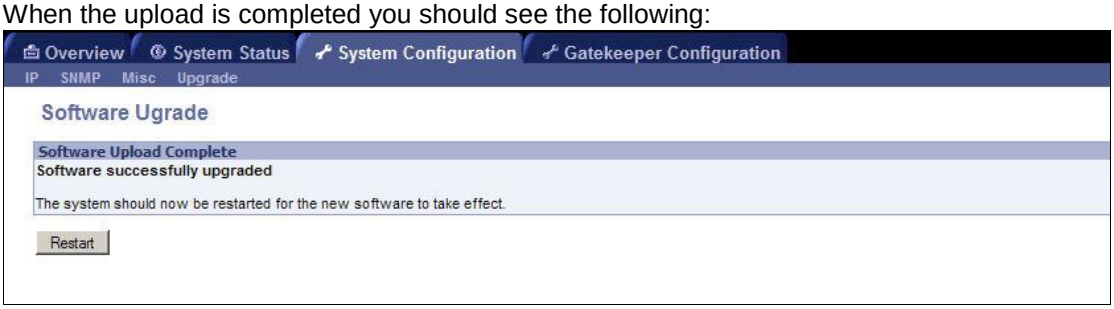
1. Point your browser at the IP address of the Gatekeeper. You will be prompted for your user name and password.
2. Enter admin as the user name and enter the password, then press OK.
3. Select the System Configuration tab, and the upgrade section.



4. Enter the release key and press Install Software. You will get a new screen where you can upload the software image:

5. Browse to the file containing the software and press Install. You should see a page indicating that upload is in progress:

6. When the upload is completed you should see the following:



7. Press Restart. You should see a confirmation window:

8. The software is installed. The system will then perform another reboot to restore system parameters. After 3-4 minutes, the Gatekeeper is ready for use.
9. If you are upgrading from an older version of the Gatekeeper, you will need to install new option keys on the *System Configuration* > *Upgrade* page.

4.2 Upgrading Using SCP

To upload using SCP you need an SCP program.

Using SCP you need to transfer two files to the Gatekeeper

- A text file containing the release key.
- A file containing the software image.

NOTE

Make sure you transfer the release key file before transferring the software image. Also make sure you name the files exactly as described below.

NOTE

The release key file should contain just the 16 character release key.

To upgrade using SCP, do the following:

1. Connect the supplied null-modem RS-232 cable from Data 1 to a PC running a terminal program to monitor the transfer. You can also use SSH to monitor the transfer.
2. Start the terminal program and configure it with baud rate 115200, 8 data bits, no parity, 1 stop bit and no flow control.
3. Make sure the system is turned on and available on IP.
4. Upload the release key file using scp to the /tmp folder on the system e.g.
   `scp release-key root@10.47.8.247:/tmp/release-key`
5. Enter password when prompted.
6. Copy the software image using SCP. The target name must be /tmp/tandberg-image.tar.gz, e.g.
   `scp s42000n10.tar.gz root@10.47.8.247:/tmp/tandberg-image.tar.gz`
7. Enter password when prompted.
8. Wait until the software has installed completely. This should not take more than 2 minutes.
9. Reboot the system.
10. After about four minutes the system will be ready to use.

5 Configuring the Gatekeeper

This chapter lists the basic usage of each command. The commands also support more advanced usage, which is outside the scope of this document.

5.1 Status

The status root command, xstatus, returns status information from the Gatekeeper.

To list all xstatus commands type

```
xstatus ?
```

To list all status information, type

```
xstatus
```

Command	*Usage*	*Description*
Calls	`xstatus Calls` `xstatus Calls Call <n>`	Returns a list of active calls on the system or information about a specific call.
Ethernet	`xstatus Ethernet MacAddress`	Reports the active configuration of the Ethernet interface. `MacAddress`: The MAC address of the LAN 1 interface. `Speed:` The speed of the Ethernet link. Reports Down if the link is down or not connected.
ExternalManager	`xstatus ExternalManager`	Returns the IP address, protocol and URL of the External Manager. The External Manager is the remote system (such as the Tandberg Management System (TMS)) used to manage the endpoints and network infrastructure.
Feedback	`xstatus Feedback` `xstatus Feedback <n>`	Returns all currently registered feedback expressions or the feedback expression at index n
IP	`xstatus IP`	Returns the active IP configuration of the system with IP address, subnet mask and gateway. Note that if you have changed the IP configuration without rebooting, xstatus IP will return the original settings currently in effect.
LDAP	`xstatus Ldap`	Reports the status of any connection to an LDAP server.
Links	`xstatus Links`	Reports call and bandwidth information for all links on the system.
Pipes	`xstatus Pipes`	Reports call and bandwidth information for all pipes on the system.
Registrations	`xstatus Registrations` `xstatus Registrations Registration <n>`	Returns a list of registered endpoints on the system or information about a specific registration.

Command	*Usage*	*Description*
ResourceUsage	`xstatus ResourceUsage`	Reports usage of system resources. `Registrations`: Number of currently registered endpoints. `MaxRegistrations`: Maximum number of registered endpoints since system start. `PortRegistrations`: Total number of currently registered endpoints and services. `MaxPortRegistratoins`. Maximum number of registered endpoints and services since system start. `TraversalCalls`: Number of currently active traversal calls. `MaxTraversalCalls`: Maximum number of traversal calls since system start. `TotalTraversalCalls`: Total number of traversal calls since system start. `NonTraversalCalls`: Number of currently active non traversal calls. `MaxNonTraversalCalls`: Maximum number of non traversal calls since system start. `TotalNonTraversalCalls`: Total number of non traversal calls since system start. `IntraZoneBandwidth`: Total bandwidth used intra zone. `InterZoneBandwidth`. Total bandwidth used to all neighboring zones.
SubZones	`xstatus SubZones`	Reports call and bandwidth information for all subzones on the system.
SystemUnit	`xstatus SystemUnit`	Reports information about the system • Product name • Uptime • Software version • Software name • Release date • Number of calls supported • Number of registered endpoints and services supported • Hardware serial number
`Traversal`	`xstatus Traversal`	Reports whether or not the Gatekeeper has registered with the Border Controller and established a traversal link.
`Zones`	`xstatus Zones`	Reports the call and bandwidth information for all zones on the system.

5.2 Configuration

The configuration root command, xconfiguration, is used to set configuration settings.

To list all xconfiguration commands type

```
xconfiguration ?
```

To list all configuration data, type

```
xconfiguration
```

To show a specific configuration value, type

```
xconfiguration <name>
```

To show usage information for a specific configuration value, type

```
xconfiguration <name> ?
```

To set a configuration element type

```
xconfiguration <name> <param1>: value1 <param2>: value2
```

There is also a shorthand for configuration element with several parameters:

```
xconfiguration <name> value1 value2
```

NOTE

Remember to use the colon after naming the parameters.

Configuration commands	***Description***
`xConfiguration Authentication Database: <LocalDatabase/LDAPDatabase>`	Selects between a local and remote LDAP repository of password information for authentication. Default is LocalDatabase.
`xConfiguration Authentication LDAP BaseDN: <S: 0, 255>`	The Distinguished Name to use when connecting to an LDAP server. Default is an empty string.
`xConfiguration Authentication Mode: <On/Off>`	Whether or not to use H.235 authentication of calls and registrations. Default is off.
`xConfiguration Authentication Credential [1..1000] Name: <username>`	Specifies the username of a credential in the authentication credential list
`xConfiguration Authentication Credential [1..1000] Password: <password>`	Specifies the password of a credential in the authentication credential list
`xConfiguration DNS Server Address:<IPAddr>`	Sets the IP address of the DNS server to be used when resolving domain names. You must restart the system for changes to take effect.
`xConfiguration Ethernet Speed: <Auto/10half/10full/100half/100full/>`	Sets the speed of the Ethernet link. Use auto to automatically configure the speed. To get the current speed, use the `xstatus Ethernet Speed` command. You must restart the system for changes to take effect.
`xConfiguration ExternalManager Address: <IPAddr>`	Sets the IP address of the External Manager. The External Manager is the remote system (such as the Tandberg Management System (TMS)) used to manage the endpoints and network infrastructure.
`xConfiguration ExternalManager Path: <path>`	Sets the path of the External Manager, e.g.: xConfiguration ExternalManager Path: "tms/public/external/management/SystemManagementService.asmx"

Configuration commands	*Description*
`xConfiguration Gatekeeper AlternateGK [1..5]: <IPAddr>`	List of Alternate Gatekeepers' IP addresses.
`xConfiguration Gatekeeper AutoDiscovery: <On/Off>`	Specifies if the Gatekeeper supports automatic registration of endpoints. The default is On.
`xConfiguration Gatekeeper CallsToUnknownIPAddresses: <Off/Direct/Indirect>`	Specifies whether or not the Gatekeeper will attempt to call systems which are not registered with any Gatekeeper. See Calling for further detail. The default is Indirect.
`xConfiguration Gatekeeper CallTimeToLive: <60..65534>`	Interval in seconds at which endpoints are polled to verify that they are still in a call. The default is 120 seconds.
`xConfiguration Gatekeeper DNSResolution Mode: <On/Off>`	Determines whether or not DNS lookup of H.323 URI's is enabled on this system.
`xConfiguration Gatekeeper Downspeed PerCall Mode: <On/Off>`	Determines whether or not the system will attempt to down-speed a call if there is insufficient per-call bandwidth configured to fulfill the request. The default is On.
`xConfiguration Gatekeeper Downspeed Total Mode: <On/Off>`	Determines whether or not the system will attempt to down-speed a call if there is insufficient total bandwidth available to fulfill the request. The default is On.
`xConfiguration Gatekeeper ForwardLocationRequests: <On/Off>`	Determines behavior on receipt of a location request from another Gatekeeper. If set to "On", if a location request cannot be resolved locally, it will be forwarded to neighbor Gatekeepers. The default is On.
`xConfiguration Gatekeeper LocalDomain DomainName`	Domain that the Gatekeeper is responsible for. Used when searching for matching endpoint registrations.
`xConfiguration Gatekeeper LocalPrefix: <prefix>`	Set the local zone prefix of the system.
`xConfiguration Gatekeeper Policy Mode: <On/Off>`	Determines whether or not the CPL policy engine is active. The default is On.
`xConfiguration Gatekeeper Registration AllowList [1..1000] Pattern: <pattern>`	Specifies a pattern in the registration allowed list
`xConfiguration Gatekeeper Registration DenyList [1..1000] Pattern: <pattern>`	Specifies a pattern in the registration denied list
`xConfiguration Gatekeeper Registration RestrictionPolicy: <None/AllowList/DenyList>`	Policy in use to determine who may register with the system. The default is None.
`xConfiguration Gatekeeper TimeToLive: <60..65534>`	The interval at which the system polls the endpoint to make sure it is still functioning. Specified in seconds. The default is 1800 seconds.
`xConfiguration HTTP Mode: <On/Off>`	Enables/disables HTTP support. You must restart the system for changes to take effect.

Configuration commands	*Description*
`xConfiguration HTTPS Mode: <On/Off>`	Enables/disables HTTPS support. Note that HTTP must also be enabled. You must restart the system for changes to take effect.
`xConfiguration IP Address: <IPAddr>`	Specify the IP address of the system. You must restart the system for changes to take effect.
`xConfiguration IP Gateway: <IPAddr>`	Specify the IP gateway of the system. You must restart the system for changes to take effect.
`xConfiguration IP SubnetMask: <IPAddr>`	Specify the IP subnet mask of the system. You must restart the system for changes to take effect.
`xConfiguration LDAP Encryption: <Off/TLS>`	Sets the encryption mode to be used on the connection to the LDAP server. The default is Off.
`xConfiguration LDAP Password: <password>`	Sets the password to be used when binding to the LDAP server.
`xConfiguration LDAP Server Address: <IPAddr>`	Sets the IP address of the LDAP server to be used when making LDAP queries.
`xConfiguration LDAP Server Port: <1..65534>`	Sets the IP port of the LDAP server to be used when making LDAP queries.
`xConfiguration LDAP UserDN: <userdn>`	Sets the user DN to be used when binding to the LDAP server.
`xConfiguration Links Link [1..100] Name: <linkname>`	Specifies the name of a link in the list of links.
`xConfiguration Links Link [1..100] Node1 Name: <nodename>`	Specifes the first node of a link. A node name may be either a Zone name or a SubZone name.
`xConfiguration Links Link [1..100] Node2 Name: <nodename>`	Specifes the second node of a link. A node name may be either a Zone name or a SubZone name.
`xConfiguration Links Link [1..100] Pipe1 Name: <pipename>`	First pipe associated with a link.
`xConfiguration Links Link [1..100] Pipe2 Name: <pipename>`	Second pipe associated with a link.
`xConfiguration Links TraversalLink Pipe1 Name: <pipename>`	First pipe associated with the traversal link.
`xConfiguration Links TraversalLink Pipe2 Name: <pipename>`	Second pipe associated with the traversal link.
`xConfiguration NTP Address: <IPAddr>`	Sets the IP address of the NTP server to be used when synchronizing system time.
`xConfiguration Option [1..64] Key: <optionkey>`	Specify the option key of your software options. The following command `xstatus system software configuration` can be used to query the existing options enabled. You must restart the system for changes to take effect.

Configuration commands	*Description*
`xConfiguration Pipes Pipe [1..100] Bandwidth Total Limit: <1..100000000>`	Bandwidth associated with a pipe, keyed by index.
`xConfiguration Pipes Pipe [1..100] Bandwidth Total Mode: <None/Limited/Unlimited>`	Whether or not a given pipe is enforcing total bandwidth restrictions. None corresponds to no bandwidth available.
`xConfiguration Pipes Pipe [1..100] Bandwidth PerCall Limit: <1..100000000>`	Per call bandwidth of a pipe.
`xConfiguration Pipes Pipe [1..100] Bandwidth PerCall Mode: <None/Limited/Unlimited>`	Whether or not a given pipe is enforcing per-call bandwidth restrictions. None corresponds to no bandwidth available.
`xConfiguration Pipes Pipe [1..100] Name: <pipename>`	Name for a pipe.
`xConfiguration SNMP CommunityName: <name>`	SNMP Community names are used to authenticate SNMP requests. SNMP requests must have this `password' in order to receive a response from the SNMP agent in the Gatekeeper. You must restart the system for changes to take effect.
`xConfiguration SNMP Mode: <On/Off>`	Turn on/off SNMP support. You must restart the system for changes to take effect.
`xConfiguration SNMP SystemContact: <name>`	Used to identify the system contact via SNMP tools such as TANDBERG Management Suite or HPOpenView. You must restart the system for changes to take effect.
`xConfiguration SNMP SystemLocation: <name>`	Used to identify the system location via SNMP tools such as TANDBERG Management Suite or HPOpenView. You must restart the system for changes to take effect.
`xConfiguration SSH Mode: <On/Off>`	Enables/disables SSH and SCP support. You must restart the system for changes to take effect.
`xConfiguration SubZones DefaultSubZone Bandwidth PerCall Limit: <1..100000000>`	Per call bandwidth of the default subzone.
`xConfiguration SubZones DefaultSubZone Bandwidth PerCall Mode: <None/Limited/Unlimited>`	Whether or not the default subzone is enforcing total bandwidth restrictions. None corresponds to no bandwidth available.
`xConfiguration SubZones DefaultSubZone Bandwidth Total Limit: <1..100000000>`	Total bandwidth available on the default subzone.
`xConfiguration SubZones DefaultSubZone Bandwidth Total Mode: <None/Limited/Unlimited>`	Whether or not the default subzone is enforcing per-call bandwidth restrictions. None corresponds to no bandwidth available.
`xConfiguration SubZones TraversalSubZone Bandwidth PerCall Limit: <1..100000000>`	Per-call bandwidth available on the traversal subzone.
`xConfiguration SubZones TraversalSubZone Bandwidth PerCall Mode: <None/Limited/Unlimited>`	Whether or not the traversal subzone is enforcing per-call bandwidth restrictions. None corresponds to no bandwidth available.
`xConfiguration SubZones TraversalSubZone Bandwidth Total Limit: <1..100000000>`	Total bandwidth available on the traversal subzone.

Configuration commands	*Description*
`xConfiguration SubZones TraversalSubZone Bandwidth Total Mode: <None/Limited/Unlimited>`	Whether or not the traversal subzone is enforcing total bandwidth restrictions. None corresponds to no bandwidth available.
`xConfiguration SubZones SubZone [1..100] Bandwidth PerCall Limit: <1..100000000>`	Per-call bandwidth available on the indexed subzone.
`xConfiguration SubZones SubZone [1..100] Bandwidth PerCall Mode: <None/Limited/Unlimited>`	Whether or not the indexed subzone is enforcing per-call bandwidth restrictions. None corresponds to no bandwidth available.
`xConfiguration SubZones SubZone [1..100] Bandwidth Total Limit: <1..100000000>`	Total bandwidth available on the indexed subzone.
`xConfiguration SubZones SubZone [1..100] Bandwidth Total Mode: <None/Limited/Unlimited>`	Whether or not the indexed subzone is enforcing total bandwidth restrictions. None corresponds to no bandwidth available.
`xConfiguration SubZones SubZone [1..100] Name: <subzonename>`	Name of the indexed subzone.
`xConfiguration SubZones SubZone [1..100] Subnet IP Address: <IPAddr>`	IP to match an endpoint which belongs in this subzone.
`xConfiguration SubZones SubZone [1..100] Subnet IP Mask: <IPAddr>`	Subnet mask to match endpoints which belong in this subzone.
`xConfiguration SystemUnit Name: <name>`	The name of the unit. Choose a name that uniquely identifies the system.
`xConfiguration SystemUnit Password: <password>`	Specify the password of the unit. The password is used to login with Telnet, HTTP(S), SSH, SCP, and on the serial port. To set an empty password type `xConfiguration SystemUnit Password: ""`
`xConfiguration Telnet Mode: <On/Off>`	Enables/disables Telnet support. You must restart the system for changes to take effect.
`xConfiguration Traversal AllowMediaDirect: <On/Off>`	Determines whether or not capable endpoints may send their media directly to the Border Controller, bypassing the Gatekeeper. The defaults is Off.
`xConfiguration Traversal Server Address: <IPAddr>`	IP address of the Border Controller that this Gatekeeper should connect to.
`xConfiguration Traversal Registration RetryInterval: <seconds>`	Frequency with which failed registrations with the Border Controller should be repeated. The default is 120 seconds.
`xConfiguration Zones DefaultZone Gatekeeper HopCount: <1..255>`	Maximum hop count to use when issuing LRQs to Gatekeepers in this zone. The default is 15 hops.
`xConfiguration Zones TraversalZone Gatekeeper HopCount: <1..255>`	Maximum hop count to use when issuing LRQs to Gatekeepers in this zone. The default is 15 hops.
`xConfiguration Zones Zone [1..100] Gatekeeper IP Address: <IPAddr>`	Specifes the IP address of neighbor gatekeeper.

Configuration commands	*Description*
`xConfiguration Zones Zone [1..100] Gatekeeper IP Port: <1..65534>`	Specifies the IP port of the neighbor gatekeeper
`xConfiguration Zones Zone [1..100] Gatekeeper HopCount: <1..255>`	Maximum hop count to use when issuing LRQs to Gatekeepers in this zone. The default is 15 hops.
`xConfiguration Zones Zone [1..100] Name: <zonename>`	Specifies the name of a zone in the zone list
`xConfiguration Zones Zone [1..100] Prefix Match: <prefix>`	Prefix to use for the indexed zone.
`xConfiguration Zones Zone [1..100] Prefix Mode: <Strip/Include>`	Whether or not to strip prefixes when forwarding an LRQ to the indexed zone. The default is Include.

5.3 Command

The command root command, xcommand, is used to execute commands on the Gatekeeper.

To list all xcommands type

```
xcommand ?
```

To get usage information for a specific command, type

```
xcommand <commandname> ?
```

Command	*Usage*	*Description*
AllowListAdd	`xCommand AllowListAdd <allowed_alias>`	Adds an entry to the allow list, used by the registration restriction policy.
AllowListDelete	`xCommand AllowListDelete <index>`	Removes the pattern from the allow list at the specified index.
Boot	`xCommand Boot`	Restarts (boots) the Gatekeeper. This takes approximately 1 minute to complete.
CheckBandwidth	`xCommand CheckBandwidth <node1> <node2> <bandwidth> <calltype>`	Diagnostic function for verifying bandwidth control. Node1, Node2 are the case sensitive names of the nodes, bandwidth the required bandwidth and calltype one of Traversal or NonTraversal.
CredentialAdd	`xCommand CredentialAdd: <username> <password>`	Adds the given username and password to the local authentication database.
CredentialDelete	`xCommand CredentialDelete: <index>`	Deletes the indexed credential.
DefaultLinksAdd	`xCommand DefaultLinksAdd`	Restores the factory default links for bandwidth control.
DefaultValuesSet	`xCommand DefaultValuesSet Level: <level>`	Resets system parameters to default values. Level 1 will reset most parameters, except networking related ones. Level 2 and 3 reset progressively more parameters.

Command	*Usage*	*Description*
DenyListAdd	`xCommand DenyListAdd <denied_alias>`	Add an entry to the deny list, used by the registration restriction policy.
DenyListDelete	`xCommand DenyListDelete <index>`	Removes the pattern from the deny list at the specified index.
DisconnectCall	`xCommand DisconnectCall <callid>`	Disconnects the specified call.
FeedbackRegister	`xCommand FeedbackRegister` `<ID> <URL> <Expression>`	Registers for notifications on the event or status change described by the Expression to be sent in XML format to the specified URL. Up to 15 Expressions may be registered for each of 3 feedback IDs. The following Expressions are valid: Event, Event/CallAttempt, Event/Connected, Event/Disconnected, Event/ConnectionFailure, Event/Registration, Event/Unregistration, Event/Bandwidth, Status, Status/Calls, Status/Registrations, History, History/Calls, History/Registrations E.g.: xCommand FeedbackRegister ID:1 URL:http://10.1.1.1/SystemManagementService.asmx Expression:Event/CallAttempt,Status/Registration
FeedbackDeregister	`xCommand FeedbackDeregister <ID>`	Deregisters the specified Feedback Expression. All registered Feedback Expressions are removed with: xCommand FeedbackDeregister 0
LinkAdd	`xCommand LinkAdd: <linkname> <node1> <node2> <pipe1> <pipe2>`	Adds a new link to the link list.
LinkDelete	`xCommand LinkDelete: <index>`	Deletes the indexed link.
OptionKeyAdd	`xCommand OptionKeyAdd: <key>`	Adds a new option key.
OptionKeyDelete	`xCommand OptionKeyDelete: <index>`	Deletes the indexed option key.
PipeAdd	`xCommand PipeAdd: <name> <totalmode> <total> <percallmode> <percall>`	Adds and configures a new pipe.
PipeDelete	`xCommand PipeDelete: <index>`	Deletes the indexed pipe.
Remove Registration	`xCommand RemoveRegistration <regid>`	Removes the specified registration.
SubZoneAdd	`xCommand SubZoneAdd: <name> <address> <mask> <totalmode> <total> <percallmode> <percall>`	Adds and configures a new subzone.

Command	*Usage*	*Description*
SubZoneDelete	`xCommand SubZoneDelete: <index>`	Deletes the indexed subzone.

ZoneAdd	`xCommand ZoneAdd <name> <address> <prefix>`	Adds a new zone with the specified name, zone prefix and IP address. E.g.
		`xCommand ZoneAdd B 65 10.0.0.30`
		`Note: the parameter order to this command has changed from N1 software.`

ZoneDelete	`xCommand ZoneDelete <index>`	Removes the zone with the specified index. E.g. `xCommand ZoneDelete 5`

5.4 History

The history root command, xhistory, is used to display history data on the Gatekeeper.

To list all xhistory commands type

```
xhistory ?
```

To list all history data, type

```
xhistory
```

To show a specific set of history data, type

```
xhistory <name>
```

History commands	*Description*
`xhistory calls` `xhistory calls call <n>`	Displays history data for up to the last 255 calls handled by the Gatekeeper. Call entries are added to the Call History on call completion. Call histories are listed in reverse chronological order of completion time.
`xhistory registrations` `xhistory registrations registration <n>`	Displays history data for up to the last 255 registrations handled by the Gatekeeper. Registration entries are added to the Registration History on unregistration of H.323 entities. Registration histories are listed in reverse chronological order of unregistration time.

5.5 Feedback

The feedback root command, xfeedback, is used to control notifications of Events and Status changes on the Gatekeeper.

A Feedback Expression describes an interesting event or change in status. When a Feedback Expression is registered, a notification will be displayed in the shell for each occurrence of the event described by that Expression. Notifications will continue to be displayed for a given event until the Expression is deregistered.

To list all xfeedback commands type

```
xfeedback ?
```

To list all currently active feedback expressions, type

```
xfeedback list
```

To register a feedback expression, type

```
xfeedback register <expression>
```

To deregister the feedback expression with index <n>, type

```
xfeedback deregister <n>
```

To deregister all feedback expressions, type

```
xfeedback deregister 0
```

Feedback commands	*Description*
`xFeedback Register Status/<Calls/Registrations>`	Registers for feedback on changes in the chosen Status, e.g.: xFeedback Register Status/Calls To register for all Status changes, use: xFeedback Register Status
`xFeedback Register History/<Calls/Registrations>`	Registers for feedback on History, e.g.: xFeedback Register History/Calls To register for all History, use: xFeedback Register History
`xFeeedback Register Event/<CallAttempt/ Connected/ Disconnected/ ConnectionFailure/ Registration/ Unregistration/ Bandwidth>`	Registers for feedback on the occurrence of the chosen Event, e.g.: xFeedback Register Event/CallAttempt To register for all available Events, use: xFeedback Register Event

5.6 Other commands

Command	*Usage*	*Description*
About	`about`	Shows information about the system.
clear	`clear [eventlog/history]`	Clears the event log or history of all calls and registrations.
eventlog	`eventlog [n/all] [level]`	Lists the eventlog with trace information. n is the number of lines from end of event log to dump all – dumps the whole event log level – sets the level of detail to dump (fatal, error, warning, info, detail). Defaults to error level if not present. If no parameters are provided, the whole event log will be dumped.

Command	*Usage*	*Description*
relkey	`Relkey`	Displays the release key that this software has been installed with.
syslog	`syslog <level> [ipaddr] [ipaddr] ...`	Enables tracing. <level> - is the log level, 0-3, 3 gives most logging. ipaddr – specify up to 10 IP addresses to log information for, all if none specified. Type syslog 0 to turn off logging.

6 Appendix: Configuring DNS Servers

In the examples below, we set up an SRV record to handle H.323 URIs of the form user@example.com. These are handled by the Gatekeeper with the fully qualified domain name of Gatekeeper1.example.com which is listening on port 1719, the default registration port.

It is assumed that an A record already exists for Gatekeeper1.example.com. If not, you will need to add one.

6.1 Microsoft DNS Server

It is possible to add the SRV record using either the command line or the MMC snap in. To use the command line: on the DNS server open a command window and enter

```
dnscmd . /RecordAdd domain service_name SRV service_data
```

Where *domain* is the domain into which you wish to insert the record, *service_name* the name of the service you're adding and *service_data* the priority, weight, port and server providing the service as defined by RFC 2782. For example:

```
dnscmd . /RecordAdd example.com _h323ls._udp SRV \
1 0 1719 gatekeeper1.example.com
```

6.2 BIND 8 & 9

BIND is a commonly used DNS server on UNIX and Linux systems. Configuration is based around two sets of text files: named.conf which describes which zones are represented by the server and a selection of zone files which describe the detail of each zone.

BIND is sometimes run chrooted for increased security. This gives the program a new root directory, which means that the configuration files may not appear where you expect them to be. To see if this is the case on your system, run

```
ps aux | grep ^named
```

This will give the command line that named (the BIND server) was invoked with. If there is a –t option, then the path following that is the new root directory and your files will be located relative to that root.

In `/etc/named.conf` look for a `directory` entry within the `options` section. This will give the directory in which the zone files are stored, possibly relative to a new root directory. In the appropriate `zone` section, a `file` entry will give the name of the file containing the zone details.

1. Edit the appropriate zone file for the domain `example.com`
2. Add an entry:

   ```
   _h323ls._udp SRV 1 0 1719 gatekeeper1
   ```

   Be careful not to end either service or target with a period (.) as this will prevent BIND adding the domain to the end of the partial name.
3. Reload the configuration files. To do this find the process id (pid) for named
   `ps aux | grep ^named`

then instruct named to reload the files
`kill –s SIGHUP pid`

4. Check the log files for any discrepancies
`tail /var/log/messages`

For more details of how to configure BIND servers and the DNS system in general see the book “DNS and BIND”[6].

6.3 Verifying the SRV record

There are a range of tools available to investigate DNS records. One commonly found on Microsoft Windows and UNIX platforms is nslookup. Use this to verify that everything is working as expected.

```
nslookup –querytype=srv  _h323ls._udp.example.com
```

and check the output.

[6] “DNS and BIND, Fourth Edition” Albitz and Liu, O’Reilly and Associates, ISBN: 0-596-00158-4

7 Appendix: Configuring LDAP Servers

7.1 Microsoft Active Directory

7.1.1 Prerequisites

These comprehensive step by step instructions assume that Active Directory is installed. For details on installing Active Directory please consult your Windows documentation. The following instructions are for Windows Server 2003 Enterprise Edition, if you are not using this version of Windows, your instructions may vary.

The following ITU specification describes the schemas which are required to be installed on the Active Directory server:

- H.350 – Directory services architecture for multimedia conferencing - An LDAP schema to represent endpoints on the network.
- H.350.1 – Directory services architecture for H.323 – An LDAP schema to represent H.323 endpoints.
- H.350.2 – Directory services architecture for H.235 - An LDAP schema to represent H.235 elements.

The schemas can be downloaded in ldif format from the web interface on the Gatekeeper. To do this, navigate to the *Gatekeeper Configuration* > *Files* page and click on the links for the schemas. Copy the downloaded schemas to the Active Directory server.

Open a command prompt and for each file execute the following command:

```
ldifde -i -c DC=X <ldap_base> -f filename.ldf
```

Where `<ldap base>` is the base DN for your Active Directory server.

7.1.2 Adding H.350 objects

Create the organizational hierarchy

Open up the Active Directory Users and Computers MMC snap-in. Under your base DN right click and select New > Organizational Unit. Create an Organizational unit called h350.

NOTE

It is good practice to keep the H.350 directory in its own organizational unit to separate out H.350 objects from other types of objects. This allows access controls to be setup which only allow the Gatekeeper read access to the BaseDN and therefore limit access to other sections of the directory.

Add the H.350 objects

Create an ldif file with the following contents:

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,dc=my-domain,dc=com
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
```

```
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
```

Add the ldif file to the server using the command:

```
ldifde -i -c DC=X <ldap_base> -f filename.ldf
```

This will add a single H.323 endpoint with an H.323 Id alias of “MeetingRoom1” and an E.164 alias of “626262”. The entry also has H.235 credentials of id “meetingroom1” and password “mypassword” which are used during authentication.

7.1.3 Securing with TLS

To enable Active Directory to use TLS, you must request and install a certificate on the Active Directory server. The certificate must meet the following requirements:

- Be located in the Local Computer's Personal certificate store. This can be seen using the Certificates MMC snap in.
- Have the private details on how to obtain a key associated for use with it stored locally. When viewing the certificate you should see a message saying “You have a private key that corresponds to this certificate”.
- Have a private key that does *not* have strong private key protection enabled. This is an attribute that can be added to a key request.
- The Enhanced Key Usage extension includes the Server Authentication object identifier, again this forms part of the key request.
- Issued by a CA that both the domain controller and the client trust.
- Include the Active Directory fully qualified domain name of the domain controller in the common name in the subject field and/or the DNS entry in the subject alternative name extension.

7.2 OpenLDAP

7.2.1 Prerequisites

These instructions assume that an OpenLDAP server has already been installed. For details on installing OpenLDAP see the documentation at http://www.openldap.org.

The following examples use a standard OpenLDAP installation on the Linux platform. For installations on other platforms the location of the OpenLDAP configuration files may be different. See the OpenLDAP installation documentation for details.

7.2.2 Installing the H.350 schemas

The following ITU specification describes the schemas which are required to be installed on the LDAP server:

- H.350 – Directory services architecture for multimedia conferencing - An LDAP schema to represent endpoints on the network.
- H.350.1 – Directory services architecture for H.323 – An LDAP schema to represent H.323 endpoints.

- H.350.2 – Directory services architecture for H.235 - An LDAP schema to represent H.235 elements.

The schemas can be downloaded in ldif format from the web interface on the Gatekeeper. To do this, navigate to the *Gatekeeper Configuration* > *Files* page and click on the links for the schemas.

Copy the downloaded schemas to the OpenLDAP schema directory:

/etc/openldap/schemas/commobject.ldif

/etc/openldap/schemas/h323identity.ldif

/etc/openldap/schemas/h235identity.ldif

Edit /etc/openldap/slapd.conf to add the new schemas. You will need to add the following lines:

```
include /etc/openldap/schemas/commobject.ldif
include /etc/openldap/schemas/h323identity.ldif
include /etc/openldap/schemas/h235identity.ldif
```

The OpenLDAP daemon (slapd) must be restarted for the new schemas to take effect.

7.2.3 Adding H.350 objects

Create the organizational hierarchy

Create an ldif file with the following contents:

```
# This example creates a single organisational unit to contain
# the H.350 objects
dn: ou=h350,dc=my-domain,dc=com
objectClass: organizationalUnit
ou: h350
```

Add the ldif file to the server using the command:

slapadd -l <ldif_file>

This organizational unit will form the BaseDN to which the Gatekeeper will issue searches. In this example the BaseDN will be “ou=h350,dc=my-domain,dc=com”.

NOTE

It is good practice to keep the H.350 directory in its own organizational unit to separate out H.350 objects from other types of objects. This allows access controls to be setup which only allow the Gatekeeper read access to the BaseDN and therefore limit access to other sections of the directory.

Add the H.350 objects

Create an ldif file with the following contents:

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,dc=my-domain,dc=com
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
```

```
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
```

Add the ldif file to the server using the command:

slapadd -l <ldif_file>

This will add a single H.323 endpoint with an H.323 Id alias of “MeetingRoom1” and an E.164 alias of “626262”. The entry also has H.235 credentials of id “meetingroom1” and password “mypassword” which are used during authentication.

7.2.4 Securing with TLS

The connection to the LDAP server can be encrypted by enabling Transport Level Security (TLS) on the connection. To do this you must create an X.509 certificate for the LDAP server to allow the Gatekeeper to verify the server’s identity. Once the certificate has been created you will need to install the following three files associated with the certificate onto the LDAP server:

- The certificate for the LDAP server.
- The private key for the LDAP server.
- The certificate of the Certificate Authority (CA) that was used to sign the LDAP server’s certificate.

All three files should be in PEM file format.

The LDAP server must be configured to use the certificate. To do this, edit /etc/openldap/slapd.conf and add the following three lines:

```
TLSCACertificateFile <path to CA certificate>
TLSCertificateFile <path to LDAP server certificate>
TLSCertificateKeyFile <path to LDAP private key>
```

The OpenLDAP daemon (slapd) must be restarted for the TLS settings to take effect.

For more details on configuring OpenLDAP to use TLS consult the OpenLDAP Administrator’s Guide.

To configure the Gatekeeper to use TLS on the connection to the LDAP server you must upload the CA’s certificate as a trusted CA certificate. To do this, navigate to the *Gatekeeper Configuration* > *Files* page and upload the certificate.

8 Approvals

The product has been approved by various international approval agencies, among others: UL and Nemko. According to their Follow-Up Inspection Scheme, these agencies also perform production inspections at a regular basis, for all production of TANDBERG's equipment.

The test reports and certificates issued for the product show that the TANDBERG Gatekeeper, Type number TTC2-02, complies with the following standards.

EMC Emission - Radiated Electromagnetic Interference

- EN55022:1994 + A1:1995 + A2:1997 Class A.
- FCC Rules and Regulations 47CFR, Part 2, Part 15.
- CISPR PUB.22 Class A

EMC Immunity

- EN 55024:1998 + A1:2001
- EN 61000-3-2:2000
- EN 61000-3-3:1995 + A1:2001

Electrical Safety

- IEC 60950 3rd edition 1999
- EN 60950 3rd edition 2000
- UL 60950 3. Edition
- CSA C22.2 No. 950-M95

9 Technical Specifications

System Capacity
100-1000 registered endpoints
25-200 concurrent calls

0-100 traversal calls
100 zones
(The system's capacity depends on the system's option key)

Ethernet Interfaces
3 x LAN/Ethernet (RJ-45) 10/100 Base-TX
(2 disabled)

System console port
2 x COM ports (front and rear), RS-232 DB-9 connector
2 x USB (disabled)

ITU standard
ITU-T H.323 version 4 including Annex O

Security Features
IP Administration passwords
Management via SSH and HTTPS
Software upgrade via HTTPS and SCP

System Management
Configuration via serial connection, Telnet, SSH, HTTP, HTTPS
Software upgraded via HTTP, HTTPS and SCP

Environmental Data
Operation temperature: 0^{o}C to 35^{o}C (32^{o}F to 95^{o}F)
Relative humidity: 10% to 90% non-condensing

Physical Dimensions
Height: 4.35 cm (1.72 inches)
Width: 42.6 cm (16.8 inches)
Depth: 22.86 cm (9 inches)
1U rack mounted chassis

Power supply
90 ~ 264V full range @47 ~ 63 Hz

Certification
LVD 73/23/EC
EMC 89/366/ECC

10 Index