Communications Networks, Content and Technology
European Commission Directorate General

DG CONNECT

European Union's FP7 Programme
DG Connect

Directorate C: Excellence in Science
Unit C1: e-Infrastructure

elcira
Europe Latin America Collaborative e-Infrastructure for Research Activities

D3.3 Guidelines for exchange points and GDS architecture for an integrated HQVCS between Latin America and Europe

A project of the Seventh Framework Programme (FP7)

This project is funded by the European Commission

A project implemented by RedCLARA

Periodical Progress Report

ELCIRA Deliverable: Guidelines for exchange points and GDS architecture for an integrated HQVCS between LA and EU

Document Full Name	**D3.3 Guidelines for exchange points and GDS architecture for an integrated HQVCS between Latin America and Europe**
Date	**2014-01-24**
Activity	**3.3. Guidelines for exchange points and GDS architecture for an integrated HQVCS between LA and EU**
Lead Partner	**RENATA**
Document status	**Final**
Classification Attribute	**Public**
Document link	

Abstract: The present document aims to be a solution plan for an integrated High Quality Video Conference Service (HQVCS) that will be implemented in every institution needing the benefits of this service. The guide provide the steps for integrating to the HQVCS service.

A project of the Seventh Framework Programme (FP7)

This project is funded by the European Commission

A project implemented by RedCLARA

A project of the Seventh Framework Programme (FP7)

This project is funded by the European Commission

A project implemented by RedCLARA

DELIVERABLE ROUTE

	Name	Member/Activity	Date	Responsible
From	Hernan Garcia	RENATA	27-10-2013	RENATA
Revised by	Gustavo Garcia	RedCLARA	13-11-2013	RENATA
Revised by	Hernan Garcia	RENATA	28-11-2013	RENATA
Revised by	Gustavo García	RedCLARA	8-1-2014	RENATA
Revised by	Thomas Fryer	DANTE	21-01-14	RENATA
Revised by	Gustavo García	RedCLARA	27-1-2014	RENATA
Approved by	Florencio Utreras	RedCLARA	27-01-2014	RENATA

TABLE OF CONTENTS

1. GLOSSARY

RAS	Registration, Admission and Status
H.323	Set of protocols for audio-visual communication
MCU	Multipoint Control Unit
DNS	Domain Name System
GDS	Global Dialling Scheme
HQVCS	High Quality Video-conference Service
NREN	Network Research and Education Network
PSTN	Public Switched Telephone Network

2. INTRODUCTION

The ELCIRA Project aims to provide collaboration tools and services over high-speed research and education networks to European and Latin American research institutions. Work Package 3 (WP3) of ELCIRA project is intended to implement a High Quality Videoconference Service (HQVCS) built collaboratively between the National Research and Education Networks (NRENs) and institutions of different countries in Europe and Latin America.

Many academic institutions worldwide have videoconference equipment, and use it harnessing research and education networks. Nevertheless, many of these elements do not work under a common service scheme, adding complexity to a service that should very easy and intuitive. Service elements such as dialling procedures, directory information, quality assurance and service support could be standardised and improved for a high quality intercontinental service.

This document will provide information about this HQVCS and how to integrate an NREN or institution into this network, and thus improve the ability of videoconferencing equipment to stay connected with a large list of organisations around the world, in a similar fashion to using the conventional telephone service.

3. HOW TO READ THIS DOCUMENT

This document aims to assist NREN administrators in setting up videoconference networks. Due to differing levels of experience and development, the document is designed in sections that can be read independently, so that a specific reader can select the part that is useful to him or her. In general terms, the reading recommendation is:

Admin experience level	Recommended reading
None or low	Read full document, including concept chapter
Medium (Use VC equipment regularly, know VC network concepts, but no gatekeeper or VC network in place)	Start at 4.3
Medium to high	Start at chapter 5. Chapters 1 to 4 for quick reference.

4. INTRODUCTION TO VIDEOCONFERENCE SERVICE NETWORKS

A videoconference network will provide communications at regional, national and international level establishing connections between two or more endpoints or videoconference equipment. For videoconferences between more than two endpoints, special elements as a Multipoint Control Unit (MCU) will be required. Usually, videoconference networks also have other infrastructure elements including gatekeepers, DNS systems, gateways, reservations systems and switches. For instance, a network element called the Gatekeeper is a call routing and control system that can direct calls to a destination endpoint using IP addresses or a dialling number. All networks are not the same, and the proper videoconference network implementation will depend on the size of the network in terms of endpoints or users to be catered for.

The project service will also implement features such as a Booking Service to allow users to schedule virtual meetings, the ability to stream videoconferences over the Internet, increase the number of meeting assistants to record sessions.

The HQVCS counts with a Certification Assurance Room Programme that will rate rooms for providing having relevant statistics (e.g. bandwidth), lighting, technical contacts and so on.

A Directory Service also is available for consulting a large list of numbers for calls to different institutions belonging to the network.

4.1. VIDEO NETWORK BENEFITS

Today organisations and universities around the world demand communication mechanisms and invest in videoconferencing equipment. Sometimes, using the equipment requires expertise in information technologies. This service aims to provide ease of use in videoconferencing over high speed networks in a similar fashion to the conventional telephone service.

The HQVCS network will make it possible to reduce costs, e.g. travel costs, for organisations who use this system. The videoconferencing network will close the gap between researchers in different countries, increasing the sharing of knowledge through virtual meetings.

The videoconference service will improve research in areas such as telemedicine and cultural collaboration, e.g. allowing musical events and developments to be shared. This service is commonly used for presentations, conferences and meetings providing more efficiency of management teams and teleworking.

4.2. H.323 STANDARD

The H.323 standard is a set of protocols with well-defined functions to establish communication between two or more exchange points. This standard can be used to transfer video, sound and data over a packet network.

H.323 is one of three main standards for videoconference communications. These are SIP, H.323 and MGCP. H.323 is chosen as it is very stable and reliable.

Figure 1 shows the **H.323 Protocol Stack** in three main columns.

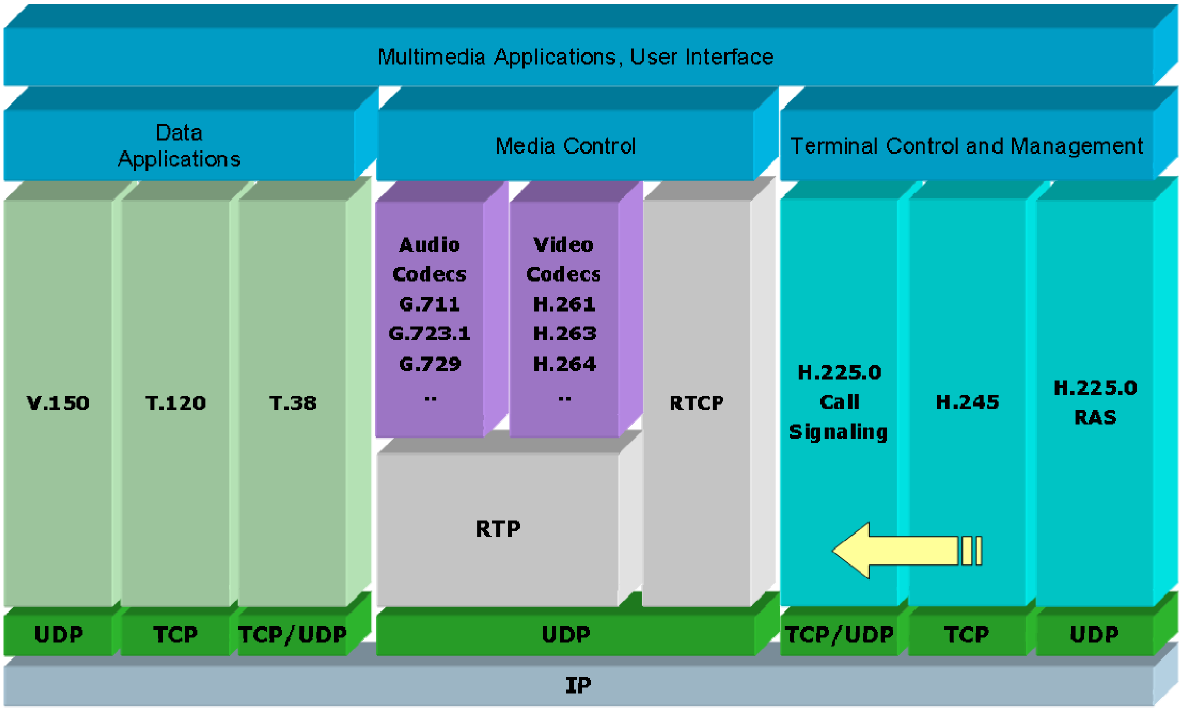

Figure 1: H.323 Protocol Stack
(Source: http://en.wikipedia.org/wiki/H.323)

The following table describes the protocols which make up the H323 stack. The description itself provides an overview of the protocol function. More detailed information can be found by searching the protocol name on the Internet.

Terminal Control and Management Protocols	
H.225	This protocol is used for call signalling and information about the call, i.e. it provides features including phone ringing, status of the call, call setup (handshake negotiation), call disengagement, etc.
H.245	Mainly used to negotiate call features such as video and audio codification, transmission bandwidth and endpoint information exchange. In some cases calls cannot be established if feature negotiation fails for codec reasons, e.g. if the codec is not supported for both endpoints even when the call setup by protocol H.225 succeeds.
H.225 RAS	RAS is for Registration, Admission and Status, this protocol consists of a series of messages for communication between endpoints and GK. These messages are commands and appends request, confirmation and reject commands, e.g.:

RAS Message	RAS Acronym

<table>
<tr><td></td><td><table><tr><td>Admission Request</td><td>ARQ</td></tr><tr><td>Admission Confirm</td><td>ACF</td></tr><tr><td>Admission Reject</td><td>ARJ</td></tr></table>
A full list of messages can be found at:
http://www.itu.int/rec/T-REC-H.225.0/en</td></tr>
<tr><td colspan="2">Media Control</td></tr>
<tr><td>Codecs</td><td>These are the different codecs supported for the endpoint. These include the H.261, H.263, and H.264 codec family, etc., depending on the brand and model of the endpoint. A codec is a format and a mechanism to encode and decode video and audio in data format.</td></tr>
<tr><td>RTP</td><td>Real-time Transfer Protocol (RTP) is a protocol adopted by the H.323 standard for audio and video data transmission with a minimum delay enabling high definition for videoconferencing communications.</td></tr>
<tr><td>RTCP</td><td>Real-time Transfer Control Protocol (RTCP) is a protocol used to collect statistics on the service including successful calls, current calls, bandwidth used, and rate of packet loss. This information can be useful for future improvements to the videoconference service.</td></tr>
<tr><td colspan="2">Data Applications</td></tr>
<tr><td colspan="2">Different applications can transfer more than audio and video. Application-sharing is supported by this series of protocols. Text data or other types of information can also be transferred during the call, an example of this could be blackboard-sharing (e.g. as with Microsoft NetMeeting).</td></tr>
</table>

A project of the Seventh Framework Programme (FP7)

This project is funded by the European Commission

A project implemented by RedCLARA

Call establishment process using a Gatekeeper intermediation

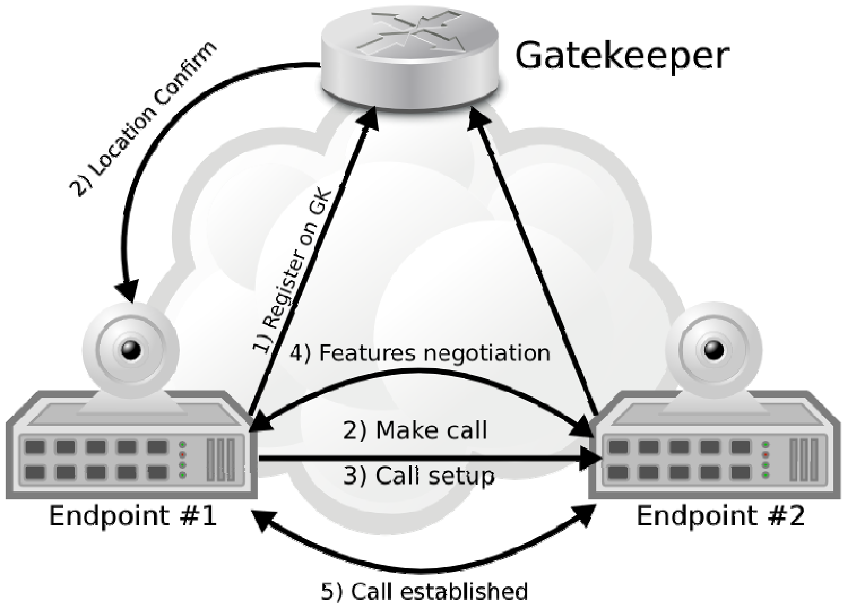

Figure 2: Call establishing process

1) The first step in the call process is that each end point automatically registers itself on a configured GK. This process is done using the H.225 RAS protocol: the endpoint sends a message called Registration Request (RRQ) and the GK will accept with Registration Confirm (RCF) or will deny with Registration Reject (RRJ).

2) The second step is to dial from one endpoint the number of the endpoint that the caller wishes to connect to. This will send an H.225 RAS message called Admission Request (ARQ) to the GK. If both endpoints are registered on the same GK, it will respond with an Admission Confirm (ACF) message that contains the information of the destination endpoint such as the IP address and other data, and the call will proceed. If they are registered on different GKs within the HQVCS network the first GK will send a Location Request (LRQ) message to its neighbours, If a neighbour GK contains an entry of the dialled number, it will respond with a Location Confirm (LCF)

message but if the entry cannot be found, each neighbouring GK will respond with a Location Reject (LRJ) message and the GK will respond with an Admission Reject (ARJ) message to the source endpoint.

3) When the first endpoint has all contact information about the destination endpoint, H.225 protocol begins interacting. This protocol is in charge of making both endpoints ring and setting up the call (handshake negotiation). With this protocol, the endpoints will inform the GK of the status of the call at all moments, including when the call is in process or if the call has ended.

4) At the precise moment when the call is answered both endpoints will setup features of the call (codecs supported, bandwidth and other features) with H.245 protocol messages.

5) Video and audio is transferred during the call using Real-time Transfer Protocol (RTP) and monitored with a protocol called Real-time Transfer Control Protocol (RTCP).

4.3. VIDEO NETWORK ELEMENTS

This section explains the different elements that are involved in a videoconference network.

- Endpoints or Exchange point

  The main user interface equipment that supports the H.323 protocol set and/or SIP. This element could be a software client or advanced equipment with a high definition camera and microphone. The endpoint can negotiate a call with other endpoints, register and make calls using a gatekeeper network, encode and decode audio and video signals, transfer data such PowerPoint presentations. Modern endpoints have advanced echo cancellation features and high definition to improve call quality.

Example:

Figure 3: Videoconference Equipment (Endpoint)

(Source: http://www.conferencetech.com/polycom)

- Multipoint Control Unit (MCU)

  The Multi-point Control Unit (MCU) is a videoconference control, switching, encoding, decoding and trans-coding element that allows the establishment of multiple user conferences. When three or more users setup a connection to an MCU, they connect to a virtual room where video is shared and transferred among participants. The MCU handles the video layout distribution, controls the bandwidth, sets auto-responses, translates different coding, and manages access, among other functions.

  Example:

Figure 4: Multipoint Control Unit (MCU)

(Source: http://www.polycom.com)

- Gatekeeper

  This is an element to provide a large-scale communication service making it possible to route calls in accordance with number prefix rules and routing policies. More information can be found in Section 3.3.1.

- Gateway

  Is an element that allows data to be sent over a different packet network that does not involve H.323 packets; a Gateway can transfer information over a Public Switched Telephone Network (PSTN).

4.3.1. THE GATEKEEPER

A Gatekeeper (GK) is an element proper of the H.323 standard which enhances features for videoconference communications with improvements including address translation, call routing and call control, thus providing scalability and decentralized management.

GKs are separate elements from endpoints. Whilst they are optional for videoconferencing communications, they are a mandatory element when building a videoconferencing network. There are proprietary implementations of this element such as the Cisco Gatekeeper Cisco Multimedia Conference Manager (CMCM) or an open-source Gatekeeper such as GNU GK can be implemented.

Another feature is zone management that consists of a collection of elements connected and managed by the GK which provides services over a sub-network enabling self-management for videoconferencing communications.

This element is usually described by its functions and it is highly recommended for large videoconference networks. If a network includes two or three endpoints, it is better to use direct calling.

These are principal features which the Gatekeeper provides:

1) Address translation
2) Admission Control

3) Zone Management
4) Call Control Signalling
5) Call Authorisation
6) Bandwidth control
7) Statistics-handling
8) Call Management
9) Bandwidth Management

5. BUILDING A HIGH QUALITY VIDEO CONFERENCE SERVICE (HQVCS)

In order to provide services and useful tools to Latin American and European organisations and researchers, the ELCIRA Project intends to build a HQVCS using the Gatekeeper hierarchy infrastructure as in shown at Figure 5.

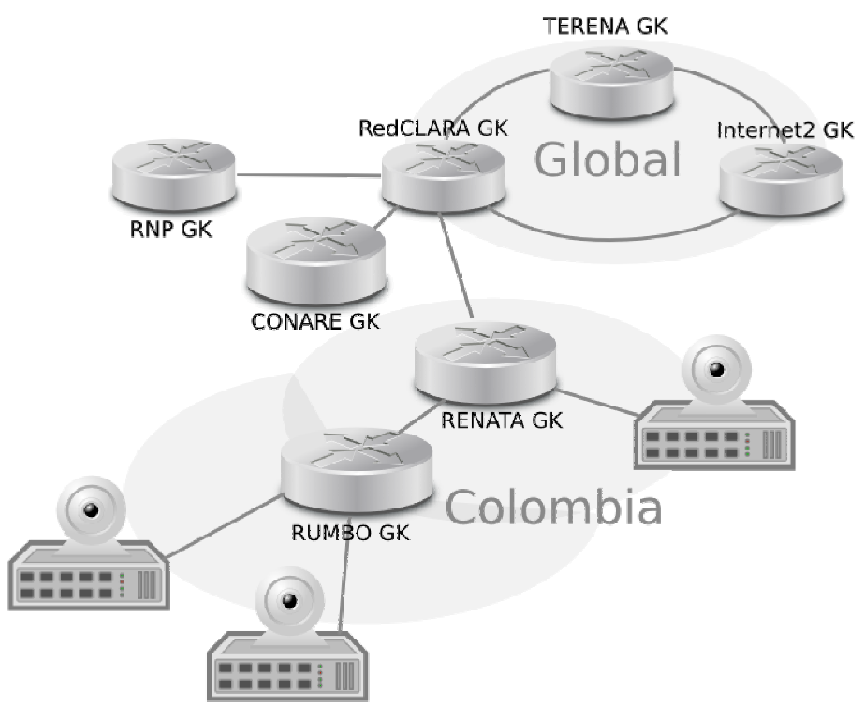

Figure 5: HQVCS Gatekeeper Infrastructure

NRENs will implement a GK to maintain connections at the national level between endpoints in the same country. Other regional organisations may implement a GK solution to provide a fine zone management but the NREN GK must be configured properly as a neighbour in order to provide an appropriate infrastructure for call routing using number prefixes in accordance with the corresponding numbering plan.

This section provides a step-by-step overview in how to setup a videoconference network and integrate it into the HQVCS initiative. This practical guide aims to provide an overview of the main concepts, and facilitate quick deployment of a videoconference network connected to the global research and education community using the HQVCS model.

5.1. DEFINE A DIALLING PLAN

As is commonly known, videoconference calls are commonly set up with IP address dialling. With this service the aim is to provide a videoconferencing service similar to the conventional telephone service with numbered dialling. Whilst each exchange point can set its own number within its configuration settings (known as Virtual Numbering), this can lead to difficulties including number collision and complicated rules for call routing using prefixes. Thus it is recommended to use the E.164 ITU recommendation to assign numbers to endpoints that belong to the large HQVCS network. This is known as the Global Dialling Scheme (GDS) that refers to a numbering plan to assign numbers according to existing country numbering codes.

A dial plan is a set of numbering rules that can be applied to video network elements. In order to have successful calls using numbers, each endpoint, and MCU virtual room will have a globally unique number. THE GLOBAL DIALLING SCHEME (abbreviated as GDS) defines a convention for assigning numbers to videoconferencing equipment. It is based on an ITU-T (ITU - Telecommunication Standardization Sector) recommendation called E.164 that defines a numbering format adopted around the world in telecommunication networks.

E.164 FORMAT: <IC><CC><ZP><EN>, Where:

IC International Code
CC Country Code
ZP Zone Prefix
EN Ending Number

Numbering in H.323 networks is usually described as either virtual or real. Virtual numbers are defined by the NREN, and will not be requested to the telecommunications regulation authorities. The above means that the video network will be always separated from public telephones network (PSTN). Real numbers have several advantages as future integration into telephone networks or public providers will be easier. Disadvantages include that in some countries; regulators only provide numbers to Telecom providers or have high charges. The integration to the NRENnum.net requires real numbers. This matter will be dealt with in section 5.4.

The ELCIRA HQVCS team strongly recommends the use of real numbers. The NREN will request a numbering range from their telecommunications regulation authority. Nevertheless, taking into account that this procedure can take some time or can have some restrictions, virtual numbering can be used. In order to start using GDS with virtual numbers, the ELCIRA HQVCS service recommends using the number 01 as the zone prefix.

For instance, if institution A is located in Colombia (57), the city of Bogota (1), and the local number is 5302604, the full GDS number would be:

00 57 1 01 5302604

This allows the institution to separate the virtual numbering, and avoid overlaps with real numbering. The zone 01 is recommended as it is not used in most Latin American countries. The following section describes how to install a Gatekeeper using the GNU software. The Gatekeeper will handle registrations and manage call routing using the dial plan defined in this section.

5.2. GNU GATEKEEPER

What is GNU Gatekeeper (also known as GNU GK)?

"*The GNU Gatekeeper is an open-source project that implements a H.323 gatekeeper. A gatekeeper provides call control services to H.323 endpoints and is an integral part of most telephony or video conferencing installations that are based on the H.323 standard.*" (Willamowius, 2013)

It is an efficient and cheap alternative to obtaining a Gatekeeper service for an extensible communication service for Voice over IP (VoIP) or Videoconferencing systems. Called "The Open Gatekeeper" it is an efficient cross-platform tool developed by Jan Willamowius under GPL License.

The official project site is: http://www.gnugk.org.

5.2.1. INSTALLING THE GNU GK

Installation requires a server able to be accessed by research and education networks. If possible connections behind a NAT should be avoided for the sake of simplicity, otherwise other advanced configurations will be required.

Server Requirements

RAM	1 GB
Hard Disk	50 GB
CPU	2 GHz
OS	Linux Debian

NOTE: Verify your firewall accepts TCP connections (1719) and UDP connections (1720) over those specific ports.

The GNU Gatekeeper installation is usually very simple. On Debian-based Linux operating systems it can be installed from repositories using the distribution package manager with the "**`install`**" option.

```
$: apt-get install gnugk
```

After this GNU GK will be installed and ready for use. It should then be configured for a specific behaviour.

For advanced installation on other Linux distributions, UNIX systems and Windows systems binaries may be downloaded from the GNU Gatekeeper official website (http://www.gnugk.org/h323download.html).

Download and extract the content of zip file. This folder contains the following directory structure:

bin/	Executables
contrib/	Contributions for extend features
docs/	Documentation of gnugk
etc/	Configuration example files
initd/	Scripts for starting gnugk as a daemon

Table 1: GNUGk Directory Structure

Copy the **gnugk** executable to the system binaries folder.

```
$: cp /path/to/bin/gnugk /usr/sbin
```

Or create a symbolic link:

```
$: cd /usr/sbin
$: ln –sf /path/to/bin/gnugk
```

NOTE: It is very important to make the **gnugk** executable accessible as **/us/sbin/gnugk**

5.2.2. CONFIGURING GNU GK

This part of the process can prove to be challenging. It is recommended a specific use design is created before implementing the service that should ease this process.

The configuration process relies on editing a specific file that should be located with the following path: **/etc/gatekeeper.ini**. The content of this file must be structured in blocks called “Sections” with specific attributes (very human-readable).

To avoid creating this file from scratch it is possible to use an example configuration file located inside GNU GK directory on the **etc/** directory.

As you can see inside this text file the configuration follows this format:

```
[Section Name]
Attribute=Value
```

NOTE: If an attribute has not been specified, the default value will be adopted.

Lines with a hash **(#)** or a semicolon **(;)** at the beginning are comments.
Below is an explanation of some of the principal configurations that must be considered when building a HQVCS. For Sections brackets **`([])`** are used and for attributes an equal sign **`(=)`** is appended to show the required value.

Gatekeeper Main Configuration

Global configurations of the GK will remain in the **`[Gatekeeper::Main]`** section. It will be necessary to set the GK name. The organisation's name is recommended.

```
[Gatekeeper::Main]
Name=RENATA
TimeToLive=60
TraceLevel=3
StatusTraceLevel=5
StatusPort=7000
```

This name will be used as an identifier by other GKs to refer to the GK. These options specify that endpoints register every 60 seconds. The status port for monitoring the GK is seven thousand (7000) and the trace level is three (3).

NOTE: It is very important if the server manages multiple network interfaces and IP addresses the IP to be used for routing RAS messages and requests must be specified. This is done by adding the following option in this section:

```
Bind=190.15.31.13
```

Substitute "190.15.31.13" for the server IP address with access to academic networks.

Configure a Neighbour

A Neighbour is a GK to route messages when a number is unknown. To configure a Neighbour, the following options are copied and modified with the corresponding values (this is self-explanatory):

```
[RasSrv::Neighbors]
RedCLARA=GnuGk

[Neighbor::RedCLARA]
GatekeeperIdentifier=RedCLARA
Host=200.0.206.181
SendPrefixes=00,!0057
AcceptPrefixes=*
ForwardLRQ=always
```

This will add the RedCLARA GK as a neighbour specifying the host IP address and will send international codes (00) and forbids route requests for numbers starting with (0057) for the Colombia code and will accept any prefixes.

Status Port Authorization

The Status Port can be accessed with the telnet tool to control and monitor the GK. With these options access to a specific IP address can be granted or forbidden.

```
[GkStatus::Auth]
rule=explicit
127.0.0.1=allow
Shutdown=forbid
```

This will enable monitoring access only by the server itself.

Accept LRQ and LCF

For a HQVCS network it is necessary to accept these types of RAS message. This enables location requests from other GKs to be processed. The following configuration is used to turn on this feature:

```
[RasSrv::LRQFeatures]
AcceptNonNeighborLRQ=1
AcceptNonNeighborLCF=1
```

For more specific and full information, consult the GNU GK Official Documentation (http://www.gnugk.org/gnugk-manual.html).

5.2.3. TESTING THE GNU GK

GnuGK runs as a daemon. To start running the Gatekeeper service, use a script located at the following path **`/etc/init.d/`** named **`gnugk`**. To start the service, pass the option "**`start`**" to the script as an argument as follows:

```
#: /etc/init.d/gnugk start
```

If GnuGk has been installed from binaries, a start-up script file located in **`initd`** directory inside of the extracted GNU GK directory should be copied to the **`/etc/init.d/`** and the command should be run as well.

At this point when the service is running, configure the endpoints to be registered with your Gatekeeper, this process may vary according to the branding of the endpoint. Also set the GK IP address and assign a call number. Once this is done the GK can be tested by making a call using the number dialling from the configured endpoint.

It is possible to see RAS messages generated during the call using the **`telnet`** tool through the monitoring port. The command for monitoring the GNU GK is:

```
$: telnet 127.0.0.1 7000
```

Accessing the GNU GK monitoring port with the telnet tool makes it possible to monitor and manipulate the GK with special commands. The list of commands that can be executed can be accessed by typing **`Help`** and hitting Enter. All commands are case-insensitive.

Some useful commands:

Reload
Apply configuration changes at run time.

Statistics, s
Print statistics for Endpoints and Calls.

PrintAllRegistrations, r, ?
Shows all registered Endpoints on the GK.

PrintCurrentCalls, c, !
Provides a summary of current calls.

Find, f <call number>
Useful command to locate an Endpoint by a call number when the GK has too many registered Endpoints.

DisconnectCall <call number>
Every call has an id number that can be found by printing all current calls. Giving an id for a call will perform a disengage request and the call will end.

Debug <opt>
This feature makes it possible to print and modify the GK configuration. All changes will be lost after a service shutdown. This is for debugging purposes only. These are the options for this command:

- trc [+|-|n]
  Increase/decrease or set a specific value for trace level.
- cfg <section> <attribute>
  Print the value for given section and attribute.
- set cfg <section> <attribute> <value>
  Assign a value for a given section and specific attribute.
- remove <section> | <section> <attribute>
  Removes a section or an attribute and sets its defaults value.

Exit, Quit, q, Ctrl-D
Close telnet connection.

MakeCall <source number> <destination number>
With this command GK will perform an ARQ message from the given source number and will establish a call between these two endpoints.

Another method for debugging the GK is capturing output from the log file and viewing RAS messages. The command for capturing the output is:

```
$: tail –f /var/log/gnugk/gnugk.log
```

This output is very useful for debugging although is not readable.

5.3. INTEGRATE WITH THE LATIN AMERICAN GATEKEEPER

This service is developed and maintained by RedCLARA. Its main function is to route calls for all Latin American NRENs to end sites behind other networks such as GÉANT and Internet2. In order to redirect calls to a specific country, the NREN GK must be added as a neighbour of the RedCLARA GK.

To do this, contact the RedCLARA GK administrator and provide the following information about the NREN GK:

- IP address
- Configuration file
- Technical contact information
- Country code

5.4. INTEGRATION WITH NRENUM.NET

E.164 Telephone Number Mapping (ENUM) is a standard defined by the Internet Engineering Task Force's (IETF's) Telephone Number Mapping working group; it uses DNS servers to translation numbers to a domain name and to enable the use of telephone-style numbers. The difference with the use of GKs is that DNS servers will resolve the address instead of routing call with number prefixes.

There is a DNS service provided by *Réseaux IP Européens Network Coordination Centre* (RIPE NCC) for "e164.arpa" (also known as Golden ENUM tree). NRENum.net is an alternative to the Golden ENUM tree for academia, implemented and managed by TERENA as a free service in collaboration with NRENs.

The NRENum.net service is a research and education network initiative designed to use the ENUM standard to translate telephone numbers to resource addresses (URI). With NRENum, an NREN will be able to set up a DNS to resolve its country numbers, and access the worldwide tree to carry out translations for other countries. NRENum.net is a tree infrastructure of DNS servers as is shown in Figure 6, where the top level DNS server (TIER-0) manages the "nrenum.net" zone and delegates country zone management to different NRENs (TIER-1).

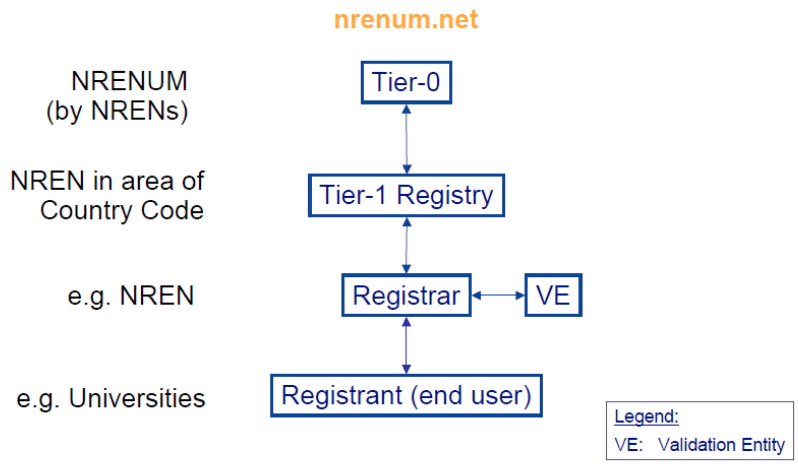

Figure 6: NRENum.net tree infrastructure

NRENs will populate registries in their DNS servers to assign numbers to different videoconferencing elements such as endpoints, MCUs and specific rooms. In many cases the NREN will act as the Registrar and Validation Entity at the same time, which consists of registering numbers and validating them according to a numbering plan approved by the NRENum.net delegation group.

5.4.1. CONFIGURING THE DOMAIN NAME SYSTEM

It is necessary to implement two (2) DNS servers, one master and one slave to manage the zone.

To implement an ENUM server it is possible to use Internet Systems Consortium (ISC) **bind9** software and configure a DNS service. The zone must be configured as follows: **<Reverse Dotted Country Code>.nrenum.net**. The Colombian Country Code is (57) and for this will use 7.5.nrenum.net.

These are example steps how to create the zone:

1) Add the following line to the **/etc/bind/named.conf** file:

```
include "/etc/bind/named.conf.enum";
```

2) Create the file: **/etc/bind/named.conf.enum** and enter the following configuration:

```
zone "7.5.nrenum.net" {
  type master;
  file "/etc/bind/db.7.5.nrenum.net";
};
```

3) Create the file: **/etc/bind/db.7.5.nrenum.net** and enter the following configuration:

```
$TTL   604800
@     IN    SOA   ns.7.5.nrenum.net. ingenieria.renata.edu.co. (
      2013111415; Serial
      21600     ; Refresh after 6 hours
      3600      ; Retry after 1 hour
      604800    ; Expire after 7 days
      3600      ; Minimum TTL of 1 hour
)

@     IN    NS    ns.7.5.nrenum.net.
NS    IN    A     190.15.31.17

4.0.6.2.0.3.5.1.0.7.5.nrenum.net. NAPTR 10 100 "u" "E2U+h323"
"!^.*$!h323:sala1@renata.edu.co!".
5.0.6.2.0.3.5.1.0.7.5.nrenum.net. NAPTR 10 101 "u" "E2U+h323"
"!^.*$!h323:sala2@renata.edu.co!".
```

Then use the dig tool to test your configuration:

$: dig @190.15.31.17 4.0.6.2.0.3.5.1.0.7.5.nrenum.net –t NAPTR

TThe following answer section will appear:

```
;; ANSWER SECTION:
4.0.6.2.0.3.5.1.0.7.5.nrenum.net. 604800 IN NAPTR 10 100 "u"
"E2U+h323" "!^.*$!h323:sala1@renata.edu.co!" .
```

NOTE: After this configure a secondary slave DNS server to act as a redundancy element.

For more information visit:
https://confluence.terena.org/display/NRENum/NRENum.net+service

5.4.2. REQUEST PREFIX IN NRENUM.NET

To request zone delegation, complete the Delegation Request form with the name of the organisation or NREN, contact details, technical contact and at least two primary and secondary DNS servers to which the zone should be delegated. The country dialling plan must be specified.

Delegation request form at:
https://confluence.terena.org/display/NRENum/Delegation+request

5.4.3. CONFIGURE THE GATEKEEPER TO USE ENUM DIALLING

After the zone is successfully delegated by the technical team of NRENum.net, configure the GK to use ENUM services to resolve endpoint numbers. Add the following lines to the configuration file and restart the service.

```
[RoutedMode]
ENUMservers=e164.arpa,nrenum.net

[RoutingPolicy]
default=explicit,internal,enum,srv,dns,neighbor
```

Numbers will be resolved in the order described above, with the neighbour element given the lowest priority.

5.5. INTEGRATION INTO THE LATIN AMERICAN HQVCS NETWORK

To integrate the Gatekeeper service into the Latin American HQVCS Network, follow the steps described below:

- Configure the RedCLARA Gatekeeper as a neighbour on the GK, using the following configuration:

```
[RasSrv::Neighbors]
RedCLARA=GnuGk

[Neighbor::RedCLARA]
GatekeeperIdentifier=RedCLARA
Host=200.0.206.181
SendPrefixes=00,!00<CC>
AcceptPrefixes=*
ForwardLRQ=always
```

  NOTE: Use the corresponding two-letter <CC> Country Code

- Contact the RedCLARA Gatekeeper administrator to receive instructions on configuration and call redirecting. If the request is accepted, the GK will be added as a Latin American neighbour.

- Make sure that all videoconferencing equipment points to and is registered on the implemented GK through the telnet tool as described in Section 4.2.3.

- To perform test calls, use the following numbers:

Number	H.323 ID	Endpoint Brand
0057015302604	Sala 1 RENATA	TANDBERG
0057015302605	Sala 2 RENATA	LG

6. REFERENCES

JANET. (n.d.). *JANET Videconferencing Service*. Retrieved October 2013, from JANET Library: https://community.ja.net/library/janet-services-documentation/janet-videoconferencing

Willamowius, J. (2013, September 19). *GNU Gatekeeper - a free VOIP Gatekeeper for H.323*. Retrieved October 10, 2013, from GNU Gatekeeper - a free VOIP Gatekeeper for H.323: http://www.gnugk.org/

APPENDIX A: CONFIGURATION FILE FOR RENATA GATEKEEPER

```
[Gatekeeper::Main]
Fortytwo=42
Name=RENATA
; if you have IPv6 enable this
;EnableIPv6=1
TimeToLive=60
TraceLevel=3
StatusTraceLevel=5
StatusPort=7000
CompareAliasType=0
CompareAliasCase=0

; Status port authentication and IP filtration

[GkStatus::Auth]
rule=explicit
127.0.0.1=allow
;insert a your local IP address for monitoring
;0.0.0.0=allow
Shutdown=forbid
DelayReject=5


; Log File rotation
[LogFile]
Rotate=Daily
RotateTime=23:59

[RoutedMode]
; If this is your World GK don't overload with
; NAT / Re - Routing
GKRouted=0
H245Routed=0
CallSignalPort=1720
;ENUMservers=enum.redclara.net
```

```
[RoutingPolicy]
default=explicit,internal,srv,dns,neighbor

;Temporary CDR file creation - It will enable call debugging
calls ;more easily
[FileAcct]
DetailFile=/var/log/gnugk/cdr.log
StandardCDRFormat=0
CDRString=%g|%n|%d|%c|%s|%u|%{gkip}|%{CallId}|%{ConfId}|%{set
up-time}|%{connect-time}|%{disconnect-time}|%{caller-
ip}|%{caller-port}|%{callee-ip}|%{callee-port}|%{src-
info}|%{dest-info}|%{Calling-Station-Id}|%{Called-Station-
Id}|%{Dialed-Number}
Rotate=daily
RotateTime=23:59

; Neighbor WORLD GK
[RasSrv::Neighbors]
RedCLARA=GnuGk

[RasSrv::GWRewriteE164]
RedCLARA=out=0055=

[Neighbor::RedCLARA]
GatekeeperIdentifier=RedCLARA
Host=200.0.206.181
SendPrefixes=00,!0057
AcceptPrefixes=*
ForwardLRQ=always

;enable the IPv6 ip address if using IPv6 and disable IPv4
;Host=[2001:808::20:0:161:50]

[RasSrv::LRQFeatures]
AcceptNonNeighborLRQ=1
AcceptNonNeighborLCF=1
;SendRIP=3000
```