



Computing Center of Max-Planck-Society and
Institute of Plasmaphysics

Building and maintaining GnuGK

**TelOzConf
AARNet IP Telephony Working Group
Australia
September 2004**



Outline

- GnuGK
 - What is it?
 - Why GnuGK?
 - The Proxy
 - Authentication methods
 - H.350
 - H.235
 - Some more features
- Setup/Installation
- Configuration
- Maintaining/Monitoring
- Software to enhance/adopt services
- Resources/More Information





What is GnuGK?

- GnuGK is a fully functional OpenSource Gatekeeper
- Available for free → GPL
- It supports H.323 V.4 (depending on used libraries → later)
- Software is based on theopenh323 stack (→ later)
- Beside the standard features like Bandwidth Control, Address Translation, Admission Control, Zone Management and Call Control Signaling, GnuGK has a wide range of endpoint authentication methods and a media proxy (Authentication/Proxy → later)



Why GnuGK?

- It's free → GPL
- It runs on Linux/UNIX, Windows and Macs
 - Precompiled binaries are available for several platforms (Win32, Linux, Solaris,...)
 - Some features are not (yet) available on Windows
- It comes with a media proxy (→ next slide)
- Several endpoint authentication methods
- New services/features can be applied by using other tools, GnuGK can interact with



The Proxy

- GnuGK comes with a fully feature media proxy
 - H.323 uses a few fixed ports, like 1718, 1719 tcp
 - H.323 negotiate used communication ports dynamically during the Setup process of a call
 - Used port range: 2^{10} to 2^{16} (1024 – 65535) udp
 - Approx. 4 to 8 ports are used per call
 - This dynamic behavior causes problems with Firewalls, aka. as the “H.323 {– Firewall} problem”

How do you open ports if you don't know them?

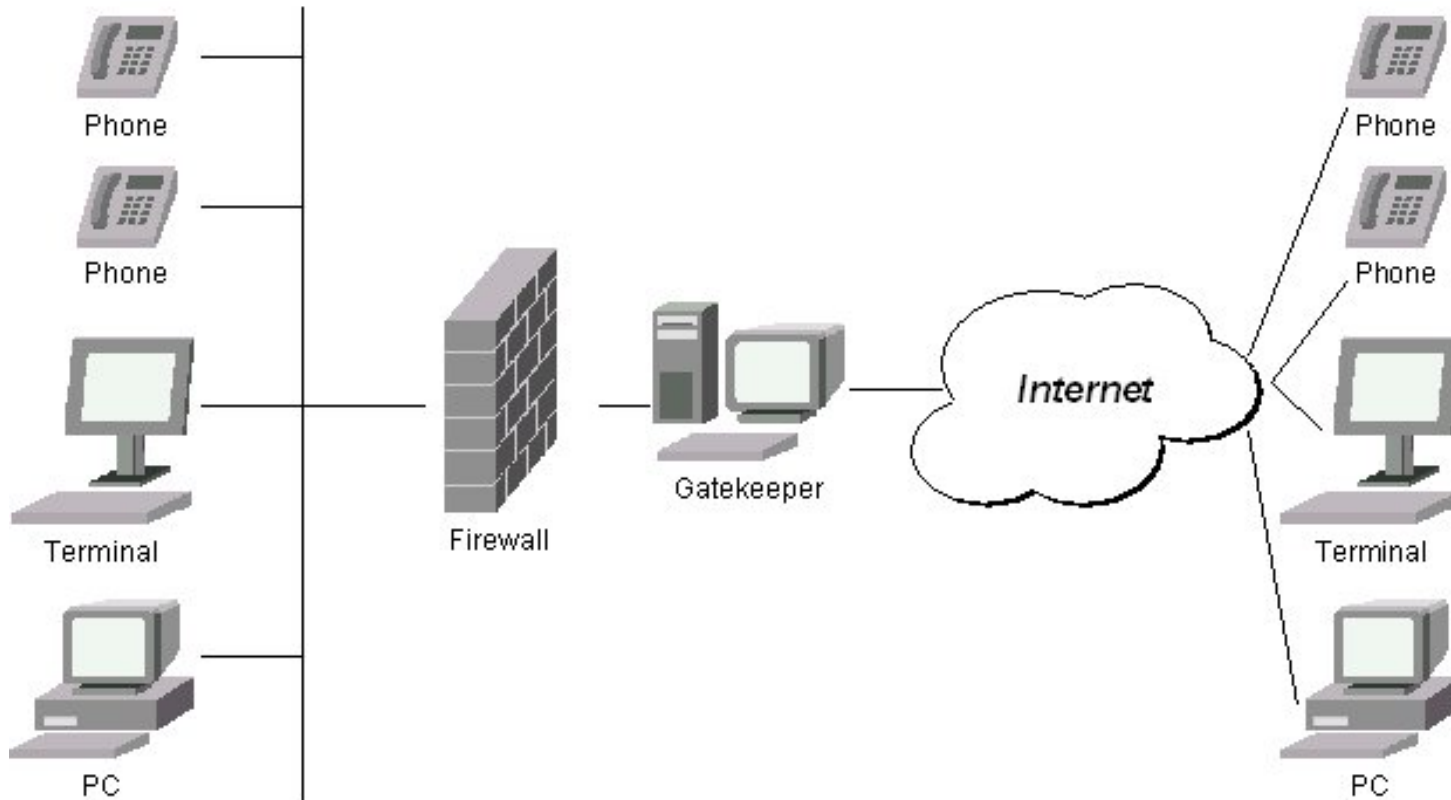


The Proxy cont'

- If proxy is used, firewalls can be bypassed
 - The proxy 'proxies' all streams/signals (TCP/UDP)
 - Signaling flow (TCP): Endpoint ↔ GK/Proxy ↔ Endpoint
 - Media streams (UDP): Endpoint ↔ GK/Proxy ↔ Endpoint
 - Only the GK/Proxy system is allowed to 'bypass' the firewall
 - Only the ports for the GK/Proxy IP need to be opened
 - ALL traffic, tcp/udp is handled by the proxy ("all streams are proxy'ed")
 - The endpoints don't know they are talking to a proxy. They believe it's the other endpoint



The Proxy cont'





The Proxy cont'

- What does it mean “all streams are proxy’ed”?



When every thing goes ‘arse-up’, NZ’ers come out on top.

If you try to call me by dialing 00498932996006 the streams are running around the world over ~ 50 hops, with ~ 500ms delay



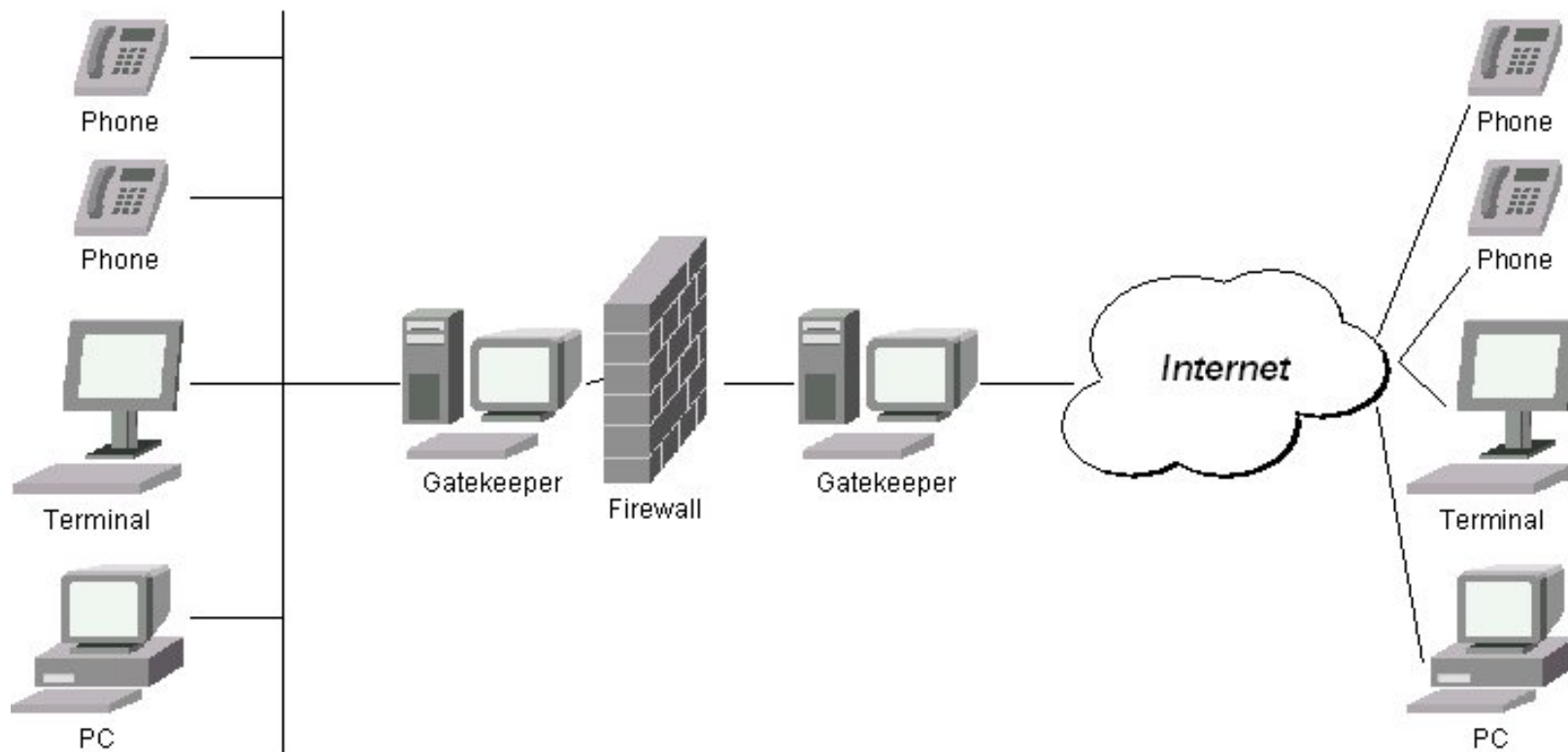
The Proxy cont'

- Security??
 - **ALL SYSTEMS WHO HAVE INTERNET/NETWORK CONNECTIONS CAN BE HACKED/HIGHJACKED/...**
 - Endpoints, e.g. VC system or IP Phone are protected by the firewall. They are just allowed to talk to the gatekeeper (...but they don't know they talk to a proxy)
 - GK/Proxy located in DMZ
 - VC Systems behind the Firewall were not vulnerable against the H.323 attack (earlier this year)
 - Is it possible to secure it even more?

YES



The Proxy cont'





The Proxy cont'

- **Activated/Deactivated/partial deactivated Proxy**
 - Proxy can be fully/partial deactivated
 - If Proxy is fully deactivated, GnuGK just works as a standard Gatekeeper
 - If Proxy is just partial deactivated, internal calls are not proxy'ed, only calls with external participant are proxy'ed
- **Other media streams/standards**
 - Proxy can handle T.120, H.239, People+Content, Duovideo, H.263, H.263+ (Problem has been solved), H.264, all audio codecs (e.g. G.711, G.728, G.722, Siren,...), AES/DES encrypted streams, Proxy is able to handle exotic clients, like H.323-VRVS, FVC Server, etc.



The Proxy cont'

- Used Port range can be limited for H.245 channels, RTP channels, T.120
 - This reduces the # of concurrent calls
 - Can cause trouble with MCUs



Authentication methods

- To make sure that no one who is not allowed to use your Gatekeeper, you have to authenticate the user/endpoint
- Possible methods:
 - IP, Prefix, Alias based
 - MySQL/PGSql authentication
 - Radius authentication
 - H.350 authentication (LDAP based)
 - H.235 authentication (encrypted password)



Authentication methods

- H.350 authentication as an example
 - Endpoints sends RRQ to Gatekeeper
 - Gatekeeper looks up Endpoint/User information in a H.350 directory
 - Iff H.350 directory has data (and this is not otherwise restricted), the Gatekeeper sends a RCF to Endpoint
 - (To add more security, you could send an H.235 password)
 - (To add more security, you can authenticate user/endpoint at any other message, like ARQ, etc. again)





Authentication methods

- A statement about H.235

----- Original Message -----

Subject: Re: Advice on Recent Gateway Issue

Date: Tue, 07 Sep 2004 15:18:22 -0400

From: Tyler Johnson <trjohns1@email.unc.edu>

Reply-To: <videnet_all_zone_admin@listserv.unc.edu>

To: <videnet_all_zone_admin@listserv.unc.edu>

[...] In my view we should all ensure that each time we let a contract for conferencing equipment (gatekeepers, endpoints, MCUs, gateways, etc.) that contract should *require* the equipment to use H.235 authentication.

- H.235 is more than just AES/DES encryption !





Some more features

- GnuGK supports NATed endpoints
- Load Balancing (Alternate GKs/several CPUs)
- Call Queuing (with third party tool)
- Call forwarding
- H.235
- ToS Bit forwarding
- Accounting (File, mySQL, Radius)
- Call Limitation for Prefixes, IPs, Subnets, etc.
- ...



Setup/Installation

- The following setup/installation instructions are based on a self-compiled version of GnuGK running on Linux/Unix...

...lets do it



Setup/Installation

- Hardware requirements
 - First installed GK was a PIII, 800MHz, SuSE Linux 7.3
 - System was too slow and was replaced after 4 weeks
 - Second installed GK was a PIII, 1.6GHz, SuSE Linux 7.3
 - System was up and running for more than 2 years and handled roughly 1000 calls per month and a data throughput of approx. 120GB per month; allover 6 crashes
 - Third installed GK is a Quad Intel Xeon 2.4GHz, Redhat Linux 9
 - System is up and running since 03/2004

A modern standard PC for \$1000 will do the job.



Setup/Installation

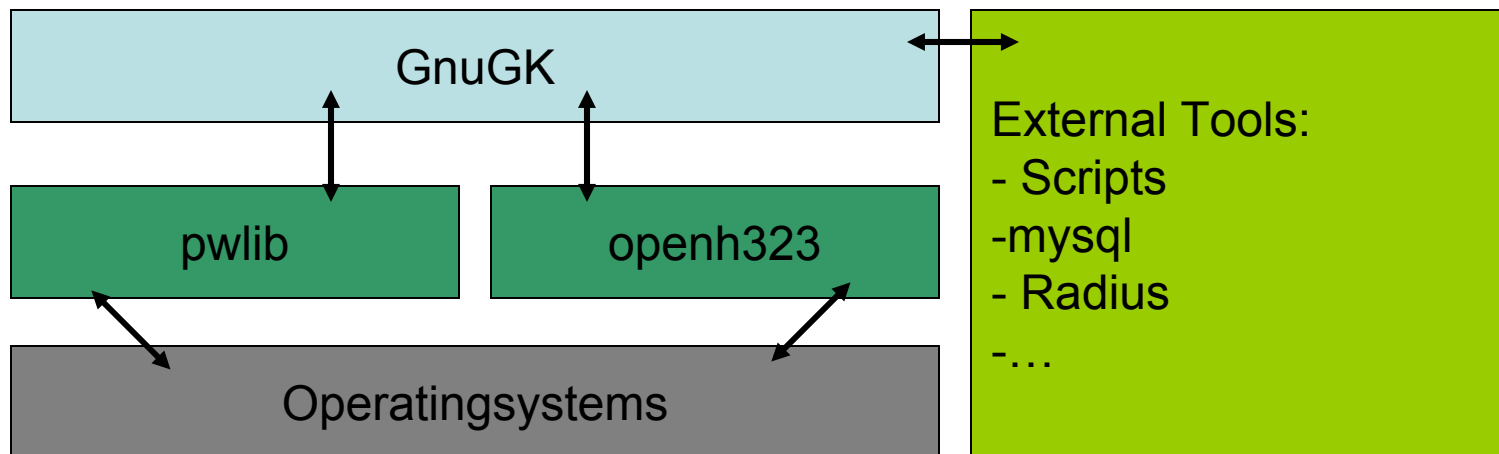
- Download GnuGK at <http://www.gnugk.org>
(Current version: 2.0.8)
- Download openh323 libraries at:
<http://sourceforge.net/projects/openh323/>
(Current version: 1.15.0)
- Download pwlib libraries at:
<http://sourceforge.net/projects/openh323/>
(Current version: 1.8.0)

Do not use openh323 1.12.2 and pwlib 1.5.2, they have a problem with H.263+ (Polycom systems)!!



Setup/Installation

- Why the libraries?/The concept





Setup/Installation

- 'Un'gz and 'Un'tar pwlib-x.xx.x.tar.gz to any directory you want, e.g. /usr/local/lib/pwlib
- `export PWLIBDIR=<your-path-to-pwlib>`
- `cd PWLIBDIR`
- `./configure` {set options if you have to, like `--prefix`}
- `make both` (other options like *optnoshare*, *debug*, etc. are available; see Makefile for details)
- (make install is not necessary)



Setup/Installation

- 'Un'gz and 'Un'tar `openh323-x.xx.xx.tar.gz` to any directory, e.g. `/usr/local/lib/openh323`
- `export OPENH323DIR=<your-path-to-openh323>`
- `cd OPENH323DIR`
- `./configure` {set options if you have to, like `--prefix`}
- `make both` (other options like *optnoshare*, *debug*, etc. are available; see Makefile for details)
- (make `install` is not necessary)



Setup/Installation

- 'Un'gz and 'Un'tar gnugk-x.x.x.tar.gz to any directory, e.g. /opt/gnugk-x.x.x
- `export LD_LIBRARY_PATH=$PWLIBDIR/lib:
$OPENH323DIR/lib:$LD_LIBRARY_PATH`
- If you want a 'standard' configuration (that includes mysql, pgsq, ldap, radius, etc.):

`make both`



Setup/Installation

- 'Faster', No PGSql, no Radius, no LDAP, just mySQL

```
LARGE_FDSET=16384 NO_RADIUS=1 NO_LDAP=1 NO_PGSQL=1  
MYSQLDIR=/usr/include/mysql MYSQLLIBDIR=/usr/lib/mysql  
make both
```

- The documentation section on the webpage is a little bit dodgy. Even if mysql support is not disabled, mysql support won't be compiled until you explicitly set the path to the include dir and library dir



Setup/Installation

- Just GnuGK, nothing else

```
NO_MYSQL=1 NO_LDAP=1 NO_PGSQL=1 NO_RADIUS=1 make both
```

- If compilation was successful, you will find a binary `gnugk` in the directory `/<your-path-to-gnugk>/obj_linux_x86_r/`
- For a first test you can just start it with

```
/<your-path-to-gnugk>/obj_linux_x86_r/gnugk -ttt
```



Configuration

- General configuration
 - Create a configuration file e.g. gk.conf in any directory you like, e.g. /opt/gnugk-x.x.x/config/gk.conf or /etc/gk/gk.conf
 - Comments within the configuration file are ‘introduced’ by #
 - Configuration file is separated into several logical parts
 - Each part has ‘Headline’ prefaced with [...]
 - Sample basic configuration → next slide



Configuration

- Sample basic configuration

*This configuration file says:
I have a Gatekeeper named
telozconf.australia.au, running on the
IP address 10.10.2.10. The TTL
for the registration of Endpoints is
300 seconds, my status port is
7000 (Telnet ☹). The system does
no routing, proxy is disabled
and every one is allowed to see the
status*

[Gatekeeper::Main]

```
Fourtytwo=42  
Name=ozconf.australia.au  
Home=10.10.2.10  
NetworkInterface=10.10.2.10/24  
EndpointIDSuffice=_telozconf.aus  
tralia.au  
TimeToLive=300  
TotalBandwidth=-1  
StatusPort=7000
```

[RoutedMode]

```
GKRouted=0
```

[Proxy]

```
Enabled=0
```

[GKStatus:Auth]

```
rule=allow
```





Configuration

- Sample configuration with GK routing, Proxy only for external participants

```
[Gatekeeper::Main]  
Fortytwo=42
```

```
...
```

```
[RoutedMode]  
GKRouted=1  
H245Routed=0
```

```
[Proxy]  
Enabled=1  
InternalNetwork=10.10.2.0/24
```



Configuration

- Sample configuration for full proxy

```
[Gatekeeper::Main]  
Fourtytwo=42
```

```
...
```

```
[RoutedMode]  
GKRouted=1  
H245Routed=1
```

```
[Proxy]  
Enabled=1
```



Configuration

- Sample configuration for the use with a country/world gatekeeper

```
[Gatekeeper::Main]  
Fourtytwo=42
```

```
...
```

```
[RasSrv::Neighbors]  
CGK=10.10.10.10:1719;*;
```



Configuration

- Sample configuration with Prefix authentication and no call limitation for the endpoints

```
[Gatekeeper::Main]
```

```
Fourtwo=42
```

```
...
```

```
[Gatekeeper::Auth]
```

```
PrefixAuth=mandatory;RRQ;ARQ
```

```
default=deny
```

```
[PrefixAuth]
```

```
ALL=deny ipv4:ALL
```

```
ALL=deny ipv4:0.0.0.0
```

```
ALL=allow alias:^00611234{xxxx}
```

```
ALL=allow alias:^00614321{xxxx}
```

```
ALL=deny alias:^00619876{xxxx}
```





Configuration

- Sample configuration for Prefix authentication, IP based, and call limitation for IP 10.10.2.5

```
[Gatekeeper::Main]
Fourtwo=42
...
[Gatekeeper::Auth]
PrefixAuth=mandatory;RRQ;ARQ
default=deny

[PrefixAuth]
ALL=deny ipv4:ALL
ALL=deny ipv4:0.0.0.0
ALL=allow ipv4:10.10.3.1/24
0061=allow ipv4:10.10.2.5/24
```



Configuration

- Sample configuration for
mySQL authentication

```
[Gatekeeper::Main]
Fourtytwo=42
...
[Gatekeper:Auth]
MySQLAliasAuth=required;RRQ;ARQ
default=deny
```

```
[MySQLAliasAuth]
;
; Select ip FROM db.table WHERE
      IDField=%0:h323_ID
;
Host=localhost
Database=db
Table=table
User=userwhohasaccess
Password=secret
IDField=alias
IPField=ip
CacheTimeout=300
```



Configuration

- E.164 rewrite, just 10.10.1.1 is allowed to view status

```
Gatekeeper::Main]
Fourtywo=42
...
```

```
[GKStatus::Auth]
rule=explicit
10.10.1.1=allow
```

```
# Rewrite
```

```
911=0061911
912=0061912
1001=0061911**0061912
```



Configuration

- **File Accounting**

```
[Gatkeeper::Main]
Fourtytwo=42
...
[CallTable]
GenerateNBCDR=1
GenerateUCCDR=1
DefaultCallTimeout=0
AcctUpdateInterval=0

[Gatekeeper::Acct]
FileAcct=required;start,update,stop,on,off
default=accept

[FileAcct]
DetailFile=/opt/gk-x.x.x/log/gk_acct.log
Rotate=0
```



Maintaining/Monitoring

- Unfortunately remote monitoring is just available via Telnet Port 7000 (default, Port can be changed via config file), and allowed hosts/subnets can be specified

```
130.183.3.40 - PuTTY
Version:
Gatekeeper(GNU) Version(2.0.8) Ext(pthread=1,acct=1,radius=0,mysql=1,pgsql=0,ld
ap=0,large_fdset=16384) Build(Aug 7 2004, 14:35:14) Sys(Linux i686 2.4.26)
Large fd_set(16384) enabled

CkStatus: Version(1.0) Ext()
Toolkit: Version(1.0) Ext(basic)
Startup: Wed, 25 Aug 2004 12:13:48 +0200   Running: 17 days 01:32:13
;
RCF|130.183.121.29:1720|C-IPP-WL:h323_ID=00498932996105:dialedDigits|terminal|5850_rzg.mpg.de
;
RCF|141.61.65.16:1720|C-BIO-HARTL:h323_ID=00498932996602:dialedDigits|terminal|5845_rzg.mpg.de;
RCF|194.94.233.16:1720|HCW-IPP-DIR:h323_ID=00493834881005:dialedDigits|terminal|5837_rzg.mpg.de;
█
```





Maintaining/Monitoring

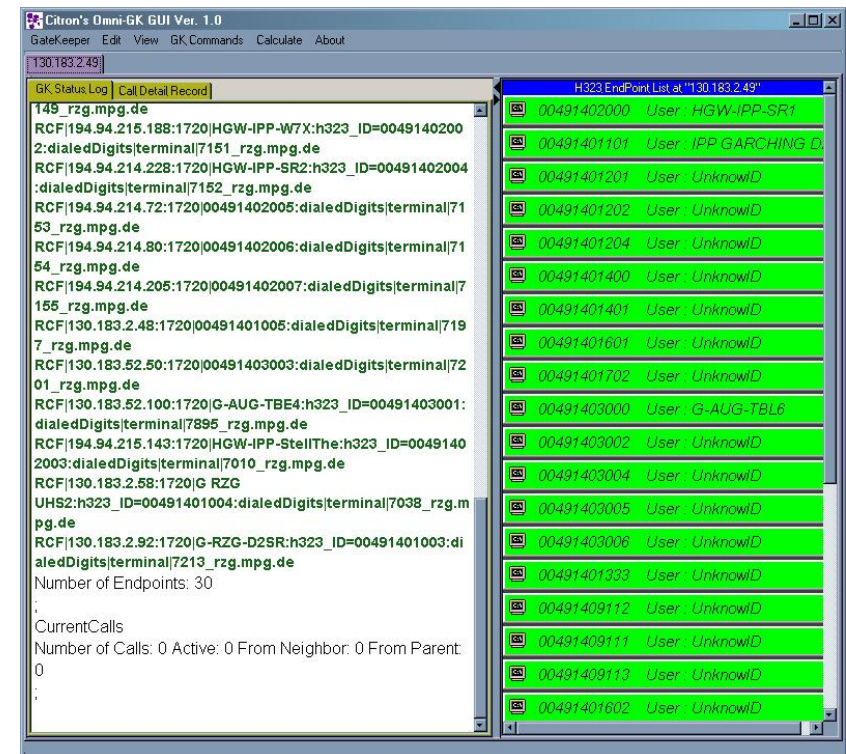
- Configuration can be changed on the fly, without restarting GnuGK. Via Telnet Status Windows send `reload` command
- Telnet Status Window gives the following information
 - Gatekeeper status (`status`)
 - Current registered endpoints (`currentregisteredendpoints`)
 - Current Calls (`printcurrentcalls`)
 - ...
- Other commands can be send as well
 - Unregister an IP (`unregisterip 10.10.2.10`)
 - Transfer call (`transfercall <source> <destination>`)
 - Disconnect Call (`disconnectcall <callnr>`)
 - ...





Maintaining/Monitoring

- A Java GUI is available for download at <http://www.gnugk.org/h323dev/elp.html#java> but it is not really stable or reliable





Maintaining/Monitoring

- Write/Get a couple of CGI/Perl/PHP/Python/etc. Scripts and write your own Monitoring 'Tool' for a Browser
- Is available online at <http://www.rzg.mpg.de/vc/status.php>

Zone: Garching, 0049893299xxxx

No.	E.164	Alias	IP address	Email	Type	Status
121	00498932996104	G-IPP-VAD129	130.183.121.129	michael.winkler@ipp.mpg.de	Tandberg 1000	
112	00498932996501	G-AUG-TBL6	130.183.52.80	kcb@ipp.mpg.de	Tandberg 6000	
2	00498932996004	G-RZG-UHS2	130.183.2.58	schwena@rzg.mpg.de	Tandberg 1000	
113	00498932996502	G-AUG-TBE4	130.183.52.100	kcb@ipp.mpg.de	Tandberg 500/550	
123	00498932996002	G-RZG-VCTERM1	130.183.2.68	schwena@rzg.mpg.de	Polycom ViaVideo	
144	00498932996113	G-IPP-VSX3	130.183.2.183	schwena@rzg.mpg.de	Polycom VSX 7000	
111	00498932996007	G-RZG-HKS	130.183.2.83			
134	00498932996105	G-IPP-WL	130.183.121.29			
170	00498932996115	G-IPP-PCS5	130.183.2.185			
171	00498932996116	G-IPP-PCS6	130.183.2.186			
120	00498932996251	G-MPA-VCR	130.183.85.191			
106	00498932996003	G-RZG-D2SR	130.183.2.92			
169	00498932996006	NZ-RZG-KFS	130.216.13.164			

Zone: Greifswald, 0049383488xxxx

No.	E.164	Alias	IP address	Email
110	00493834881005	HGW-IPP-DIR	194.94.233.16	tw@
108	00493834881003	HGW-IPP-WTX	194.94.215.188	tw@
107	00493834881002	HGW-IPP-SR2	194.94.214.228	tw@
109	00493834881004	HGW-IPP-STTH	194.94.215.143	tw@

Current Calls

General Info		Caller Info			Callee Info			
Call No.	Call Duration	Dialed Nr.	IP address	H.323 alias	E.164	IP address	H.323 alias	E.164
893	11.20 min.	004910791311	130.216.13.164	NZ-RZG-KFS	00498932996006	194.95.240.223	DFN-MCU 107	0049107
894	10.28 min.	00498932996004	194.95.240.223	DFN-MCU 107	0049107	130.183.2.58	G-RZG-UHS2	00498932996004
895	9.52 min.	00498932996002	194.95.240.223	DFN-MCU 107	0049107	130.183.2.68	G-RZG-VCTERM1	00498932996002
896	9.15 min.	00498932996113	194.95.240.223	DFN-MCU 107	0049107	130.183.2.183	G-IPP-VSX3	00498932996113
897	8.68 min.	00498932996007	194.95.240.223	DFN-MCU 107	0049107	130.183.2.83	G-RZG-HKS	00498932996007
898	8.28 min.	00498932996115	194.95.240.223	DFN-MCU 107	0049107	130.183.2.185	G-IPP-PCS5	00498932996115
899	8.20 min.	00498932996116	194.95.240.223	DFN-MCU 107	0049107	130.183.2.186	G-IPP-PCS6	00498932996116
900	7.73 min.	00498932996003	194.95.240.223	DFN-MCU 107	0049107	130.183.2.92	G-RZG-D2SR	00498932996003
901	7.32 min.	00493834881002	194.95.240.223	DFN-MCU 107	0049107	194.94.214.228	HGW-IPP-SR2	00493834881002
902	7.12 min.	00493834881004	194.95.240.223	DFN-MCU 107	0049107	194.94.215.143	HGW-IPP-STTH	00493834881004
903	6.63 min.	00493834881003	194.95.240.223	DFN-MCU 107	0049107	194.94.215.188	HGW-IPP-WTX	00493834881003
904	6.38 min.	00493834881005	194.95.240.223	DFN-MCU 107	0049107	194.94.233.16	HGW-IPP-DIR	00493834881005
905	5.45 min.	00498932996105	194.95.240.223	DFN-MCU 107	0049107	130.183.121.29	G-IPP-WL	00498932996105
906	4.88 min.	00498932996251	194.95.240.223	DFN-MCU 107	0049107	130.183.85.191	G-MPA-VCR	00498932996251
907	3.48 min.	00498932996104	194.95.240.223	DFN-MCU 107	0049107	130.183.121.129	G-IPP-VAD129	00498932996104
908	2.83 min.	00498932996501	194.95.240.223	DFN-MCU 107	0049107	130.183.52.80	G-AUG-TBL6	00498932996501

v.0.5, last update 05/01/2004, Kevin Stoeckigt

Who is registered?

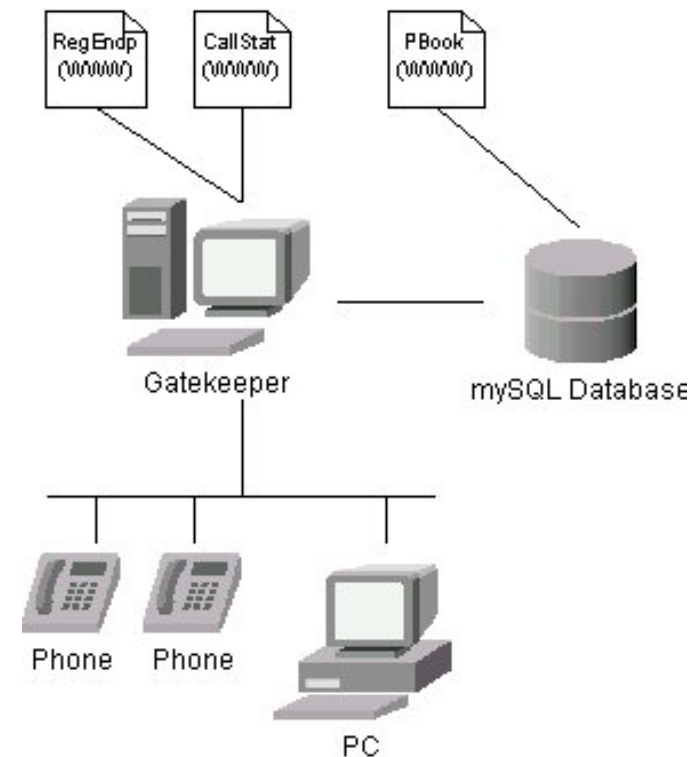
Who is in call?





Maintaining/Monitoring

- **Sample Setup**
 - Central DB used for
 - Authentication
 - Phonebook
 - Host Information
 - Accounting
 - RegEndp+CallStat get Information from GK and additional Information from DB
 - Phonebook created from DB





'Celebrity' Gatekeeper

- My GK
- German Country GK
- Hungarian Country GK
- AFAIK Spanish Country GK
- HEAnet has at least one
- Several others at German Universities (Berlin, Hamburg, Dresden, ...) and Research Societies/Groups
- Several other all over Europe and the Rest of the World
- ...maybe your place soon...





Software to enhance/adopt services

- MySQL (for Authentication, Accounting)
- OpenLDAP (for Authentication (H.350))
- OpenRadius/FreeRadius (for Authentication/Accounting)
- Bunch of DIY-Scripts
- ...and the best...its ALL free !



Resources/more Information

- me 😊
- <http://www.gnugk.org>
- <http://www.rzg.mpg.de/vc/> (there you can find many more slides and information)



Computing Center of Max-Planck-Society and
Institute of Plasmaphysics

Final slide - 1

If you have any question, need any information or
want a 'special' configuration, please contact me

Kewin Stoeckigt

+64 9 367 7100 x 32012

kfs@rzg.mpg.de or ksto033@ec.auckland.ac.nz



Computing Center of Max-Planck-Society and
Institute of Plasmaphysics

Final slide

Thank you