```
**********************************
* Info - GNU GK CESNET           *
*                                *
* autor:    M.Voznak             *
* mailto:   miroslav.voznak@vsb.cz *
* tel:      +420 596991699       *
* vytvoreno: 9.12.2004           *
* zmeneno  : 13.2.2005           *
*                                *
**********************************
```


Uvod:
CESNET provozuje ve sve H.323 topologii dva GK, ktere jsou otevrene a umoznuji pristup do vnitrni site H.323
a zaroven slouzi pro peering s H.323 zarizenimi, ktere jsou mimo infrastrukturu CESNET2 (napr. SANET, Hungarnet,
AARNET, atd...). Tyto GK jsou dosazitelne pres DNS jako gk1ext.cesnet.cz a gk2ext.osanet.cz a jsou umisteny
v Praze a v Ostrave.

Podminky pouziti:
Oba gk1ext.cesnet.cz a gk2ext.cesnet.cz je mozne pouzivat za dodrzeni nasledujicich podminek:
A/ pro odzkouseni H.323 zarizeni, otestovani vzajemne kompatibility, overeni jejich vlastnosti.
B/ v pripade trvale registraci na techto GK je podminkou zaslani registracnich informaci
mailem na miroslav.voznak@vsb.cz , kde pozadujeme uvest "e164 id - tel.c.", "h.323 id - jmeno" a
nazev organizace ci osoby tuto regstraci vyuzivajici

Obsah:

1. Instalace GNUGK
2. Zmena konfigurace za behu GNUGK
3. Accounting - zaznamy o hovorech
4. DRC a GRC mody
5. Pridani GK
6. Pridani GW
7. Prepisovaci pravidla
8. Autentizace
9. Debug pomoci Tethereal a tcpdump
10. Debug pres telnet

1. Instalace GNUGK

```
/* Debian ma pripravene 2 balicky s GK, zastaraly OpenH323 a aktulani GNUGK
gk2ext:~# apt-cache search gnugk
gnugk - OpenH323 Gatekeeper - The GNU Gatekeeper
openh323gk - Legacy package for openh323gk that you should remove

gk2ext:~#
gk2ext:~# apt-get install gnugk

/* restart GNUGK
gk1ext:/etc/init.d# ./gnugk restart
```

2. Zmena konfigurace za behu GNUGK

```
/*  konfigurak je v gatekeeper.ini
gk2ext # vi /etc/gatekeeper.ini

/* nactení konfigurace se udela prikazem reload přes telnet na portu 7000
gk2ext: # telnet 195.113.113.131 7000
reload
exit
```

3. Accounting - zaznamy o hovorech

```
/* kazdy uskutecneny hovor se ihned zapise do /var/log/gnugk/cdr.log
/* jakmile velikost souboru presahne 100KB, tak se prepisuje od znova,
/* jeden zaznam ma 256 B, takze by to melo drzet vzdy poslednich 400 CDR
/* do gatekeeper.ini

[Gatekeeper::Acct]
;RadAcct=optional;start,stop,on,off
FileAcct=sufficient;stop

[FileAcct]
DetailFile=/var/log/gnugk/cdr.log
Rotate=S100k

gk2ext:~# more /var/log/gnugk/cdr.log
CDR|4|02 1f a7 11 55 81 15 b1 12 7d 56 34 34 34 34 ef|6|Thu, 09 Dec 2004
21:11:44 +0100|Thu, 09 Dec 2004 21:11:50 +0100|195.113.113.
138:1720|3801_endp|195.113.144.77:1720| |420596991699:dialedDigits|voznak
miroslav:h323_ID=42059611699:dialedDigits|gk2ext;
gk2ext:~#
```

4. DRC a GRC mody

```
/* rezim se nastavuje v gatekeeper.ini , kdyz GK jede v DRC rezimu, tak vyzizuje
pouze RAS signalizaci

[RoutedMode]
GKRouted=0
H245Routed=0

/* pro GRC s Q.931 , ale bez H.245 se zadava

[RoutedMode]
GKRouted=1
H245Routed=0


/* pro GRC s Q.931 a H.245 se zadava

[RoutedMode]
GKRouted=1
H245Routed=1

/* rezim Proxy, tzn. ze vsechno vcetne RTP tece přes GK, ale musi byt zapnut GRC

[Proxy]
Enable=1
```

5. Pridani GK

```
/* otoceni GK proti vnitrnim GK1 a GK2 Cesnetu, vse co zacina 420, tak posila na
ne

[RasSrv::Neighbors]
LSU=GnuGK
HUGK=GnuGK
GK1-CESNET=CiscoGK
GK2-CESNET=CiscoGK

[Neighbor::LSU]
Host=130.39.252.36
SendPrefixes=1225578
AcceptPrefixes=*

[Neighbor::GK1-CESNET]
Host=195.113.144.84
;SendPrefixes=*
AcceptPrefixes=*

[Neighbor::GK2-CESNET]
Host=195.113.144.85
;SendPrefixes=*
AcceptPrefixes=*
```

6. Pridani GW

```
/* otoceni proti IP to IP GW Cesnetu, vse co zacina 420 se posila na GW
/* pozor !!! IP2IP GW ma problem se SlowStart/H323v1 ,tzn. netmeeting zazvoni,
ale nespoji se

[RasSrv::PermanentEndpoints]
193.84.207.194:1720=GW1-SLU-OP;420553684
```

7. Prepisovaci pravidla

```
/* u verze GNUGK 2.2.1 jsou vetsi moznosti prepisovacich pravidel, jsou pridany
... jako pocet
mist, potom % je wildcard a ! ma opacny vyznam (!2=00 kdyz neobsahuje cislici 2,
tak prepis 00)
/* kdyz prijde 4209500 a pet cisel za tim,tak to vezme jako 9500 a tech pet
cisel

[RasSrv::RewriteE164]
4209500.....=9500.....

/* kdyz si zadefinuju nazev GW, coz je jeho alias, pod kterym je veden na GK a
prefix,
tak lze ke konkretnimu prefixu jdouci na konkretni GW udel prepisovaci pravidlo
in nebo out,
nejdrive je cislo puvodni a potom nasleduje jak ma byt prepsane
[RasSrv::GWPrefixes]
GW-VUTBR=54114

[RasSrv::GWRewriteE164]
GW-VUTBR=out=54114=42054114
```

8. Autentizace

/* overenim hesla se rozumi overeni obsahu pole cryptoTokens (hashed by MD5) v konkretni zprave RAS, pricemz uzivatelske jmeno je ve zprave videt transparentne
/* v GNUGK je zadano, aby se overovala zprava RRQ a pokud neprojde, tak se jeste necha projit jinymi pripadnymi pravidly overovani v sekci autorizace

```
[Gatekeeper::Auth]
SimplePasswordAuth=optional;RRQ
```

/* zde se zada uzivatelske jmeno a heslo ziskane pomoci utility addpasswd , zadavane heslo v gatekeeper.ini neni stejne jako v telefonu!

```
[SimplePasswordAuth]
cesnet=FVqqGh4sTxE=
```

/* utilita addpasswd ma syntaxi - addpasswd config section userid password a ziskane heslo si prectu, postup je nasledujici

```
gk1ext:~# addpasswd /etc/gnugkpasswd.conf passwd cesnet cesnet
gk1ext:~# addpasswd /etc/gnugkpasswd.conf passwd michal popokatepetl
gk1ext:~# addpasswd /etc/gnugkpasswd.conf passwd karel praha

gk1ext:~# more /etc/gnugkpasswd.conf
[passwd]
cesnet=FVqqGh4sTxE=
michal=+cpVm3SuBWu4ndVrBHMTbw==
karel=dPy7gm/tLX4=
```

/* do koncoveho zarizeni je nutne zadat uzivatelske jmeno i heslo, (napr. v SJ phone se zaskrtne v masce Initialization Gatekeeper Account a Gatekeeper Password, pri zvoleni initialization se zada Account a Password), to se overuje, napr. cesnet cesnet (to dame asi jako testovaci ucet)

funkcnost byla dnes overena, tzn. ze mame urcity nastroj k zabezpeceni pristupu a kazdemu uzivateli muzeme pridelit nejake heslo, je to sice jednoduche, ale vzhledem k tomu, ze pres GNUGK gk1ext.cesnet.cz se neda dovolat do verejne site, tak to povazuju za dostacujici, overeni probiha na zpravu RRQ, tzn. pouze na ty, co jsou primo registrovani na GK (tyka se telefonu), da se ovsem zapnout i na dalsi zpravy LRQ, atd..., ale to by nam mohlo zpusobit problemy s peeringem, protoze vetsina kooperujicich instituci ma problem vubec peering proti Cesnetu rozchodit, natoz se nejak autentizovat

dalsi problem vidim v portfoliu produktu, nebot timto je definitivne pohrben Microsoft Netmeeting (autentizaci heslem neumi) a v teto chvili mam odzkouseny pouze SJ Labs Phone (ten jsem zkousel za NAT pres cesneti VPN, takze asi tak, jak to bude potencionalni "Milanek chce volat mamince", pouzivat) a v praci zkusim Welltech LP101 a Siemens Optipoint

/* da se to vyresit autentizacim modulem [RasSrv::RRQAuth], autorizuje se proti IP

```
[Gatekeeper::Auth]

SimplePasswordAuth=optional;RRQ

AliasAuth=required;RRQ

default=allow

[RasSrv::RRQAuth]

950012345=sigip:195.113.150.124:1720

default=confirm
```

9. Debug pomoci Tethereal a tcpdump

```
/* jelikoz vetsina kodu h323 je zpracovana prekladacem ASN1.PER, nastroje jako
tcpdump nebo ngrep nepostacuji
/* nejvykonnejsim free nastrojem je bezesporu ethereal, pro prikazovou radku
teethereal
vera:~# apt-get install tethereal

/* nekdo je zvykly na tcpdump
vera:~# apt-get install tcpdump

/* filtr na zachyceni paketu obsahujici konkretni IP

vera:~# tcpdump host 192.168.1.100
vera:~# tethereal -R "ip.addr == 192.168.1.100"
Capturing on eth0
  8.375328 192.168.1.13 -> 192.168.1.100 H.225.0 CS: releaseComplete
  8.377426 192.168.1.100 -> 192.168.1.13 TCP 1720 > 32769 [ACK] Seq=156 Ack=265
Win=8154 Len=0 TSV=66951 TSER=110057
  8.399290 192.168.1.100 -> 192.168.1.13 H.225.0 RAS: disengageRequest
  8.410228 192.168.1.13 -> 192.168.1.100 H.225.0 RAS: disengageConfirm

/* filtr na zachyceni paketu obsahujici konkretni dve IP adresy
tcpdump host 192.168.1.100 or host 192.168.1.12
tethereal -R "ip.addr == 192.168.1.100 or ip.addr == 192.168.1.12"

tcpdump host 192.168.1.100 or host 192.168.1.12 and not tcp port 22
tethereal -R "ip.addr == 192.168.1.100 or (ip.addr == 192.168.1.12 and not
tcp.port == 22)"

/* filtr na zachyceni paketu obsahujici konkretni IP a UDP port
tcpdump host 192.168.1.100 and tcp port 1720
tethereal -R "ip.addr == 192.168.1.12 and udp.port == 1719"

/* filtr zachycujici vse krome konkretni IP
tcpdump not host 192.168.1.12
tethereal -R "not ip.addr eq 192.168.1.12"

/* filtr zachycujici vse souvisejici s konkretni IP krome portu 22
tcpdump host 192.168.1.12 and not tcp port 22
tethereal -R "ip.addr == 192.168.1.12 and not tcp.port == 22"

/* ulozit do souboru
tcpdump -vv -w /home/voz29/logeth2
tethereal -w "/home/voz29/log.eth"

tethereal -w "/home/voz29/log.eth" host 192.168.100


tethereal -f "ip.addr == 192.168.1.100" -w "/home/voz29/log.eth"
```

10. Debug pres telnet

```
/* na portu 7000

telnet 195.113.113.131 7000

/* logovani do souboru
```

```
setlog /var/log/gnugk/trace1.log

/* zapnuti debug, cislo urovne (napr. 2 je takova jednodussi,
debug trc 2


2004/12/13 15:55:56.544 2             RasSrv.cxx(357)
ACF|195.113.113.135:1720|9394_endp|24867|420950012345:dialedDigits|Mir:h323_
ID=420950012346:dialedDigits|false;

/* uroven 3 jsou uz zpravy podrobne rozepsane
debug trc 3
debug trc 5

/* zkousel jsem i uroven 5 a ta se moc nelisila od urovne 99
/* u reseni problemu doprucuji zacit 2-hou, potom 3-ti a potom 5-tou
/* odejiti z telnetu
exit

/* podivati se, co tam mame
more /var/log/gnugk/trace1.log
rm /var/log/gnugk/trace1.log

/* kdo je prihlasen, registrace
printallregistrations


rm /var/log/gnugk/trace1.log
setlog /var/log/gnugk/trace1.log
debug trc 3

debug trc 0
rotatelog
exit

more /var/log/gnugk/trace1.log


setlog /var/log/gnugk/trace4.log
more /var/log/gnugk/trace4.log

more /var/log/gnugk/trace1.log
rm /var/log/gnugk/trace1.log
```