Building Certificate Authority for Grid Computing
Gadjah Mada University and University of Indonesia

Building Certificate Authority for Grid Computing
Gadjah Mada University and University of Indonesia

Atik Pilihanto

mailto : anto@g-ti.com

http://g-ti.com

0x00 - Latar Belakang

Pada awal tahun 2006 Direktorat Jendaral Pendidikan Tinggi (DIKTI) membangun jaringan INHERENT dengan tujuan untuk peningkatatan mutu pendidikan tinggi yang pada akhirnya diarahkan meningkatkan daya saing bangsa yang dilandasi adanya otonomi penyelenggaraan pendidikan dan kesehatan organisasi.

Jaringan INHERENT adalah jaringan komunikasi tertutup antar perguruan tinggi di Indonesia. Pada awal tahun 2006 telah terbangun *interkoneksi 32 localnode* yang berada di perguruan-perguruan tinggi di ibukota propinsi di Indonesia serta kantor DIKTI. Jaringan INHERENT ini menggunakan koneksi dedicated *SONET oc-3* atau biasa dikenal dengan *STM-1* dengan kecepatan koneksi 155 MBps. Dengan jaringan INHERENT sharing resource antar universitas menjadi lebih mudah dan effisien. Universitas Gadjah Mada merupakan salah satu node dari *32 localnode* di Indonesia yang bertanggung jawab dalam mengkoordinasi universitas – universitas di Yogyakarta dan sekitarnya untuk terhubung ke jaringan ke INHERENT.

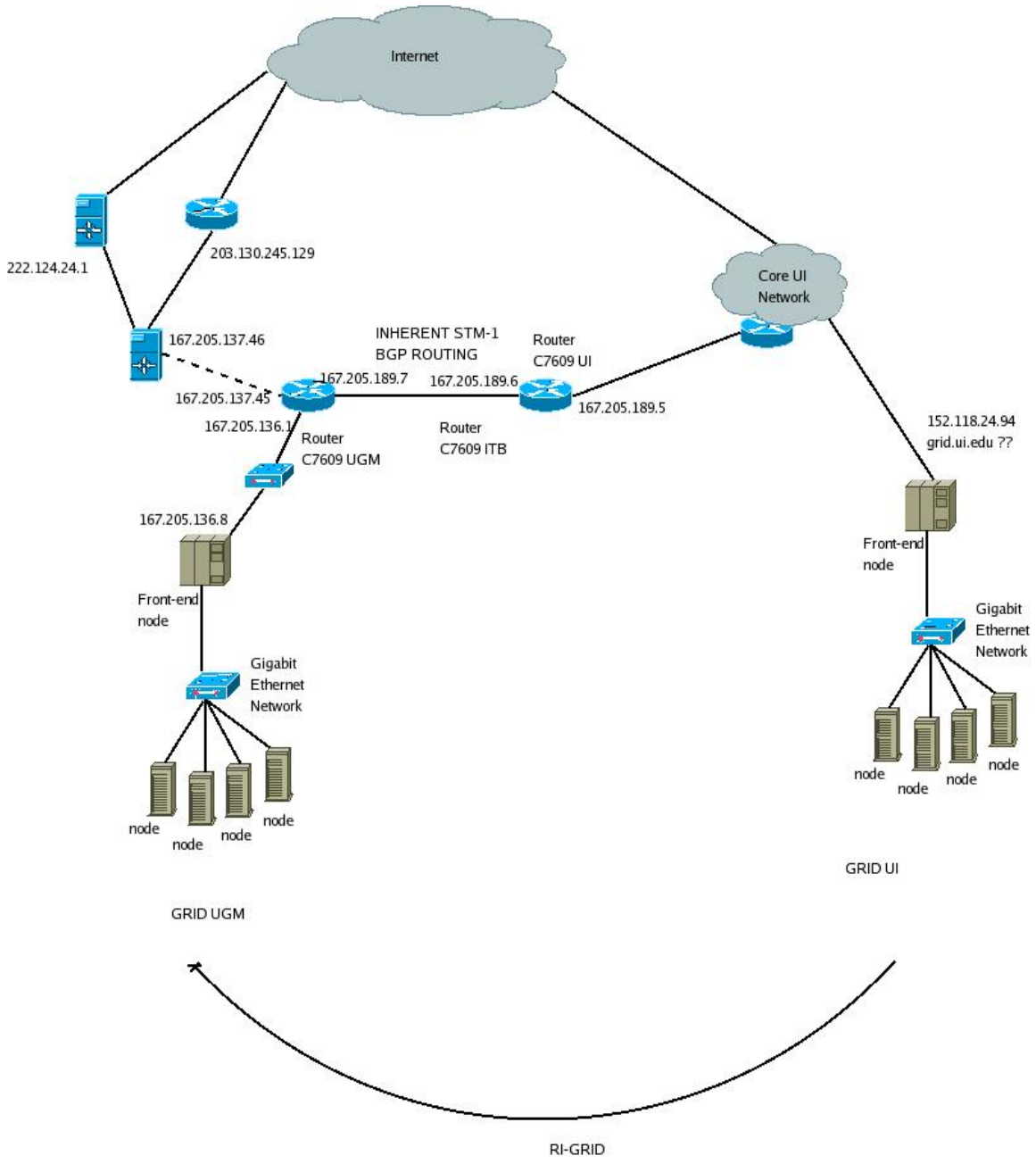
Resource – resource yang mungkin di share oleh universitas – universitas di Indonesia bisa berupa hasil riset, perpustakaan digital, e-learning dan beragam kontent antar universitas yang bisa saling melengkapi. Beberapa engineer TI di universitas yang terhubung ke INHERENT berencana membangun sebuah *grid computing* agar bisa sharing resource komputasi. Share resource komputasi ini bertujuan untuk membuat sebuah sistem *High Performance Computing (HPC)* yang diharapkan mampu memecahkan beragam permasalahan yang tidak bisa dipecahkan oleh proses komputasi tradisional menggunakan sebuah komputer.

0x01 - Grid Computing

Grid computing merupakan kumpulan node komputasi yang saling bekerja sama membentuk sebuah "*virtual supercomputer*". Node – node komputasi ini bisa terletak di beragam lokasi geografis yang berbeda dengan domain administrative yang berbeda juga. Beberapa universitas yang sedang mengembangkan komputasi grid adalah Institute Teknologi Bandung (ITB), Universitas Indonesia (UI), dan Universitas Gadjah Mada (UGM).

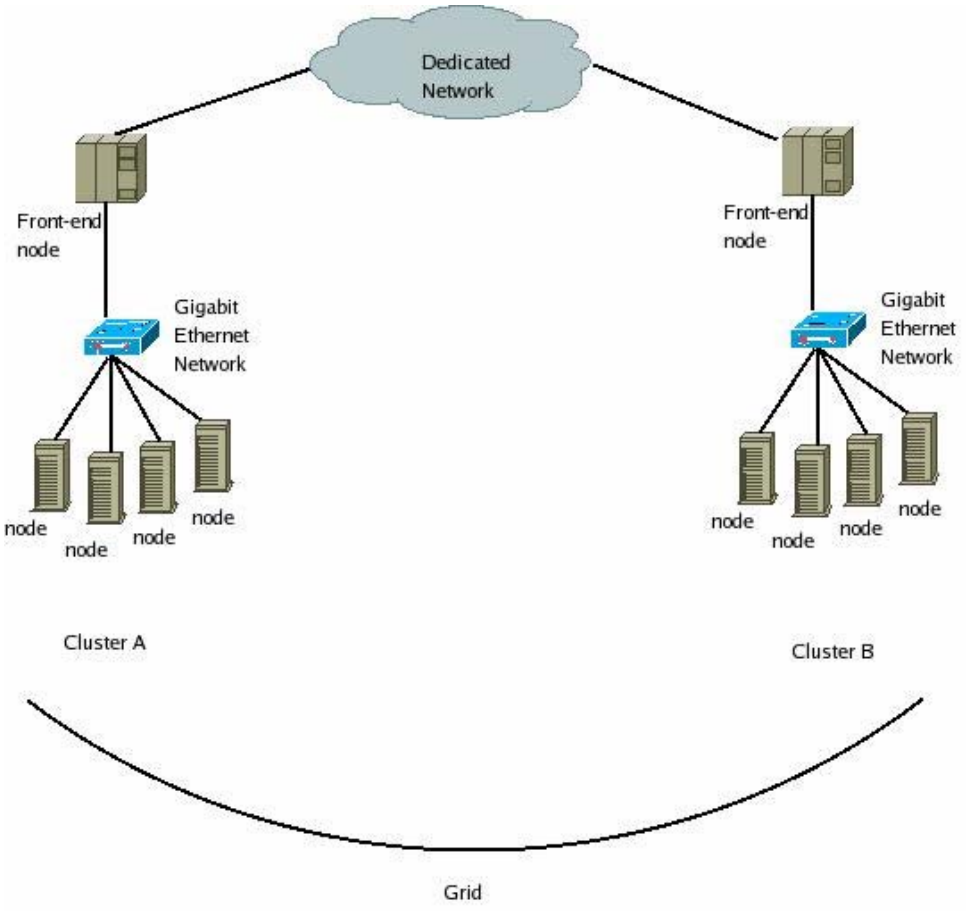
Portal pengembangan grid komputasi UI bisa di kunjungi di http://grid.ui.ac.id sedangkan UGM bisa di kunjungi di http://hpc.ugm.ac.id dan http://grid.te.ugm.ac.id . Kedua universitas ini berencana menggabungkan grid komputasinya yang nantinya disebut dengan inGRID. Gambaran secara umum bagaimana kedua grid komputasi milik UI dan UGM terhubung seperti terlihat pada gambar (i) di bawah ini.

Dalam komputasi grid digunakan *Certificate Authority* (CA) yang berguna untuk memastikan bahwa resource yang terhubung dalam grid atau user yang menggunakan resource komputasi grid adalah yang sah (*legitimate*). Certificate Authority pada dasarnya merupakan sertifikat digital yang berisi sebuah *public key* dan identitas owner. Beberapa aplikasi opensource untuk membuat *Certificate Authority* adalah OpenCA (http://openca.org), OpenXPKI (CA dalam Server Public Key Infrastructure – http://openxpki.org). Dalam grid computing CA dibuat menggunakan Globus SimpleCA yang sudah dibundle dalam Globus Toolkit (http://globus.org).



0x02 - Implementasi SimpleCA pada Grid Security

SimpleCA merupakan sebuah aplikasi terbundle dalam globus toolkit yang berfungsi untuk memberikan sertifikat digital. Dalam komputasi grid SimpleCA diimplementasi di masing – masing front-end node dari cluster komputasi.



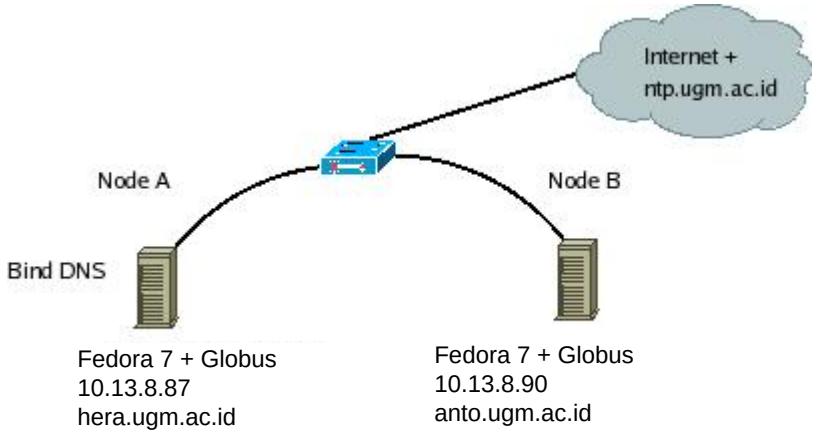
Pada gambar di atas terlihat sebuah grid komputasi yang terdiri dari dua buah cluster komputasi masing – masing cluster A dan cluster B. Cluster A dan cluster B mungkin saja terpisah secara geografis sehingga tidak ada yang menjamin hubungan kedua front-end adalah *trusted*. Untuk menghindari *untrusted communication* ini digunakanlah *Certificate Authority* (CA). Untuk mengimplementasi CA ada beberapa hal yang harus dilakukan sebelumnya yaitu :

- Sinkronisasi waktu dikedua front-end node, bisa dilakukan menggunakan *Network Time Protocol* (NTP) . Lakukan pengeditan seperlunya pada */etc/ntp.conf* atau gunakan unix command line *ntpdate*.
- Pastikan bahwa DNS *forward lookup* dan DNS *reverse lookup* telah bekerja dengan baik. Lakukan pengeditan pada zone file *named.conf*.

jika anda bukan pengelola nameserver jaringan, mintalah kepada admin yang menghandle *authority* DNS.

- Pastikan kedua front-end sudah terkoneksi dengan baik. Diperlukan *robust routing* untuk menjamin *connectivity* kedua front-end.

Untuk mensimulasikan bagaimana CA pada dua front-end bekerja, saya menggunakan dua buah PC yang terinstall Fedora dan globus toolkit. Arsitektur simulasi kedua front-end node sebagai berikut :



Node A mewakili front-end cluster komputasi A sedangkan node B mewakili front-end cluster komputasi B. Di mesin A selain terinstall feisty dan globus toolkit juga terinstall DNS server. (note : nama – nama domain hanya karangan saya saja tidak ada dijaringan produktif). Setelah dipastikan bahwa kedua node A dan node B terkoneksi dengan baik, saya mulai melakukan sinkronisasi waktu menggunakan unix command line *ntpdate* ke ntp.ugm.ac.id yang ber IP address 222.124.24.4.

Di node A

ntpdate 222.124.24.4

25 Jan 03:50:48 ntpdate[4185]: adjust time server 222.124.24.4 offset -0.004291 sec

date

Fri Jan 25 03:57:25 WIT 2008

Di node B

ntpdate 222.124.24.4

24 Jan 12:52:51 ntpdate[25586]: step time server 222.124.24.4 offset 10.094016 sec

date

Thu Jan 24 12:58:34 PST 2008

Mesin A menggunakan waktu WIT (*West Indonesian Time*) sedangkan mesin B menggunakan waktu PST (*Pasific Standard Time*) sehingga muncul perbedaan tanggal dan waktu namun kedua mesin telah disinkronisasi waktunya.

DNS server dikonfigurasi agar bisa melookup domain anto.ugm.ac.id dan hera.ugm.ac.id. Adapun konfigurasi DNS servernya sebagai berikut :

Potongan dari /etc/bind/named.conf

```
zone "ugm.ac.id" IN {
        type master;
        file "/etc/bind/data.ugm.ac.id";
};
zone "8.13.10.in-addr.arpa" IN {
        type master;
        file "/etc/bind/data.10.13.8.87.reverse";
};
```

Potongan dari /etc/bind/data.ugm.ac.id

```
hera    IN      A       10.13.8.87
anto    IN      A       10.13.8.90
```

Potongan dari /etc/bind/data.10.13.8.87.reverse

```
87      IN      PTR     hera.ugm.ac.id.
90      IN      PTR     anto.ugm.ac.id.
```

Di /etc/resolv.conf kedua mesin

```
nameserver 10.13.8.87
```

Lakukan di mesin A dan B

```
host hera.ugm.ac.id
hera.ugm.ac.id has address 10.13.8.87
host 10.13.8.87
87.8.13.10.in-addr.arpa domain name pointer hera.ugm.ac.id.
host anto.ugm.ac.id
anto.ugm.ac.id has address 10.13.8.90
host 10.13.8.90
90.8.13.10.in-addr.arpa domain name pointer anto.ugm.ac.id.
```

Konfigurasi *reverse* dan *forward lookup* telah berkerja dengan baik. Selanjutnya saya mulai melakukan installasi globus toolkit mengacu pada dokumetasi quickstart globus pada : http://www.globus.org/toolkit/docs/4.0/admin/docbook/quickstart.html. Waktu yang dibutuhkan untuk installasi dan kompilasi pada mesin Pentium 4 2GHz dengan memory 512 M sekitar 3 jam.

Installasi dan konfigurasi SimpleCA dimulai dari mesin hera.ugm.ac.id (Node A) dengan mengikuti petunjuk yang ada pada quickstart. Berikut ini resume step by step konfigurasi SimpleCA dan sedikit rekomendasi.

Gunakan user *globus* untuk mengeksekusi perintah – perintah berikut :

export GLOBUS_LOCATION=/usr/local/globus-4.0.5/

source $GLOBUS_LOCATION/etc/globus-user-env.sh

$GLOBUS_LOCATION/setup/globus/setup-simple-ca

(Enter PEM pass phrase as you wish misal 'zeusjuga')

(Lihat isi direktori ~/.globus/ dan ~/.globus/simpleCA/)

Gunakan user *root* untuk mengeksekusi perintah – perintah berikut :

$GLOBUS_LOCATION/setup/globus_simple_ca_6297b2b2_setup/setup-gsi -default

(Lihat is direktori /etc/grid-security/ dan /etc/grid-security/certificates/)

source $GLOBUS_LOCATION/etc/globus-user-env.sh

grid-cert-request -host hera.ugm.ac.id

(Parameter host gunakan FQDN – jangan mengunakan perintah *hostname*)

Gunakan user *globus* untuk mengapprove request certificate

grid-ca-sign -in /etc/grid-security/hostcert_request.pem -out hostsigned.pem

Gunakan user *root* untuk menyalin certificate yang telah di approve ke /etc/grid-security/

cp ~globus/hostsigned.pem /etc/grid-security/hostcert.pem

(Kita harus menyalin hostcert.pem dan hostkey.pem yang dimiliki *root* agar bias di baca oleh user *globus*)

cp hostcert.pem containercert.pem

cp hostkey.pem containerkey.pem

chown globus:globus container*.pem

(Sampai disini host certificate sudah selesai dikonfigurasi, sekarang saya hendak membuat user certificate untuk user *zeus*)

Gunakan user *zeus* untuk mengeksekusi perintah-perintah berikut :

export GLOBUS_LOCATION=/usr/local/globus-4.0.5

source $GLOBUS_LOCATION/etc/globus-user-env.sh

grid-cert-request

(Enter PEM pass phrase as you wish misalnya 'useruga')

cat ~zeus/.globus/usercert_request.pem | mail -s "request cert"

globus@hera.ugm.ac.id

Gunakan user *globus* untuk mengapprove request :

grid-ca-sign -in request.pem -out signed.pem

cat signed.pem|mail -s "approved cert" zeus@hera.ugm.ac.id

Gunakan user zeus untuk menyalin signed.pem ke ~zeus/.globus/

cp signed.pem ~zeus/.globus/usercert.pem

Gunakan user root untuk membuat /etc/grid-security/grid-mapfile sebagai berikut:

cat /etc/grid-security/grid-mapfile

"/O=Grid/OU=GlobusTest/OU=simpleCA-hera.ugm.ac.id/OU=ugm.ac.id/CN=zeus" zeus

(DONE)

Konfigurasi CA menggunakan SimpleCA di hera.ugm.ac.id (Node A) selesai. Konfigurasi SimpleCA di mesin anto.ugm.ac.id (Node B) sebagai berikut :

Gunakan user *globus* untuk menjalankan perintah – perintah berikut :

scp globus@hera.ugm.ac.id:.globus/simpleCA/ globus_simple_ca_6297b2b2_setup-0.19.tar.gz .

export GLOBUS_LOCATION=/usr/local/globus-4.0.5/

$GLOBUS_LOCATION/sbin/gpt-build globus_simple_ca_6297b2b2_setup-0.19.tar.gz

$GLOBUS_LOCATION/sbin/gpt-postinstall

Gunakan user root untuk mengeksekusi perintah – perintah berikut :

export GLOBUS_LOCATION=/usr/local/globus-4.0.5/

$GLOBUS_LOCATION/setup/globus_simple_ca_6297b2b2_setup/setup-gsi –default

(Lihat is direktori /etc/grid-security/ dan /etc/grid-security/certificates/)

source $GLOBUS_LOCATION/etc/globus-user-env.sh

grid-cert-request –host anto.ugm.ac.id

(Parameter host gunakan FQDN – jangan mengunakan perintah *hostname*)

Gunakan user *globus* untuk mengapprove request certificate

grid-ca-sign -in /etc/grid-security/hostcert_request.pem –out hostsigned.pem

Gunakan user *root* untuk menyalin certificate yang telah di approve ke /etc/grid-security/

cp ~globus/hostsigned.pem /etc/grid-security/hostcert.pem

(Kita harus menyalin hostcert.pem dan hostkey.pem yang dimiliki *root* agar bias di baca oleh user *globus*)

cp hostcert.pem containercert.pem

cp hostkey.pem containerkey.pem

chown globus:globus container*.pem

(Sampai disini host certificate sudah selesai dikonfigurasi, sekarang saya hendak membuat user certificate untuk user *zeus*)

Gunakan user zeus untuk mengeksekusi perintah – perintah berikut :

scp –r zeus@hera.ugm.ac.id:.globus ~zeus/

Gunakan user root untuk membuat /etc/grid-security/grid-mapfile sebagai berikut:

cat /etc/grid-security/grid-mapfile

"/O=Grid/OU=GlobusTest/OU=simpleCA-hera.ugm.ac.id/OU=ugm.ac.id/CN=zeus" zeus

(DONE)

Konfigurasi CA di kedua mesin Node A dan Node B yang dalam hal ini menggambarkan dua buah front-end node selesai. Untuk memastikan CA berjalan saya melakukan pengujian menggunakan GridFTP server. Lakukan installasi GridFTP server pada mesin anto.ugm.ac.id dan hera.ugm.ac.id dengan langkah - langkah silakan mengacu pada dokumen quickstart globus toolkit. Pengujian GridFTP sebagai berikut :

Di mesin hera.ugm.ac.id dengan menggunakan user *zeus*
source /usr/local/globus-4.0.5/etc/globus-user-env.sh
grid-proxy-init -verify –debug
(Masukkan PEM pass phrase untuk user zeus yaitu : userjuga)
Download /etc/passwd dari anto.ugm.ac.id
globus-url-copy gsiftp://anto.ugm.ac.id/etc/passwd file:///tmp/passwd-anto
head -2 /tmp/passwd-anto
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
Upload /etc/group ke anto.ugm.ac.id di folder /tmp/group-hera
globus-url-copy file:///etc/group gsiftp://anto.ugm.ac.id/tmp/group-hera
Jika semua berjalan lancar maka akan ada file /tmp/group-hera di mesin anto.ugm.ac.id

Lakukan pengujian serupa untuk mengupload dan mendownload file di mesin anto.ugm.ac.id. Jika tidak ada error saat proses penyalinan file menggunakan GridFTP berarti baik GridFTP maupun CA sudah terkonfigurasi dengan baik. Lakukan debugging mode penyalinan file jika terjadi error saat pengujian menggunakan GridFTP. Misalnya untuk mengetahui masalah penyalinan terkait dengan kegagalan CA dan domain, gunakan perintah berikut untuk melakukan analisis dalam mencari letak masalah.

```
globus-url-copy -vb -dbg -ss "`grid-cert-info -subject`" file:///etc/group
gsiftp://anto.ugm.ac.id/tmp/group-hera
```

0x03. Guidelines Implementasi Cetificate Authority pada Grid Komputasi UGM dan UI.

(I) Routing dan Konektifitas

Universitas Gadjah Mada dan Universitas Indonesia terhubung melalui jaringan INHERENT dengan kapasitas koneksi STM-1 155,5 Mbps menggunakan routing dinamik *Border Gateway Protocol* (BGP). Mesin hpc.ugm.ac.id (167.205.136.8) langsung terhubung ke router INHERENT dengan *default gateway* 167.205.136.1 pada jaringan 167.205.136.0/27. IP ini harus diadvertise di router INHERENT Cisco 7609.

```
router bgp 65005
  network 167.205.136.0 mask 255.255.255.224
```

Hasil traceroute dari hpc.ugm.ac.id ke grid.ui.edu dan dari lg.ui.edu ke hpc.ugm.ac.id sebagai berikut :

```
traceroute grid.ui.edu
traceroute to grid.ui.edu (152.118.24.94), 30 hops max, 38 byte packets
 1  167.205.136.1 (167.205.136.1)  0.716 ms  0.418 ms  0.289 ms
 2  pos1-0-1-stm1-bb-v4-itb-ugm.inherent-dikti.net (167.205.189.6)  7.050 ms  6.957 ms  6.945 ms
 3  pos1-0-1-stm1-bb-v4-ui-itb.inherent-dikti.net (167.205.189.4)  11.169 ms  11.134 ms  11.131 ms
 4  ui-inherent.gw.ui.ac.id (152.118.255.249)  11.074 ms  11.077 ms  11.059 ms
 5  * * *
(paket di drop oleh ui-inherent gateway)
```

```
traceroute to hpc.ugm.ac.id (167.205.136.8), 30 hops max, 40 byte packets
 1  ui-external.gw.ui.ac.id (152.118.24.1)  1.360 ms  0.136 ms  0.123 ms
 2  inherent-ui.gw.ui.ac.id (152.118.255.250)  0.423 ms  0.322 ms  0.298 ms
 3  pos1-0-0-stm1-bb-v4-itb-ui.inherent-dikti.net (167.205.189.5)  4.560 ms  4.502 ms  4.476 ms
 4  pos1-0-0-stm1-bb-v4-ugm-itb.inherent-dikti.net (167.205.189.7)  11.293 ms  11.209 ms  11.213 ms
 5  167.205.136.8 (167.205.136.8)  11.203 ms  11.237 ms  11.238 ms
```

(II) Sinkronisasi Waktu

Sinkronisasi waktu menggunakan *Network Time Protocol* (NTP) diarahkan ke ntp.ui.edu (152.118.24.8) menggunakan perintah *ntpdate*.

```
ntpdate ntp.ui.edu
echo “ntpdate ntp.ui.edu” >> /etc/rc.local
```

(III) Konfigurasi DNS

Authority *lookup forward* hpc.ugm.ac.id dihandle ns1.ugm.ac.id yang dikelola oleh admin UGM Bapak Agung Ariansyah ,S.Kom. Authority *reverse forward* dikelola oleh admin ITB. Sampai saat ini *reverse forward* belum didelegasikan oleh ITB ke UGM sehingga proses konfigurasi *Certificate Authority* (CA) masih belum terselesaikan. Di sisi UI, grid.ui.edu baik *forward* maupun *reverse lookup* sudah terhandle dengan baik.

```
host grid.ui.edu
grid.ui.edu has address 152.118.24.94
host 152.118.24.94
94.24.118.152.in-addr.arpa domain name pointer grid.ui.ac.id.
host hpc.ugm.ac.id
hpc.ugm.ac.id has address 167.205.136.8
host 167.205.136.8
;; connection timed out; no servers could be reached
```