**3413ICT Network Security - Lab 4 griffith_logo**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Firewalls**

Firewalls  are  a  network  access  control  system  that  divides  a  network  that  we  presume

it’s  secure  from  a  network  that  may  be  unsecure.  Although  it  can  control  the  ingoing

and   outgoing   traffic,   the   most   common   usage   of   firewalls  is   to   control   the   ingoing

traffic.  Note  that  Firewalls do  not  provide any  security  from  internal  attacks.

**Network Firewalls (packet filtering)**

Routers  can control  the  IP  packets  that  go  across  them  by  accepting/denying  traffic

according  to  policies  affecting  to  protocol  headers  (IP,  ICMP,  UDP,  TCP).  We  can

analyze  source/destination  addresses  and  ports,  protocol  types,  packet  contents  and

size,  etc.  There  are  two  general  policies:  a)  accept  all  packets  except  for  a  finite  set  of

cases,  and  b)  deny  all  traffic  except  for  a  finite  set  of  cases.  Case  b  is  more  difficult  to

implement,  but  it is generally more  recommendable.

Each  packet  reaching  the  device  will  lookup  the  filtering  rules  and  stop  at  the  first

match,  and  after  that  will  decide  the  decision  of  either  denying  or  accepting  the  traffic.

A  default  policy is always set.

**Proxies (Application Gateways)**

They   behave   as   Application-level   retransmission   devices.   Network users   establish   a

communication  with  the  proxy,  thus  dividing  the  source-destination  connection  in  two

independent  connections  (source-firewall   and  firewall-destination).  The  proxy  server

manages the  requested  connections .

This   technology   has   a   slower   performance   that   network   firewalling   because   it   is

working  on  the  upmost  OSI  layer.  It  is usual  to  use both  firewalls at  the same  time.

Cache   Proxies   are   a   popular   way   to   increase   performance   by   storing   the   data   the

gateway  transmits  into  the  firewall,  so  it  is  not  necessary  to  lookup  in  the  Internet  for

the  same  data  next  time  another  computer  requests  it.

**Lab Description**

*Lab 4*has   two   departments,   each   one   with   its   own   network   (LAN1  and

LAN2), trying to access a database server where a database with customers

information   is   stored,   and   an   e-mail   and   HTTP   server.   At   the   same   time,   some

company  guys  are  using  illegal  multimedia  downloading,  and  so  slowing  the  Internet

link  performance.  The  company  is  requesting  to  set  up  a  Firewall  to  avoid  multimedia

traffic  in  order to decrease  the  mean  database  access  time  to  a  1  sec  threshold.

**Creating the Scenario**

1. Open   OPNET   IT   Guru   Academic   Edition:   (**File 🡪** **New   Project**)   using   the following

parameters  (use  default  values  for  the  remainder):

 Project  Name:   <your\_name>\_  Firewall

 Scenario Name:   NoFirewall

 Network  Scale:   Campus

 Size:   100x100  meters

Press**Next** several  times until  we finish  the Startup  Wizard.

1. Network  creation:

We  create  the  scenario  of  picture  L4.1.   The  components  that  are  used  and  the

palette   where   they   can   be   found   in   the**Object   Palette**   are   summarized   in

Table  L4.2.



**L4.1 The Scenario**

****

**L4.2 Components List**

**Right  click**  on  every  node,  click  on**Set  Name**  and  write  the  same  names  as

seen  in  the  picture.

1. Setting  up  the**Application Config**  control:

Select  the  Application  Config  control,  and  go  to**Edit  Attributes**.  All  we  need  to

modify  are  the  Application  Definitions.  Delete  all  the  applications  that  may  be

defined  (tip:  set**rows:  0**),  and  create  4  applications  as  seen  in  the  picture  (set

**rows:  4**  and  edit  the  four  applications  as  seen  in  the  picture  L4.3).  First  step  is

to   change   the   Name:**Email,   HTTP,   DB   and   MusicAndVideo.**   Change   the

application load  afterwards:

 HTTP:   Permits  HTTP  (Light  Browsing).

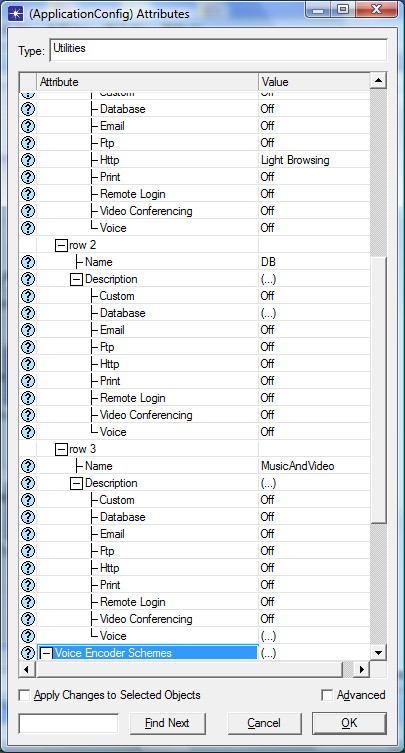
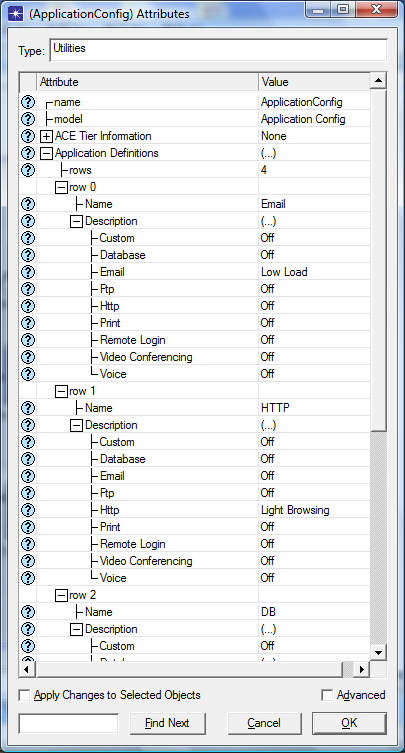
 Email:   Permits  Email  (Low Load)

These  two  applications  can  be  configured  automatically  by  double-clicking  on

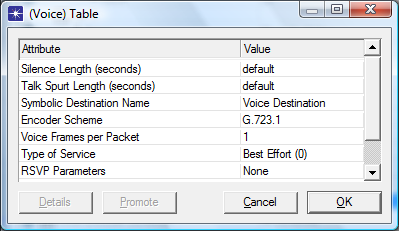
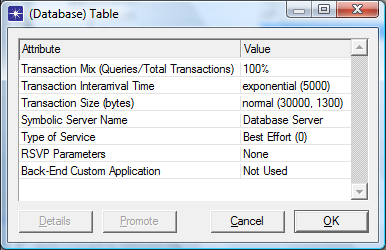
the  corresponding  fields.  To  configure**MusicAndVideo**  and**DB**,  double-click

on   the   fields   of   picture   L4.3   marked   with   the**(...)**   symbol:**DB 🡪** **Database,**

**MusicAndVideo 🡪 Voice**, and  then  set  the  values  as  in  pictures L4.4  and  L4.5.



**L4.3 Application Config Attributes**



**L4.4   and L4.5 Configuring the application traffic**

Select  the  control**Profile  Config**  and  use  the**right  button**  to  click  on**Edit**

**Attributes** and  create  4  profiles:

 **EMailProfile**,  to admit  Email  application

 **WebBrowser**, to admit  HTTP application

 **BDProfile**,  to  admit  DB  application

 **MusicAndVideoProfile**,   to  admit  MusicAndVideo  application

We  have  to  do  the  same  steps  as  before:  Set  0  rows  to  erase  all  rows  we  may

have,  and  then  set  4  rows  to  program  the  four  applications,  and  deploy  each

row   and   set   the   values   as   seen   on   pictures.   The   hierarchies   that   are   not

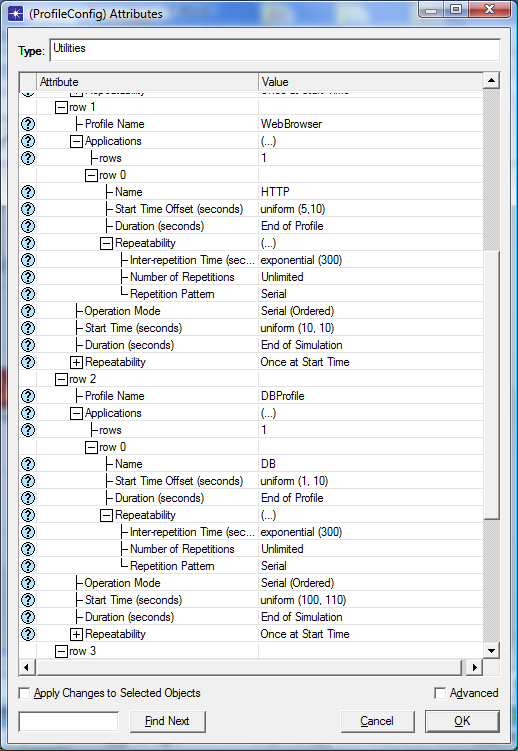
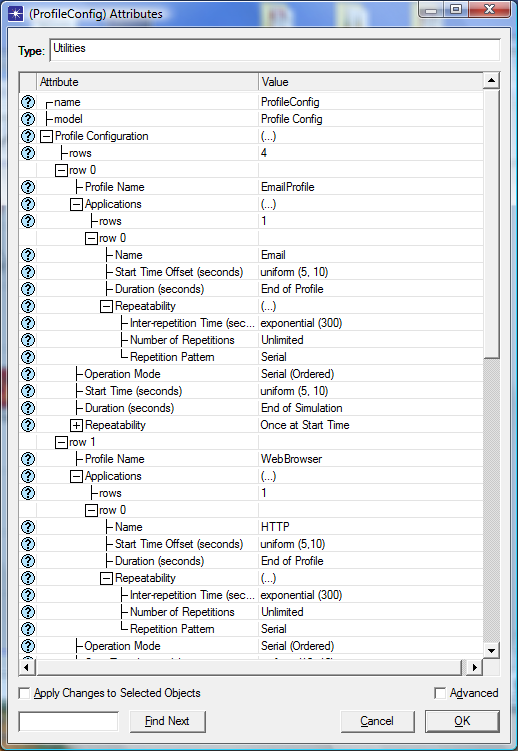
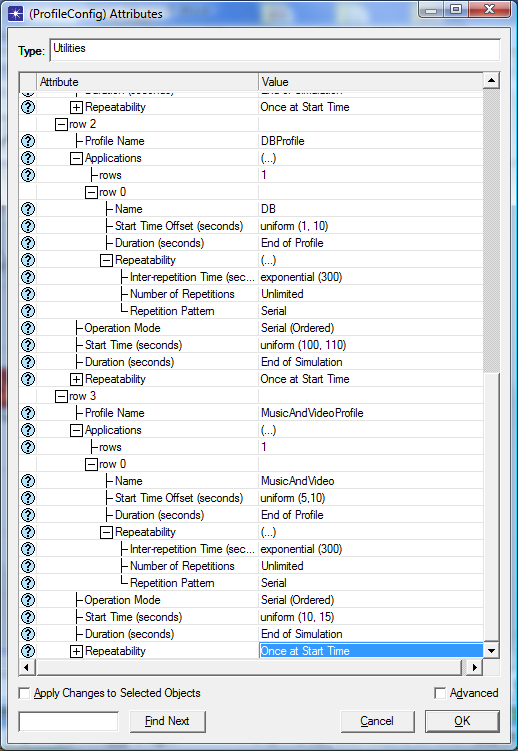
deployed   on   pictures   use   default   values.   Applications   can   be   appended   to

profiles  adding  new  rows  to  the  Applications  field,  and  setting  the  field**Name**

on  every**row 0**  of  the  Applications  branch.  We  can  also  modify  the**Start  Time**

of  all  Applications  and  Profiles  (packet  reception  distribution),  the**Operation**

**Mode**, and  the**Repetition Pattern**.

**L4.6 Configuring Profile Config**

1. Setting  up  the Firewall:

This  first  scenario  permits  the  voice  traffic.  Picture  L4.7  shows  the  main  options

to  be  configured  in  the  router. The  attributes to  modify  are  the  following:

 Address   and   Subnet   Mask:   AutoAssigned   on   all   rows   of**IP   Routing**

**Parameters 🡪** **Interface Information** and **IP Routing** **Parameters 🡪**

**Loopback Interfaces**.

 We need to set up the routing protocol OSPF: **OSPF** **Parameters 🡪**

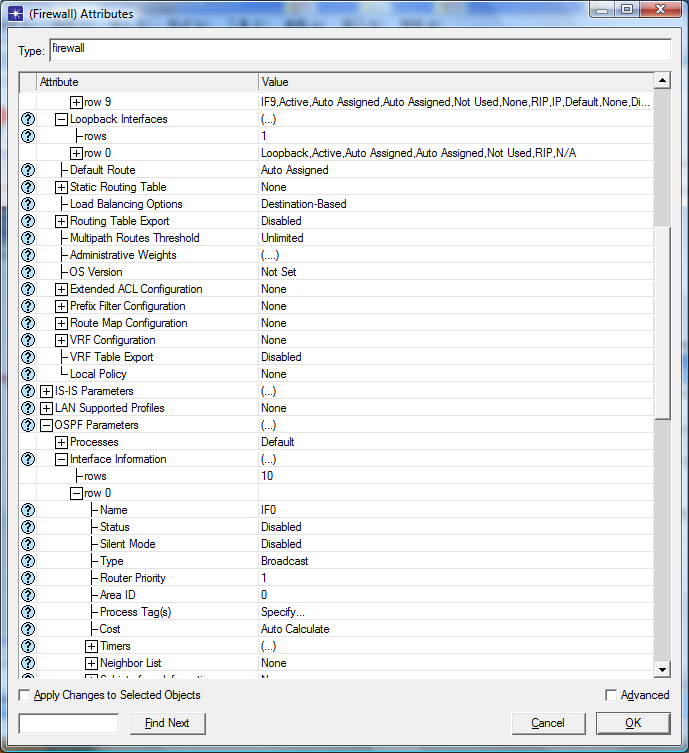
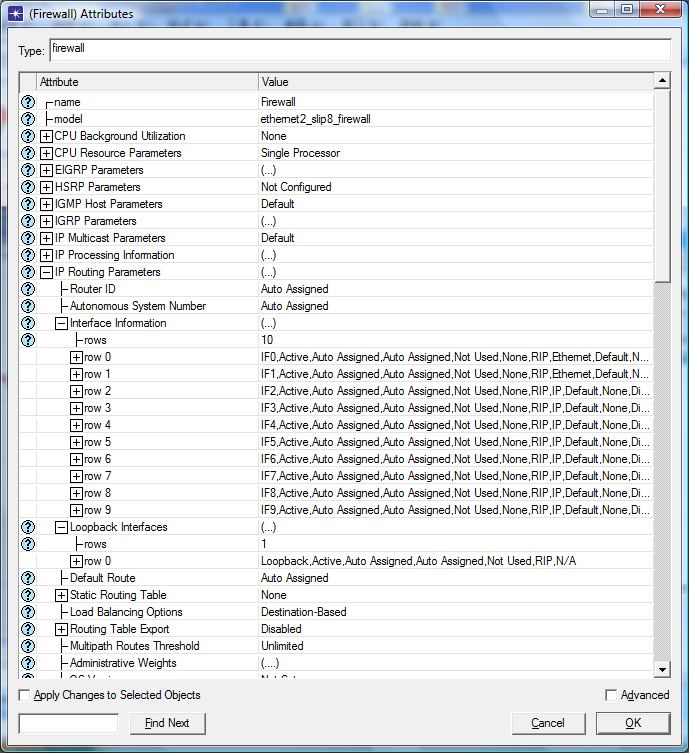
**Interface   Information 🡪** **row   0**   and**row   1**   (the   unique router  interfaces) **🡪**

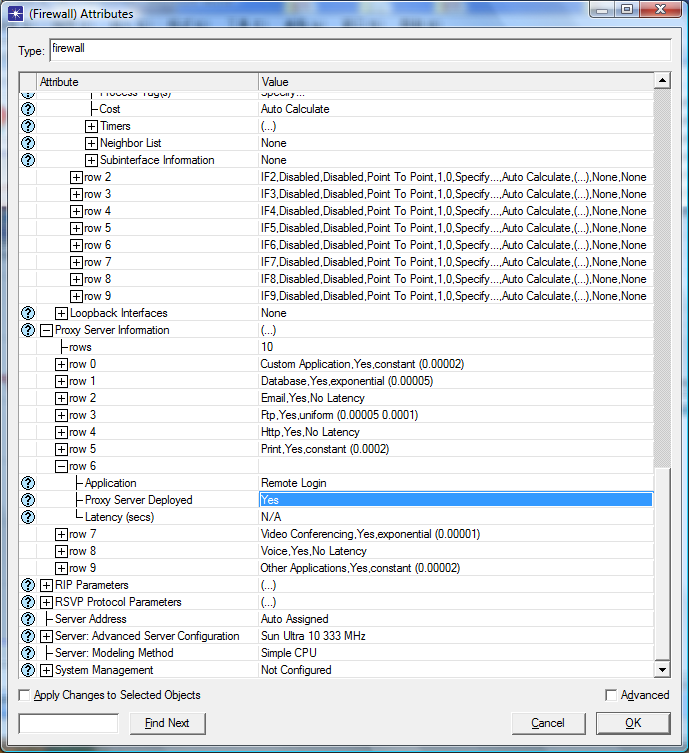
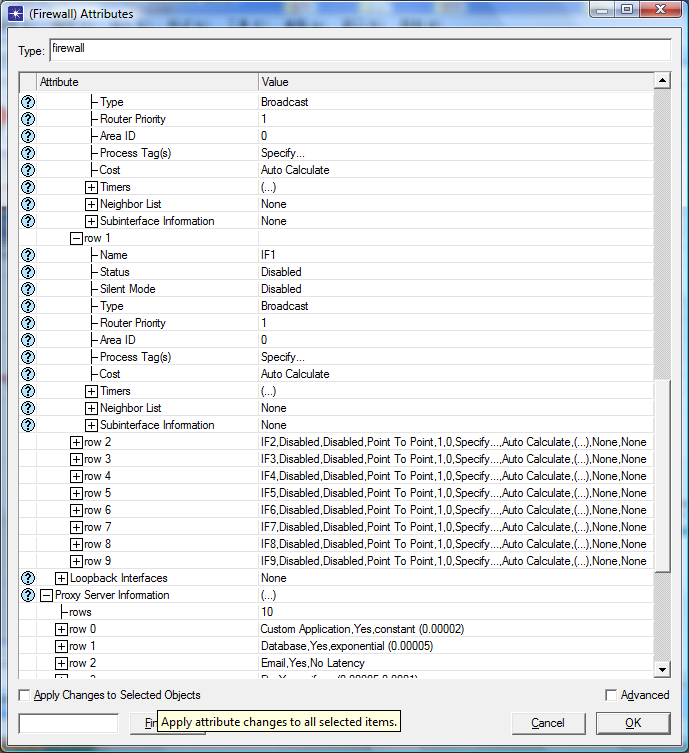
**Type:  Broadcast**.  Set**Point  to  Point**  to  the  remainder (rows 2  –  9)  .

 **Proxy  Server  Information 🡪** **row  6**  (corresponds  to**Application  Remote**

**Login,**   necessary   for   Database   access) **🡪** **Proxy   Server   Deployed:   Yes**,

this ensures  that  database traffic has  the  right  to pass.





**L4.7 Configuring the  Firewall**

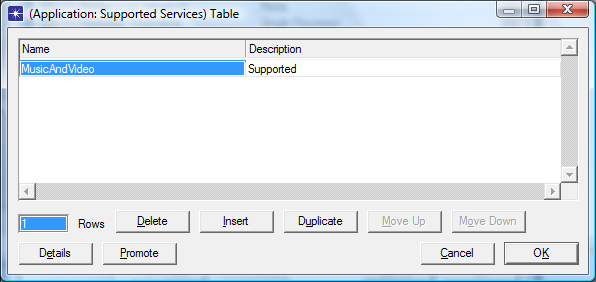
1. Setting  up  MusicAndVideoServer:

Right  click  on  the MusicAndVideoServer  and  click  on**Edit  Attributes**.

We   have   to   modify   the   Application:**Supported   Services**,   by   setting   the

parameters  as  seen  in  the  picture  below  (we  need  to  set  rows:  1  to  accept

MusicAndVideo).  Leave  the  remainder options  with  default  values.



**L4.8 MusicAndVideoServer supported Services**

1. Setting  up  the DBServer and  WebAndEmailServer:

This  server **Supported  Services**  have  to  be  set  as seen  in  the  picture  below:

|  |  |
| --- | --- |
| **Server** | **Supported Services** |
| **DBServer** | DB |
| **WebAndEmailServer** | HTTP  Email |

**L4.9 Supported Services**

1. Configuring  LANs:

Select**LAN 1**  by  clicking  on  it,  and  then**right button 🡪** **Edit  Attributes.**

Use the values from picture L4.10 (non-deployed branches use default

parameters). This  configuration  will  use  250  workstations  for  each  and  every

LAN  (**Number  of  Workstations**),  5  of  them  will  be  doing  web  browsing,  5  will

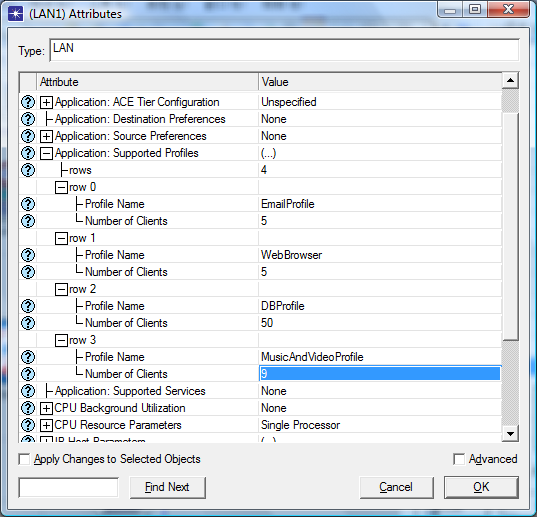
be using email, 50 attempting to connect to the database and 9 using

MusicAndVideoServers illegally (**Application:** **Supported** **Profiles**). When

finished,  click on**OK**.

LAN  2  will  be  configured  with  the  same  values.  Use  Copy  &  Paste  to  duplicate

the  LAN  and  change  the   name  afterwards.



**L4.10  Assigning profiles to workstations at  LAN 1**

1. Internet-Firewall  link configuration:

**Right-click**  on  the  link  and**Edit  Attributes**.  Set**Data Rate**:**T1**.

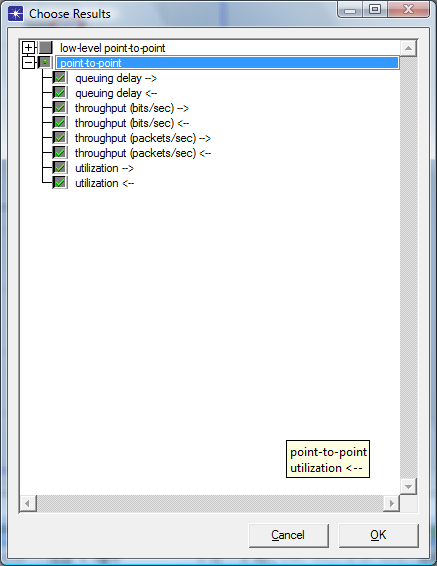
1. Configuring  the  simulation  statistics:

The   performance   and   throughput   statistic   parameters   can   give   interesting

information,  as well  as the  DB  Query  delay:

 **Right  click**  on  the  Internet-Firewall  link **🡪 Choose  Individual  Statistics**

and  mark the checkboxes as in  picture L4.11.  Click**OK**.

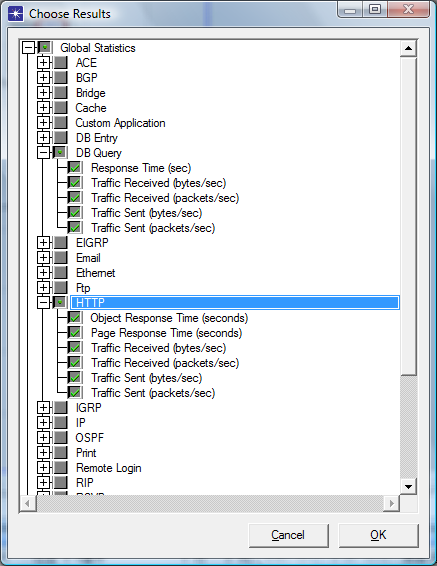


**L4.** **11 Internet-Firewall link  statistics**

 In  order  to  choose  the  DB  Query  simulation  statistics,**right  click**  anywhere

else  in  the  grid  except  of  a  node,  select**Choose  Individual  Statistics**  and

check the  fields as in  picture  L4.12.  Click**OK**.



**L4.12 Global statistics**

To  check  all  the  son  statistics  of  a  parent  node,  click  on  the  parent  node  and

then  all  the  son  nodes  will  be check  marked.

10. Configuring  the simulation:

From the Project Editor, click on **configure/run** **simulation**, set

**Duration: 1 hour(s)**.   Don’t  start  the  simulation  yet.

**Creating the second scenario**

The  second  scenario  is  a  duplicate  of  the  first,  but  with  some  router  rules  avoiding

particular  packets  from  and  to  music  and  data  services.  Later  on  we  will  see  how  this

decreases  the  internet  link  throughput  and  database  access  time  fair  enough  below

the 1  second  limit.

From the **Project** **Editor**, **Scenarios 🡪** **Duplicate** **Scenario**... Rename the new

scenario:**WithFirewall**,  and**right  click**  on**Firewall**  and**Edit  Attributes**.  Leave  all

the values as they are, except the **Proxy** **Server** **Information 🡪** **row** **8**

(**Application Voice** data),  using**Proxy Server Deployed**: **No**.

**Results Analysis**

Run  all  the  simulations  of  the  scenarios,  and  take  a  look at  the  graphics:

1. At   the**Project  Editor**,**Scenarios** 🡪**Manage   Scenarios...**   and   configure   the

simulation parameters as seen in the picture, setting **<collect>** on the

**Results**  row  on  both  scenarios   (use**<recollect>**  if  this  is  not  the  first  time

you  run  the  simulation).  Click**OK**.

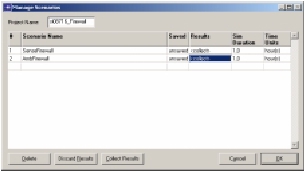
1. Compare  the**DB  Query  Response Time**  by**right-clicking**  on  the  Grid  on  any

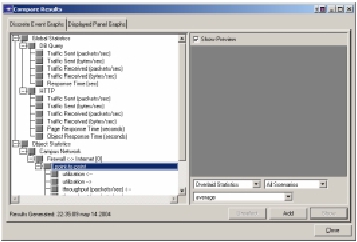
scenario and **Compare** **Results.** Now we can browse in all the general

statistics  we  programmed  before  in  the  left  side  tree.  Check  out  that**Overlaid**

**Statistics**,**All Scenarios** and**average**  options  are  marked.

**L3.13 Manage Scenarios**





**L4.14 Compare Results**

**Questions**

**Question 1**

Compare the DB Query Response time (sec). Can you see a significant improvement  when  the  firewall  is  implemented  at  the  proxy?

**Question 2**

Compare   the   point-to-point   throughput   (packets/sec)   in   any   direction   of   the

Firewall-Internet  link. How  is  the  non-illegal  applications  effective  bandwidth  affected

by the proxy?

**Question 3**

Compare  the  utilization  of  the  same  link.  What   changes  do  you   appreciate?