RHODES UNIVERSITY
Grahamstown • 6140 • South Africa

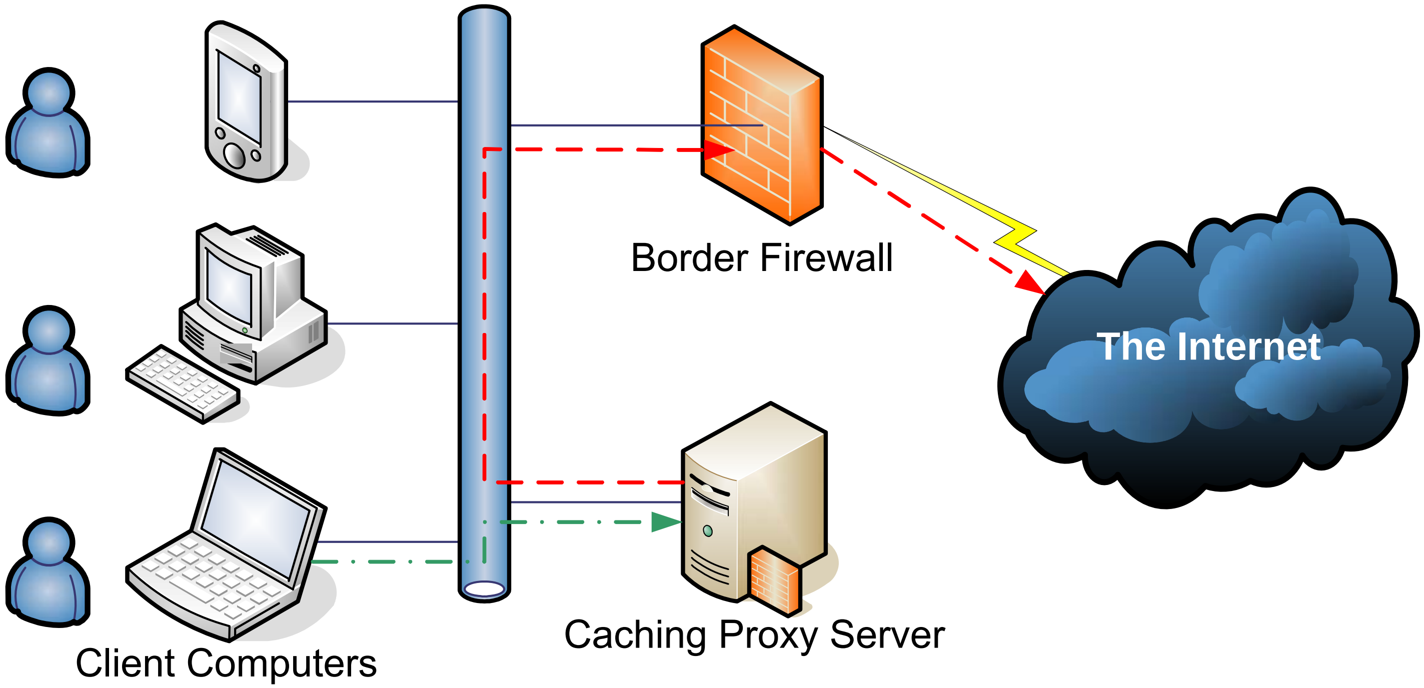
Bandwidth Management with the Squid Caching Proxy Server

Guy Antony Halse
<G.Halse@ru.ac.za>

Quick Overview of Squid

- Squid is a caching proxy server.
- It’s the open-source equivalent of products like Novell’s BorderManager, Microsoft’s ISAS, and Cisco’s ACNS.
- You can download it for free at http://www.squid-cache.org/

How Squid Fits Into Your Network



Bandwidth Control Features in Squid

- Access Control Lists
- Redirectors
- Authenticators
- Delay Pools

We'll talk about each of these in turn, and then look at some examples that show how they can all fit together

Access Control Lists

- Traditionally used to define who can access what …

```
acl all src 0.0.0.0/0.0.0.0
acl RHODESIP src 146.231.0.0/16
acl RHODESDNS srcdomain .ru.ac.za
acl ACZADEST  dstdomain .ac.za

http_access deny all !RHODESIP !RHODESDNS
http_access allow ACZADEST
http_access deny all
```

Access Control Lists

- But in reality have a lot more flexibility

`acl ACLNAME` *`keyword`* where keyword is one of:

```
   arp
   srcdomain, dstdomain, src, dst
   time
   url_regex, url_path, urllogin, port, proto, method
   brower, referer_regex
   proxy_auth, proxy_auth_regex, ident, ident_regex
   src_as, dst_as
   req_mime_type, req_header, rep_mime_type, rep_header
   myip, myport
   external
```

Access Control Lists

- Which allows us to write rich rule sets to match our needs
- e.g. All student public labs are only allowed to access academic sites during working hours.

```
acl PUBLICLAB src 146.231.104.0/21
acl WORKHOURS time MTWTF 08:00-17:00
acl ACADEMIC dstdomain .ac.za .edu .ac.uk
http_access deny PUBLICLAB WORKHOURS !ACADEMIC
http_access allow PUBLICLAB
```

Redirectors

- Redirectors allow us to re-write URLs before we fetch them
- For instance, we could rewrite a popular site to a local mirror:

http://www.php.net/ → http://za2.php.net/

Redirectors

- Redirectors are simple programs and can be easily customised:

```
#!/usr/bin/perl -w
while (<STDIN>) {
       s{^http://www.php.net}{http://za2.php.net};
       print;
}
```

- And added to Squid:

```
redirect_program /usr/local/bin/myredirector
redirector_access allow all
```

Redirectors

- Redirectors are commonly used to block adverts on web pages.
- There are lots of open-source packages that do this, for example AdZapper (http://adzapper.sourceforge.net/)
- Advert blocking saves bandwidth but is controversial because many sites rely on advertising for revenue.

Redirectors

- Redirectors offer a lot of control over content

  BUT

- You can only have one redirector, so you have to think carefully what you want to do with it

Authenticators

- Authenticators are external programs that define how the `proxy_auth` ACL works.
- This lets you force your clients to supply a username and password before granting them access – good for public access computers.
- Like redirectors, you can only have one authenticator. That's not usually a problem though.

Authenticators

- Authenticators are also simple programs that read from STDIN and write to STDOUT.

```
guy@walrus:~% ./sampleauthenticator
guy notmypassword
ERR
ghalse mypassword
ERR
guy mypassword
OK
```

Authenticators

- Squid comes with a lot of authenticators out-the-box: smb, ldap, pam, unix, ntlm, yp/nis, etc.
- Perhaps the most useful of these is `pam_auth` which uses the pluggable authentication module architecture.
- PAM allows you to chain authenticators and use multiple authentication sources.

Delay Pools

- Delay pools are Squid’s answer to bandwidth management.
- They allow you to control the amount of bandwidth a particular computer, subnet or proxy server may use.

Delay Pools

- Delay Pools work like a bucket and a tap.
- You can empty the bucket as fast as you like, but it can only fill as fast as the tap will let it.
- So important variables are the size of the bucket and the rate at which it refills.

Pic: http://www.wildlife-art.co.nz/

Delay Pools

- Squid defines three types of buckets
  - aggregate

    an aggregate bucket applies to the whole proxy server
  - network

    a network bucket applies to the user’s class C network (/24, i.e. third octet of IP address).
  - individual

    an individual bucket applies to the user’s PC (i.e. the fourth octet of an IP address)

Delay Pools

- These buckets combine into three classes of delay pool:
  - Class 1

    has only an aggregate bucket
  - Class 2

    has an aggregate bucket and an individual bucket
  - Class 3

    has aggregate, network and individual buckets

Delay Pools

- For each bucket we define a restore rate (B/s) and a maximum size (B).

```
delay_pools 1
delay_class 1 2
delay_parameters 1 -1/-1 8000/8000 600/8000
```

- We use -1 to signify “unlimited”
- The maximum size is important as it specifies the burst bandwidth available – this can be used to penalize only certain types of download.

Delay Pools

- We use ACLs to define who gets put into which delay pools.
- e.g. All residence machines are subject to bandwidth controls

```
acl RESIDENCES src 146.231.136.0/20
acl all src 0.0.0.0/0

delay_pools 1
delay_class 1 2
delay_parameters 1 -1/-1 8000/8000 600/8000

delay_access 1 allow RESIDENCES
delay_access 1 deny all
```

Examples and Case Studies

Advert Blocking

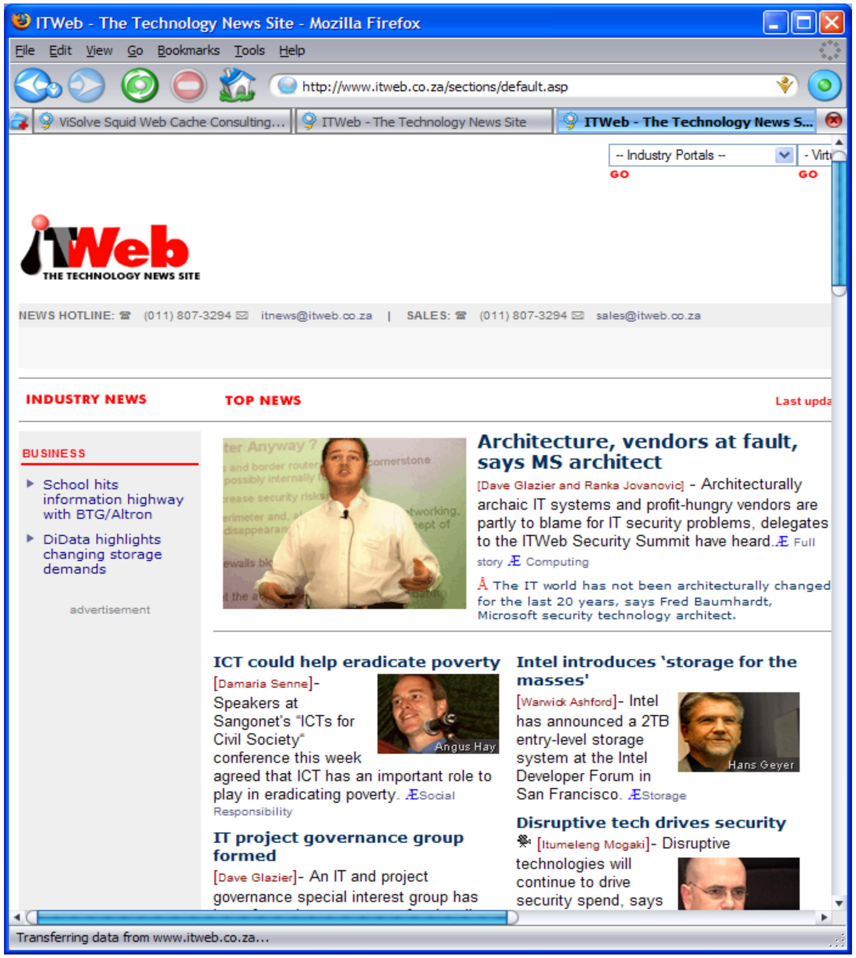
- Advert blocking saves bandwidth, but
- School of Journalism needs adverts to teach new media

```
http_port cache.ru.ac.za:3128
http_port adcache.ru.ac.za:3128

redirect_program /usr/local/bin/adzapper
acl ADCACHE myip adcache.ru.ac.za
redirector_access deny ADCACHE
redirector_access allow all
```

- Caches bind two IP addresses and only block adverts on one.
- Clients choose whether they want adverts or not.

Advert Blocking



ITWeb - The Technology News Site - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.itweb.co.za/sections/default.asp

ViSolve Squid Web Cache Consulting...
ITWeb - The Technology News Site
ITWeb - The Technology News S...
-- Industry Portals --
- Virt
GO
GO
THE TECHNOLOGY NEWS SITE

NEWS HOTLINE: ☎ (011) 807-3294 ✉ itnews@itweb.co.za | SALES: ☎ (011) 807-3294 ✉ sales@itweb.co.za

INDUSTRY NEWS TOP NEWS Last upda

BUSINESS

- School hits information highway with BTG/Altron
- DiData highlights changing storage demands

advertisement

Architecture, vendors at fault, says MS architect

[Dave Glazier and Ranka Jovanovic] - Architecturally archaic IT systems and profit-hungry vendors are partly to blame for IT security problems, delegates to the ITWeb Security Summit have heard. Æ Full story Æ Computing

Å The IT world has not been architecturally changed for the last 20 years, says Fred Baumhardt, Microsoft security technology architect.

ICT could help eradicate poverty

[Damaria Senne]- Speakers at Sangonet's "ICTs for Civil Society" conference this week agreed that ICT has an important role to play in eradicating poverty. ÆSocial Responsibility

IT project governance group formed

[Dave Glazier]- An IT and project governance special interest group has

Intel introduces 'storage for the masses'

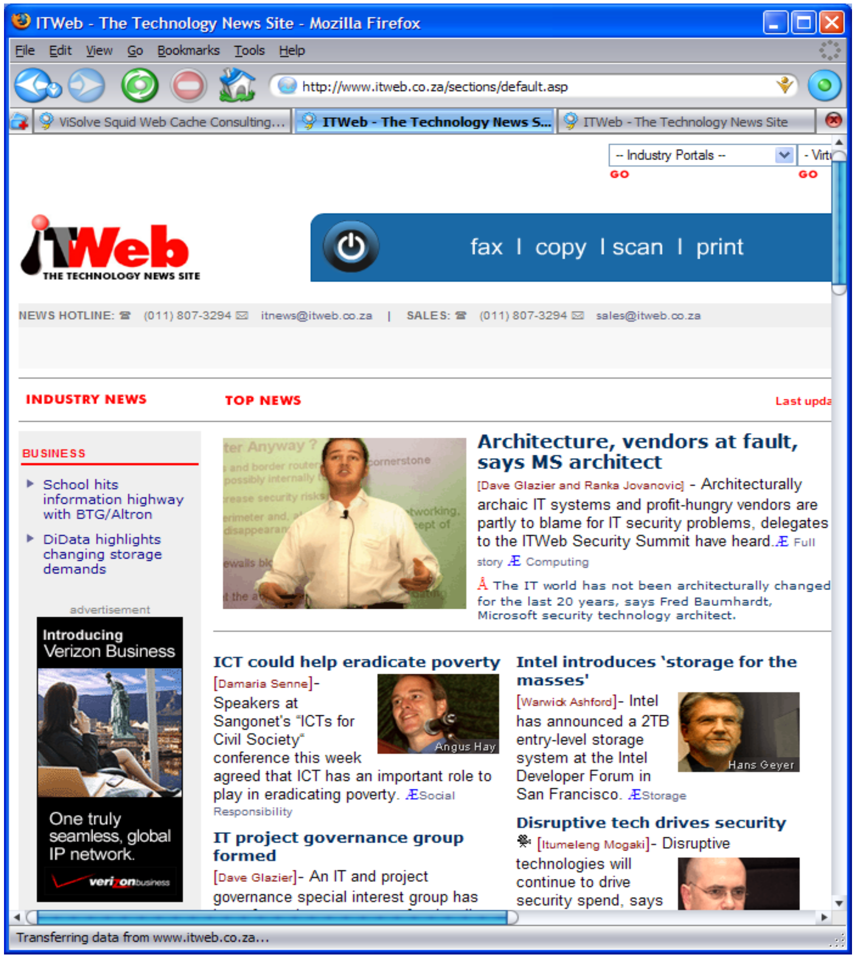
[Warwick Ashford]- Intel has announced a 2TB entry-level storage system at the Intel Developer Forum in San Francisco. ÆStorage

Disruptive tech drives security

[Itumeleng Mogaki]- Disruptive technologies will continue to drive security spend, says

Transferring data from www.itweb.co.za...

cache.ru.ac.za



ITWeb - The Technology News Site - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.itweb.co.za/sections/default.asp

ViSolve Squid Web Cache Consulting... ITWeb - The Technology News S... ITWeb - The Technology News Site

-- Industry Portals -- - Virt GO GO

THE TECHNOLOGY NEWS SITE

NEWS HOTLINE: ☎ (011) 807-3294 ✉ itnews@itweb.co.za | SALES: ☎ (011) 807-3294 ✉ sales@itweb.co.za

INDUSTRY NEWS TOP NEWS Last upda

BUSINESS

- School hits information highway with BTG/Altron
- DiData highlights changing storage demands

advertisement

Architecture, vendors at fault, says MS architect

[Dave Glazier and Ranka Jovanovic] - Architecturally archaic IT systems and profit-hungry vendors are partly to blame for IT security problems, delegates to the ITWeb Security Summit have heard. Æ Full story Æ Computing

Å The IT world has not been architecturally changed for the last 20 years, says Fred Baumhardt, Microsoft security technology architect.

ICT could help eradicate poverty

[Damaria Senne]- Speakers at Sangonet's "ICTs for Civil Society" conference this week agreed that ICT has an important role to play in eradicating poverty. ÆSocial Responsibility

Angus Hay

IT project governance group formed

[Dave Glazier]- An IT and project governance special interest group has

Intel introduces 'storage for the masses'

[Warwick Ashford]- Intel has announced a 2TB entry-level storage system at the Intel Developer Forum in San Francisco. ÆStorage

Hans Geyer

Disruptive tech drives security

[Itumeleng Mogaki]- Disruptive technologies will continue to drive security spend, says

Transferring data from www.itweb.co.za...

adcache.ru.ac.za

Quota System @ Rhodes

Quota System @ Rhodes

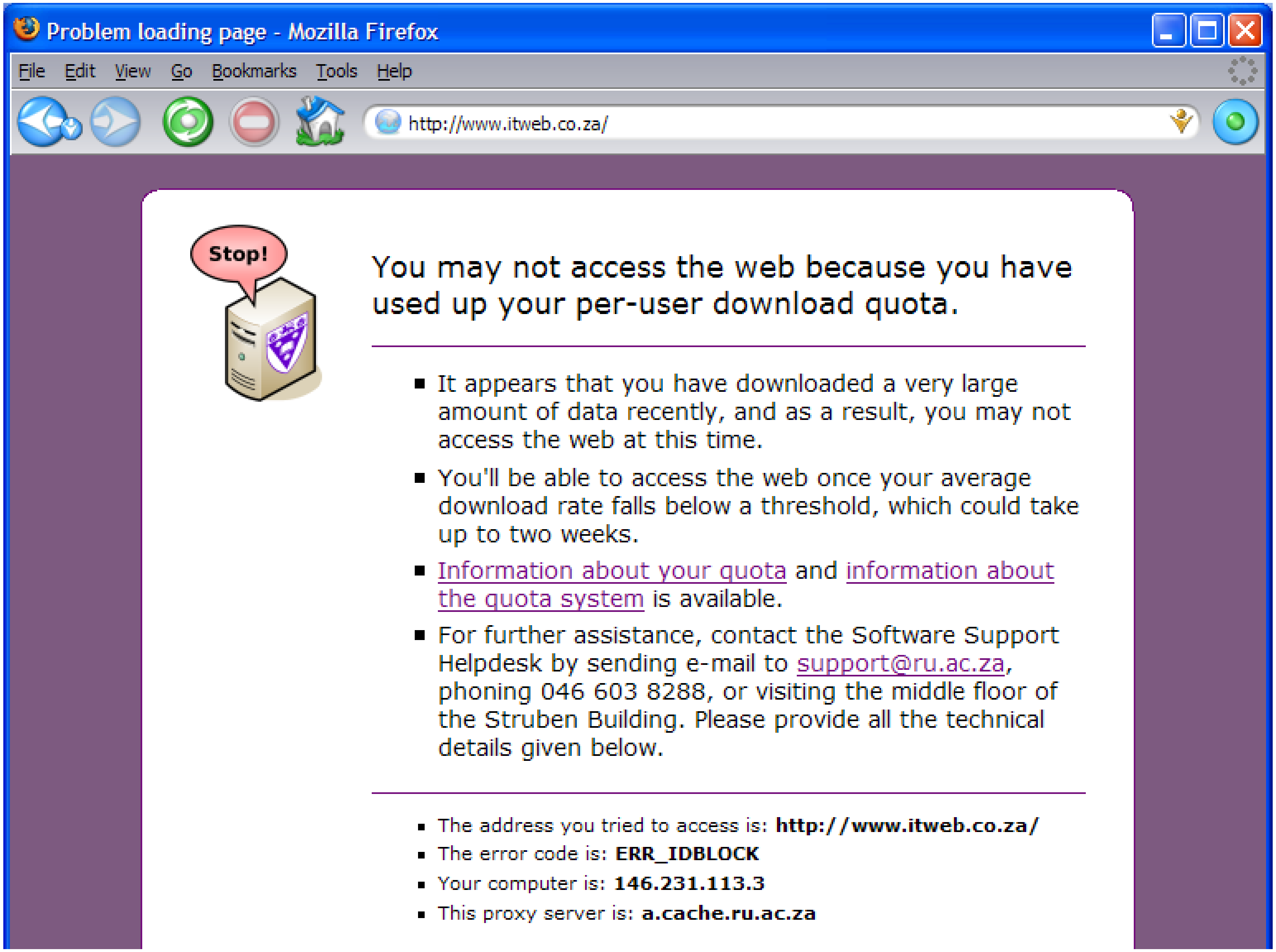
```
acl IDLOW        proxy_auth_regex -i "/idquotalow.acl"
acl IDHIGH       proxy_auth_regex -i "/idquotahigh.acl"
acl IDBLOCK      proxy_auth_regex –I "/squid/idquotablock.acl"
deny_info        ERR_IDBLOCK IDBLOCK

# SLOW = 0.5% * total PVC, rounded to nearest 0.5kBps
# V. SLOW = 0.5 * SLOW
delay_parameters 3 -1/-1 -1/-1 2560/20480
delay_parameters 4 -1/-1 -1/-1 1280/10240

# This MUST be the first rule that requests a username
http_access allow LOGIN !IDBLOCK !NOAUTH

# proxy auth based delay pools
delay_access    3 allow IDLOW
delay_access    3 deny all
delay_access    4 allow IDHIGH
delay_access    4 deny all
```

Quota System @ Rhodes


Problem loading page - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.itweb.co.za/
Stop!

You may not access the web because you have used up your per-user download quota.

- It appears that you have downloaded a very large amount of data recently, and as a result, you may not access the web at this time.
- You'll be able to access the web once your average download rate falls below a threshold, which could take up to two weeks.
- Information about your quota and information about the quota system is available.
- For further assistance, contact the Software Support Helpdesk by sending e-mail to support@ru.ac.za, phoning 046 603 8288, or visiting the middle floor of the Struben Building. Please provide all the technical details given below.

- The address you tried to access is: **http://www.itweb.co.za/**
- The error code is: **ERR_IDBLOCK**
- Your computer is: **146.231.113.3**
- This proxy server is: **a.cache.ru.ac.za**

Dynamic Delay Pools @ UKZN

- All TENET sites have bandwidth that's categorized into national/international traffic, and this is displayed on graphs at http://www.tenet.ac.za/
- The problem is how to make most efficient use of this bandwidth – how to allow users to download as fast as possible without impacting usability

This is the work of

Richard Stubs
<stubbs@ukzn.ac.za>

at the University of Kwazulu Natal.

Dynamic Delay Pools @ UKZN

Unauthenticated Requests

- One of the biggest bandwidth users these days is software updates. In particular, software that polls for updates every time it detects a network connection
- One way to keep some degree of control over this is to enable proxy authentication – to require a username and password to use the web.

Unauthenticated Requests

- The down side of this is that some software goes mad when it gets an HTTP 407 response. Software developers don’t implement incremental back-off algorithms.
- How do we let users know what’s going on?

Unauthenticated Requests

- Our solution forms part of the quota system you just heard about. It's just another quota.
- Users lose access when they've exceeded 1440 TCP_DENIED/407 messages a day, and regain it automatically when they drop below this.
- Just another file-based ACL list.