Bandwidth Management

Chris Wilson
Aptivate Ltd, UK

AfNOG 2012

Download this presentation at:
http://www.ws.afnog.org/afnog2012/tutorials/bmo

Ingredients

- **What is bandwidth management**
- When to manage bandwidth
- Troubleshooting an Internet connection
- Monitoring an Internet connection
- Setting policy
- Enforcing Policy
  - Social measures
  - Technical measures
- Summary and resources

What is Bandwidth Management?

- Network management of slow links, and the networks that use them?
  - Do you have a better definition?
- Particularly important to internet users
- Users often complain that “the internet is slow” or “the internet is down”
- You may need more bandwidth, but:
  - Without management, no amount of bandwidth is enough
  - Bandwidth is very expensive
  - Good management can save you a lot of money

Meeting Expectations

- Users have an expectation of network performance
- Set by previous experience, e.g. cyber cafés, friends, other employers, connection at home
- Users will ask for more bandwidth than you can supply (if it doesn't cost them more money)
- In a commercial and academic context, it's important to facilitate peoples' work use of Internet
- May mean reducing, eliminating or moving non-work or unnecessary traffic to make more capacity available

Bandwidth Mis-management

- If an internet connection is not well managed:
  - PCs will become infected with viruses and worms
  - Virus and worm traffic will fill the connection
  - P2P users and download managers will fight for the rest
  - Ordinary web browsing will become impossible
  - Skype, VoIP and other interactive applications will be unusable
- Departments may demand a separate connection
  - Wastes resources that could be better pooled
  - Appears to work for a while, then suffers the same fate

AfNOG

Next

- ✓ What is bandwidth management
- ➢ **When to manage bandwidth**
- Troubleshooting an Internet connection
- Monitoring an Internet connection
- Setting policy
- Enforcing Policy
  - Social measures
  - Technical measures
- Summary and resources

When to Manage Bandwidth

- Do we need bandwidth management?
  - Internet (or internal) link overloaded (and only then!)
  - Users complaining about poor performance
  - Link billed by usage
  - Link throttled by usage
  - Complaints from upstream provider
  - Need to improve quality of service (e.g. for VoIP)
  - Downgrade connection to save money
  - Not sure? Monitor whether link is overloaded
  - Monitoring can give early warning of problems
- Link not overloaded? Management will not help

Next

- ✓ What is bandwidth management
- ✓ When to manage bandwidth
- ➢ **Troubleshooting an Internet connection**
- Monitoring an Internet connection
- Setting policy
- Enforcing Policy
    - Social measures
    - Technical measures
- Summary and resources

AfNOG

The Internet is so slow!

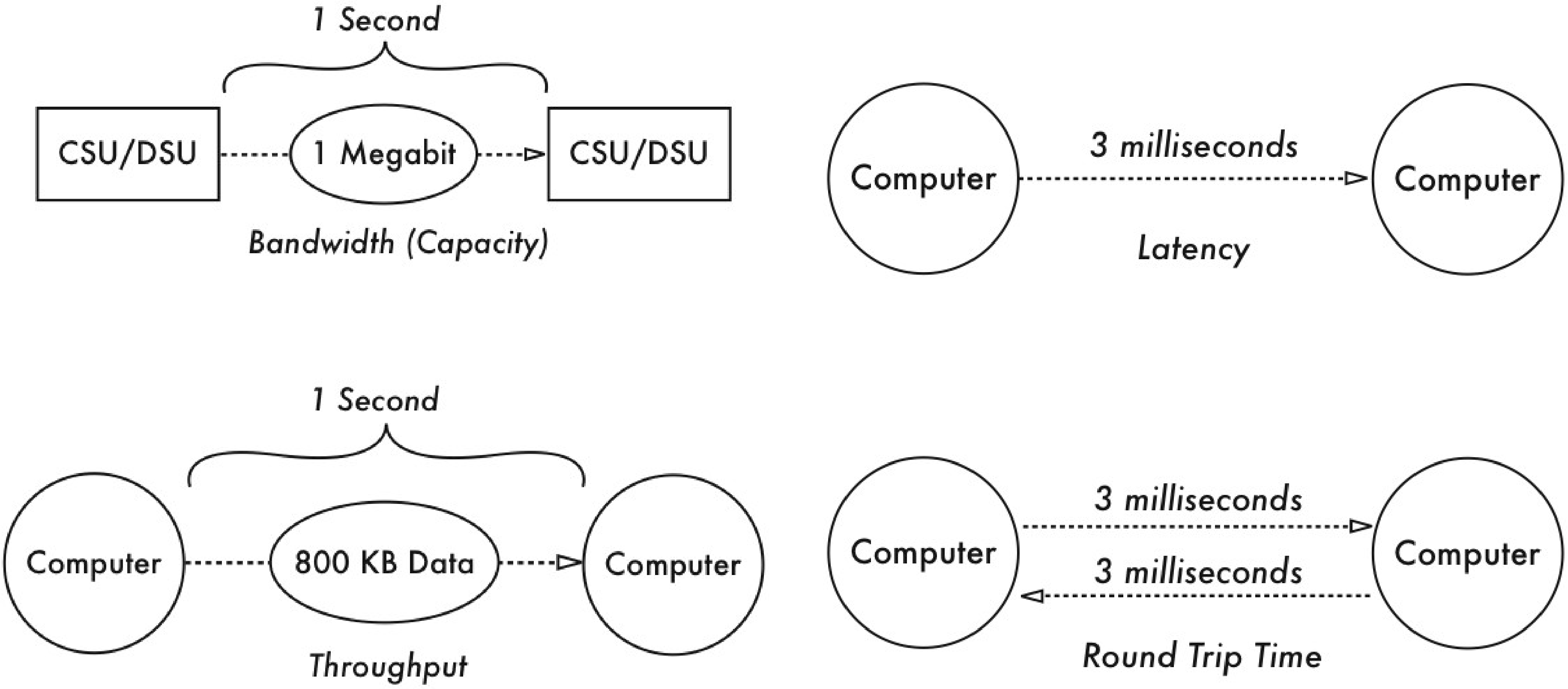
- What do we mean by “slow”?
  - completely down?
  - packet loss (tcp backoff)
  - long ping times (round-trip times)
  - long DNS lookup times (or DNS failure)
- Other related problems:
  - Jitter (mostly affects Skype and other VoIP)
- What doesn’t work?
  - Access to ordinary web pages? (HTTP)
  - BitTorrent and P2P software?
  - Skype and other real-time network applications?

In Case of Repeated Fires

- Sometimes (not always!) the problem will be that your connection is too often full (used to capacity)
- You can ping the router on your side without problems, but pinging your ISP’s router shows:
  - very high latency (over 1 second) to your ISP
    - Windows reports latency over 4 seconds as “request timed out”
  - packet loss over 1% to your ISP
  - DNS timeouts or slow replies from your ISP (not cached)
  - high jitter (subjective, maybe over 20 ms stdev?)
- Could also be a faulty link or router on either end

Definitions

- From the Bandwidth Management Book, http://bwmo.net:



Diagnosing the Problem

- Check that your connection works
- Check that your DNS works
- Traceroute to the remote server, looking for:
  - sudden increase in ping times or packet loss
  - jitter (standard deviation changes)
  - identify between which hops this occurs
- Ping the remote server
- `telnet www.google.com 80`

  -
    ```
    GET / HTTP/1.0
    Host: www.google.com
    ```
- Monitor intermittent problems with trending tools

Ping

- Useful for spot checking:
  - reachability (try *www.google.com* or *4.2.2.2*)
  - round trip time (RTT), also known as latency
  - packet loss (ping -f, ping -c 1000 -s 1400 may help)
  - jitter (ping -c 1000 and check *mdev/stddev*)
  - fragmentation (ping -s 1483)

Matt’s Traceroute (MTR)

- Interactive, repeating version of Traceroute
  - ***sudo -E pkg_add -r mtr*** (or ***mtr-nox11***)
  - ***mtr -r -c10 download.java.sun.com***

  -
    ```
    HOST: rocio.int.aidworld.org       Loss%   Snt   Last   Avg  Best  Wrst StDev
      1. 196.200.217.254                0.0%    10    1.6   1.7   1.6   1.8   0.1
      2. rtr-tedata.mtg.afnog.org       0.0%    10    2.0   2.2   2.0   3.2   0.4
      3. host-196.219.220.81-static.t   0.0%    10    5.5   8.4   4.0  45.0  12.9
      4. host-163.121.160.229.tedata.   0.0%    10    6.7   4.8   4.3   6.7   0.8
      5. host-163.121.189.73.tedata.n   0.0%    10    4.4  11.3   4.4  63.4  18.4
      6. host-163.121.186.253.tedata.   0.0%    10    4.5   5.1   4.5   7.4   0.9
      7. host-163.121.184.61.tedata.n   0.0%    10    5.0   5.7   4.6  13.5   2.8
      8. pal6-telecom-egypt-1-eg.pal.   0.0%    10   72.3  66.4  54.5 100.7  15.4
      9. ash1-new11-racc1.ash.seabone   0.0%    10  150.3 154.2 150.3 175.9   7.8
     10. ntt-1-ash1.ash.seabone.net    40.0%    10  153.7 152.7 146.7 154.5   3.0
     11. as-3.r20.snjsca04.us.bb.gin.   0.0%    10  153.7 182.7 146.1 219.0  36.8
     12. as-3.r20.snjsca04.us.bb.gin.  10.0%    10  215.9 255.3 214.3 370.0  54.4
     13. ge-3-3.r03.snjsca04.us.ce.gi  10.0%    10  216.9 253.5 216.2 402.0  63.7
     14. border2.te8-1-bbnet2.sfo002.  10.0%    10  216.9 218.7 215.8 230.7   5.0
     15. border2.te8-1-bbnet2.sfo002.  50.0%    10  215.2 215.6 214.9 216.9   0.8
     16. ???                           100.0    10    0.0   0.0   0.0   0.0   0.0
    ```
- Problem is between hops 7 and 9?

AfNOG

Who Controls the Broken Link

- Every link is between two hops
- May be able to identify them from reverse DNS, or looking at your network map
- Both ends are responsible for the link
- Usually cannot tell which end has the problem except by swapping it out
- Who controls the nearest end?
  - You? (investigate the traffic on the link)
  - Your ISP? (call your ISP)
  - Their carrier? (call your ISP, and pray)

Next

- ✓ What is bandwidth management
- ✓ When to manage bandwidth
- ✓ Troubleshooting an Internet connection
- ➢ **Monitoring an Internet connection**
- ◆ Setting policy
- ◆ Enforcing Policy: Social measures
- ◆ Enforcing Policy: Technical measures
- ◆ Summary and resources

AfNOG

Monitoring an Internet connection

- What do we want to monitor?
  - The same factors that we want to use for troubleshooting
  - The same factors that affect quality of service
  - Local and remote router availability and ping times (packet loss and latency)
  - Local and remote caching DNS server availability and query response times (failure rate and latency)
  - Link traffic overall, and by host and type
  - Remote websites (end-to-end test)
- Long-term monitoring helps to identify trends and sudden large changes

AfNOG

What Kind of Monitoring

- Spot check tools can identify some problems immediately
- Many problems require an idea of baseline performance (what changed? and how much?)
- Trending tools can gather baseline data
- Trending tools can help investigate problems after they disappear (e.g. intermittent, recurring)
- Trending tools require significant CPU, disk space, bandwidth and infrastructure investment

Tools of the Trade

Variable	Spot Check	Trending
End-to-end HTTP	wget, fetch, httperf	Smokeping, Nagios
Ping latency	Ping, Traceroute, MTR	Smokeping, Nagios
Ping packet loss	Ping, Traceroute, MTR	Smokeping, Nagios
DNS latency	Host, Resperf	Smokeping, Nagios
DNS errors	Host, Resperf	Smokeping, Nagios
Total bandwidth use	Cisco “show interfaces”	Cacti, MRTG
Traffic flows	Cisco Top Talkers, Ntop	NfSen, Argus, pmGraph
Individual packets	Wireshark	tcpdump, Argus

AfNOG

Quality of Service Monitoring

- Nagios to monitor websites, routers and DNS servers (local and upstream) and send alerts
- Cacti to monitor total bandwidth use on each interface, CPU and memory use on routers and switches
- Smokeping to monitor websites, latency and packet loss on upstream connections
- NfSen or pmGraph to monitor traffic flows on Internet connections

Installing and Configuring Nagios (1)

- `cd /usr/ports/www/apache22`
  - `sudo make install clean`
  - `sudo sh -c 'echo apache22_enable="YES" >> /etc/rc.conf'`
  - `sudo /usr/local/etc/rc.d/apache22 start`
- `cd /usr/ports/net-mgmt/nagios`
  - `sudo make install clean`
  - `sudo sh -c 'echo nagios_enable="YES" >> /etc/rc.conf'`
- `cd /usr/ports/net-mgmt/nagios-plugins`
  - `sudo make install clean`
- `cd /usr/local/etc/nagios`
  - `sudo cp nagios.cfg-sample nagios.cfg`
  - `sudo cp cgi.cfg-sample cgi.cfg`
  - `sudo cp resource.cfg-sample resource.cfg`

AfNOG

Configuring Nagios (2)

- Edit *nagios.cfg* and comment out this line:
  - `cfg_file=/usr/local/etc/nagios/objects/localhost.cfg`
- `cd objects`
- `sudo cp commands.cfg-sample commands.cfg`
- `sudo cp contacts.cfg-sample contacts.cfg`
- Edit *contacts.cfg* and change `nagios@localhost` to your email address
- `sudo cp timeperiods.cfg-sample timeperiods.cfg`
- `sudo cp templates.cfg-sample templates.cfg`

Configuring Nagios (3)

- Create */usr/local/etc/apache22/Includes/nagios.conf* with the following contents:

  -
    ```
    <Directory /usr/local/www/nagios>
        Order deny,allow
        Allow from all
        AuthName "Nagios Access"
        AuthType Basic
        AuthUserFile /usr/local/etc/nagios/htpasswd.users
        require valid-user
    </Directory>
    <Directory /usr/local/www/nagios/cgi-bin>
        Options ExecCGI
    </Directory>
    ScriptAlias /nagios/cgi-bin/ /usr/local/www/nagios/cgi-bin/
    Alias /nagios/ /usr/local/www/nagios/
    ```

-
  ```
  sudo htpasswd -c /usr/local/etc/nagios/htpasswd.users \
  nagiosadmin
  ```

-
  ```
  sudo /usr/local/etc/rc.d/apache22 reload
  ```

Monitoring Routers with Nagios

- Edit *templates.cfg* and add these lines at the end:

  -
    ```
    define host {
            host_name router-local
            use generic-host
            address br01.mtg.afnog.org
            max_check_attempts 5
    }
    define host {
            host_name router-simbanet
            use generic-host
            address 41.188.165.49
            max_check_attempts 5
    }
    define hostgroup {
            hostgroup_name routers
            members router-local, router-simbanet
    }
    define service {
            service_description ping
            use generic-service
            hostgroup routers
            check_command check_ping!30,10%!100,40%
    }
    ```

Monitoring DNS Servers with Nagios

```
define hostgroup {
    hostgroup_name dns-servers
}
define host {
    name dns-server
    max_check_attempts 5
    hostgroups dns-servers
    register 0
}
define host {
    host_name noc
    use dns-server
    address 196.200.223.1
}
define host {
    host_name google
    use dns-server
    address 8.8.8.8
}
define command {
    command_name check_dns
    command_line $USER1$/check_dns -H www.yahoo.com -s $HOSTADDRESS$
}
define service {
    service_description dns
    use generic-service
    hostgroup dns-servers
    check_command check_dns
}
```

Monitoring web sites with Nagios

-
  ```
  define hostgroup {
      hostgroup_name websites
  }
  define host {
      name website
      max_check_attempts 5
      hostgroups websites
      register 0
  }
  define host {
      host_name www.yahoo.com
      use website
      address www.yahoo.com
  }
  define host {
      host_name www.google.com
      use website
      address www.google.com
  }
  define command {
      command_name check_site
      command_line $USER1$/check_http -H $HOSTADDRESS$
  }
  define service {
      service_description http
      use generic-service
      hostgroup websites
      check_command check_site
  }
  ```

Installing Smokeping (1)

- Install Smokeping's dependencies (saves time):

  -
    ```
    sudo -E pkg_add -r perl rrdtool fping
    echoping p5-CGI-Session p5-CGI-SpeedyCGI
    p5-Digest-HMAC p5-SNMP_Session p5-libwww
    p5-Net-DNS
    ```
- Install Smokeping from ports:

  -
    ```
    cd /usr/ports/net-mgmt/smokeping
    ```

  -
    ```
    sudo -E make install clean
    ```
  - Enable the following options: fping, EchoPing and AnotherDNS probes
- Add the following line to */etc/rc.conf*:

  -
    ```
    smokeping_enable="YES"
    ```

Installing Smokeping (2)

- Edit */usr/local/etc/smokeping/config* and change:
  - `sendmail = `***`/usr/sbin/sendmail`***
  - `step = `***`60`***
  - remove the *Slaves* section and “slaves =” lines
  - remove from “+ Test” to end of file

Installing Smokeping (3)

- Create */usr/local/etc/apache22/Includes/smokeping.conf* with the following contents:

  ```
  Alias /smokeping /usr/local/smokeping/htdocs
  <Location /smokeping>
    DirectoryIndex smokeping.cgi
    AddHandler cgi-script .cgi
  </Location>
  <Directory /usr/local/smokeping/htdocs>
    Allow from all
  </Directory>
  ```

- Tell Apache to reload its configuration:

  ```
  sudo /usr/local/etc/rc.d/apache22 reload
  ```

Monitoring Routers with Smokeping

- Edit */usr/local/etc/smokeping/config* and append:
  - `+ qcell`
  - `probe = FPing`
  - `host = 196.46.232.115`
  - `+ gamtel`
  - `probe = FPing`
  - `host = 212.60.64.90`
  - `+ unique`
  - `probe = FPing`
  - `host = 212.60.65.118`
- Restart Smokeping:
  - `sudo /usr/local/etc/rc.d/smokeping reload`

Monitoring DNS Servers

- In the *** Probes *** section, add:

  -
    ```
    + DNS
    binary = /usr/bin/dig
    lookup = www.yahoo.com
    ```
- In the *** Targets *** section, add:

  -
    ```
    + soekris
    probe = DNS
    host = 196.200.223.1
    ```

  -
    ```
    + google
    probe = DNS
    host = 8.8.8.8
    ```
- `sudo /usr/local/etc/rc.d/smokeping reload`

Monitoring Web Servers

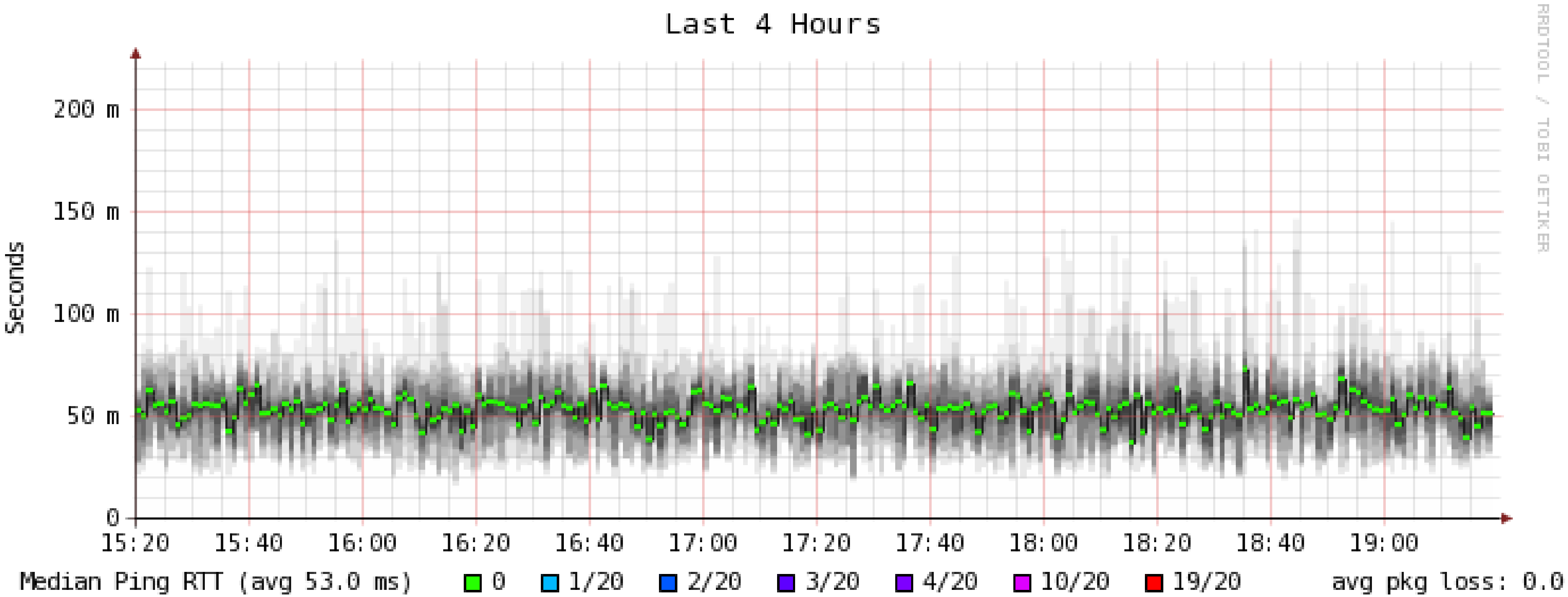
- In the *** Probes *** section, add:

  -
    ```
    + EchoPingHttp
    binary = /usr/local/bin/echoping
    ```
- In the *** Targets *** section, add:

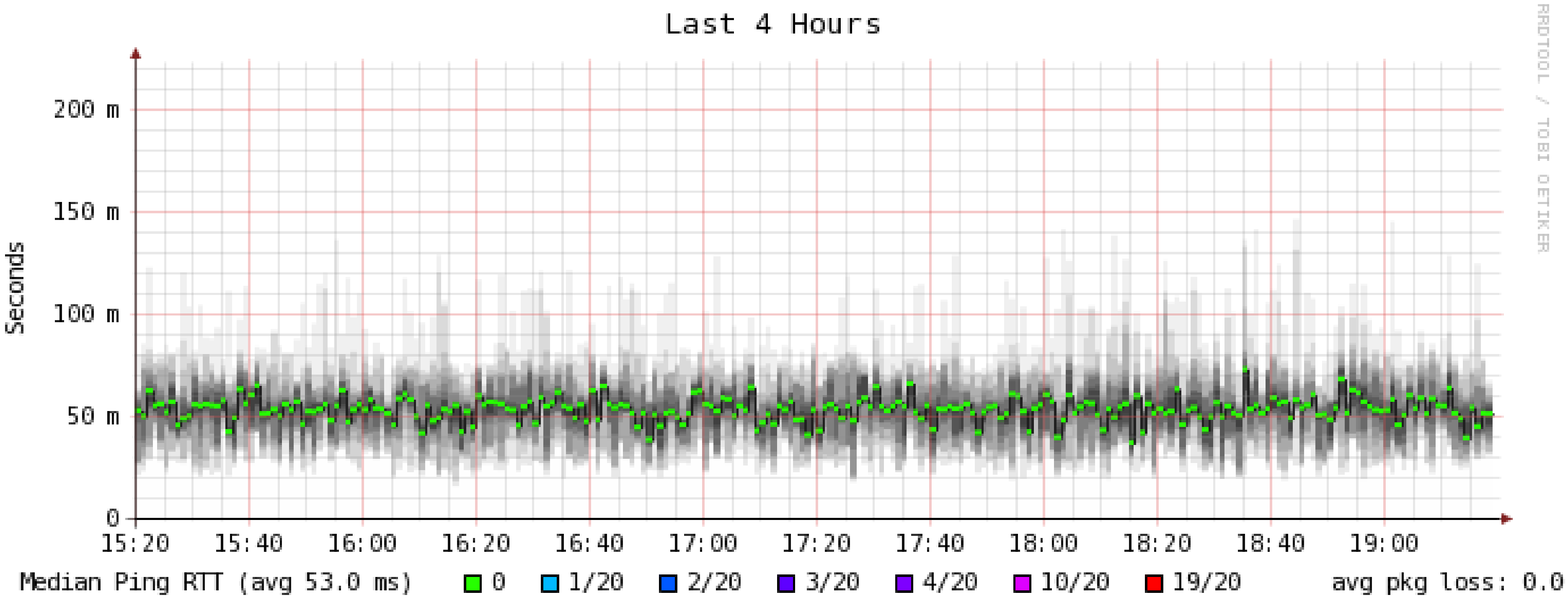
  -
    ```
    + google
    probe = EchoPingHttp
    host = www.google.com
    ```

  -
    ```
    + yahoo
    probe = EchoPingHttp
    host = www.yahoo.com
    ```
- `sudo /usr/local/etc/rc.d/smokeping reload`

Reading Smokeping Graphs (1)

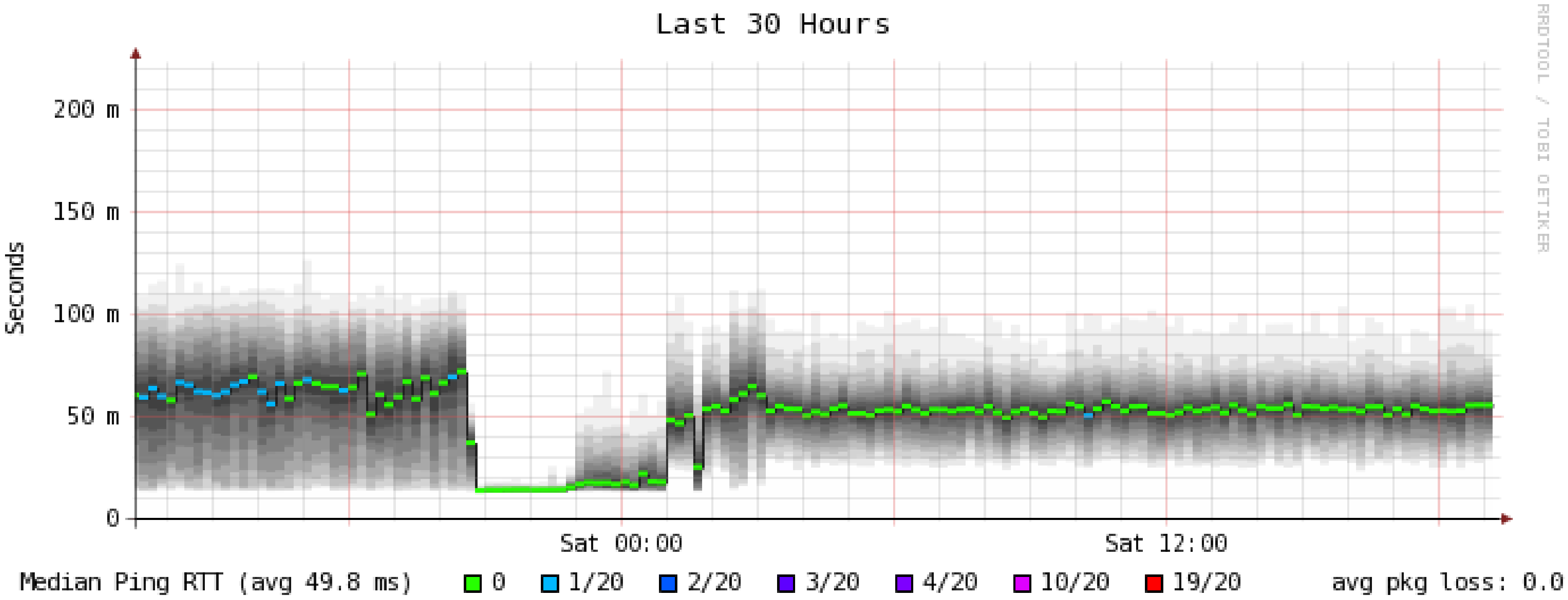


Reading Smokeping Graphs (1)

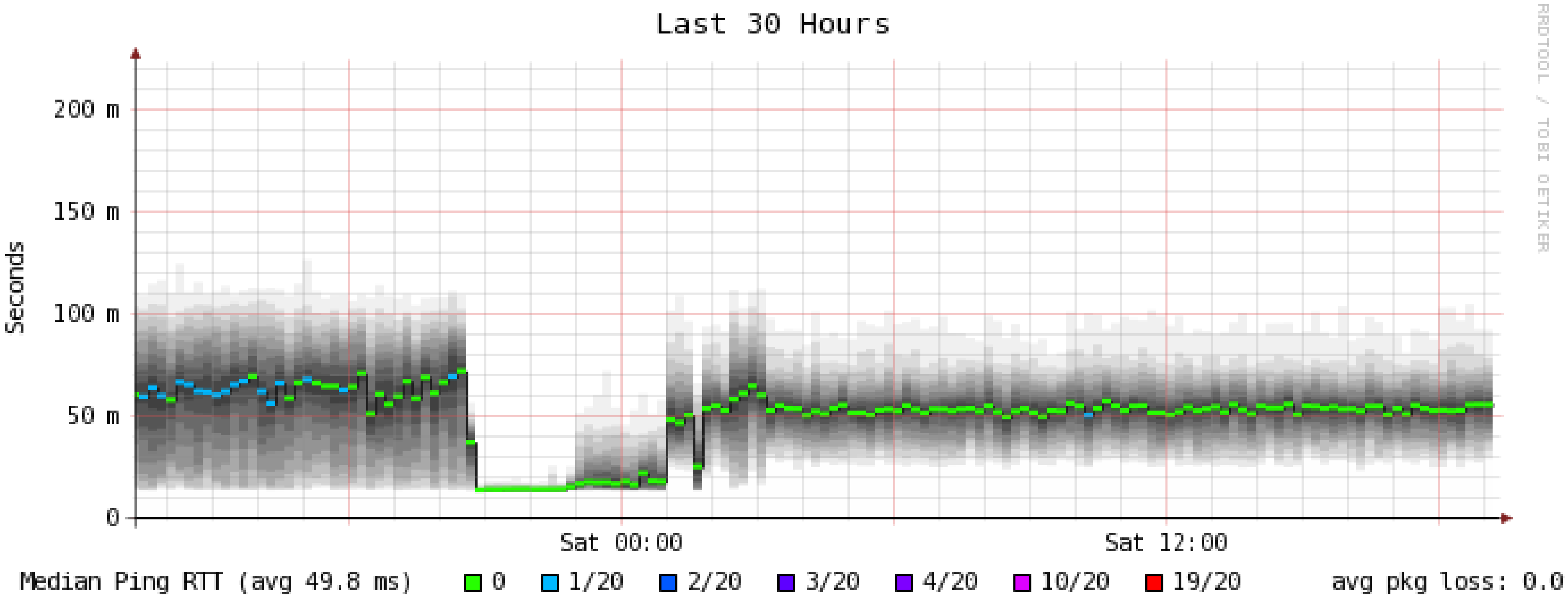


- Overall latency a little high for first hop
- Rather high jitter
- No packet loss

Reading Smokeping Graphs (2)



Reading Smokeping Graphs (2)



- Significant drop in latency and packet loss for a short period
- Conclusion: link is heavily loaded most of the time

Installing Cacti on FreeBSD (1)

- `sudo -E pkg_add -r mysql55-server cacti`
- Edit */etc/rc.conf* and add the following line:
  - `mysql_enable="YES"`
- `sudo /usr/local/etc/rc.d/mysql-server start`

-
  ```
  echo "GRANT ALL ON cacti.* TO
  cactiuser@localhost IDENTIFIED BY 'topsecret';"
  | mysql -u root
  ```
- Edit */usr/local/share/cacti/include/config.php*:
  - `$database_password = "`***`topsecret`***`";`

Installing Cacti on FreeBSD (2)

- Reconfigure PHP to enable the Apache module:
  - `cd /usr/ports/lang/php5`
  - `sudo make deinstall clean config`
  - Enable the Apache option
  - `sudo make install clean`
- Create */usr/local/etc/apache22/Includes/cacti.conf*:
  - `Alias /cacti "/usr/local/share/cacti/"`
- Restart Apache:
  - `sudo /usr/local/etc/rc.d/apache22 restart`

Diagnosing Busy Connections

- Heavily loaded link could be due to:
  - inbound traffic
    - downloads, bittorrent, attacks, incoming spam
  - outbound traffic
    - uploads, bittorrent, virus or worm-infected PCs, outgoing spam
  - both at the same time
- Total volume of traffic is not helpful
- Need to identify the source of the traffic
  - Identifying the destination may not help

Finding the Culprit

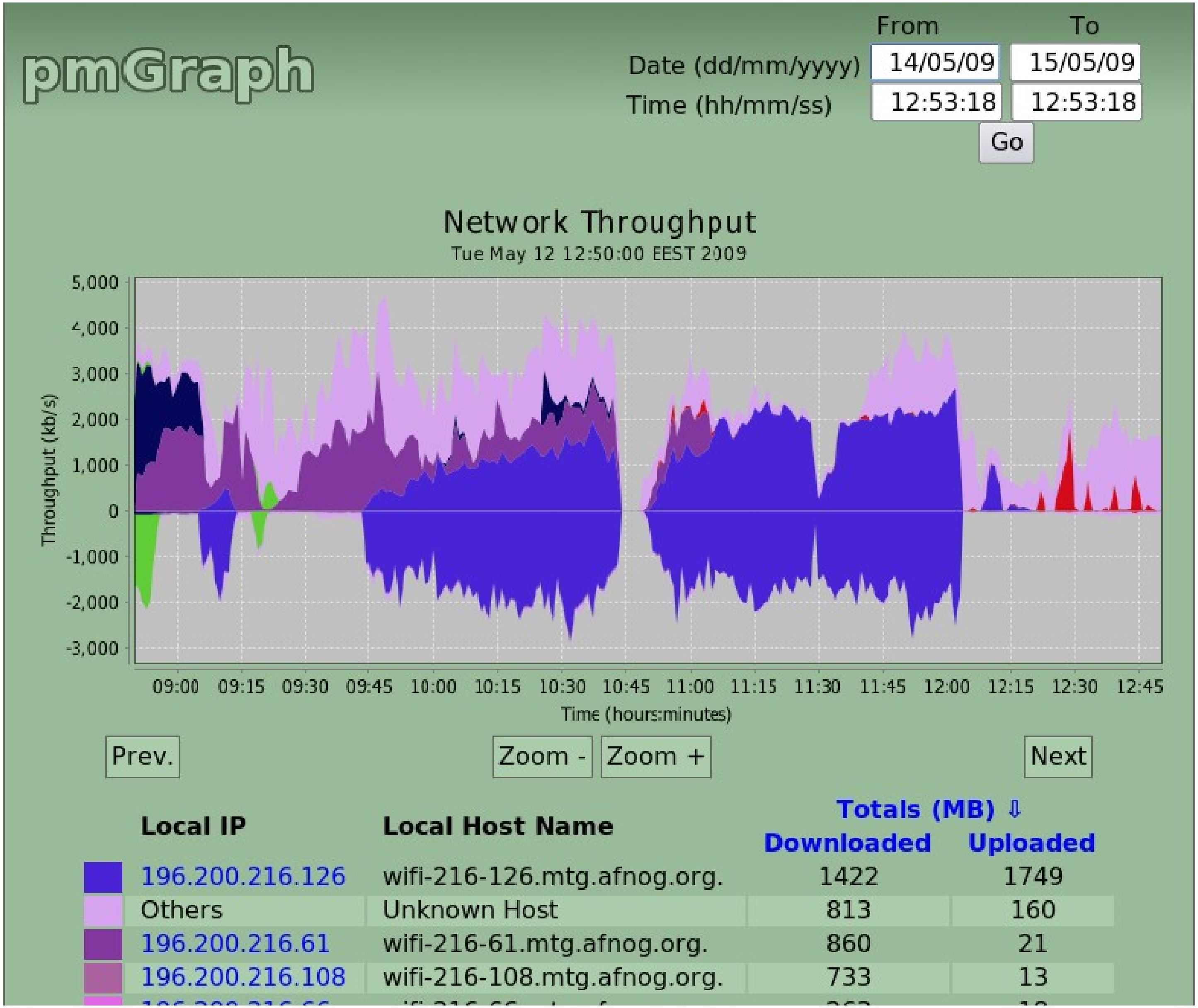
- Switch LEDs may help you track down busy ports
  - Do not discriminate between local and remote traffic
- Managed switched can have traffic on each port monitored remotely by SNMP
- Flows are the next level down
  - Cisco or Juniper router with NetFlow/sFlow
  - Unix router or bridge running *pmacct* or *ntop*
- Packets are the lowest level
  - Unix router or transparent bridge running *Wireshark*
  - Expensive hardware network analysers

Going with the Flow

- Flows are useful tools for traffic monitoring
  - Identify who is talking to who, and often the protocol or type of traffic
  - Much less verbose and easier to understand than packets
- A flow is (usually) a unique:
  - pair of IP addresses
  - pair of ports
  - protocol
- Flows are sampled (number of bytes reported) at fixed time intervals to add a sixth dimension
- Get flow data from a router or transparent bridge

AfNOG

What do Flows Look Like



pmGraph

	From	To
Date (dd/mm/yyyy)	14/05/09	15/05/09
Time (hh/mm/ss)	12:53:18	12:53:18

	Local IP	Local Host Name	Totals (MB) ⇩ Downloaded	Uploaded
■	196.200.216.126	wifi-216-126.mtg.afnog.org.	1422	1749
■	Others	Unknown Host	813	160
■	196.200.216.61	wifi-216-61.mtg.afnog.org.	860	21
■	196.200.216.108	wifi-216-108.mtg.afnog.org.	733	13

AfNOG

Enabling Netflow on Cisco (1)

- You should enable Netflow on all active interfaces

```
rtr-tedata> show interface summary
  Interface            IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
----------------------------------------------------------------------
  FastEthernet0/0        0     0    0     0     0    0     0    0    0
* FastEthernet0/1        1     0    0     0 1684000 369 1944000 315  0
* Serial0/0/0            0     0    0     0 957000  148 703000  165  0
* Serial0/0/1            0     0    0     0 1324000 182 1223000 201  0
* Serial0/2/0            0     0    0     0 469000  101 887000  140  0
```

```
rtr-tedata# conf t
rtr-tedata(config)# interface FastEthernet0/1
rtr-tedata(config-if)# ip route-cache flow
rtr-tedata(config-if)# exit
rtr-tedata(config)# interface Serial0/0/0
rtr-tedata(config-if)# ip route-cache flow
rtr-tedata(config-if)# exit
```

```
rtr-tedata# show ip flow top-talkers
SrcIf       SrcIPaddress    DstIf   DstIPaddress    Pr SrcP DstP Bytes
Se0/0/0     213.136.96.104  Fa0/1*  196.200.216.77  11 04AA 04A4  1539K
Se0/0/0     24.17.17.180    Fa0/1*  196.200.216.125 06 A6CE 1C2A  1522K
Se0/0/0     188.24.50.177   Fa0/1*  196.200.216.125 06 E87A 1C2A  1433K
Se0/2/0     207.148.178.122 Fa0/1*  196.200.216.125 06 BE90 1C2A   834K
Se0/0/1     195.226.227.100 Fa0/1*  196.200.216.125 06 EEA3 1C2A   647K
```

Enabling Netflow on Cisco (2)

- Try just the external interfaces:

```
rtr-tedata> show interface summary
Interface              IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
----------------------------------------------------------------------
* FastEthernet0/0        0   240    0     0 1136000 162 585000 556   3
  FastEthernet0/0.72     -     -    -     -       -   -     -    -   -
* FastEthernet0/0.701   -     -    -     -       -   -     -    -   -
* FastEthernet0/0.702   -     -    -     -       -   -     -    -   -
* FastEthernet0/0.703   -     -    -     -       -   -     -    -   -
rtr-tedata> enable
rtr-tedata# conf t
rtr-tedata(config)# interface FastEthernet0/0.701
rtr-tedata(config-if)# ip flow ingress
rtr-tedata(config-if)# ip flow egress
rtr-tedata(config-if)# interface FastEthernet0/0.702
rtr-tedata(config-if)# ip flow ingress
rtr-tedata(config-if)# ip flow egress
```

Installing nfSen on FreeBSD

- `sudo -E pkg_add -r rrdtool m4 php5`
- `cd /usr/ports/net-mgmt/nfsen`
- `sudo -E make install clean`
- Enable the `READPCAP` option
- Edit /etc/rc.conf and add the following line:
  - nfsen_enable=”YES”
- Start nfsen:
  - sudo /usr/local/etc/rc.d/nfsen start

Installing pmacct on FreeBSD (1)

- Install *pmacct* from ports:
  - ***cd /usr/ports/net-mgmt/pmacct***
  - ***sudo make install clean***
    - Enable MySQL support
- Add the following line to */etc/rc.conf*:
  - ***mysql_enable="YES"***
- Start the MySQL server:
  - ***sudo /usr/local/etc/rc.d/mysql-server start***

AfNOG

Configuring pmacct for Netflow

- Create */usr/local/etc/pmacctd.conf* with the following contents:

  -
    ```
    daemonize: false
    debug: true
    pidfile: /var/run/nfacctd.pid
    ! logfile: /var/log/nfacctd.log
    ! syslog: daemon
    nfacctd_port: 4096
    plugins: mysql
    aggregate: src_host, src_port, dst_host, dst_port, proto
    sql_db: pmacct
    sql_table: acct_v8
    sql_history: 1m
    sql_history_roundoff: m
    sql_table_version: 8
    sql_host: 127.0.0.1
    sql_user: pmacct
    sql_passwd: XXXXXXXXX
    sql_refresh_time: 60
    sql_dont_try_update: true
    sql_optimize_clauses: true
    sql_preprocess: minb = 10000
    ```

AfNOG

Installing pmacct on FreeBSD (2)

- Create the MySQL database for pmacct:
  - mysqladmin -u root -p create pmacct
    - The password might be “afnog”
  - mysql -u root -p pmacct < /usr/local/share/pmacct/pmacct-create-db_v8.mysql
  - mysql -u root -p pmacct
    - grant all on pmacct.* to pmacct@localhost identified by “somepassword”
    - alter table acct_v8 drop primary key, add index (stamp_inserted);

Running nfacct for Netflow logging

- Start *nfacctd* running in debug mode:
  - ***sudo /usr/local/sbin/nfacctd -f /usr/local/etc/pmacctd.conf -d***
- Look for *ERROR* lines in the output

Exporting Netflow Data from Cisco

- If your collector’s IP address is 1.2.3.4:
  - ***ssh cisco***
  - ***enable***
  - ***conf t***
  - ***ip flow-cache timeout active 1***
  - ***ip flow-cache timeout inactive 60***
  - ***ip flow-export version 5***
  - ***ip flow-export destination 10.0.0.1 4096***
  - ***exit***
  - ***write***

Alternative: Monitoring Box

- Need a Unix box that can sniff the traffic:
    - Attached to a monitoring port of a managed switch
    - Attached to a dumb hub
    - Routing traffic between subnets
    - Bridging two LANs
- Options:
    - Use an existing Unix router or proxy
    - Create a new transparent bridge
    - Add a router outside of LAN (e.g. WAN side)
    - Reconfigure entire LAN

Transparent Bridging with FreeBSD (1)

- Need a PC with at least two LAN/VLAN interfaces
- Add the following lines to */etc/rc.conf*:
  - ***cloned_interfaces="bridge0"***
  - ***ifconfig_bridge0="addm em0 addm em1 up inet*** <IP>***"***
  - ***ifconfig_em0="up"***
  - ***ifconfig_em1="up"***
- Restart networking:
  - ***sudo /etc/rc.d/netif restart***
- Insert bridge in front of client PC(s)
- Test that clients can still access the Internet!

AfNOG

Configuring pmacct for Sniffing

- Modify */usr/local/etc/pmacctd.conf* as follows (changes highlighted):

  -
    ```
    daemonize: false
    debug: true
    pidfile: /var/run/pmacctd.pid
    ! logfile: /var/log/pmacctd.log
    ! syslog: daemon
    ! nfacctd_port: 4096
    plugins: mysql
    aggregate: src_host, src_port, dst_host, dst_port, proto
    sql_db: pmacct
    sql_table: acct_v8
    sql_history: 1m
    sql_history_roundoff: m
    sql_table_version: 8
    sql_host: 127.0.0.1
    sql_user: pmacct
    sql_passwd: XXXXXXXXX
    sql_refresh_time: 60
    sql_dont_try_update: true
    sql_optimize_clauses: true
    sql_preprocess: minb = 10000
    ```

Running pmacctd for Sniffing

- Start *nfacctd* running in debug mode:
    - ***sudo /usr/local/sbin/nfacctd -f /usr/local/etc/pmacctd.conf -d***
- Look for *ERROR* lines in the output

Checking the database contents

- Log into the MySQL database:
  - ***mysql pmacct -u root -p***
    - mysql> ***select ip_src, ip_dst, port_src, port_dst, bytes, stamp_inserted from acct_v8 limit 5;***

```
+-----------------+-----------------+----------+----------+-------+---------------------+
| ip_src          | ip_dst          | src_port | dst_port | bytes | stamp_inserted      |
+-----------------+-----------------+----------+----------+-------+---------------------+
| 196.200.223.2   | 196.200.208.4   |    60346 |       22 | 37792 | 2009-05-09 17:22:00 |
| 196.200.223.2   | 196.200.208.4   |    52755 |       22 | 37872 | 2009-05-09 17:27:00 |
| 196.200.216.38  | 196.200.208.20  |    50689 |       22 | 12976 | 2009-05-09 17:48:00 |
| 196.200.216.51  | 196.200.208.20  |    52059 |       23 | 12108 | 2009-05-09 17:48:00 |
| 196.200.216.32  | 69.147.102.99   |    64980 |       80 | 10292 | 2009-05-09 17:50:00 |
+-----------------+-----------------+----------+----------+-------+---------------------+
5 rows in set (0.00 sec)
```

- Add this command to /etc/rc.local:
  - ***/usr/local/sbin/pmacctd -f /usr/local/etc/pmacctd.conf -D***
  - Note that we've changed the ***-d*** option (*debugging*) to ***-D*** (*daemonize*)

Installing Tomcat

- Install Tomcat from ports:
  - ***cd /usr/ports/www/tomcat6***
  - ***sudo make install clean***
- You may need to follow the instructions to download the 60 MB diablo-caffe port of Java
- Add the following lines to */etc/rc.conf*:
  - ***tomcat60_enable=YES***
  - ***tomcat60_java_opts="-Djava.awt.headless=true"***
- Start Tomcat now (for the first time):
  - ***/usr/local/etc/rc.d/tomcat6 start***

Installing pmGraph

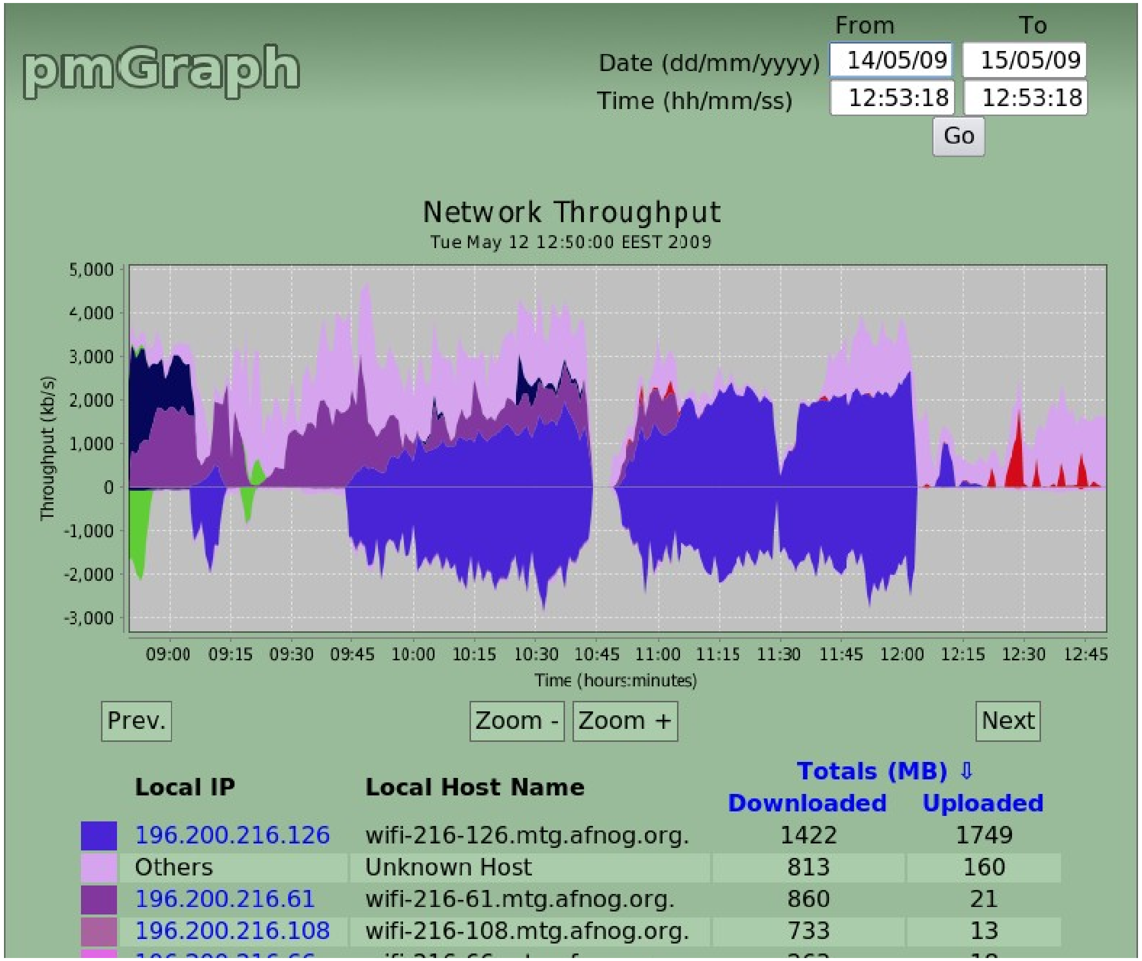
- You can read more about pmGraph at http://pmgraph.sourceforge.net
- Download the latest *pmgraph.war* file from:
  - http://sourceforge.net/projects/pmgraph/files/pmgraph/
  - There should already be a copy in */usr/ports/distfiles* on your machine
- Install it into Tomcat's webapps directory:
  - ***cd /usr/local/apache-tomcat6.0/webapps***
  - ***sudo mkdir pmgraph***
  - ***cd pmgraph***
  - ***sudo jar xf /usr/ports/distfiles/pmgraph.war***

Configuring pmGraph

- ***cd /usr/local/apache-tomcat6.0/webapps/pmgraph/WEB-INF/classes***
- ***sudo vi database.properties***
  - DatabaseURL = jdbc:mysql://***localhost/pmacct***
  - DatabasePass = ***XXXXXXXX***
  - LocalSubnet = ***196.200.219.***
- ***sudo /usr/local/etc/rc.d/tomcat6 restart***

Testing pmGraph

- Try: `fetch http://196.200.218.200/bigfile`
- Open http://localhost:8180/pmgraph:



	From	To
Date (dd/mm/yyyy)	14/05/09	15/05/09
Time (hh/mm/ss)	12:53:18	12:53:18

	Local IP	Local Host Name	Totals (MB) ⇩ Downloaded	 Uploaded
■	196.200.216.126	wifi-216-126.mtg.afnog.org.	1422	1749
■	Others	Unknown Host	813	160
■	196.200.216.61	wifi-216-61.mtg.afnog.org.	860	21
■	196.200.216.108	wifi-216-108.mtg.afnog.org.	733	13

Next

- ✓ What is bandwidth management
- ✓ When to manage bandwidth
- ✓ Troubleshooting an Internet connection
- ✓ Monitoring an Internet connection
- ➢ **Setting policy**
- Enforcing Policy
  - Social measures
  - Technical measures
- Summary and resources

What Next?

- Internet connection is sometimes full
- What can be done about it?
  - Block traffic that nobody wants (viruses, spam)
  - Efficiency savings (perhaps 10-50%)
  - Changing user behaviour
- Changing behaviour requires education and policy

Blocking Unwanted Traffic

- Outbound worm traffic is the most likely candidate
  - Identify infected machines (using monitoring tools)
  - Clean them and install antivirus software
  - Keep antivirus up to date
  - Block ports used by worms
  - Set alarms to detect infected machines in future
- Incoming spam may waste some capacity
  - Monitoring will tell you how much traffic is email
  - Good local spam filtering can help, but is difficult!
  - Remote email filtering services can help (e.g. Barracuda, LBSD)

Efficiency Savings

- Run a local DNS cache
- Run a local web cache
- Identify commonly downloaded files as candidates for local mirroring
- Check for inter-site traffic due to Active Directory and VPNs
- Don’t expect too much improvement here

What is a Policy

- Rules on what a network (or Internet connection) can or can’t be used for
  - Also known as an Acceptable Use Policy (AUP)
- Every good network has some kind of Acceptable Use Policy
- Users of a shared connection are entitled to agree on rules for sharing it
  - Rules imposed from above are usually unpopular
- How can we set policy fairly?

Why Set a Policy

- Network abuse is a social problem
- Social problems require social solutions
  - Changing network traffic means changing user behaviour
  - Rules, conventions, debate, consultation and consensus can be more persuasive than technical solutions
  - Requires buy-in from the top levels of organisations
- Policy guides implementation
  - Easier to decide what to block or restrict
  - Implementation without policy can be accused of being unaccountable, unfair, arbitrary or just wrong

AfNOG

What’s in a Policy

- The best Acceptable Use Policies would be:
  - Based on evidence
  - Set by consensus
  - Known by all
  - Monitored
  - Enforced
  - Reviewed regularly

Collecting Evidence

- Show effects of high network traffic on essential applications (e.g. by correlation or measurement)
- Show how much network traffic is used for different purposes (without prejudging)
- Show how much network traffic is used by the top users and departments (without naming them)
- Show the causes of high network traffic (applications, working practices, visibility)
- Show how much could be saved by efficiency measures (e.g. caches)

AfNOG

Proposing a Policy

- Consider whether certain applications have a good case for work use
  - Who says P2P, banner adverts or Skype are not business functions?
- Consider charging for usage (by volume or rate)
- Consider quotas on bandwidth use
- Consider throttling user traffic based on usage
- Consider applying the same rules as for phone calls, printing, photocopying

Reaching Consensus

- Involve all stakeholders (worth the effort)
- Present the evidence, and create space for discussion
- Explore all possible social and technical solutions
- Ensure that all views are taken into account
    - Try to accommodate dissent, e.g. allow personal use out of hours or within defined limits
- Try to avoid "design by committee" bloat
    - Make a case for simplicity
    - Don't be afraid to leave open to interpretation, e.g. "academic use" or "business use"

AfNOG

Consensus Failure

- If consensus cannot be reached:
  - Find out why it’s being blocked
  - Check that all views were taken into account
  - Make another proposal
  - Consider delaying implementation
  - Try a different decision mechanism
  - Consider imposing a temporary policy (with a time limit)

AfNOG

Publishing Policy

- Important that all users knows the policy
  - Users won't follow unwritten rules
- Post in the usual places (computer rooms, letters to new members and users)
- If possible, collect signatures before allowing access (issuing user identifiers)
- Publish the complete policy
  - even if some of it only applies to some users
  - more reason to keep it short and simple!

Reviewing Policy

- Decide and publish the review date in the policy
- Users are more likely to accept a temporary restriction than a permanent one
- Users are more likely to agree if they feel that:
  - They are being listened to
  - Their views have an influence on the policy
- Solicit comments in the policy document itself
- Log comments for review time
- Help people to comment anonymously

AfNOG

Next

- ✓ What is bandwidth management
- ✓ When to manage bandwidth
- ✓ Troubleshooting an Internet connection
- ✓ Monitoring an Internet connection
- ✓ Setting policy
- ➢ **Enforcing Policy**
  - Social measures
  - Technical measures
- Summary and resources

Monitoring Compliance

- Easy to set policy and never monitor compliance
- Sometimes only checked when a breach is suspected
- Data may no longer be available
- Users will lose respect for policy over time
- Better to at least collect compliance data continuously
- Good idea to delete data after some time
- Good idea to inform users (privacy policy)

Accountability

- Monitoring often gives a list of IP addresses
- How to connect them to users?
  - NAT problem
  - IP address spoofing
  - MAC address spoofing
  - Switch port security
  - Shared computers (e.g. labs)
  - Wireless clients
- 802.1x authentication solves many problems
- Proxy authentication can be a partial solution

AfNOG

Next

- ✓ What is bandwidth management
- ✓ When to manage bandwidth
- ✓ Troubleshooting an Internet connection
- ✓ Monitoring an Internet connection
- ✓ Setting policy
- ➢ Enforcing Policy
  - **Social measures**
  - Technical measures
- Summary and resources

AfNOG

Social Measures

- Network abuse is a social problem, not technical
- In most cases, social solutions work better:
  - Users may not be aware of their bandwidth use
  - Consider educating users on bandwidth use and tools
  - Likely to be few network abusers (about 5%)
  - Likely to be the most technically skilled
  - Discuss the problem with them first, in private
  - Consider publishing a list of the heaviest users
  - Consider disciplinary action, revoking privileges
- If necessary, technical options are available

Next

- ✓ What is bandwidth management
- ✓ When to manage bandwidth
- ✓ Troubleshooting an Internet connection
- ✓ Monitoring an Internet connection
- ✓ Setting policy
- ➢ Enforcing Policy
  - ✓ Social measures
  - **Technical measures**
- Summary and resources

Technical Measures

- Traffic prioritisation (tc, dummynet, altq)
- Limiting bandwidth used by some kinds of traffic
- Interactive fair sharing between IPs (SFQ, WFQ)
- Hard bandwidth quotas (cut off users over limit)
- Soft bandwidth quotas (throttle users over limit)
- Flexible throttling (progressively reduce bandwidth)

Transparent Bridge Filtering

- Need to enable packet filtering on the bridge
- Edit */etc/rc.conf* and add these lines:
  - ***firewall_enable="YES"***
  - ***firewall_type="open"***
- Start the firewall:
  - ***sudo bash /etc/rc.firewall***
- Enable firewall for bridged packets:
  - Edit */etc/sysctl.conf* and add the following line:
    - ***net.link.bridge.ipfw=1***
  - ***sudo /etc/rc.d/sysctl restart***

Traffic Prioritisation (1)

- On the client:
  - `ping 4.2.2.2`
  - `fetch http://196.200.218.200/bigfile`
- On the bandwidth management box:
  - `sudo kldload ipfw dummynet`
  - `sudo ipfw add pipe 1 ip from any to 196.200.218.0/24`
  - `sudo ipfw add pipe 2 ip from 196.200.218.0/24 to any`

AfNOG

Traffic Prioritisation (2)

```
sudo ipfw queue 1 config pipe 1 weight 100
sudo ipfw queue 2 config pipe 1 weight 50
sudo ipfw queue 3 config pipe 2 weight 100
sudo ipfw queue 4 config pipe 2 weight 50
sudo ipfw flush
sudo ipfw add queue 1 icmp from any to 196.200.218.0/24
sudo ipfw add queue 2 ip from any to 196.200.218.0/24
sudo ipfw add queue 3 icmp from 196.200.218.0/24 to any
sudo ipfw add queue 4 ip from 196.200.218.0/24 to any
```

Hard quotas

- pmacct database comes in very useful!
-
  ```
  echo 'SELECT ip_dst, sum(bytes) AS bytes
  FROM acct_v6
  WHERE ip_dst LIKE "196.200.218.%"
  AND ip_src NOT LIKE "196.200.218.%"
  GROUP BY ip_dst
  HAVING bytes > 1000000' |
  mysql pmacct -u root |
  while read ip bytes; do
      ipfw add deny ip from $ip to any
      ipfw add deny ip from any to $ip
  done
  ```