Could SP-NAT Save the Internet?

WAND, University of Waikato

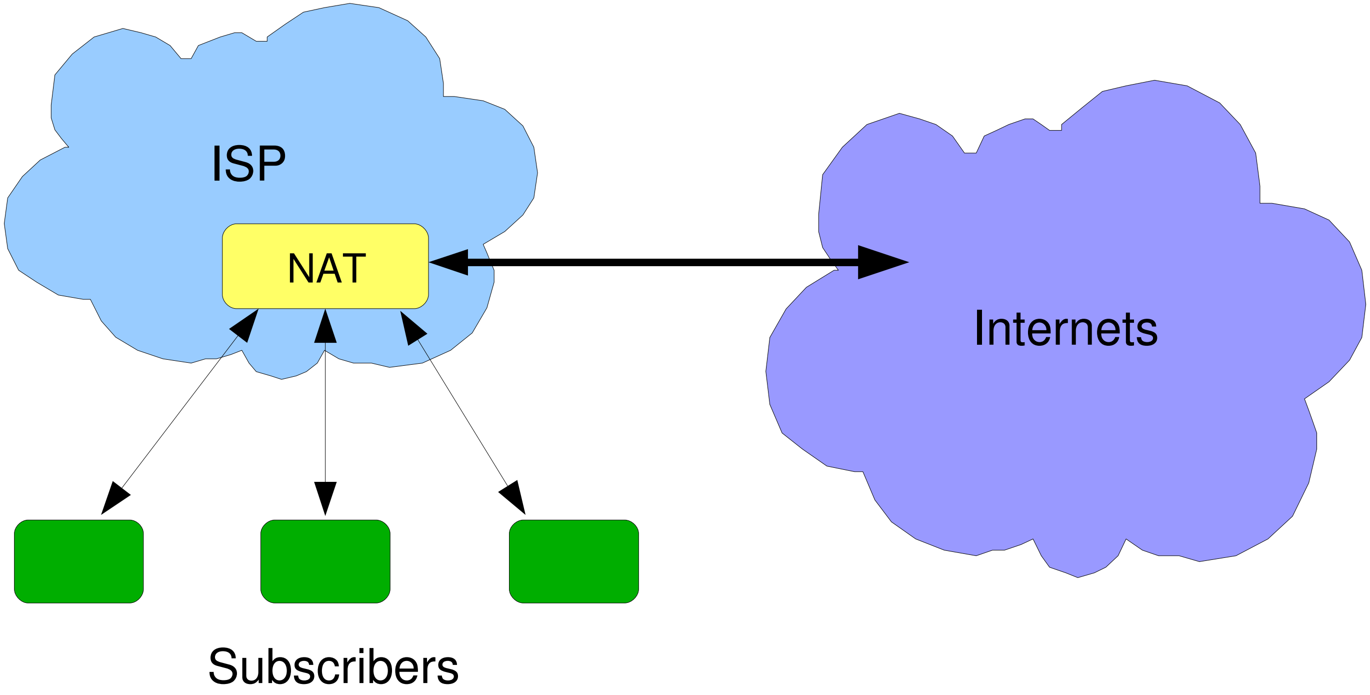
THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

29 January 2009

WAND Network Research Group

Service Provider NAT

- Aim is to reduce IPv4 address consumption
- Multiple subscribers share a single public IPv4 address
- NAT device is located within the ISP-managed network



Research Questions

- Provisioning
  - How many subscribers per NAT device?
  - Can existing subscriber behaviour be accommodated?
  - What level of restrictions would affect the least subscribers?

- Incoming sessions
  - How many subscribers are accepting incoming sessions?
  - What services are those subscribers running?

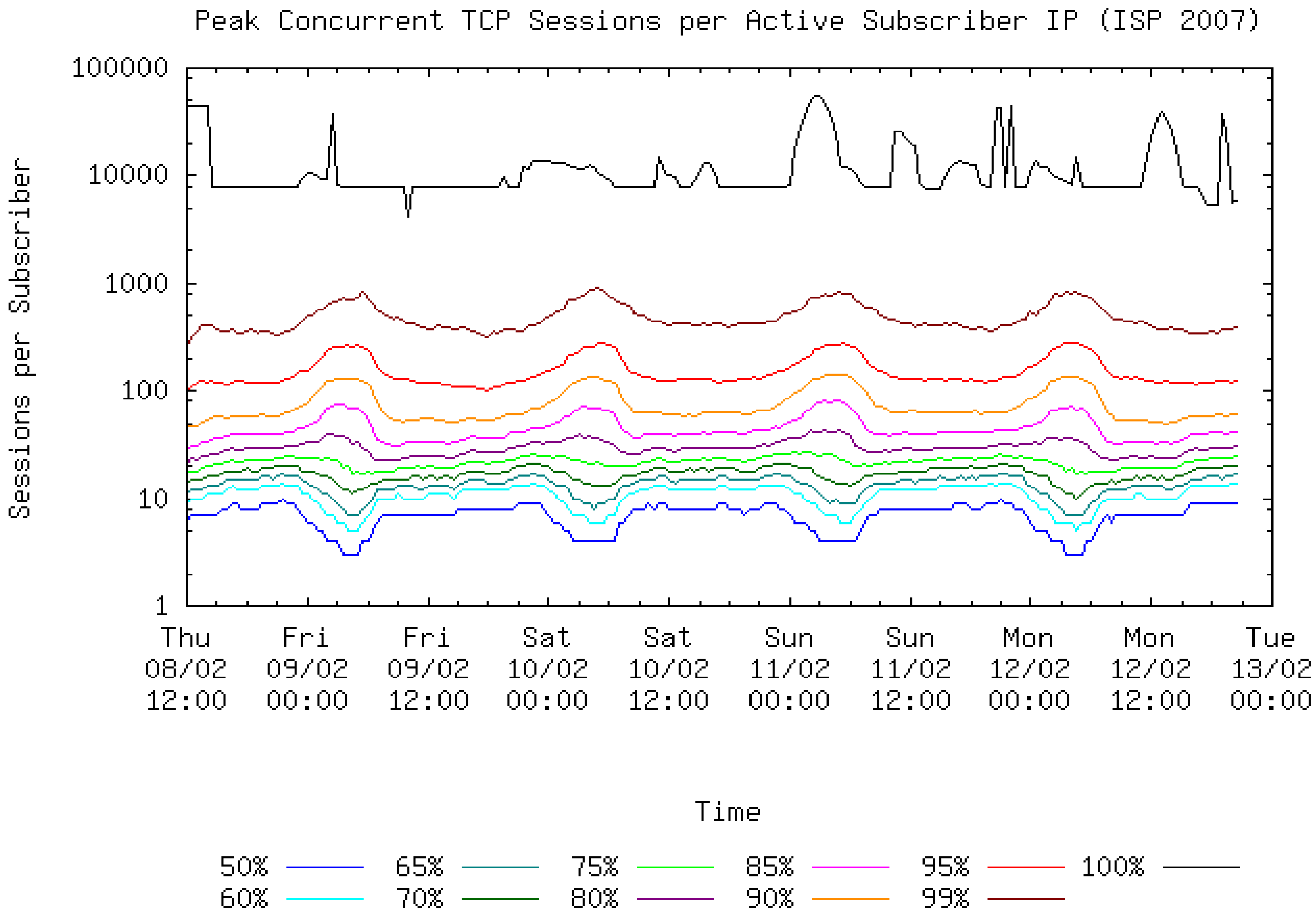
Analysis

- Analyse traces captured from two different NZ ISPs
  - ISP 2007 – DSL customer traffic from February 2007
  - ISP 2009 – Captured from a new monitor in January 2009
- Track sessions (flows) for each subscriber IP
  - Outgoing session creation rate
  - Peak concurrent outgoing sessions
  - Incoming sessions – quantity and protocol

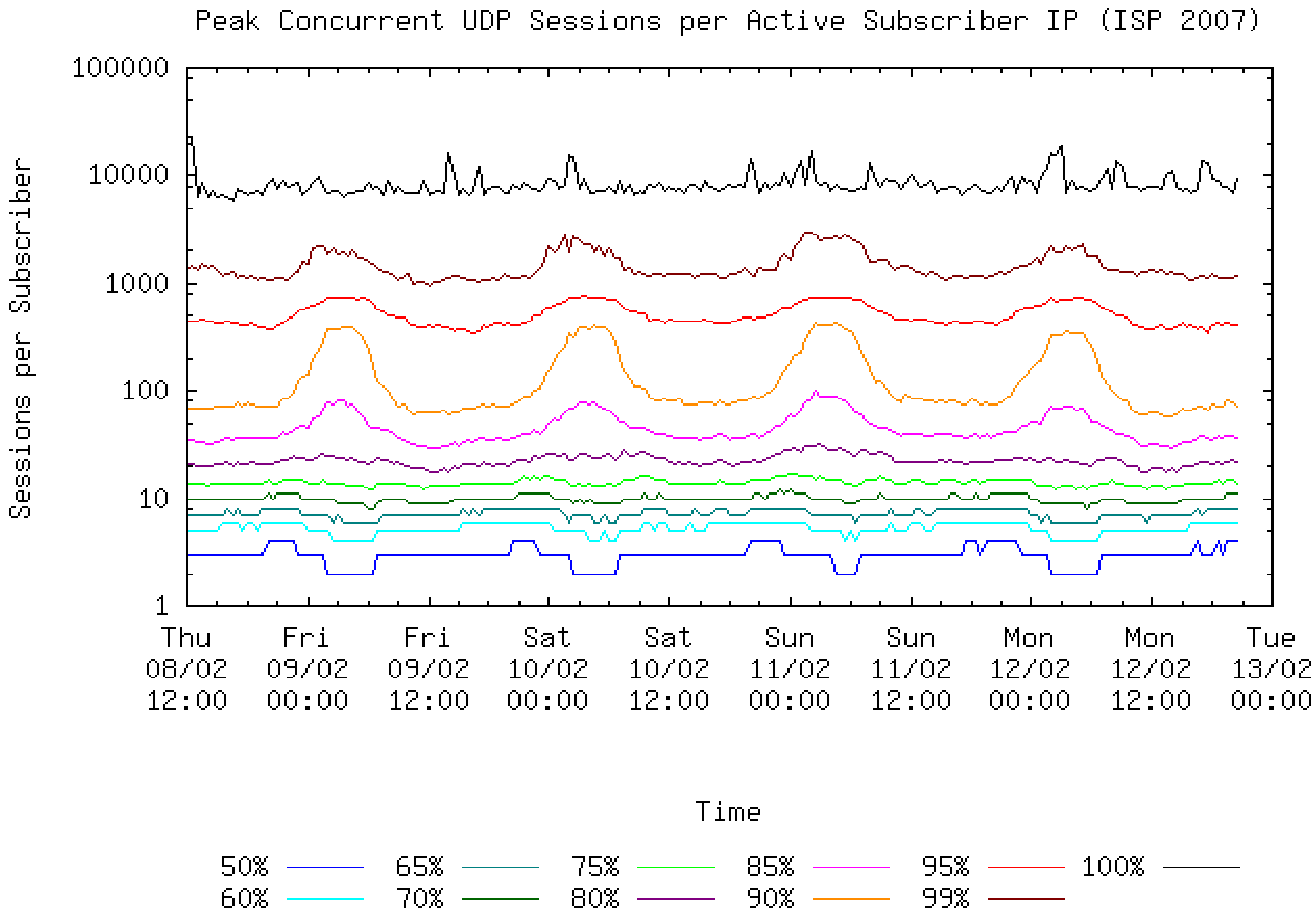
Session Counting

- TCP Sessions
  - Must begin with a SYN packet
  - Incoming sessions must also observe a SYN ACK
  - A session is expired after a period of inactivity
    - Incomplete 3-way handshake = 4 minutes
    - Established TCP connection = 2 hours and 4 minutes
    - If a RST or FIN ACK is observed = immediate expiry
- UDP Sessions
  - All sessions are expired after 2 minutes and 20 seconds of inactivity

Outgoing Sessions



Outgoing Sessions



Incoming Sessions

- NAT violates the IP connectivity model
  - External devices cannot directly connect to hosts behind NAT
- This creates problems for end-users that wish to ...
  - Operate Internet services, such as a web server
  - Participate in peer-to-peer

Incoming Sessions

- Possible solutions
    - Port forwarding
        - Subscribers cannot interact with the NAT device directly
        - Can only forward each port number once per NAT device
    - NAT traversal techniques
        - Supported by some but not all applications
        - Lack of standardisation for NAT device behaviour
            - BEHAVE IETF working group is trying to resolve this

Incoming Sessions

- Questions
  - How many subscribers are accepting incoming connections?
  - What services are they operating?
  - What ports are being used to run services?
  - As an aside, how useful are port numbers for identifying services?

Incoming Sessions

- Observed subscriber IPs that accept an incoming TCP connection
  - For ISP 2007:

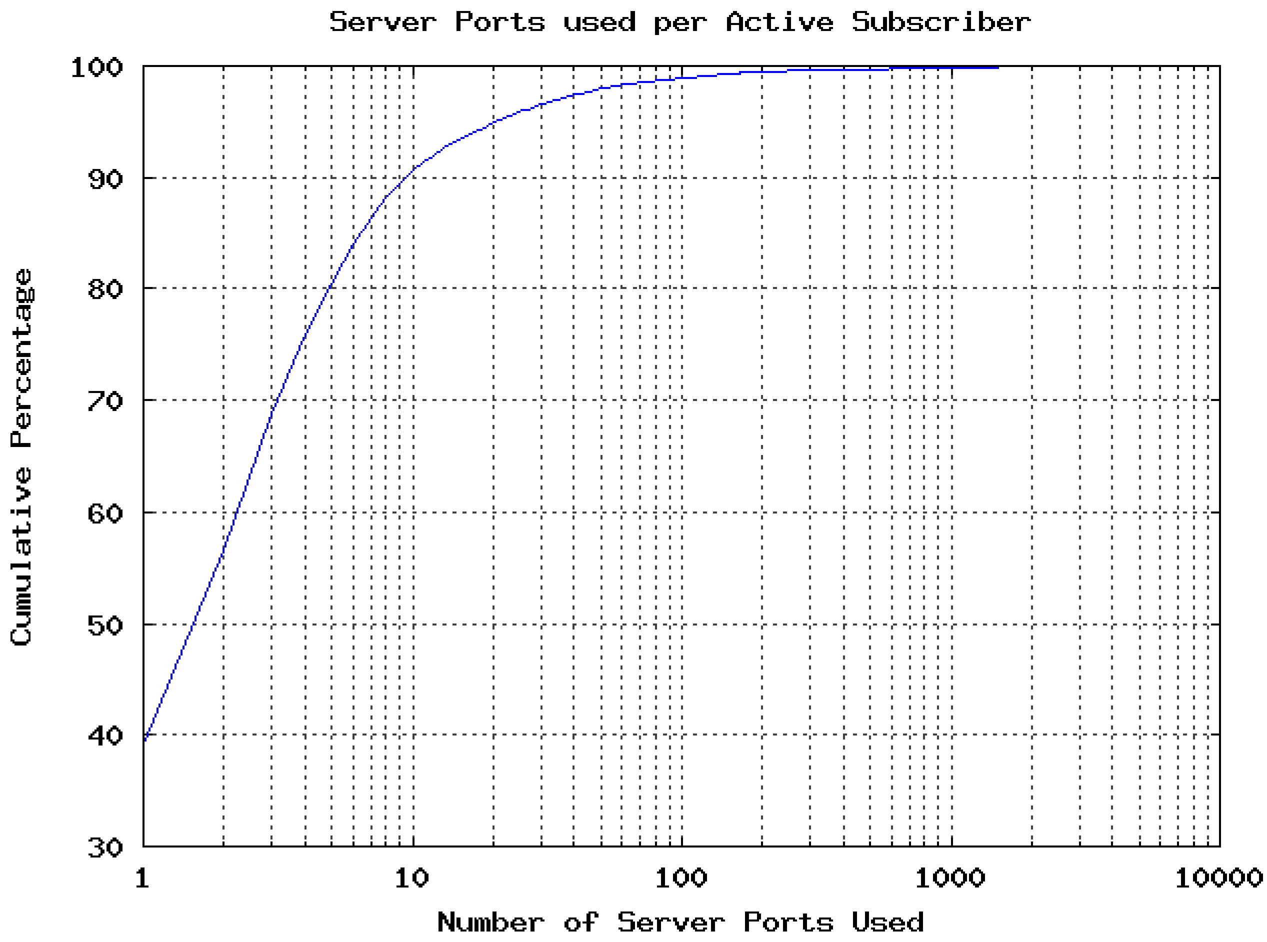
44.2 %

  - For ISP 2009:

30.8 %

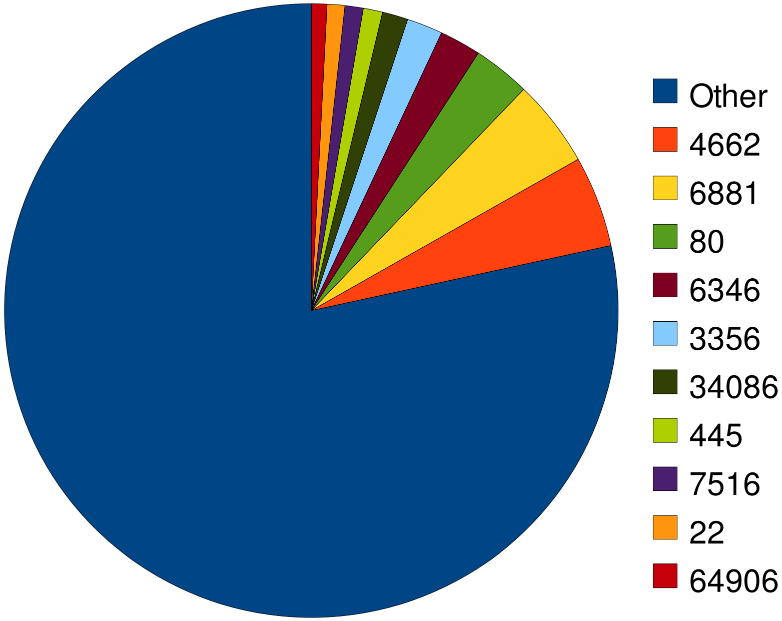
Incoming TCP Sessions (ISP 2007)

- How many server ports are being used by each IP?



Incoming TCP Sessions (ISP 2007)

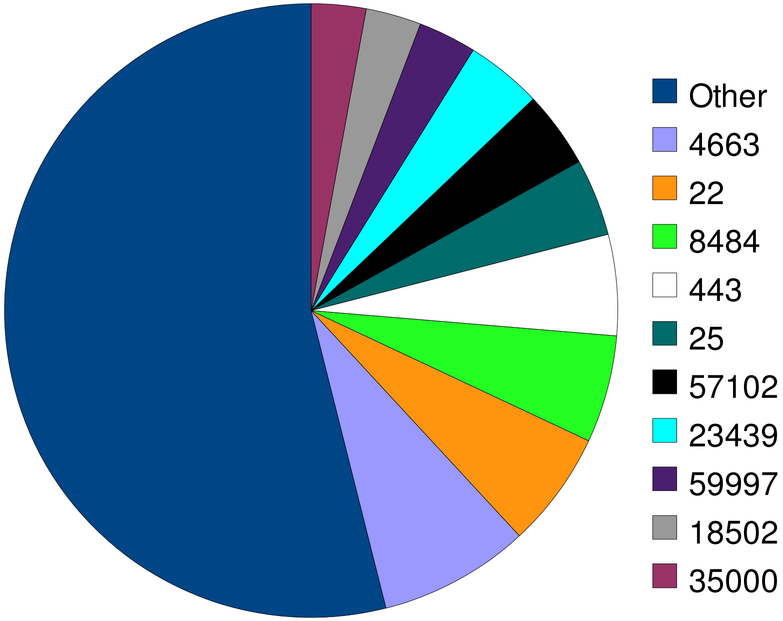
- Broken down by server port



Port	Flows (%)
4662	4.799
6881	4.614
80	3.021
6346	2.177
3356	1.889
34086	1.360
445	1.023
7516	0.964
22	0.924
64906	0.823
Other	78.406

Incoming TCP Sessions (ISP 2009)

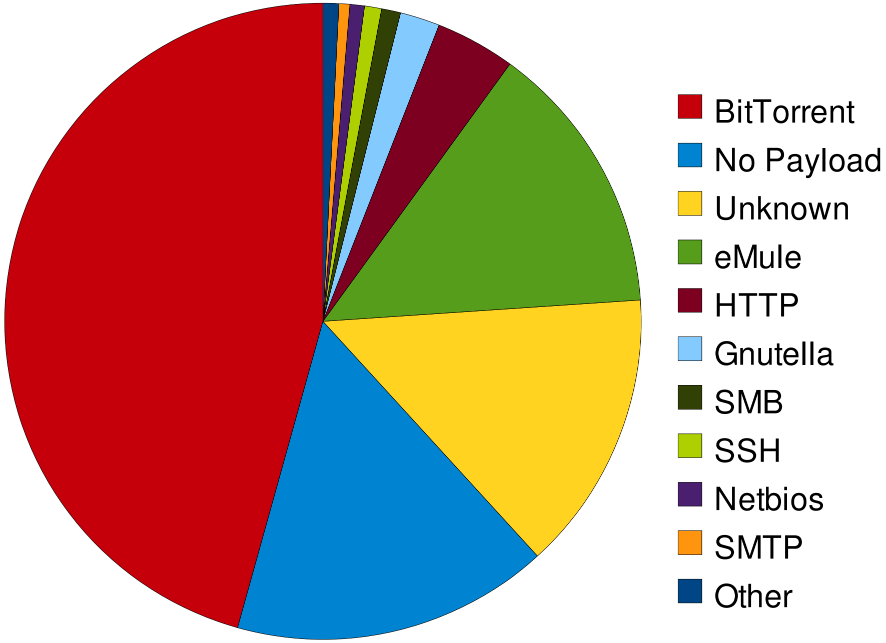
- Broken down by server port



Port	Flows (%)
4663	7.955
22	6.139
8484	5.650
443	5.320
25	4.064
57102	4.039
23439	4.028
59997	3.061
18502	2.922
35000	2.884
Other	53.938

Incoming TCP Sessions (ISP 2007)

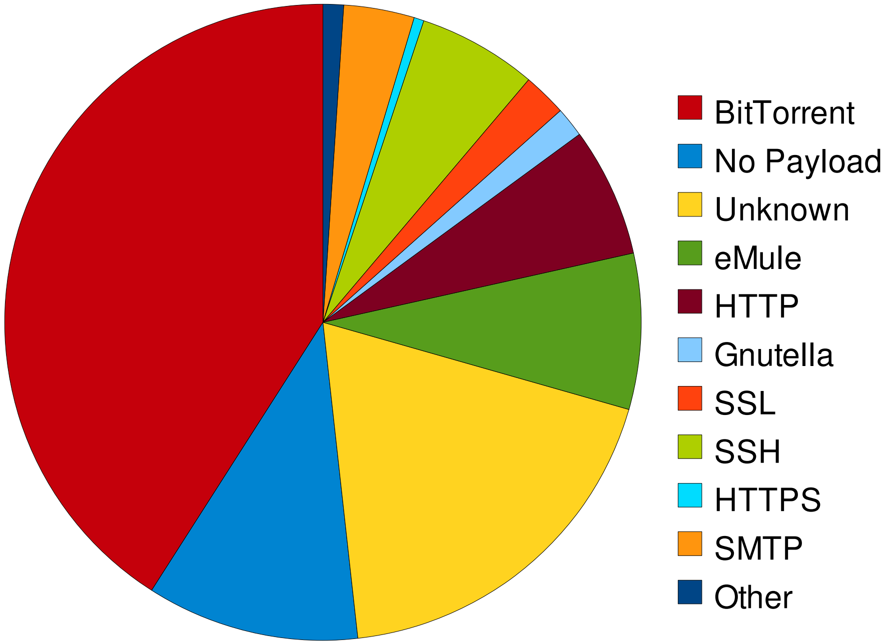
- Using the four-byte L7 protocol analysis rules



Protocol	Flows (%)
BitTorrent	45.678
No Payload	16.108
Unknown TCP	14.282
eMule	13.933
HTTP	4.060
Gnutella	2.013
SMB	0.965
SSH	0.868
Netbios	0.744
SMTP	0.539
Other	0.810

Incoming TCP Sessions (ISP 2009)

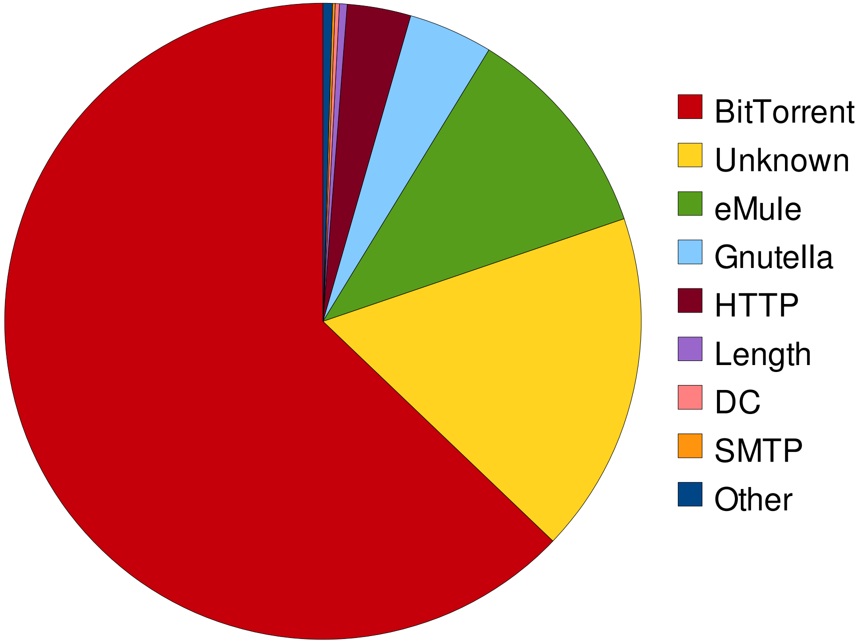
- Using the four-byte L7 protocol analysis rules



Protocol	Flows (%)
BitTorrent	40.963
Unknown TCP	18.830
No Payload	10.790
eMule	7.912
HTTP	6.572
SSH	6.050
SMTP	3.576
SSL	2.222
Gnutella	1.520
HTTPS	0.514
Other	1.051

Incoming TCP Sessions (ISP 2007)

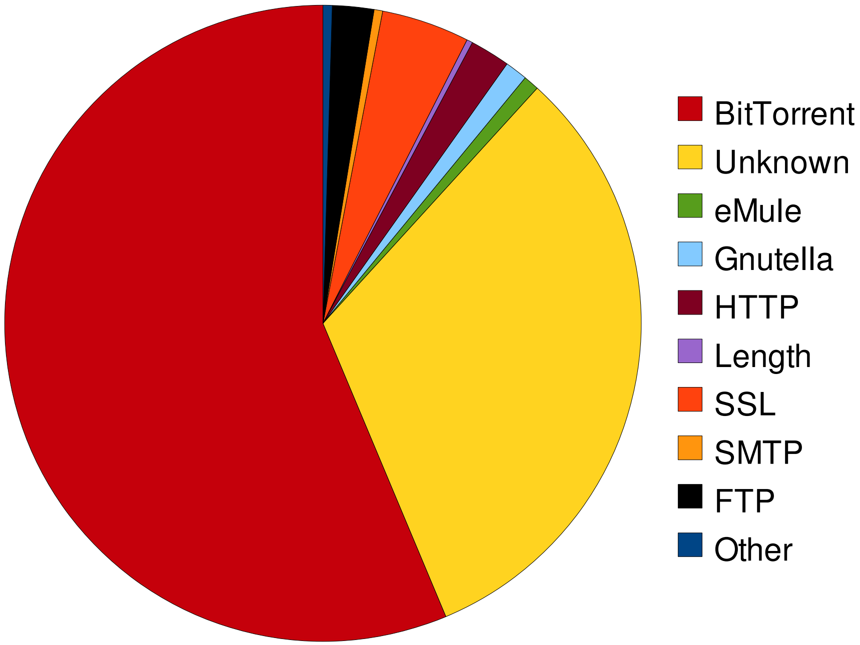
- Byte counts instead of flow counts



Protocol	Bytes (%)
BitTorrent	62.862
Unknown TCP	17.365
eMule	11.045
Gnutella	4.273
HTTP	3.241
Length	0.386
DirectConnect	0.215
SMTP	0.129
Other	0.484

Incoming TCP Sessions (ISP 2009)

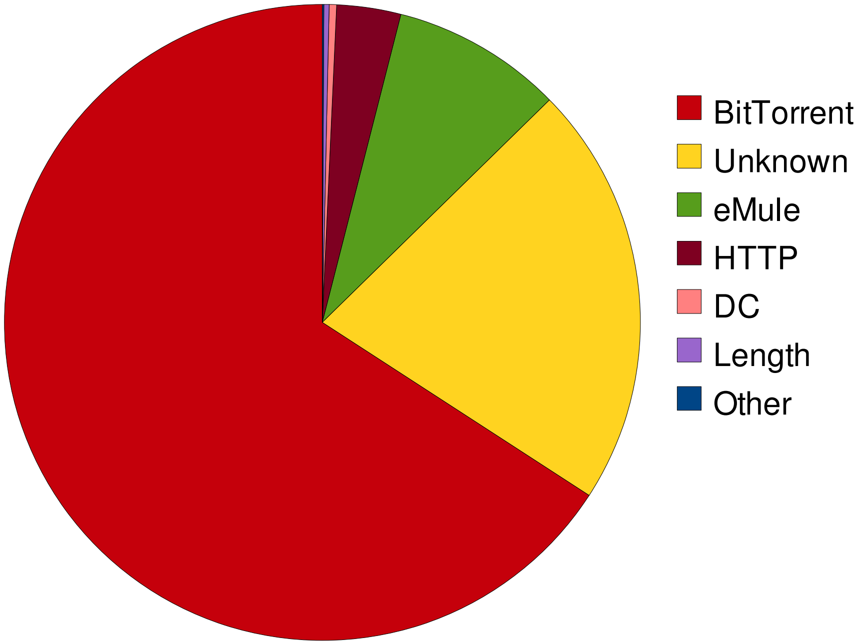
- Byte counts instead of flow counts



Protocol	Bytes (%)
BitTorrent	56.327
Unknown TCP	31.924
SSL	4.470
FTP Data	2.106
HTTP	2.053
Gnutella	1.135
eMule	0.787
SMTP	0.437
Length	0.291
Other	0.470

Incoming TCP Sessions (ISP 2007)

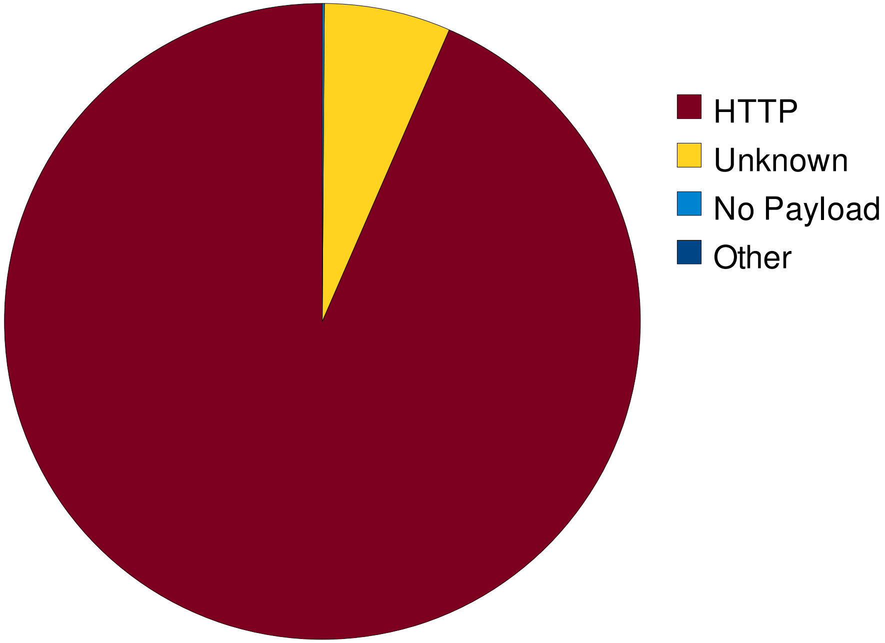
- Utilization of TCP port 80 (byte counts)



Protocol	**Bytes (%)**
BitTorrent	65.839
Unknown TCP	21.501
eMule	8.682
HTTP	3.263
DirectConnect	0.372
Length	0.269
Other	0.074

Incoming TCP Sessions (ISP 2009)

- Utilization of TCP port 80 (byte counts)



Protocol	Bytes (%)
HTTP	93.467
Unknown TCP	6.422
No Payload	0.110
Other	0.001

Handy Links

- http://www.wand.net.nz/~salcock/nznog09/
- Email: salcock@cs.waikato.ac.nz

WAND Network Research Group
Department of Computer Science
The University of Waikato
Private Bag 3105
Hamilton, New Zealand

www.crc.net.nz
www.wand.net.nz
www.waikato.ac.nz