This weeks DDoS against the root and TLDs

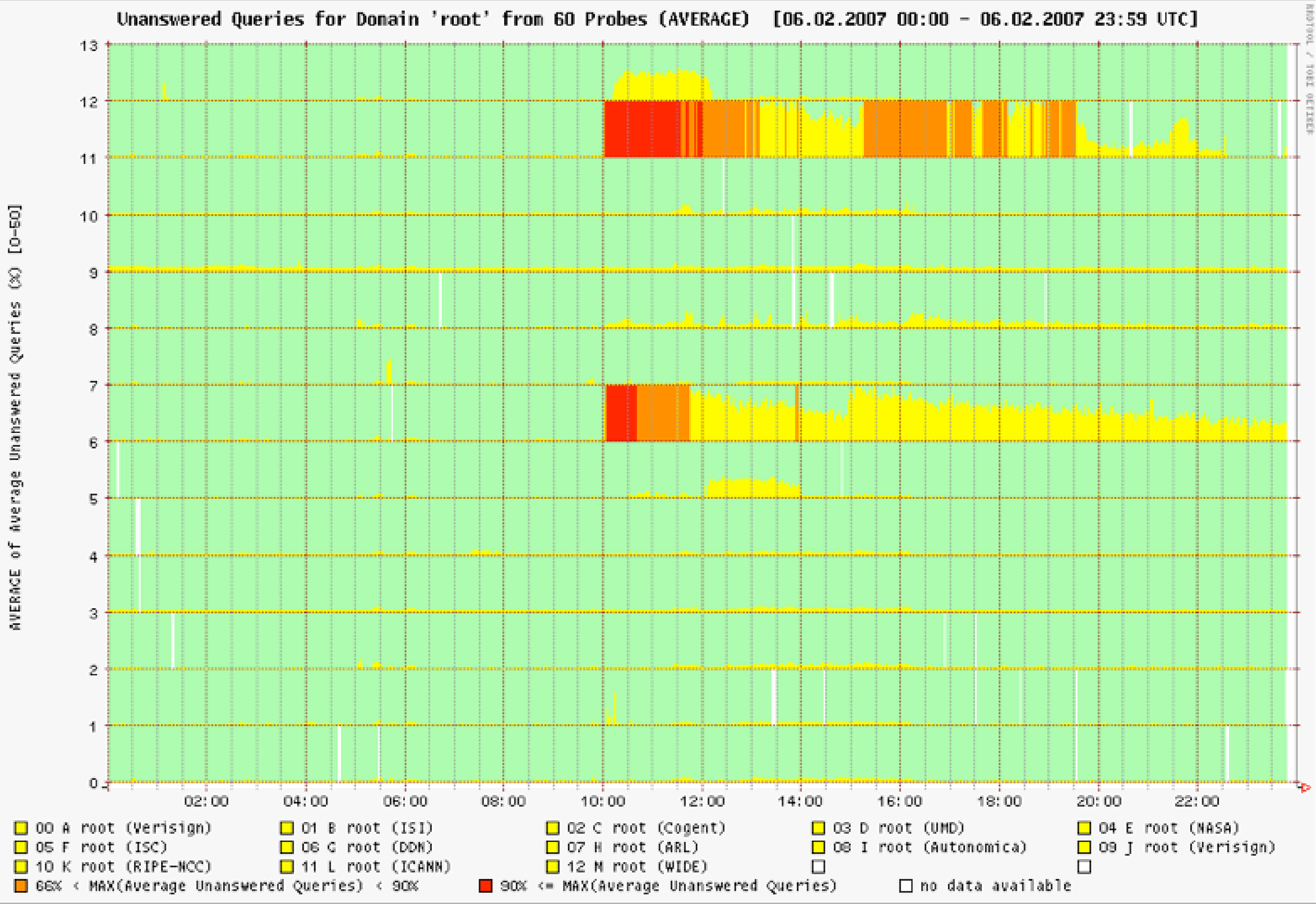
Dave Knight

Nanog 39, Toronto

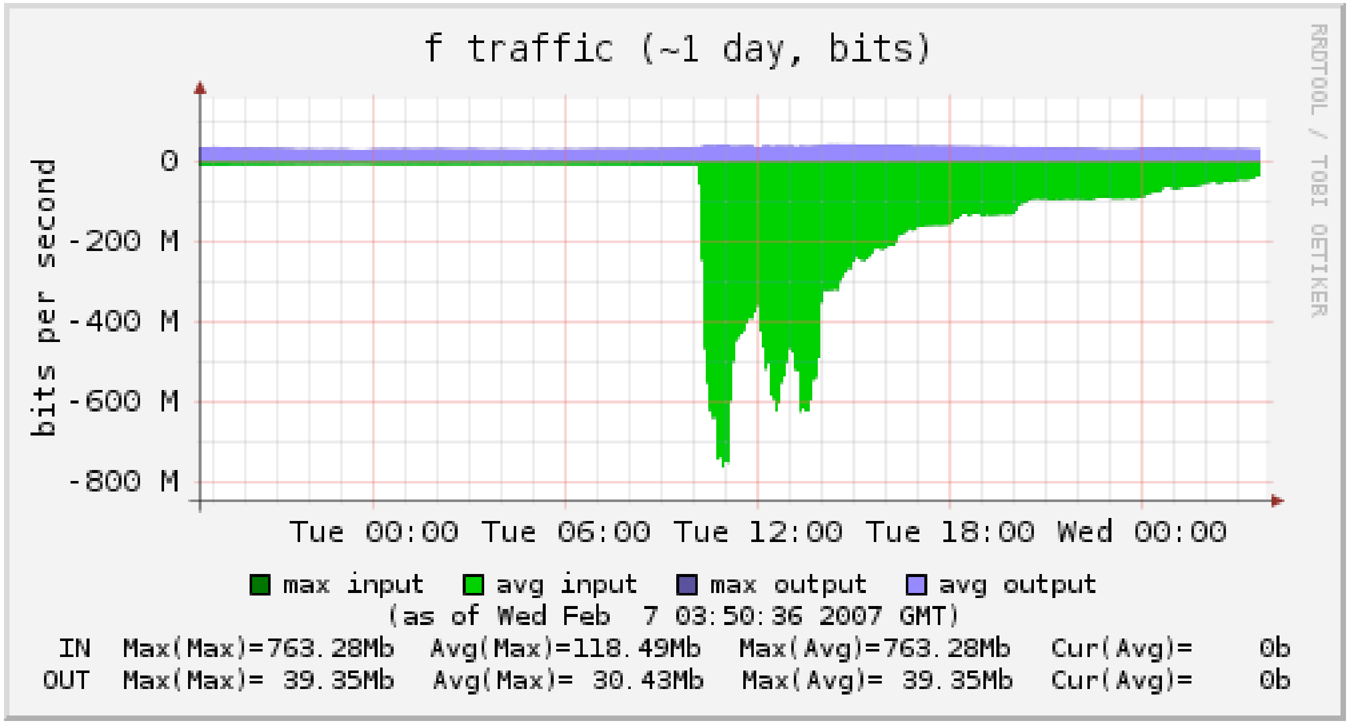
February 6th 2007, 10:00 UTC

A number of the Internet root and TLD name servers sustained a DDoS attack. While this attack didn't have an impact on the service to end-users it was measured and we'll share the preliminary observations made at F-root including the type, quantity and distribution of attack traffic and how we coped.

http://dnsmon.ripe.net

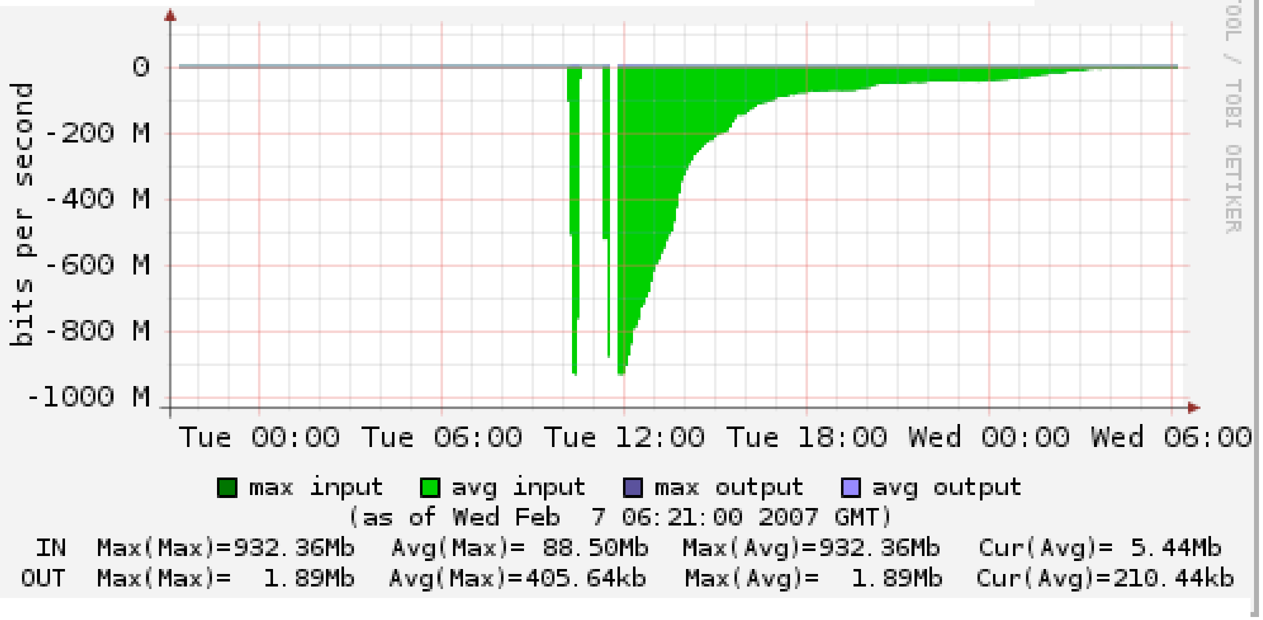


Aggregated traffic arriving at F-root name servers globally



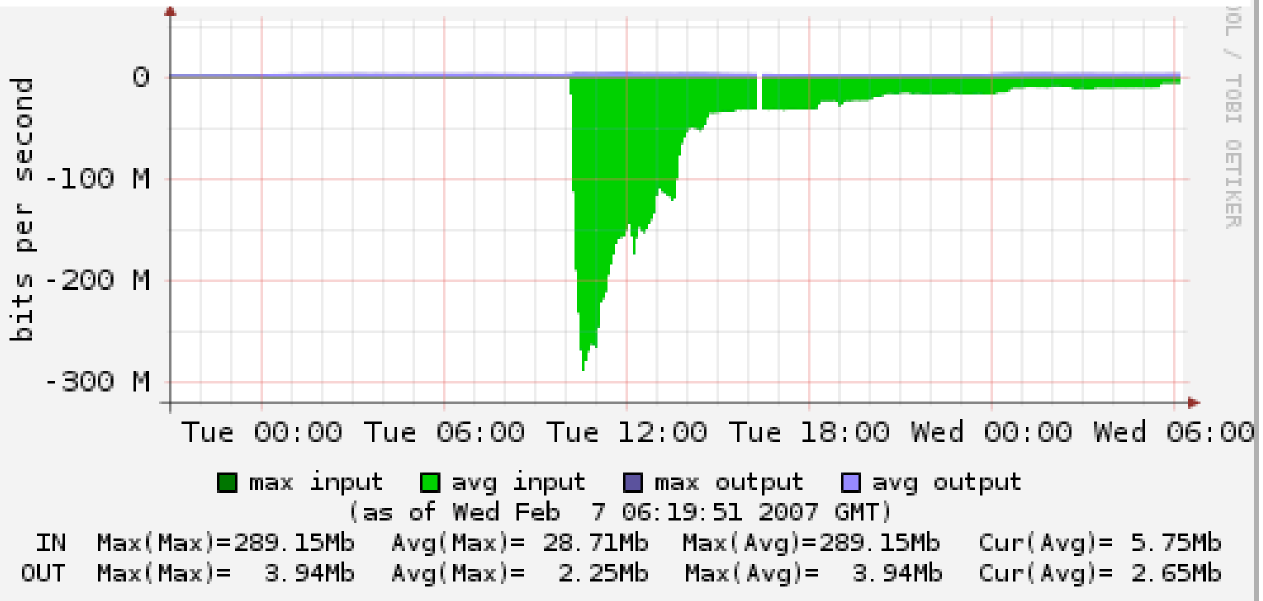
```
                         (as of Wed Feb  7 03:50:36 2007 GMT)
 IN  Max(Max)=763.28Mb  Avg(Max)=118.49Mb  Max(Avg)=763.28Mb  Cur(Avg)=     0b
OUT  Max(Max)= 39.35Mb  Avg(Max)= 30.43Mb  Max(Avg)= 39.35Mb  Cur(Avg)=     0b
```

Seoul - capped at 1Gb/s



```
                (as of Wed Feb  7 06:21:00 2007 GMT)
 IN  Max(Max)=932.36Mb   Avg(Max)= 88.50Mb   Max(Avg)=932.36Mb   Cur(Avg)= 5.44Mb
OUT  Max(Max)=  1.89Mb   Avg(Max)=405.64kb   Max(Avg)=  1.89Mb   Cur(Avg)=210.44kb
```

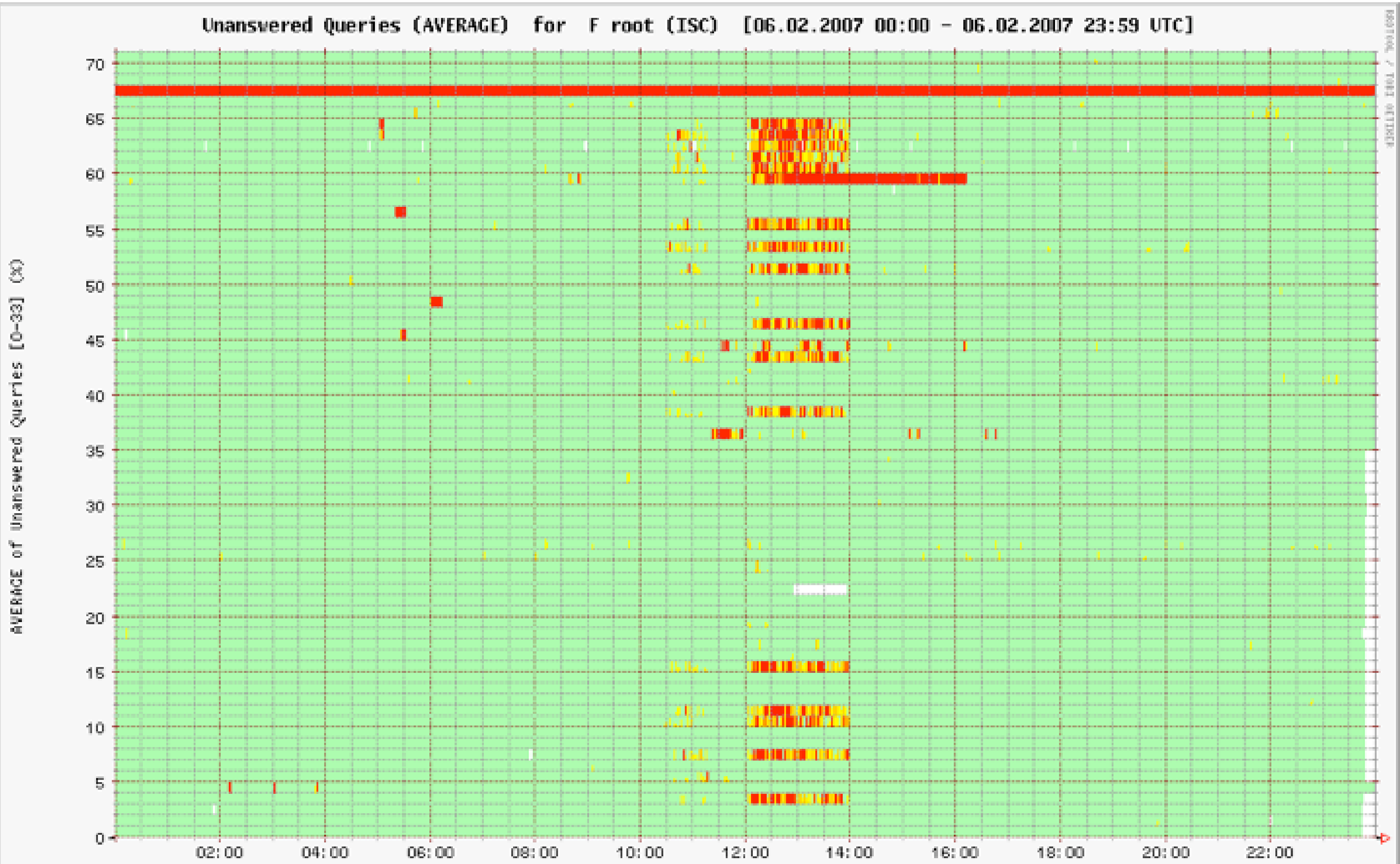
Beijing - peaked at 300Mb/s



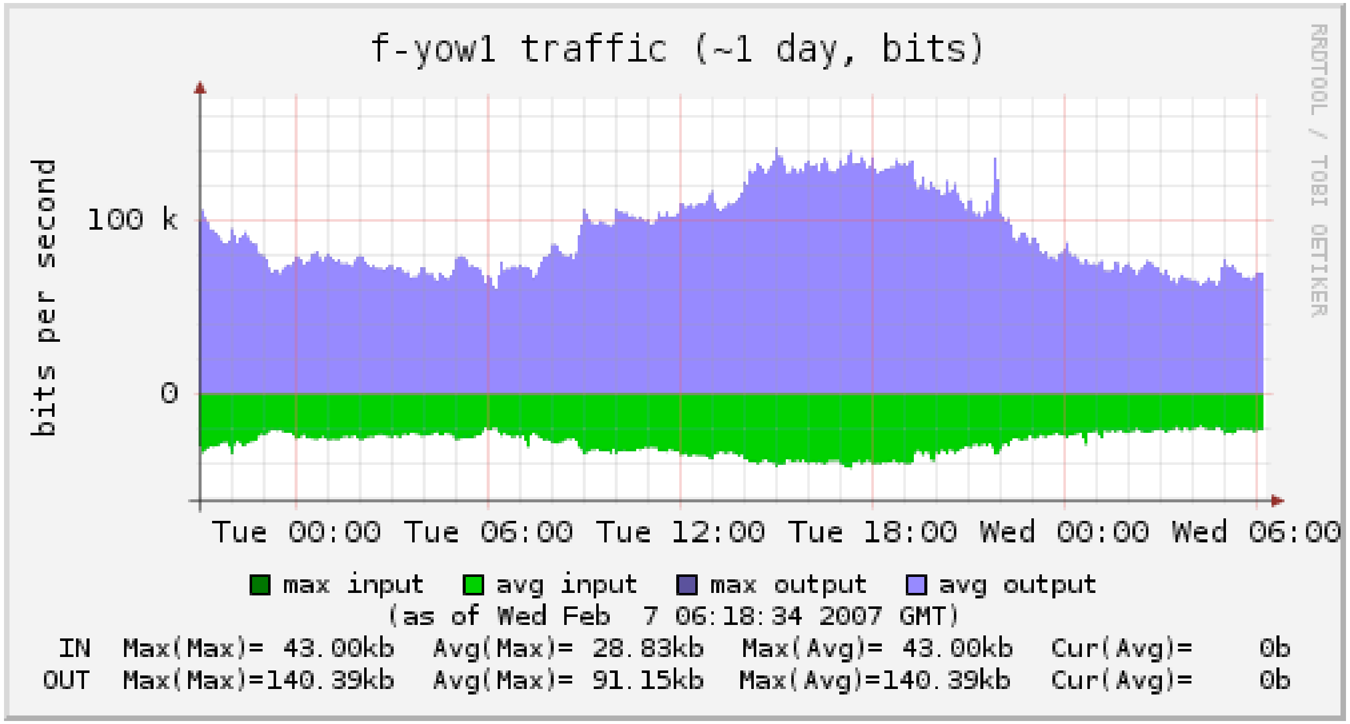
```
                (as of Wed Feb  7 06:19:51 2007 GMT)
 IN  Max(Max)=289.15Mb   Avg(Max)= 28.71Mb   Max(Avg)=289.15Mb   Cur(Avg)= 5.75Mb
OUT  Max(Max)=  3.94Mb   Avg(Max)=  2.25Mb   Max(Avg)=  3.94Mb   Cur(Avg)= 2.65Mb
```

The bulk of the traffic toward F-root was contained by these two local nodes

F-root service was degraded from some vantage points during the first two hours of the attack

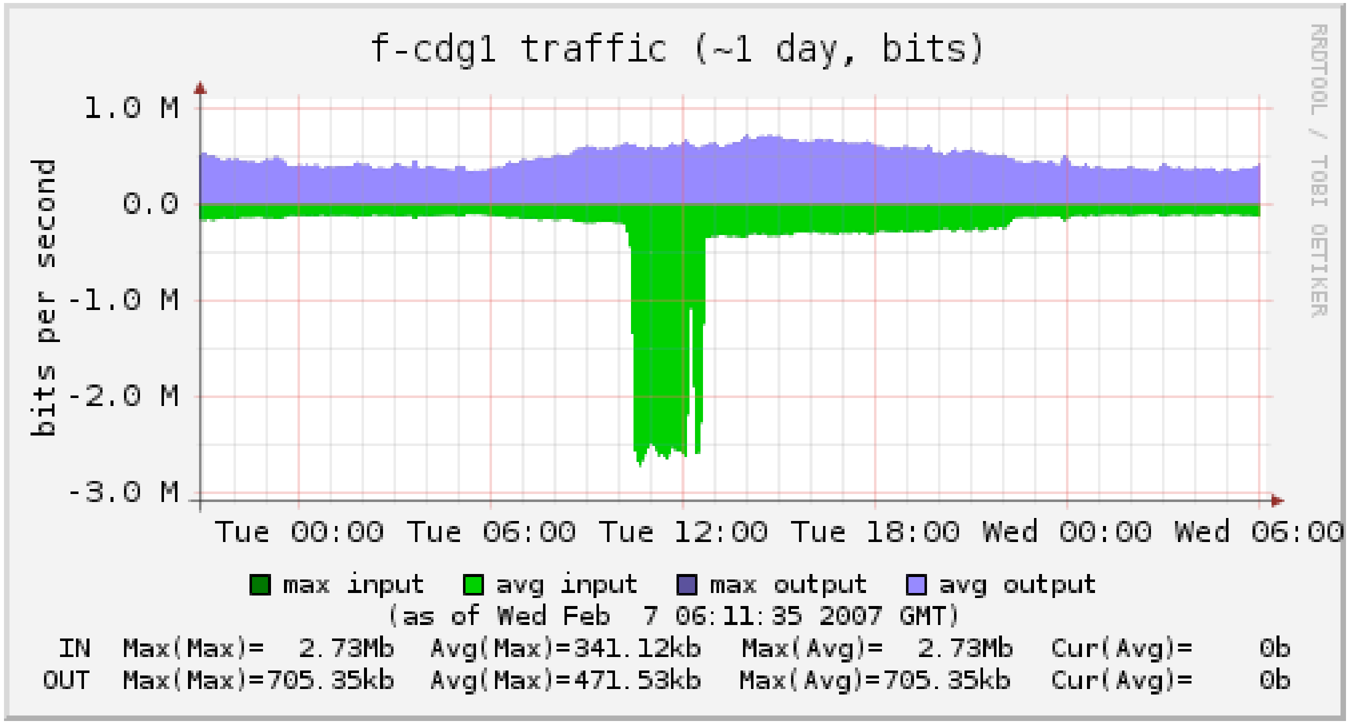


Some local nodes saw no attack traffic at all - this is Ottawa

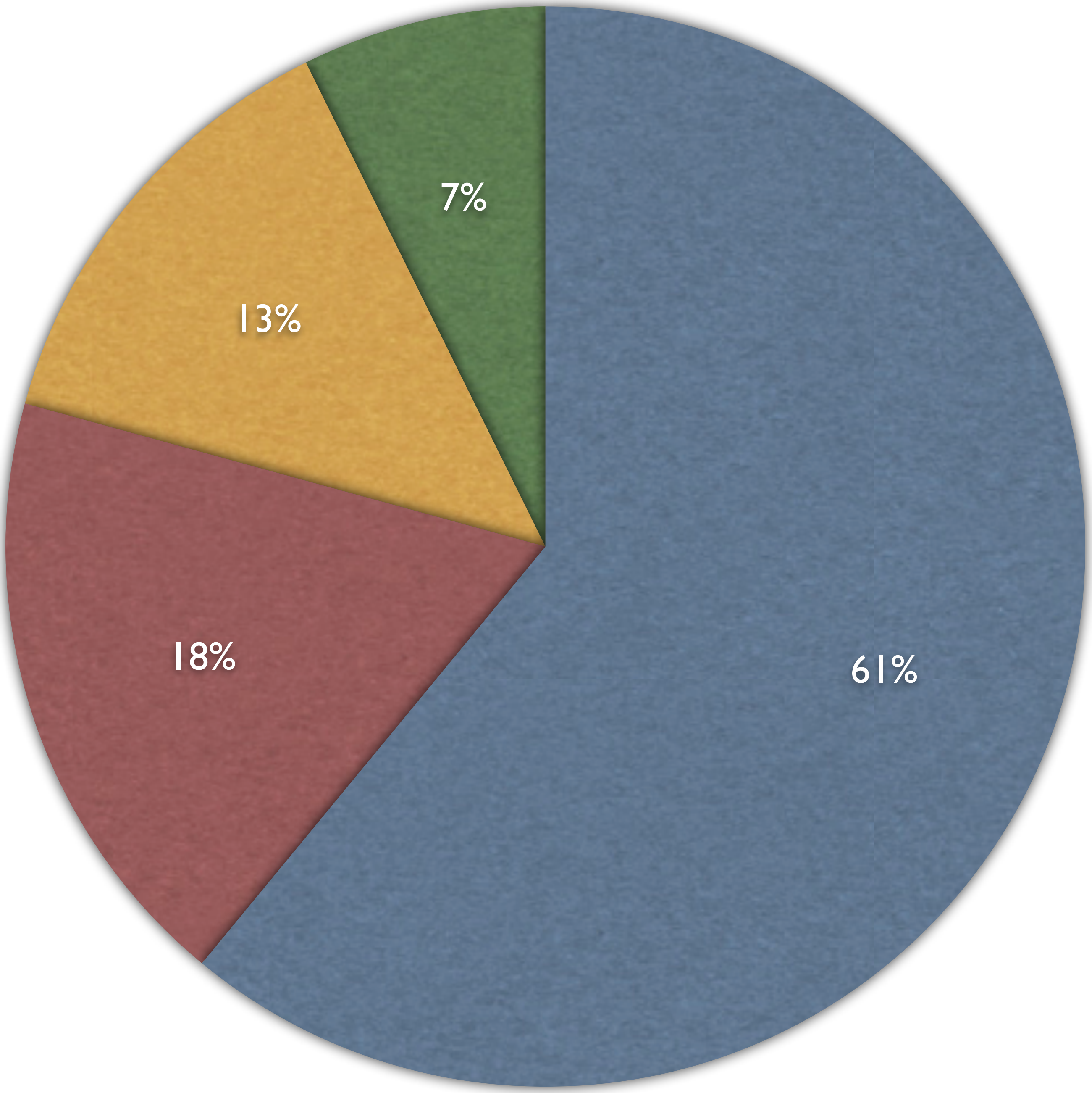


```
■ max input   ■ avg input   ■ max output   ■ avg output
              (as of Wed Feb  7 06:18:34 2007 GMT)
 IN  Max(Max)= 43.00kb  Avg(Max)= 28.83kb  Max(Avg)= 43.00kb  Cur(Avg)=    0b
OUT  Max(Max)=140.39kb  Avg(Max)= 91.15kb  Max(Avg)=140.39kb  Cur(Avg)=    0b
```

Some local nodes saw this odd shape - ad-hoc filtering of attack traffic in some networks?



Global Distribution of attack traffic



- 🟦 Seoul
- 🟥 Beijing
- 🟨 San Francisco
- 🟩 Other

Other equates to 35 F-root anycast nodes

What the packets looked like

Were bigger than normal

More than 350 bytes

Partially formed DNS messages

Contained broken query and update message, or just incorrect syntax altogether

Conclusion

Anycast did what it was supposed to and contained the bulk of the attack traffic within the region of origin.

This has been a very preliminary summary of our observations. In depth analysis of this attack will be continued within ISC's OARC for DNS. The collected data and the results of the analysis work will be available to OARC members.