Internet Background Radiation: Monitoring the Packet Plague

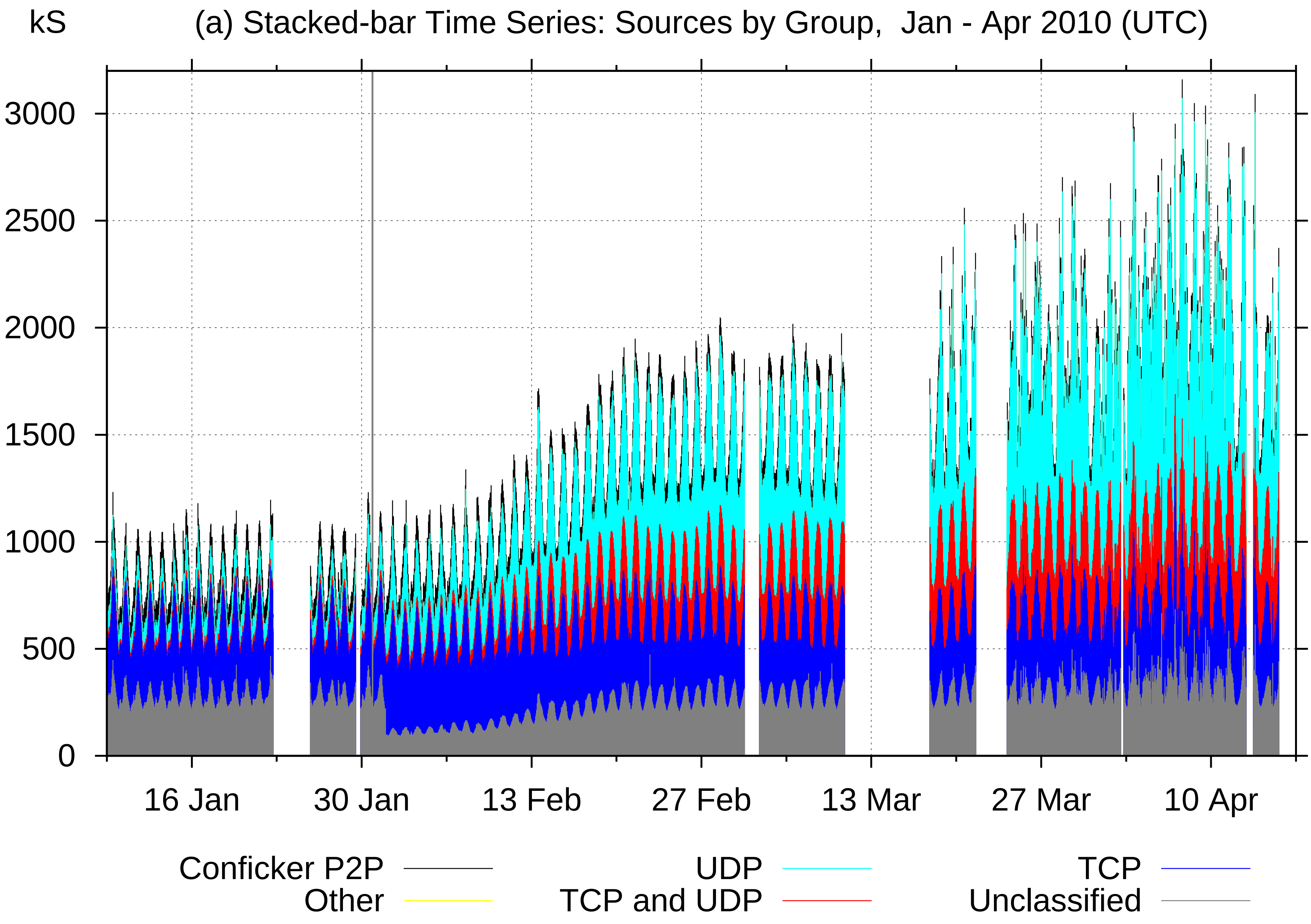
WAND group, Friday 18 Jun 10

Nevil Brownlee

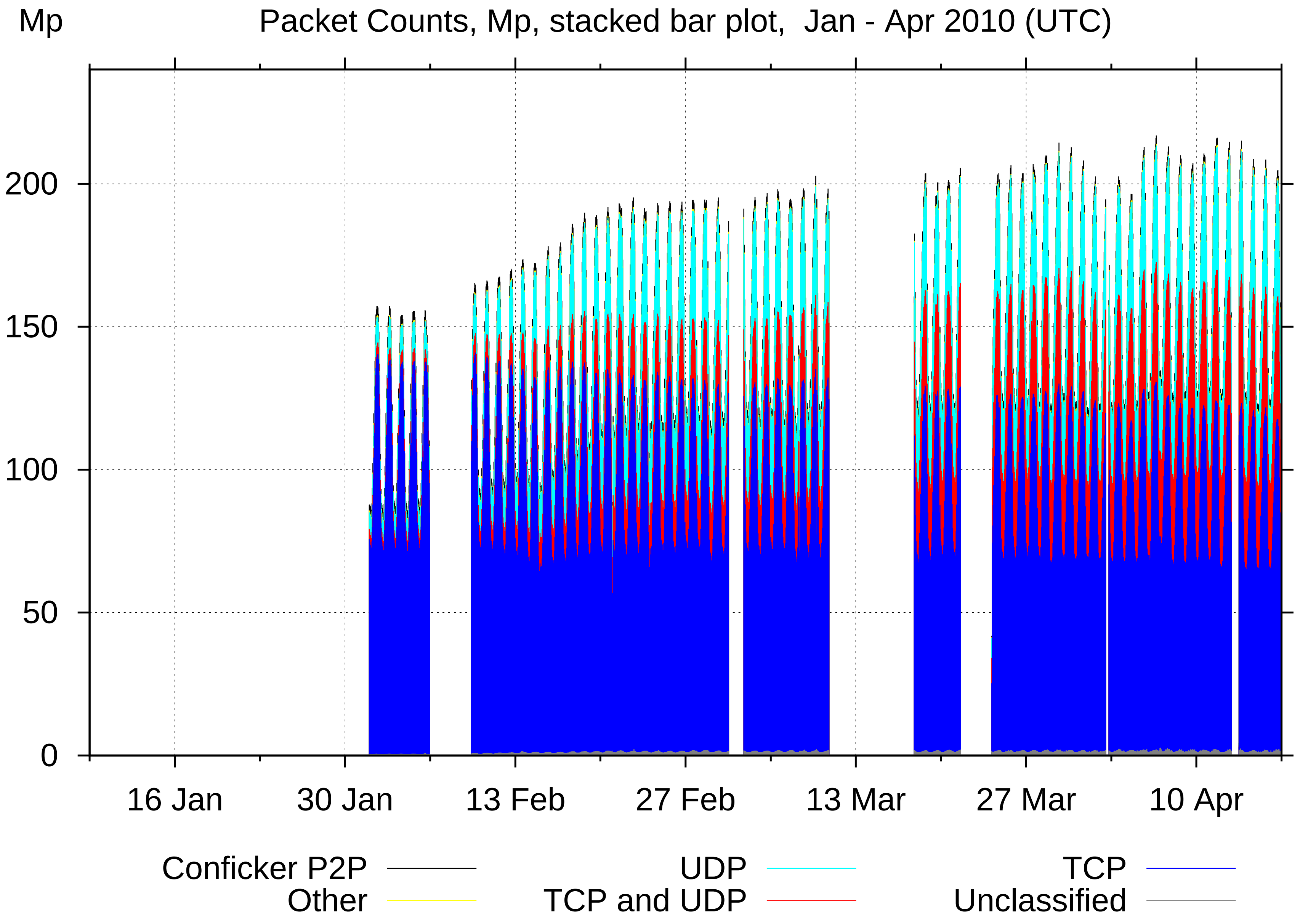
Unsolicited Packets: Source Taxonomy

Description	Source Type
TCP only, many addrs, same port	**TCP port probe**
TCP only, single packet per destination	TCP only, $>$1 pkt/addr
TCP only, single packet per destination	TCP only, 1 pkt/addr
UDP only, many addrs, same port	**UDP port probe**
UDP only, more than one packet per destination	UDP only, $>$1 pkt/addr
UDP only, single packet per destination	UDP only, 1 pkt/addr
Mixed TCP and UDP packets	**Both TCP and UDP**
Only other protocols	Other protocols
TCP only, ACK flag set	Backscatter
All packets Conficker C p2p	**Only Conficker p2p**
TCP+UDP only, some Conficker C packets	Mixed Conficker p2p
Source sent less than 20 (10 at trace end) packets	Unclassified

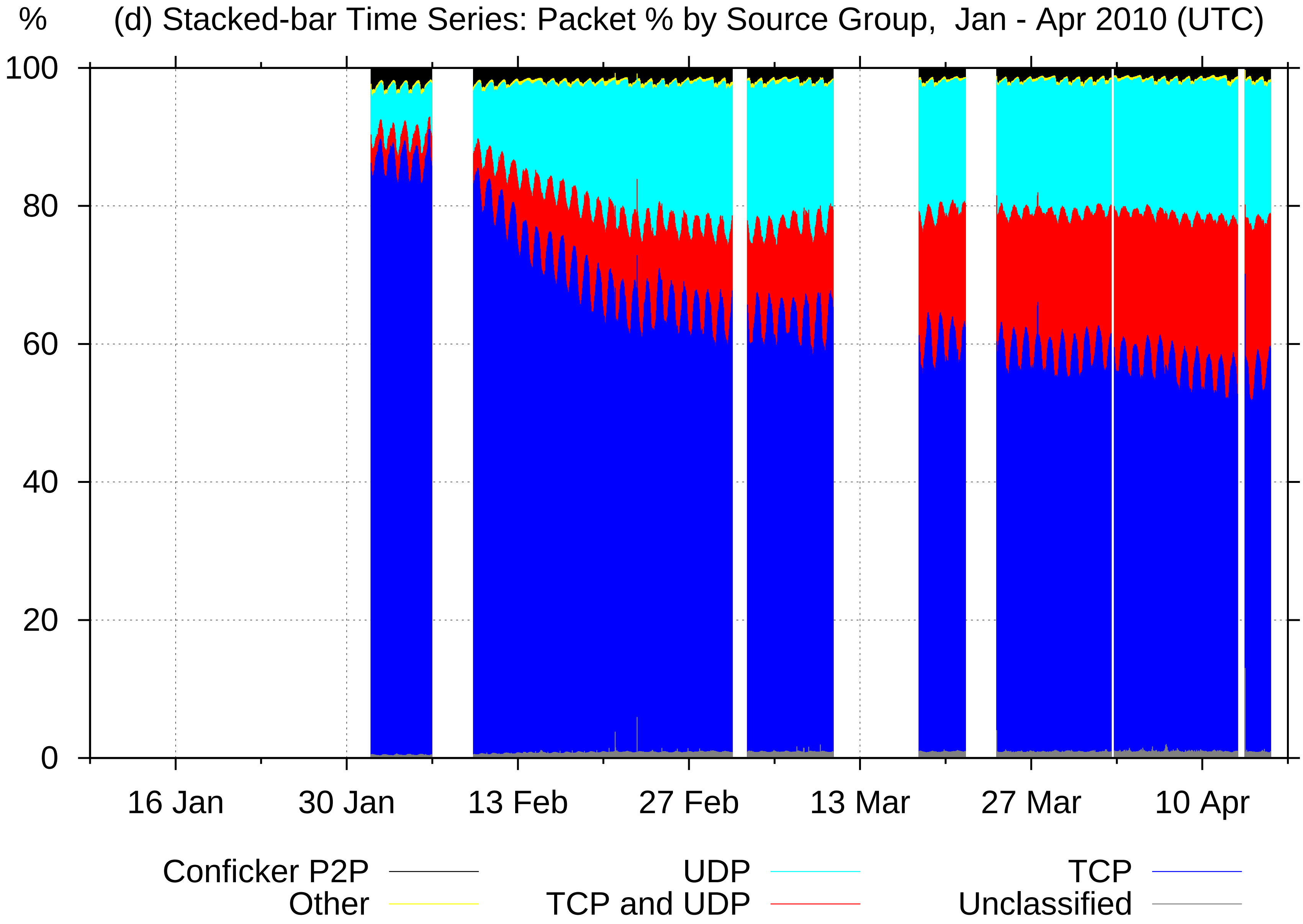
Aggregated Source Groups, kS/h



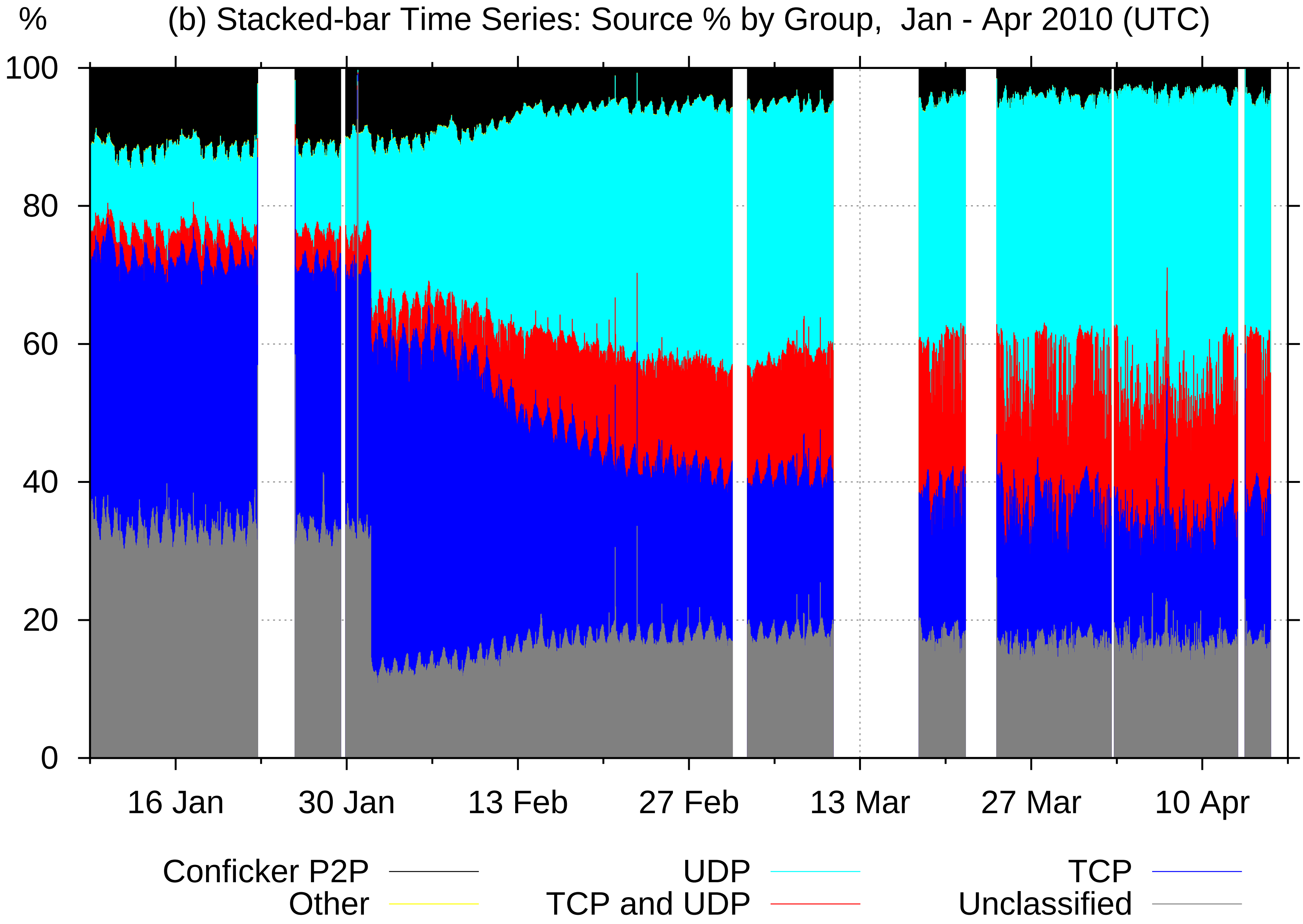
Packet Counts, Mp/h



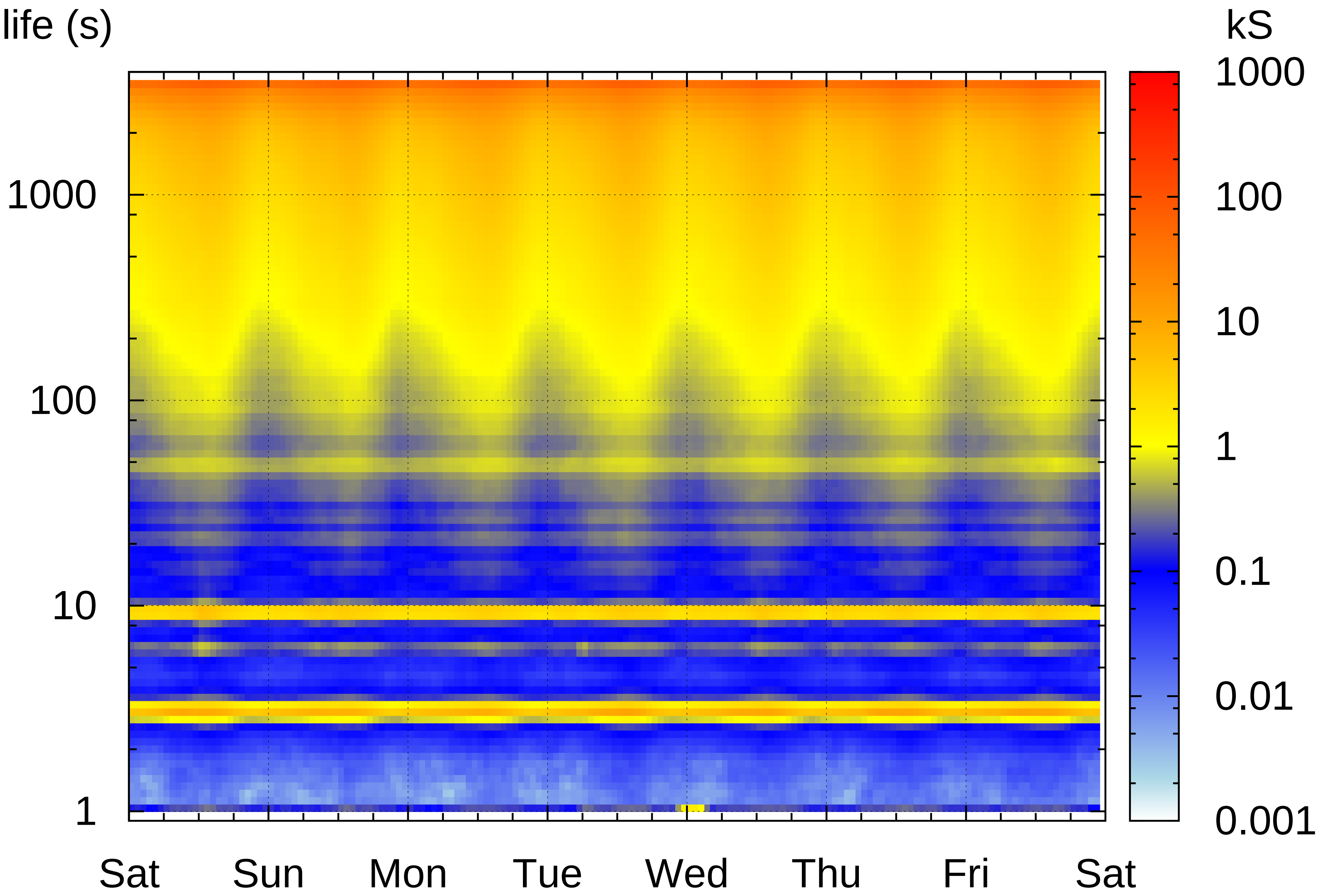
Packet Counts, % by Source Group



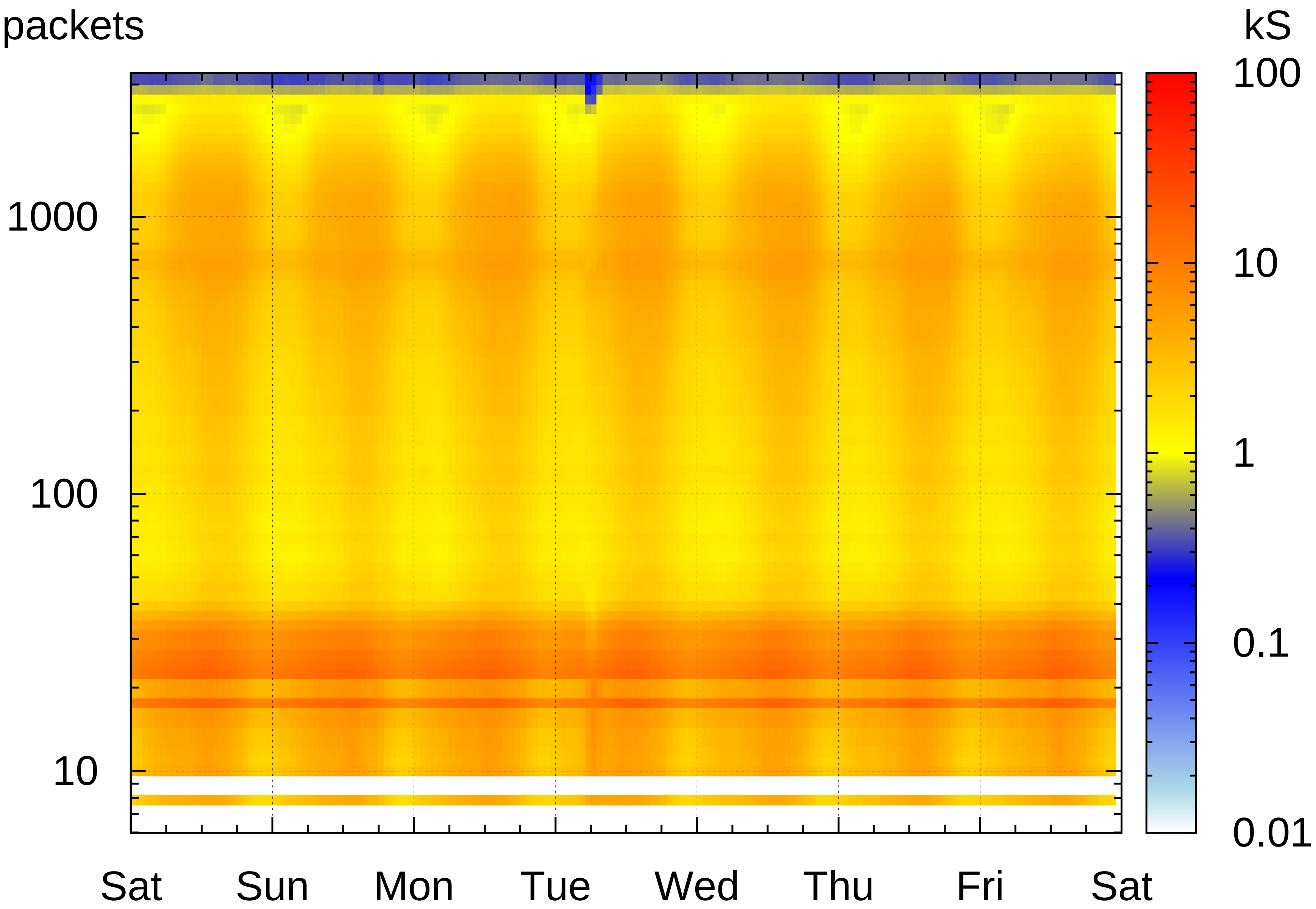
Aggregated Sources, % by Group



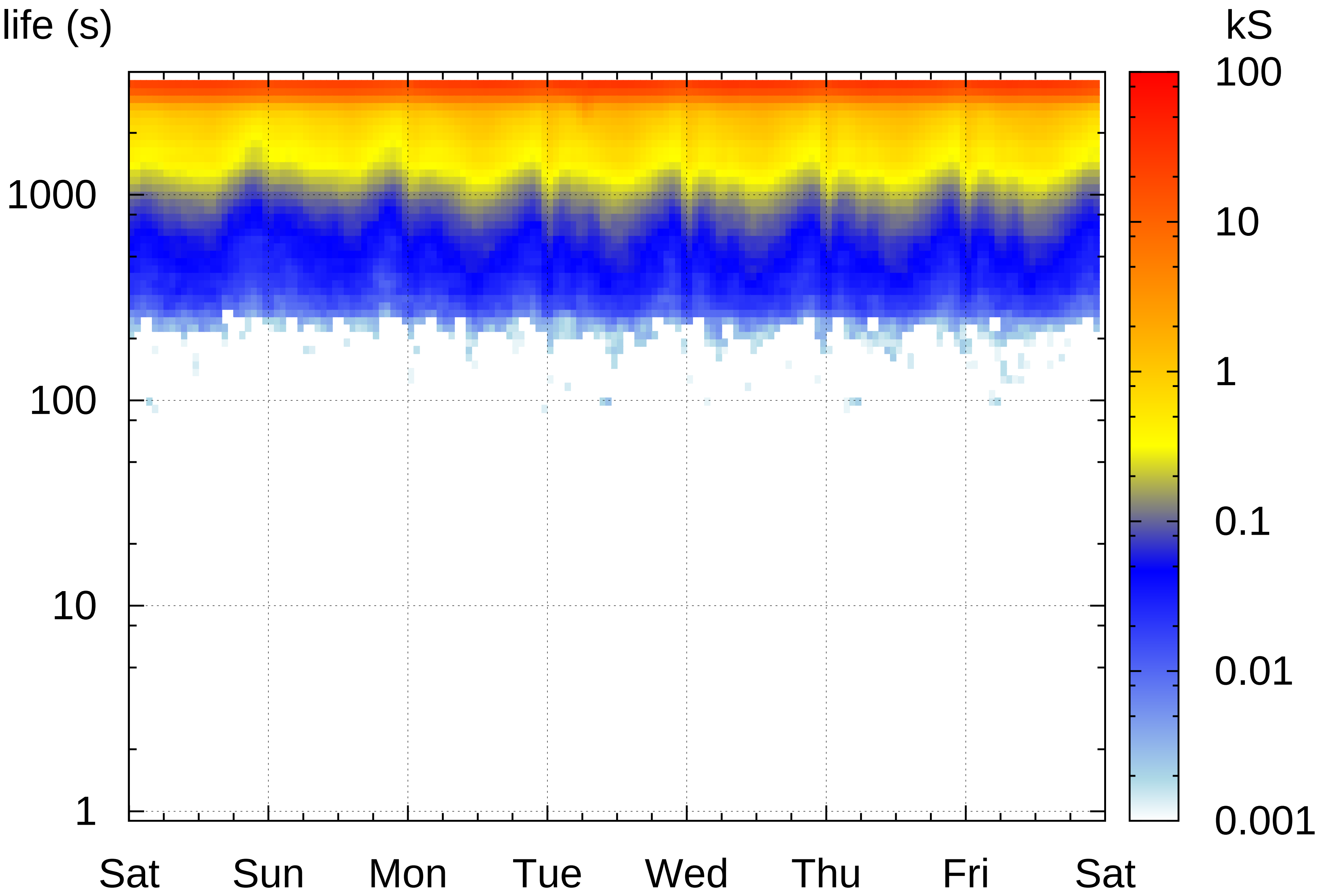
Lifetime of *TCP Probe* sources



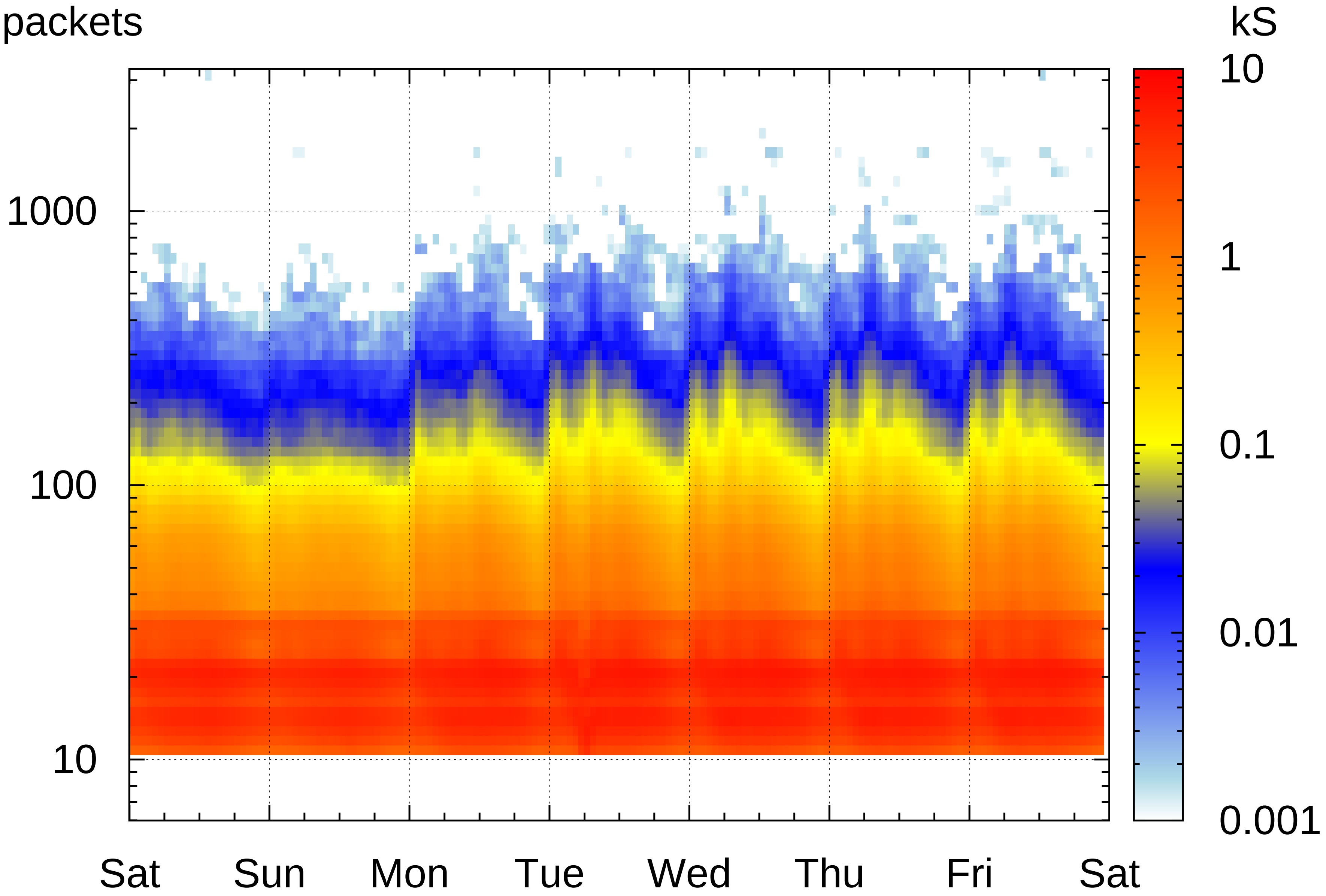
Packet Count of *TCP Probe* sources



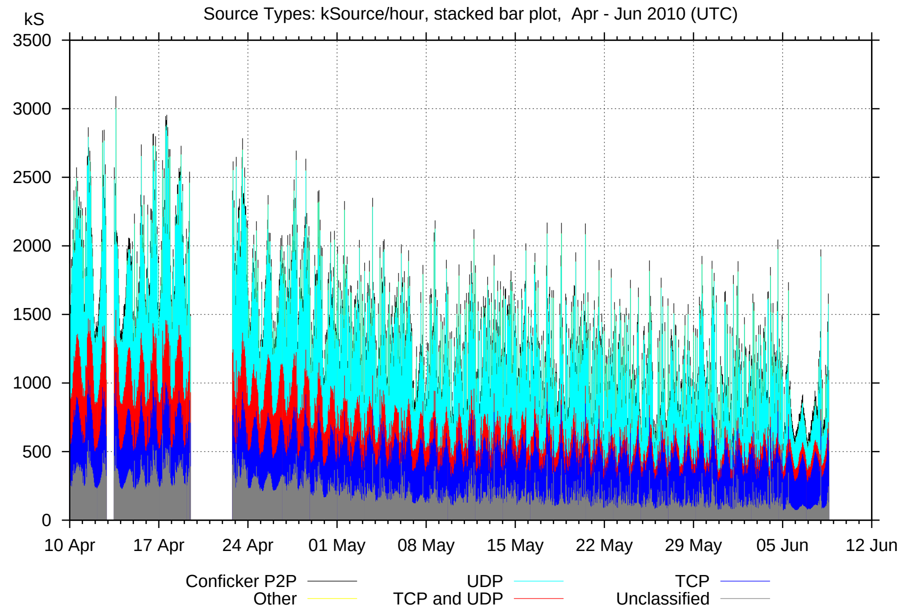
Lifetime of *Only Conficker P2P* sources



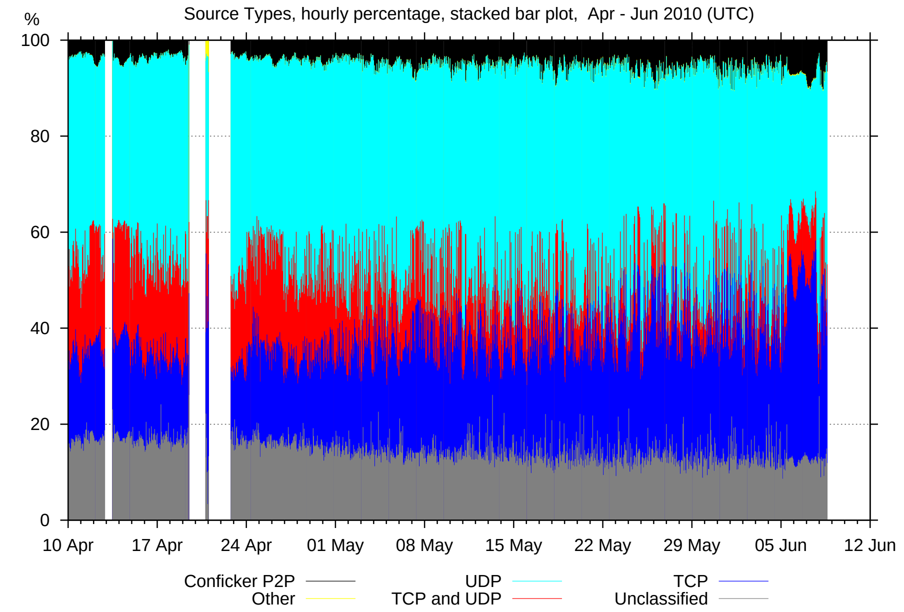
Packet Count of *Only Conficker P2P* sources



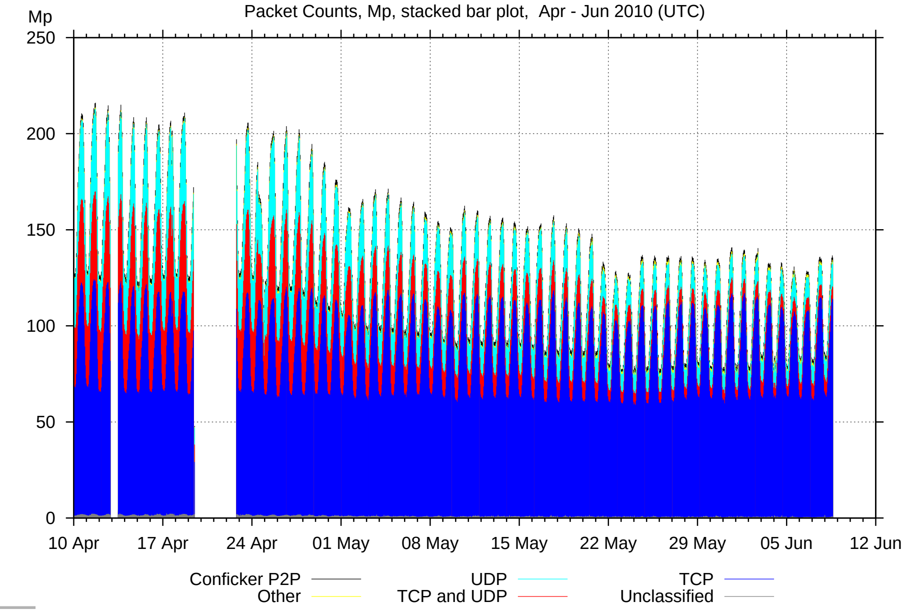
What happened after April 2010 ...



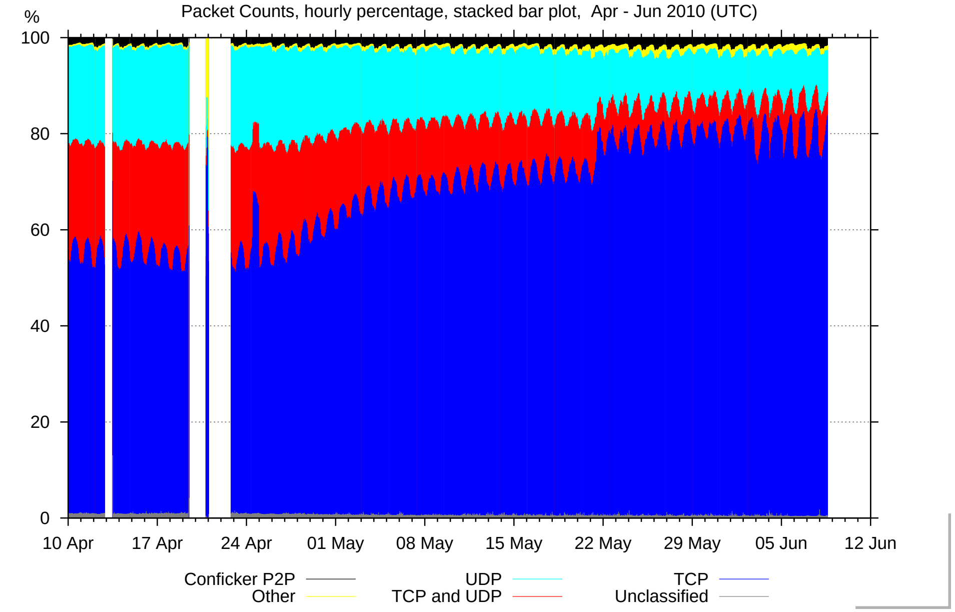
Source Types: kSource/hour, stacked bar plot, Apr - Jun 2010 (UTC)



Source Types, hourly percentage, stacked bar plot, Apr - Jun 2010 (UTC)



Packet Counts, Mp, stacked bar plot, Apr - Jun 2010 (UTC)

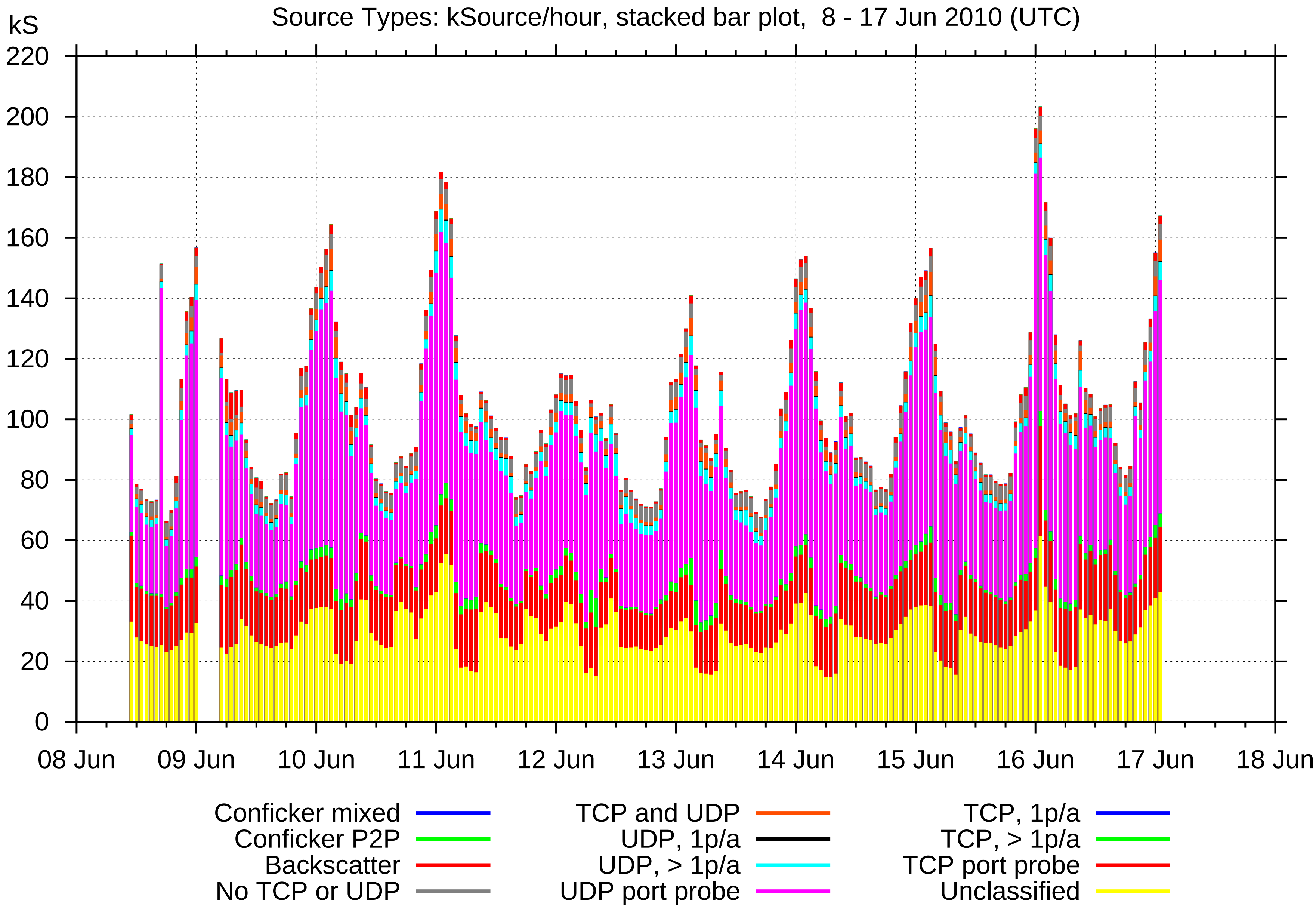


Packet Counts, hourly percentage, stacked bar plot, Apr - Jun 2010 (UTC)

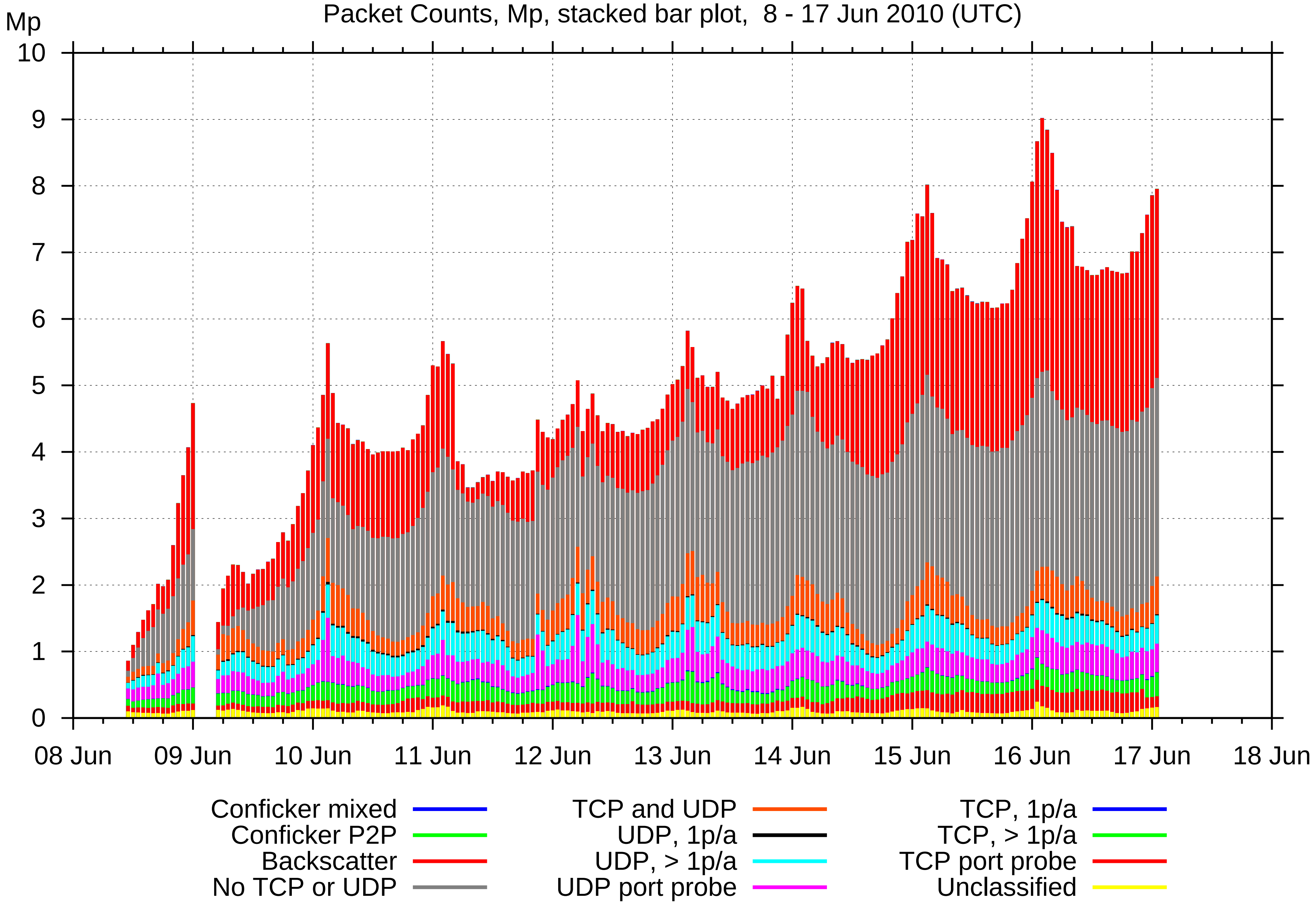
Monitoring IBR at U Auckland

- I've extended `owtmon` to watch one-way traffic
  - Ignore streams that have packets both in and out of UA
  - It can take 40 or more packets in before we see one out!
  - Hard work to get data structure locking between threads correct!
- Has now run for nine days to Thursday 17 June
- Not enough data collected yet to really comment on
  - Making plots for this talk revealed more bugs
  - i.e. packet counters not being reset each hour
- Two plots of Auckland data follow . . .
  - Size of groups at Auckland clearly different to that at UCSD

U Auckland Source Groups, kS/h



U Auckland Packet Counts, Mp/h


Packet Counts, Mp, stacked bar plot, 8 - 17 Jun 2010 (UTC)
Mp
08 Jun
09 Jun
10 Jun
11 Jun
12 Jun
13 Jun
14 Jun
15 Jun
16 Jun
17 Jun
18 Jun
Conficker mixed
Conficker P2P
Backscatter
No TCP or UDP
TCP and UDP
UDP, 1p/a
UDP, > 1p/a
UDP port probe
TCP, 1p/a
TCP, > 1p/a
TCP port probe
Unclassified