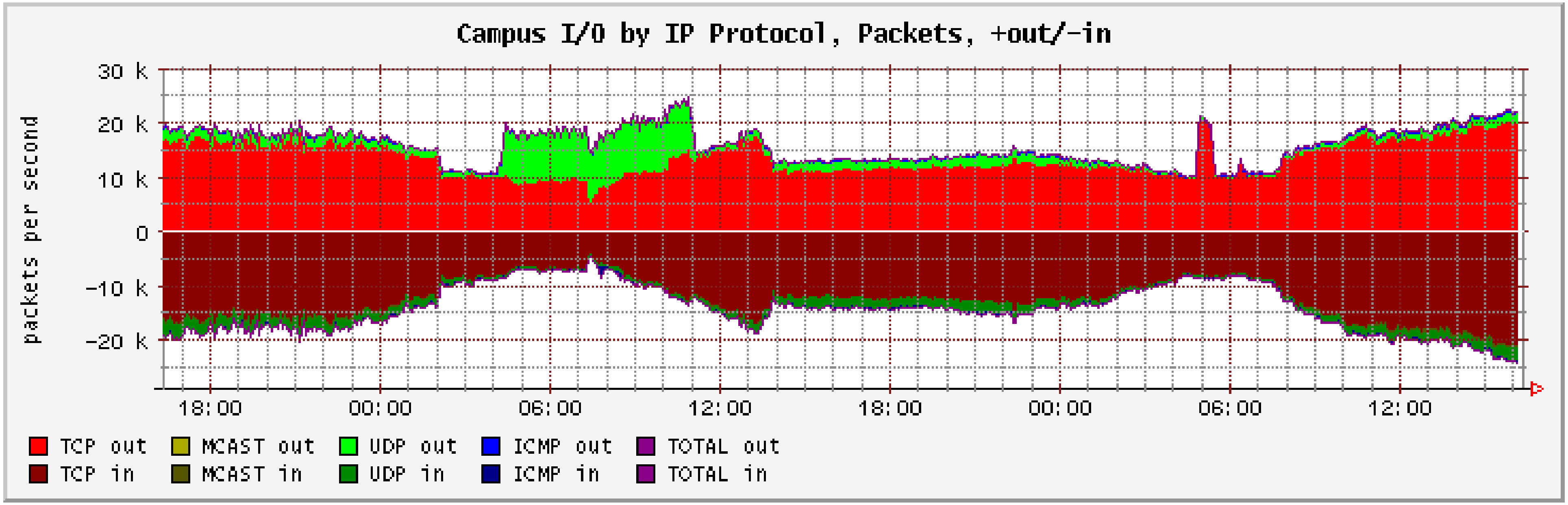
Network Anomaly Confirmation, Diagnosis and Remediation

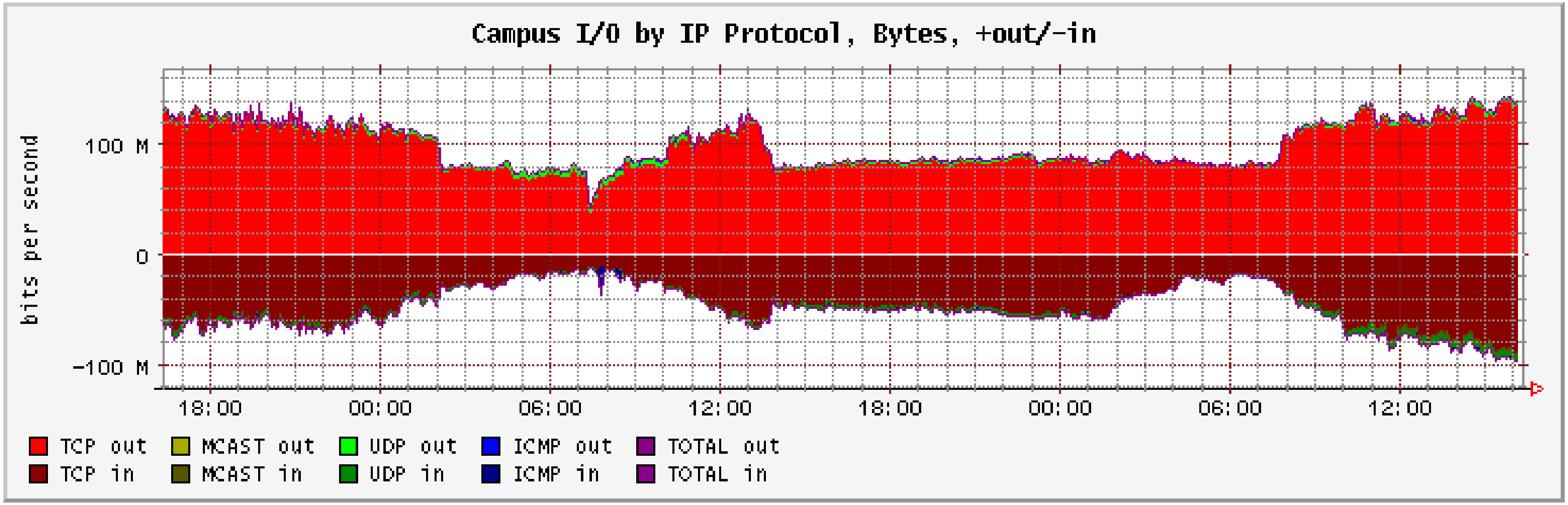
Allerton Conference 2009, September 30, 2009

THE UNIVERSITY of WISCONSIN MADISON

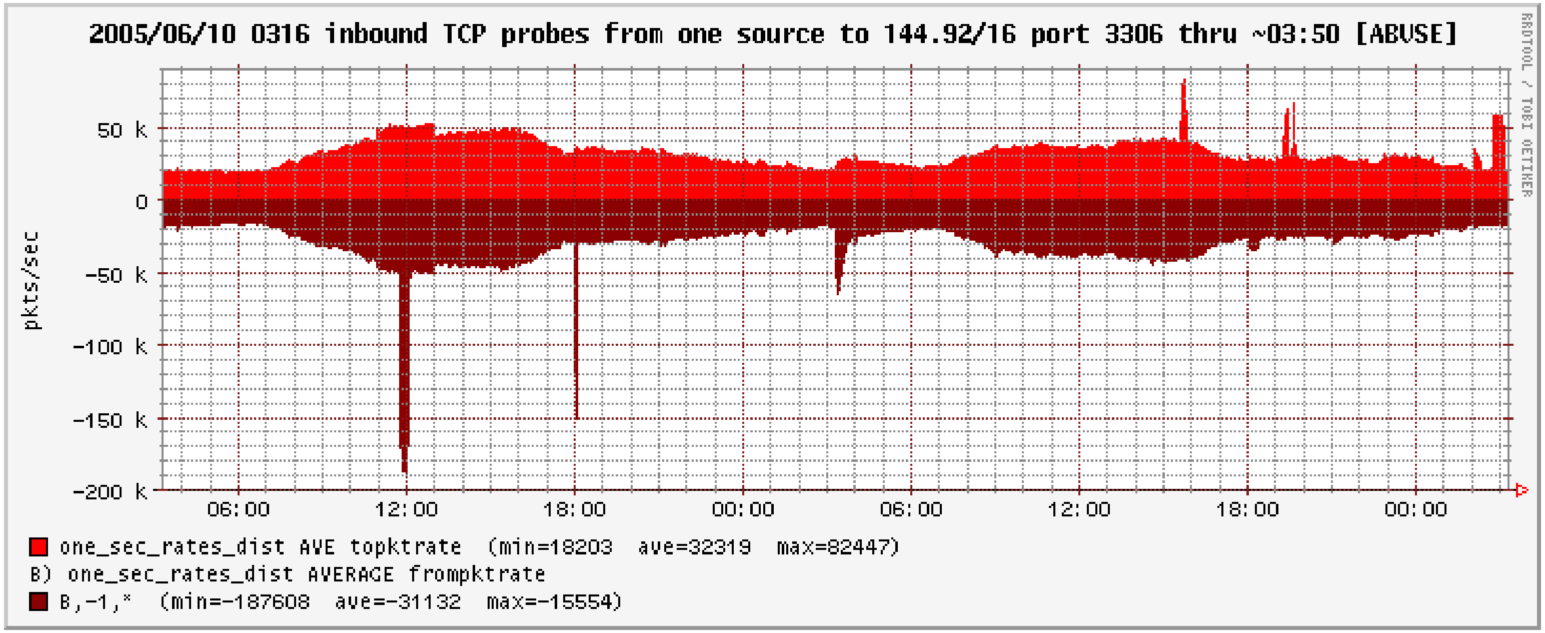
David Plonka & Paul Barford
{plonka,pb}@cs.wisc.edu

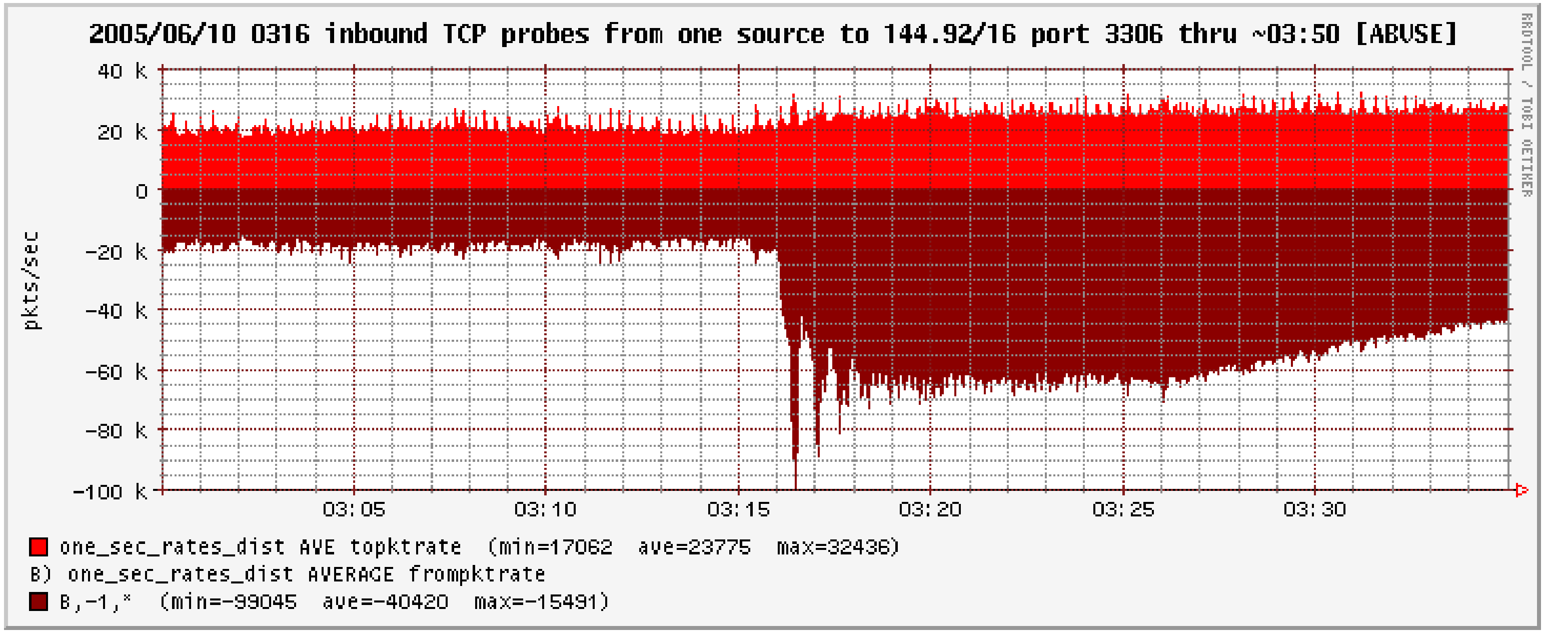
Packet and Bit Rate Time Series



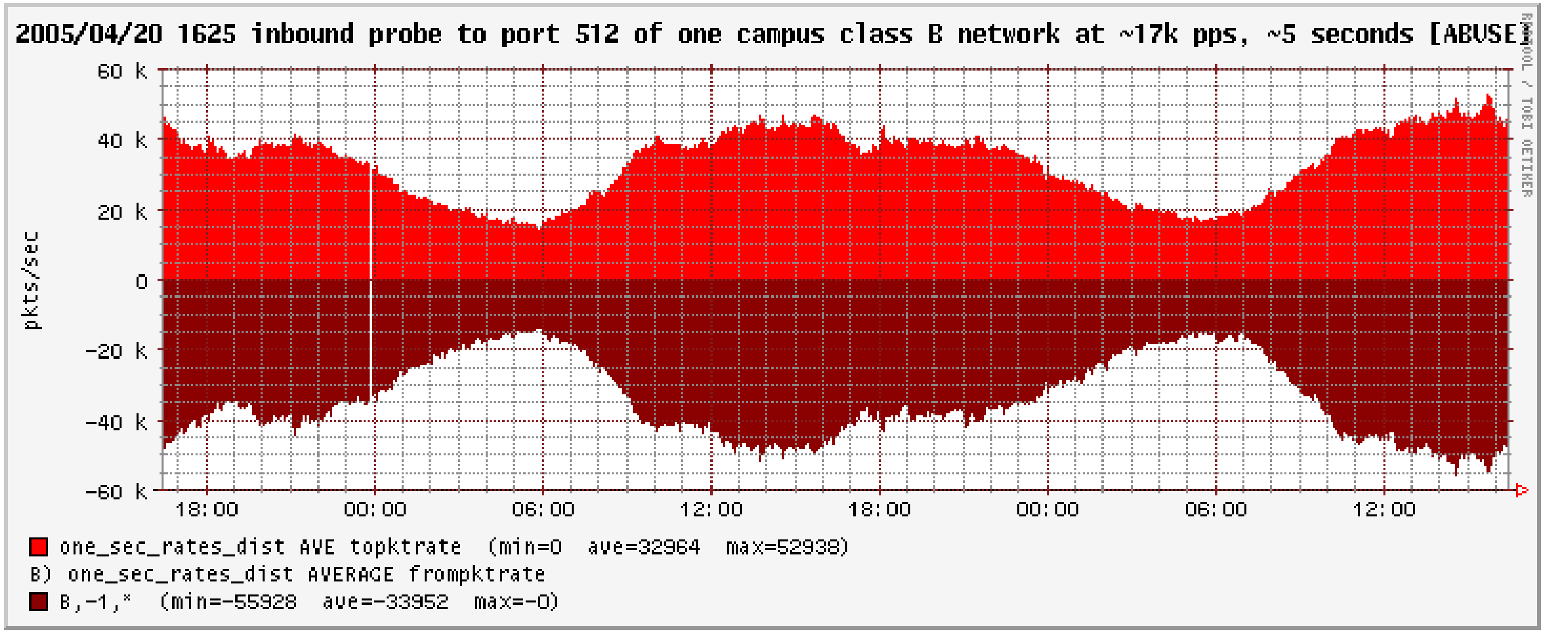


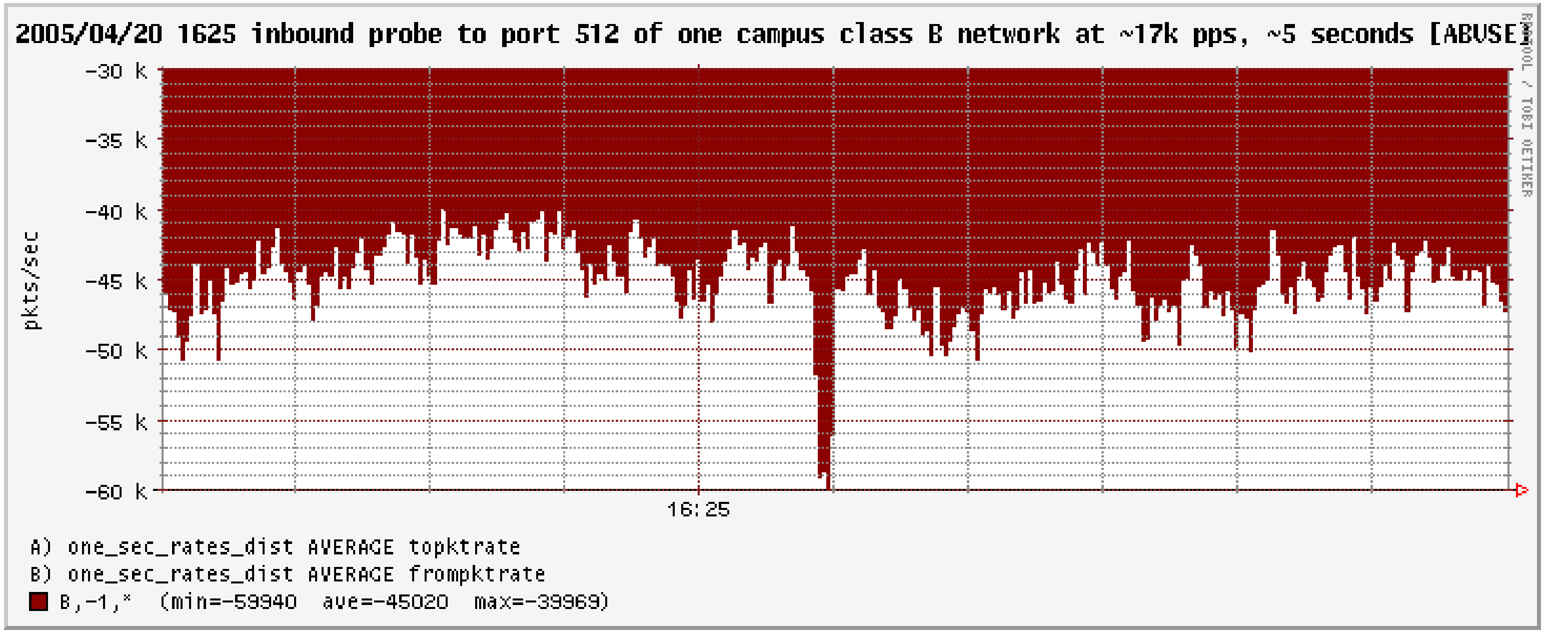
3306/tcp (MySQL) probe/flood to 64k campus IPs



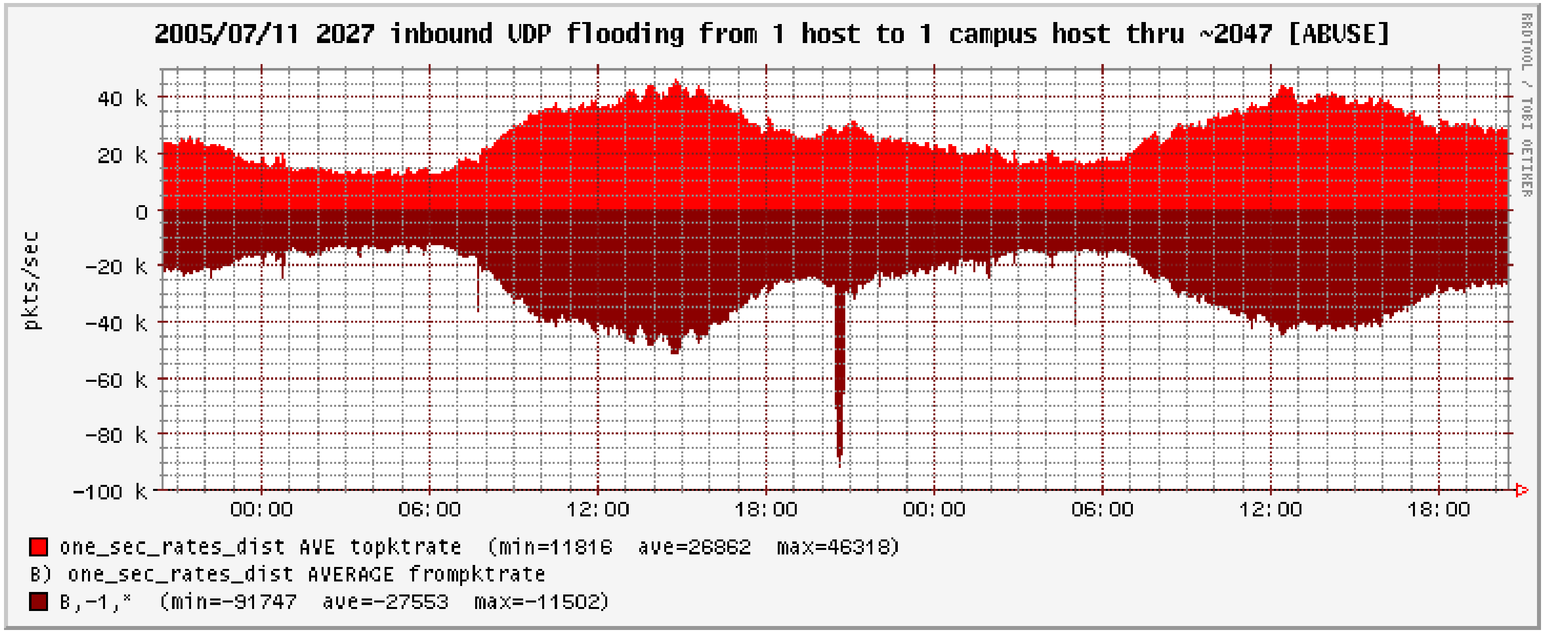


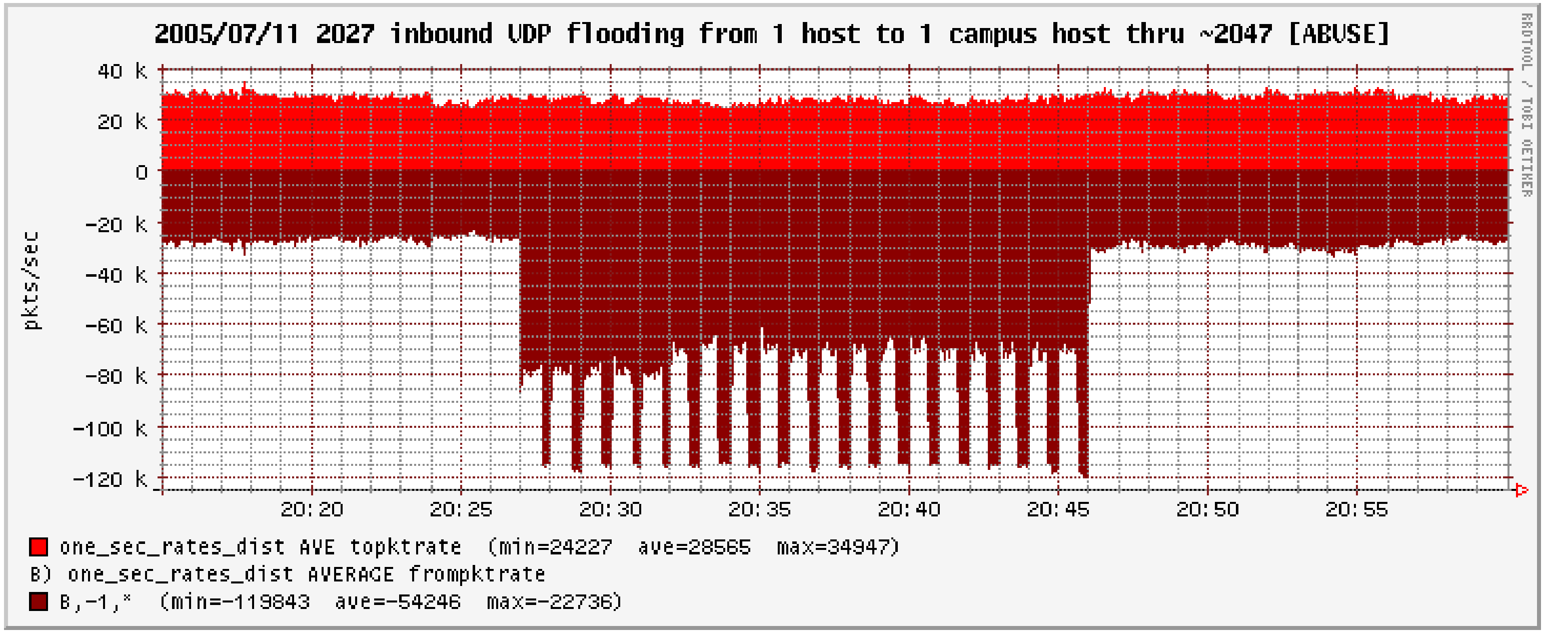
512/tcp (exec) probe to 64k campus IP addresses



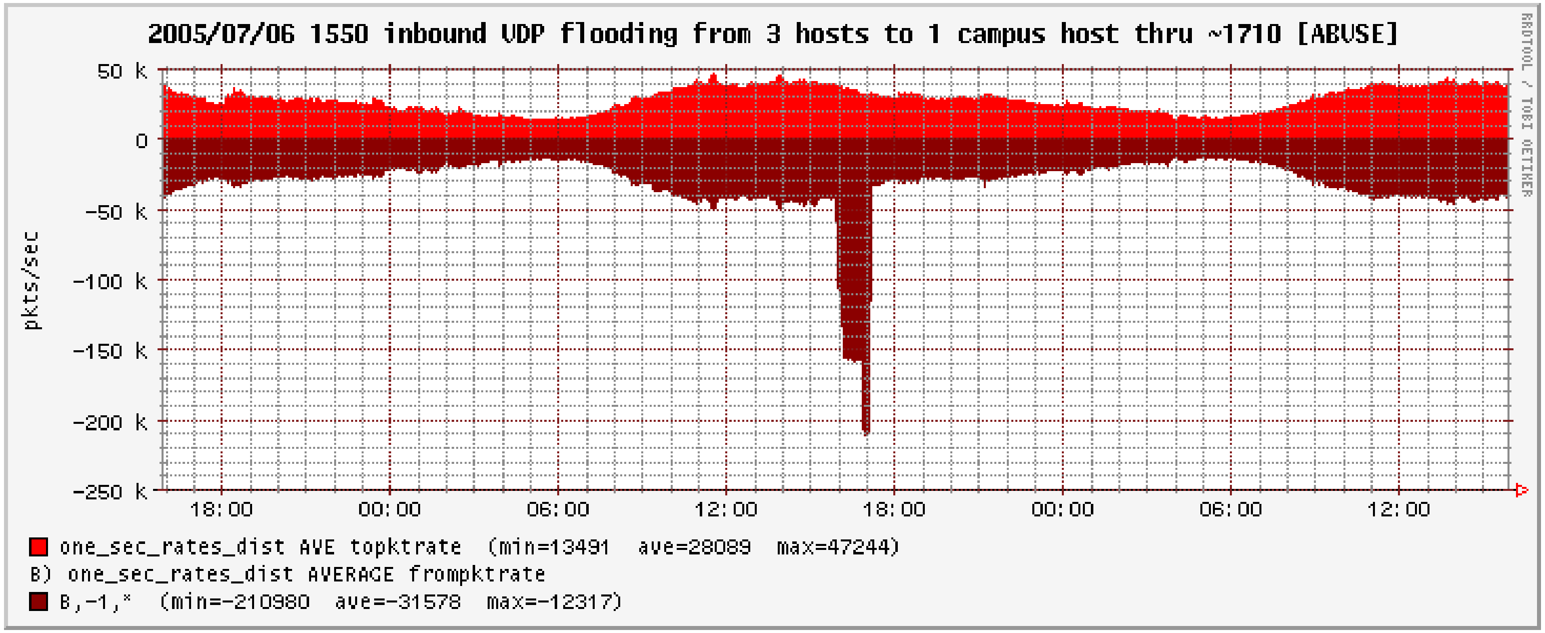


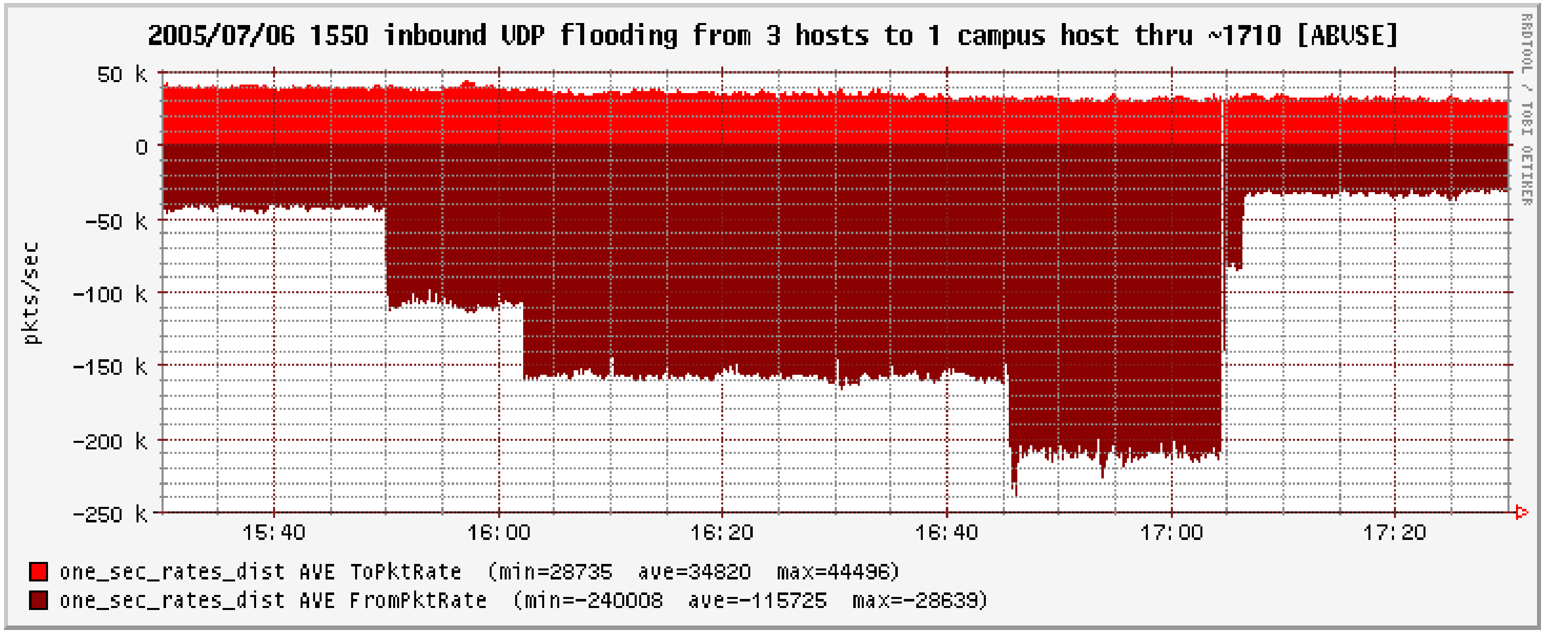
UDP flood from one host to one campus host


2005/07/11 2027 inbound UDP flooding from 1 host to 1 campus host thru ~2047 [ABUSE]


2005/07/11 2027 inbound UDP flooding from 1 host to 1 campus host thru ~2047 [ABUSE]

UDP flood from three hosts to one campus host

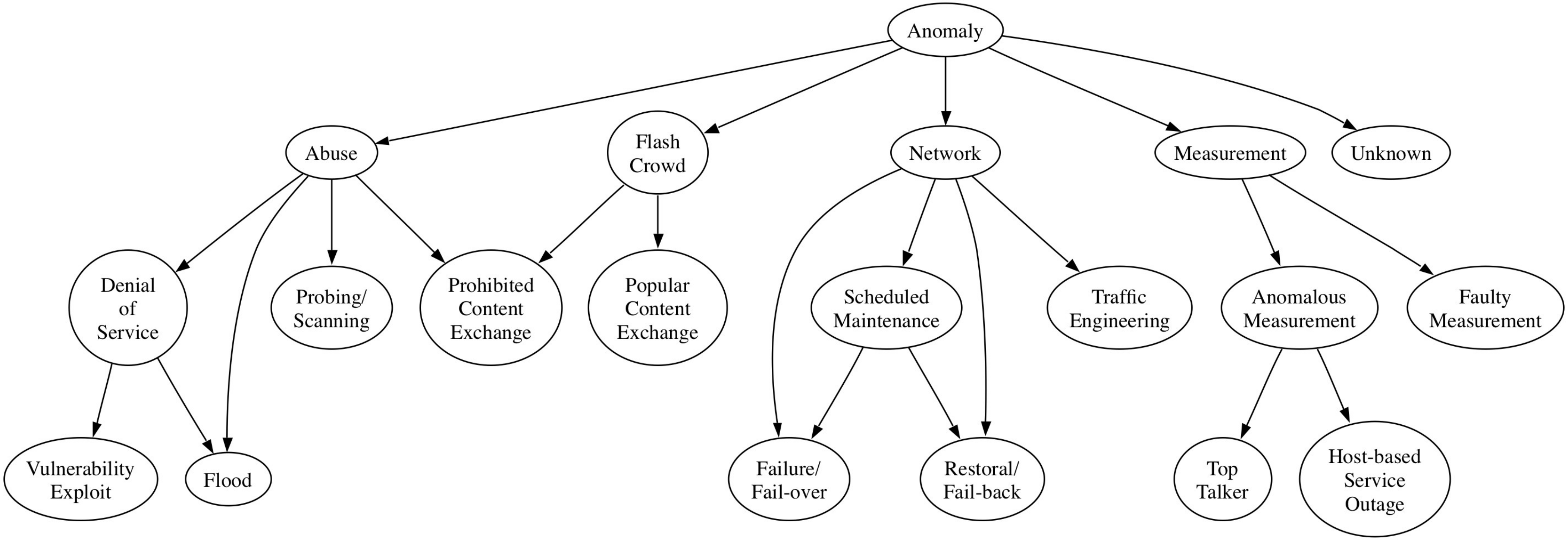




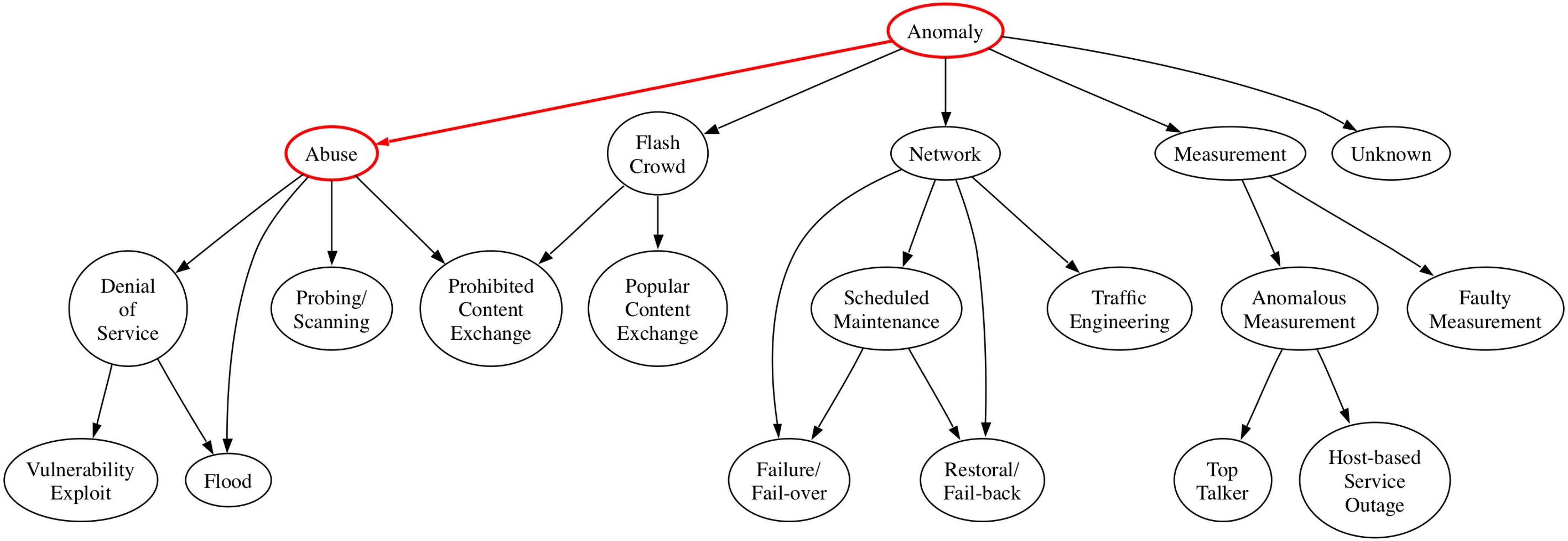
Problem Statement

- Q: What does one do *after a NADS* (Network Anomaly Detection System) reports an anomaly?
- A: Perform *CDR* – Confirmation, Diagnosis and Remediation.
  - *Anomaly Confirmation* is the process of verifying that an anomaly is authentic.
- Challenge: develop a CDR Framework based on practice in network operations.

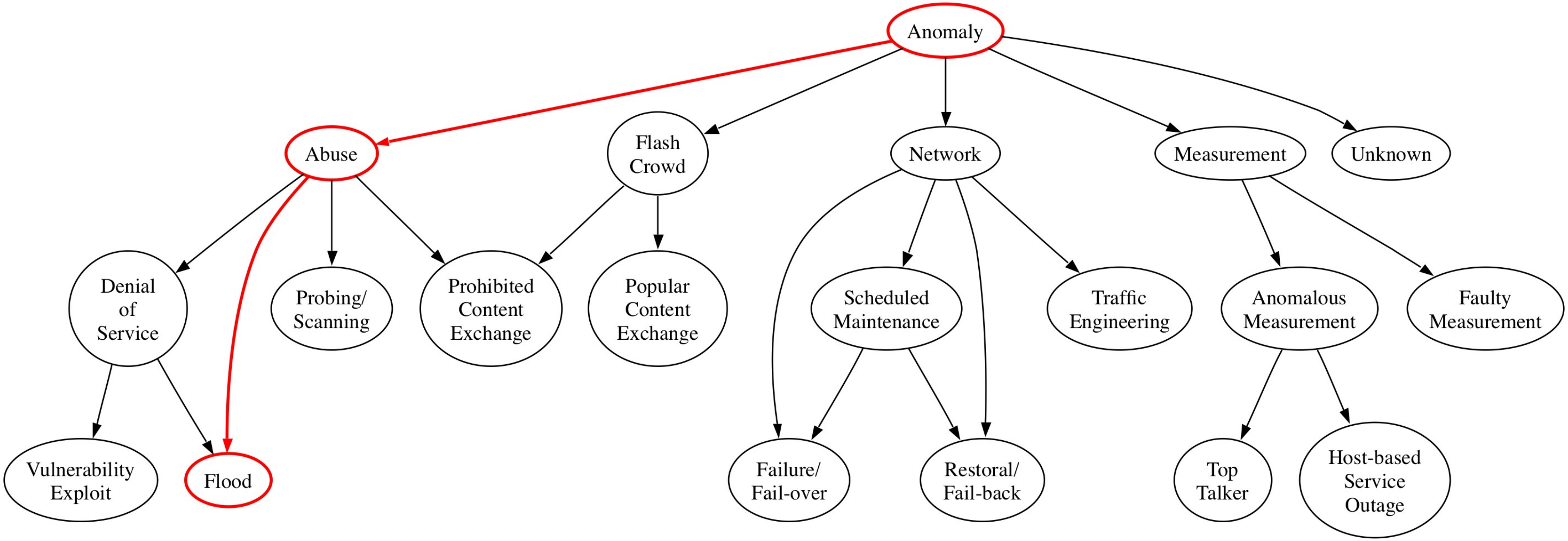
An Anomaly Taxonomy



An Anomaly Taxonomy



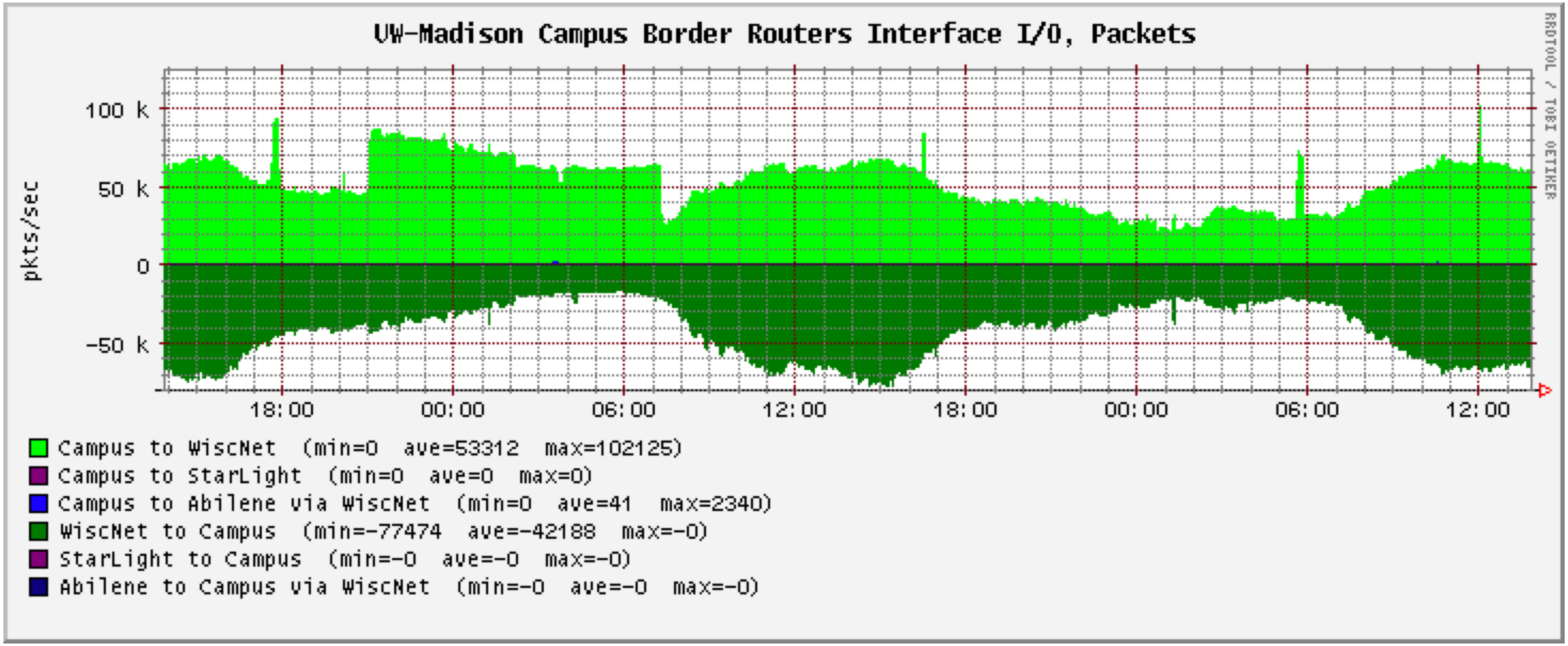
An Anomaly Taxonomy



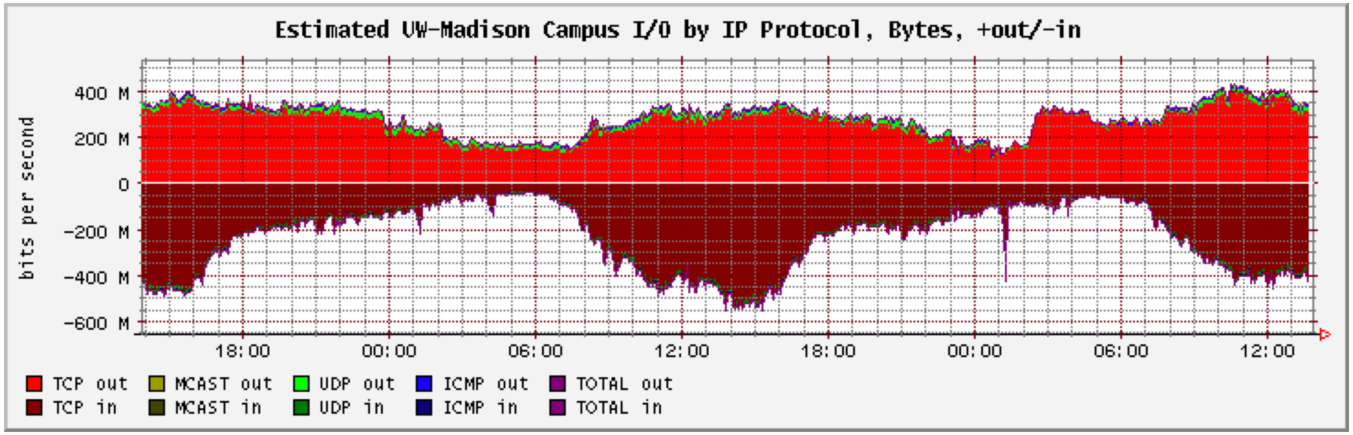
Anomaly Confirmation Workflow

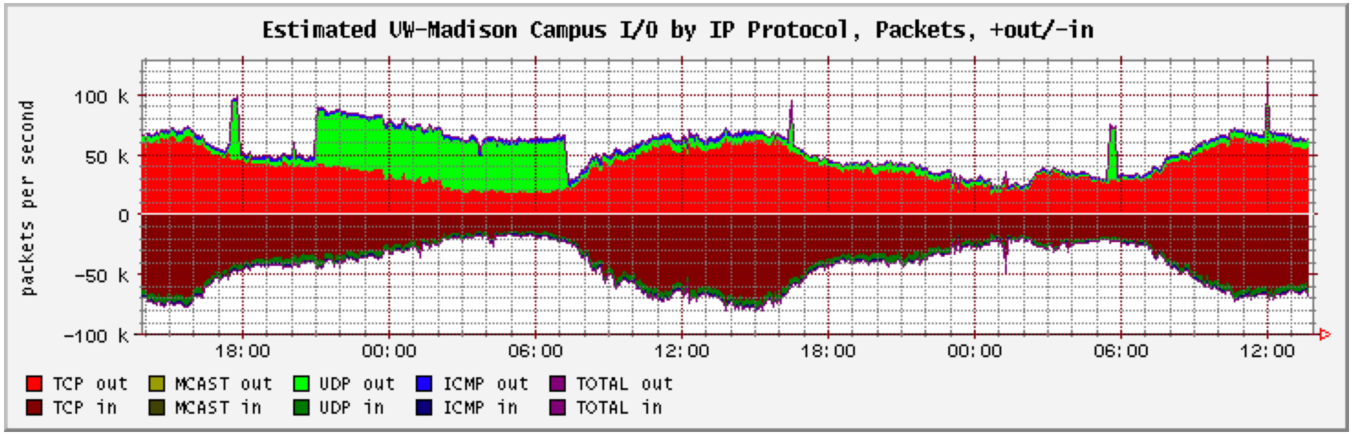
- *Input nodes* specify the required measurements.
- *Decision nodes* pose questions and the possible answers.
- *Directed edges* express prerequisites.
- *Dashed elements* involve operator intuition and experience and are new candidates for automation.
- *Join nodes* …
- *Output nodes* express positive or negative confirmation by anomaly type.

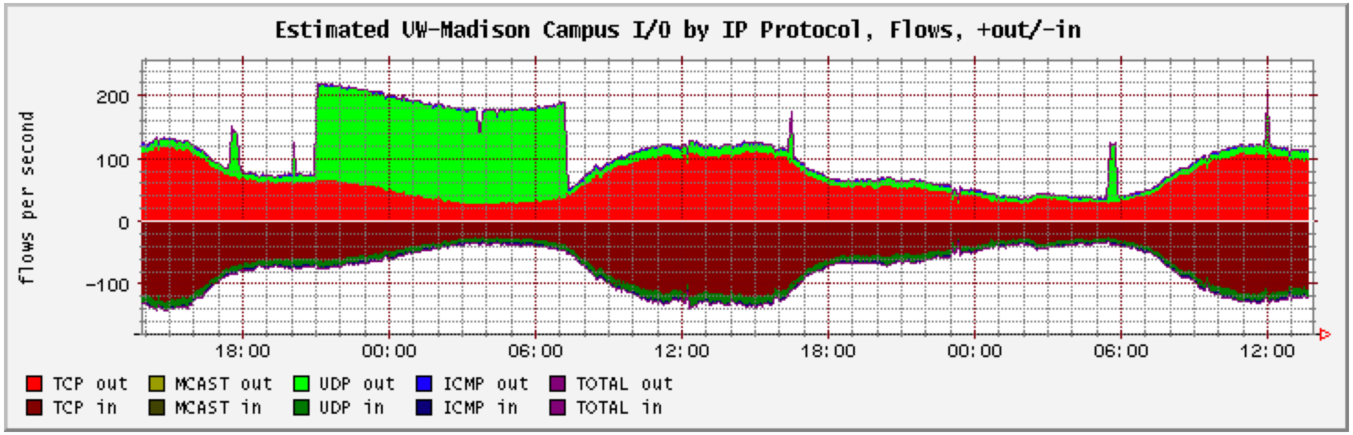
SNMP time-series: Inteface Packet Rate

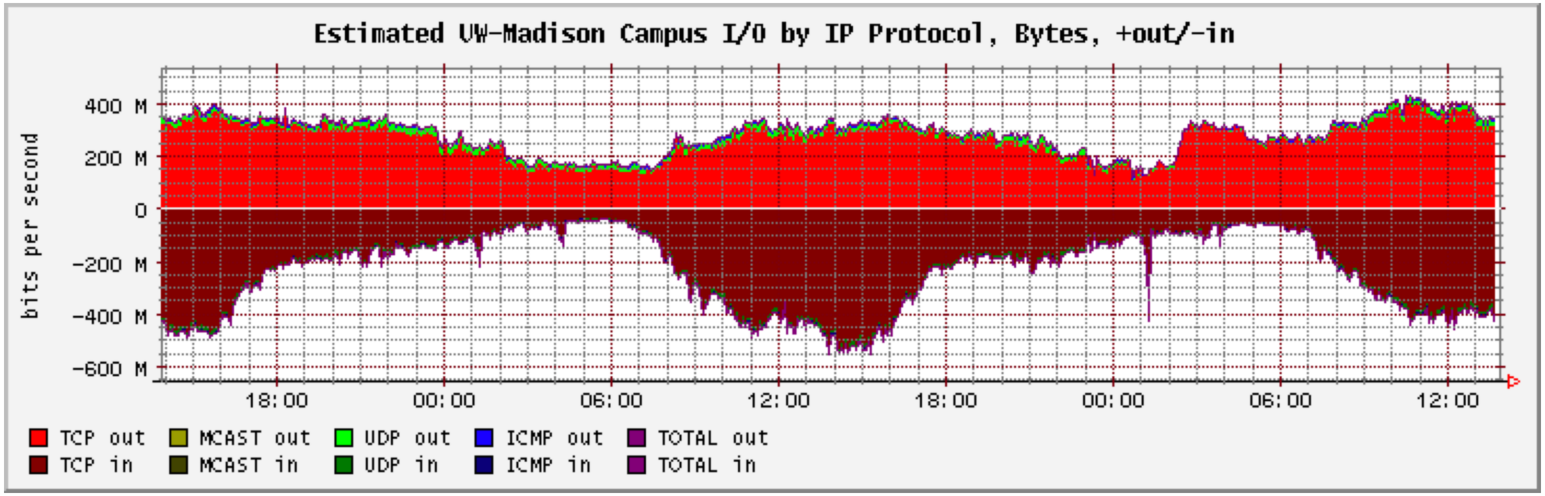


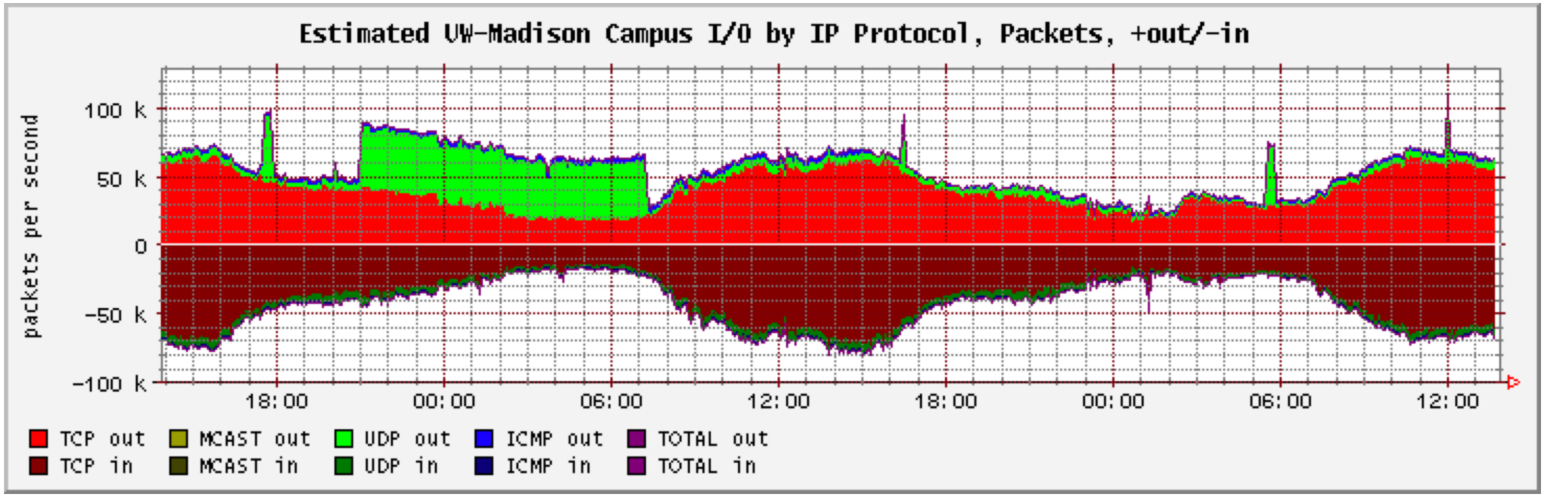
Bit, Packet, and Flow Rates by Protocol

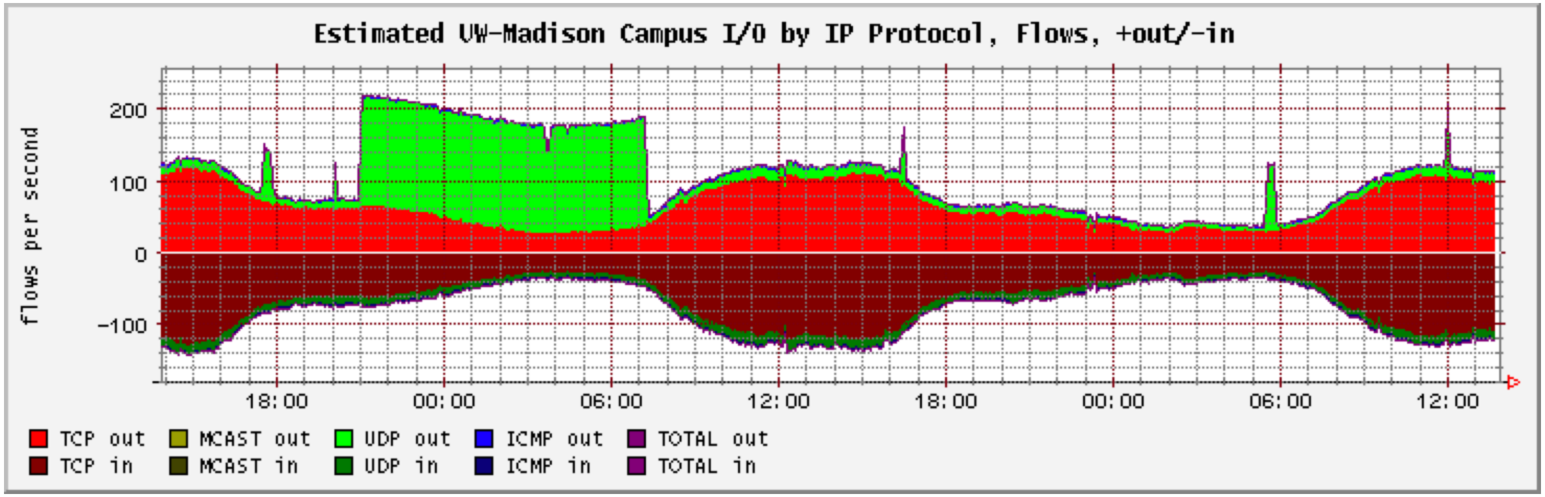




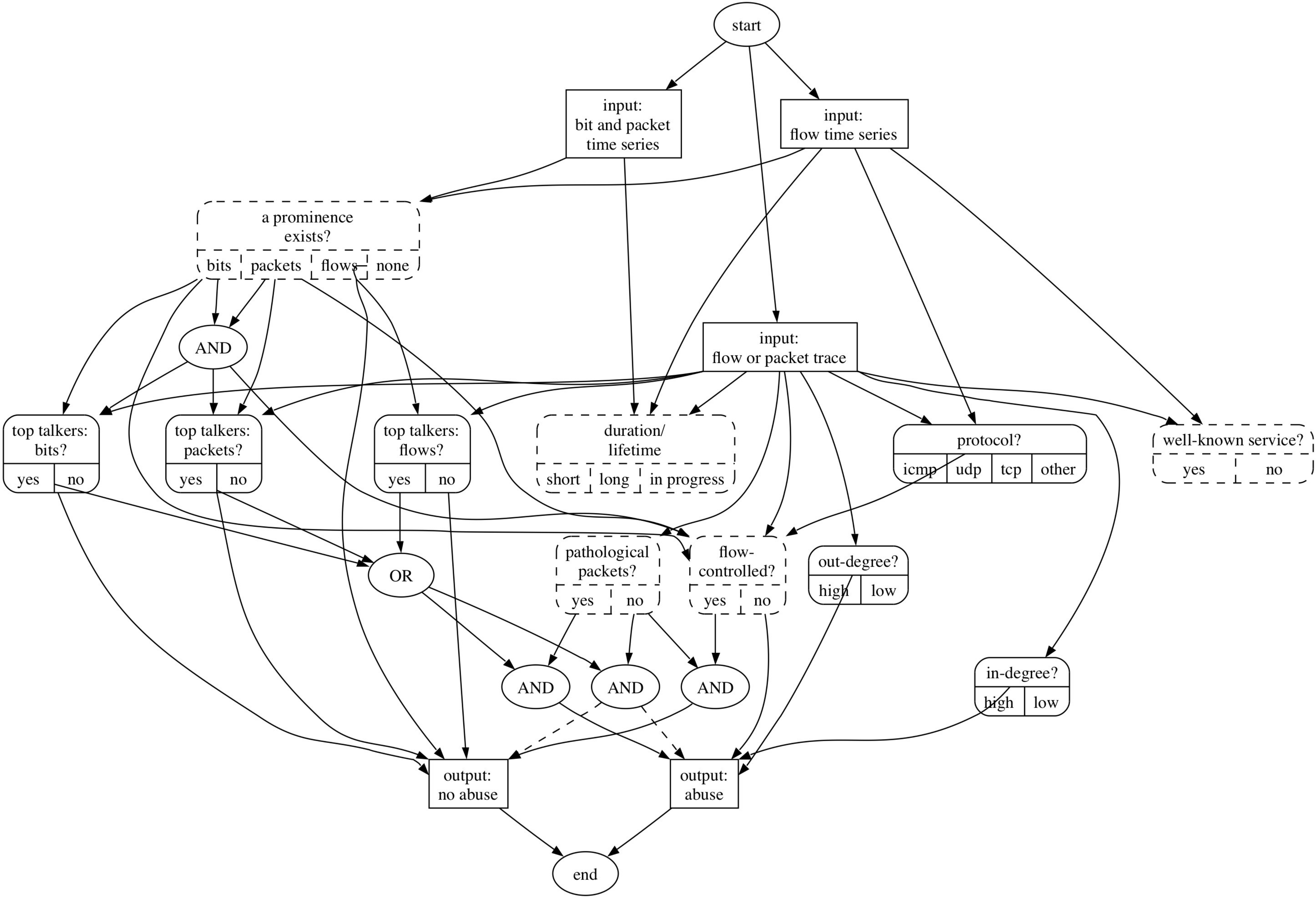



Estimated UW-Madison Campus I/O by IP Protocol, Bytes, +out/-in
bits per second
400 M
200 M
0
-200 M
-400 M
-600 M
18:00
00:00
06:00
12:00
18:00
00:00
06:00
12:00
TCP out
MCAST out
UDP out
ICMP out
TOTAL out
TCP in
MCAST in
UDP in
ICMP in
TOTAL in

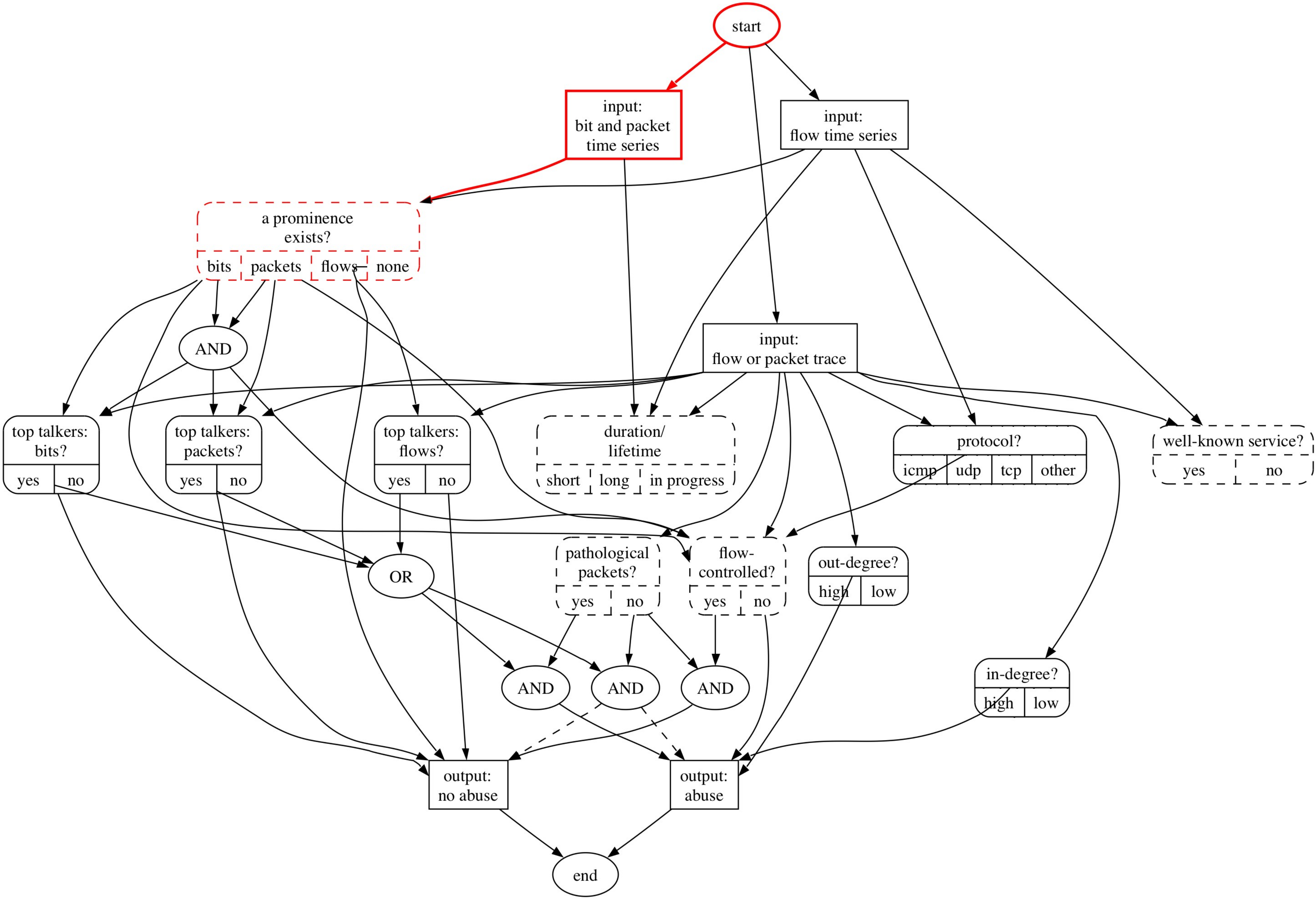

Estimated UW-Madison Campus I/O by IP Protocol, Packets, +out/-in
packets per second
100 k
50 k
0
-50 k
-100 k
18:00
00:00
06:00
12:00
18:00
00:00
06:00
12:00
TCP out
MCAST out
UDP out
ICMP out
TOTAL out
TCP in
MCAST in
UDP in
ICMP in
TOTAL in


Estimated UW-Madison Campus I/O by IP Protocol, Flows, +out/-in
flows per second
200
100
0
-100
18:00
00:00
06:00
12:00
18:00
00:00
06:00
12:00
TCP out
MCAST out
UDP out
ICMP out
TOTAL out
TCP in
MCAST in
UDP in
ICMP in
TOTAL in

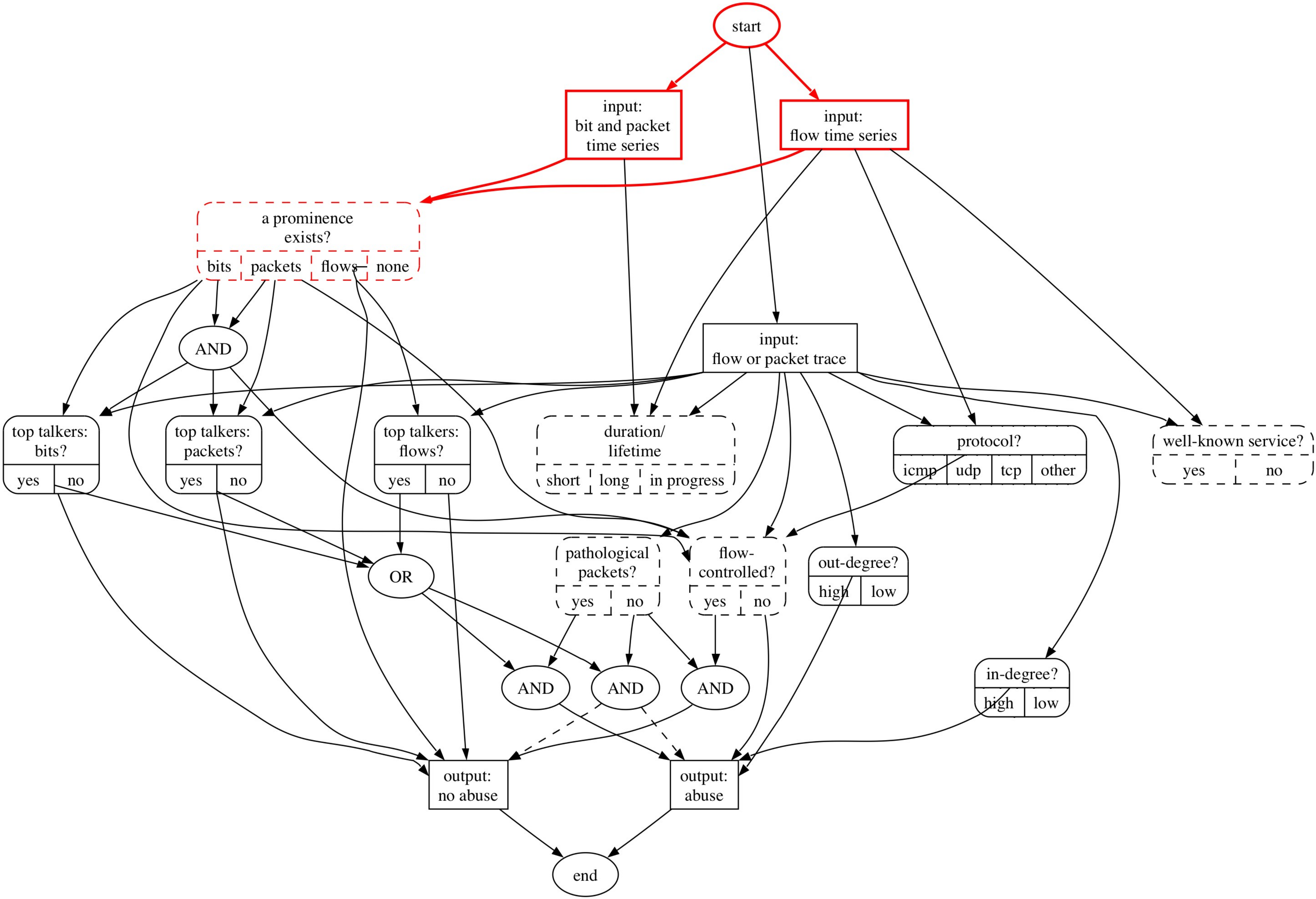
A Confirmation Workflow for Flood



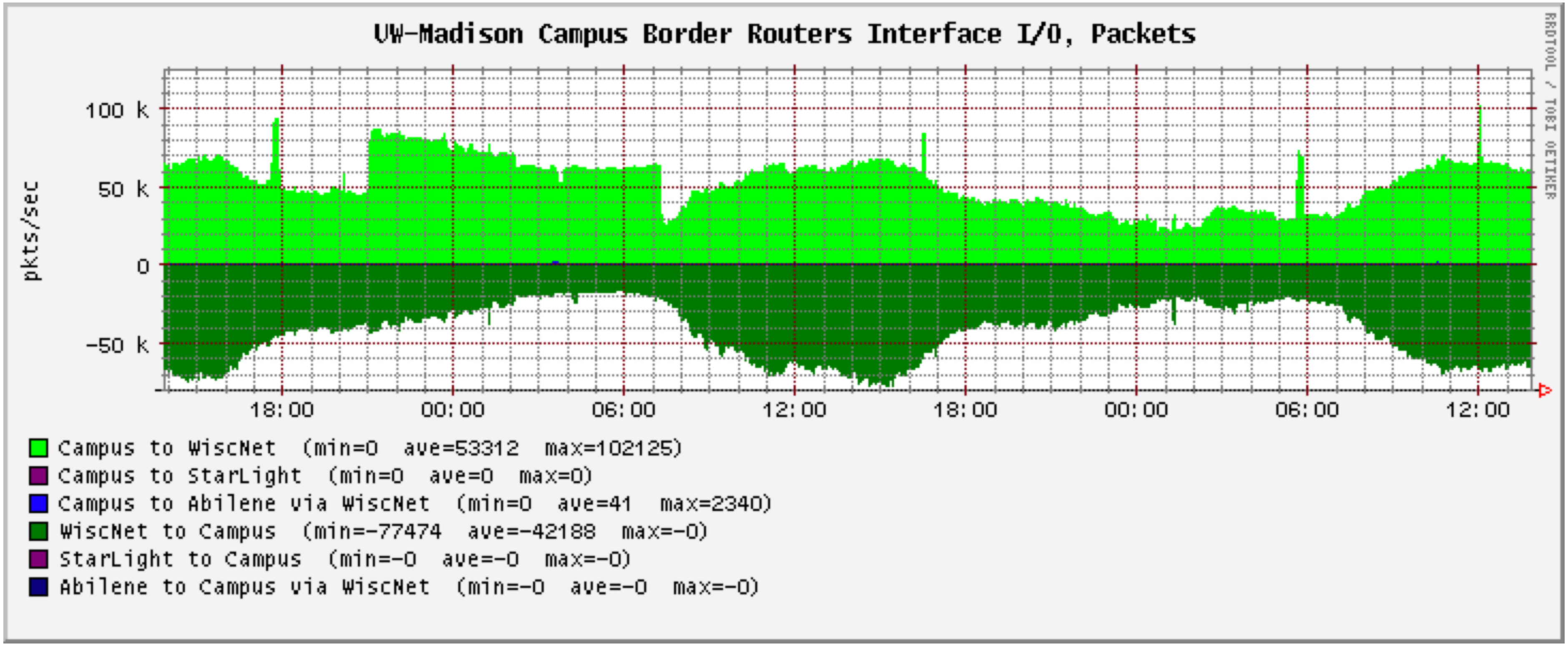
A Confirmation Workflow (1)



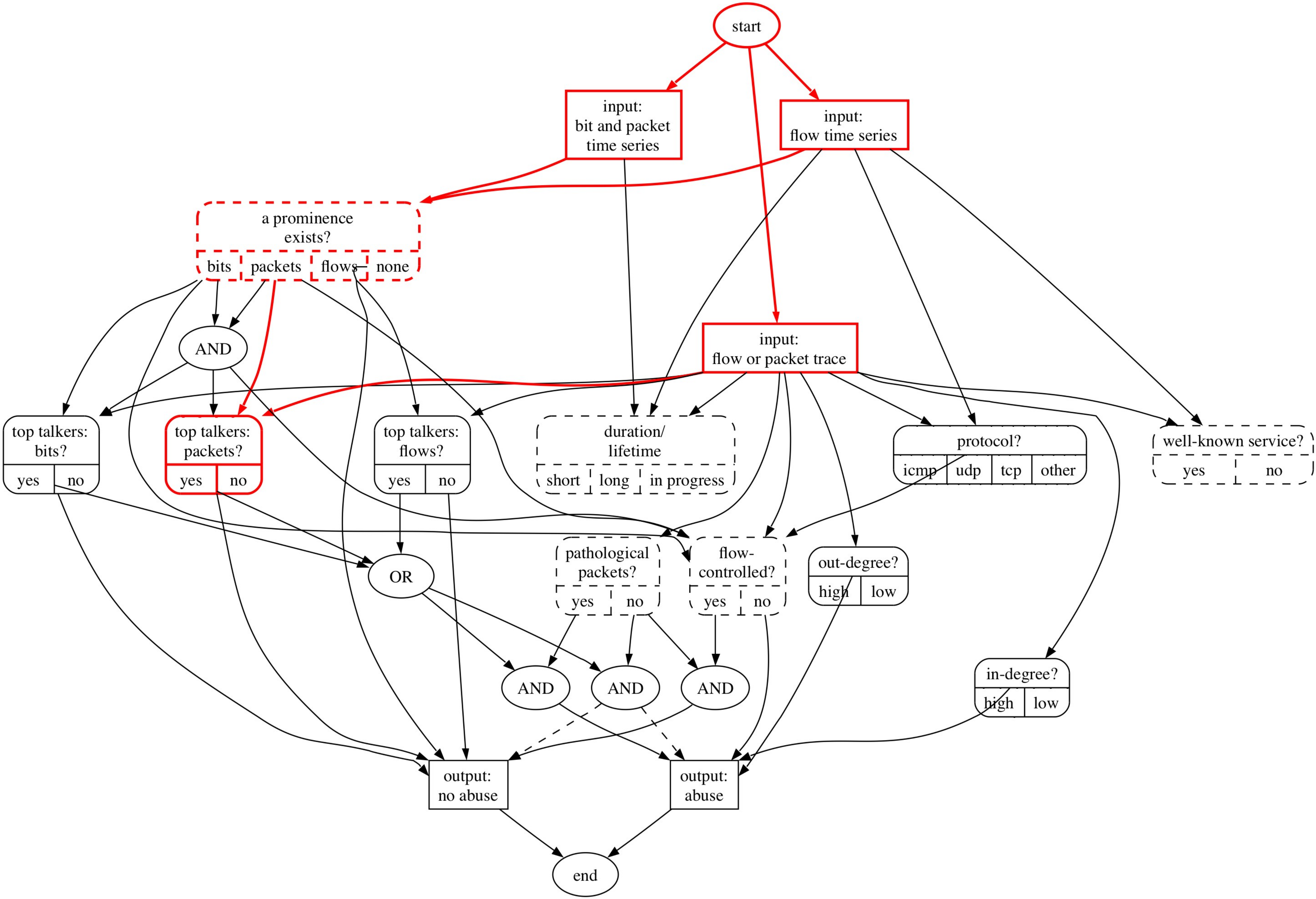
A Confirmation Workflow (2)



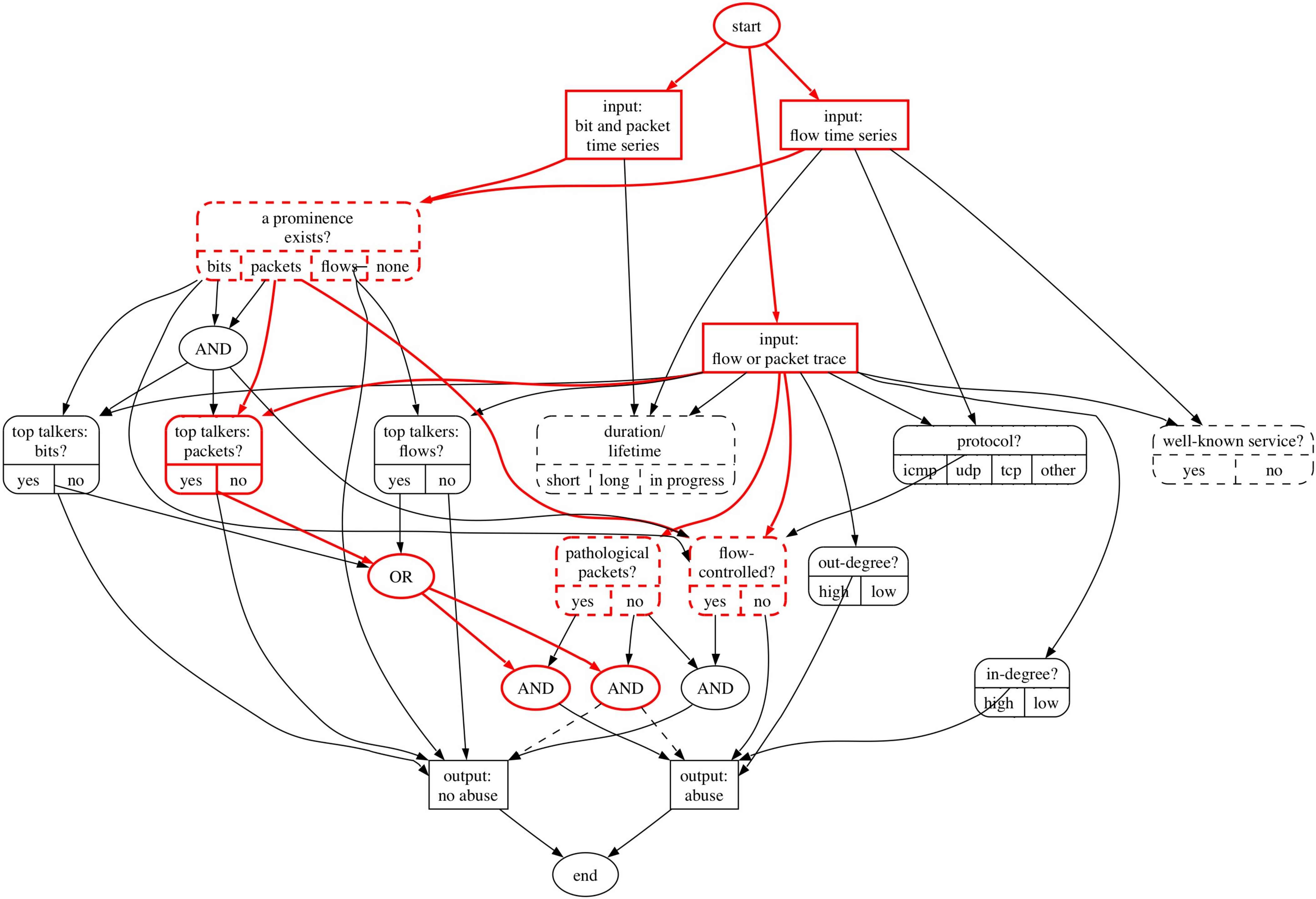
SNMP time-series: Inteface Packet Rate



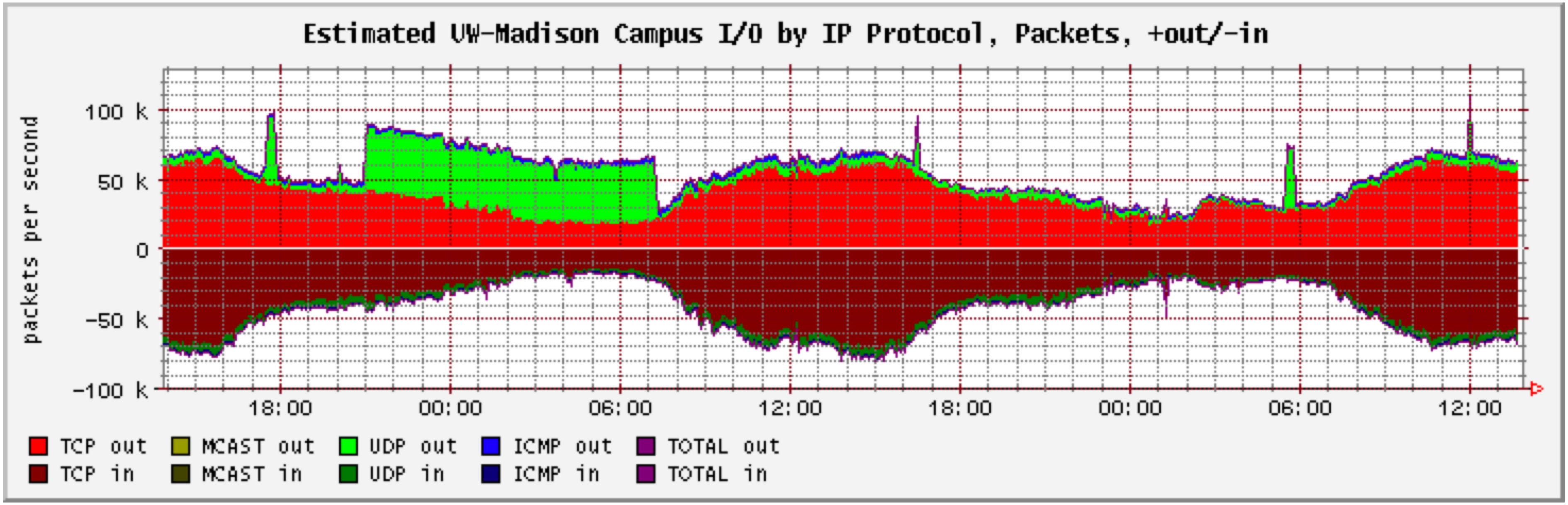
A Confirmation Workflow (3)



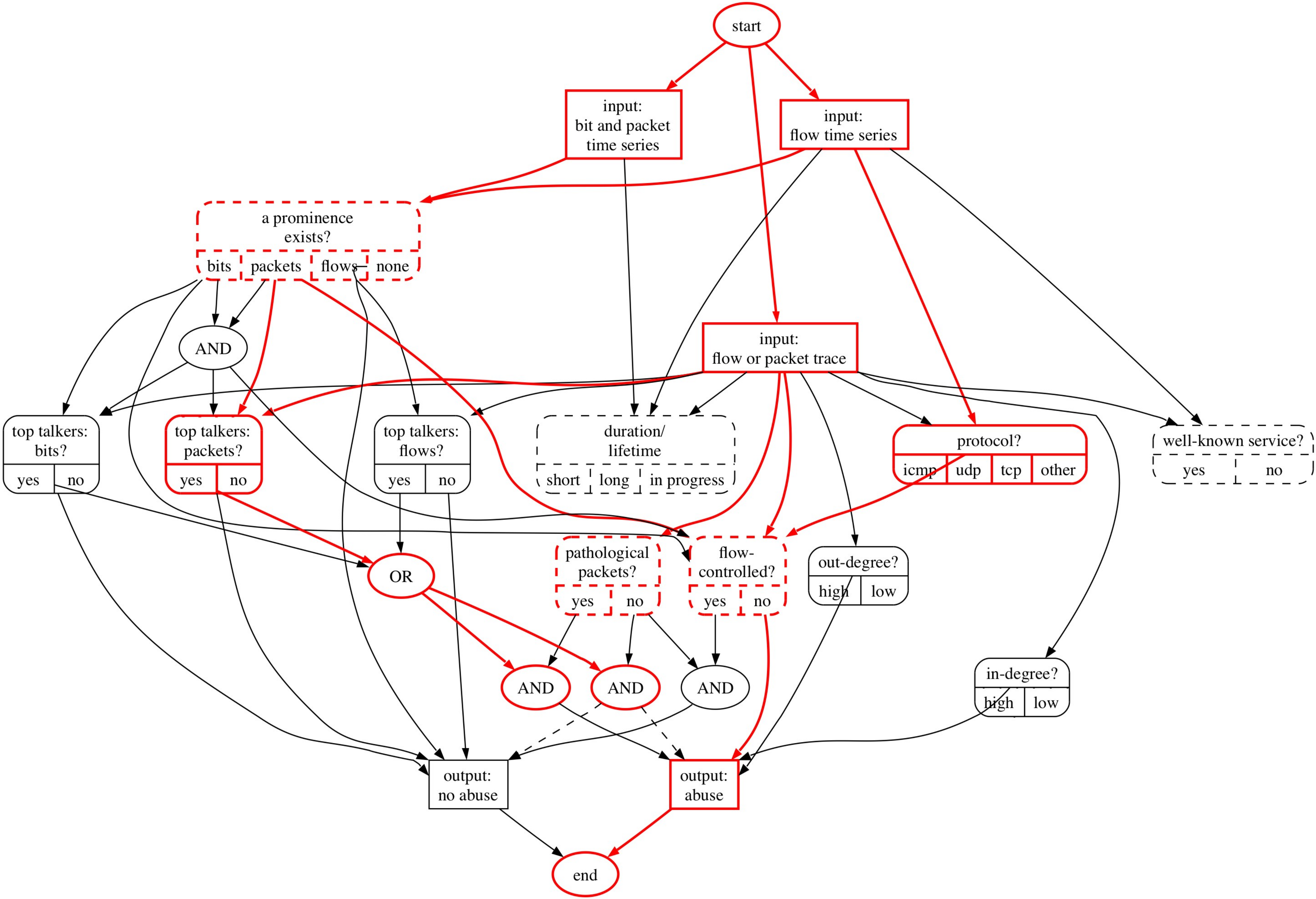
A Confirmation Workflow (4)



Flow time-series: Packet Rate by Protocol



A Confirmation Workflow (5)



Challenges

- *Framework Completeness:* One can sometimes Confirm without Diagnosis. Remedies?
- *Anomaly Lifetime:* Some anomalies are better detected when observed at inception and/or termination.
- *Anomaly Correlation:* Some anomalies are related serially or in parallel.
- *Anomaly Atomicity:* Anomalies can overlap in time, with consequences for CDR.

Challenges (2)

- *Detail and Time Scales:* Input details and time scale determine whether or not anomalies can be distinguised from each other or discerned at all.
- *Probabilistic Reasoning:* While we use simple join nodes (*i.e.,* AND, OR), Bayesian networks have aided anomaly detection, and may enhance CDR as well.

Summary

- We formalize network traffic anomaly CDR toward the goal of increased operational efficiency.
- We describe a CDR workflow framework with a:
  - Taxonomy of anomaly types
  - Data sets
  - Process steps, including decision points
- This yields an extensible, partially-ordered basis for automating Confirmation, Diagnosis, and Remediation.

Thank you!

THE UNIVERSITY of WISCONSIN MADISON

David Plonka & Paul Barford
{plonka,pb}@cs.wisc.edu