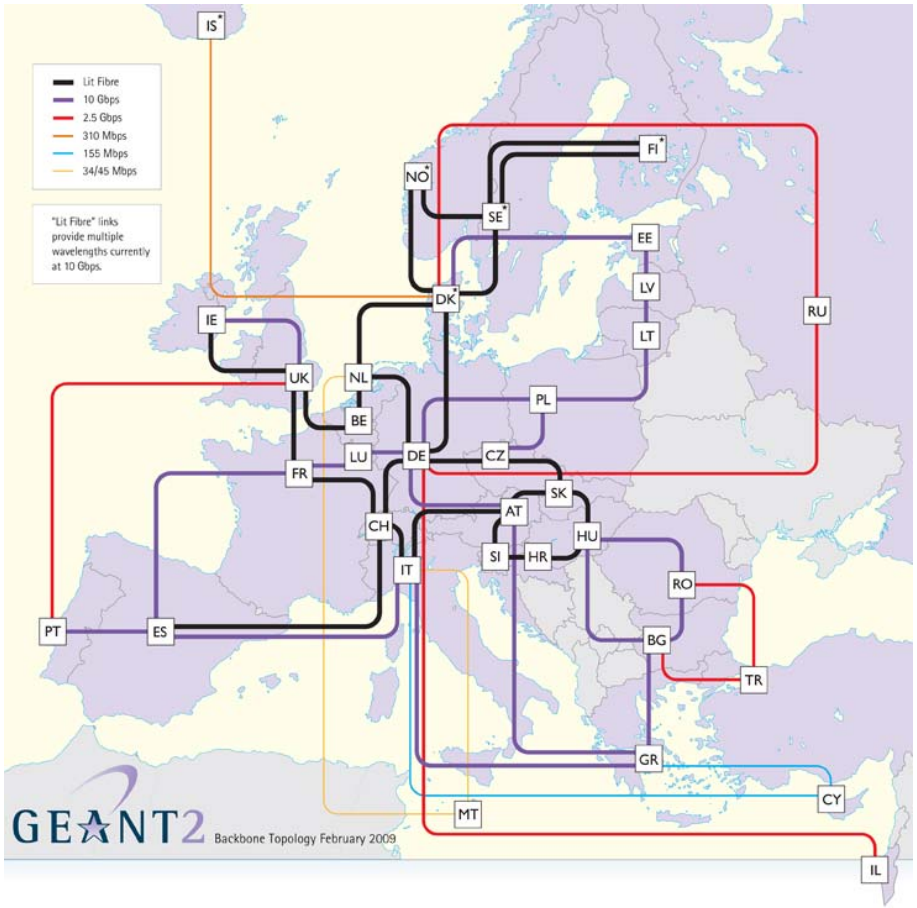
An Anomaly Tool Implementation in GEANT
– Part Three of Three

Wayne Routly, DANTE

TF-CSIRT, Leon; Spain, 18 May 2009

Anomaly Tool Testing in GEANT

- A History Of The Process
  - Confirming Anomalies
  - Testing Three Products
  - Analysing Results
- …And The Winner Is !
- Sneak Peak Of Chosen Solution
- Where We Stand Now



A History Of The Process

- Using Nfsen & Internally Developed Database
- Discussed Collaboration with Various NREN CERTS (Vienna)
- Confirmed Presence of Anomalies in Geant network
- Entered into Trial with Three Industry Anomaly Detection Tools
- Analysed +1000 Unique Events Over Two Week Period
- Presented Results to TF-CSIRT (Riga) & APM Meeting (Cambridge)

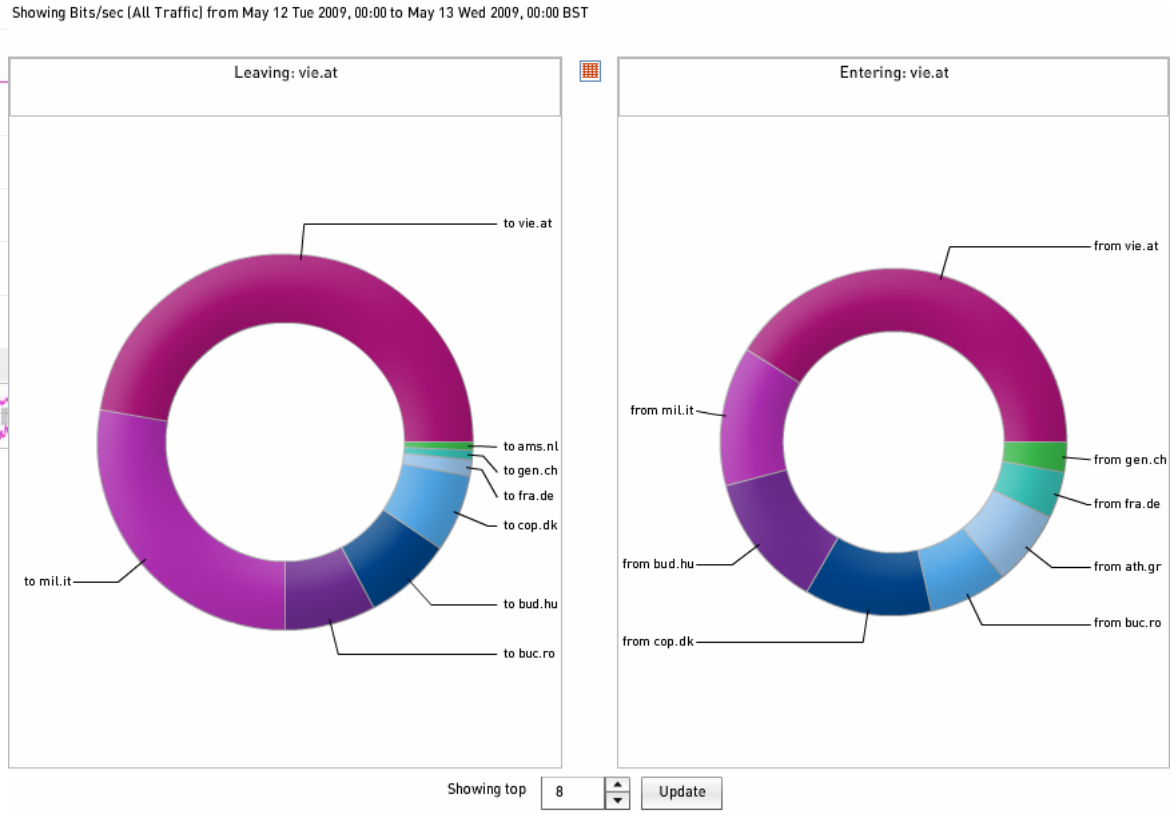
…And The Winner Is…

- Netreflex – Guavus
  - Fuses BGP & ISIS Data
  - Creates an 18 x 18 Router Matrix
  - 21.7 Anomalies per Day (True), 4.6 (False)
  - True False Ratio – 21%
  - Strengths Cover Scans & (D)Dos
  - Origin of Anomalies – Well Balanced NREN vs Non
  - Tests Used 1/1000 Sampling
  - Detected Anomalies In All Peers
  - Higher Cross Section Of Detected Anomalies
  - Changed to 1/100 Sampling

Topology Analysis

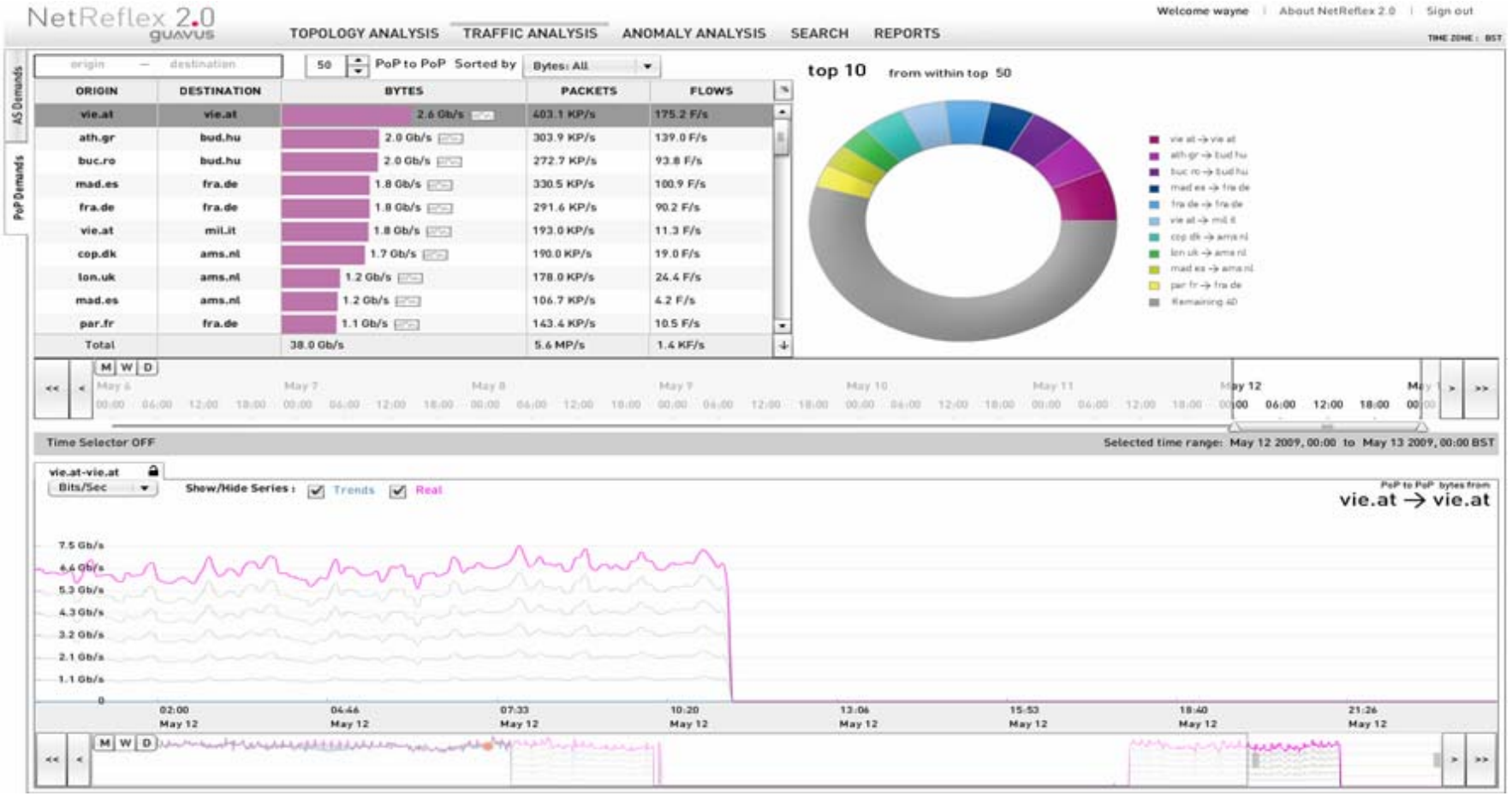
- Landing Page
- Heat Maps (in pipe line)

Topology Analysis…cont



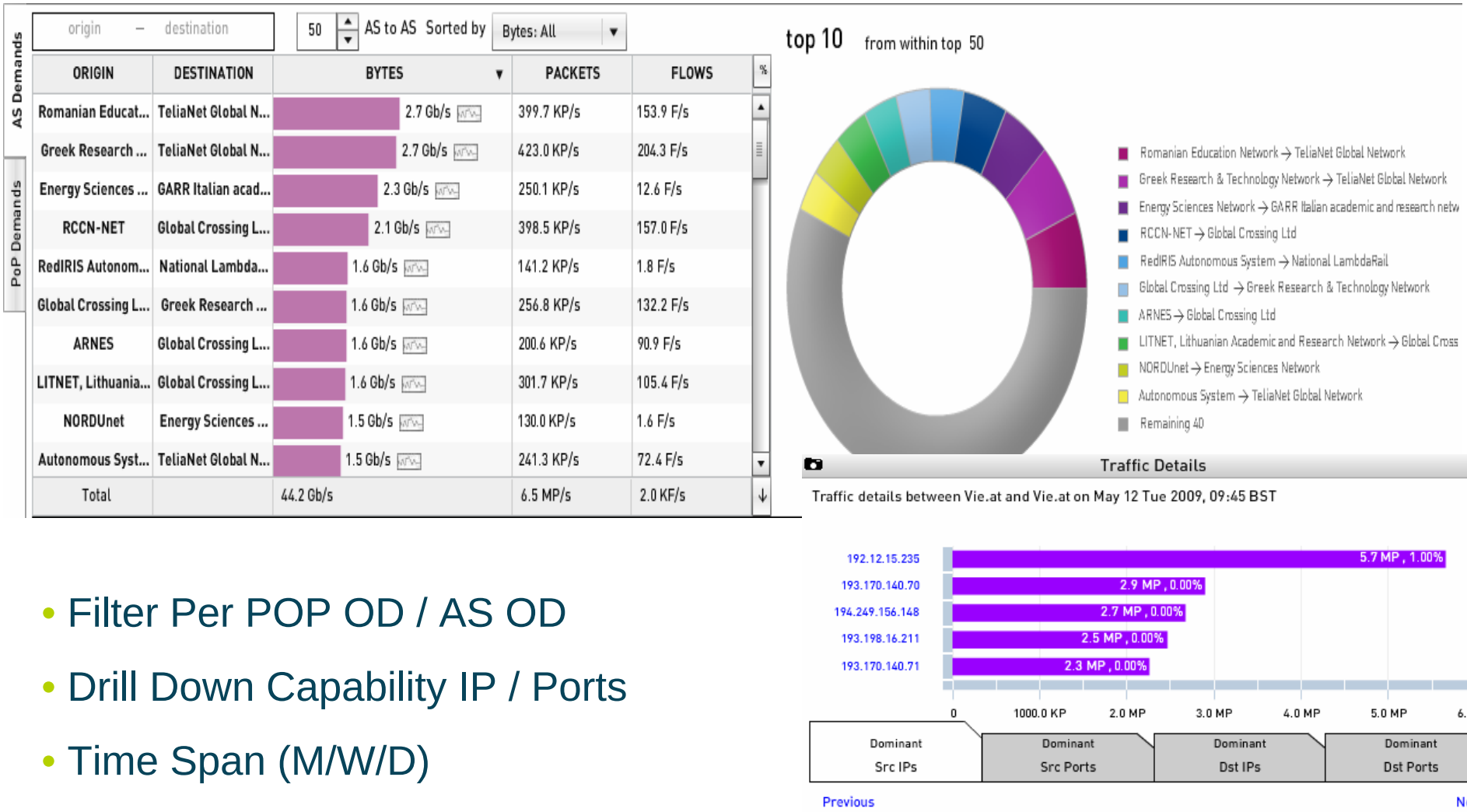
- Cross Section of Traffic (Link)
- Router Level Traffic Analysis
- Time Span (M/W/D)

Traffic Analysis



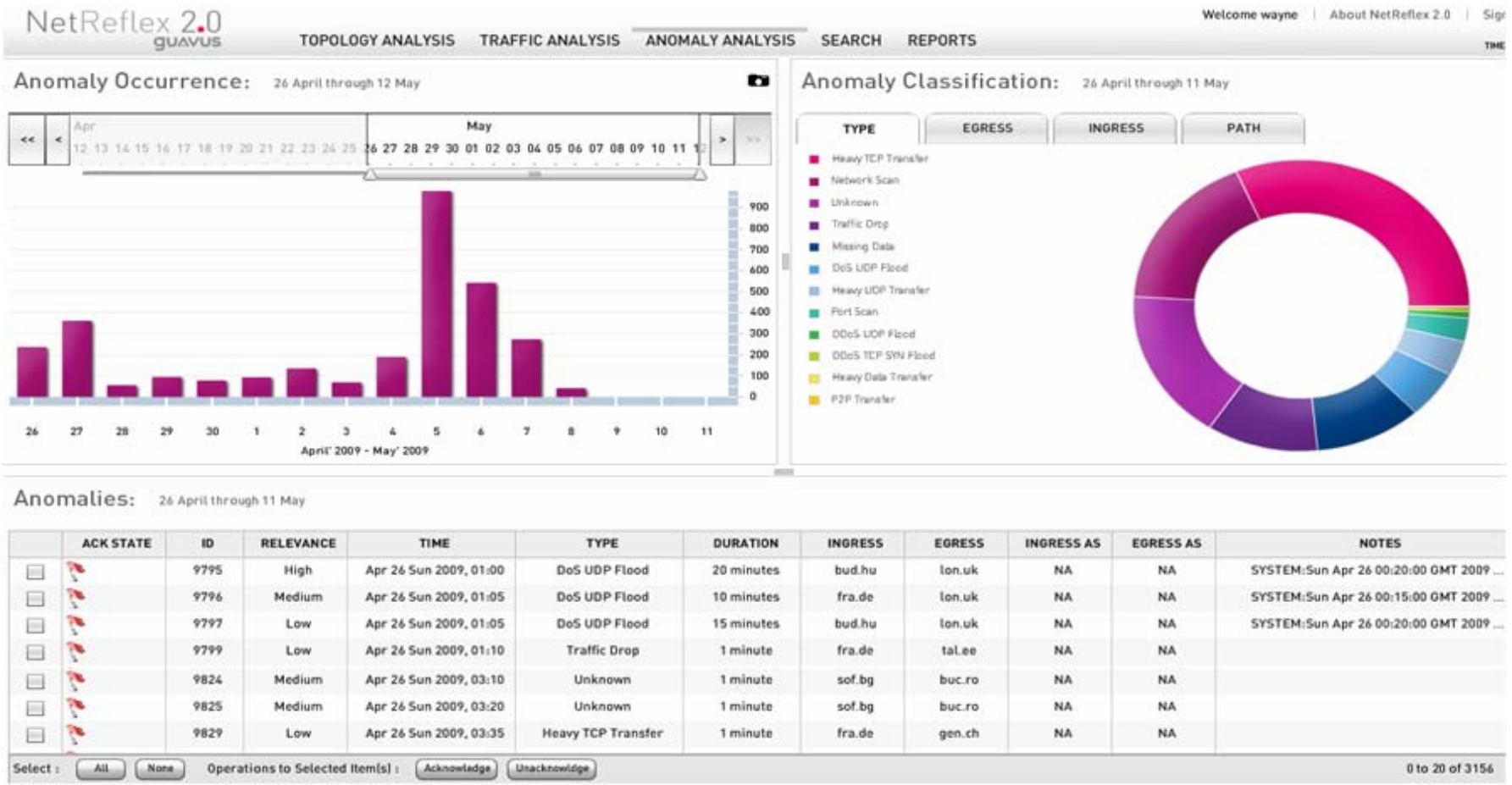
- Multiple Methods to View Data
- Clear Easy to Interpret Interface

Traffic Analysis



- Filter Per POP OD / AS OD
- Drill Down Capability IP / Ports
- Time Span (M/W/D)
- Traffic Planning Possibilities

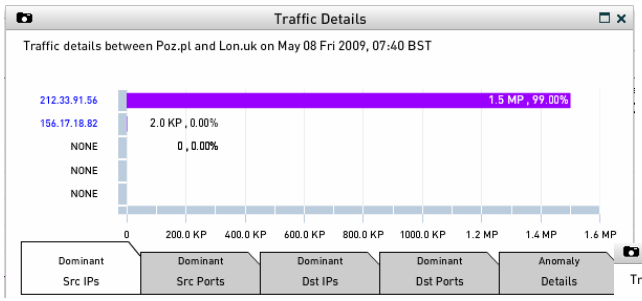
Anomaly Analysis

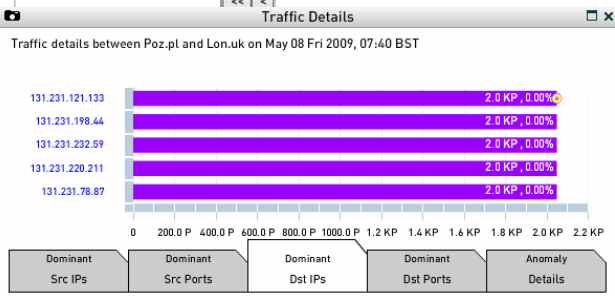


- Anomaly Interface / Alerts
- Per Ingress / Egress / Type / Path

Anomaly Analysis

- Highlight Anomaly Per Type / OD
- Acknowledge Event
- Add Notes
- View SRC / DST / Ports
- Associated Points
- Look at Preceding / Post Times





Conclusion (Not a TBC ☺)

- Started Down Long Road Of Tool Testing
- Sifted Through Hundreds of Results (Forest For The Trees)
- Presented Results To Community
- Chose Solution (Easier Than Said)
- Working Towards Final Implementation
- Work With NREN Partners To Facilitate A Secure GEANT

Questions ?

THANK-YOU!

wayne.routly@dante.net