Why?

• Visualize internet activity
• Visualize large portions of the internet
• Aggregate data according to
  – Continent
  – Country
  – AS
  – IP Prefix
• Identify emerging threats and network anomalies
Data

• Collect via different methods
  – Border gate router log
  – Flow traces
  – Router logs
  – GeoIP
• Store everything in a commercial OLAP
Data

• 2 Dimensions:
  – Address space:
    • 7 continents
    • 190 countries
    • 23054 autonomous systems
    • 197427 prefixes
  – Time:
    • Millisecond
    • Seconds
    • Minutes
    • Hours
    • Days
    • Months
    • Years
Display

- Use hierarchical trees
- Each node = a rectangle
- All children -- inside the parent
- Parent size ~ no. nodes it contains
- Each leaf color = analyzed fact
Features

• Complete space utilization
• Rather easy to generate
• Stable under strong changes
• Easy to understand
• Hard to comprehend
HistoMap - limitations

- Must remove less significant nodes
- Doesn’t aggregate properly under zooming
- Displays only node measurements not interactions
HistoMap results

Geographic HistoMap layout of the upper two levels of the IP hierarchy. Size represents the number of IP addresses assigned to each country. A seventh continent is placed below Australia to visualize ASes without country reference, anonymous proxies, and satellite providers.
HistoMap results

HistoMap 1D layout of all autonomous systems in Germany. The measure (number of incoming connections) of each item is expressed through color.
Order Preserving Layout

- Use StripTree Layout
  - Star with a row
    - Add nodes while the aspect ratio decreases
  - Create a new row and continue
HistoMap – The Internet

Anonymized outgoing traffic connections from our university gateway on November 29th, 2005 showing all 197427 IP prefixes
Visual Analysis of Network Traffic for Resource Planning, Interactive Monitoring, and Interpretation of Security Threats

by Sorin Stancu-Mara
HistoMap – Botnet Spread

Visual Analysis of Network Traffic for Resource Planning, Interactive Monitoring, and Interpretation of Security Threats

by Sorin Stancu-Mara

March 20, 2009
Visual Analysis of Network Traffic for Resource Planning, Interactive Monitoring, and Interpretation of Security Threats

by Sorin Stancu-Mara
Conclusions

- Easy to render
- Easy to understand
- Stable under changes
- Can highlight hierarchical structure and leaf measurements
- Doesn’t show node interactions
- Requires OLAP data provider