

Flamingo: Visualizing Internet Traffic Data

Manish Karir, Jon Oberheide, Mike Goff
Networking R&D, Merit Network Inc.

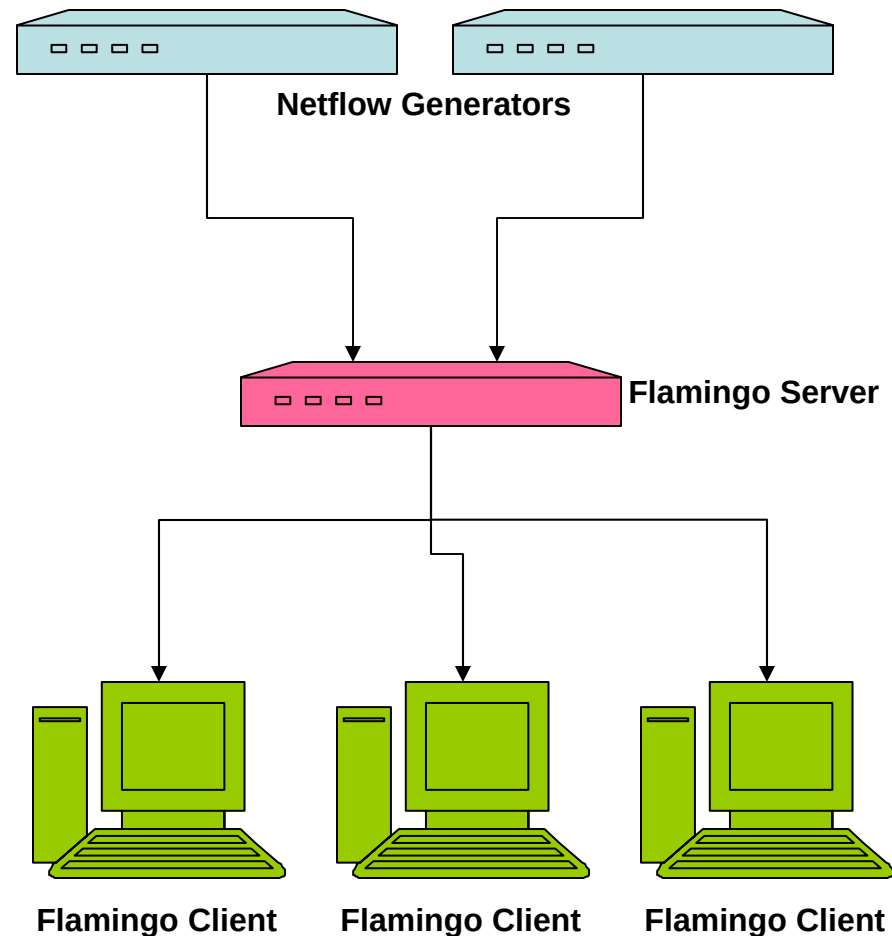
- Introduction: What is Flamingo
- Visualizations
- The Flamingo Tool
 - Combining visualization with controls
- Case Studies
 - Traffic Anomaly
 - Network Scans
 - Worm traffic
 - P2P traffic
 - The Slashdot effect!

Introduction

- Flamingo is a unique software tool that enables 3D Internet traffic data exploration in real-time
- Provides a series of different visualization methods to illustrate different aspects of the data
- Based on information extracted from netflow records
- Includes additional tools/filters to allow people to easily extract “information” from raw netflow data

Introduction: Flamingo Architecture

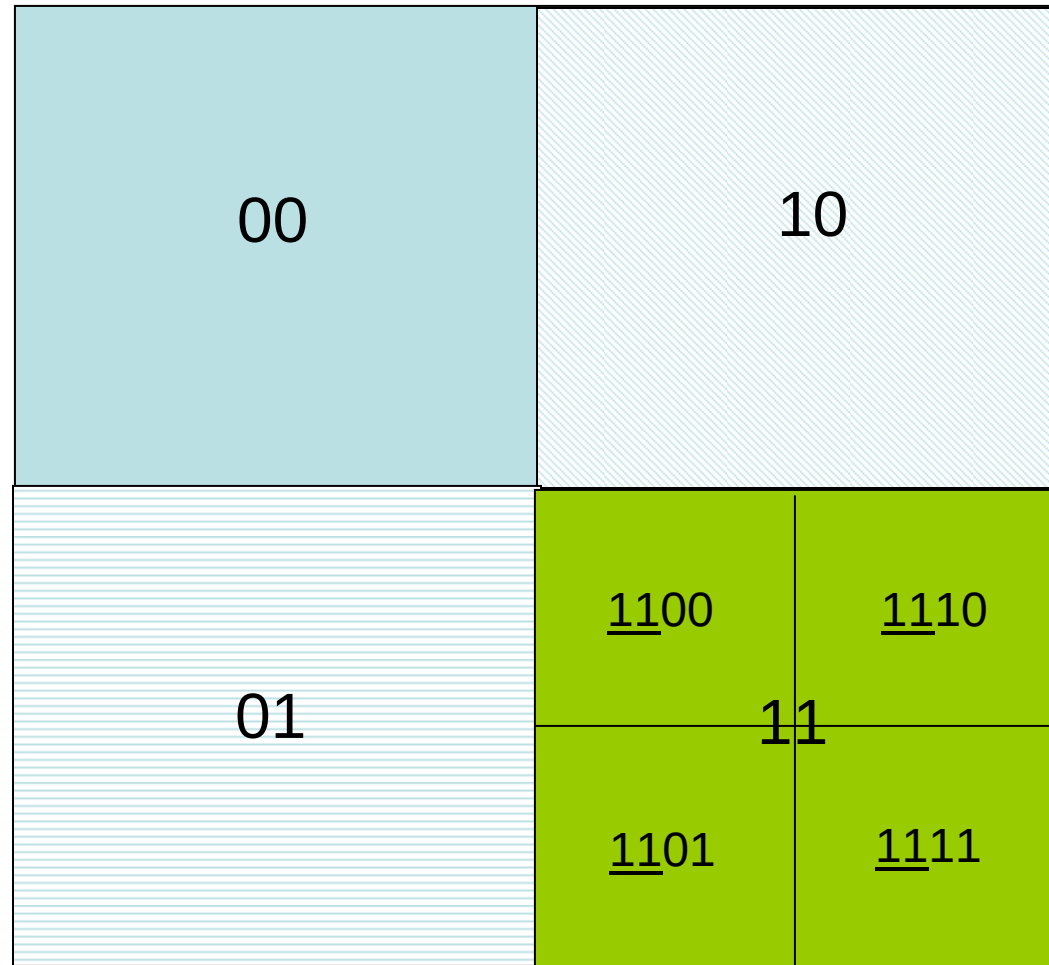
- Client/Server Architecture
- A single server can support multiple clients
- A single server can act as collector for multiple netflow feeds
- Supports both aggregation as well as non-aggregation mode



Visualization Methods

- Based on Extended Quad-Tree Implementation
- Traffic Volume by src/dst IP prefix
- Traffic Volume by src/dst AS
- Traffic distribution across src/dst ports
- Traffic flows between src/dst IP prefixes
- Traffic flows between src/dst IP/ports

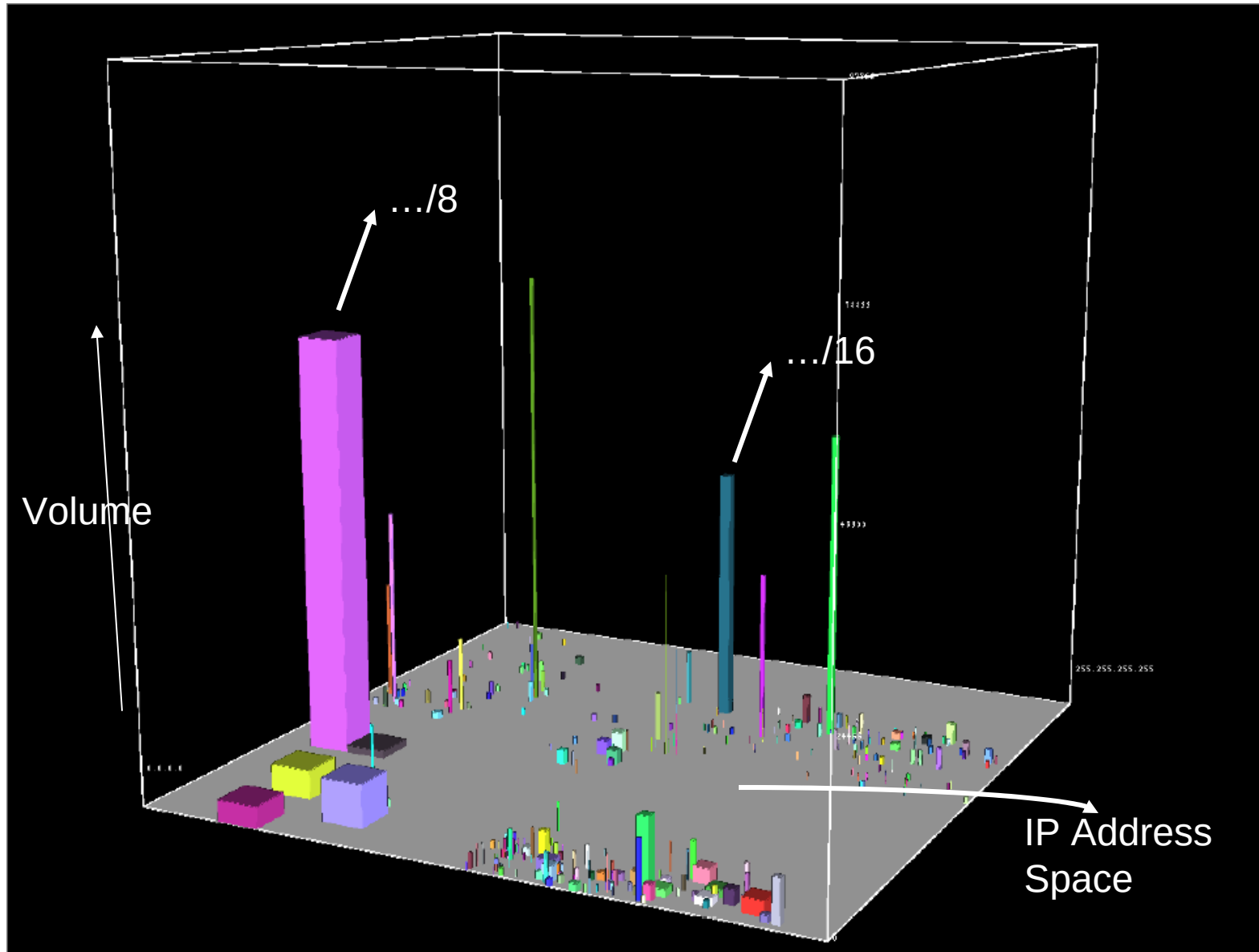
The Basic Quad-Tree



Traffic Volume by Src/Dst IP

- The 2D quad-tree map is used as the base of a visualization cube
- We plot prefixes from a BGP routing table onto the base of the cube, size of prefix determines size of representation on 2D base
- Longest prefix match is used to map netflow IP addresses onto BGP prefixes
- The z-axis/height is used to represent the volume of traffic
- Different color is used for each prefix

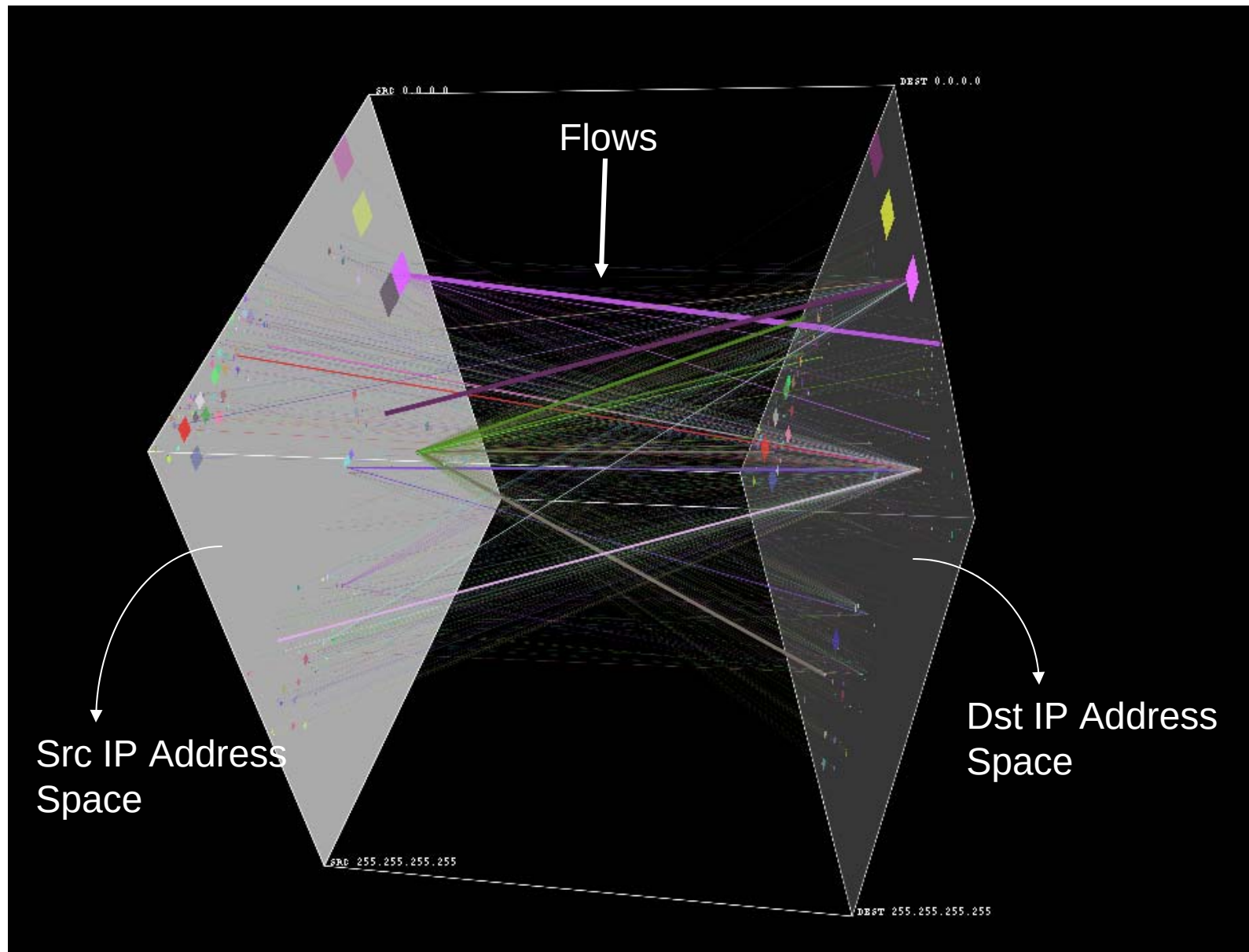
Traffic Volume by Src/Dst IP



Traffic Flows by Aggregated Src/Dst IP

- Flows contain source and destination information, which might map to 2 different prefixes, so far we only have the ability to represent a single flow
- Solution: Use 2 inside surfaces of a cube, one for source, one for destination, represent a flow by a line between them
- Thickness of line represents relative traffic volume

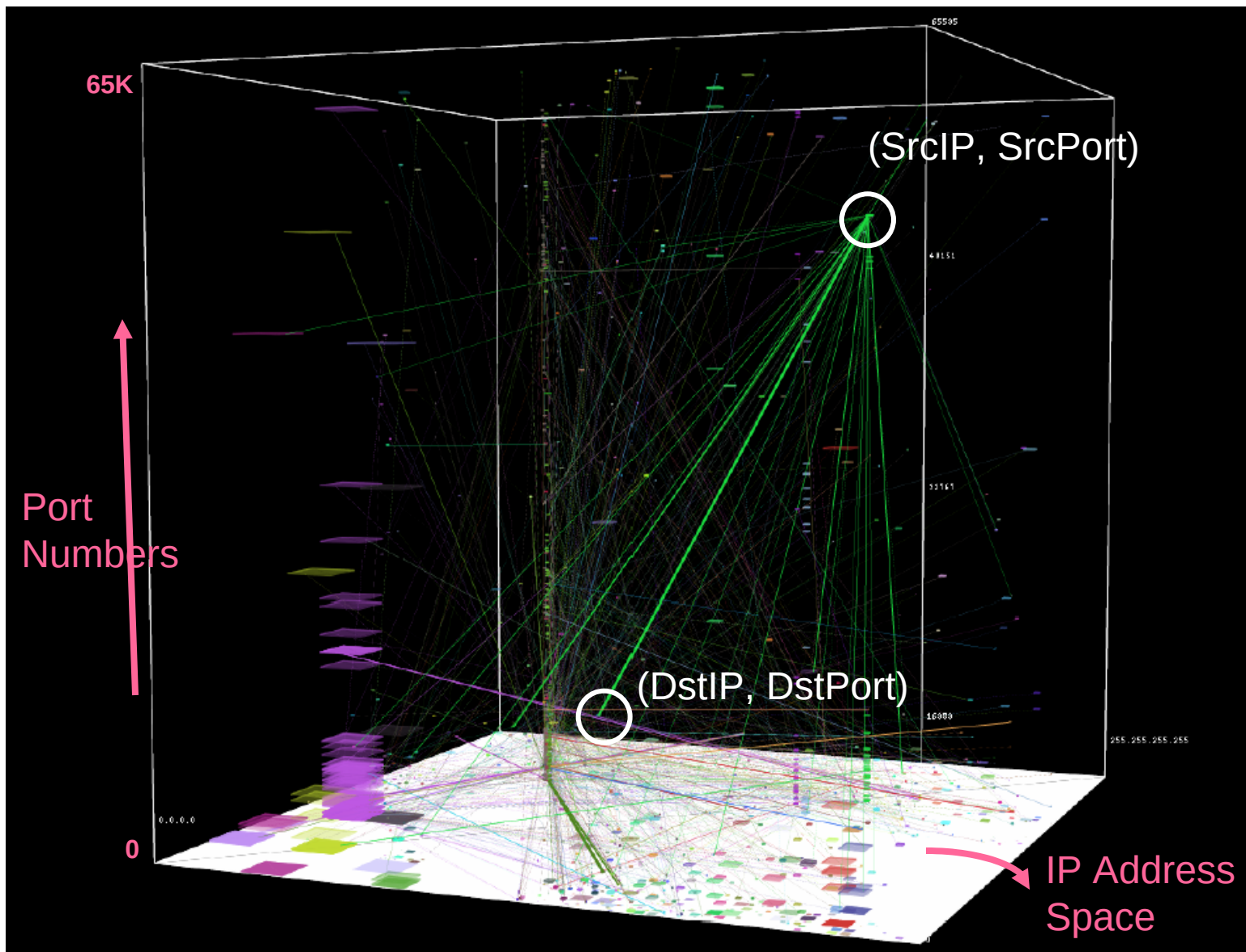
Traffic Flows by Aggregated Src/Dst IP



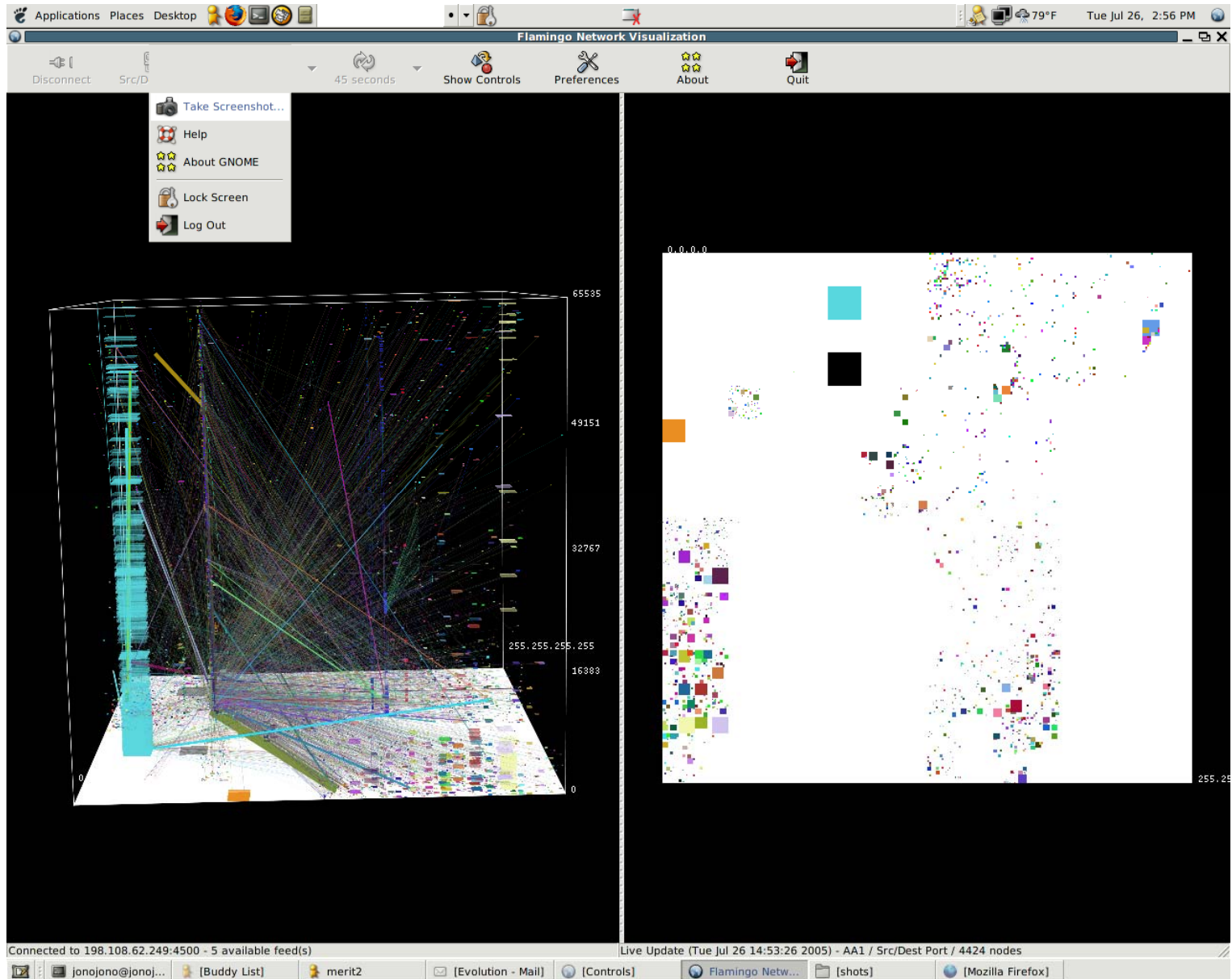
Traffic Flows by Src/Dst IP and Port

- Flows contain source/destination port number information as well
- Solution:
 - Use base of cube to represent prefixes, both source and destination are on the same base
 - The z-axis is used to represent port numbers, source and destination
 - (srcIP, srcPort) >>>>>>>>> ((x1,y1), z1)
 - (dstIP, dstPort) >>>>>>>>> ((x2,y2), z2)
 - Line between these 2 points in 3D space represents a flow from (srcIP, srcPort) to (dstIP, dstPort)
 - Line thickness represents relative volume of traffic
 - Same color used for all flows with same source IP

Traffic Flows by Src/Dst IP and Port

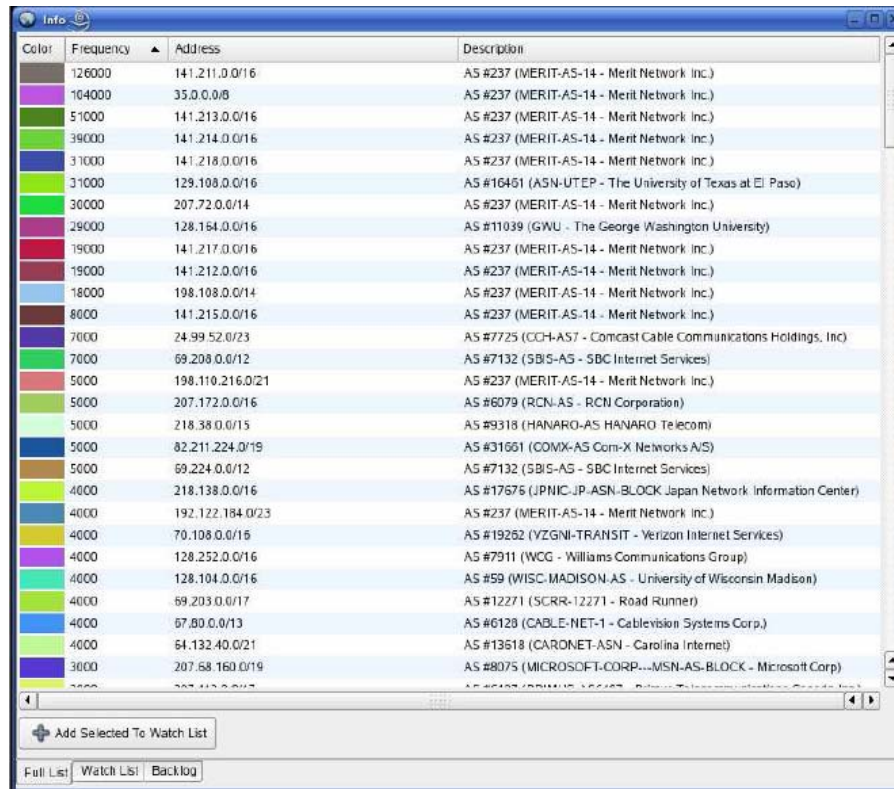


Flamingo Visualization Tool



Flamingo Controls

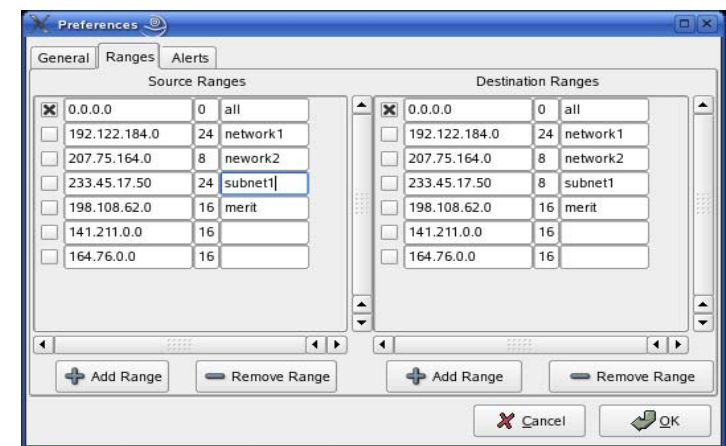
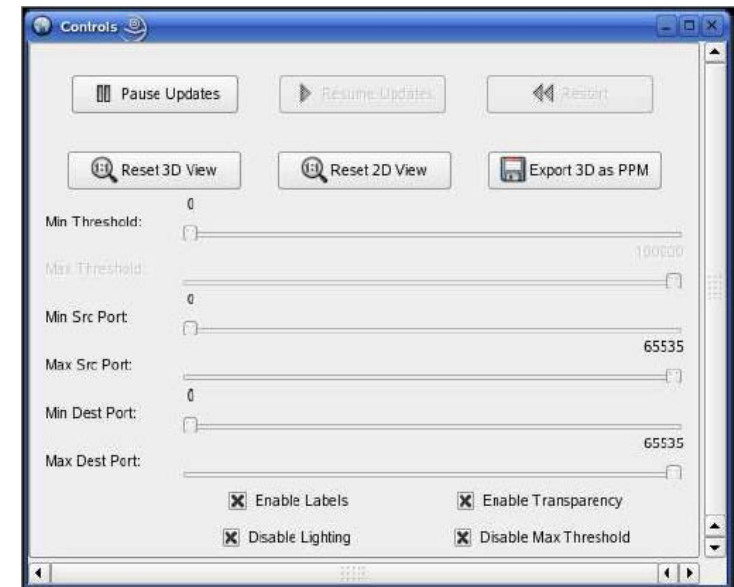
Text Representation of Visualized Information



The 'Info' window displays a table with four columns: Color, Frequency, Address, and Description. The table lists various network entries with their corresponding colors, frequencies, IP addresses, and descriptions.

Color	Frequency	Address	Description
126000	141.211.0.0/16	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
104000	35.0.0.0/8	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
51000	141.213.0.0/16	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
39000	141.214.0.0/16	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
31000	141.218.0.0/16	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
31000	129.108.0.0/16	AS #16451 (ASN-UTEP - The University of Texas at El Paso)	
30000	207.72.0.0/14	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
29000	128.184.0.0/16	AS #11039 (GWU - The George Washington University)	
19000	141.217.0.0/16	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
19000	141.212.0.0/16	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
18000	198.108.0.0/14	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
8000	141.215.0.0/16	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
7000	24.99.52.0/23	AS #7725 (CCH-AS7 - Comcast Cable Communications Holdings, Inc)	
7000	69.208.0.0/12	AS #7132 (SBC-AS - SBC Internet Services)	
5000	198.110.216.0/21	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
5000	207.172.0.0/16	AS #6079 (RCN-AS - RCN Corporation)	
5000	218.38.0.0/15	AS #9318 (HANARO-AS HANARO Telecom)	
5000	82.211.224.0/19	AS #31661 (COMX-AS Com-X Networks A/S)	
5000	69.224.0.0/12	AS #7132 (SBC-AS - SBC Internet Services)	
4000	218.138.0.0/16	AS #17676 (JPNIC-JP-ASN-BLOCK Japan Network Information Center)	
4000	192.122.184.0/23	AS #237 (MERIT-AS-14 - Merit Network Inc.)	
4000	70.108.0.0/15	AS #19262 (YZGNI-TRANSIT - Verizon Internet Services)	
4000	128.252.0.0/16	AS #7911 (WCG - Williams Communications Group)	
4000	128.104.0.0/16	AS #59 (WISC-MADISON-AS - University of Wisconsin Madison)	
4000	69.203.0.0/17	AS #12271 (SCRR-12271 - Road Runner)	
4000	67.80.0.0/13	AS #6128 (CABLE-NET-1 - Cablevision Systems Corp.)	
4000	64.132.40.0/21	AS #13618 (CARONET-ASN - Carolina Internet)	
3000	207.68.160.0/19	AS #8075 (MICROSOFT-CORP...-MSN-AS-BLOCK - Microsoft Corp)	

Slider Bar Controls

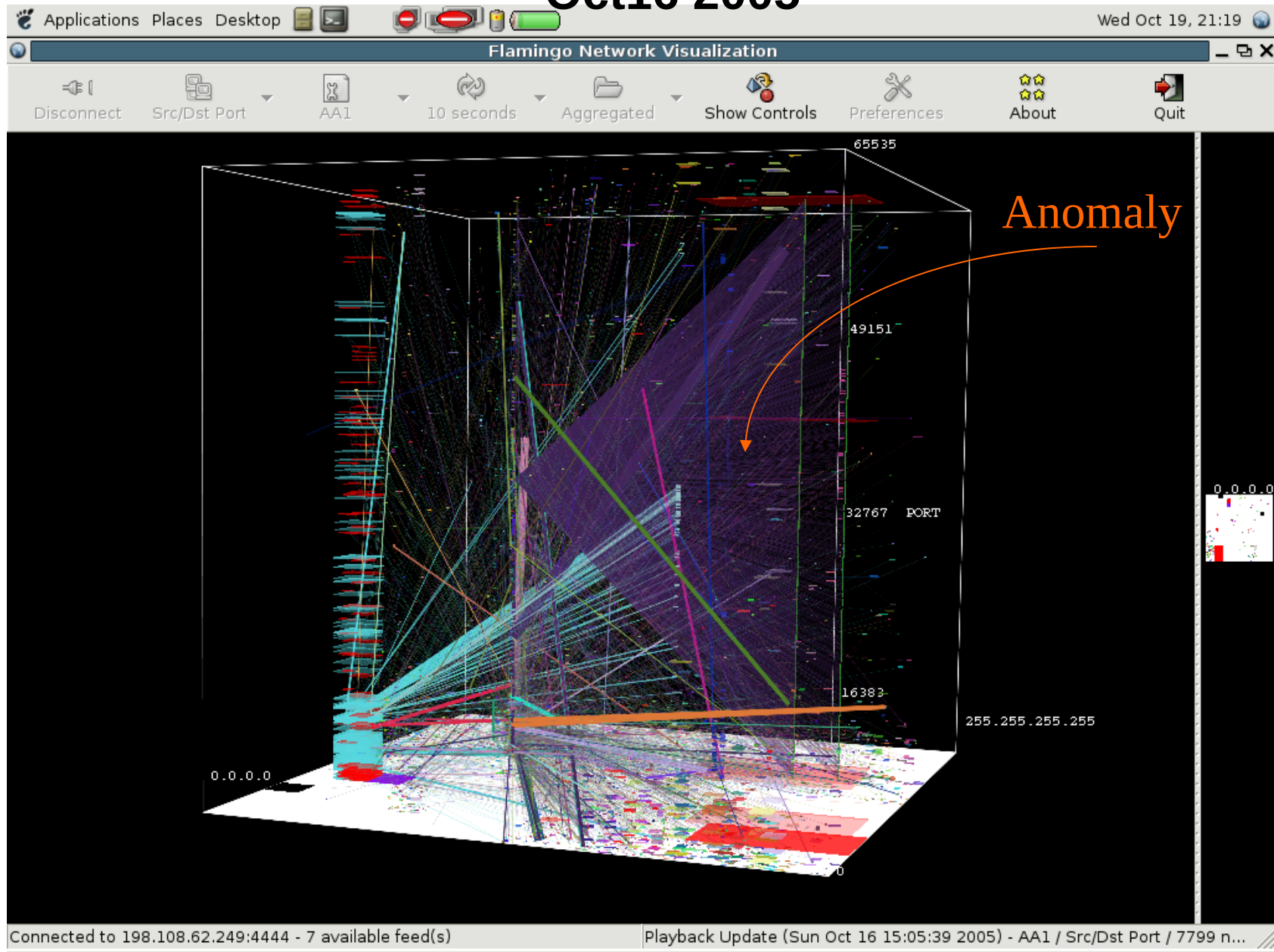


Address Range Configuration

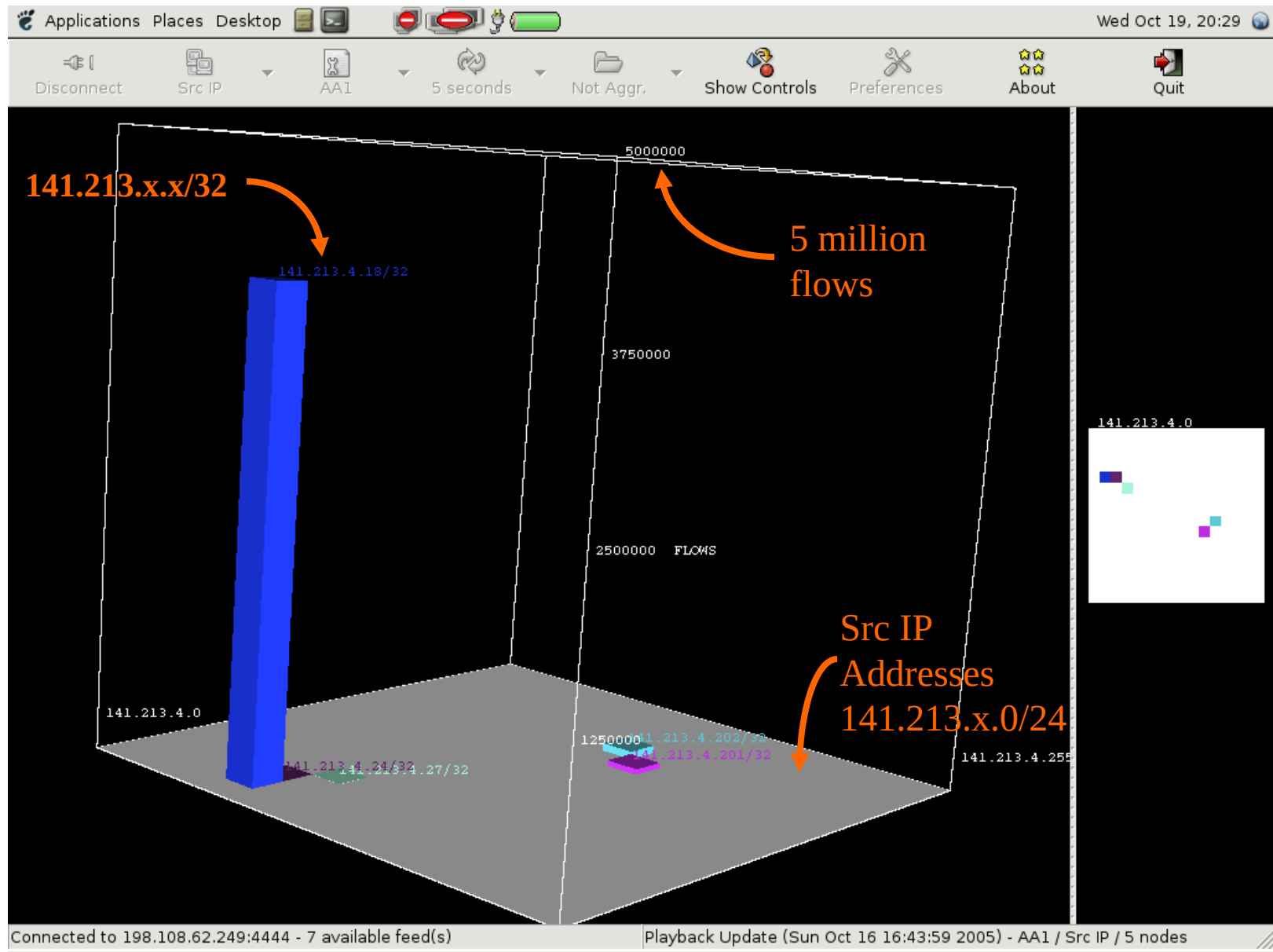
Case Study: Traffic Anomaly Sunday- Oct 16, 2005

- Large burst of traffic visible outgoing from 141.213.x.x(x.x.umich.edu)
- Start time roughly – 12PM - End time roughly – 6PM
- Single srcIP/port – few(4) targetIP's/multiple ports
- UDP flows
- Traffic pattern visible in the normal clutter
- We then proceed to examine the src (141.213.x.0/24) and target prefixes (216.74.128.0/18, 217.199.32.0/19) in more detail in the following sequence of images

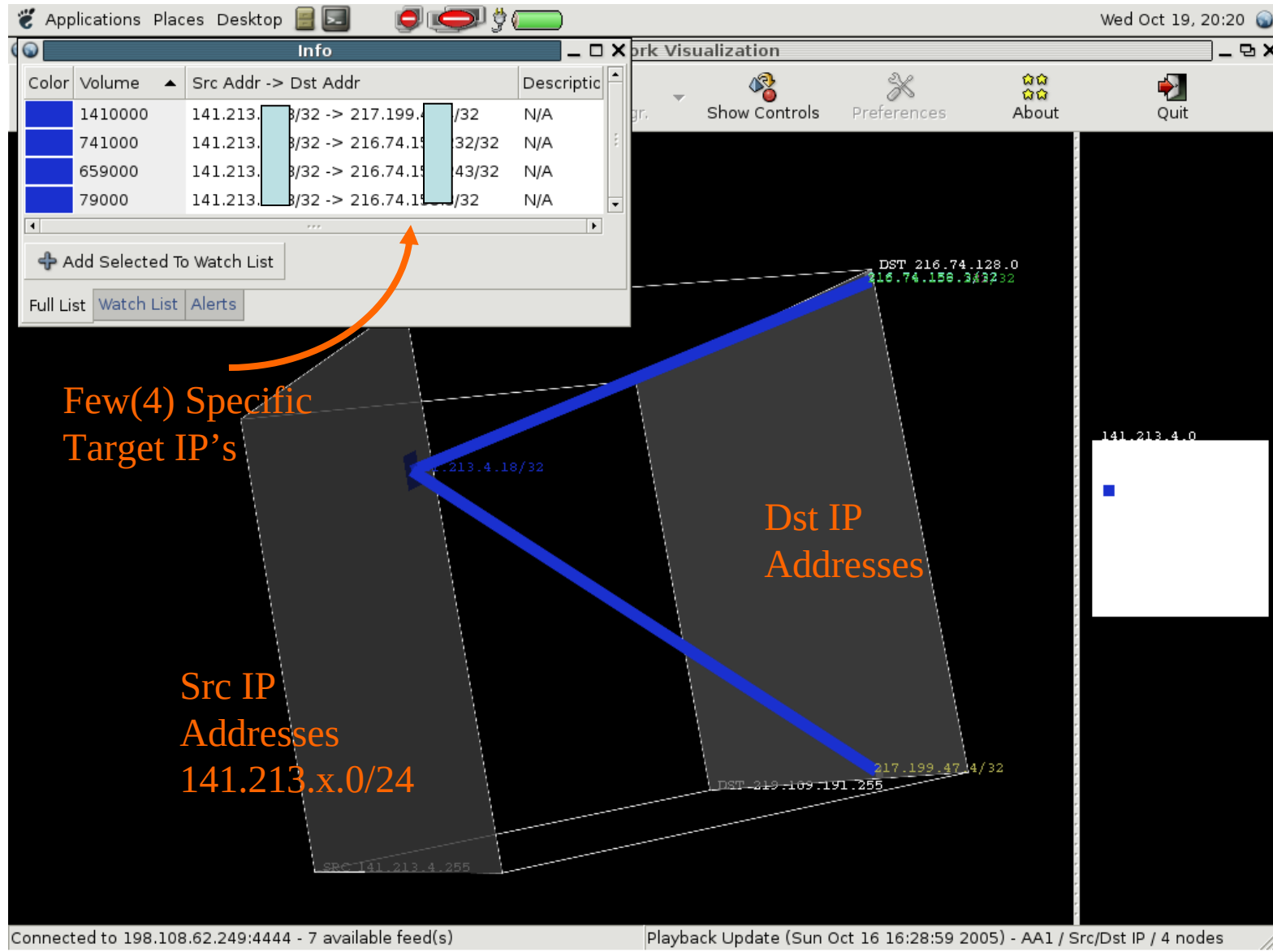
Overall Traffic Pattern at Primary Router Sunday, Oct16 2005



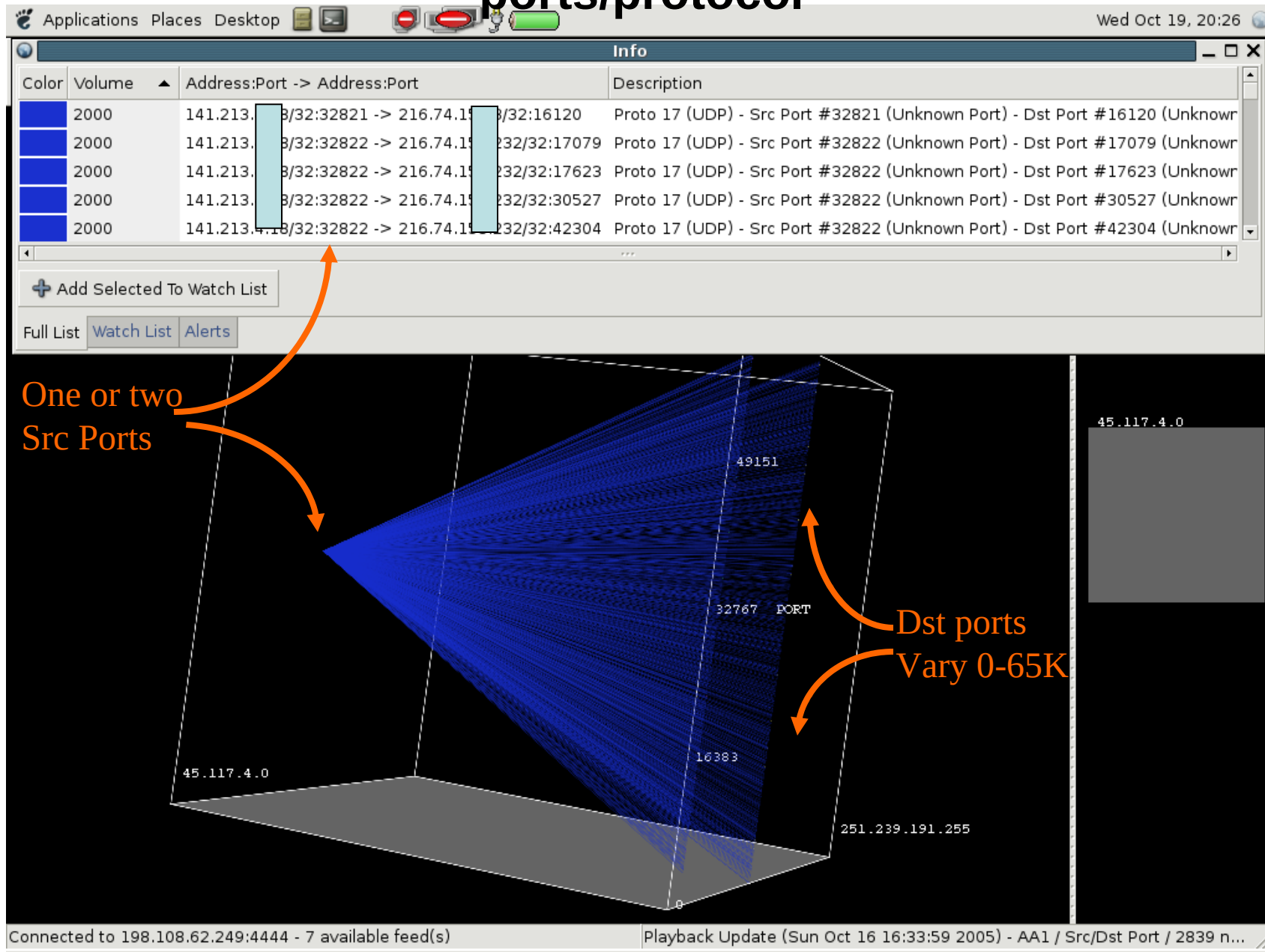
Traffic Volume sourced from /24 subnet by individual hosts



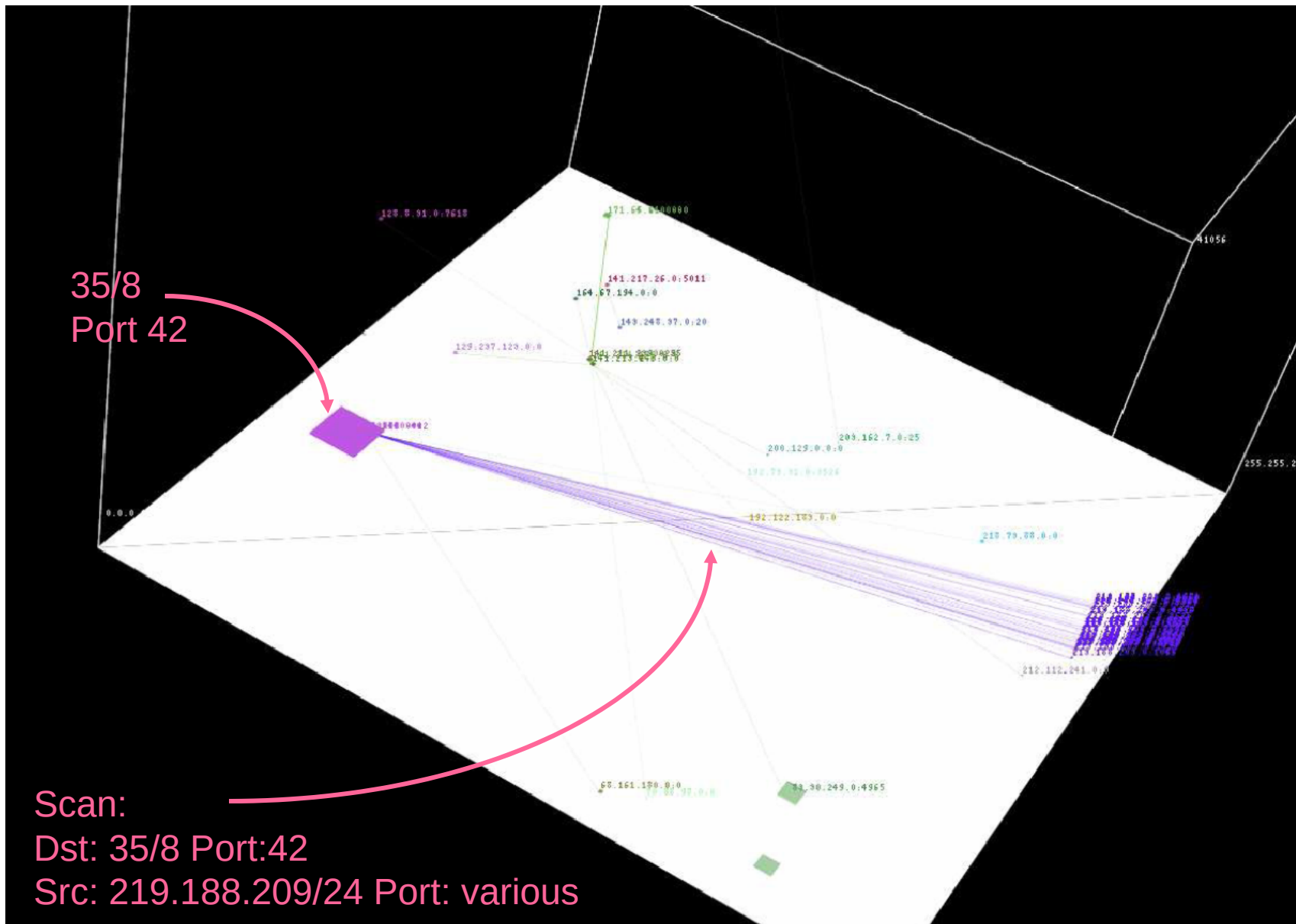
Distribution of Target IP Addresses



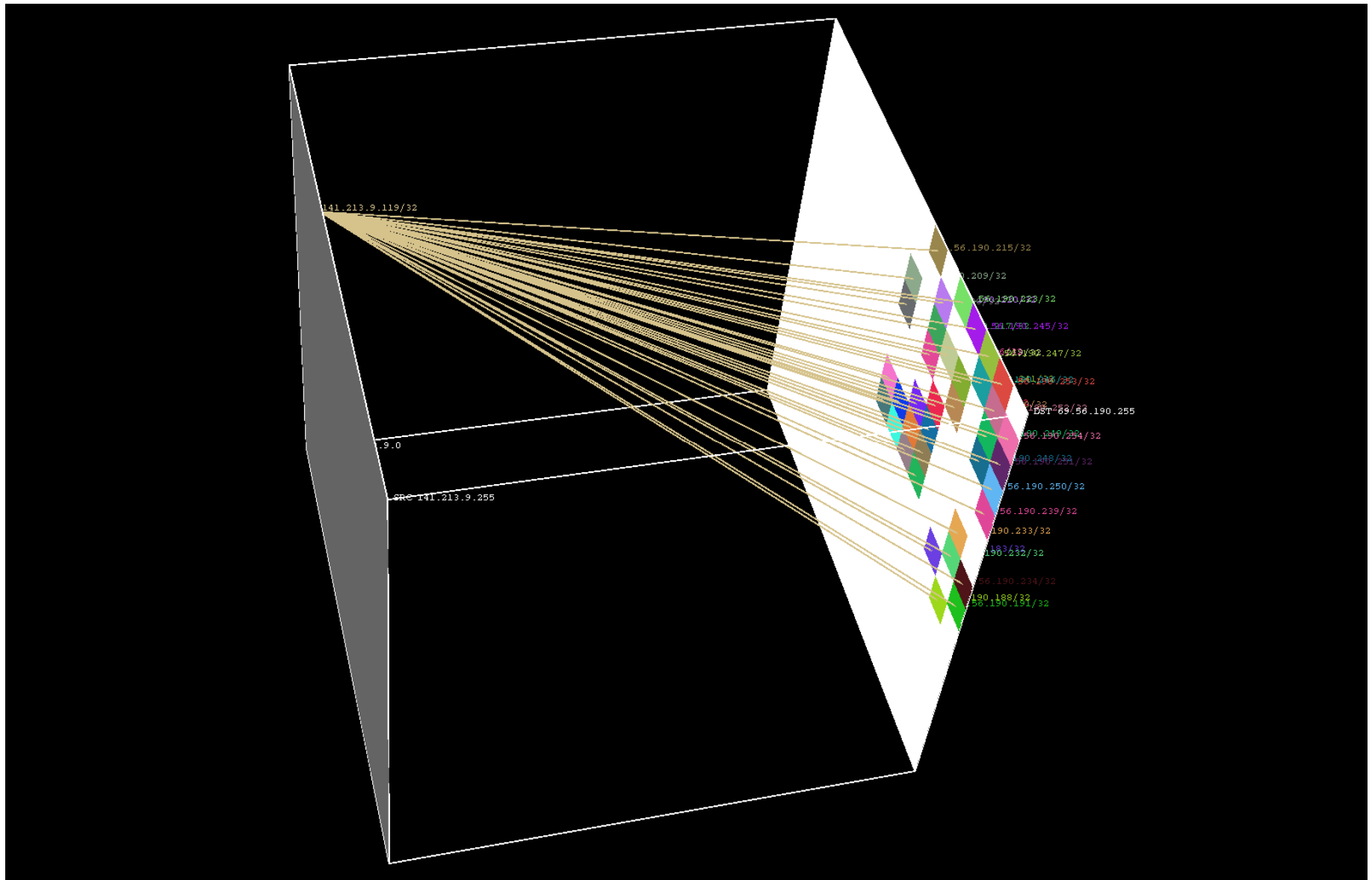
Distribution of flows in terms of src/dst ports/protocol



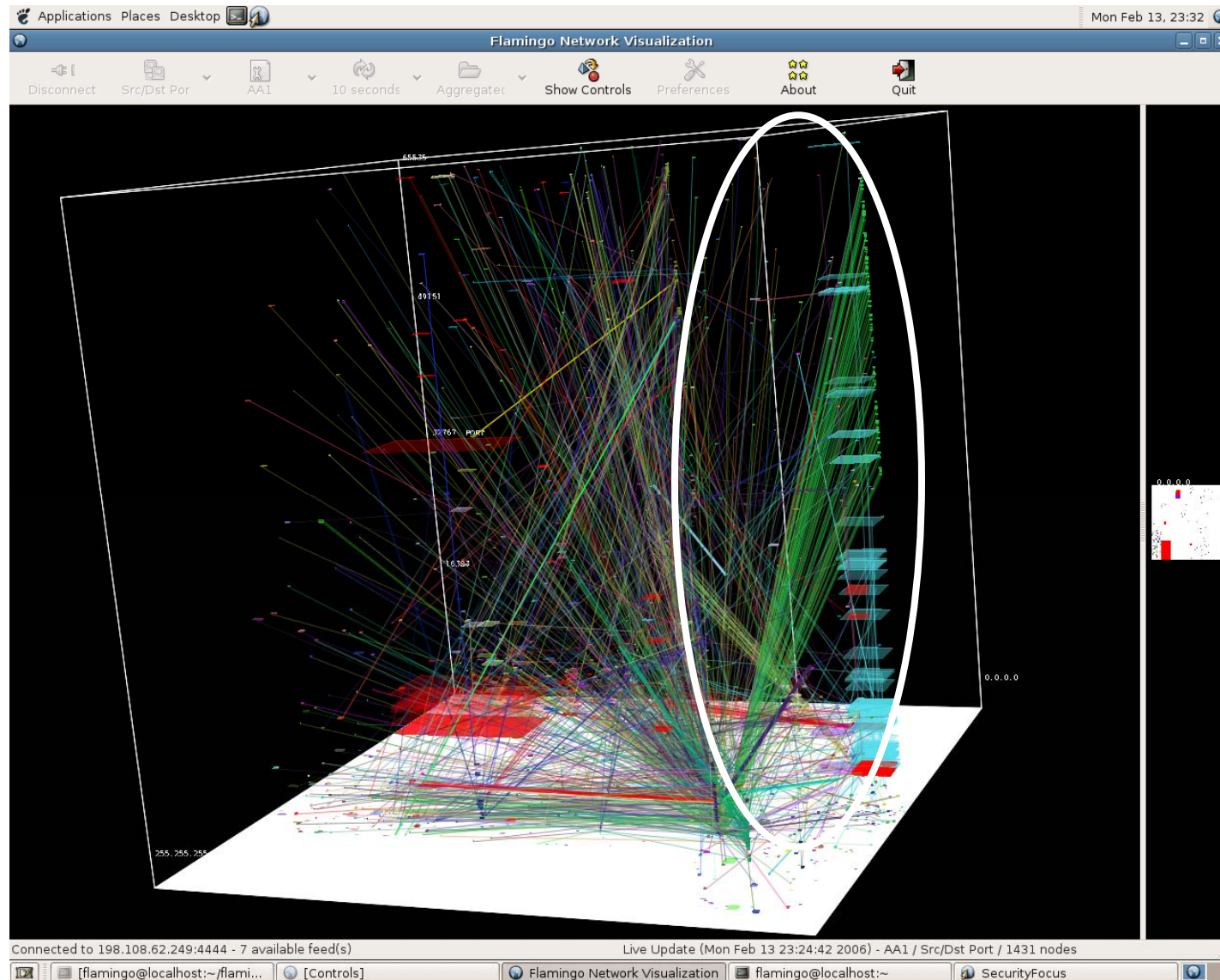
Case Study: Worm Traffic/Port 42 Scans



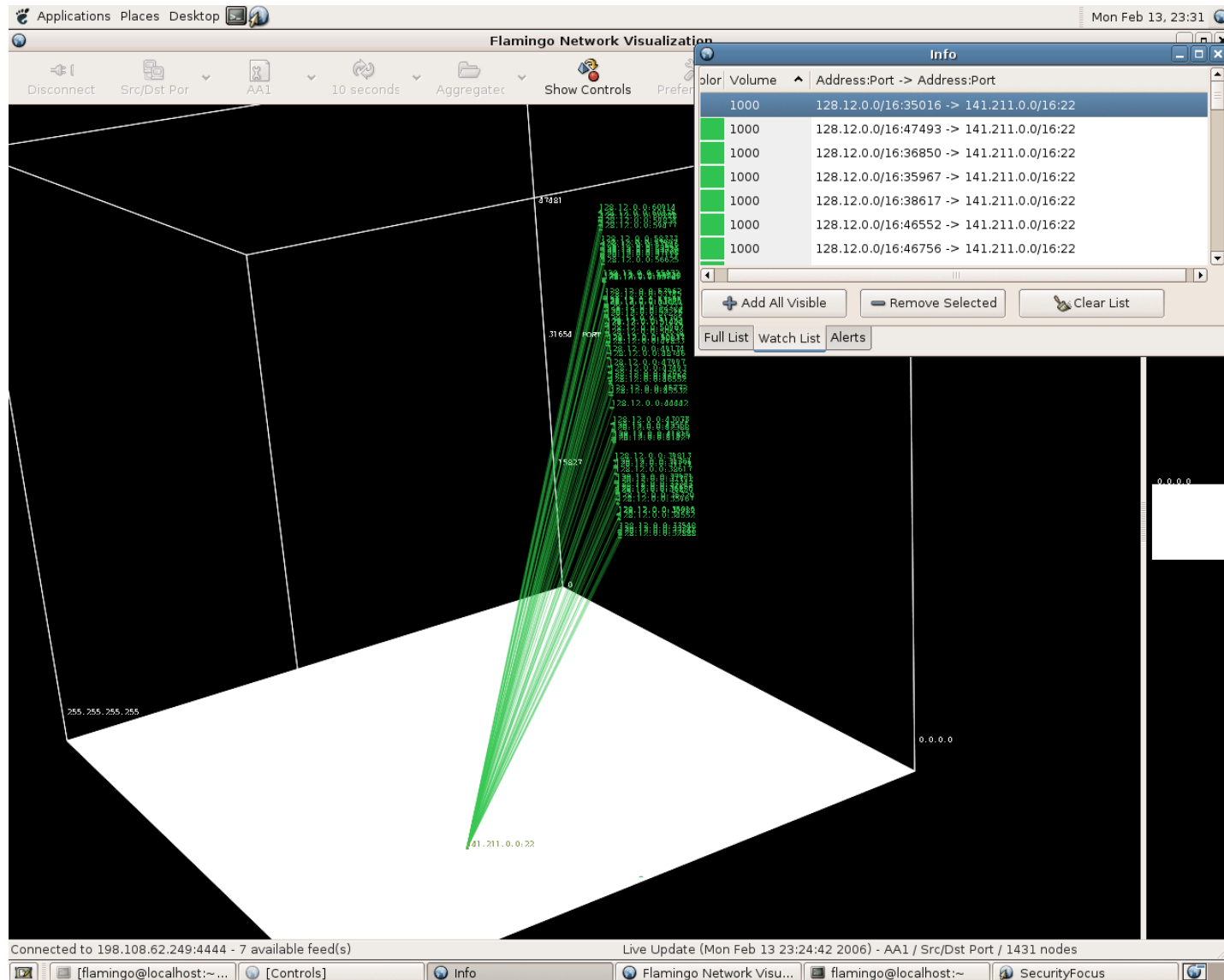
Case Study: /24 Network Scan



ssh scans

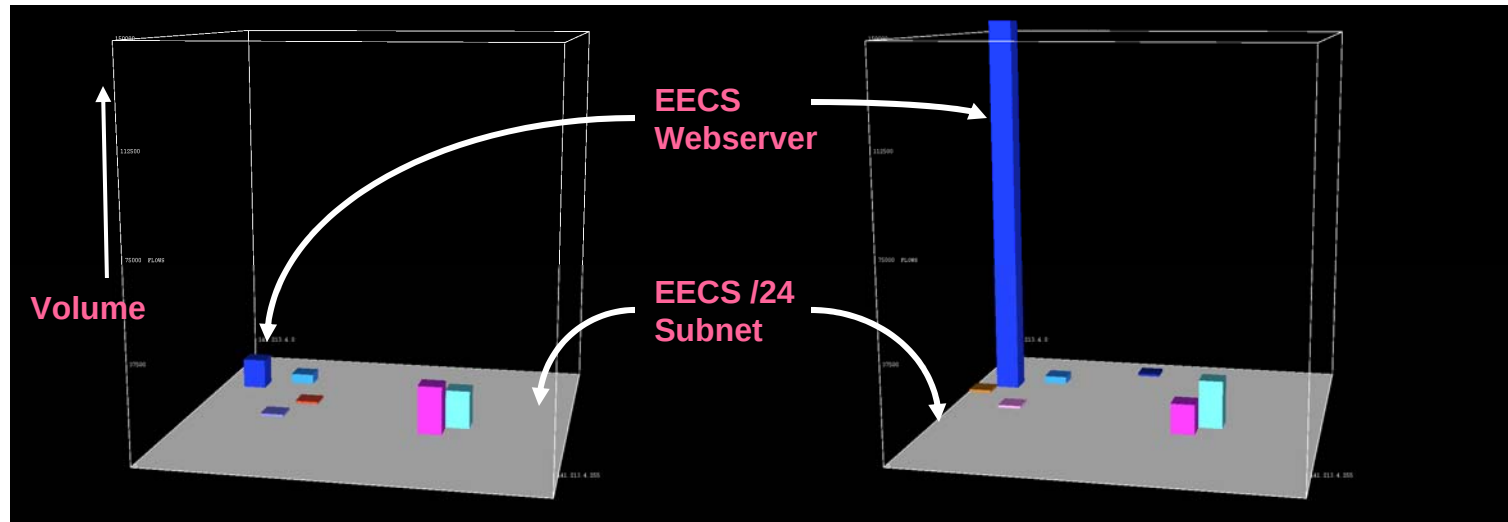


ssh scan

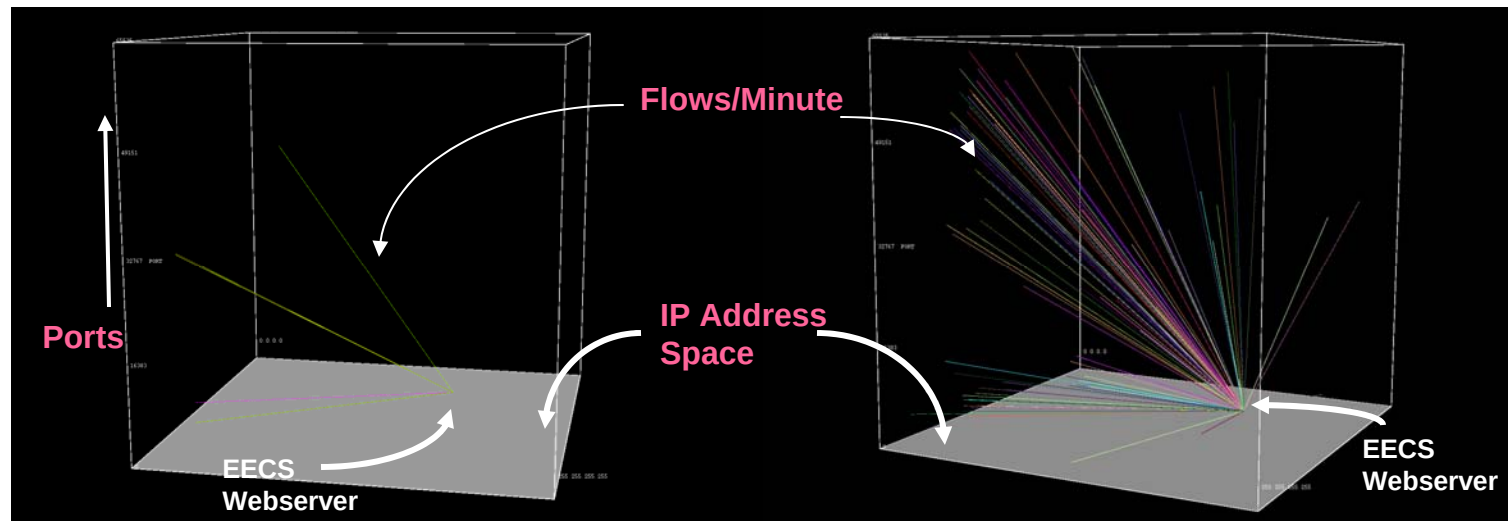


Case Study: Slashdot Event Oct 31, 2004

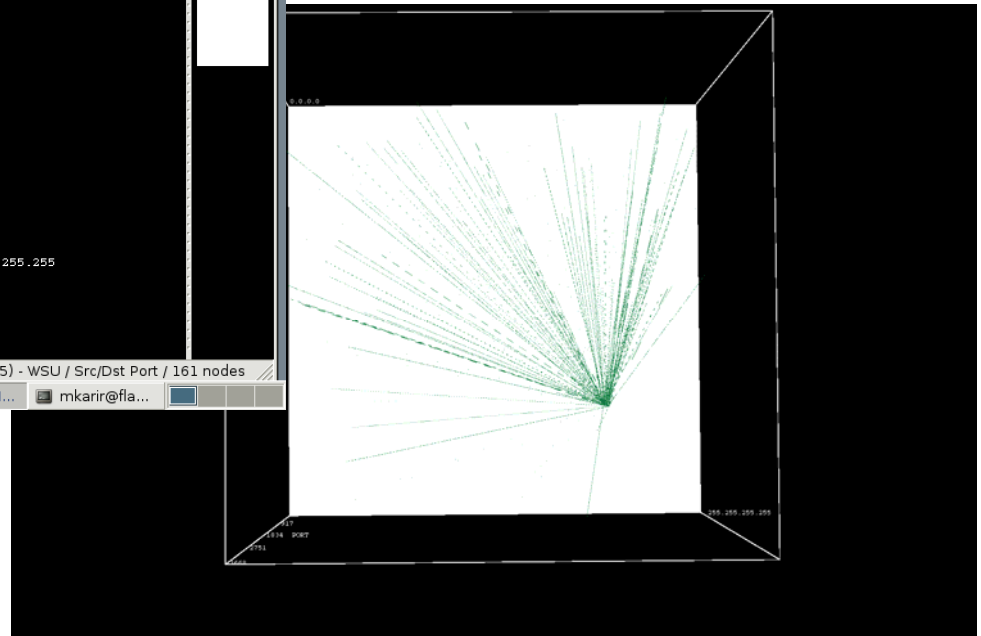
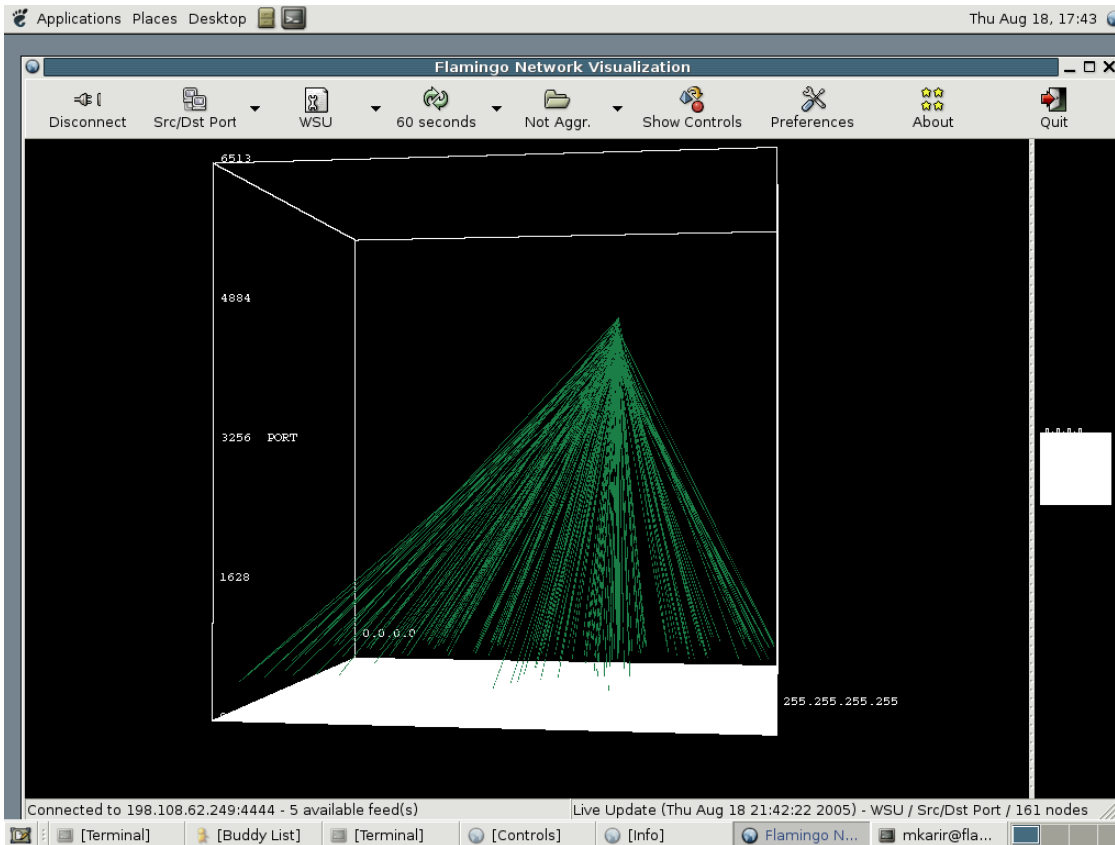
Traffic Volume



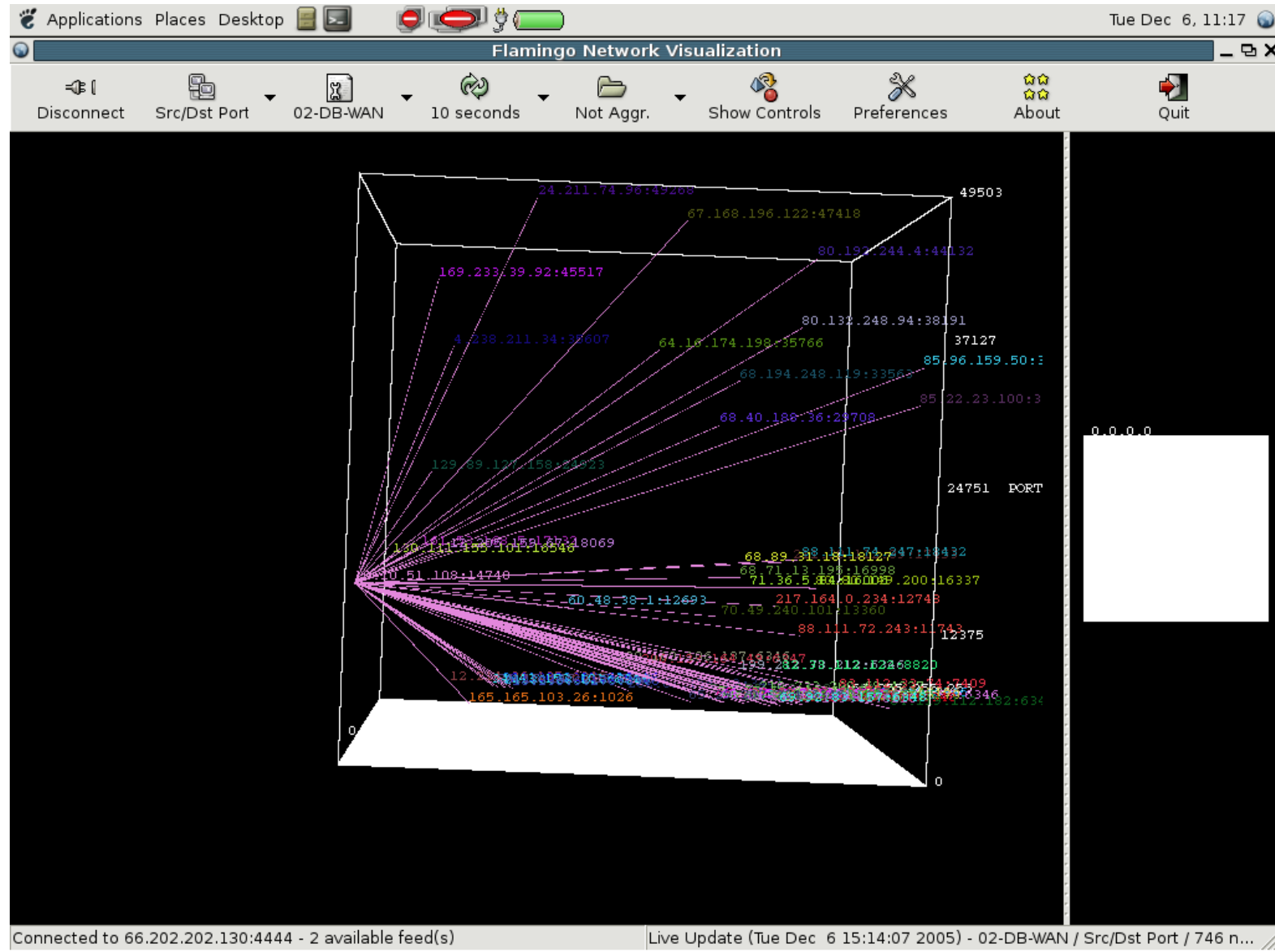
Flow Volume



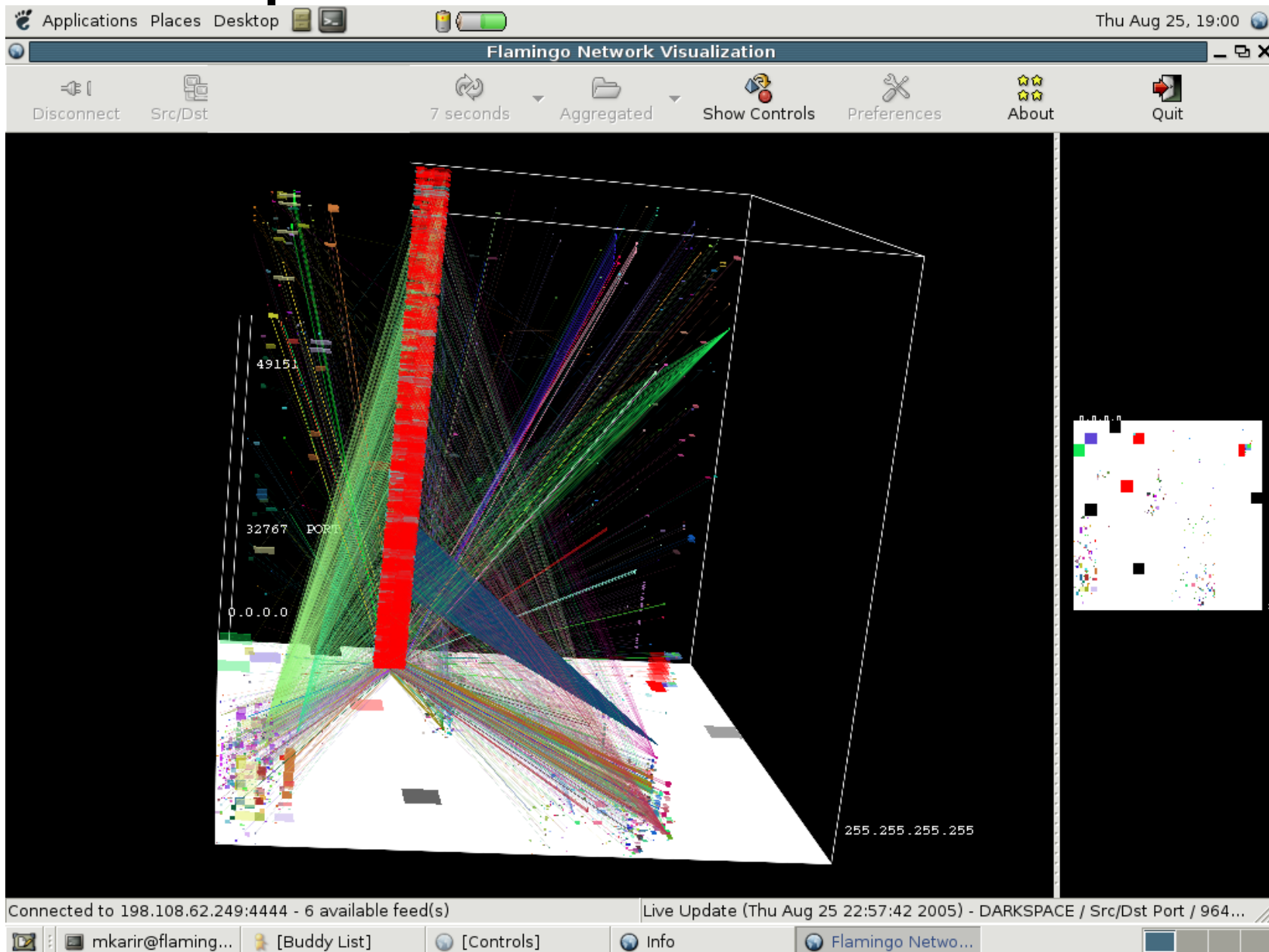
Zotob Worm Infection



P2P Traffic



Darkspace Traffic Visualization



Conclusion

- The Flamingo Visualization Tool provides users with the ability to easily explore and extract meaning information regarding traffic flows in their network
- More details can be found at:
 - <http://flamingo.merit.edu>