Extracting Information from Network Data

Manish Karir, Jon Oberheide
Merit Network, Inc.

Dionysus Blazakis
University of Maryland

Outline

- The Problem
- BGP/Routing Information
  - BGP-Inspect – Information Extraction from BGP Update messages
  - VAST – Internet AS topology Visualization
- Netflow/Traffic Information
  - Flamingo – Internet Traffic Exploration
- Conclusions

The Problem

- Large amounts of data are now, or soon will be available:
  - Route Views, RIPE Archives, PREDICT, etc
- The problem is no longer access to raw data but how to extract useful information from the raw data
- Need tools that can:
  - Scale to large input datasets
  - Provide useful data summarizations
  - Are easy to use
  - Provide useful information
- BGP-Inspect, VAST, Flamingo are tools that we have implemented that attempt to address this problem

BGP-Inspect: Why and What

- Analyzing MRT Data:
  - Large volumes of data ~RV-66G compressed
  - Extracting useful information requires writing custom parsers even for basic information
  - Lots and lots of redundancy
- Approach:
  - Preprocess Route Views data
  - Remove redundancy as much as possible
  - Use data compression to the extent possible
  - Build efficient indices to help queries
  - Pre-compute and store commonly used statistics at data load time not at query time
  - Build easy to use interface

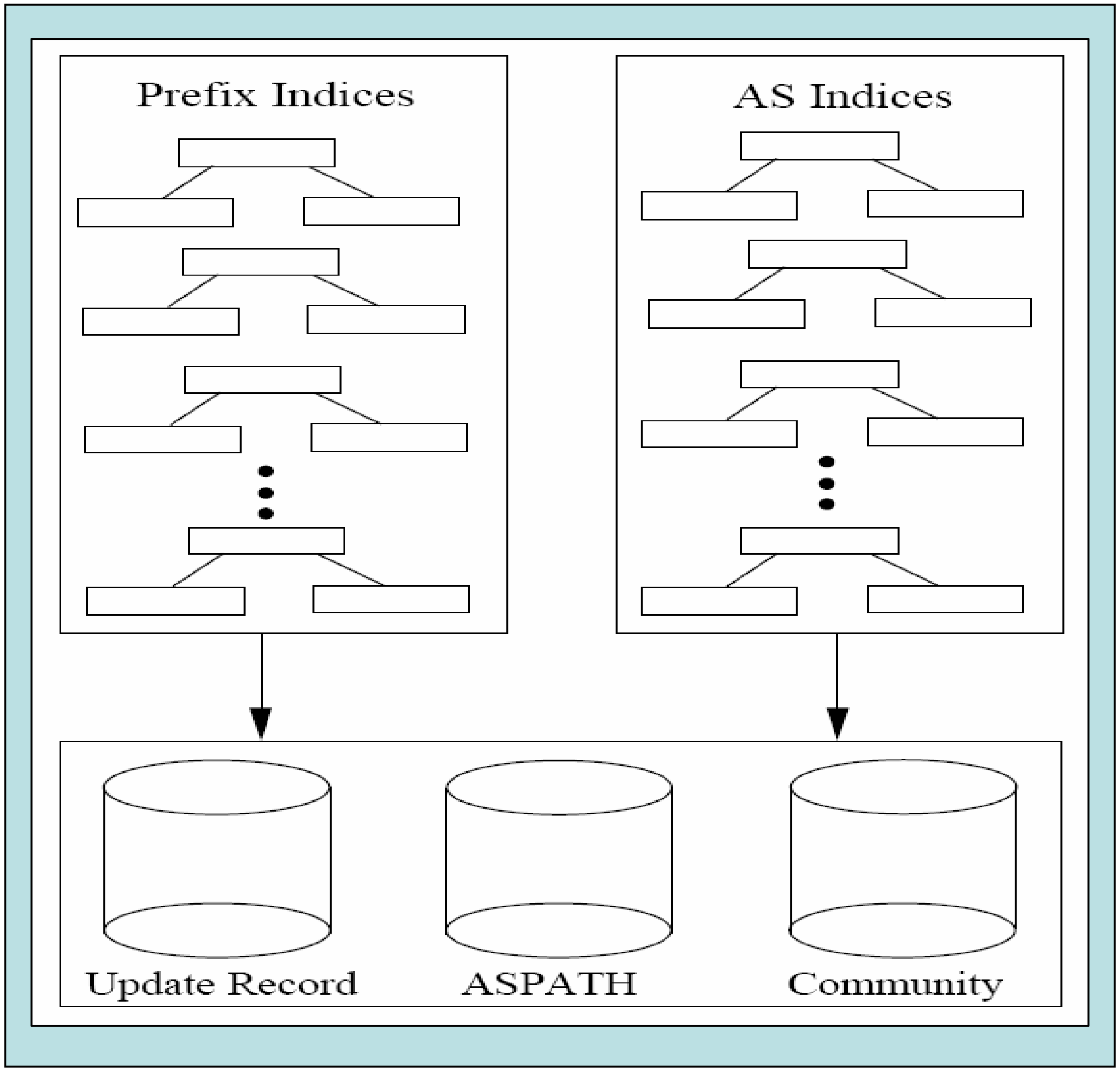
BGPdb vs. BGP-Inspect

- BGPdb is the core of the BGP-Inspect system
- BGPdb represents the pre-processed database, which is queried by the BGP-Inspect interface

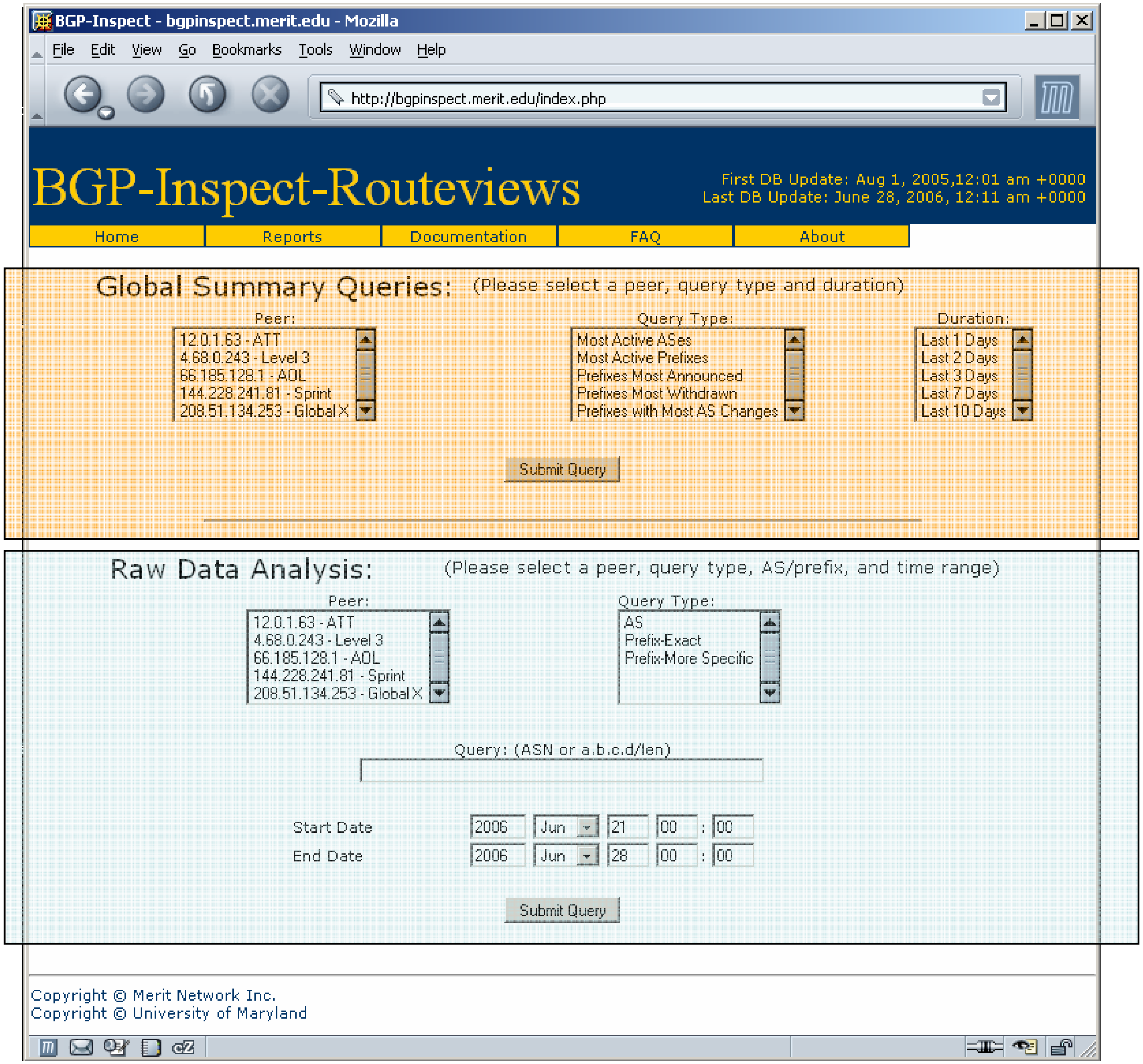
BGPdb – Techniques and Algorithms

- Removing redundancy from BGP datasets
  - ASPATH, COMMUNITY, UPDATE Msgs are repeated over and over, only time changes
- Compressed-Chunked Files
  - Compromise between size and usability
- B+ Tree indices
  - Indexing based on time, this enables fast time-range queries
- Caching while processing input datasets
  - Messages are repetitive, so keep cache of previous processing for speedup

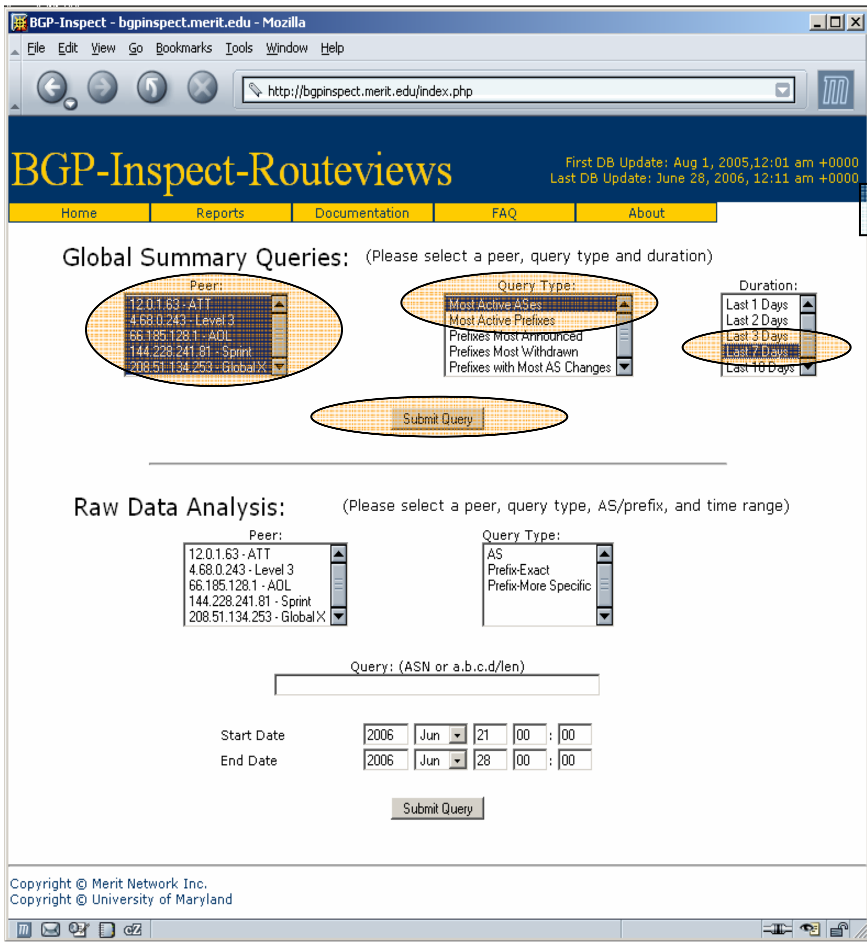
BGPdb – System Architecture

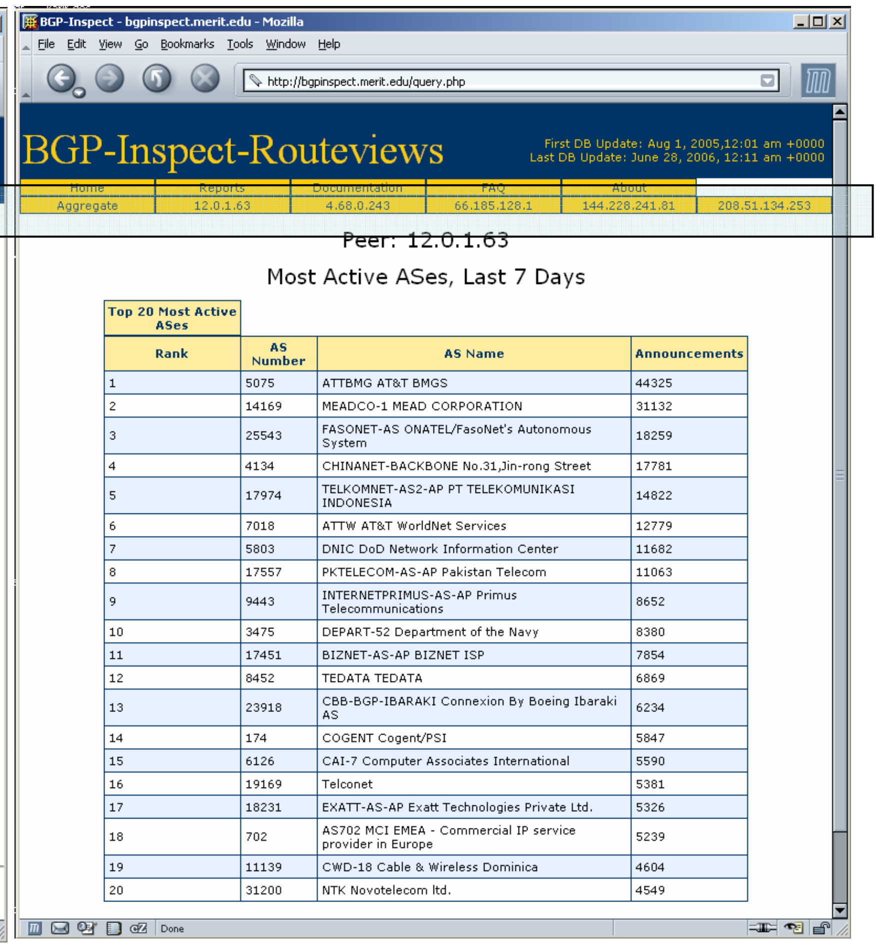


BGP-Inspect Interface



Global Queries – Most Active ASes

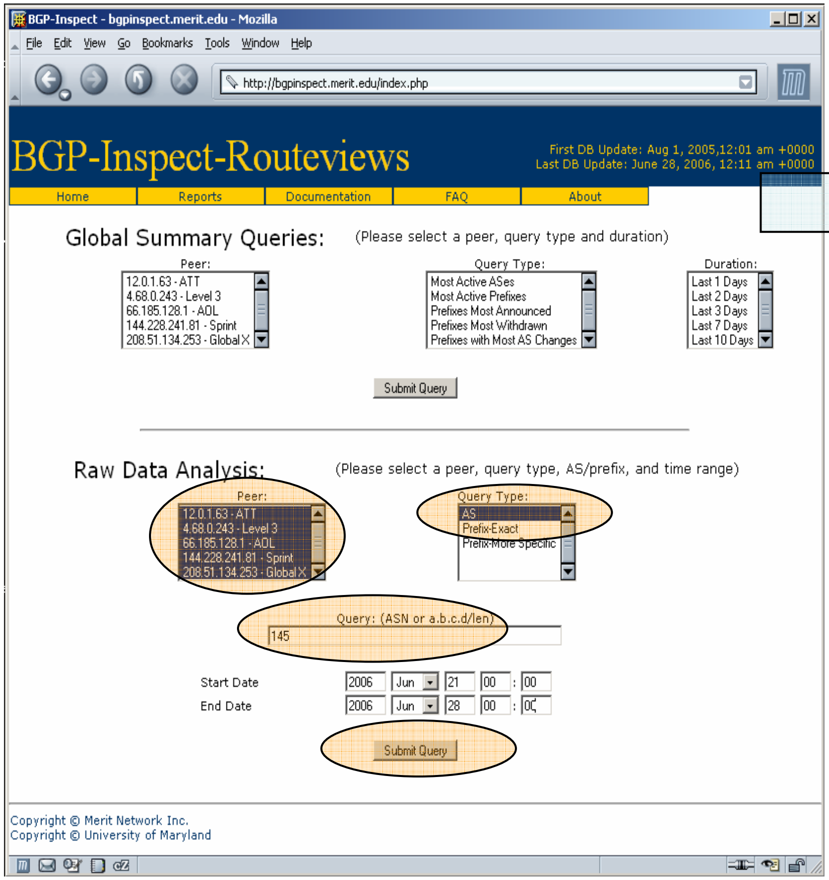


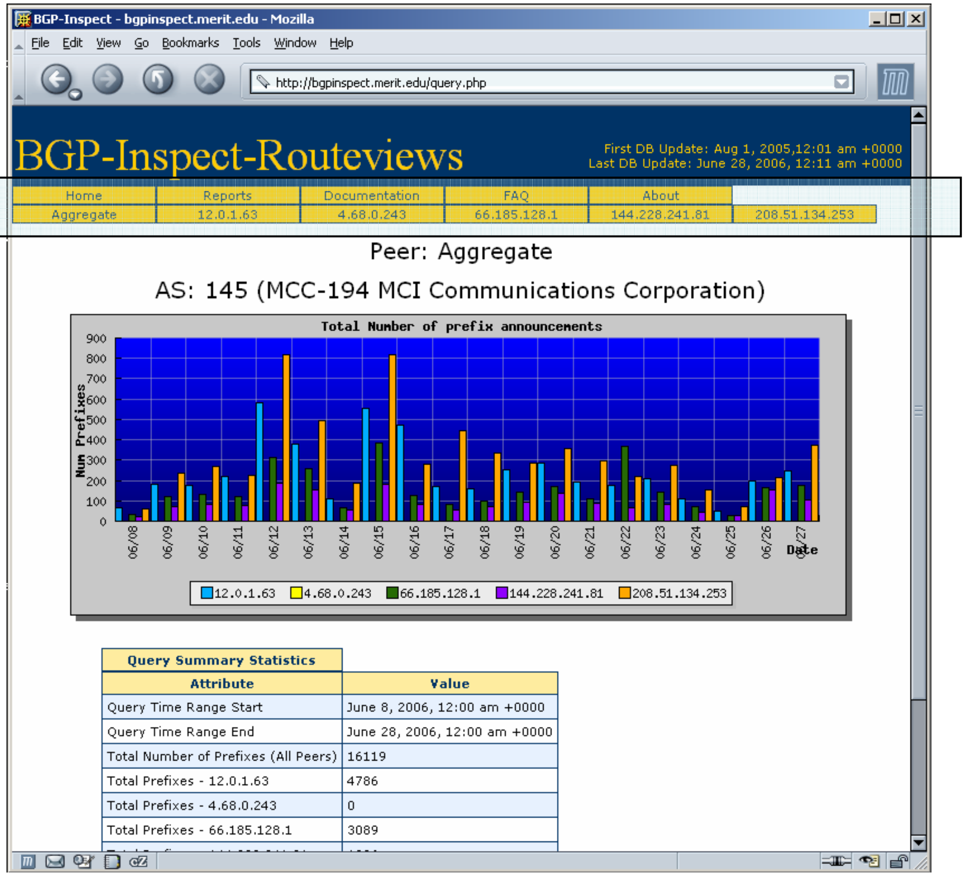


Top 20 Most Active ASes

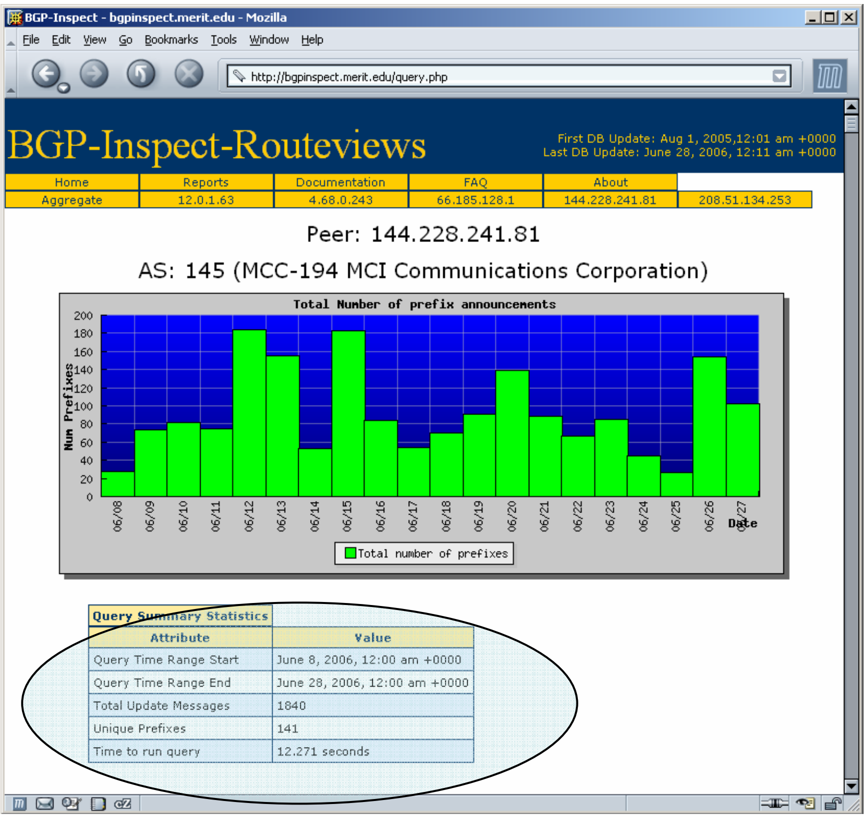
Rank	AS Number	AS Name	Announcements
1	5075	ATTBMG AT&T BMGS	44325
2	14169	MEADCO-1 MEAD CORPORATION	31132
3	25543	FASONET-AS ONATEL/FasoNet's Autonomous System	18259
4	4134	CHINANET-BACKBONE No.31,Jin-rong Street	17781
5	17974	TELKOMNET-AS2-AP PT TELEKOMUNIKASI INDONESIA	14822
6	7018	ATTW AT&T WorldNet Services	12779
7	5803	DNIC DoD Network Information Center	11682
8	17557	PKTELECOM-AS-AP Pakistan Telecom	11063
9	9443	INTERNETPRIMUS-AS-AP Primus Telecommunications	8652
10	3475	DEPART-52 Department of the Navy	8380
11	17451	BIZNET-AS-AP BIZNET ISP	7854
12	8452	TEDATA TEDATA	6869
13	23918	CBB-BGP-IBARAKI Connexion By Boeing Ibaraki AS	6234
14	174	COGENT Cogent/PSI	5847
15	6126	CAI-7 Computer Associates International	5590
16	19169	Telconet	5381
17	18231	EXATT-AS-AP Exatt Technologies Private Ltd.	5326
18	702	AS702 MCI EMEA - Commercial IP service provider in Europe	5239
19	11139	CWD-18 Cable & Wireless Dominica	4604
20	31200	NTK Novotelecom ltd.	4549

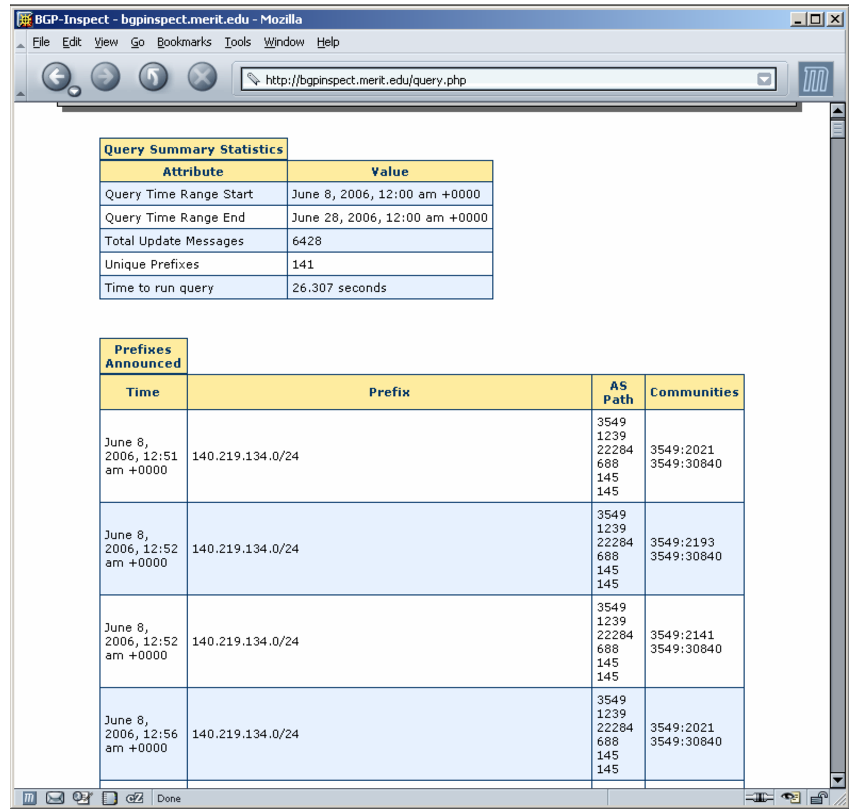
Raw Data Analysis – AS Query



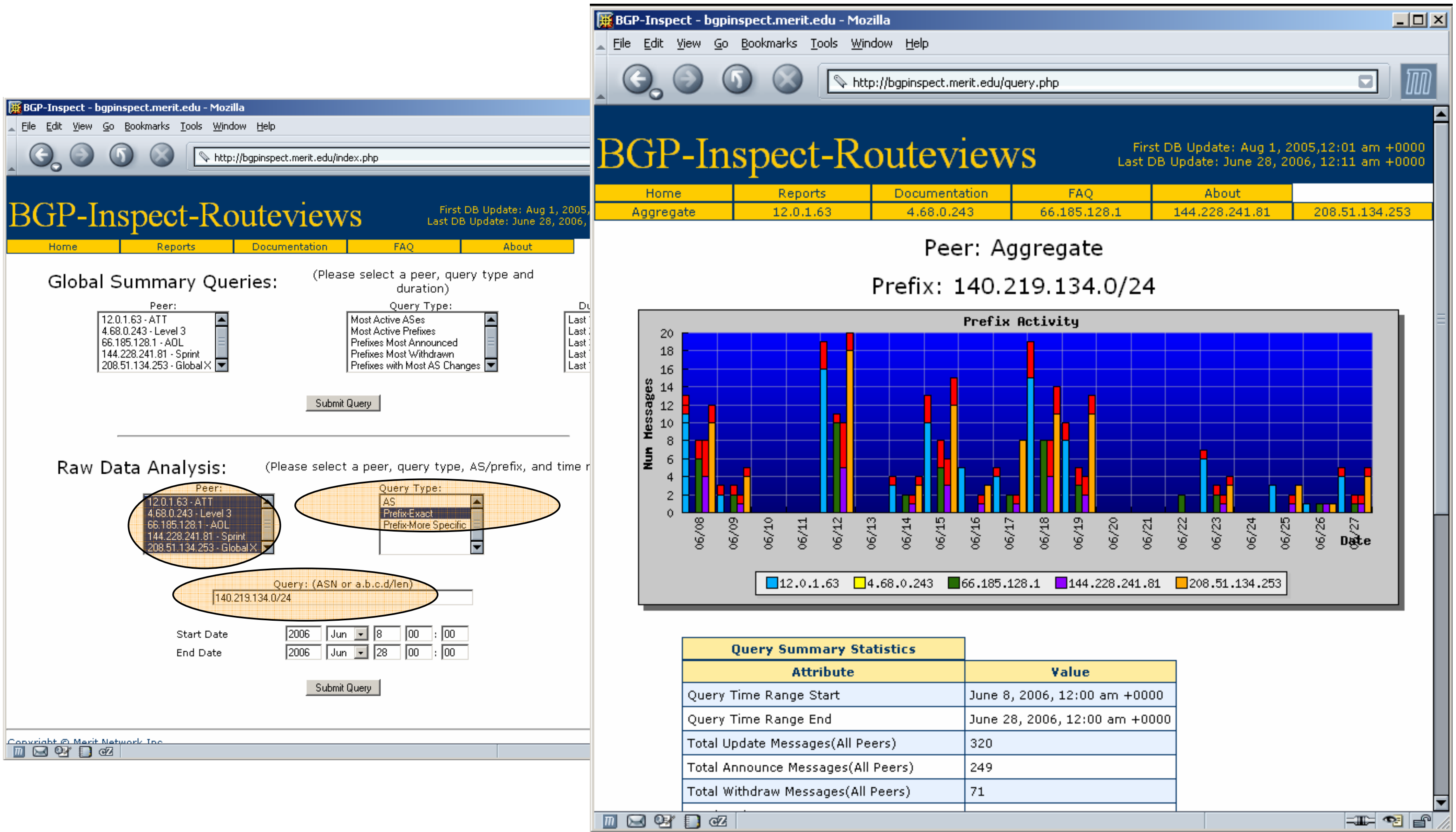


Raw Data Analysis – AS Query

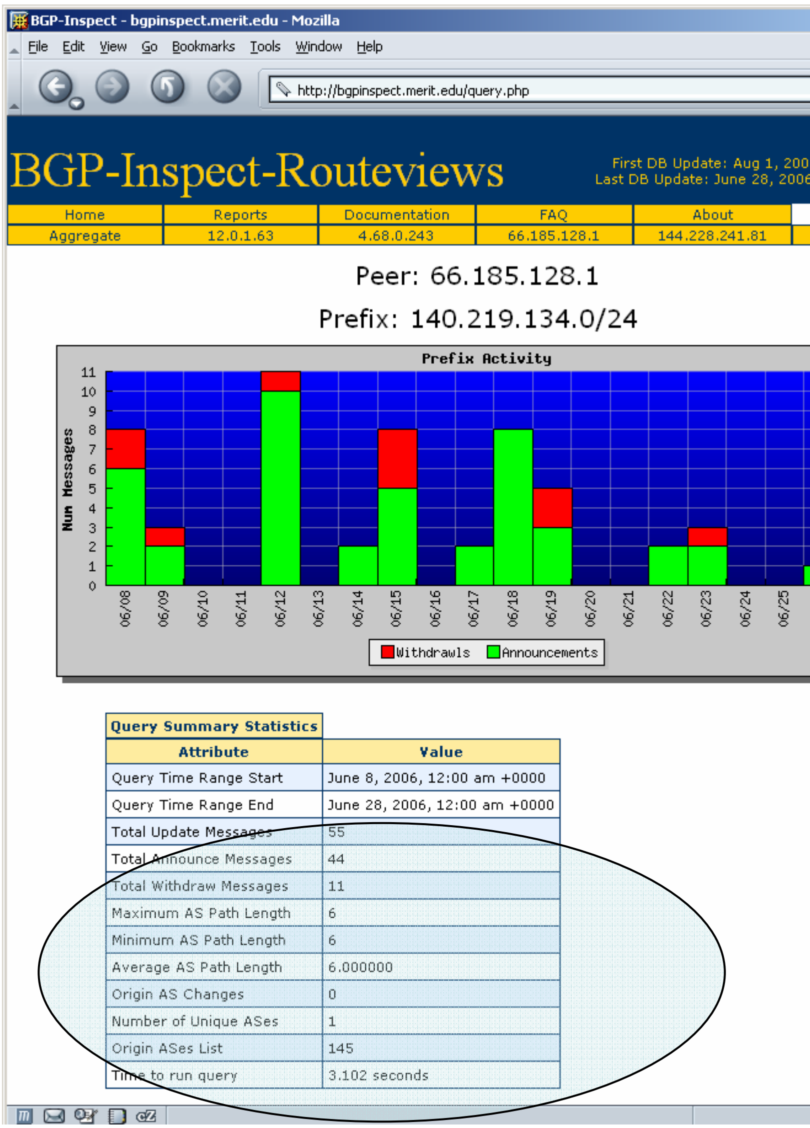




Raw Data Analysis – Prefix query

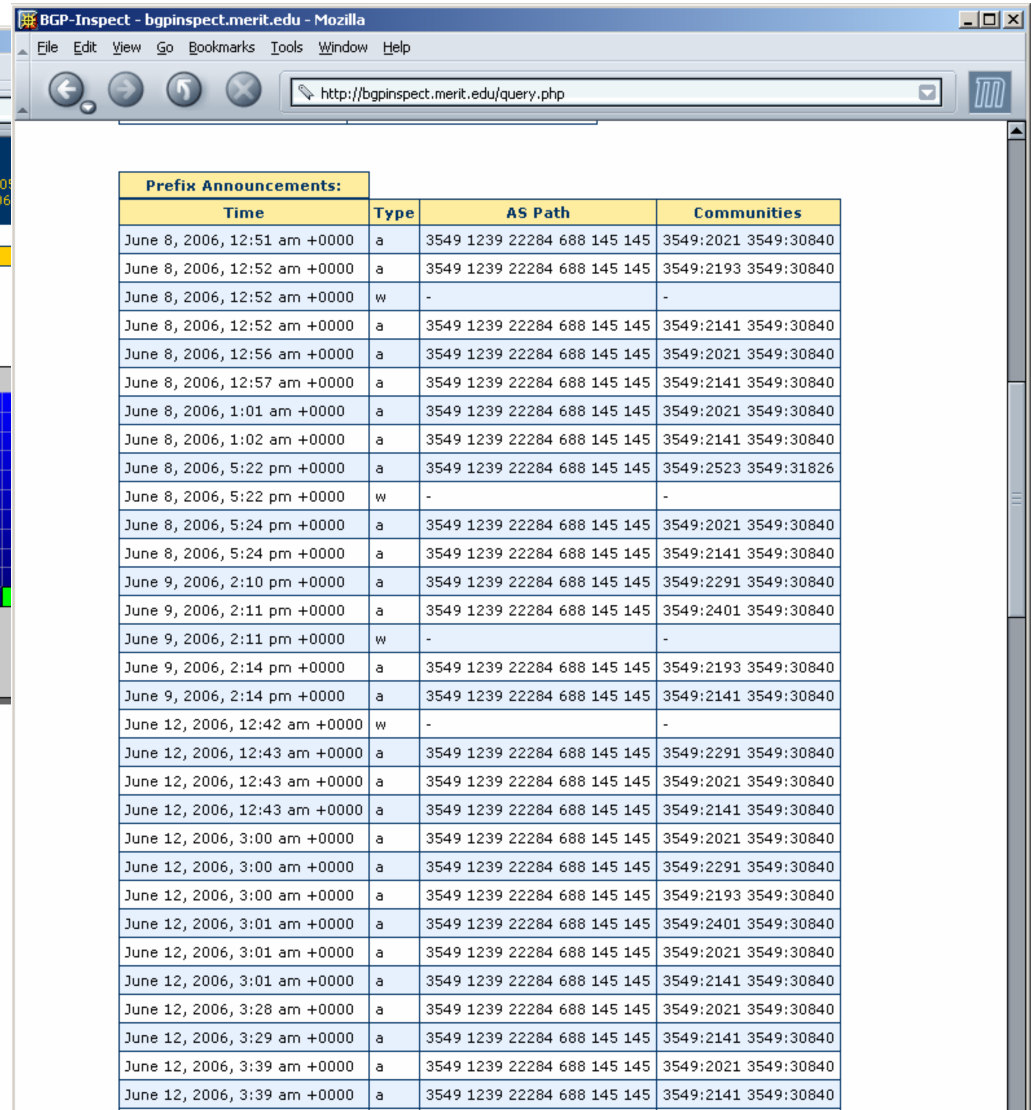


Raw Data Analysis – Prefix query



Query Summary Statistics

Attribute	Value
Query Time Range Start	June 8, 2006, 12:00 am +0000
Query Time Range End	June 28, 2006, 12:00 am +0000
Total Update Messages	55
Total Announce Messages	44
Total Withdraw Messages	11
Maximum AS Path Length	6
Minimum AS Path Length	6
Average AS Path Length	6.000000
Origin AS Changes	0
Number of Unique ASes	1
Origin ASes List	145
Time to run query	3.102 seconds



Prefix Announcements:

Time	Type	AS Path	Communities
June 8, 2006, 12:51 am +0000	a	3549 1239 22284 688 145 145	3549:2021 3549:30840
June 8, 2006, 12:52 am +0000	a	3549 1239 22284 688 145 145	3549:2193 3549:30840
June 8, 2006, 12:52 am +0000	w	-	-
June 8, 2006, 12:52 am +0000	a	3549 1239 22284 688 145 145	3549:2141 3549:30840
June 8, 2006, 12:56 am +0000	a	3549 1239 22284 688 145 145	3549:2021 3549:30840
June 8, 2006, 12:57 am +0000	a	3549 1239 22284 688 145 145	3549:2141 3549:30840
June 8, 2006, 1:01 am +0000	a	3549 1239 22284 688 145 145	3549:2021 3549:30840
June 8, 2006, 1:02 am +0000	a	3549 1239 22284 688 145 145	3549:2141 3549:30840
June 8, 2006, 5:22 pm +0000	a	3549 1239 22284 688 145 145	3549:2523 3549:31826
June 8, 2006, 5:22 pm +0000	w	-	-
June 8, 2006, 5:24 pm +0000	a	3549 1239 22284 688 145 145	3549:2021 3549:30840
June 8, 2006, 5:24 pm +0000	a	3549 1239 22284 688 145 145	3549:2141 3549:30840
June 9, 2006, 2:10 pm +0000	a	3549 1239 22284 688 145 145	3549:2291 3549:30840
June 9, 2006, 2:11 pm +0000	a	3549 1239 22284 688 145 145	3549:2401 3549:30840
June 9, 2006, 2:11 pm +0000	w	-	-
June 9, 2006, 2:14 pm +0000	a	3549 1239 22284 688 145 145	3549:2193 3549:30840
June 9, 2006, 2:14 pm +0000	a	3549 1239 22284 688 145 145	3549:2141 3549:30840
June 12, 2006, 12:42 am +0000	w	-	-
June 12, 2006, 12:43 am +0000	a	3549 1239 22284 688 145 145	3549:2291 3549:30840
June 12, 2006, 12:43 am +0000	a	3549 1239 22284 688 145 145	3549:2021 3549:30840
June 12, 2006, 12:43 am +0000	a	3549 1239 22284 688 145 145	3549:2141 3549:30840
June 12, 2006, 3:00 am +0000	a	3549 1239 22284 688 145 145	3549:2021 3549:30840
June 12, 2006, 3:00 am +0000	a	3549 1239 22284 688 145 145	3549:2291 3549:30840
June 12, 2006, 3:00 am +0000	a	3549 1239 22284 688 145 145	3549:2193 3549:30840
June 12, 2006, 3:01 am +0000	a	3549 1239 22284 688 145 145	3549:2401 3549:30840
June 12, 2006, 3:01 am +0000	a	3549 1239 22284 688 145 145	3549:2021 3549:30840
June 12, 2006, 3:01 am +0000	a	3549 1239 22284 688 145 145	3549:2141 3549:30840
June 12, 2006, 3:28 am +0000	a	3549 1239 22284 688 145 145	3549:2021 3549:30840
June 12, 2006, 3:29 am +0000	a	3549 1239 22284 688 145 145	3549:2141 3549:30840
June 12, 2006, 3:39 am +0000	a	3549 1239 22284 688 145 145	3549:2021 3549:30840
June 12, 2006, 3:39 am +0000	a	3549 1239 22284 688 145 145	3549:2141 3549:30840

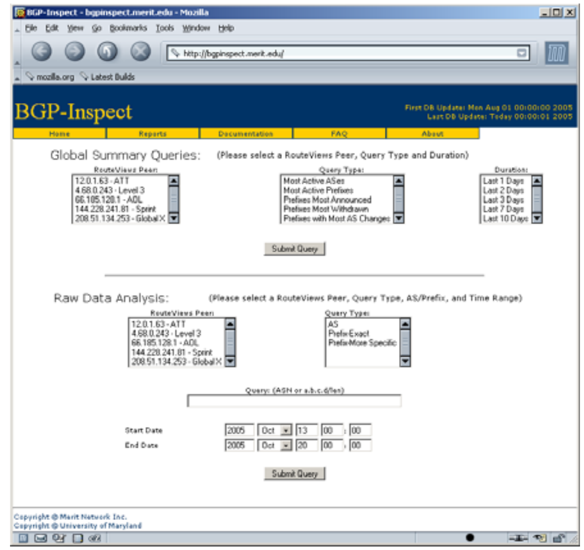
BGP-Inspect: Current State

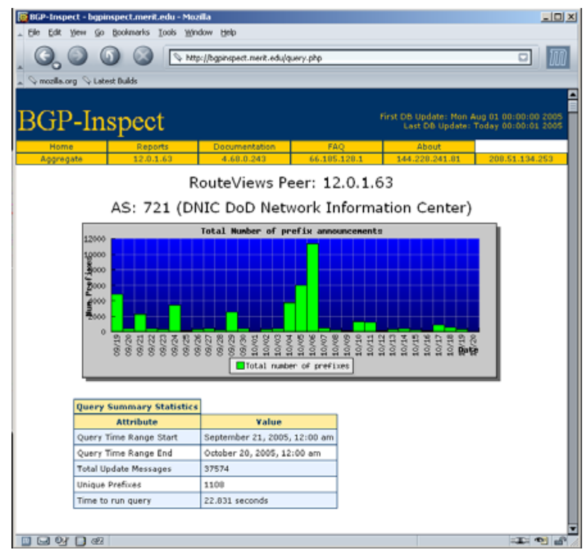
BGP-Inspect – Beta v0.5
http://bgpinspect.merit.edu

Dataset: August 1, 2005 - Present
Current BGPdb size: 170GB
Currently indexing data for 5 peers (AT&T, Level 3, AOL, Sprint, Global X)

- Example queries (per peer, 1,7,10 days):
  - Most active AS's
  - Most active prefixes
  - Prefixes with most OriginAS changes

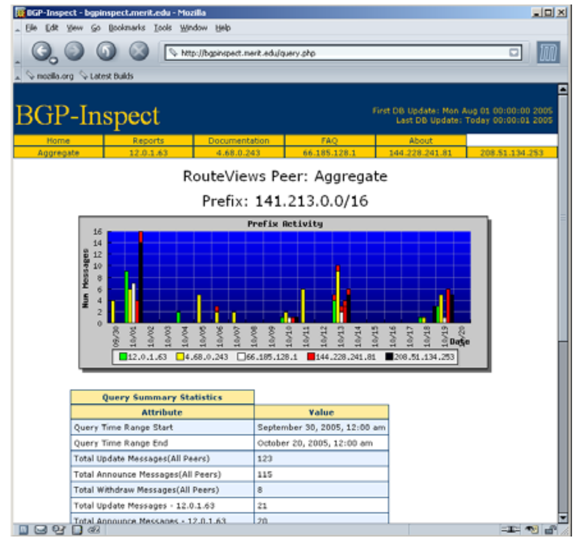
- Raw Data Analysis(per peer)
  - Prefix/AS, Time Range
  - Uniques prefixes by AS
  - OriginAS changes for a prefix
  - Time to run query
  - More specific prefixes announced

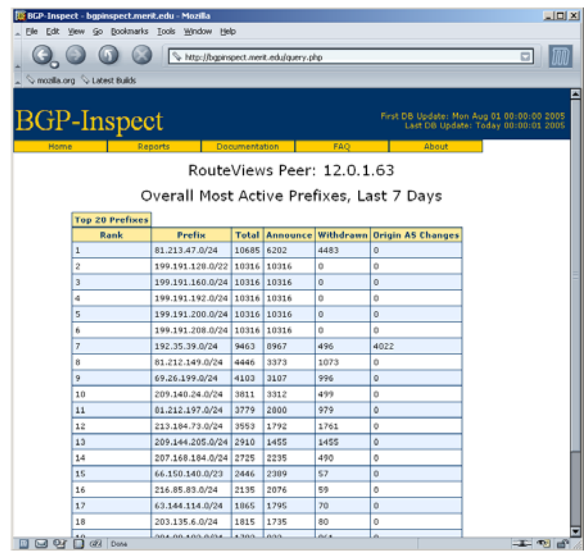




BGP-Inpsect: Current State (2)

- Equipment
  - Dell 2650 - Web and DB server
  - Dell 2850, dual Xeon with NFS mounted 500GB SATA
- Traffic?
  - ~30+ unique IPs per day





BGP-Inspect Next Steps

- BGP-Inspect is available at http://bgpinspect.merit.edu and your feedback is very much appreciated.

- Future…
  - More interesting things with the multiple peer response UI (different ways of highlighting the differences between peers)
  - pyBGPdb - a python interface to the BGPdb database providing fast raw queries

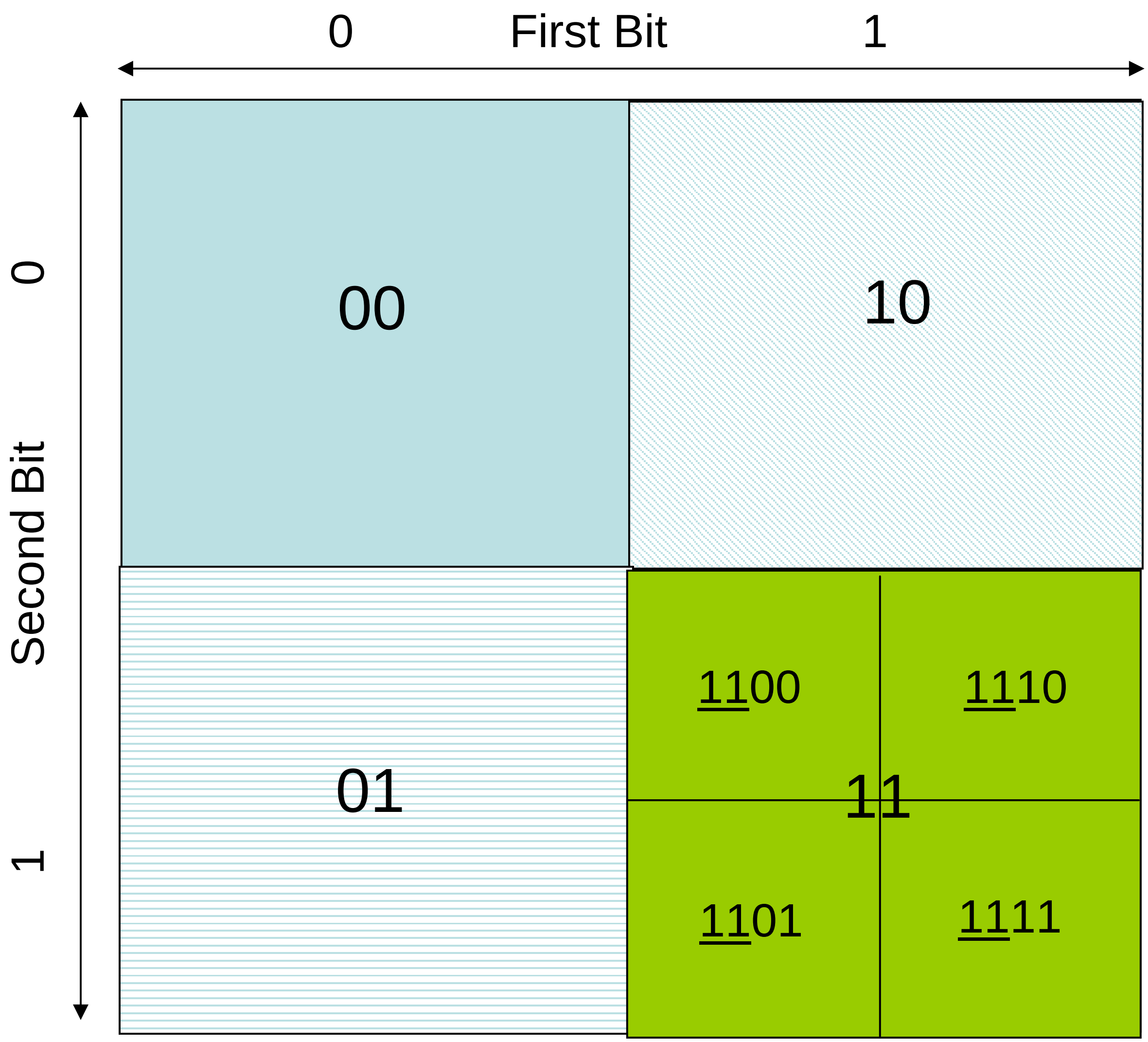
Outline

- The Problem
- BGP/Routing Information
  - BGP-Inspect – Information Extraction from BGP Update messages
  - VAST – Internet AS topology Visualization
- Netflow/Traffic Information
  - Flamingo – Internet Traffic Exploration
- Conclusions

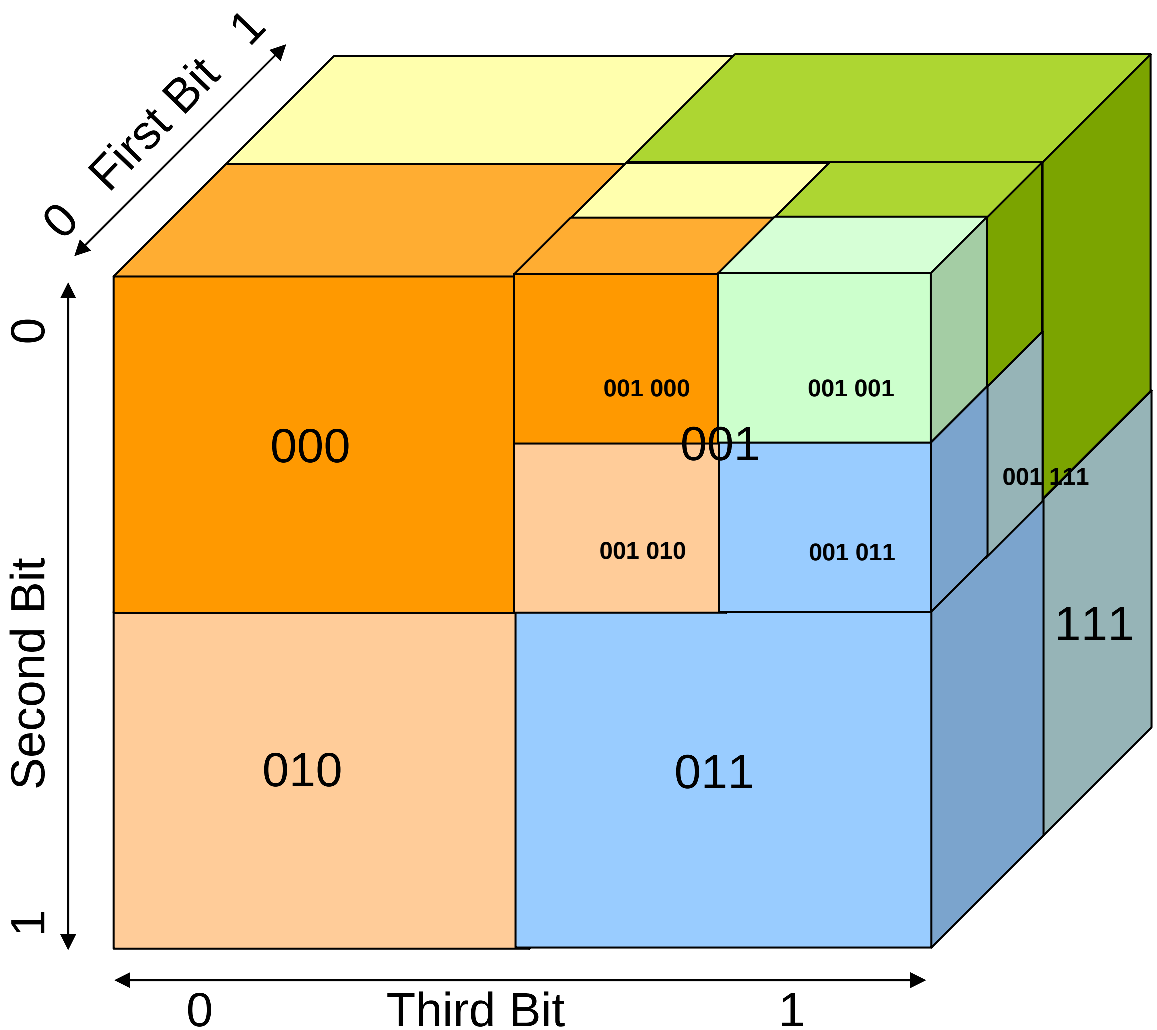
VAST – Visualizing AS Topology

- VAST allows users to easily navigate, and explore various topological properties and features extracted from raw BGP update messages
- VAST uses both a quad-tree based algorithm as well as an octo-tree based method to build various visualization
- The ability to navigate the three dimensional space to fully explore the dataset make VAST a unique tool

The Basic Quad-Tree



Octo-Tree Algorithm



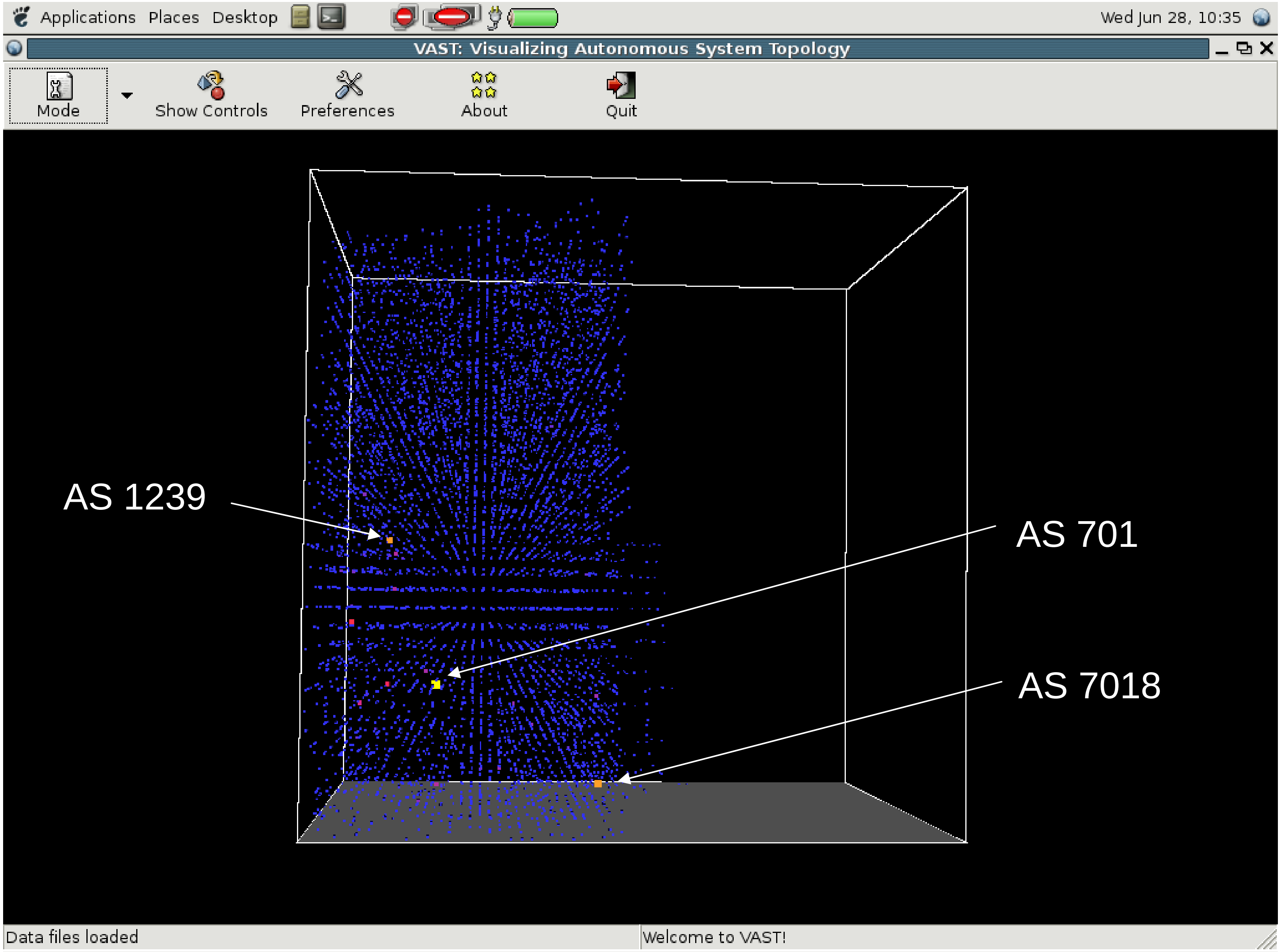
VAST - Visualization Methods

- Out-degree per AS
- Per AS unique prefix originations
- AS topology with line scaling:
  - Peer out-degree
  - Frequency with which AS pair is seen
  - Unique prefixes with certain AS pair
  - Total address space over an AS pair

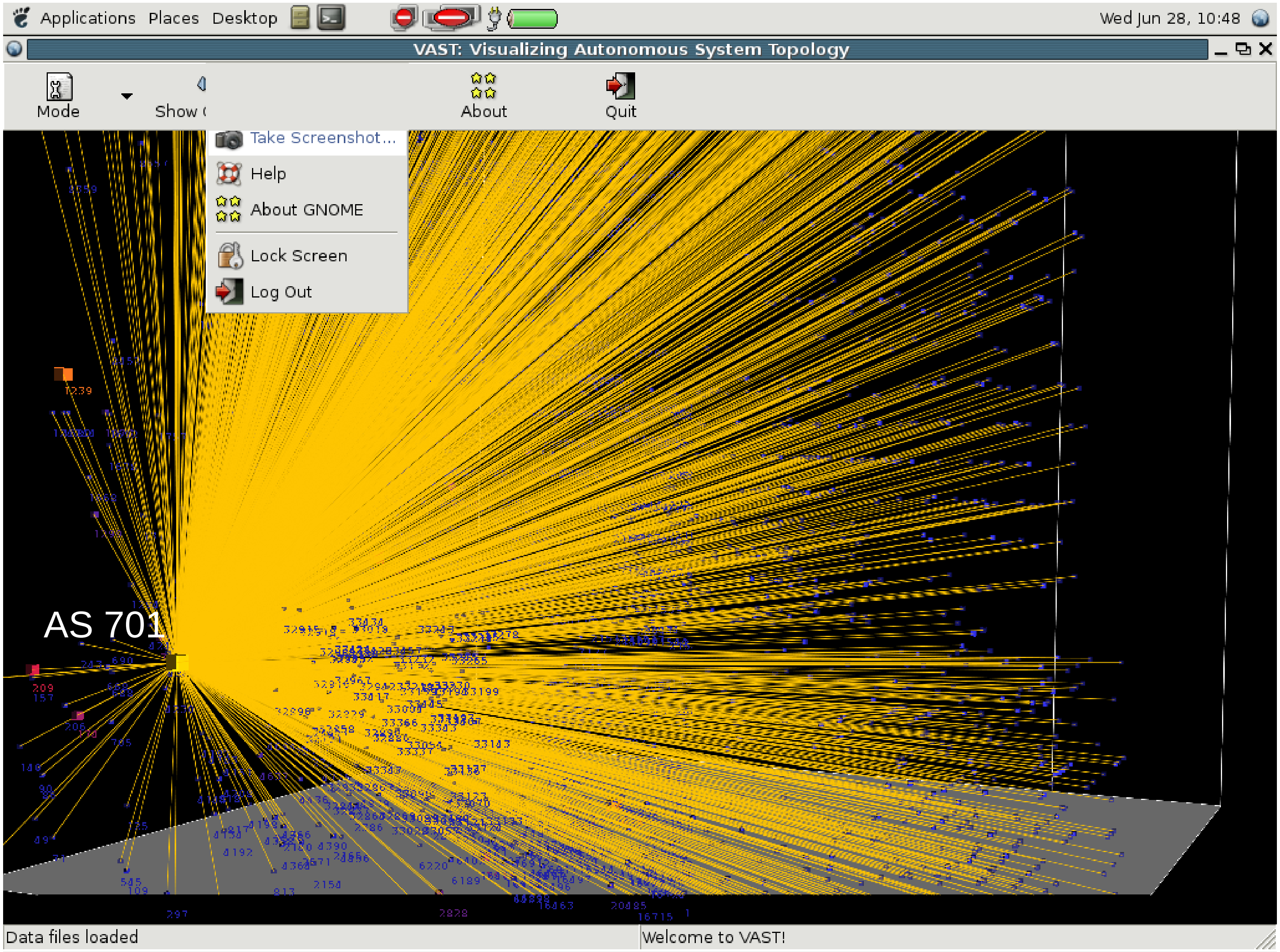
VAST – Techniques

- Position of a node determined by quad/octo-tree
- Size determined by out-degree of node, larger out-degree -> larger size
- Color determined by out-degree of node, larger out-degree -> more yellow
- Line thickness depends on various factors(selectable), out-degree of neighbor, number of prefixes, address space size, or frequency of messages
- 3D navigation of visualization, slider bar controls, selectable listing of displayed information to control/filter what is being displayed

VAST – ASN Distribution

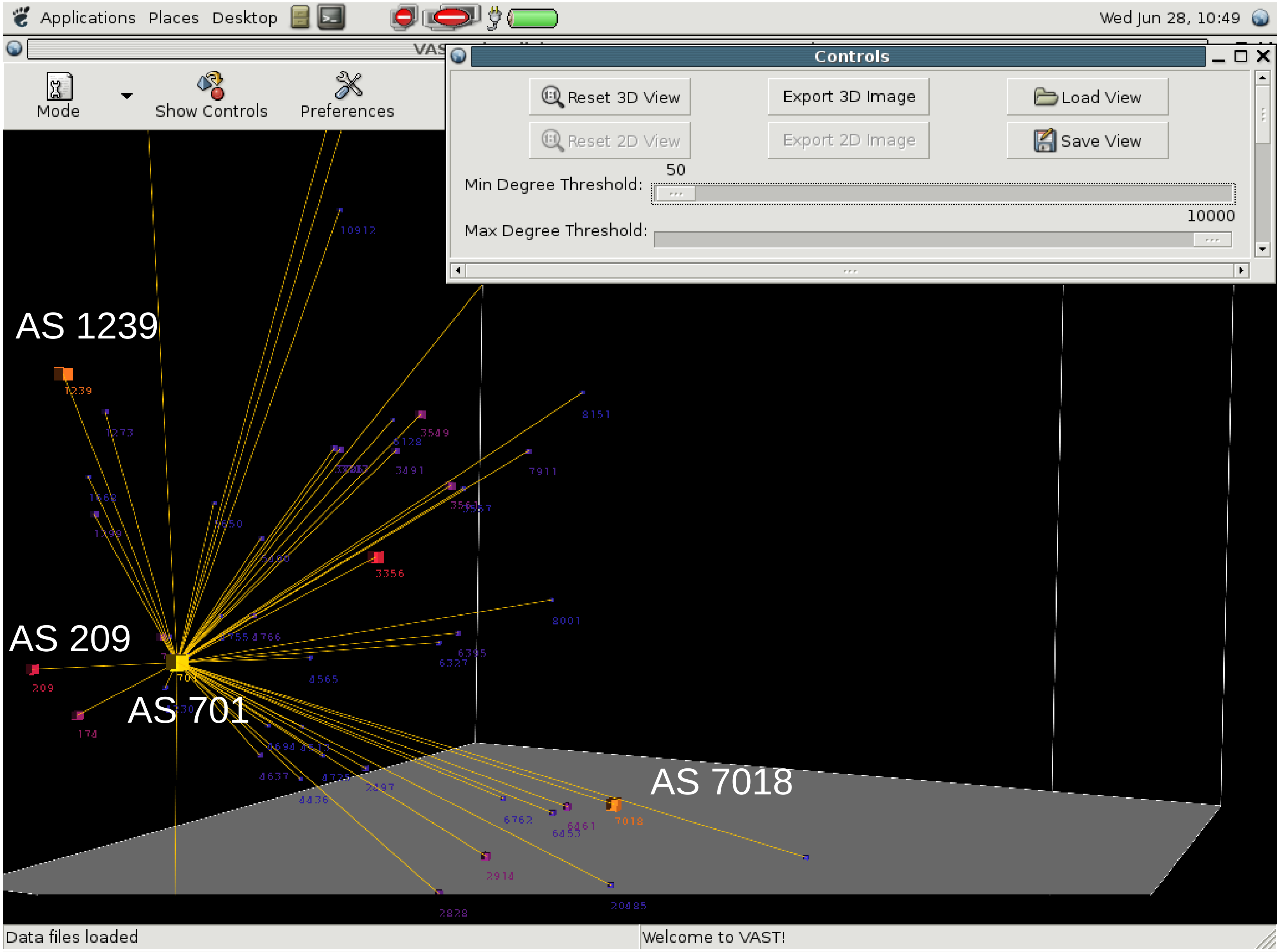


VAST - AS CORE



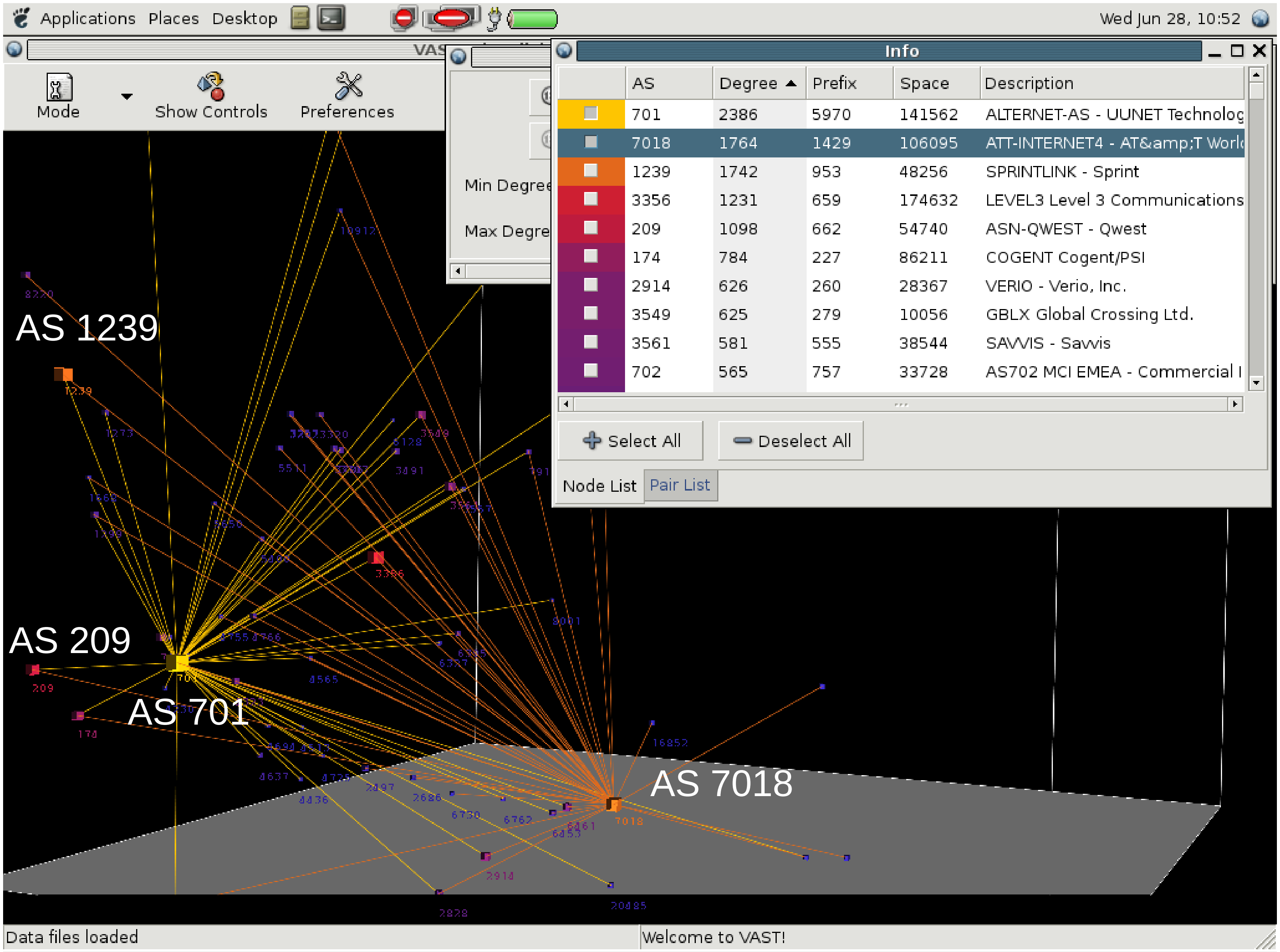
Applications Places Desktop
Wed Jun 28, 10:48
VAST: Visualizing Autonomous System Topology
Mode
Show
About
Quit
Take Screenshot...
Help
About GNOME
Lock Screen
Log Out
AS 701
Data files loaded
Welcome to VAST!

VAST – AS CORE



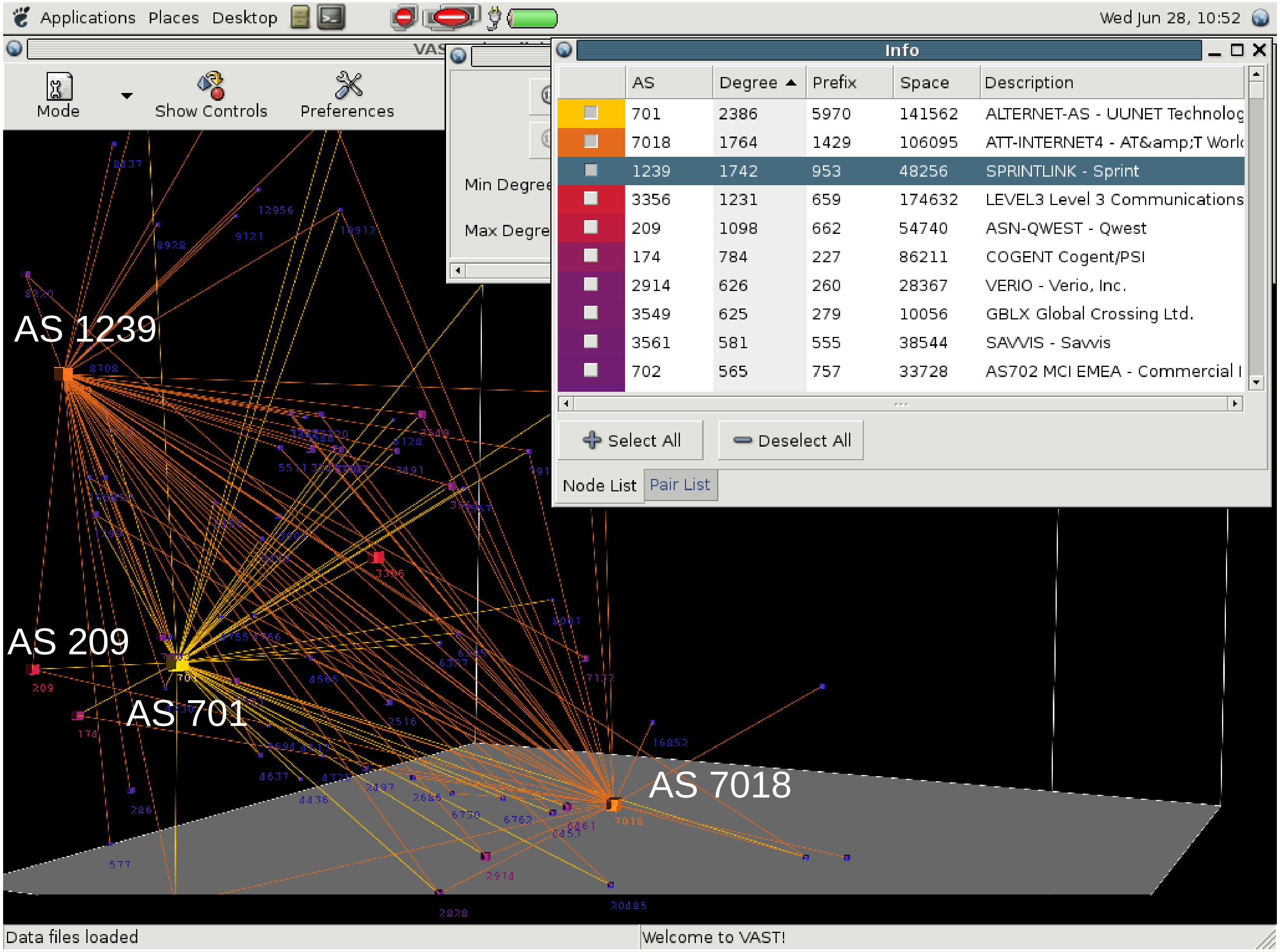
Applications Places Desktop
Wed Jun 28, 10:49
Mode
Show Controls
Preferences
Controls
Reset 3D View
Export 3D Image
Load View
Reset 2D View
Export 2D Image
Save View
Min Degree Threshold:
50
Max Degree Threshold:
10000
AS 1239
AS 209
AS 701
AS 7018
Data files loaded
Welcome to VAST!

VAST – AS CORE



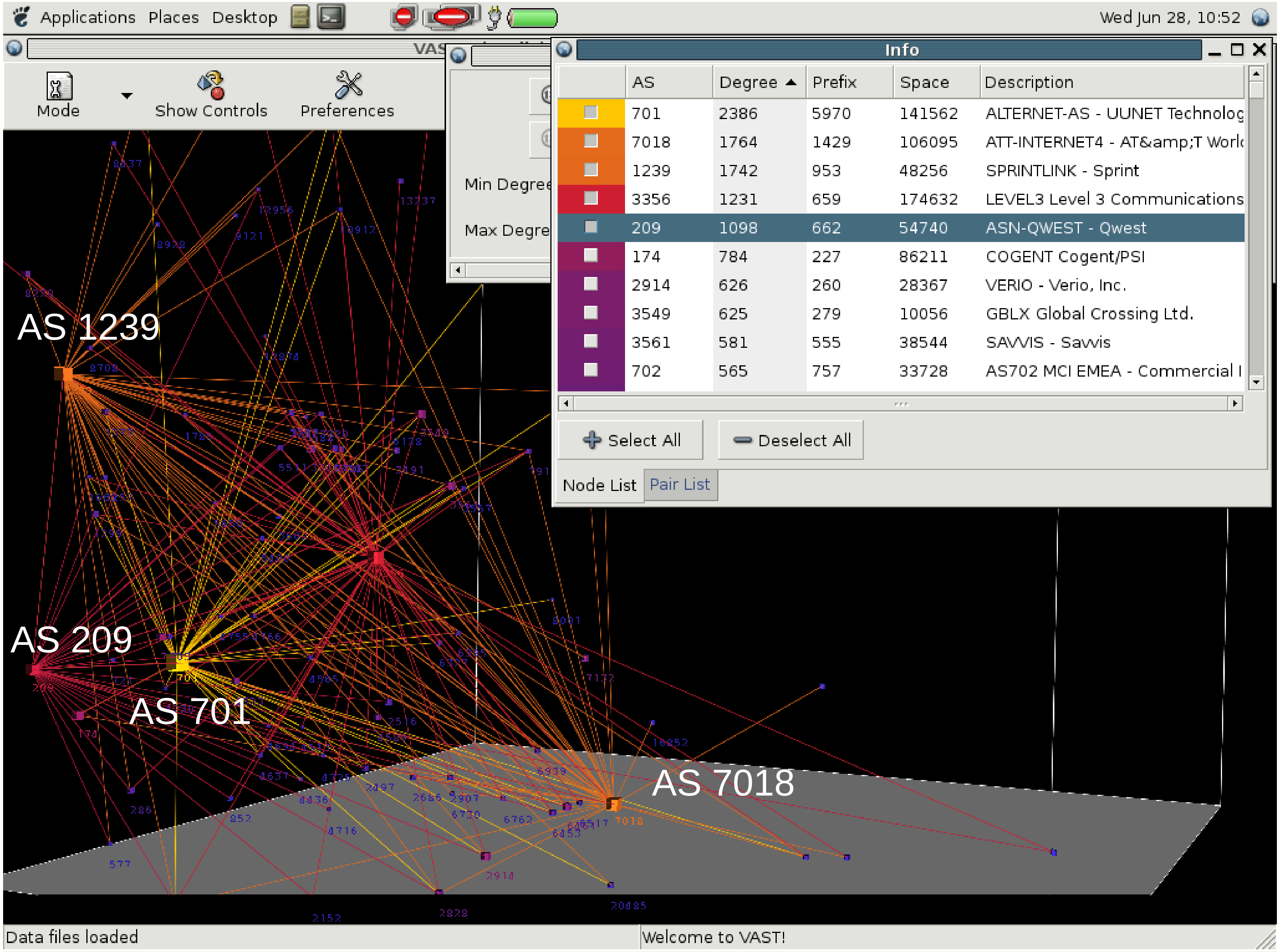
Applications Places Desktop
Wed Jun 28, 10:52
Mode
Show Controls
Preferences
Min Degree
Max Degre
Info
AS | Degree | Prefix | Space | Description
701 | 2386 | 5970 | 141562 | ALTERNET-AS - UUNET Technolog
7018 | 1764 | 1429 | 106095 | ATT-INTERNET4 - AT&T Worl
1239 | 1742 | 953 | 48256 | SPRINTLINK - Sprint
3356 | 1231 | 659 | 174632 | LEVEL3 Level 3 Communications
209 | 1098 | 662 | 54740 | ASN-QWEST - Qwest
174 | 784 | 227 | 86211 | COGENT Cogent/PSI
2914 | 626 | 260 | 28367 | VERIO - Verio, Inc.
3549 | 625 | 279 | 10056 | GBLX Global Crossing Ltd.
3561 | 581 | 555 | 38544 | SAVVIS - Savvis
702 | 565 | 757 | 33728 | AS702 MCI EMEA - Commercial I
Select All
Deselect All
Node List
Pair List
AS 1239
AS 209
AS 701
AS 7018
Data files loaded
Welcome to VAST!

VAST – AS CORE



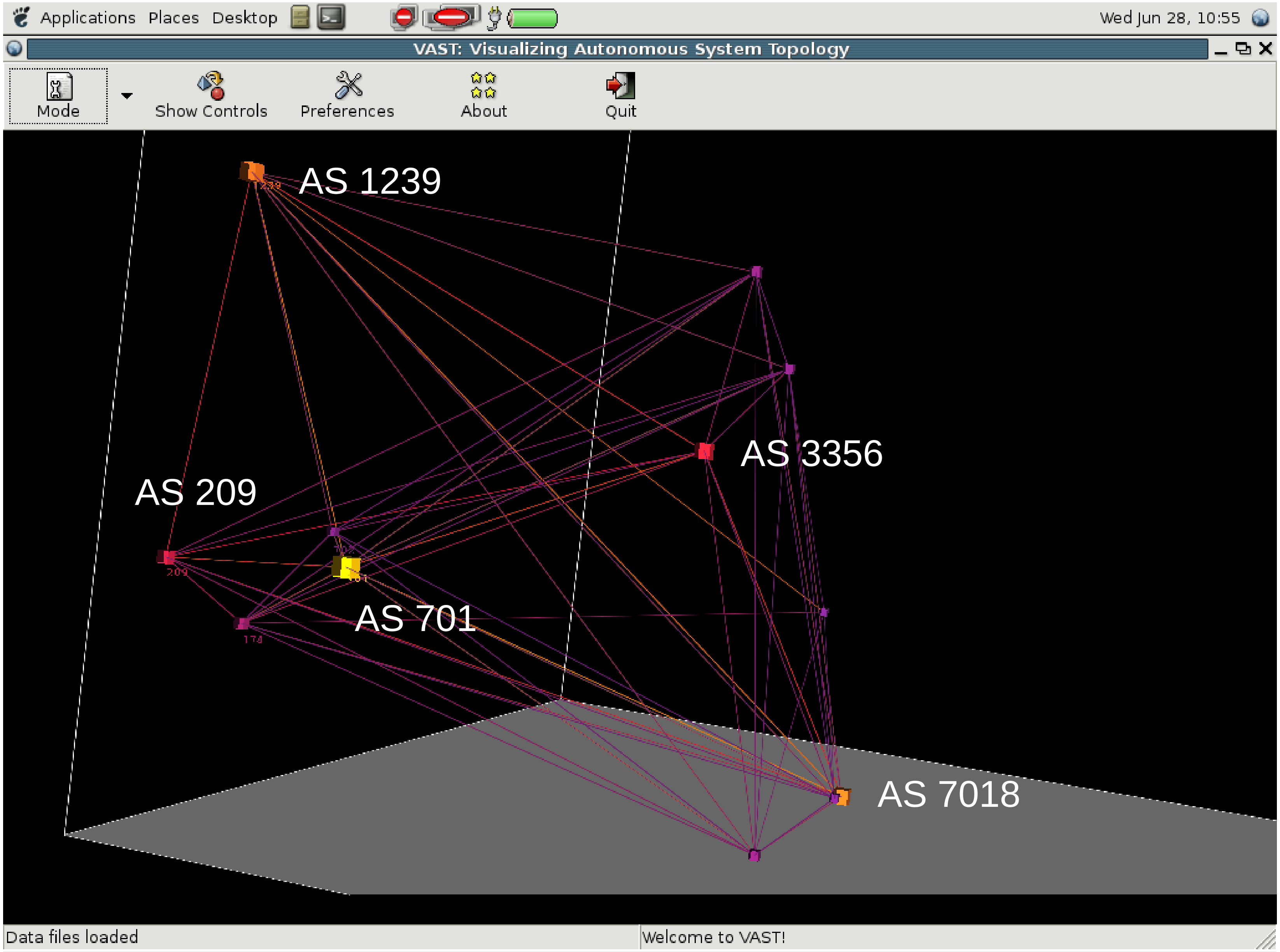
Applications Places Desktop
Wed Jun 28, 10:52
Mode
Show Controls
Preferences
Min Degree
Max Degre
Info
AS | Degree | Prefix | Space | Description
701 | 2386 | 5970 | 141562 | ALTERNET-AS - UUNET Technolog
7018 | 1764 | 1429 | 106095 | ATT-INTERNET4 - AT&T Worl
1239 | 1742 | 953 | 48256 | SPRINTLINK - Sprint
3356 | 1231 | 659 | 174632 | LEVEL3 Level 3 Communications
209 | 1098 | 662 | 54740 | ASN-QWEST - Qwest
174 | 784 | 227 | 86211 | COGENT Cogent/PSI
2914 | 626 | 260 | 28367 | VERIO - Verio, Inc.
3549 | 625 | 279 | 10056 | GBLX Global Crossing Ltd.
3561 | 581 | 555 | 38544 | SAVVIS - Savvis
702 | 565 | 757 | 33728 | AS702 MCI EMEA - Commercial I
Select All
Deselect All
Node List
Pair List
AS 1239
AS 209
AS 701
AS 7018
Data files loaded
Welcome to VAST!

VAST – AS CORE

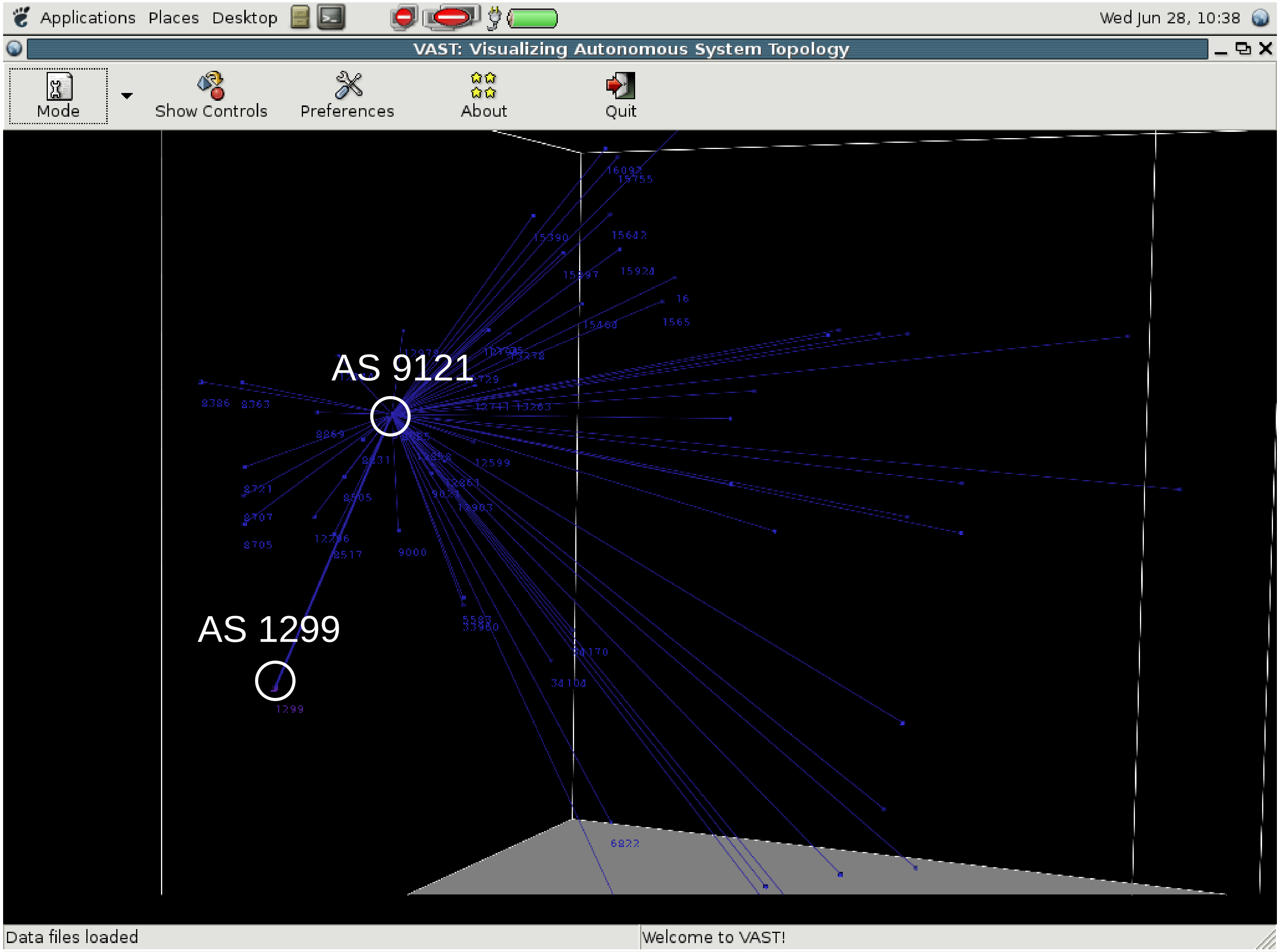


Applications Places Desktop
Wed Jun 28, 10:52
Mode
Show Controls
Preferences
Min Degree
Max Degre
Info
AS | Degree | Prefix | Space | Description
701 | 2386 | 5970 | 141562 | ALTERNET-AS - UUNET Technolog
7018 | 1764 | 1429 | 106095 | ATT-INTERNET4 - AT&T Worl
1239 | 1742 | 953 | 48256 | SPRINTLINK - Sprint
3356 | 1231 | 659 | 174632 | LEVEL3 Level 3 Communications
209 | 1098 | 662 | 54740 | ASN-QWEST - Qwest
174 | 784 | 227 | 86211 | COGENT Cogent/PSI
2914 | 626 | 260 | 28367 | VERIO - Verio, Inc.
3549 | 625 | 279 | 10056 | GBLX Global Crossing Ltd.
3561 | 581 | 555 | 38544 | SAVVIS - Savvis
702 | 565 | 757 | 33728 | AS702 MCI EMEA - Commercial I
Select All
Deselect All
Node List
Pair List
AS 1239
AS 209
AS 701
AS 7018
Data files loaded
Welcome to VAST!

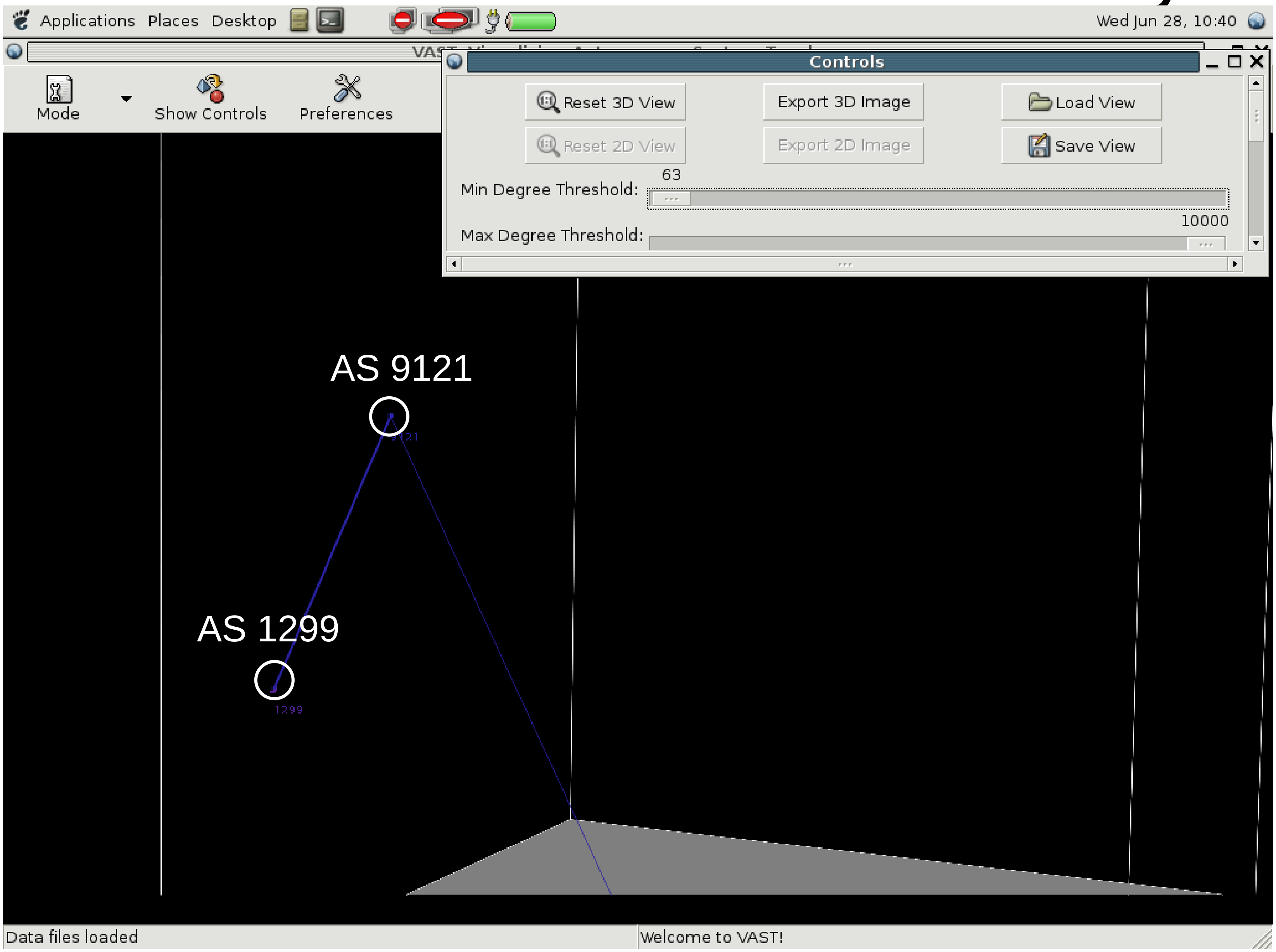
VAST – AS CORE(500 Club)



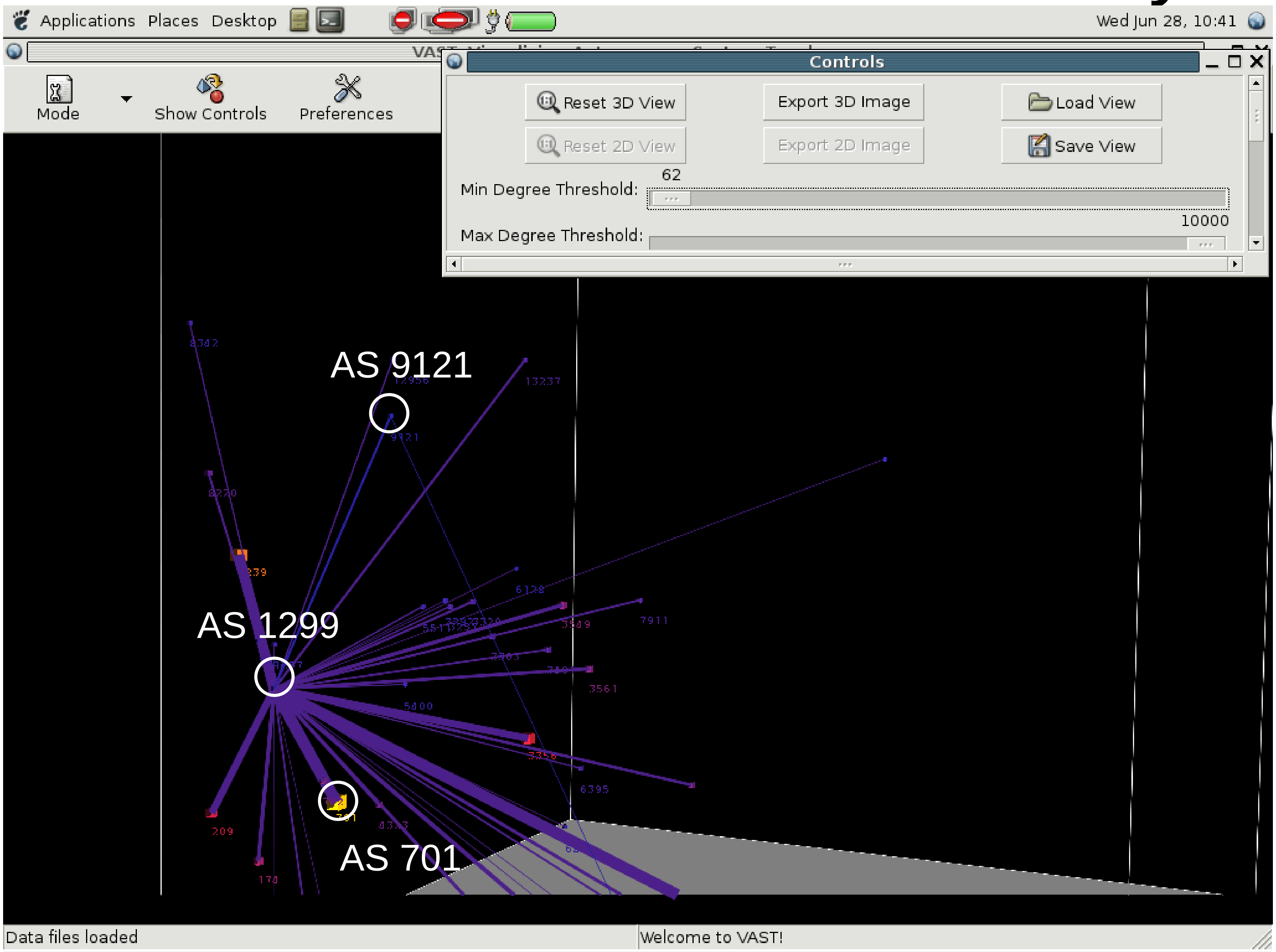
VAST – AS9121connectivity



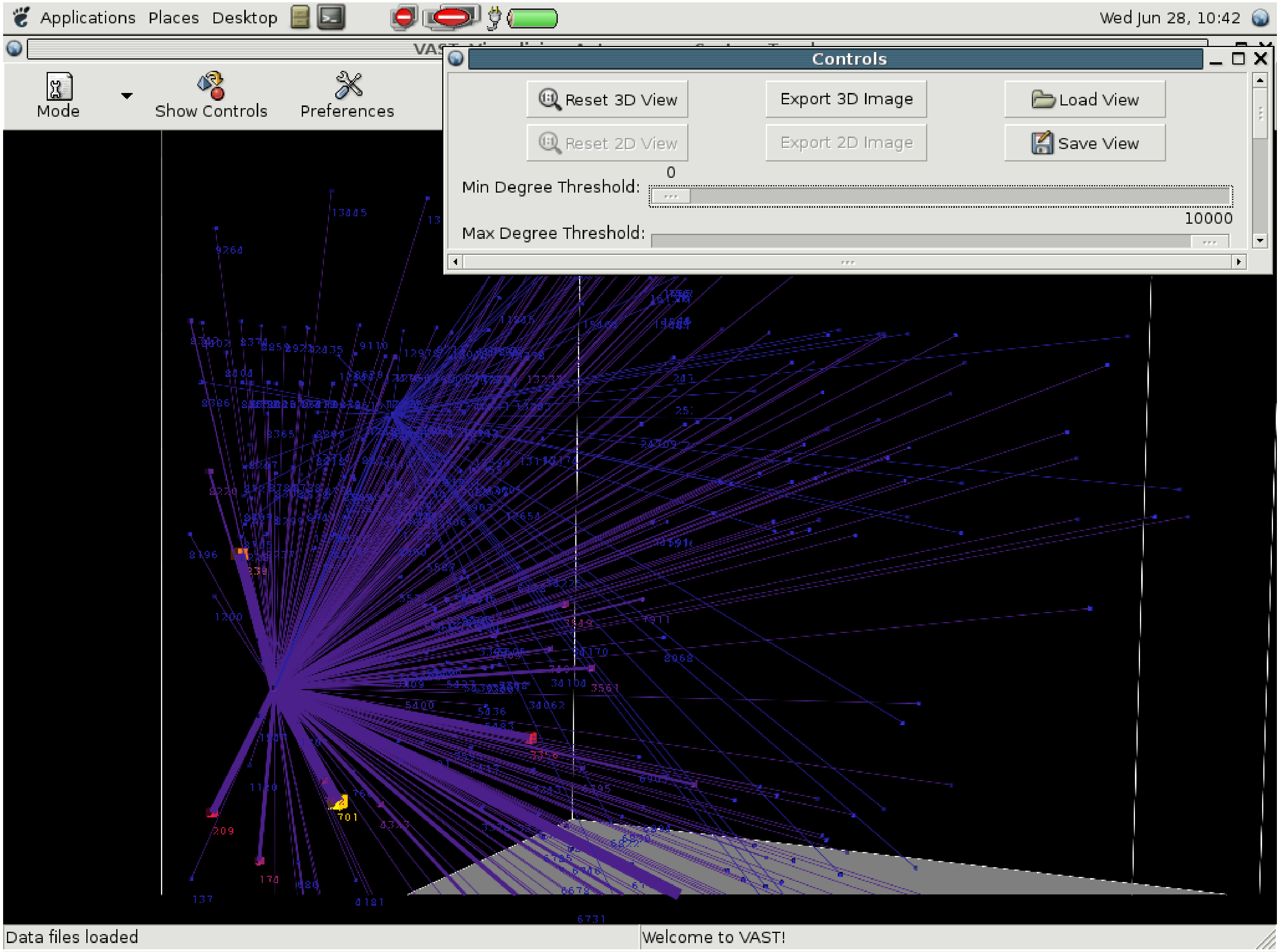
VAST – AS9121connectivity



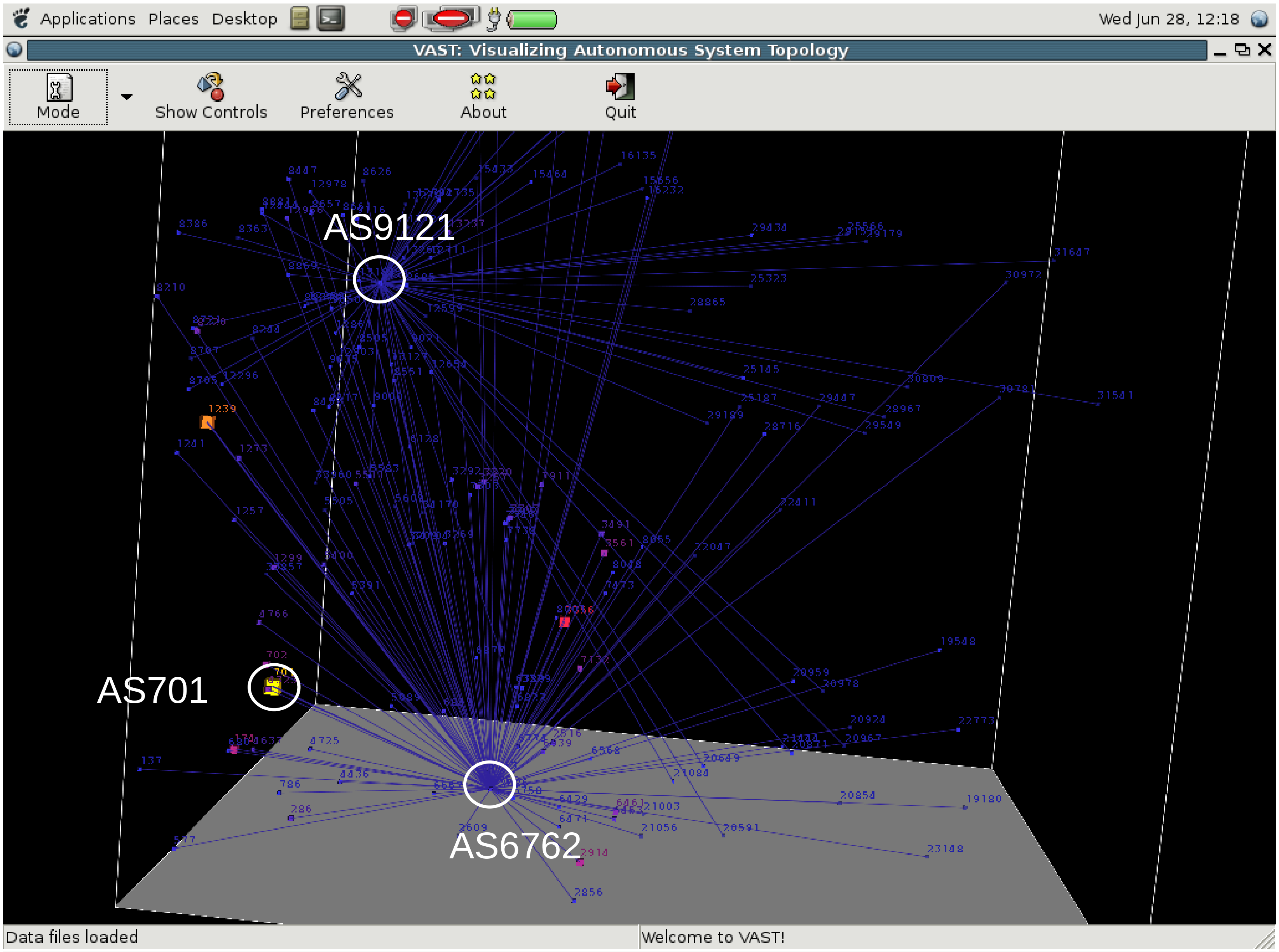
VAST – AS9121connectivity



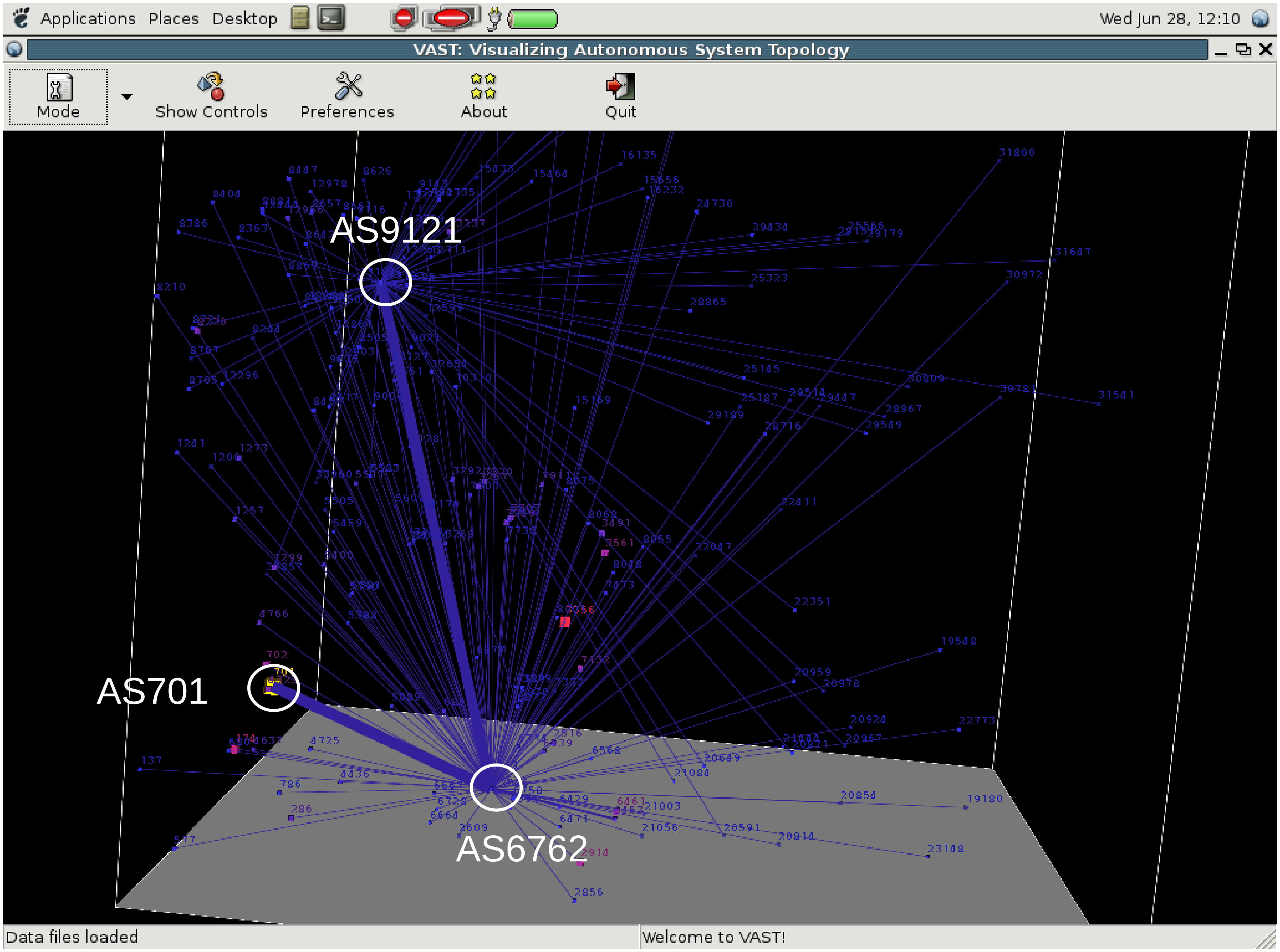
VAST – AS9121connectivity



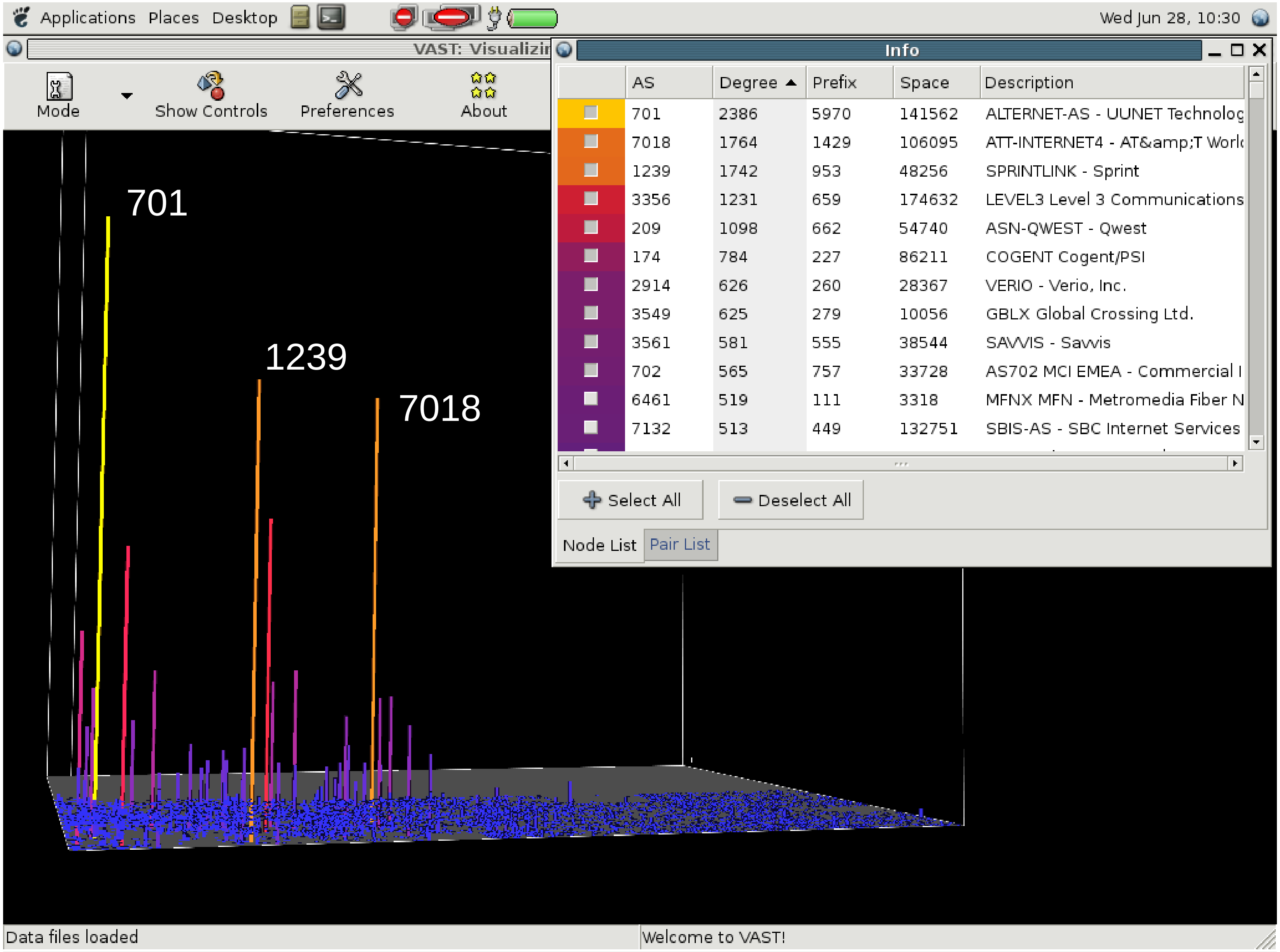
VAST – AS9121 Route Leakage



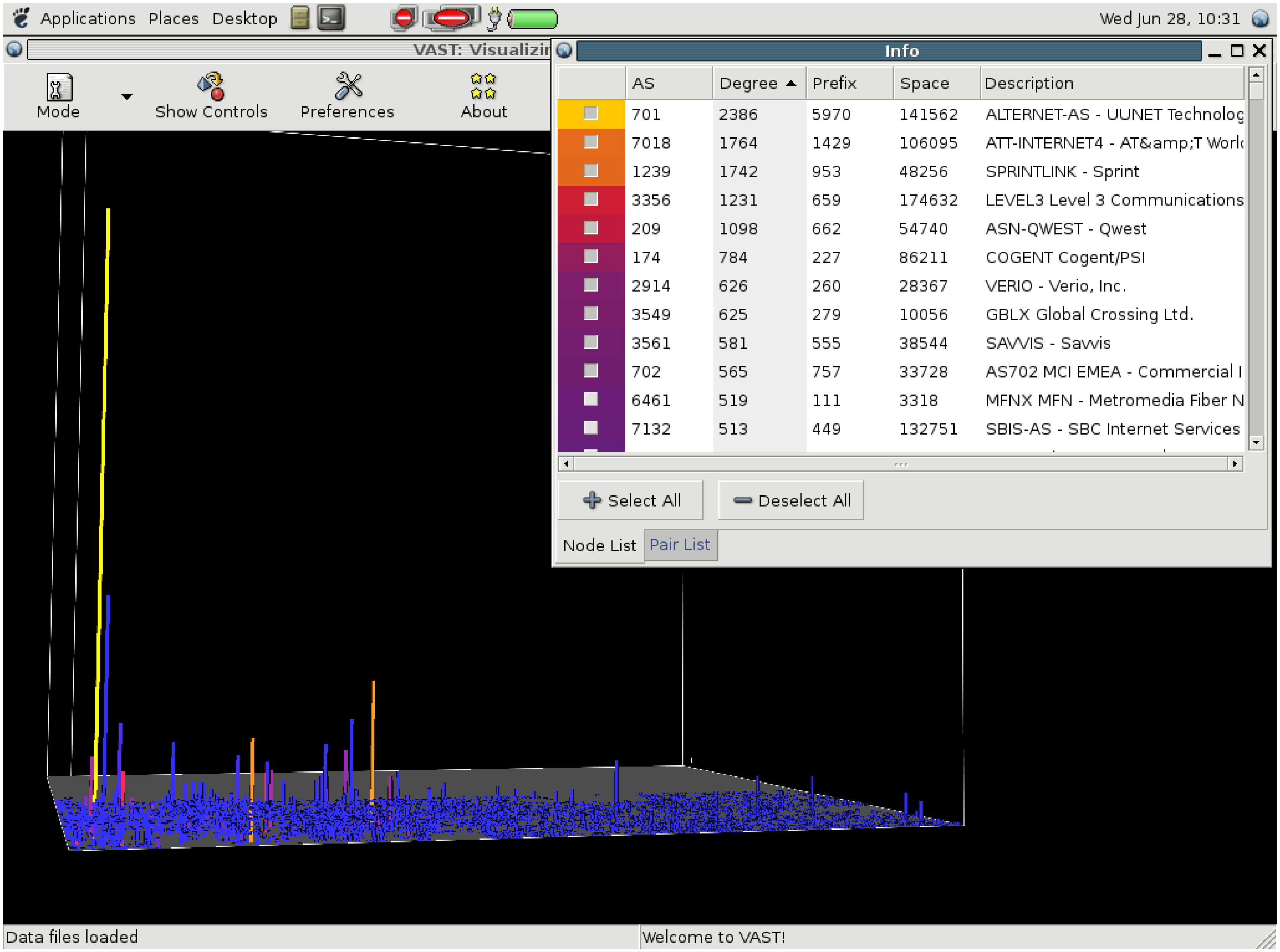
VAST – AS9121 Route Leakage



VAST – AS Out-degree



VAST – Unique Prefix



Outline

- The Problem
- BGP/Routing Information
  - BGP-Inspect – Information Extraction from BGP Update messages
  - VAST – Internet AS topology Visualization
- Netflow/Traffic Information
  - Flamingo – Internet Traffic Exploration
- Conclusions

Flamingo – Visualizing Internet Traffic Data

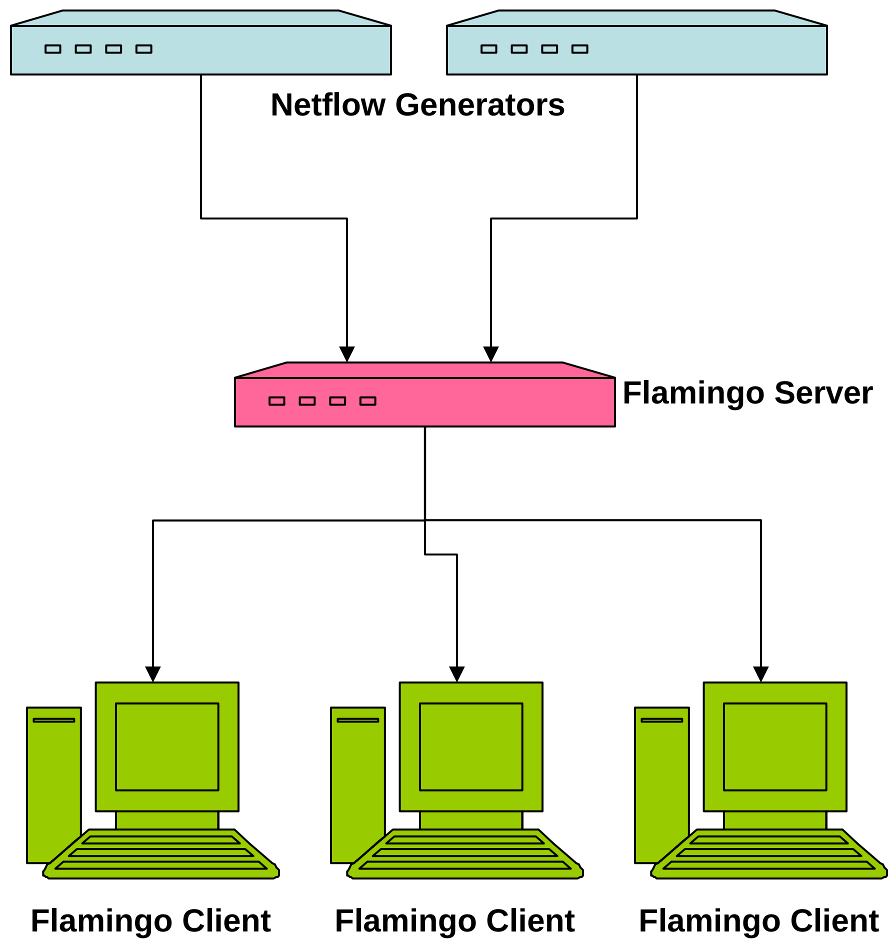
- Introduction: What is Flamingo
- Visualizations
- The Flamingo Tool
  - Combining visualization with controls
- Case Studies
  - Traffic Anomaly
  - Network Scans
  - Worm traffic
  - P2P traffic
  - The Slashdot effect!

Flamingo - 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

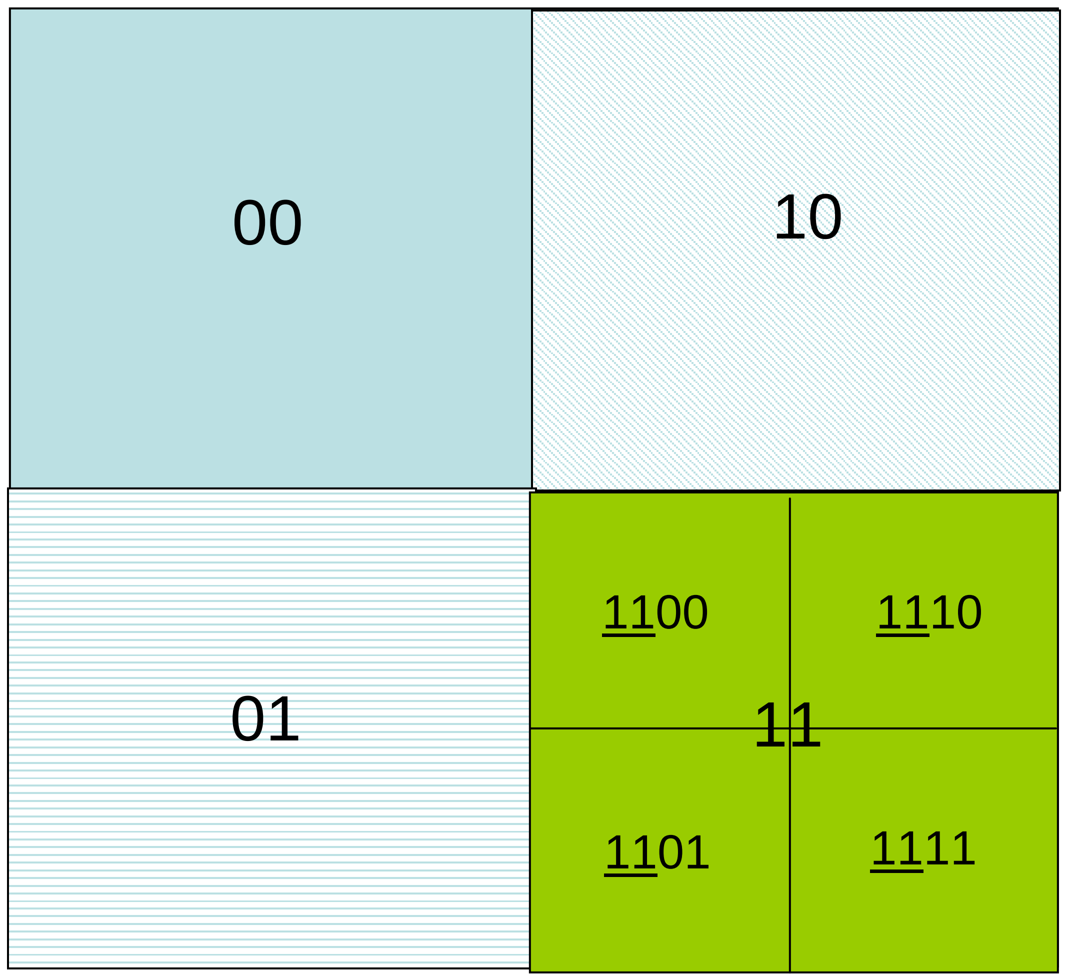
- Client/Server Architecture
- A single server can support multiple clients
- A single server can act as collector for multiple netflow feeds
- Supports both aggregation as well as non-aggregation mode



Flamingo - 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

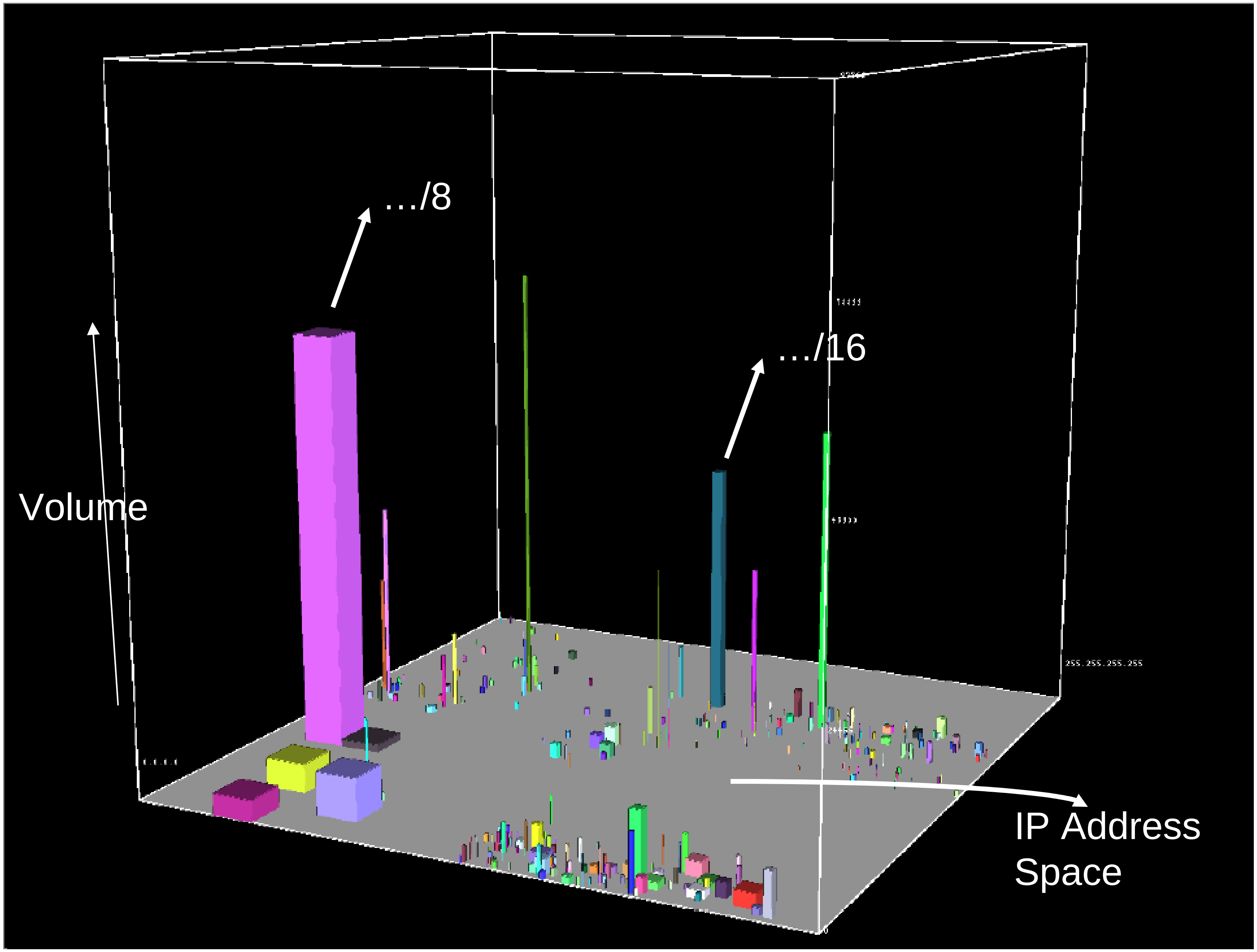
The Basic Quad-Tree



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

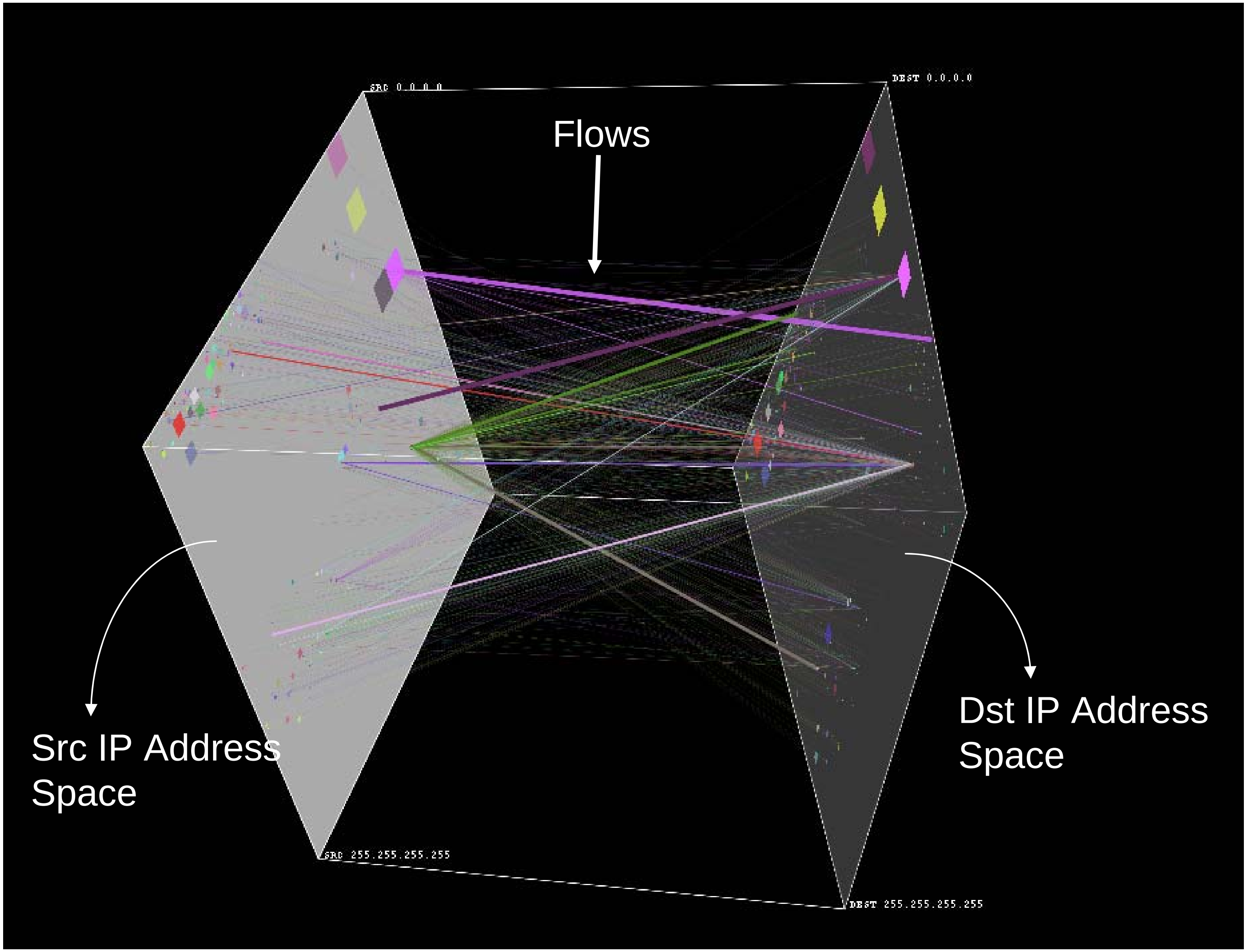
Traffic Volume by Src/Dst IP



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

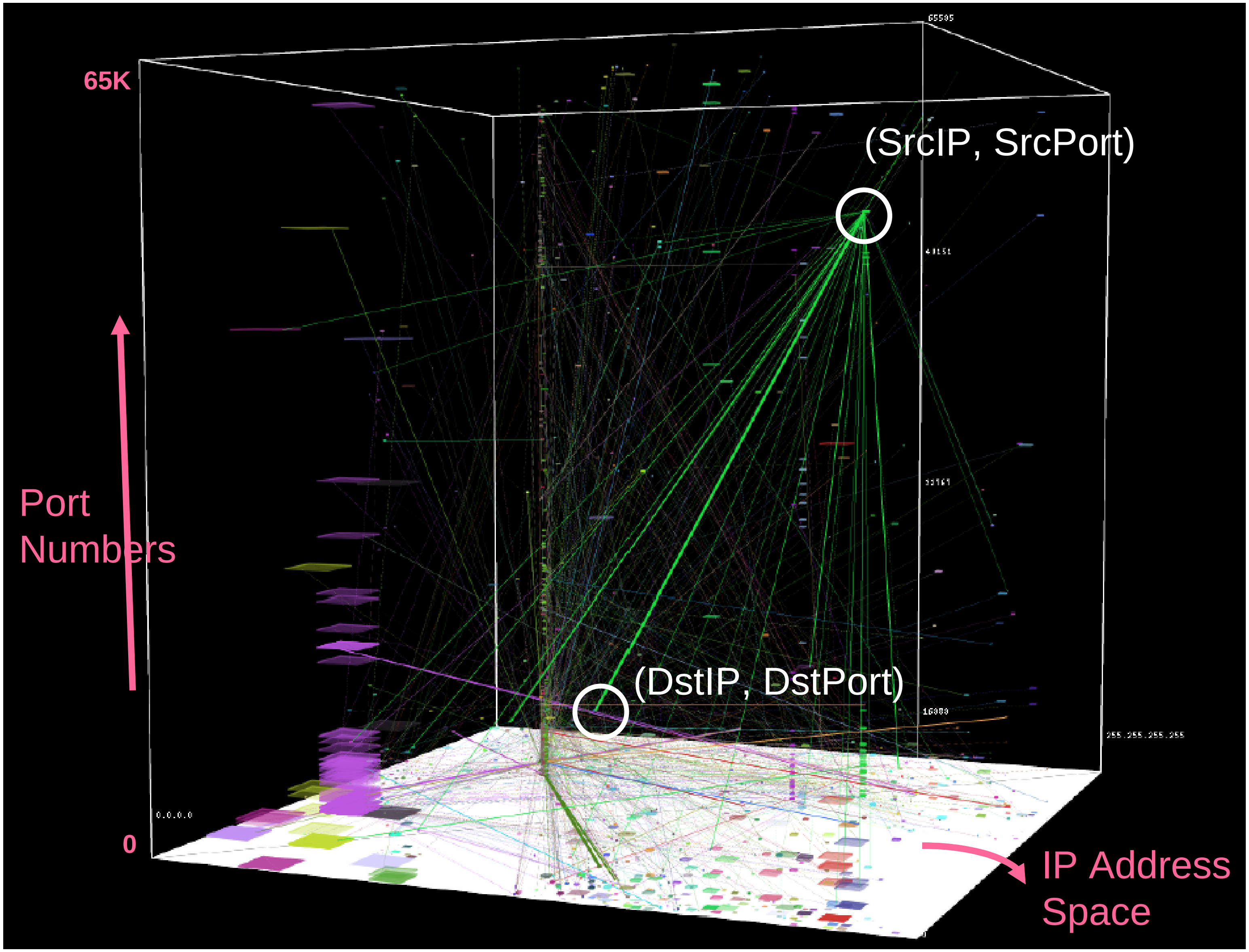
Traffic Flows by Aggregated Src/Dst IP



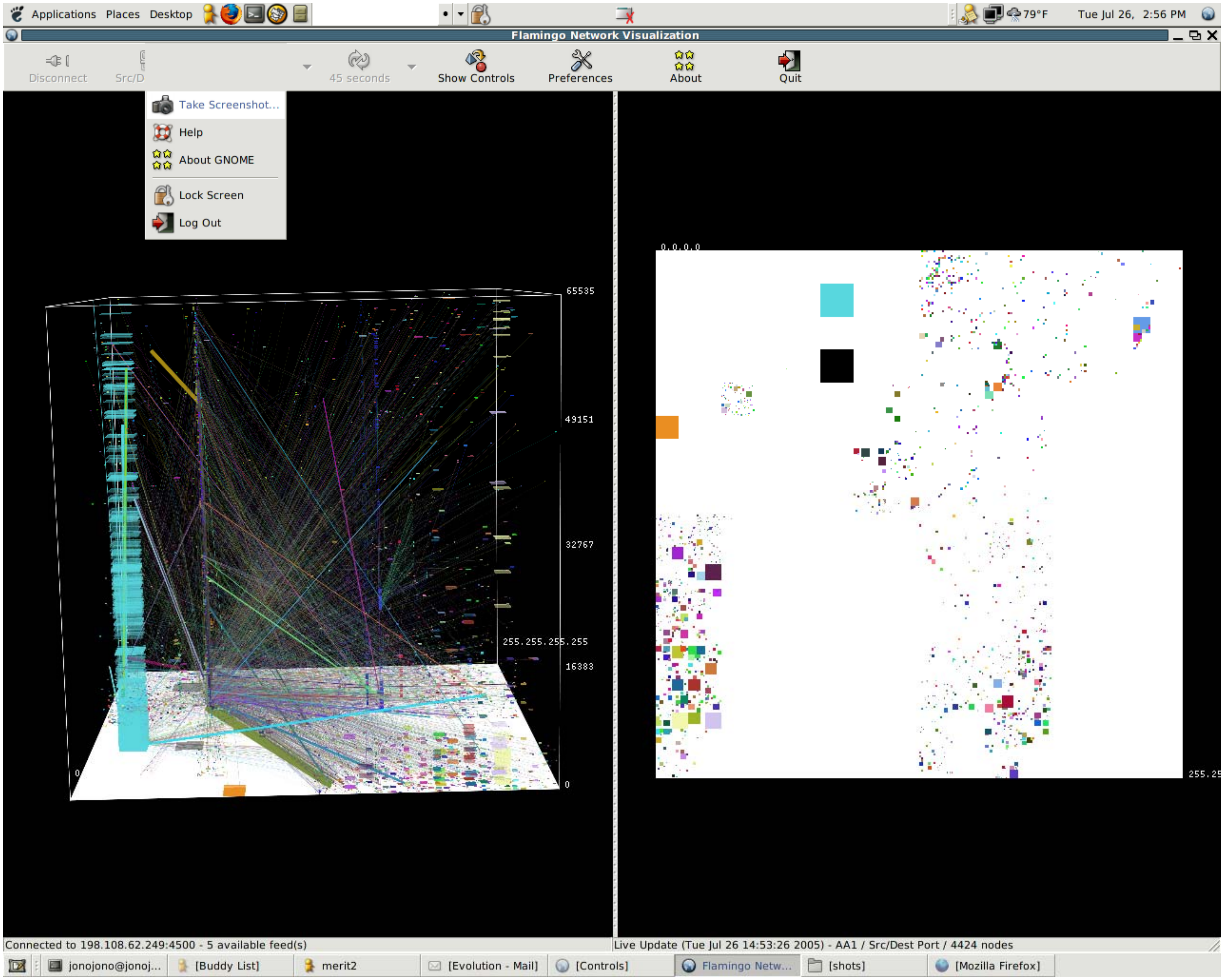
Traffic Flows by Src/Dst IP and Port

- 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

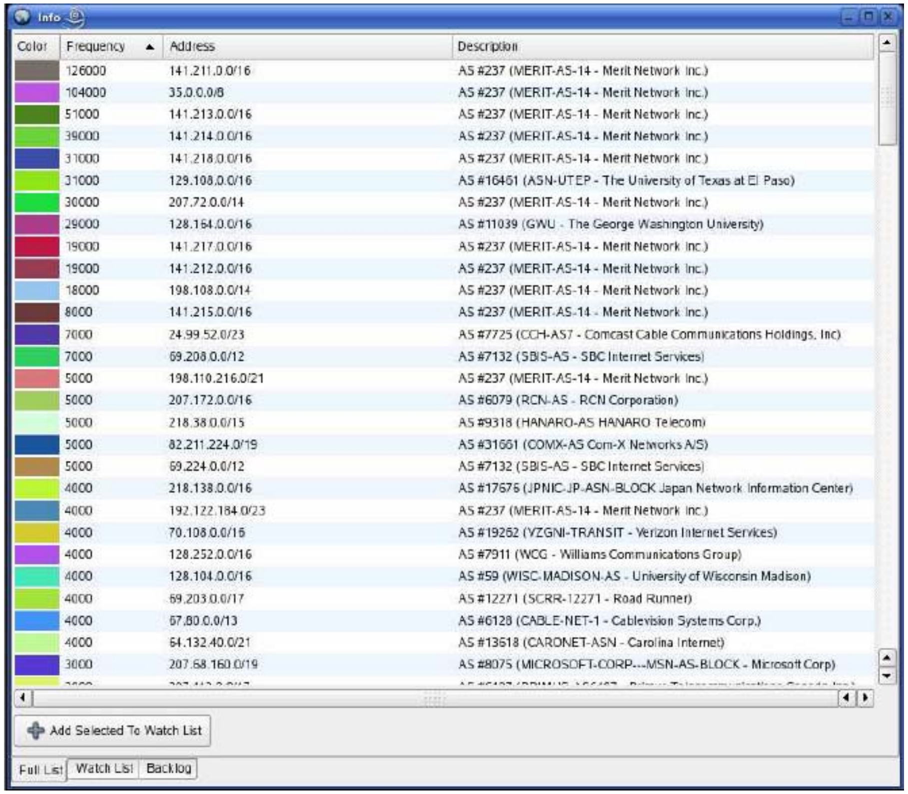


Flamingo Visualization Tool

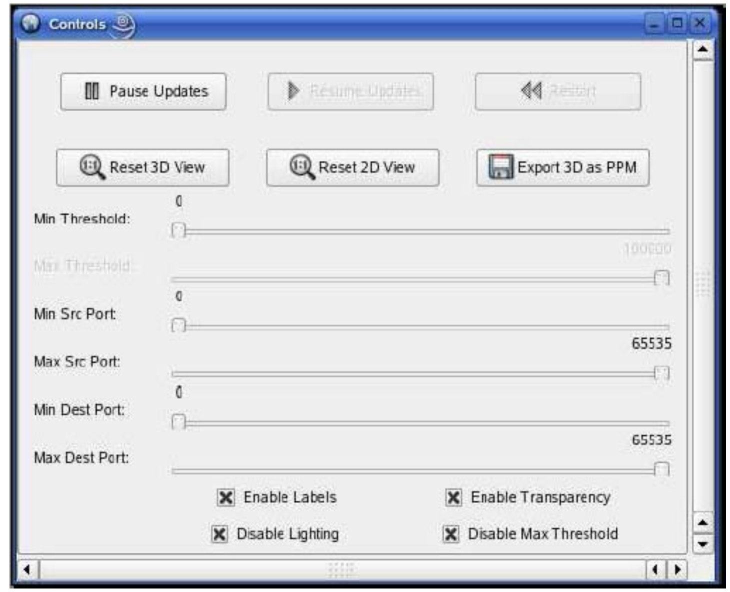


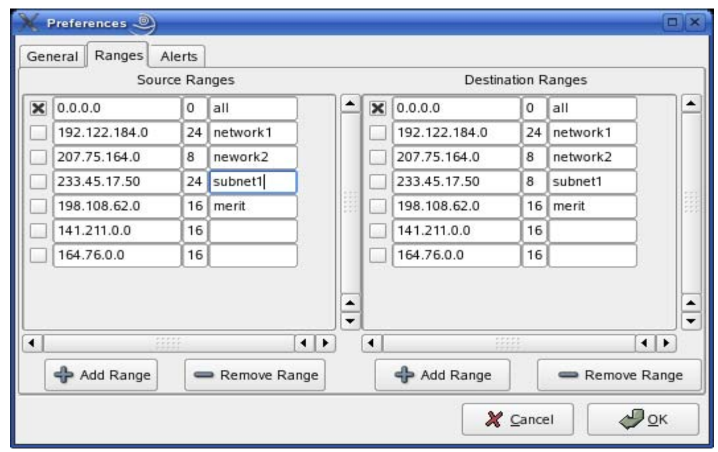
Flamingo Controls

Text Representation of Visualized Information



Slider Bar Controls



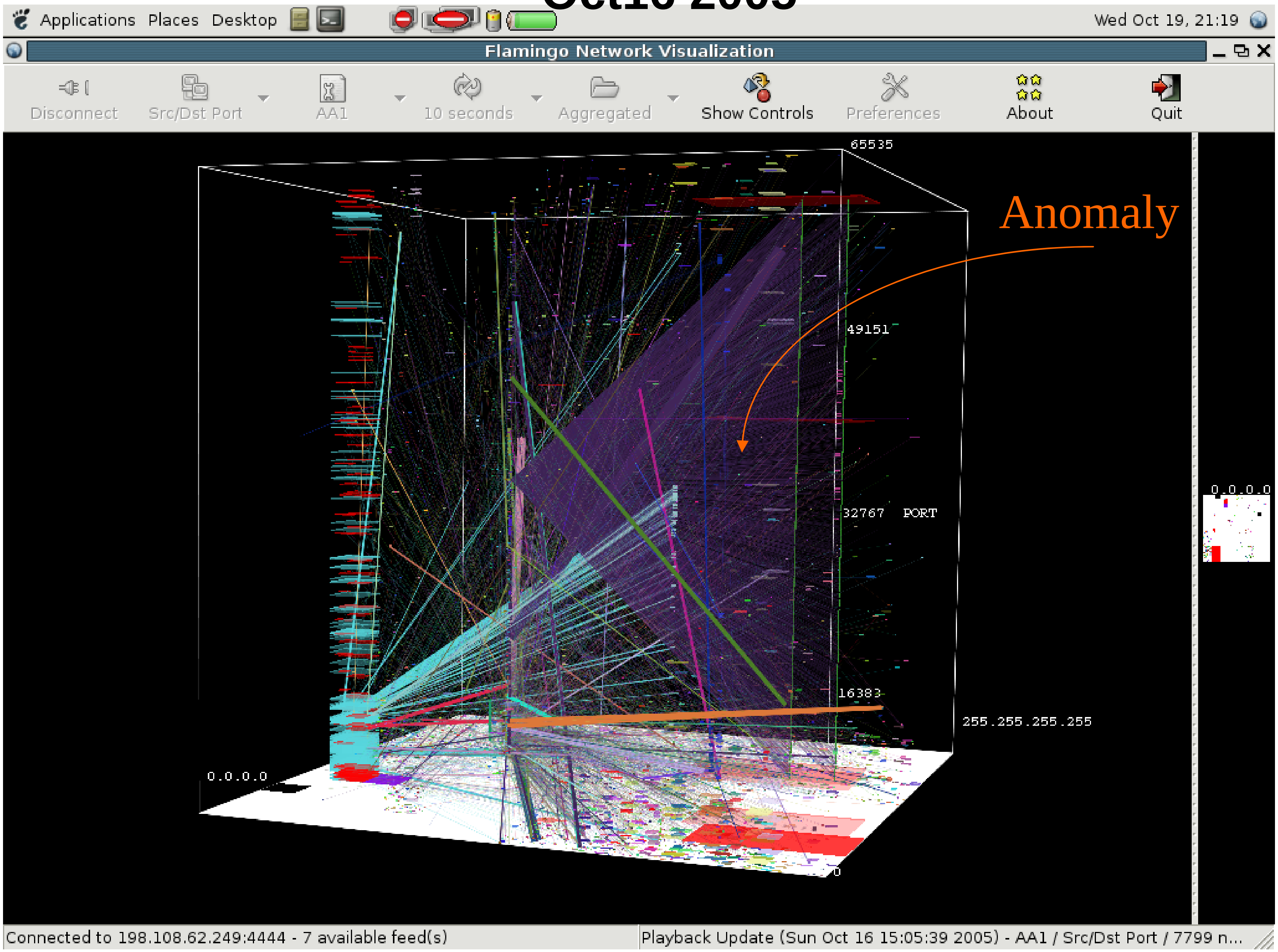


Address Range Configuration

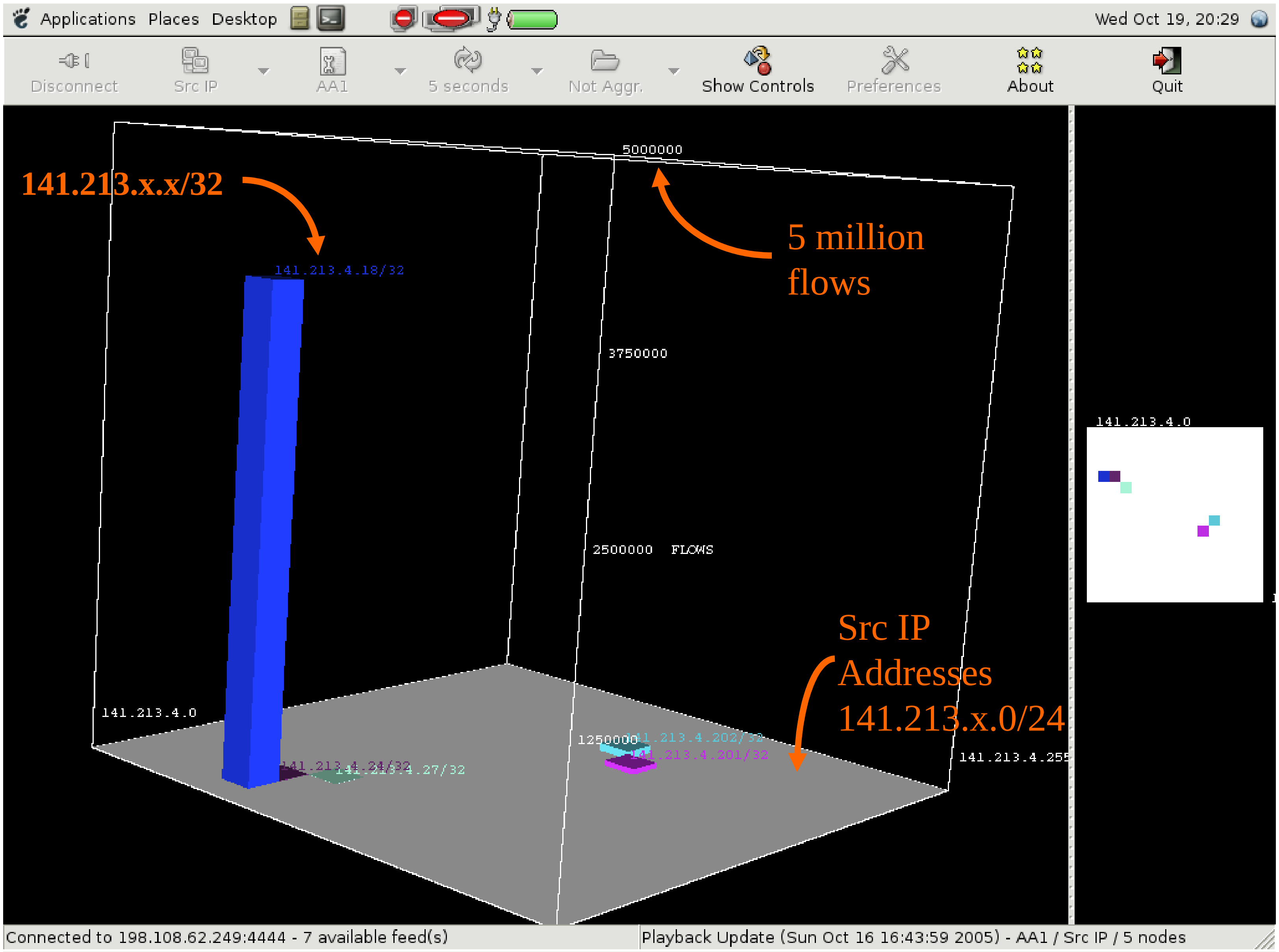
Case Study: Traffic Anomaly Sunday- Oct 16, 2005

- 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

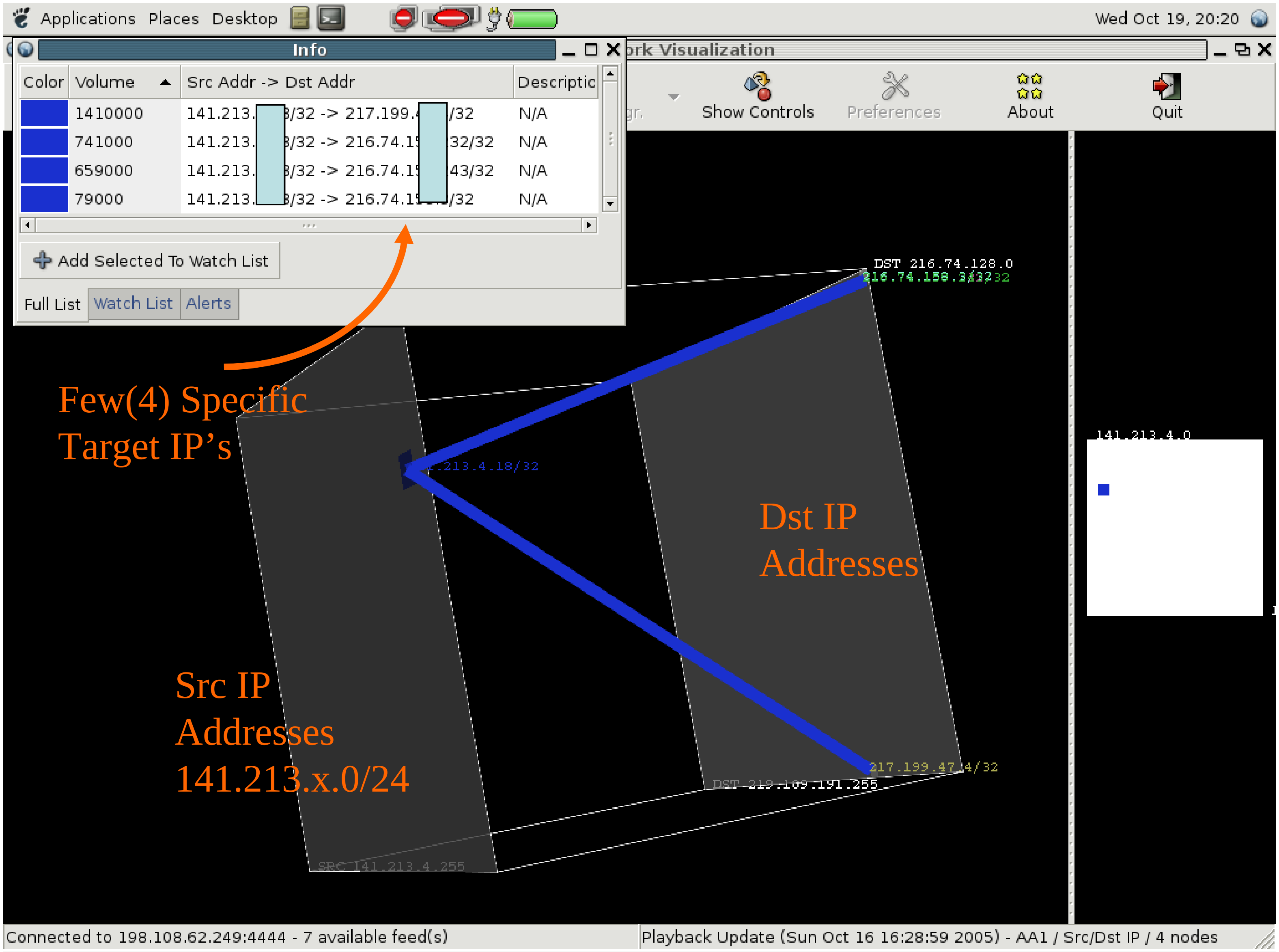
Overall Traffic Pattern at Primary Router Sunday, Oct16 2005



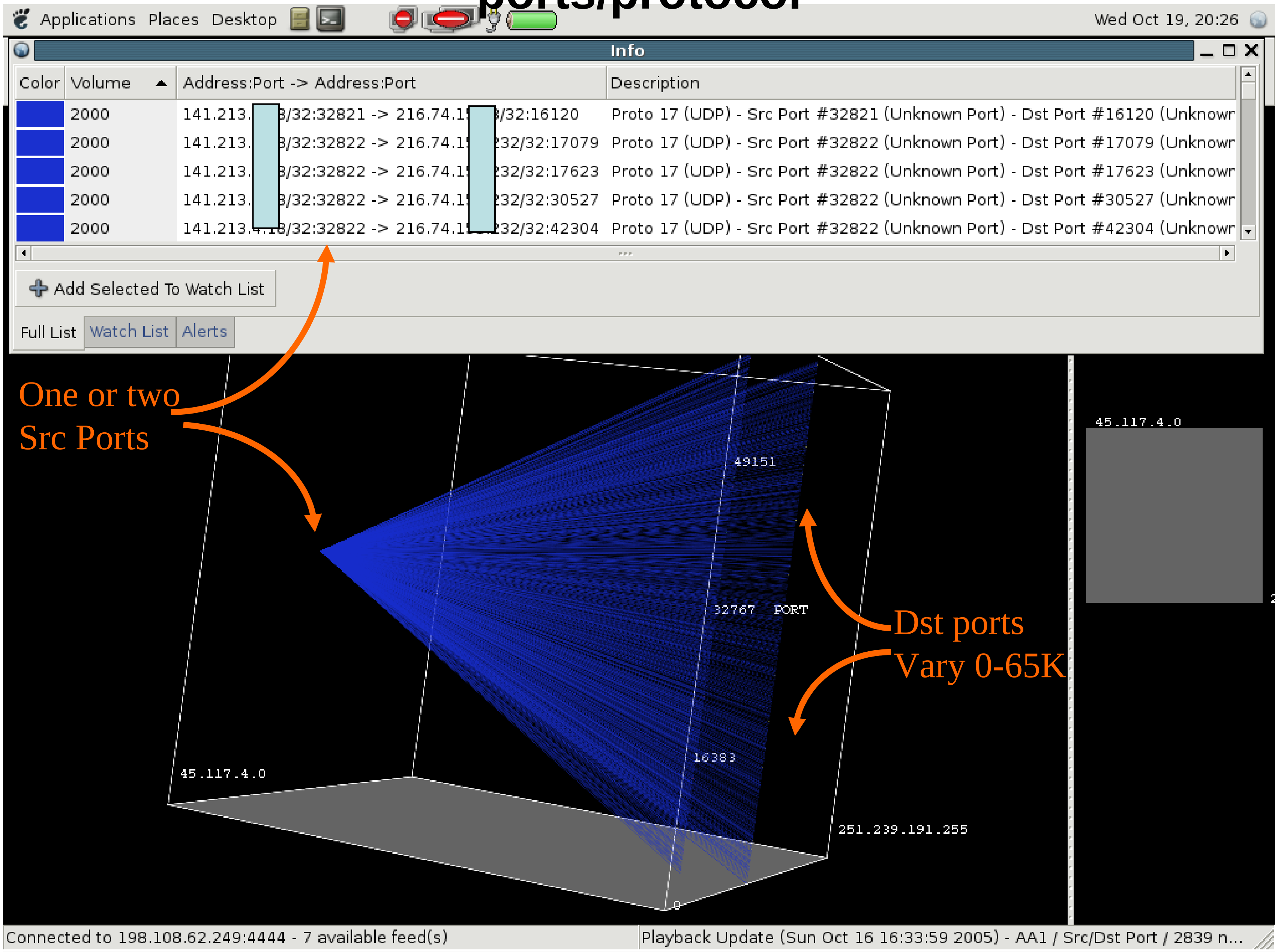
Traffic Volume sourced from /24 subnet by individual hosts



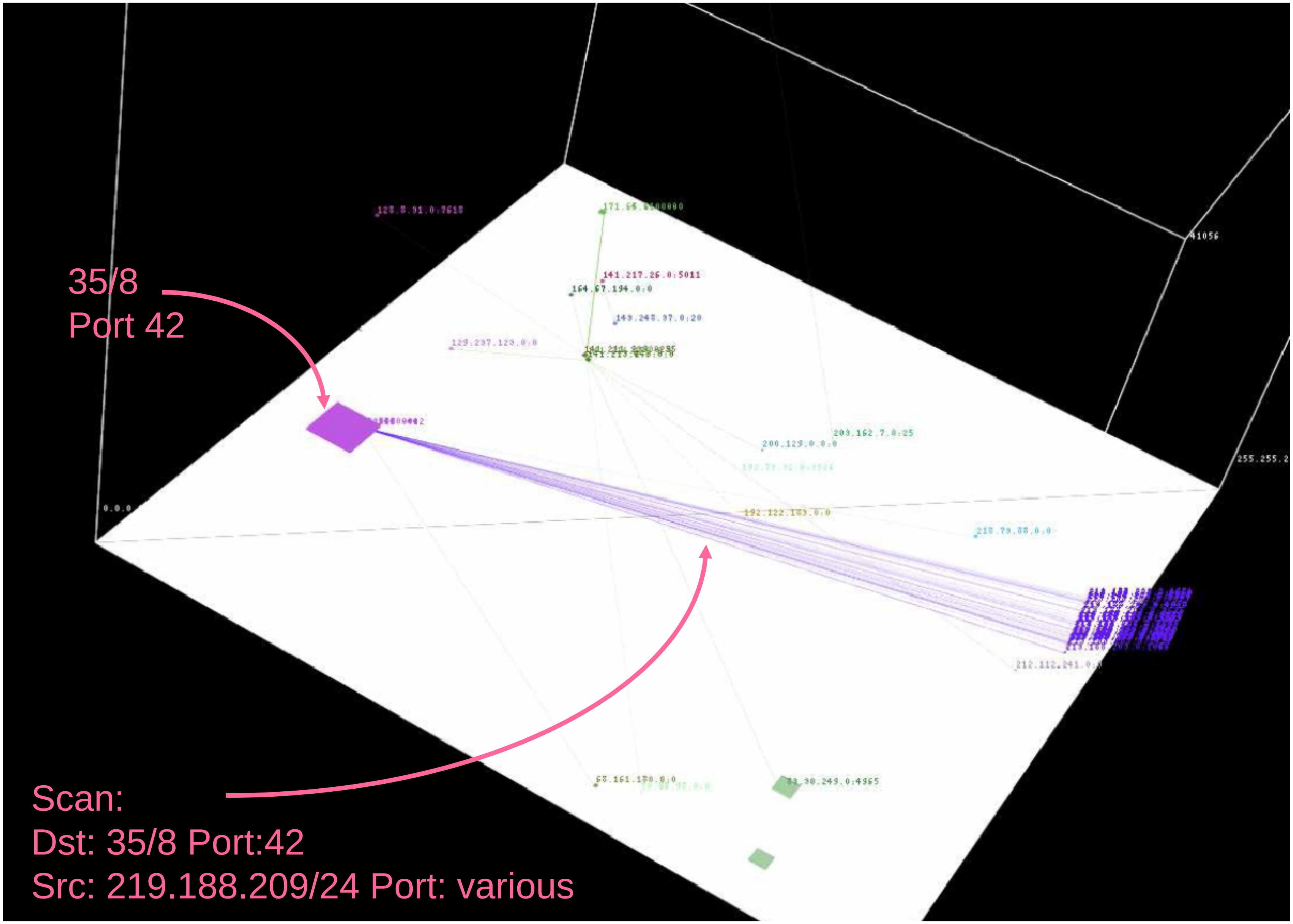
Distribution of Target IP Addresses



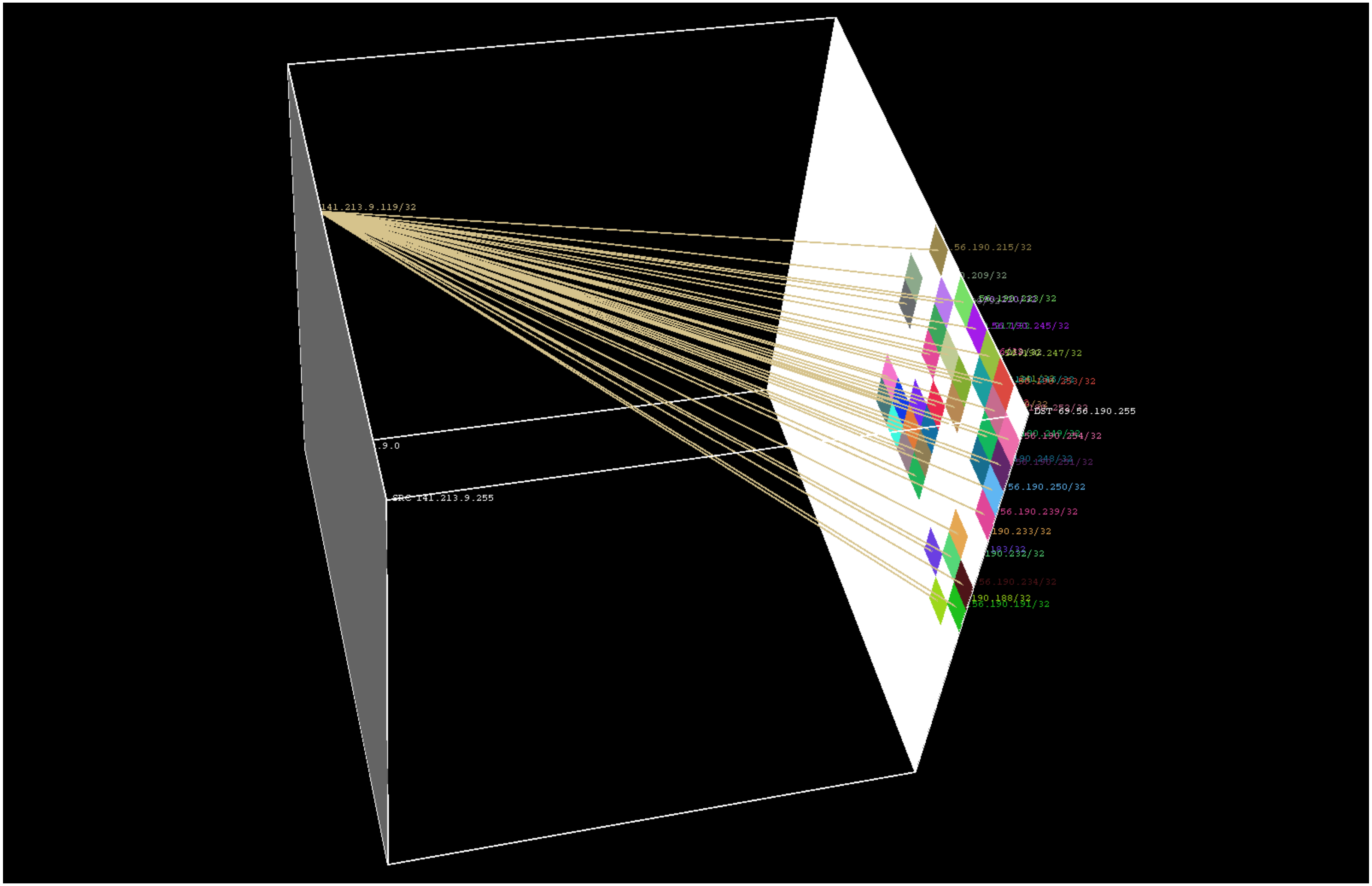
Distribution of flows in terms of src/dst ports/protocol



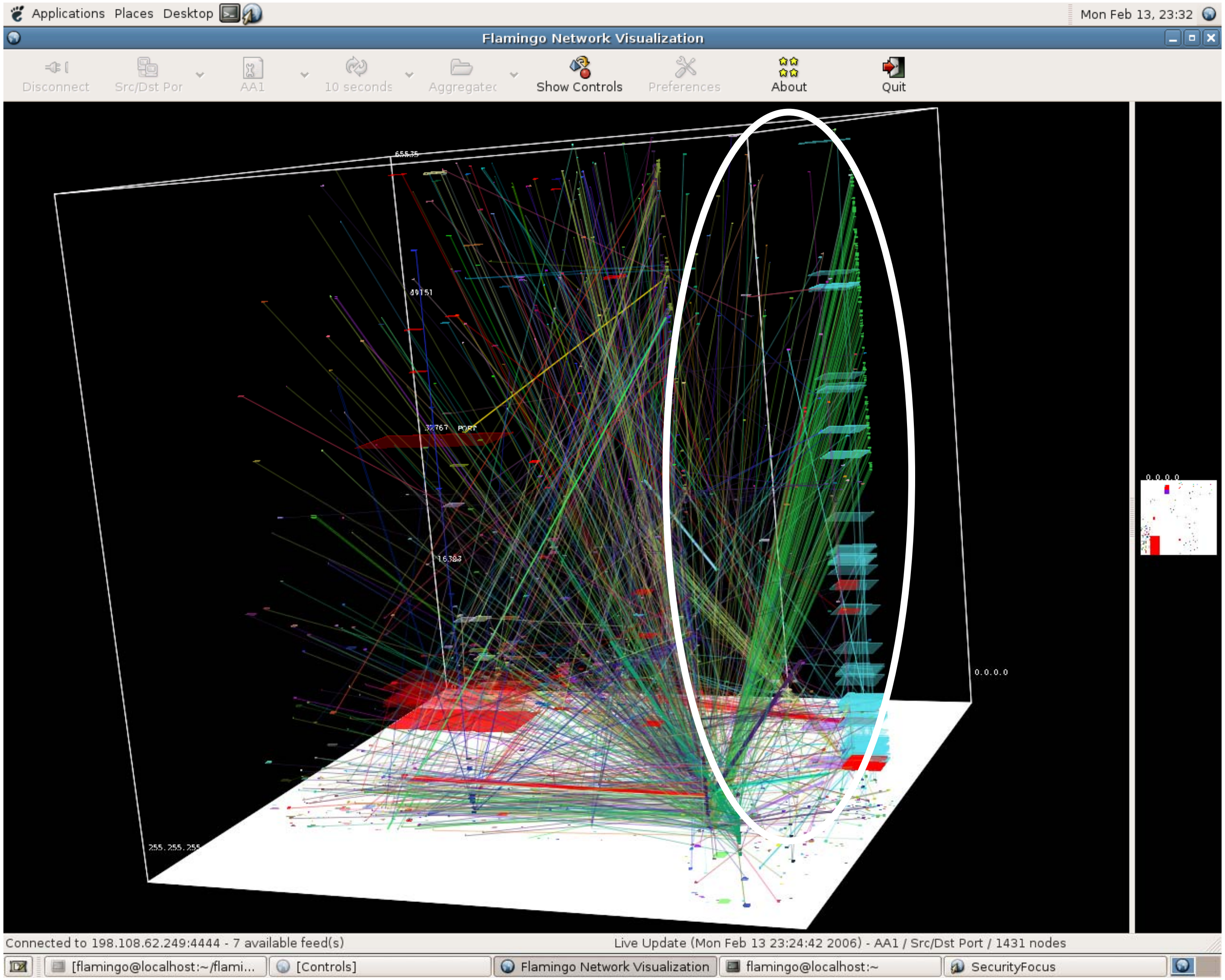
Case Study: Worm Traffic/Port 42 Scans



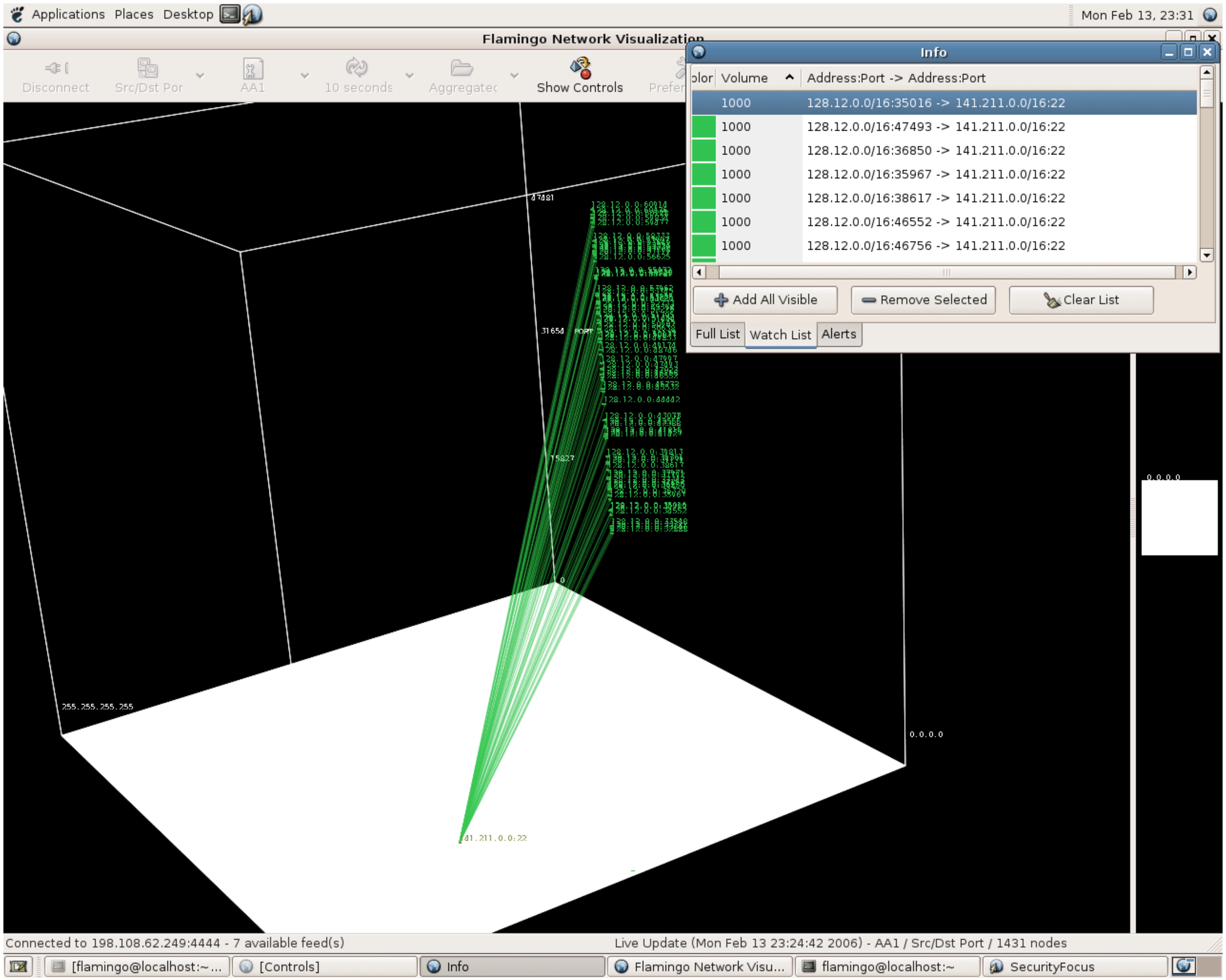
Case Study: /24 Network Scan



ssh scans


Applications Places Desktop
Mon Feb 13, 23:32
Flamingo Network Visualization
Disconnect
Src/Dst Por
AA1
10 seconds
Aggregatec
Show Controls
Preferences
About
Quit
0.0.0.0
255.255.255
Connected to 198.108.62.249:4444 - 7 available feed(s)
Live Update (Mon Feb 13 23:24:42 2006) - AA1 / Src/Dst Port / 1431 nodes
[flamingo@localhost:~/flami...
[Controls]
Flamingo Network Visualization
flamingo@localhost:~
SecurityFocus

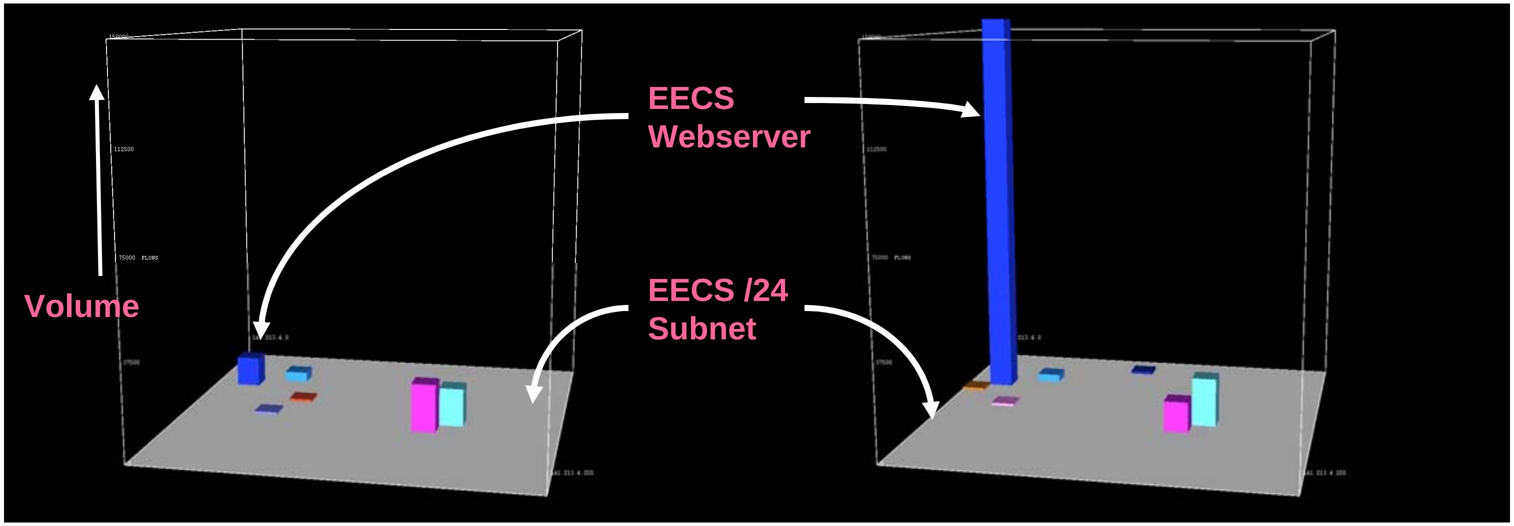
ssh scan



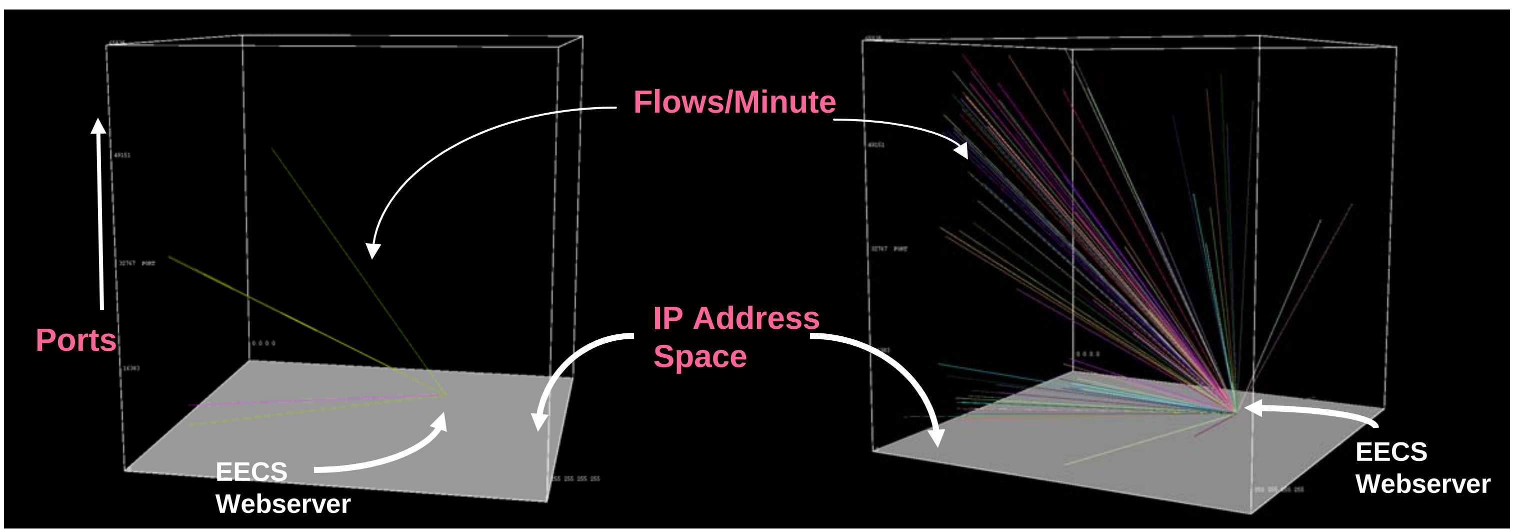
Applications Places Desktop
Mon Feb 13, 23:31
Flamingo Network Visualization
Disconnect
Src/Dst Por
AA1
10 seconds
Aggregatec
Show Controls
Info
Volume
Address:Port -> Address:Port
1000 128.12.0.0/16:35016 -> 141.211.0.0/16:22
1000 128.12.0.0/16:47493 -> 141.211.0.0/16:22
1000 128.12.0.0/16:36850 -> 141.211.0.0/16:22
1000 128.12.0.0/16:35967 -> 141.211.0.0/16:22
1000 128.12.0.0/16:38617 -> 141.211.0.0/16:22
1000 128.12.0.0/16:46552 -> 141.211.0.0/16:22
1000 128.12.0.0/16:46756 -> 141.211.0.0/16:22
Add All Visible
Remove Selected
Clear List
Full List
Watch List
Alerts
255.255.255.255
0.0.0.0
Connected to 198.108.62.249:4444 - 7 available feed(s)
Live Update (Mon Feb 13 23:24:42 2006) - AA1 / Src/Dst Port / 1431 nodes
[flamingo@localhost:~...
[Controls]
Info
Flamingo Network Visu...
flamingo@localhost:~
SecurityFocus

Case Study: Slashdot Event Oct 31, 2004

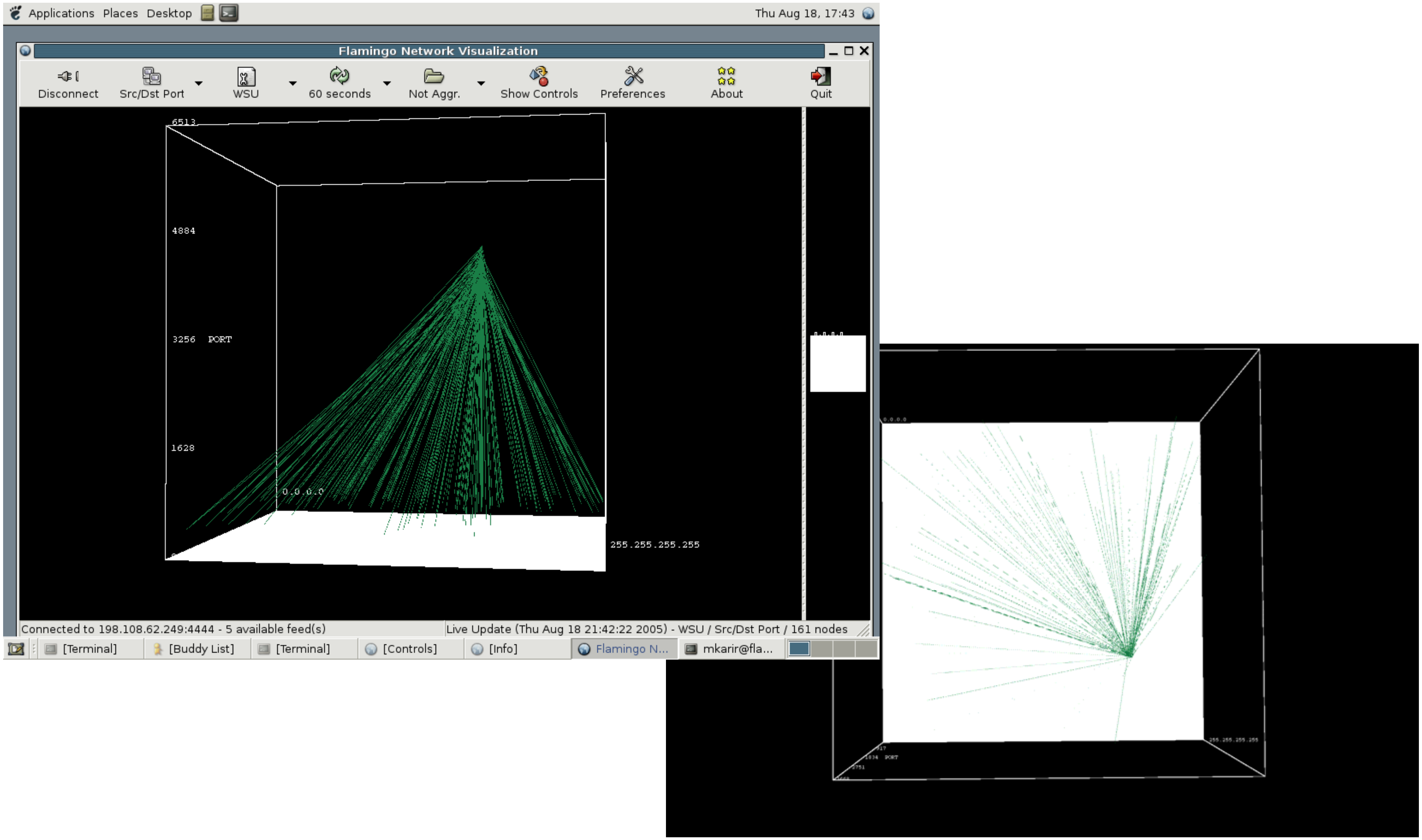
Traffic Volume



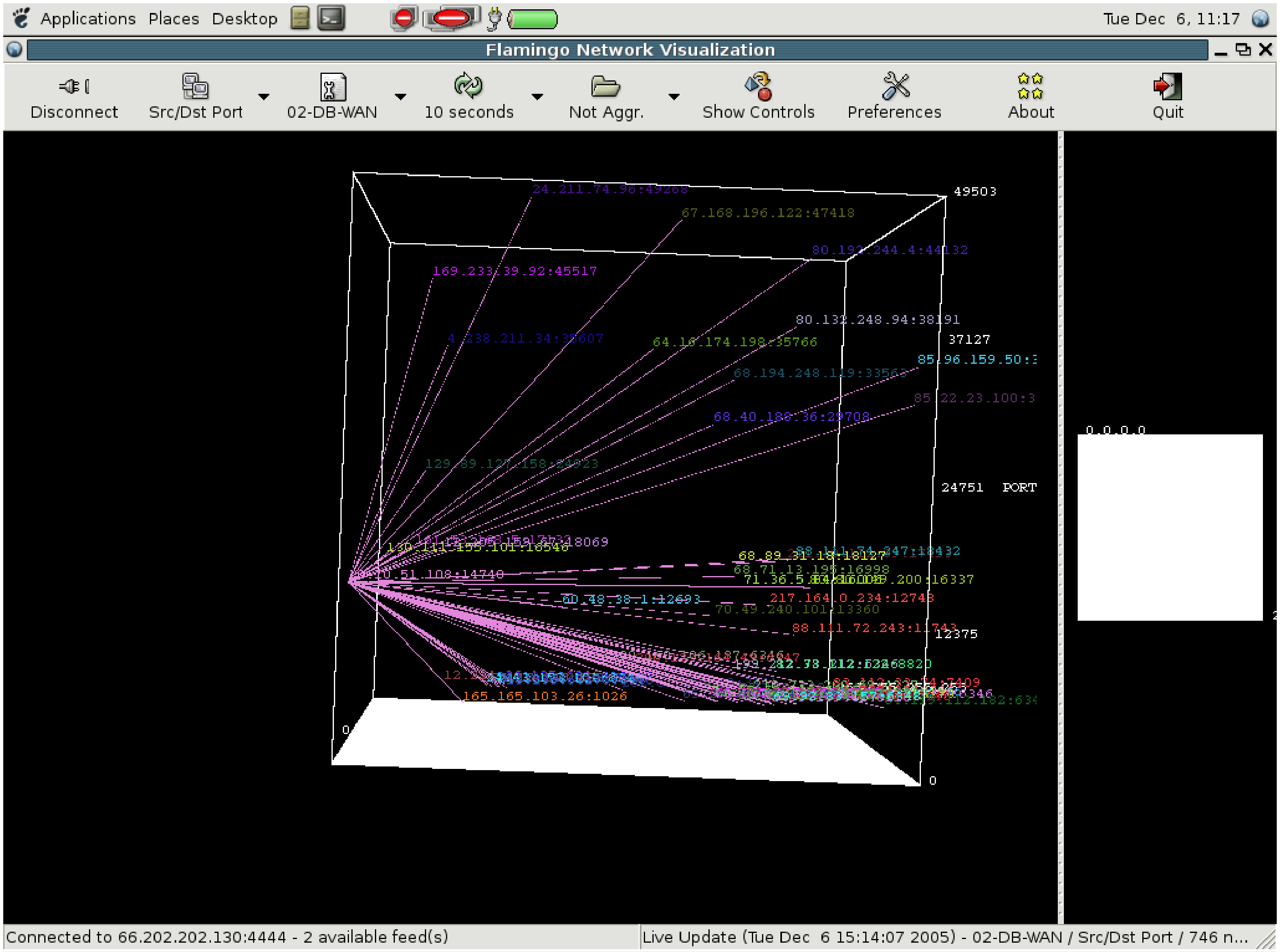
Flow Volume



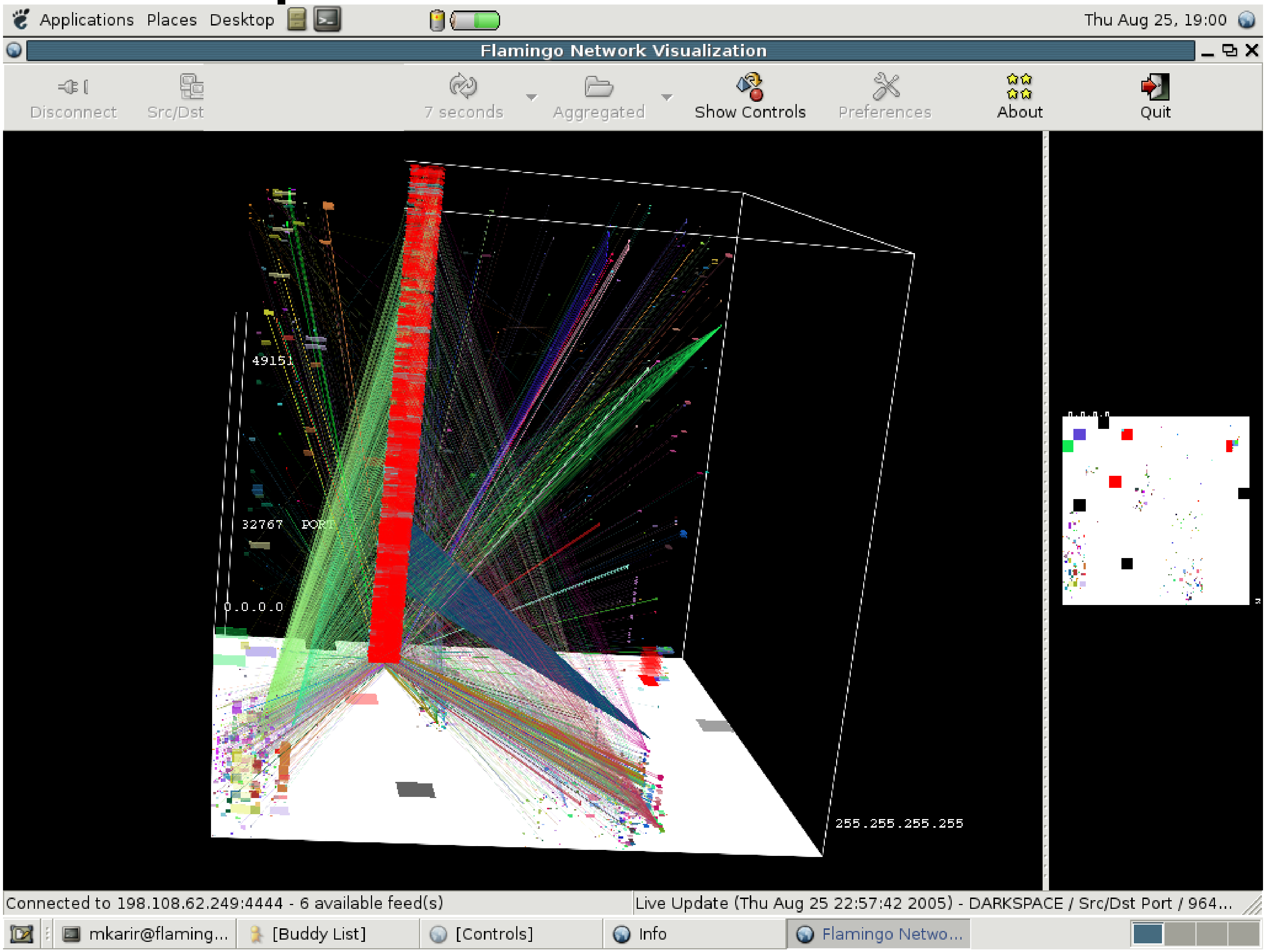
Zotob Worm Infection



P2P Traffic


Applications Places Desktop
Tue Dec 6, 11:17
Flamingo Network Visualization
Disconnect
Src/Dst Port
02-DB-WAN
10 seconds
Not Aggr.
Show Controls
Preferences
About
Quit
49503
37127
24751 PORT
12375
0
0.0.0.0
Connected to 66.202.202.130:4444 - 2 available feed(s)
Live Update (Tue Dec 6 15:14:07 2005) - 02-DB-WAN / Src/Dst Port / 746 n...

Dark-space Traffic Visualization



Conclusion

- Obtaining raw data from networks is becoming easier, however using it effectively continues to be challenging
- Tools are the key in making raw data useful
- Operators often know what they are looking for, we should just make it easier for them to quickly get the information they need; there is some incident that is brought to their attention etc.
- Visualization can help to understand complex multi-dimensional data, instead of a database based query-response system which does not allow you to easily “explore” your data