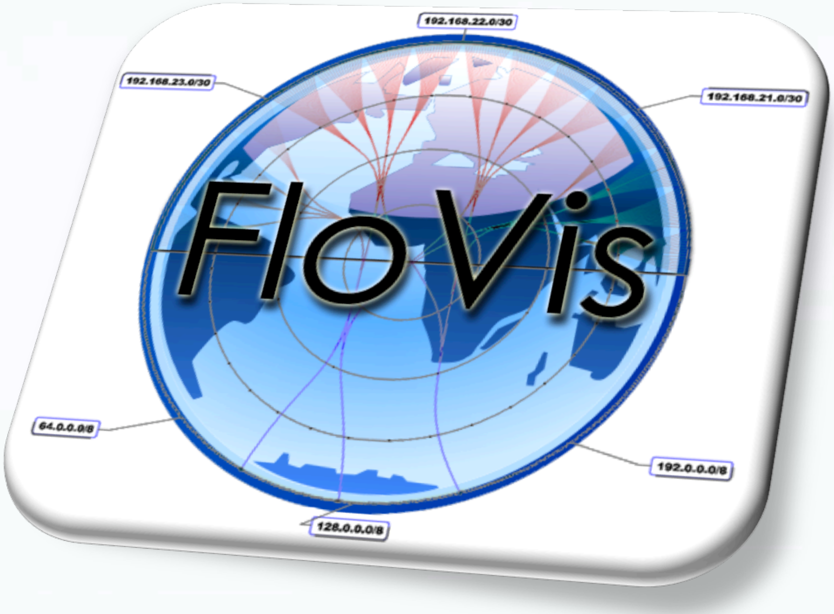


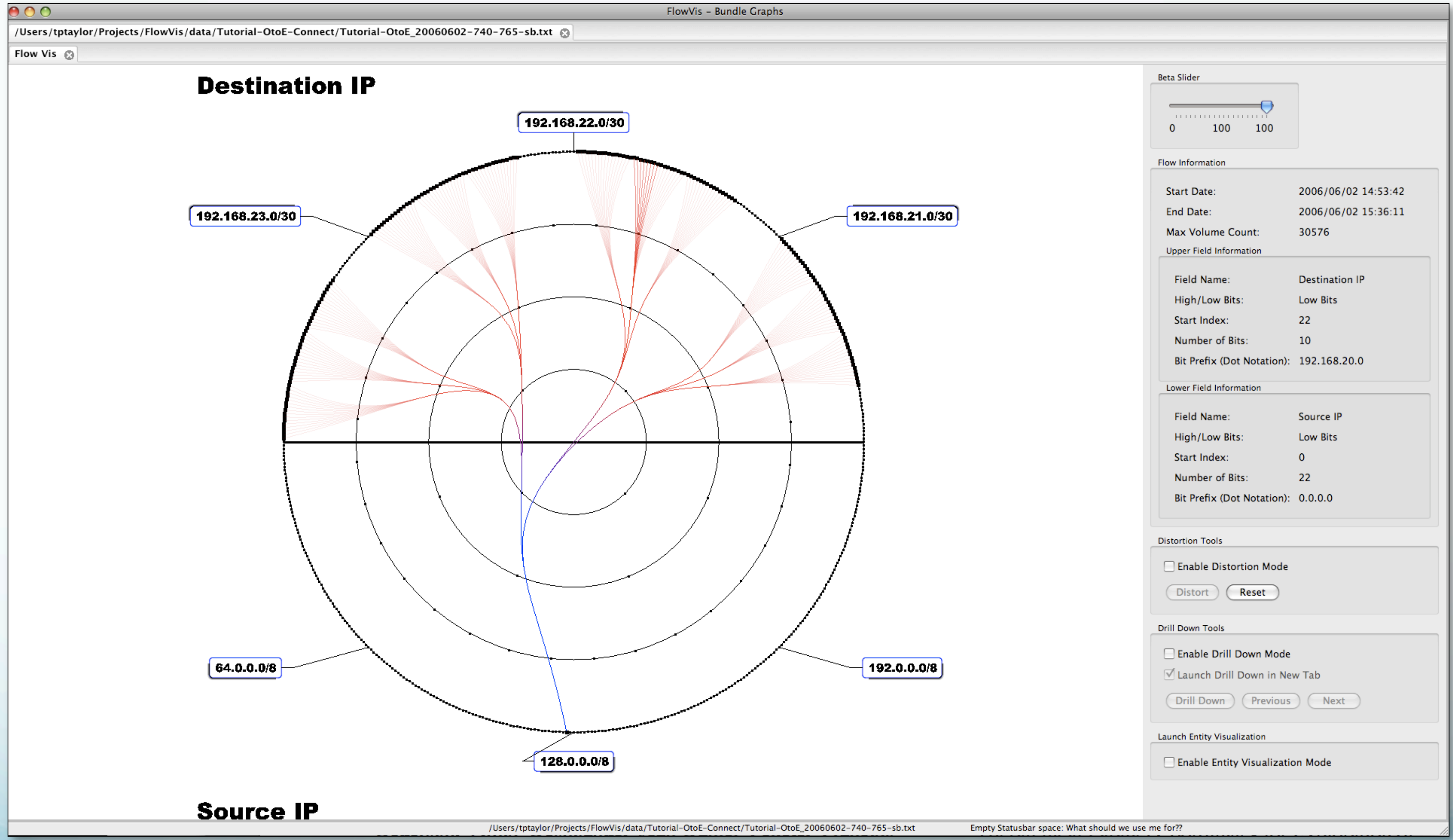
FlowBundle

Teryl Taylor

Purpose

- Visualize pair-wise data attributes from a Netflow record (e.g. source host/network vs destination host/network).
- Deal with some key issues facing current connection-based visualizations: occlusion, drill down, labeling, etc
- Incorporate other interactive features and visualizations

FlowBundle



Flow Information

Start Date:	2006/06/02 14:53:42
End Date:	2006/06/02 15:36:11
Max Volume Count:	30576

Upper Field Information

Field Name:	Destination IP
High/Low Bits:	Low Bits
Start Index:	22
Number of Bits:	10
Bit Prefix (Dot Notation):	192.168.20.0

Lower Field Information

Field Name:	Source IP
High/Low Bits:	Low Bits
Start Index:	0
Number of Bits:	22
Bit Prefix (Dot Notation):	0.0.0.0

☐ Enable Distortion Mode

☐ Enable Drill Down Mode

☑ Launch Drill Down in New Tab

☐ Enable Entity Visualization Mode

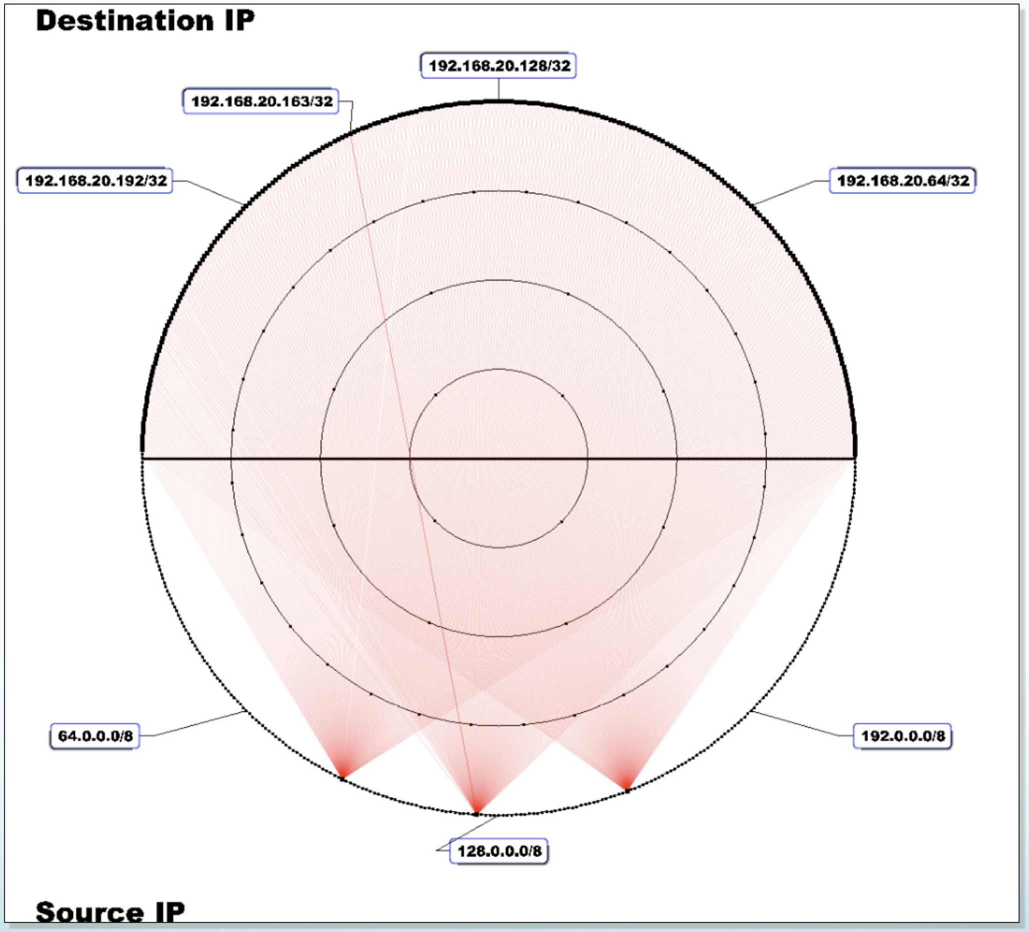
/Users/tptaylor/Projects/FlowVis/data/Tutorial-OtoE-Connect/Tutorial-OtoE_20060602-740-765-sb.txt

Empty Statusbar space: What should we use me for??

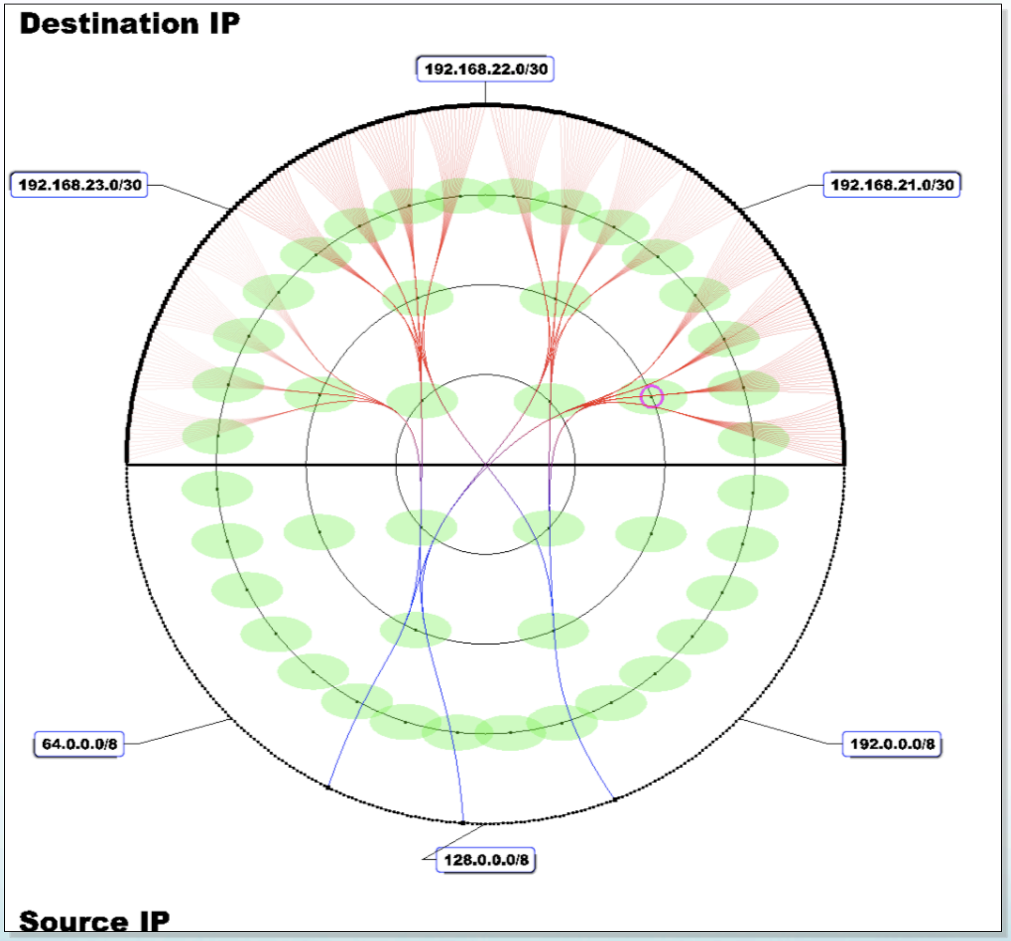
Data Considerations

- Takes a SiLK bag indexed by portions of any two scalar fields from NetFlow
- Total length of scalars must add to 32 bits
  - e.g. Top 16 bits of source address/Lower 16 bits of destination address
- Working towards creating full 64 bit indexes for full connections
- Bag counts the number of flows/bytes/packets for the index over a specified time period (hours or days)

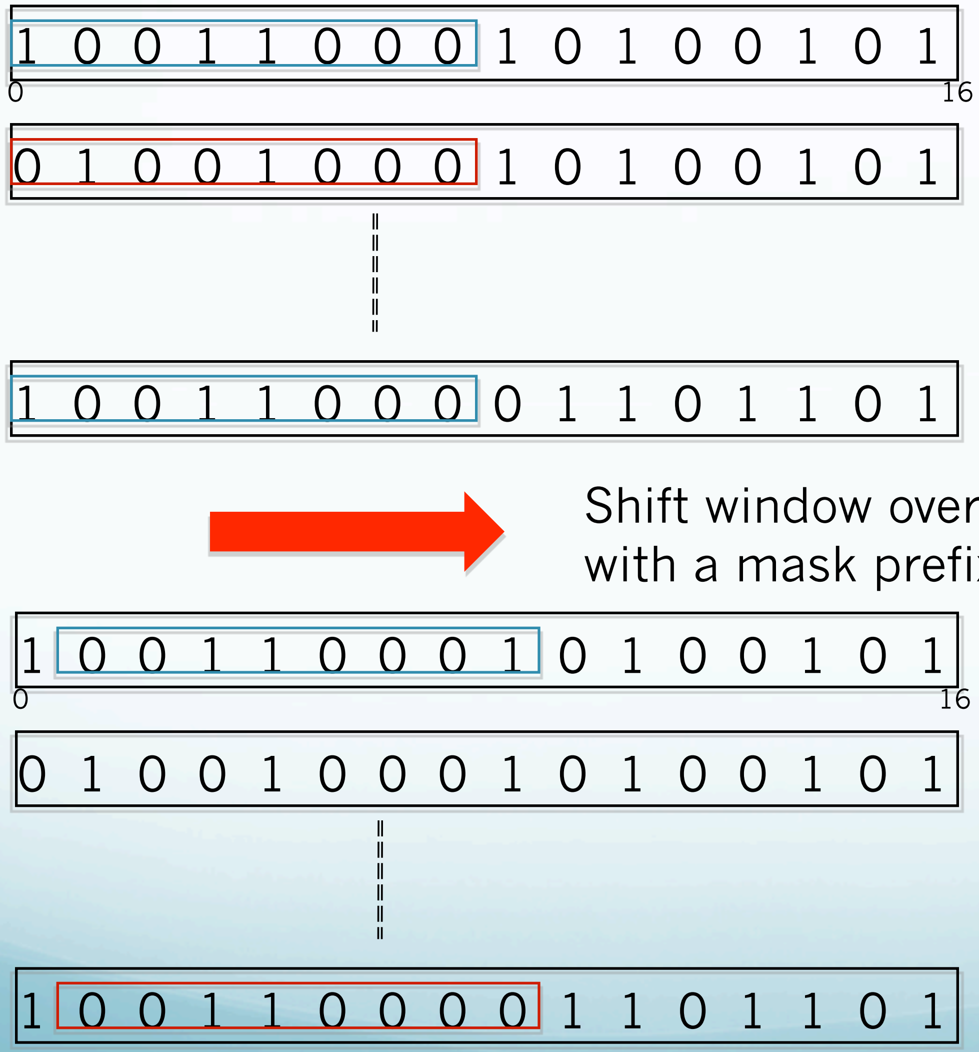
Bundle Loosening



Drill Down


Destination IP
192.168.22.0/30
192.168.23.0/30
192.168.21.0/30
64.0.0.0/8
192.0.0.0/8
128.0.0.0/8
Source IP

Drill Down Cont'd



Scalar Field (e.g.
source address)

1 0 0 1 1 0 0 0 1 0 1 0 0 1 0 1

0 16

0 1 0 0 1 0 0 0 1 0 1 0 0 1 0 1

1 0 0 1 1 0 0 0 0 1 1 0 1 1 0 1

Shift window over by one bit
with a mask prefix of 1

1 0 0 1 1 0 0 0 1 0 1 0 0 1 0 1

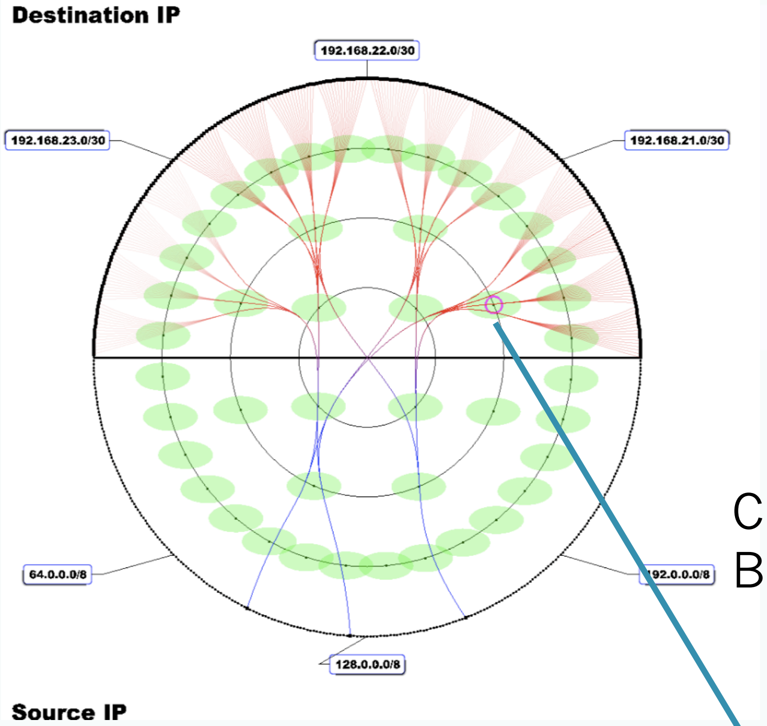
0 16

0 1 0 0 1 0 0 0 1 0 1 0 0 1 0 1

Filtered out because
first bit is 0 instead of 1

1 0 0 1 1 0 0 0 0 1 1 0 1 1 0 1

Drill Down cont'd



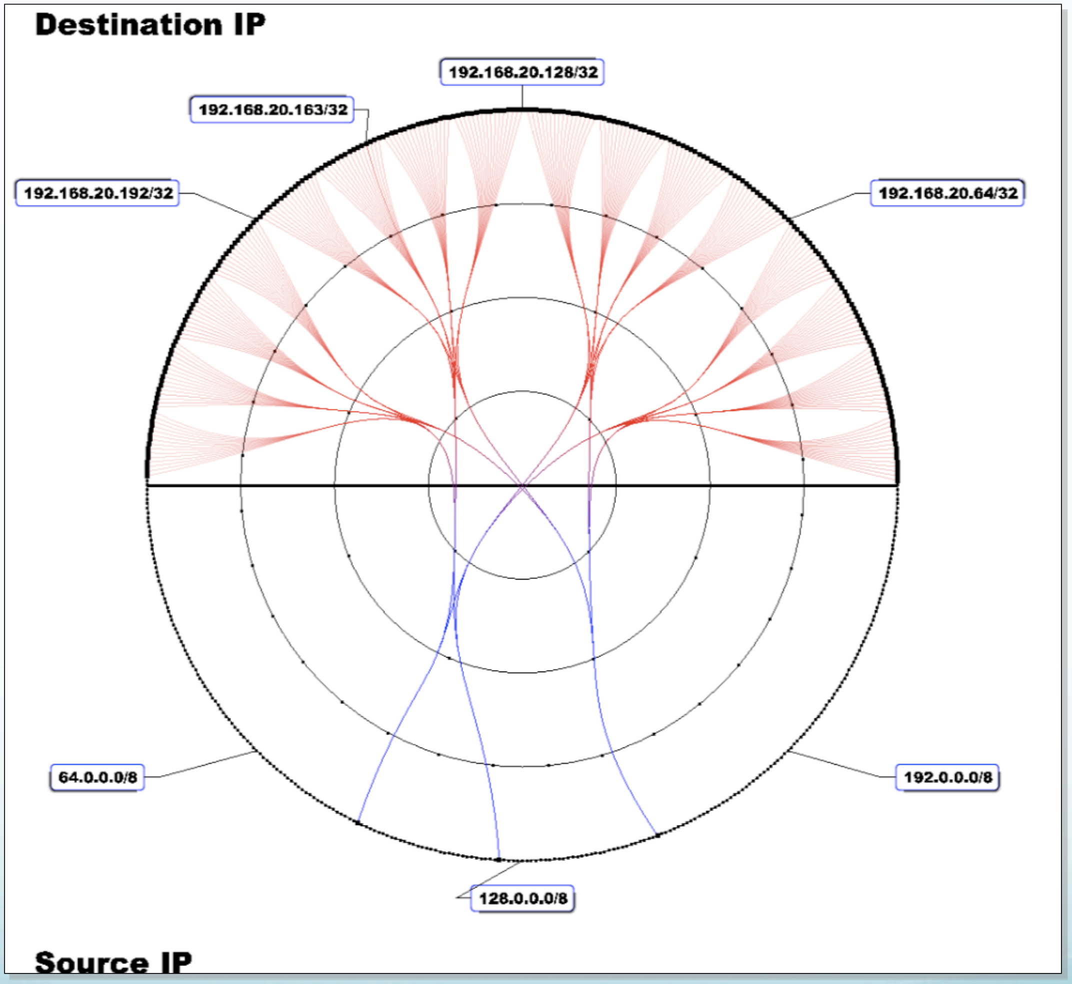
Clicking on this node is equivalent to
Bit mask: 000 ~ Bit Window Length: 3

Scalar Field (e.g.
source address)

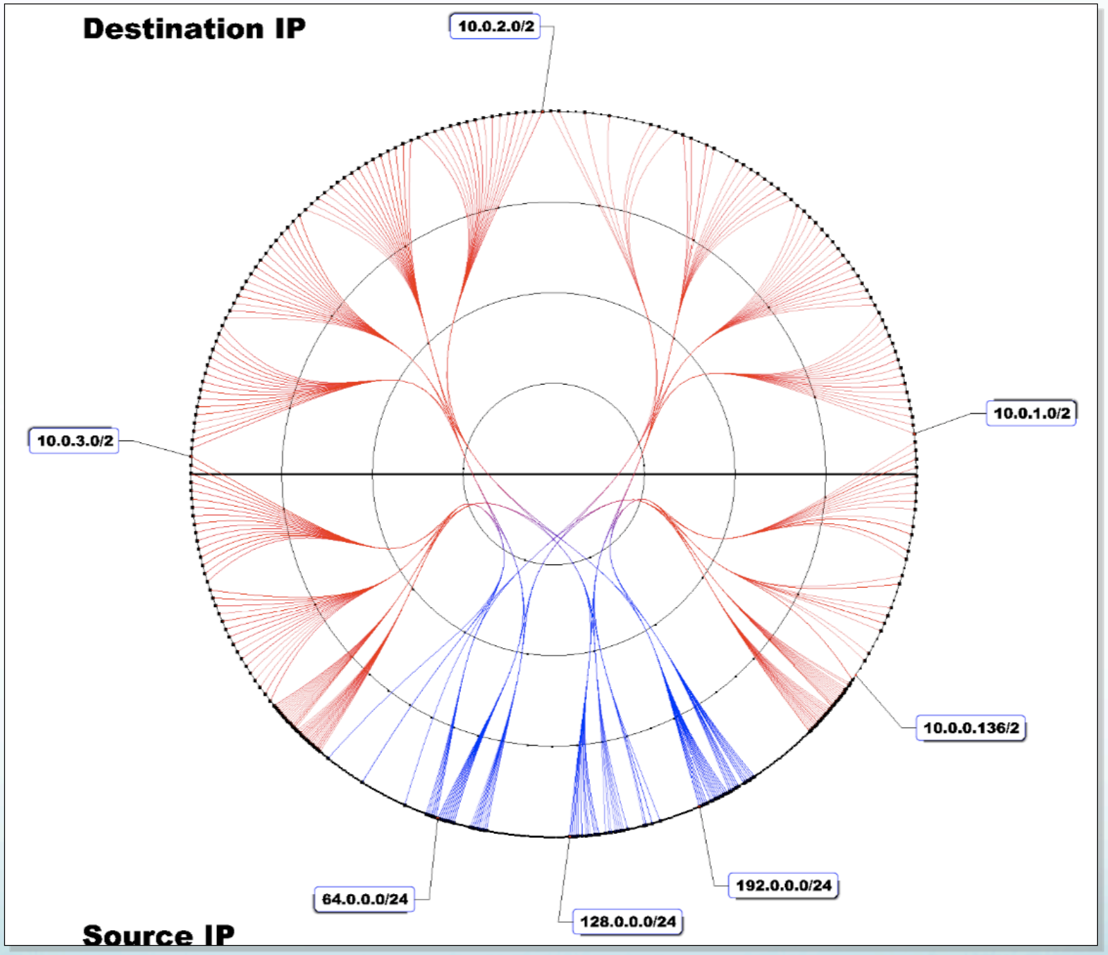
0 0 0 1 1 0 0 0 1 0 1 0 0 1 0 1

0 16

Drill Down Result



Linear Distortion



Conclusions

- FlowBundle visualizes interactions between entities on a network
  - Any 32-bit representation (e.g., source ports to dest ports, /16 subnets to dest ports, etc.)
- Utilizes node aggregation, drill down and bundling to minimize occlusion

Future Work

- Bi-directional flows
- Bundle selection, magnification and filtering