



Real Time Topology Based Flow Visualization

John K. Smith jsmith@referentia.com

Referentia Systems Incorporated

Flocon 2011, Salt Lake City, UT

Color Mapping By DSCP

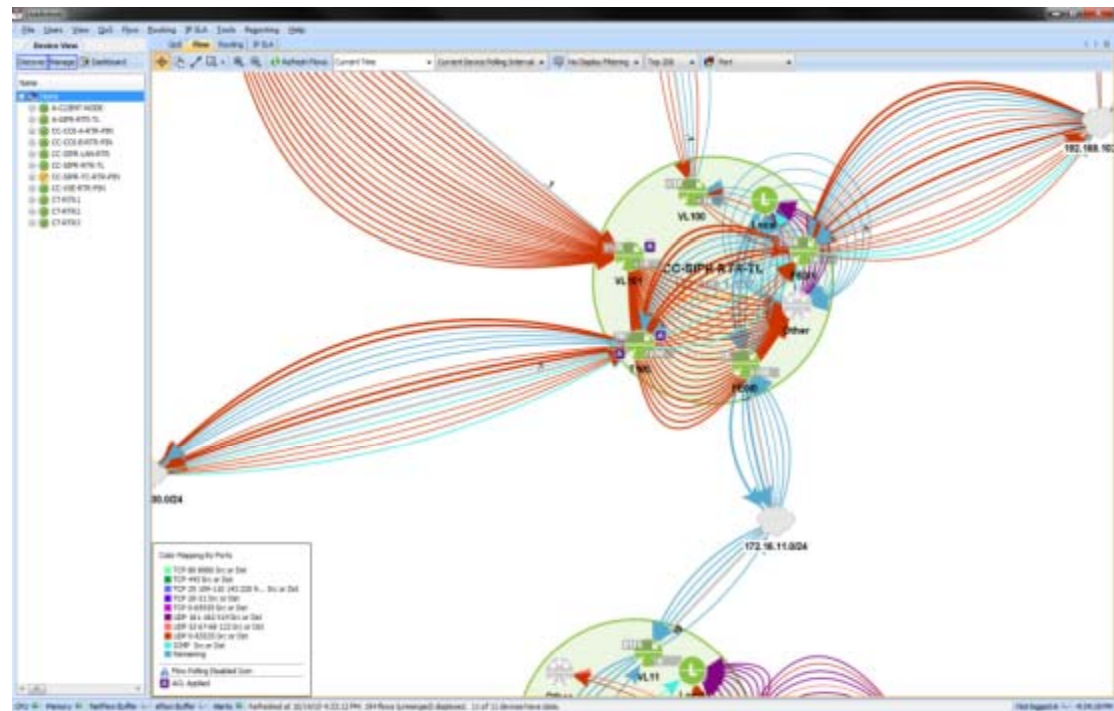
- 0 (BE)
- 18 (AF21)
- 26 (AF31)
- 34 (AF41)
- 16 (CS2)
- 24 (CS3)
- 32 (CS4)
- 48 (CS6)
- 46 (EF)
- Remaining

▲ Flow Polling Disabled Icon

▲ ACL Applied

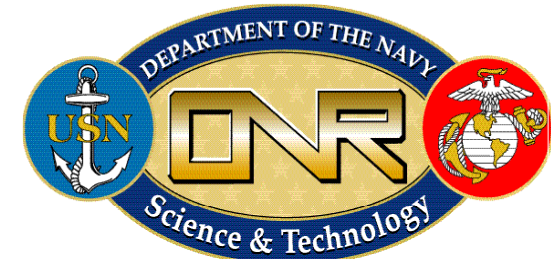
- Flow Visualization Tool Overview
- Visualizations and Design Issues
- Use Cases

NOTE: Networks shown in this presentation are simulated, not actual DoD networks, traffic or addresses.



- **Initial Goal**

- Network Quality of Service Monitor and Control
- Tactical Military Networks
- Easy to use for E3-E5 (Sergeant)



- **Working With**

- Office of Naval Research
- U.S. Marines
 - Marine Forces Pacific (MARFORPAC)
 - 3rd Marine Expeditionary Force (III MEF)



Quality of Service

Routing Visualizations

Flow

Service Level Agreement

Network Management

Network Situational Awareness

Computer Network Defense

Configuration

Monitoring

Historical Analysis

Visualization

Quality of Service

Routing Visualizations

Flow

Service Level Agreement

Network Management

Network Situational Awareness

Computer Network Defense

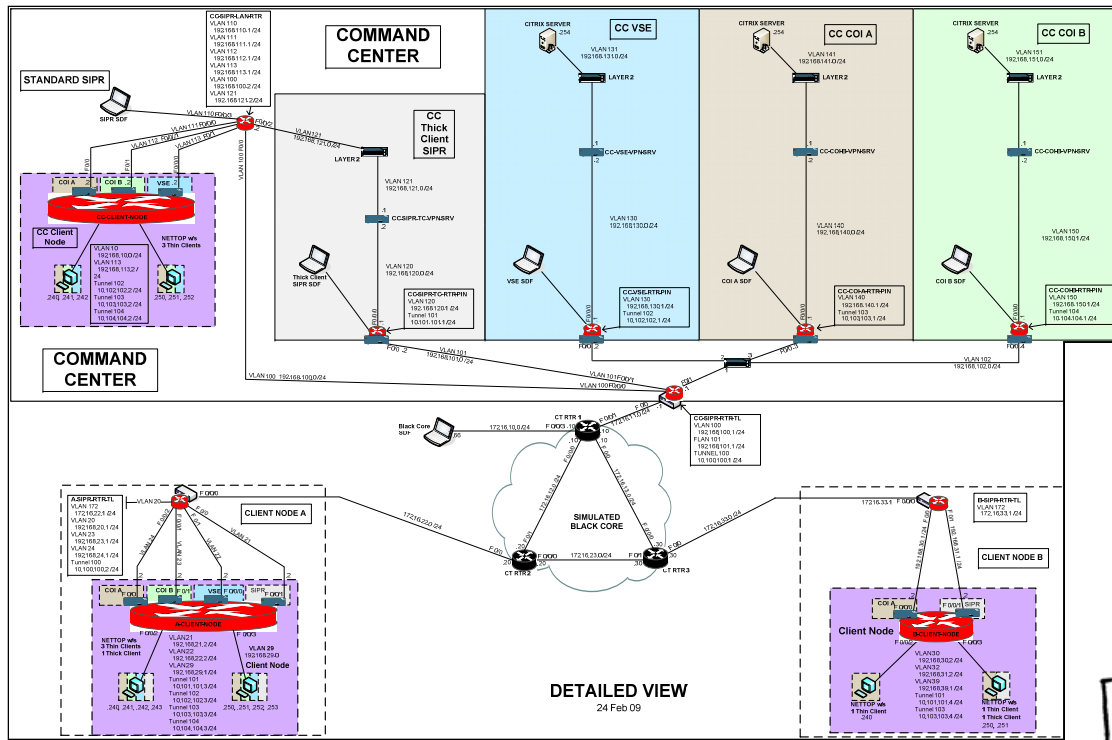
Configuration

Monitoring

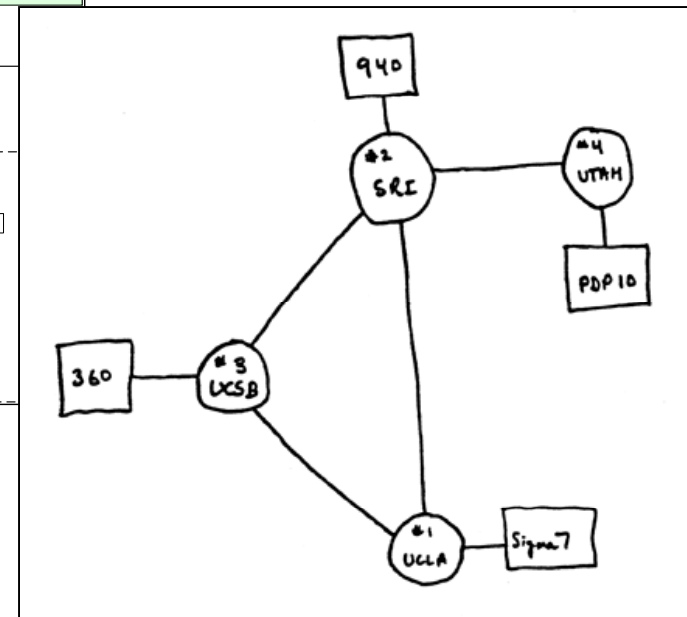
Historical Analysis

Visualization

Why Topology Based Visualization Model

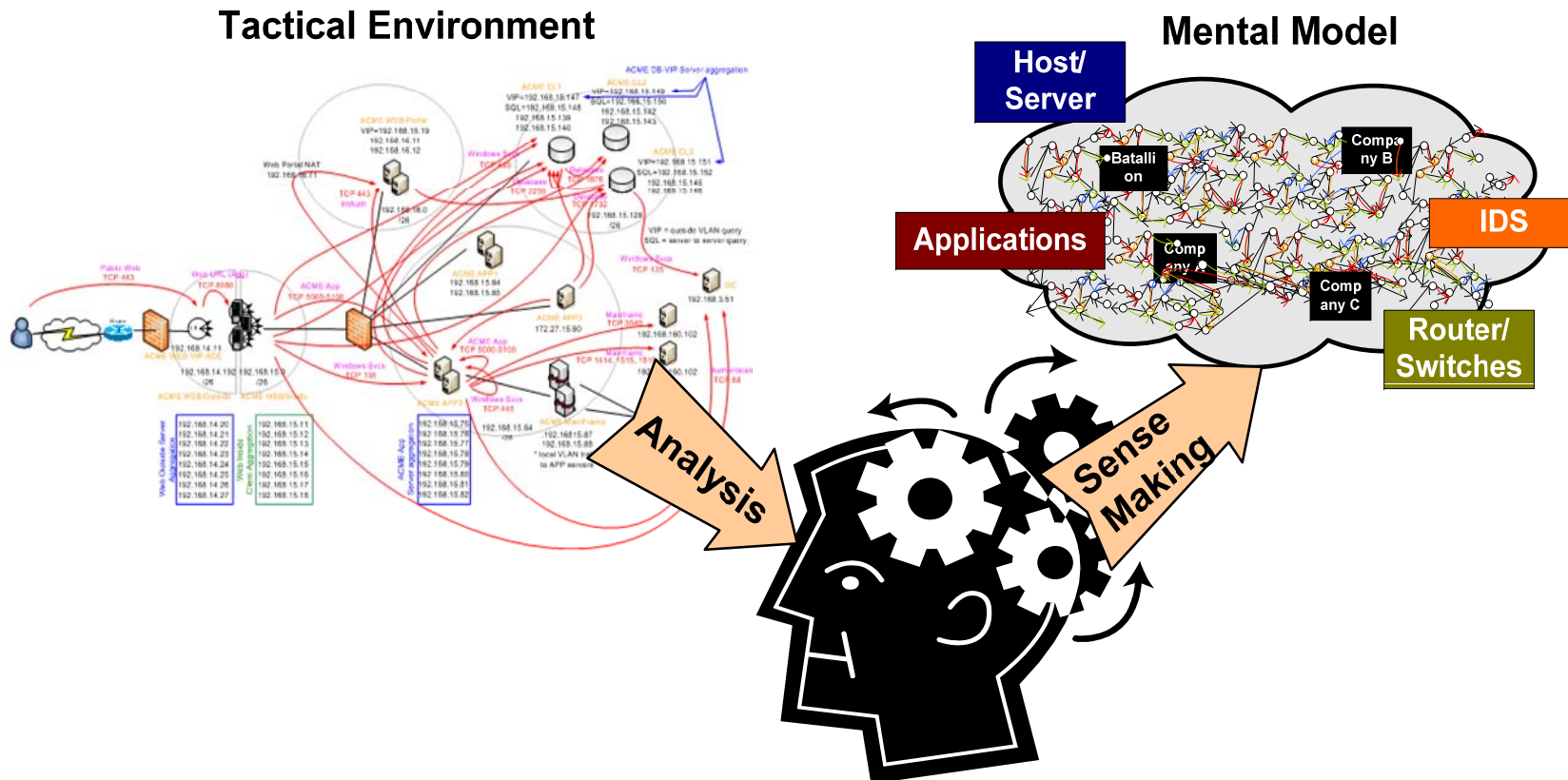


Hand Drawings

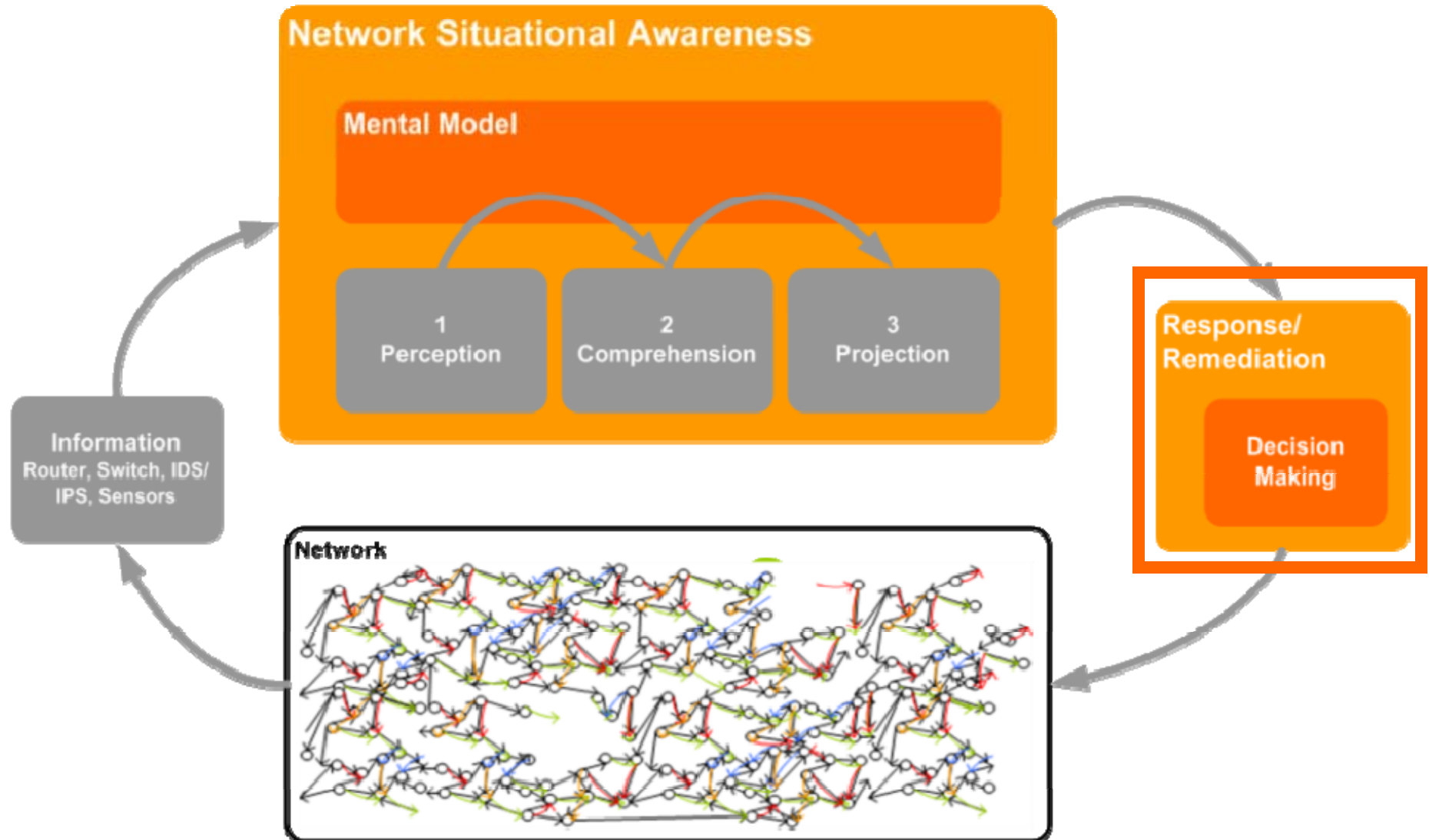


Visio Diagrams

- Can't interactively explore
- No correlation to live network data
- Not always accurate or kept current



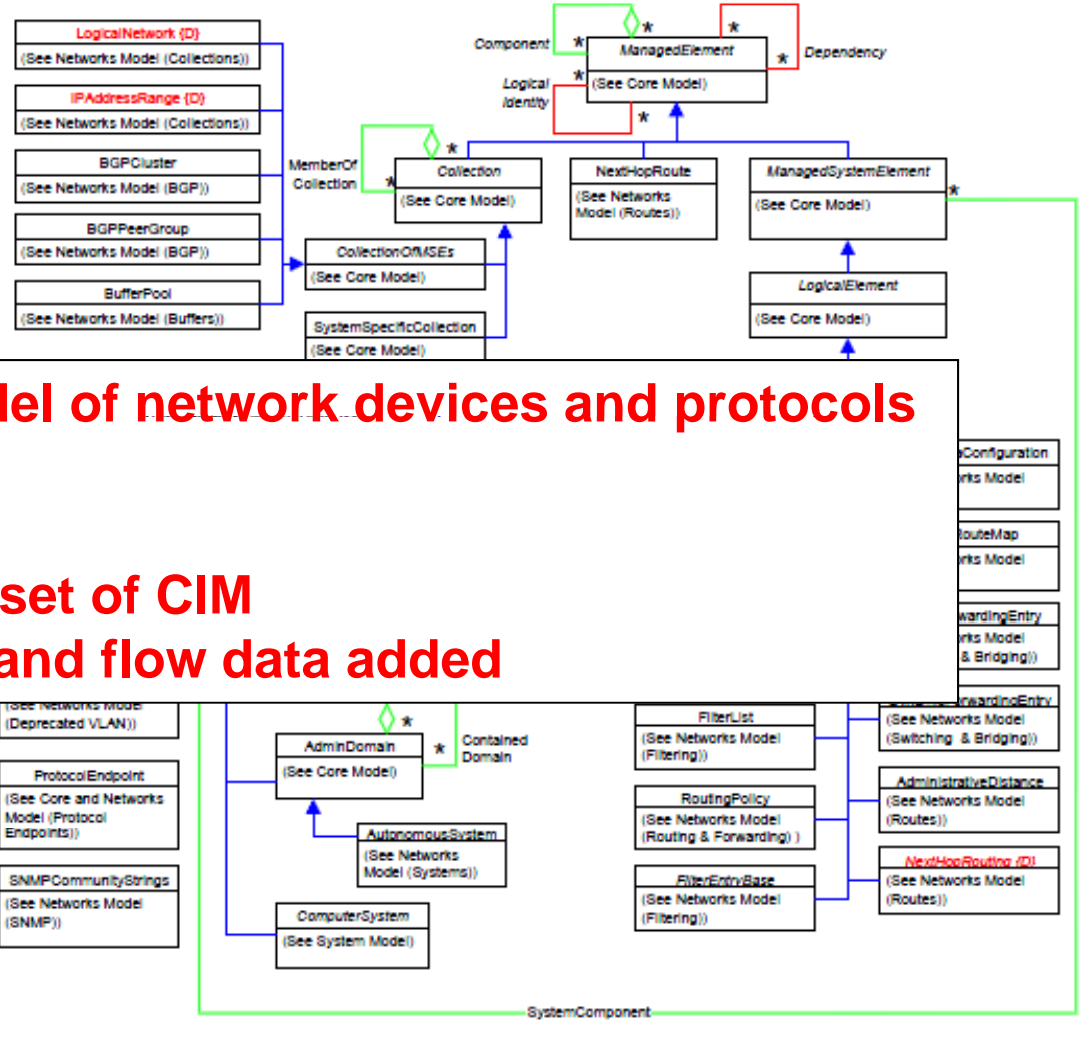
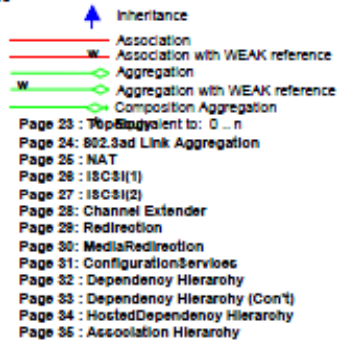
- Accuracy and fidelity of the model
- Ability to explore the model
- Interact with the model



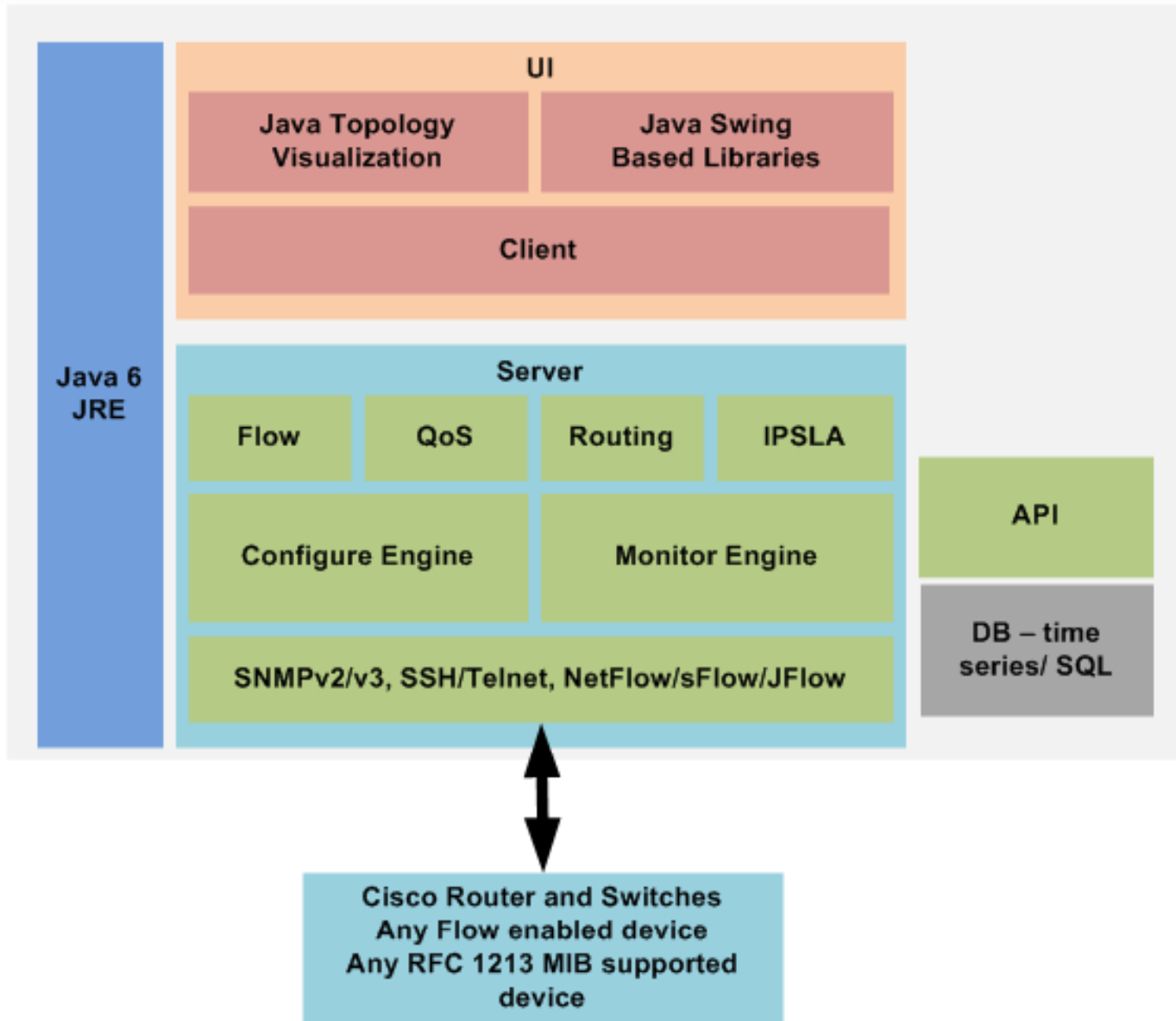
DMTF CIM Model

Title : Network Specification Version V2.18
 Author : DMTF Networks Working Group
 Updated : 21 April 2008

Page 1 : Overview
 Page 2 : Network Systems
 Page 3 : Network Collections
 Page 4 : Protocol Endpoints
 Page 5 : Protocol Endpoints (2)
 Page 6 : Protocol Endpoints (3)
 Page 7 : Routing and Forwarding
 Page 8 : Routes
 Page 9 : Pipes
 Page 10 : Filtering and Filter Entries
 Page 11 : Buffer Pools (Network Resources)
 Page 12 : SNMP
 Page 13 : OSPF
 Page 14 : BGP
 Page 15 : BGP (Continued)
 Page 16 : Switching and Bridging
 Page 17 : QoS
 Page 18 : QoS Conditioning
 Page 19 : IPsec
 Page 20 : VLAN
 Page 21 : MPLS(1)
 Page 22 : MPLS(2)



- Very detailed model of network devices and protocols
- Vendor neutral
- Currently we use
 - A simpler subset of CIM
 - Performance and flow data added

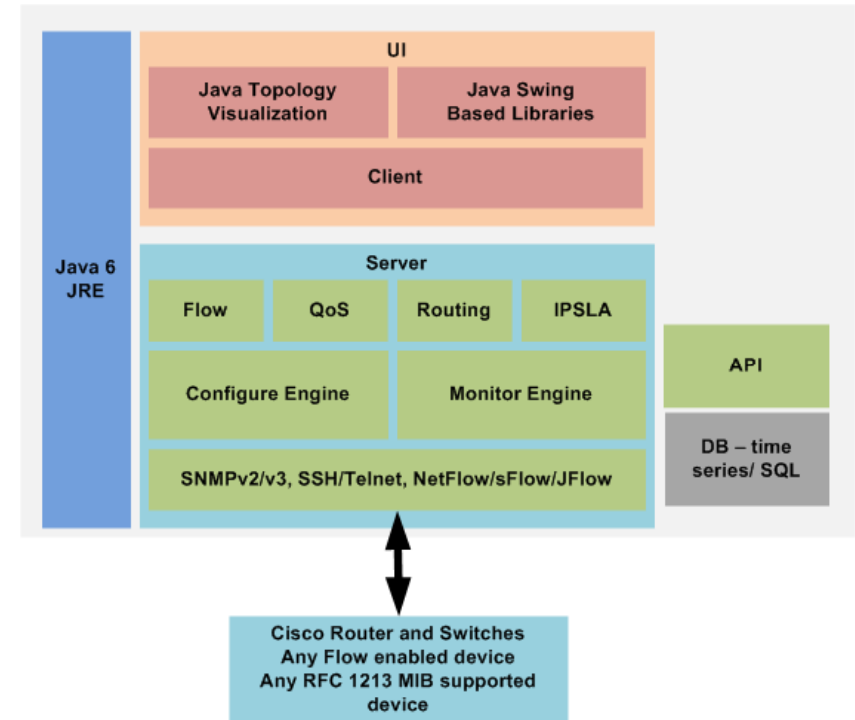


- **Flow Collector**

- Not generator like Argus or YAF
- Time series storage
- Netflow v5-v9, sFlow, Jflow
- Cisco Flexible Netflow setup

- **Flow Visualization**

- Topology from real networks
 - Discovery
 - Model creation from config
 - Node and edge displays
- Flow Projection
 - “Real Time” – as real time as NetFlow can be
 - Projection of flows onto topology



- **Network Management**

- Its really hard to know what's going on in a router
- Let alone across routers in a network
- Where problem locations are, where to fix

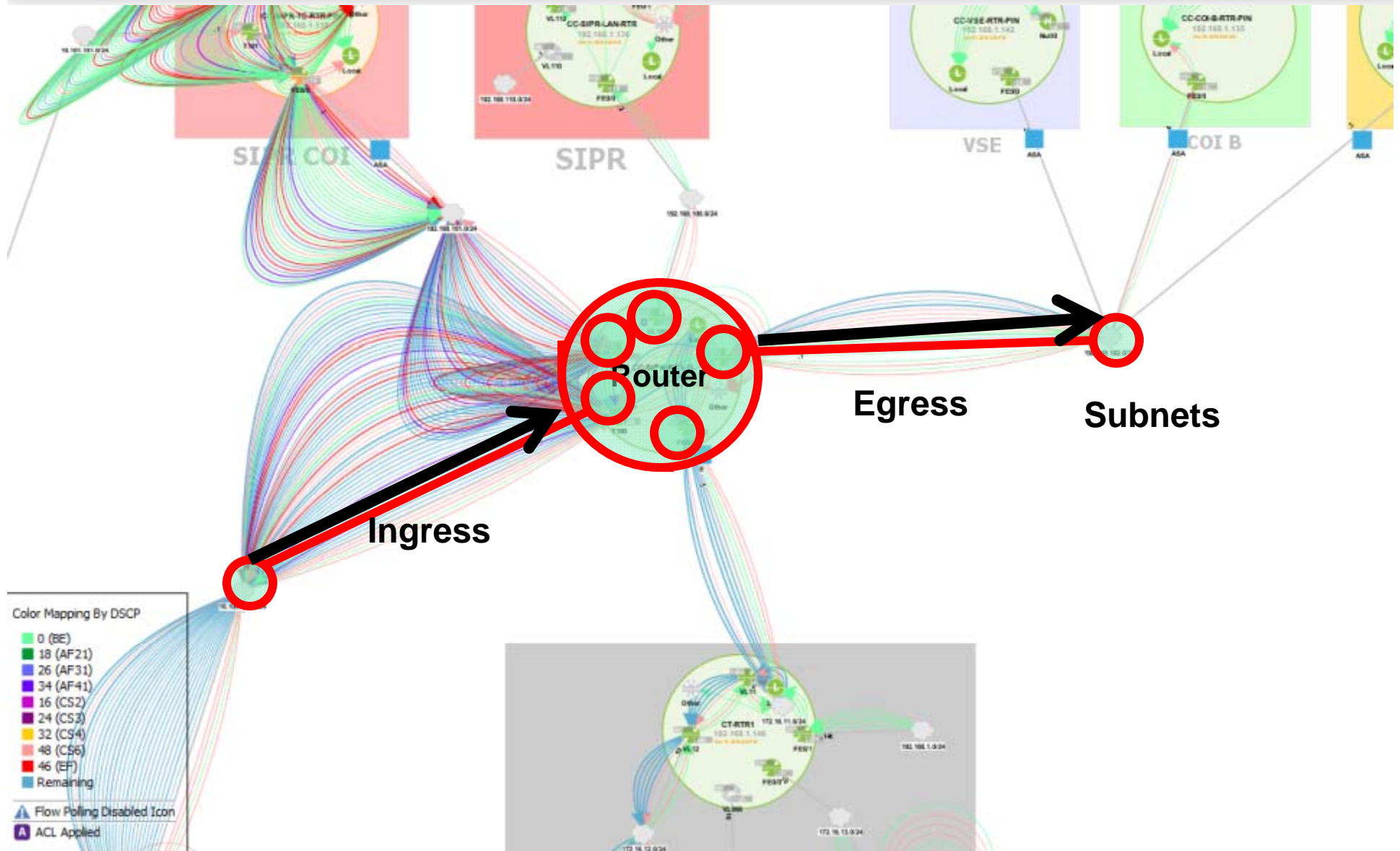
- **Network SA**

- Knowing how flows are routed
- Knowing direction, load sharing
- Flow – Routing – QoS – SLA

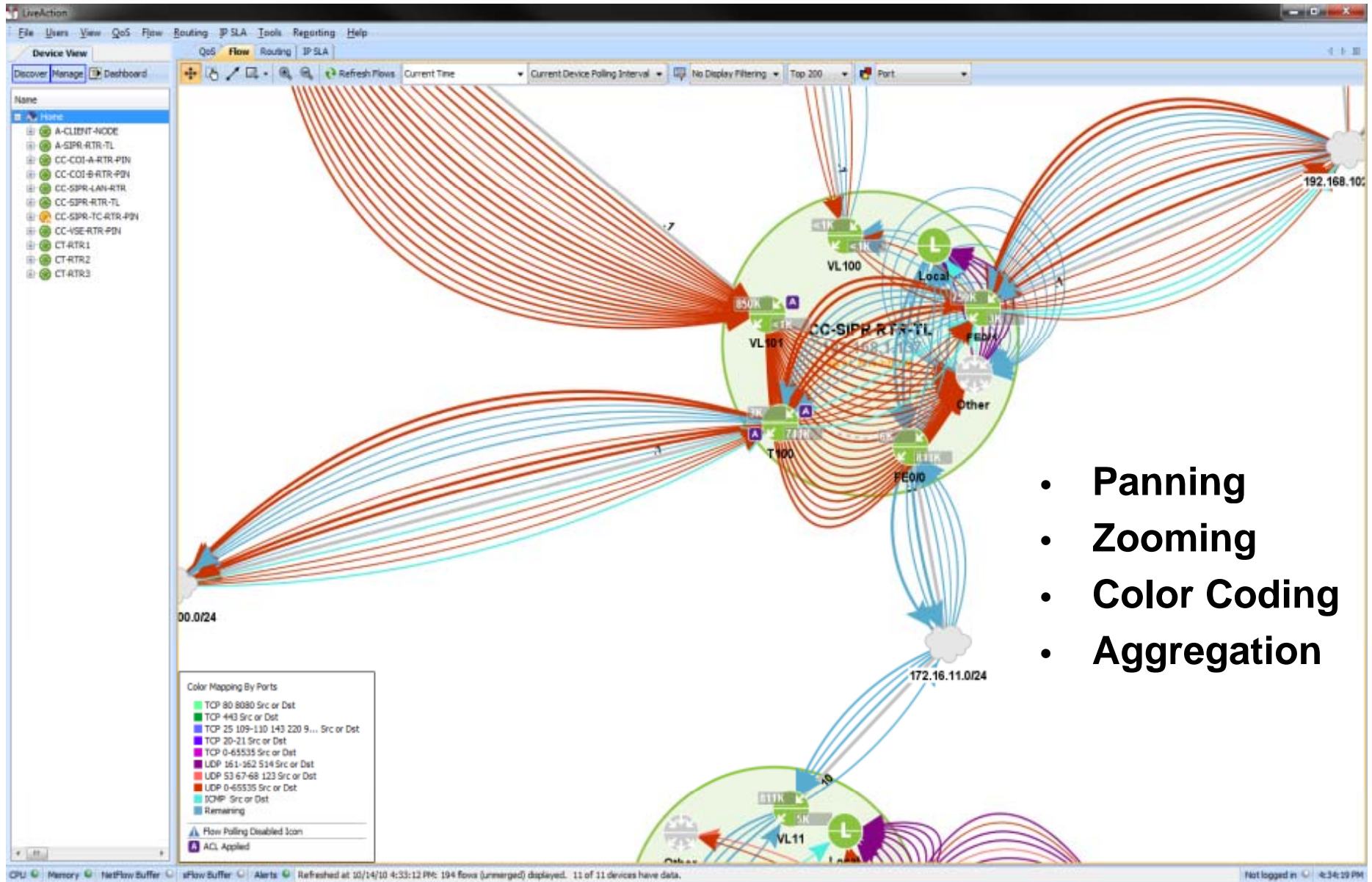
- **CND**

- **Doesn't solve finding needle in haystack problem**
- **Doesn't do pattern analysis**
- Can be used with sensors to alert and monitor events
- Response planning and actions
- Compliments forensic analysis

Flow System View



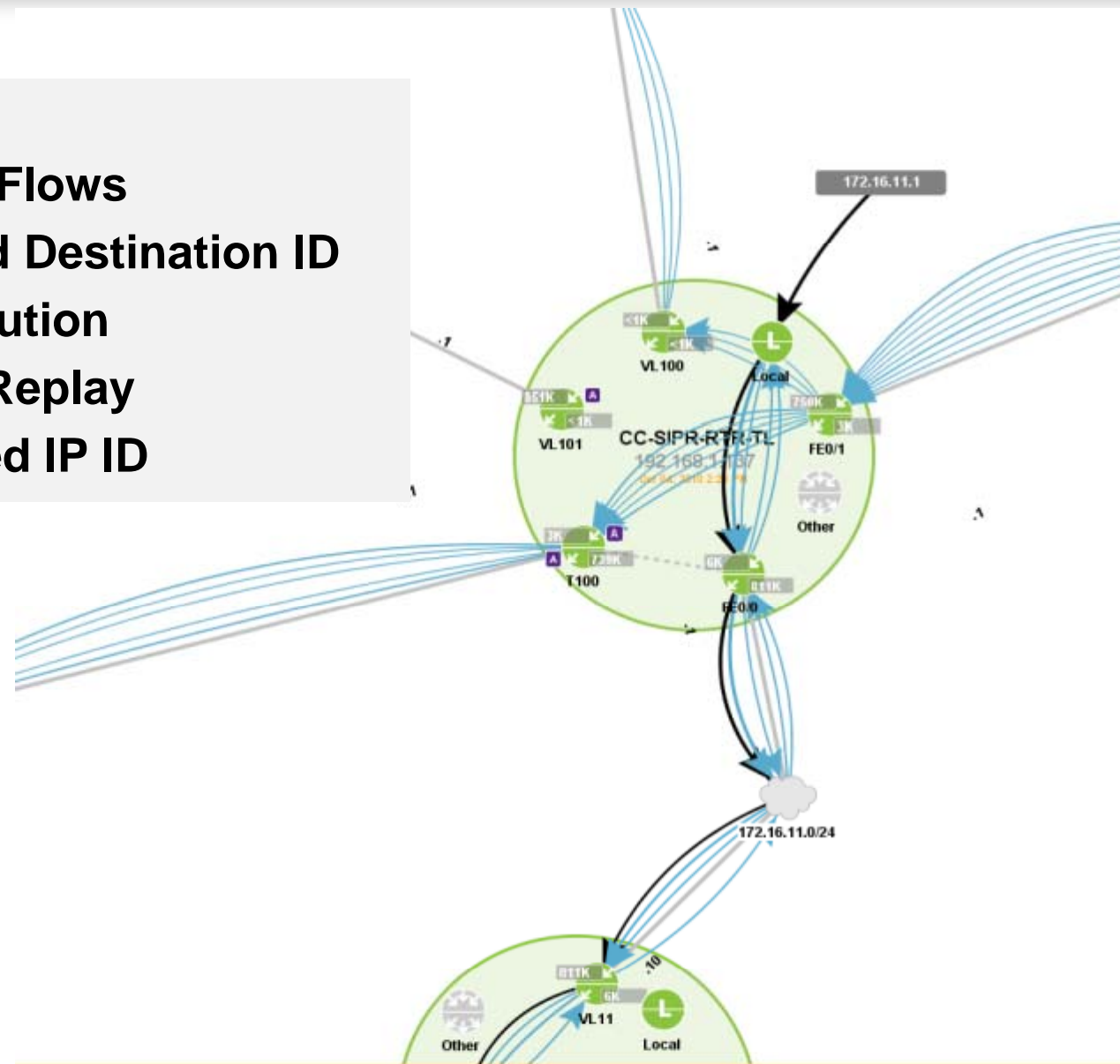
Flow System View



- Panning
- Zooming
- Color Coding
- Aggregation

Flow System View

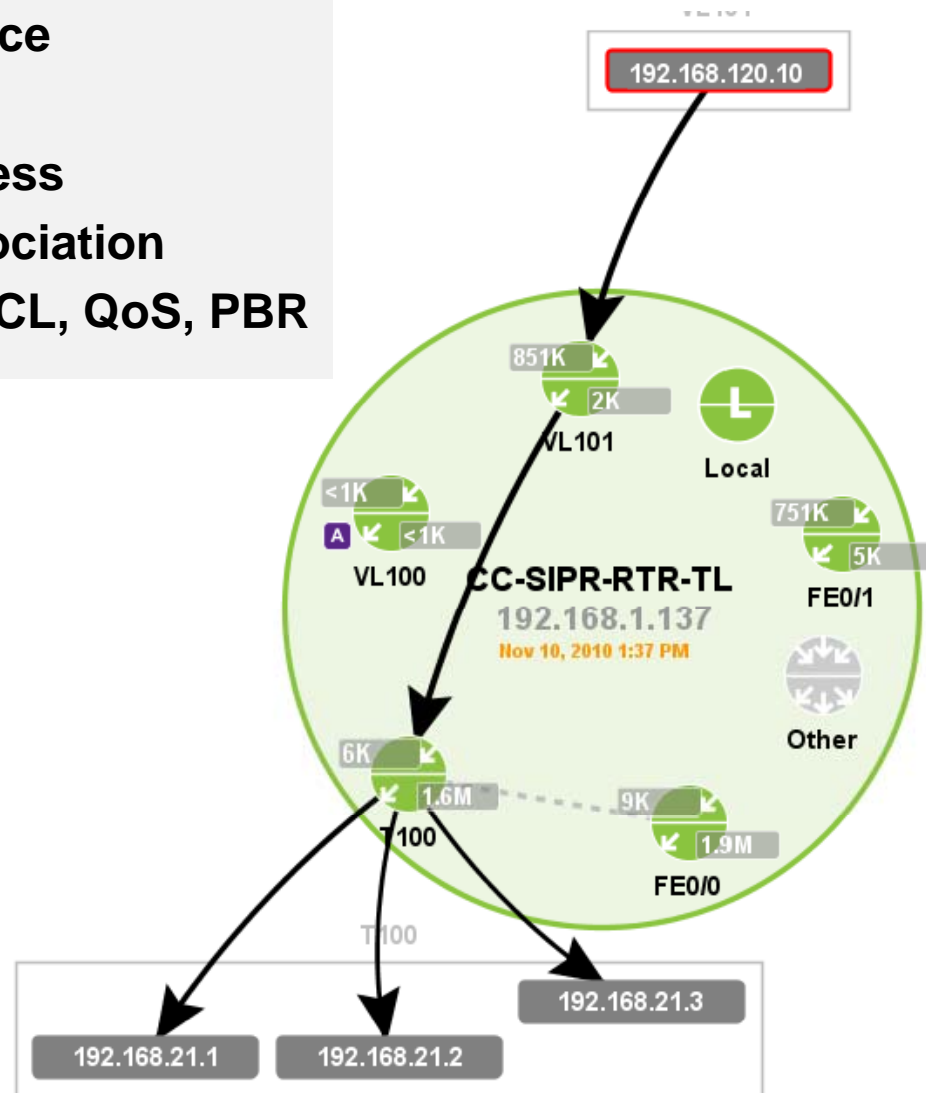
- Filtering
- Tracing of Flows
- Source and Destination ID
- DNS Resolution
- Historical Replay
- Black Listed IP ID



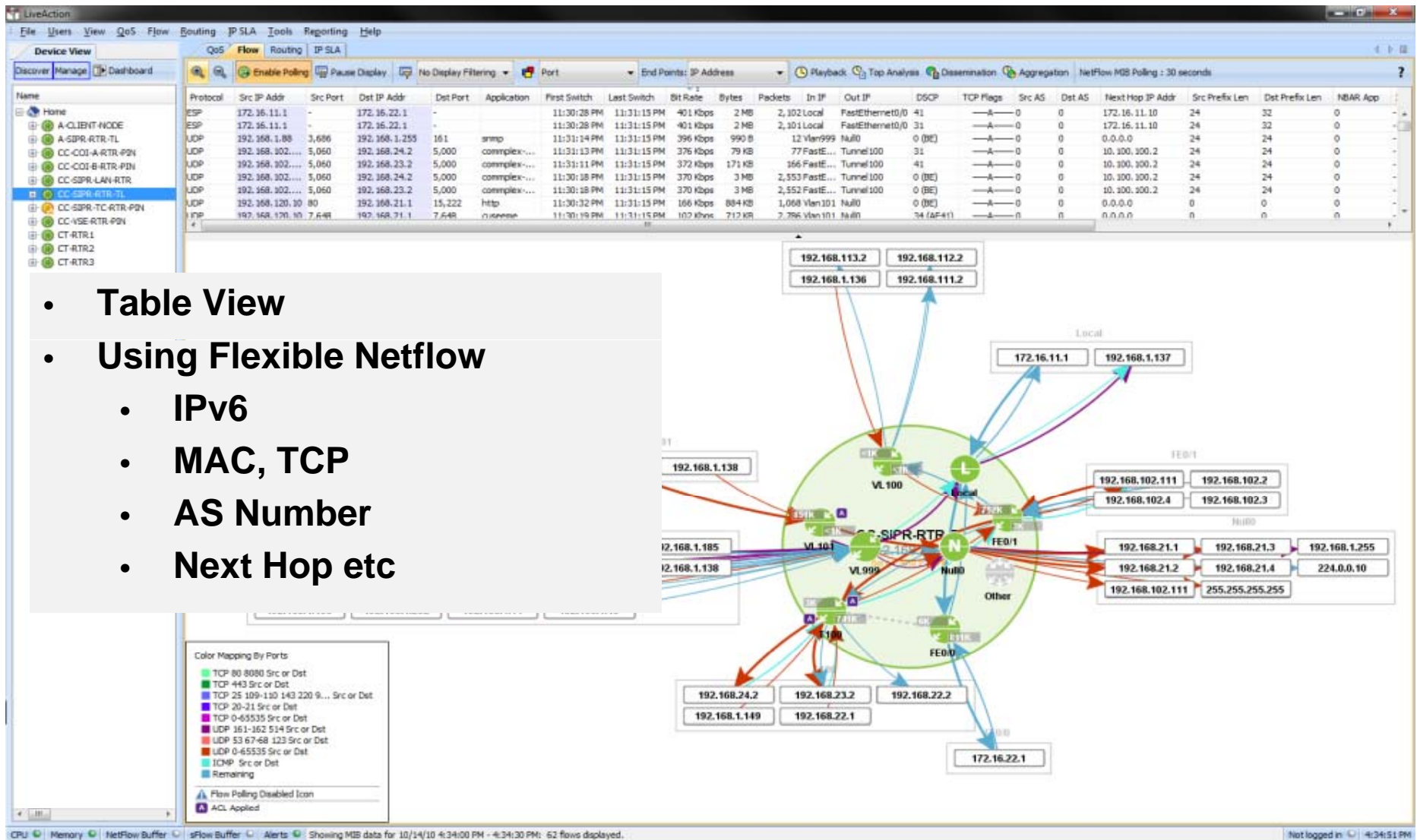
3:12 PM: 15 flows (unmerged) displayed. 11 of 11 devices have data.

Individual Flow

- Isolation down to particular source
- Aggregation along shared path
- Highlighting of black listed address
- Tunnel to physical interface association
- Indicators for policies such as ACL, QoS, PBR



Device Topology View



The screenshot displays the LiveAction interface with a table of network flows and a device topology diagram. The table view shows various protocols, IP addresses, ports, applications, and traffic statistics. The topology diagram illustrates the network structure, including a central router (CC-SIPR-RTP) and various interfaces connected to different IP addresses.

Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	First Switch	Last Switch	Bit Rate	Bytes	Packets	In IP	Out IP	DSCP	TCP Flags	Src AS	Dest AS	Next Hop IP Addr	Src Prefix Len	Dst Prefix Len	NBAR App
ESP	172.16.11.1	-	172.16.22.1	-	-	11:30:28 PM	11:31:15 PM	401 Kbps	2 MB	2,102	Local	FastEthernet0/0	41	-A-0-0	0	0	172.16.11.10	24	32	0
ESP	172.16.11.1	-	172.16.22.1	-	-	11:30:28 PM	11:31:15 PM	401 Kbps	2 MB	2,101	Local	FastEthernet0/0	31	-A-0-0	0	0	172.16.11.10	24	32	0
UDP	192.168.1.88	3,686	192.168.1.253	161	snmp	11:31:14 PM	11:31:15 PM	396 Kbps	990 B	12	Vlan999	Null0	0 (BE)	-A-0-0	0	0	0.0.0.0	24	24	0
UDP	192.168.302...	5,060	192.168.24.2	5,000	complex...	11:31:13 PM	11:31:15 PM	376 Kbps	79 KB	77	FastE...	Tunnel100	31	-A-0-0	0	0	10.100.100.2	24	24	0
UDP	192.168.302...	5,060	192.168.23.2	5,000	complex...	11:31:11 PM	11:31:15 PM	372 Kbps	171 KB	166	FastE...	Tunnel100	41	-A-0-0	0	0	10.100.100.2	24	24	0
UDP	192.168.302...	5,060	192.168.24.2	5,000	complex...	11:30:18 PM	11:31:15 PM	370 Kbps	3 MB	2,553	FastE...	Tunnel100	0 (BE)	-A-0-0	0	0	10.100.100.2	24	24	0
UDP	192.168.302...	5,060	192.168.23.2	5,000	complex...	11:30:18 PM	11:31:15 PM	370 Kbps	3 MB	2,552	FastE...	Tunnel100	0 (BE)	-A-0-0	0	0	10.100.100.2	24	24	0
UDP	192.168.120.10	80	192.168.21.1	15,222	http	11:30:32 PM	11:31:15 PM	166 Kbps	884 KB	1,068	Vlan101	Null0	0 (BE)	-A-0-0	0	0	0.0.0.0	0	0	0
UDP	192.168.120.10	7,648	192.168.21.1	7,648	no sense	11:30:19 PM	11:31:15 PM	107 Kbps	717 KB	2,786	Vlan101	Null0	34 (AF41)	-A-0-0	0	0	0.0.0.0	0	0	0

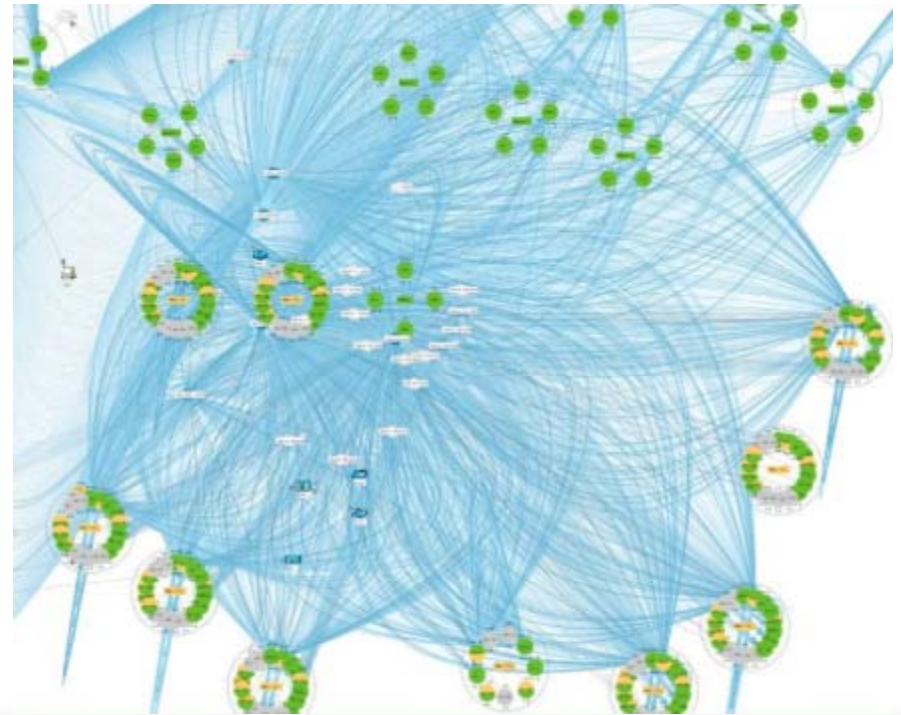
- Table View
- Using Flexible Netflow
 - IPv6
 - MAC, TCP
 - AS Number
 - Next Hop etc

- **Static display easier, real time* is harder**
- **How long to leave flows displayed**
 - Process flow records as they come in
 - Update/Refresh rate of the display – 10 sec
 - Aging of the flows out of the display
 - Router – active/inactive timer settings

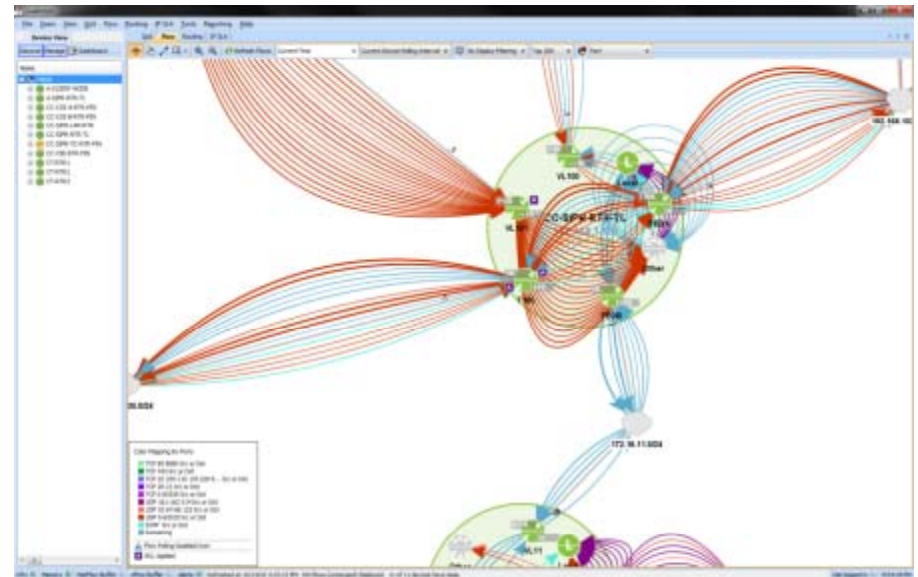
	Poll	Aging	Time																												
	10 sec	2 min	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#	#
40 sec flow			real flow			X																									
							aging																								
2 min flow			real flow						X																						
								aging							aging																
4 min flow			real flow						X																						
									X	aging					X	aging															

Active Timer 1 min
Inactive Timer 10 sec

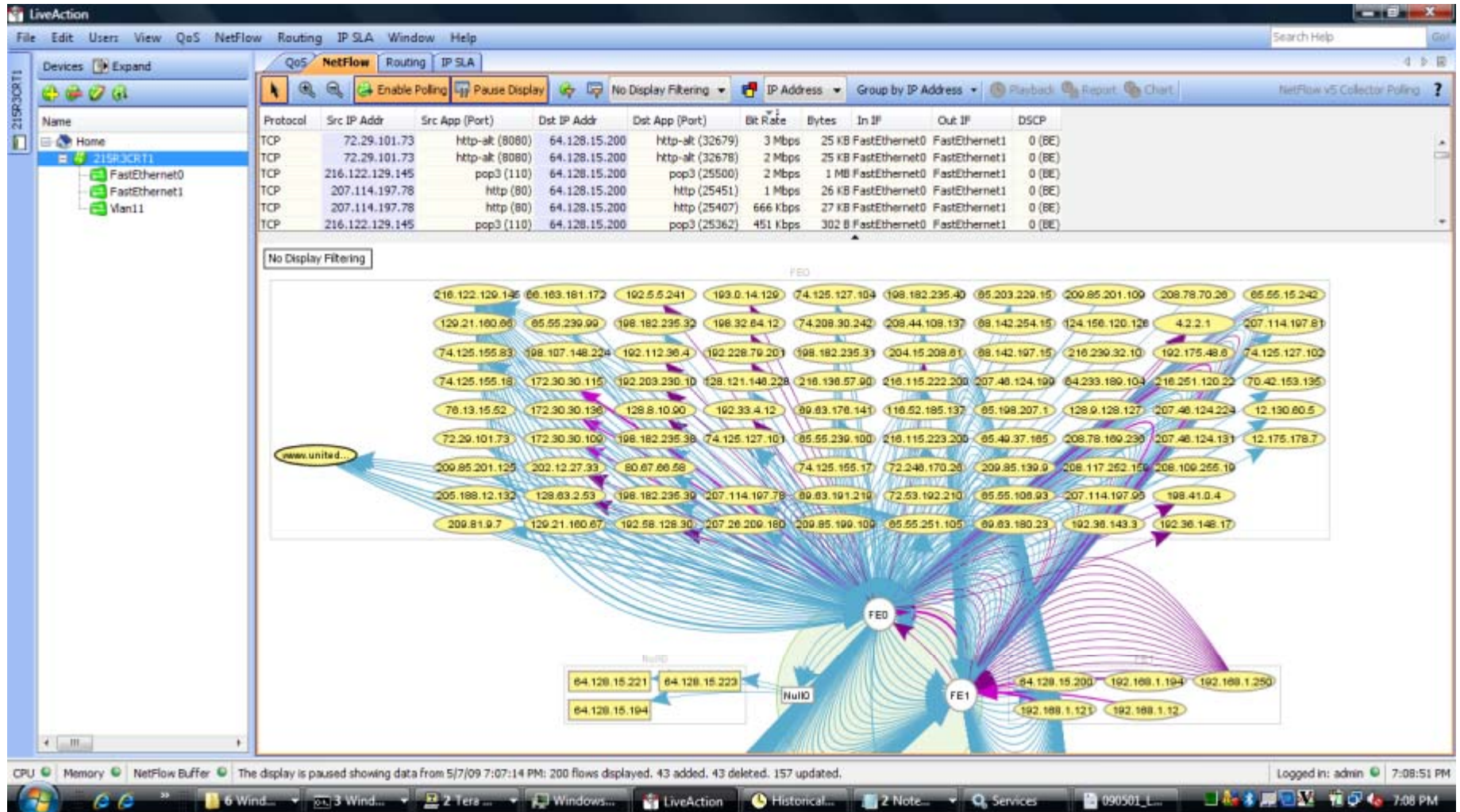
- **Issues**
 - Shear number of flows
 - Efficient storage and retrieval for display
 - Temporal aspect of flows
 - Display layer performance
- **Top N or Bottom N Flows**
 - Reduce amount of displayed items
 - Aggregation of same flow records
- **Merging**
 - Merge flows based on attributes
 - DSCP, IP address, Rate, Bytes
 - Match based
- **Filtering**
 - Basic - src/dst ip, port, dscp etc
 - Advanced – BGP AS, next hop, ..



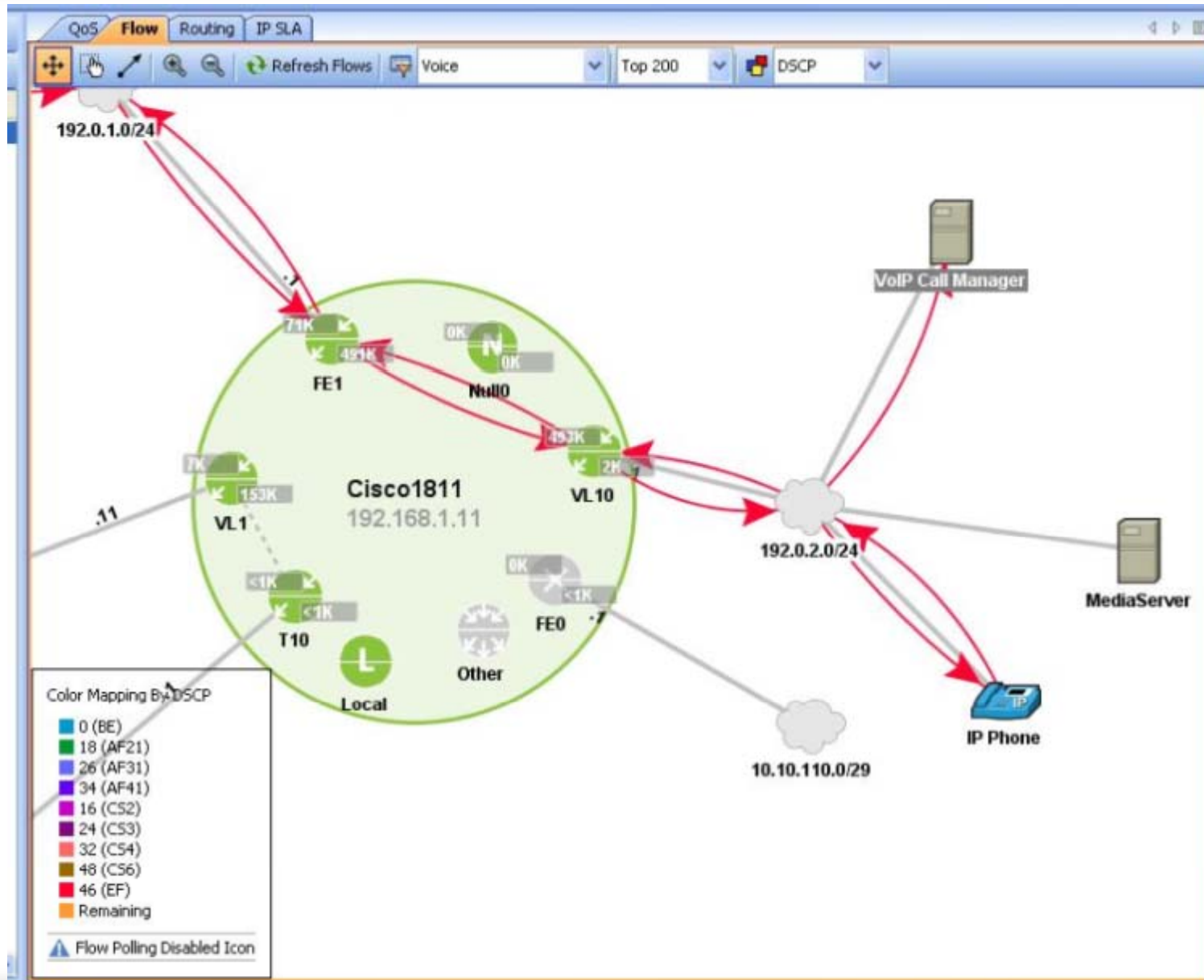
- **Flow Data**
 - Router sourced or consumed flows
 - Index to interface number mapping, Null/Local
 - Not always correct, MIB issues
- **Differences**
 - ASA vs Router vs Switch
 - Intra VLAN, Layer 3
 - NetFlow and sFlow
 - SNMP based flow
- **Time Related**
 - Flow time outs – active/inactive
 - Flow time stamps
- **NetFlow configuration**
 - Flexible NetFlow



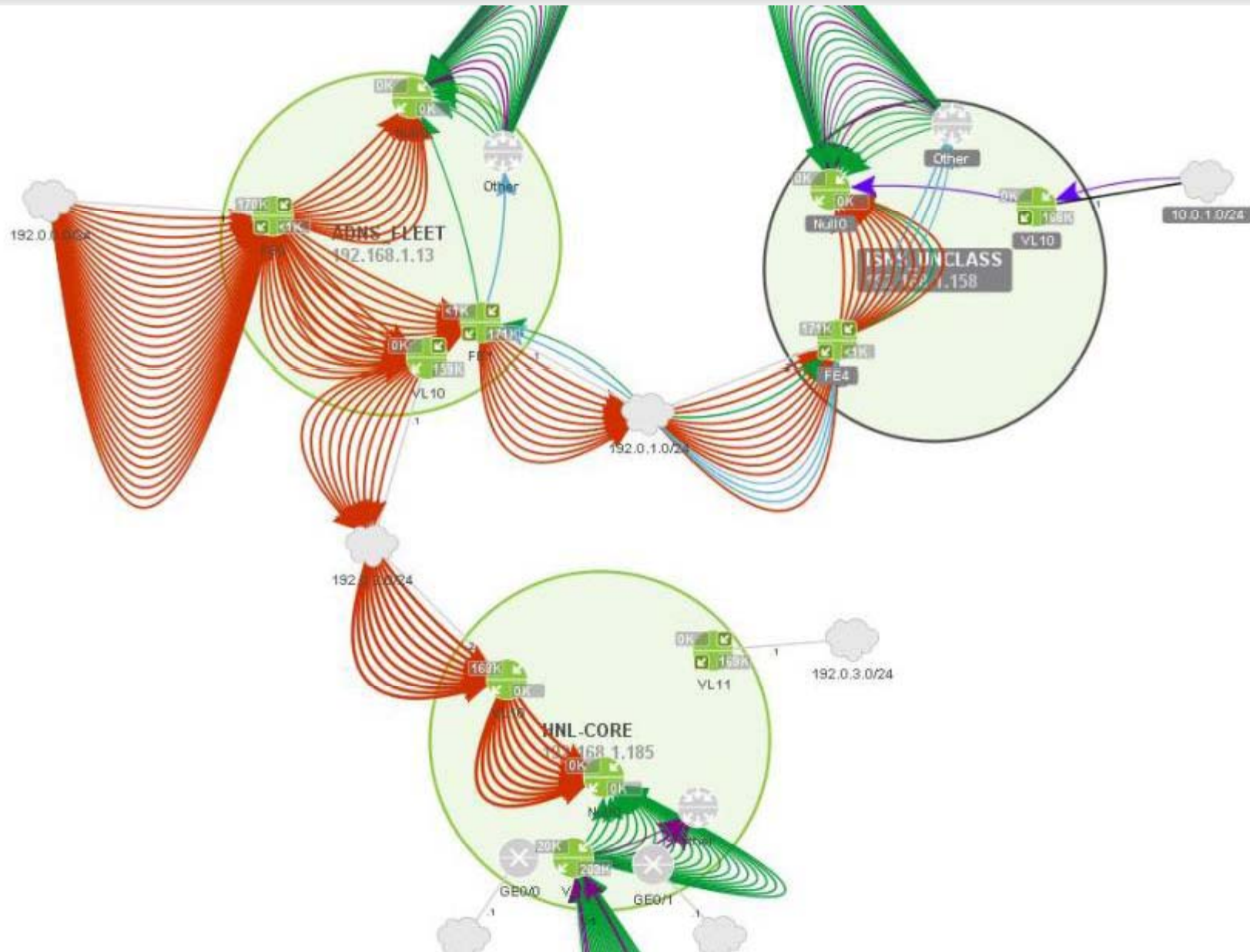
Visualization - Scanning

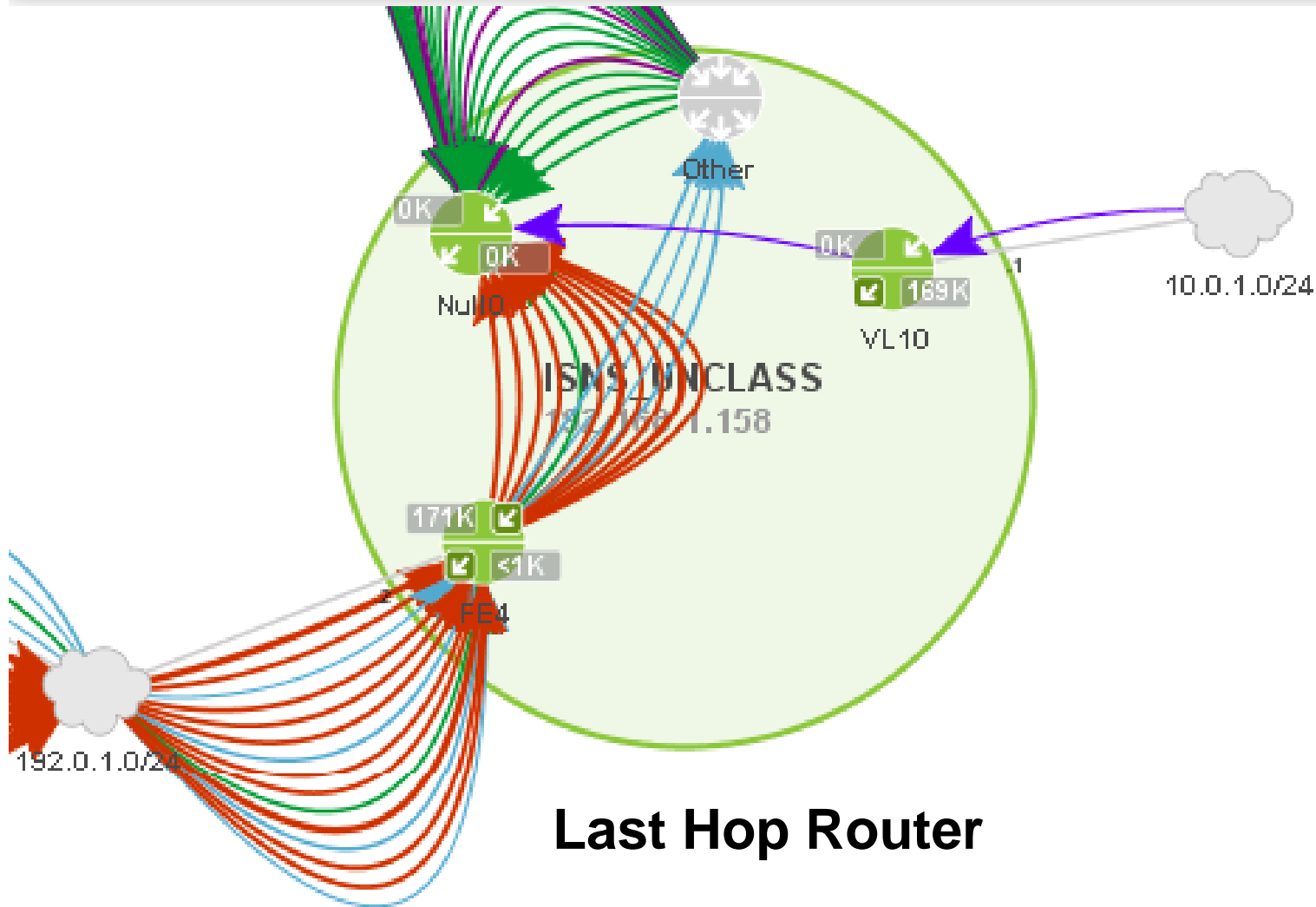


Visualization - VoIP Call Tracing



Visualization - Multicast Traffic

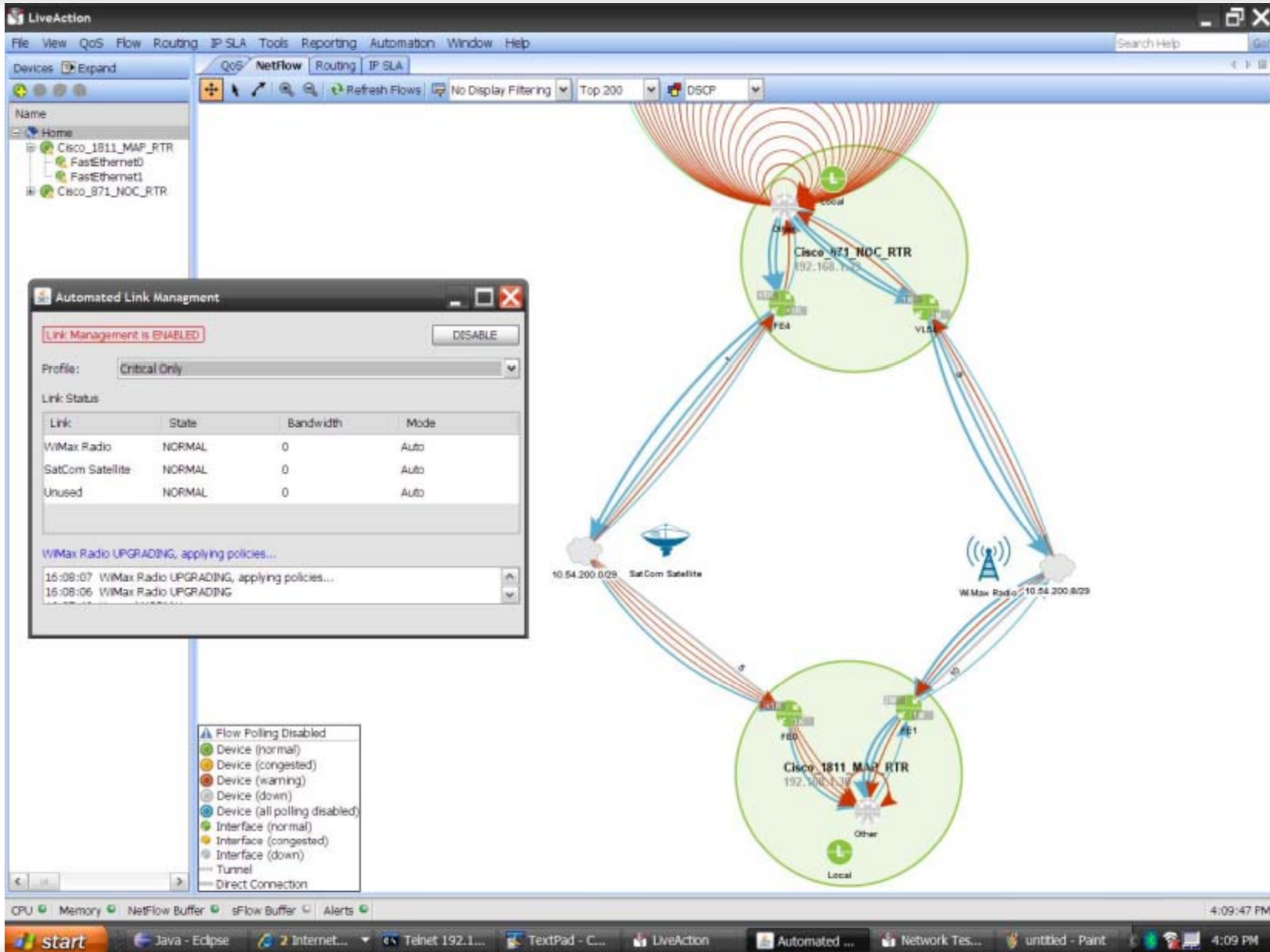




Last Hop Router

- Egress flows not showing
- Traffic shown as going to Null but really router CPU

Visualization - Load Sharing



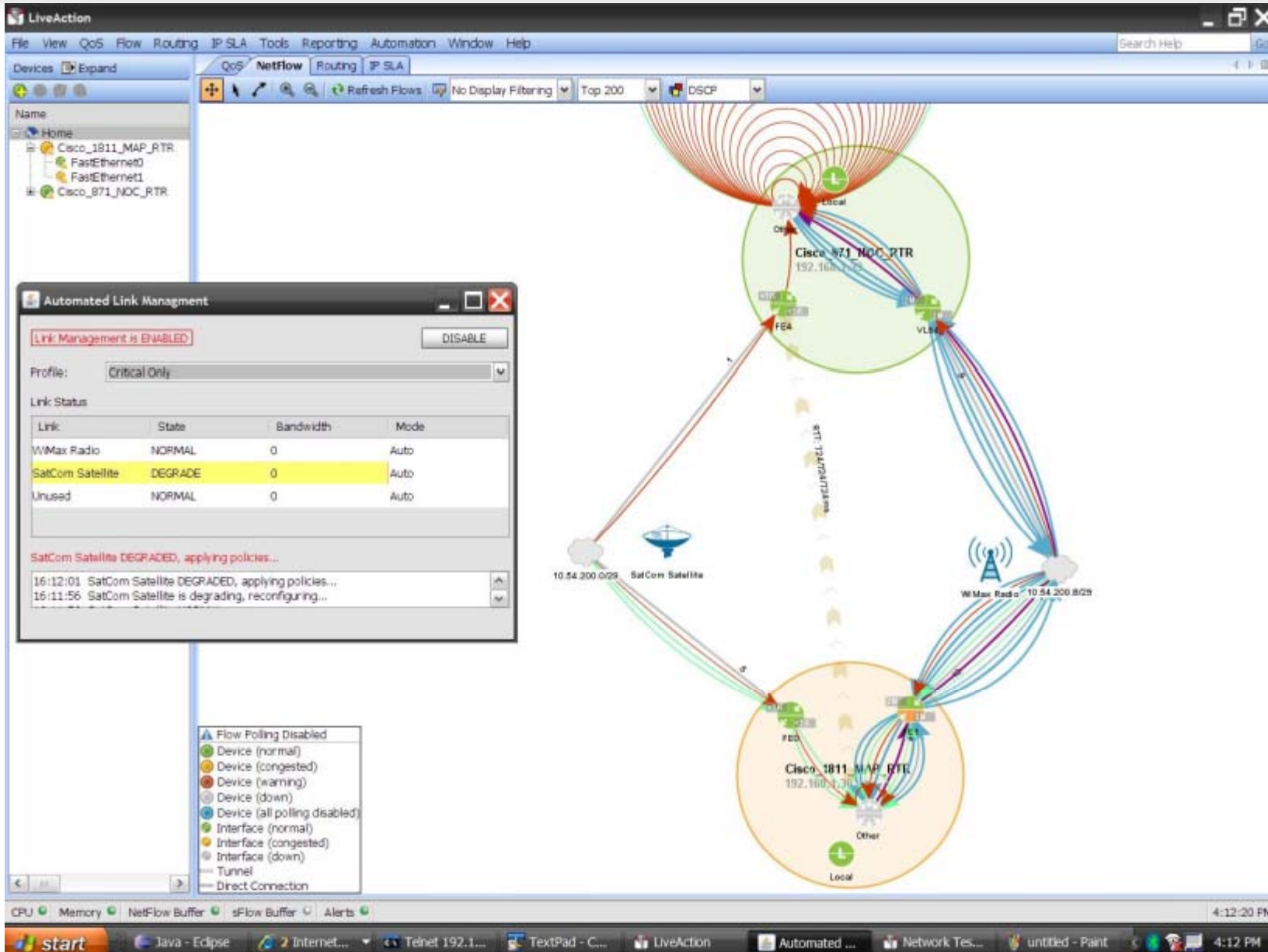
The screenshot displays the LiveAction network management interface. The main window shows a network topology with three routers: Cisco_1811_MAP_RTR (IP: 192.168.1.1), Cisco_871_NOC_RTR (IP: 192.168.1.2), and Cisco_1811_MAP_RTR (IP: 192.168.1.3). The routers are interconnected via various interfaces (FastEthernet0, FastEthernet1, E0/0, E1). The network is connected to external links: SatCom Satellite (IP: 10.54.200.0/29) and WiMax Radio (IP: 10.54.200.8/29). The interface shows a legend for link status, including 'Flow Polling Disabled', 'Device (normal)', 'Device (congested)', 'Device (warning)', 'Device (down)', 'Device (all polling disabled)', 'Interface (normal)', 'Interface (congested)', 'Interface (down)', 'Tunnel', and 'Direct Connection'. The 'Automated Link Management' window is open, showing 'Link Management is ENABLED' and a table of link status.

Link	State	Bandwidth	Mode
WiMax Radio	NORMAL	0	Auto
SatCom Satellite	NORMAL	0	Auto
Unused	NORMAL	0	Auto

Log messages in the Automated Link Management window:

- 16:08:07 WiMax Radio UPGRADING, applying policies...
- 16:08:06 WiMax Radio UPGRADING

Visualization - Load Sharing



The screenshot displays the LiveAction network management interface. The main window shows a network diagram with several nodes and connections. The nodes include:

- Cisco_1811_MAP_RTR (192.168.1.30) - Local
- Cisco_871_NOC_RTR (192.168.1.75) - Local
- SatCom Satellite (10.54.200.0/29)
- WMax Radio (10.54.200.8/29)

The diagram shows connections between these nodes, with various colored lines representing different links or flows. A legend at the bottom left of the diagram area lists various status icons: Device (normal), Device (congested), Device (warning), Device (down), Device (all polling disabled), Interface (normal), Interface (congested), Interface (down), Tunnel, and Direct Connection.

An "Automated Link Management" window is open in the foreground, showing the following details:

- Link Management is ENABLED
- Profile: Critical Only
- Link Status table:

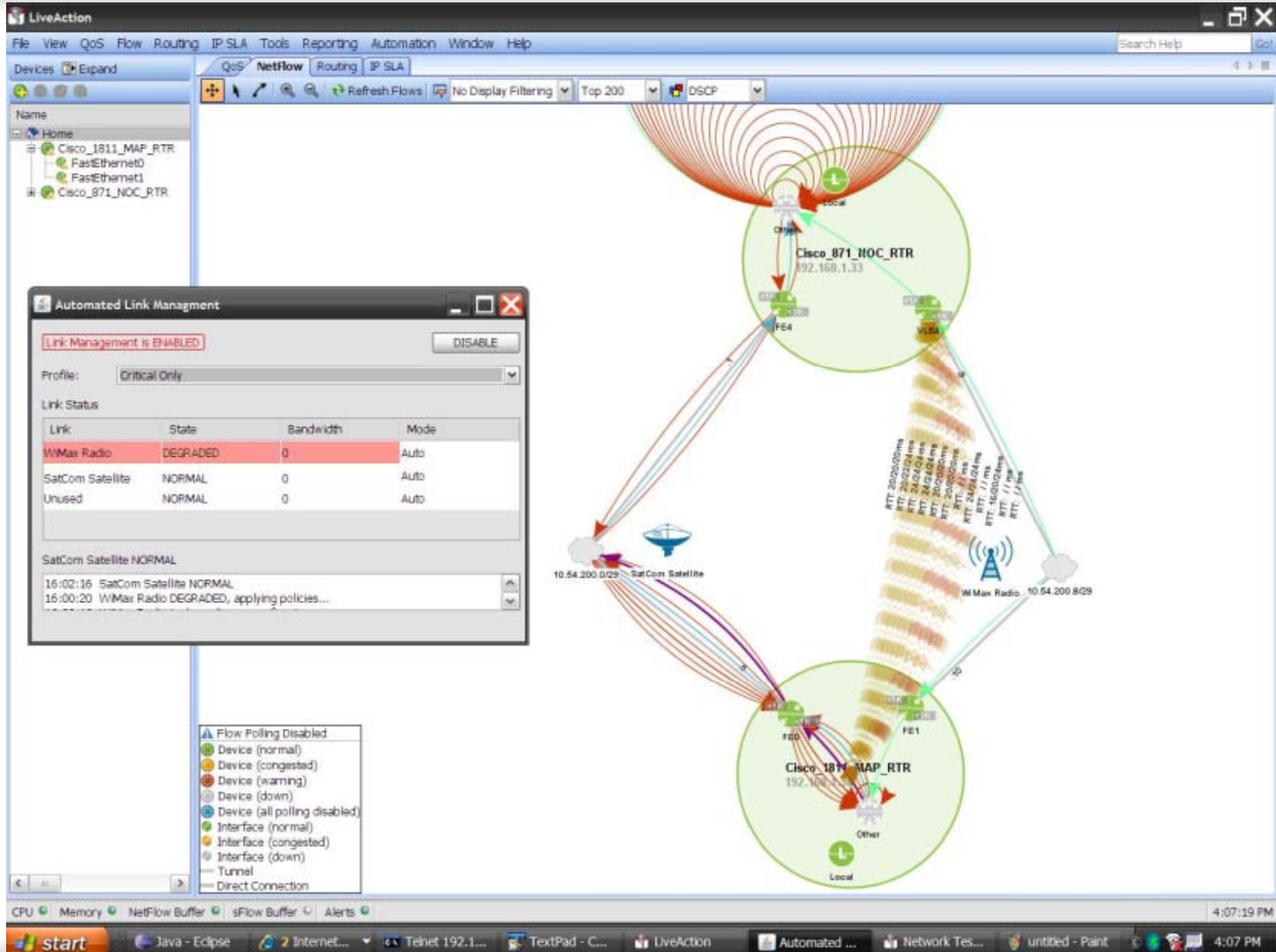
Link	State	Bandwidth	Mode
WMax Radio	NORMAL	0	Auto
SatCom Satellite	DEGRADE	0	Auto
Unused	NORMAL	0	Auto

Below the table, a log shows the following messages:

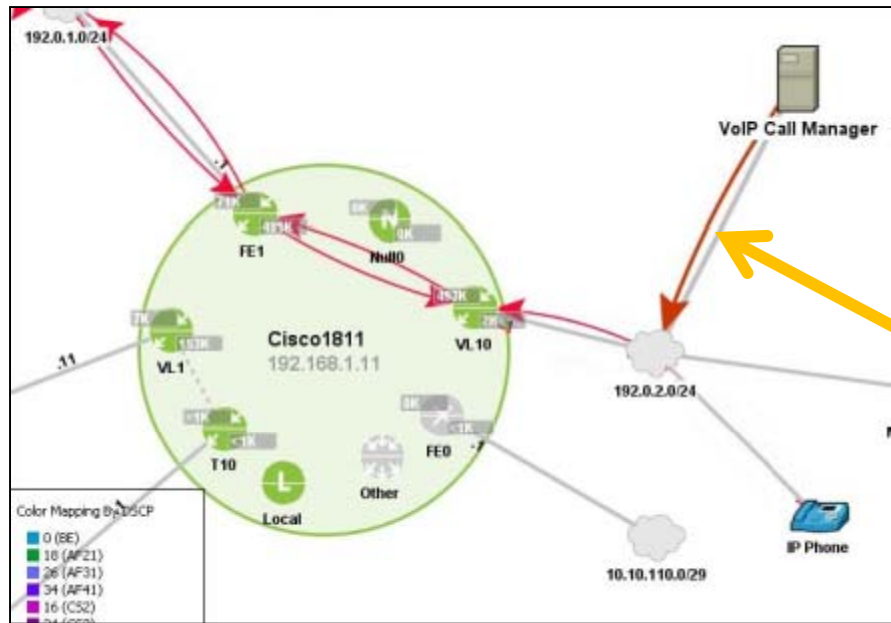
- SatCom Satellite DEGRADED, applying policies...
- 16:12:01 SatCom Satellite DEGRADED, applying policies...
- 16:11:56 SatCom Satellite is degrading, reconfiguring...

The bottom of the screenshot shows the Windows taskbar with the following open applications: Java - Eclipse, Internet..., Telnet 192.1..., TextPad - C..., LiveAction, Automated ..., Network Tes..., and untitled - Paint. The system clock shows 4:12 PM.

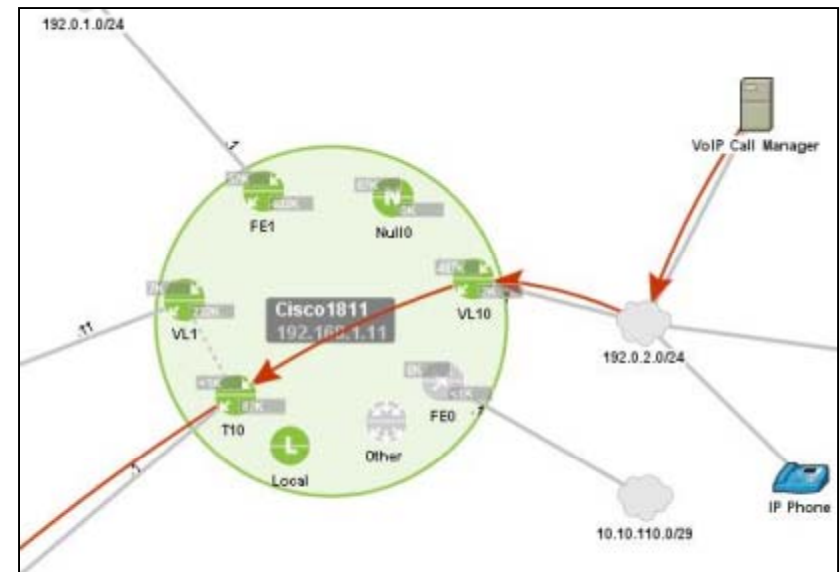
Visualization - Load Sharing

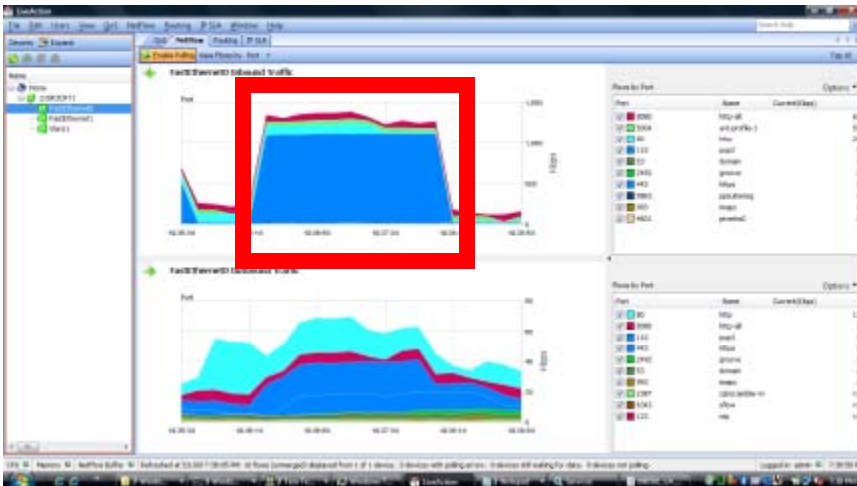
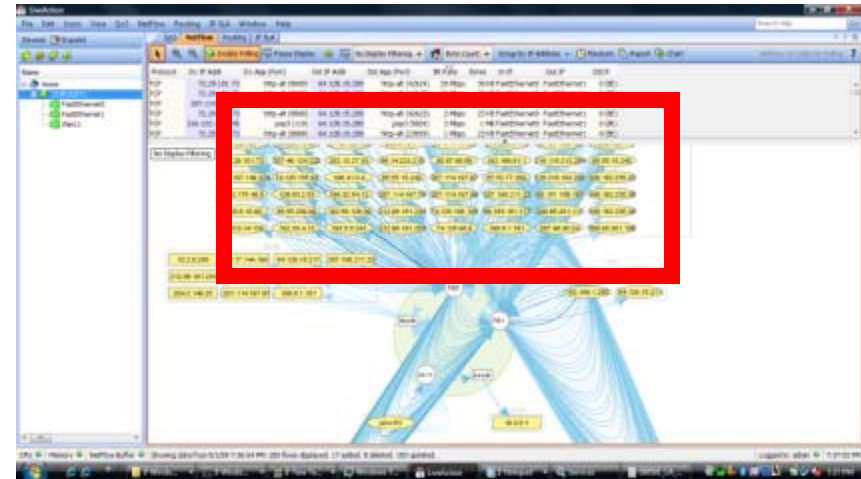
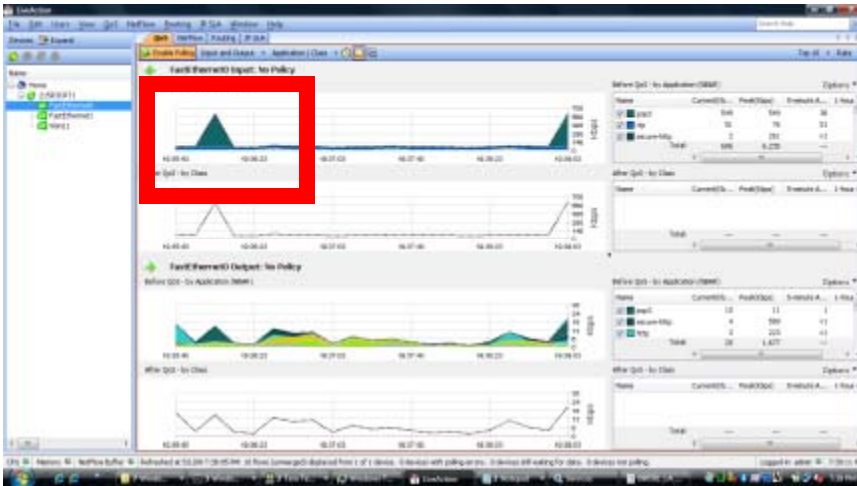


Interactions with Flows



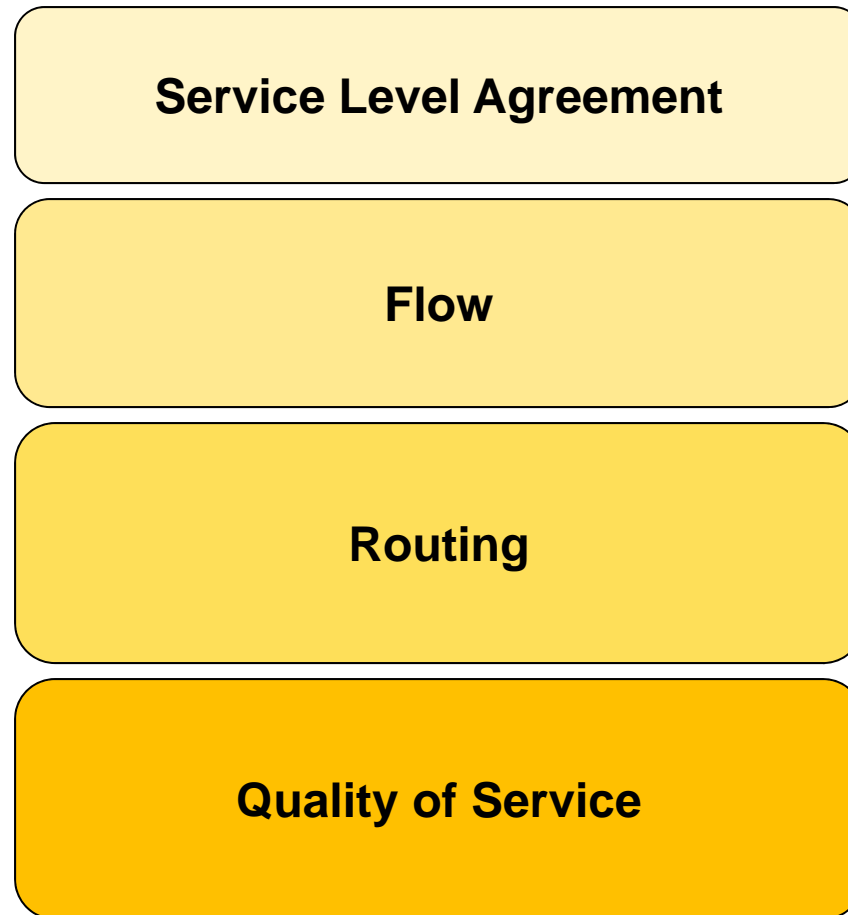
- 1) Identify flow visually
- 2) Create ACL
- 3) ACL for PBR



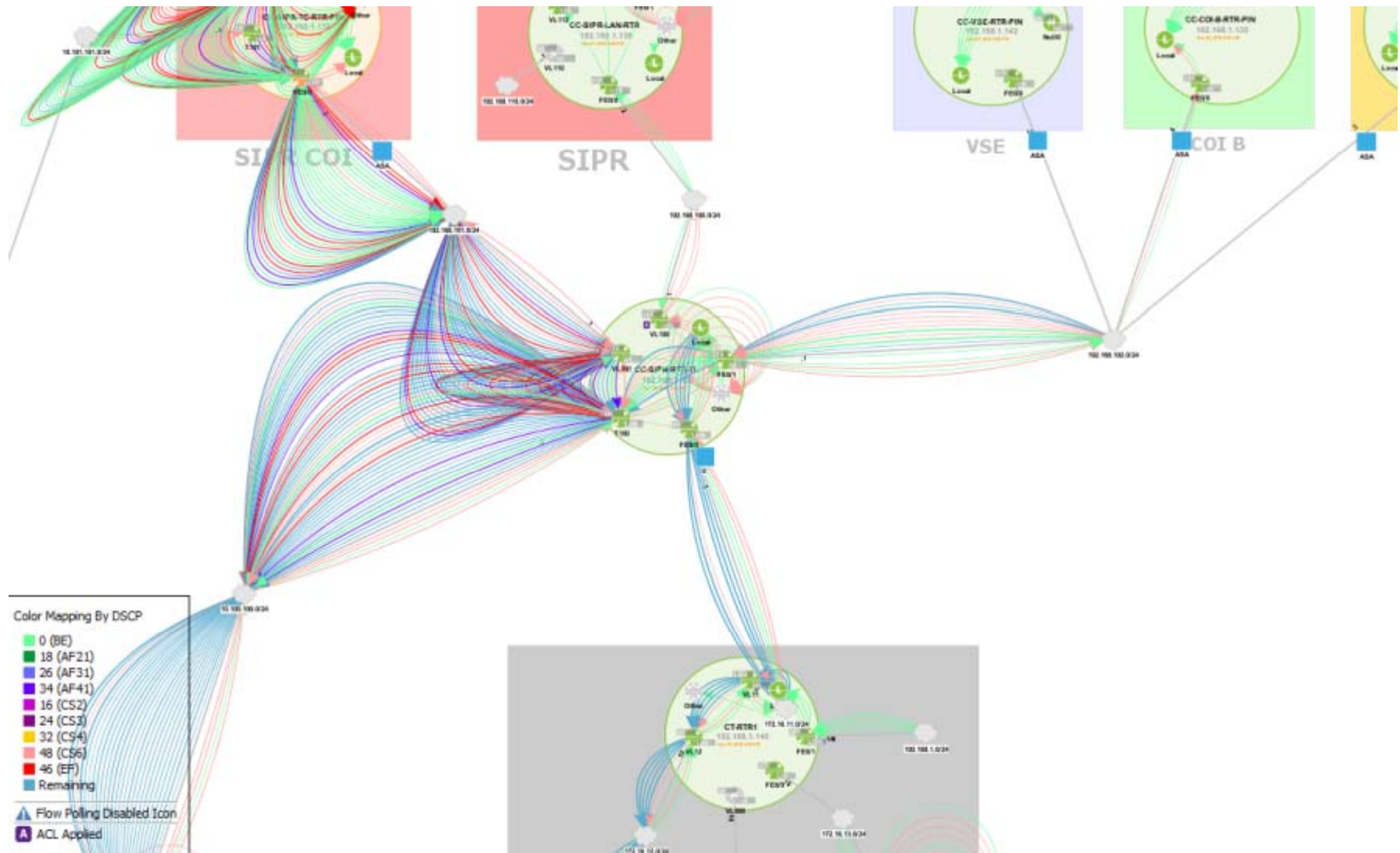


Investigating Inbound Traffic Spike

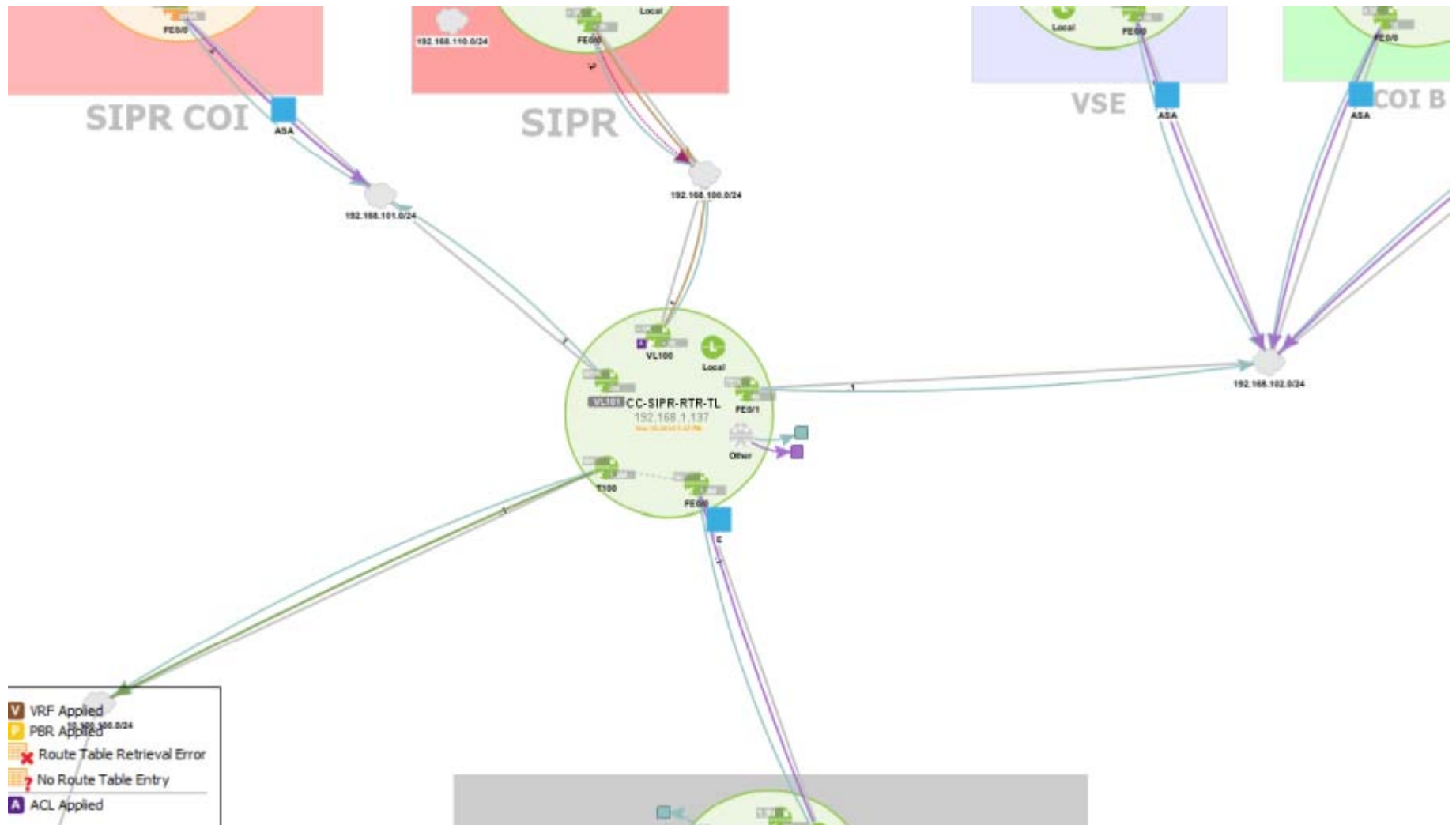
- FA0 interface showed spike in flows
- Inbound flow graphed
- Correlated to QoS statistics graph



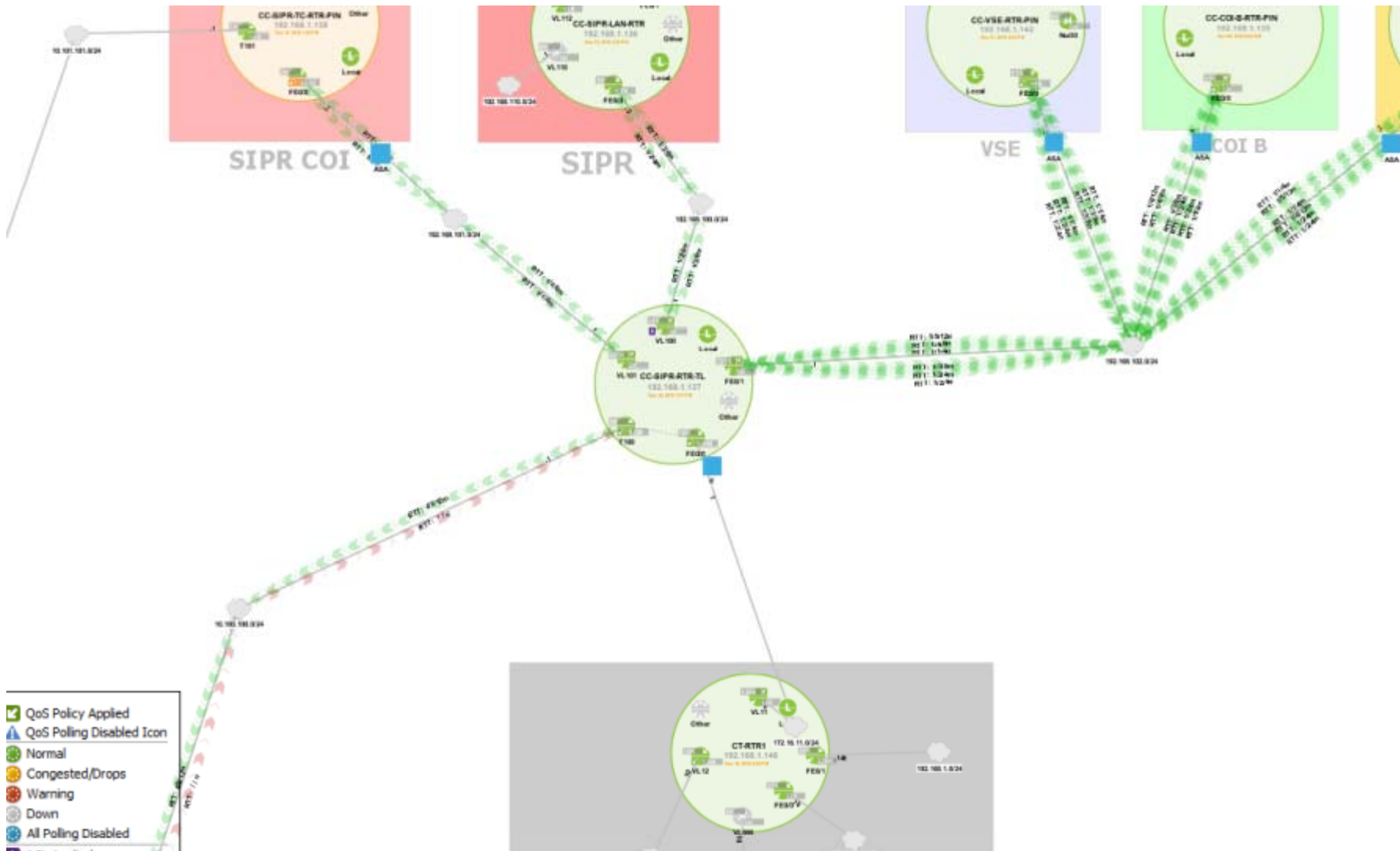
Flow Layer Visualization



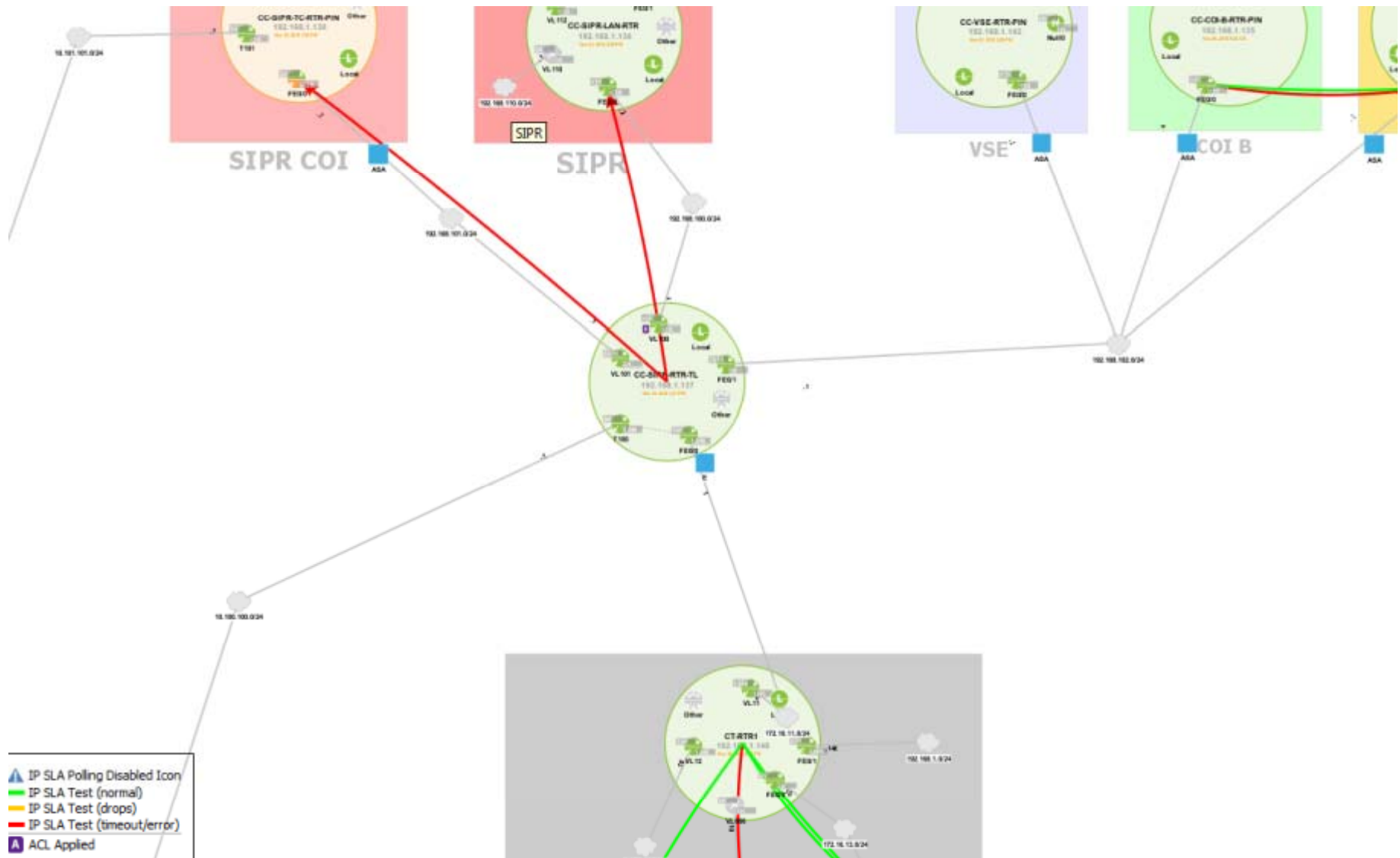
Routing Layer Visualization



Quality of Service and Ping Visualization



Service Level Agreement Visualization



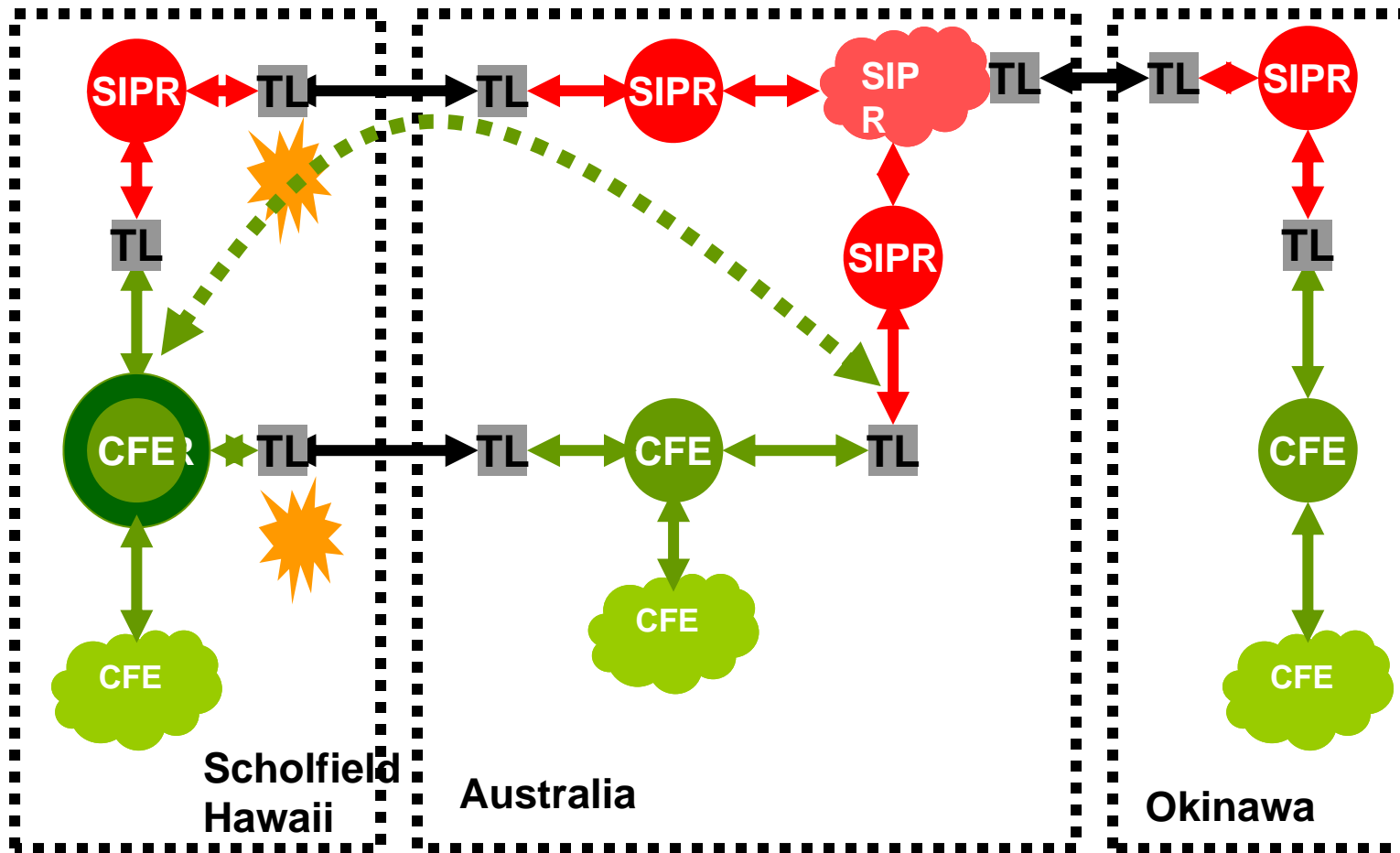
Service Level Agreement
Latency, Jitter, Loss, MOS

Flow
Actual Path, Load Sharing

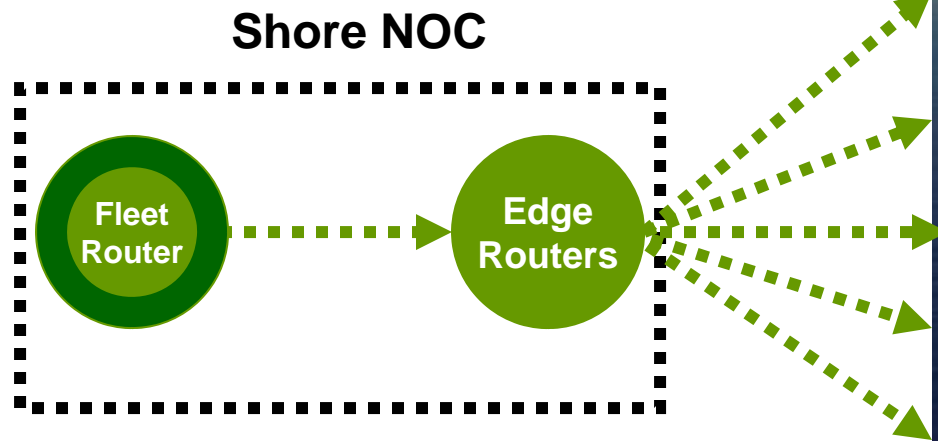
Routing
**Route Path, Asymmetric,
Summarization**

Quality of Service
Priority, BW, Queues, Drops

Usage : Talisman Saber Exercises US Marines referentia



Marines III MEF



- **Fleet monitoring of operational traffic**
 - Traffic over satcom
 - Voice from ship to shore
- **CND exercise**
 - Monitoring red team attacks
 - Working with sensors

- **Not Good At**
 - Showing large quantities of flows
 - Finding needle in hay stack
 - Pattern or algorithm analysis
- **Usage Issues**
 - Access to routers
 - Over WAN usage
 - Flow from multiple routers
 - Bandwidth in monitoring

- **Future Work**
 - Additional Network SA
 - Distributed Architecture
 - Cisco Flexible Netflow
- **For More Information**
 - jsmith@referentia.com
 - www.actionpacked.com

