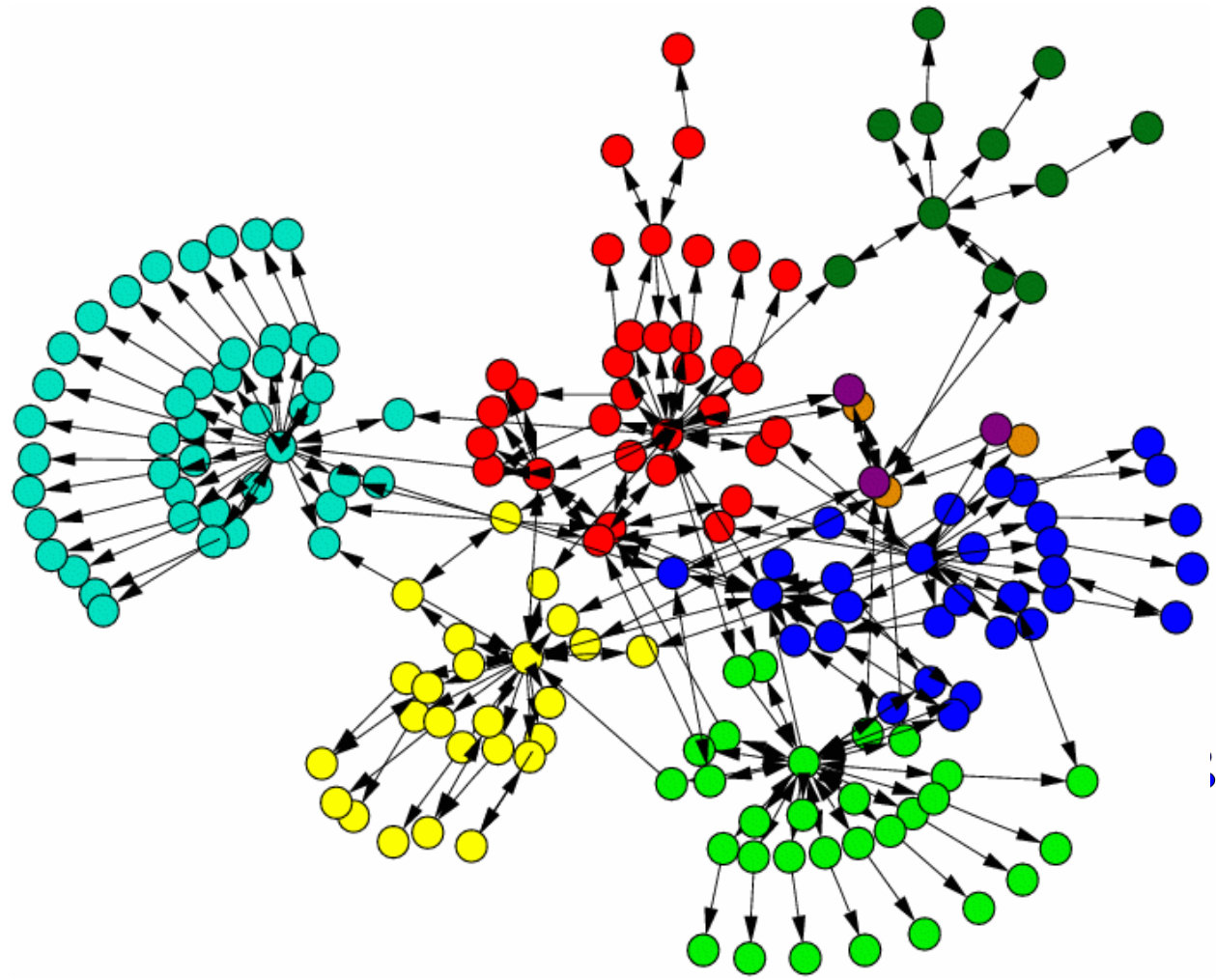


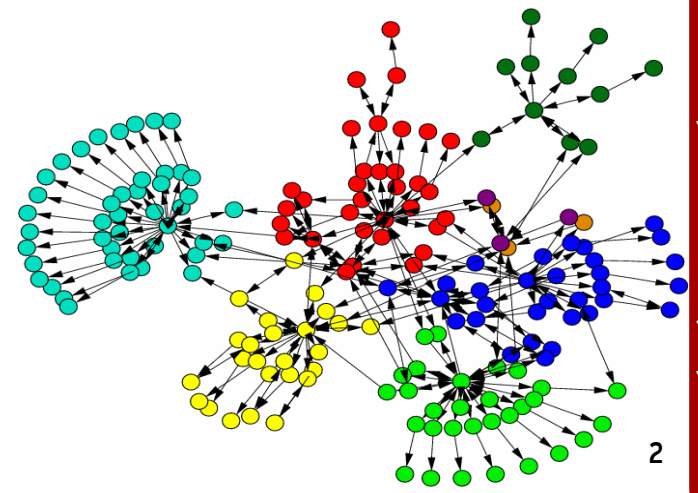
JxNAP

A Distributed Network Monitoring Platform



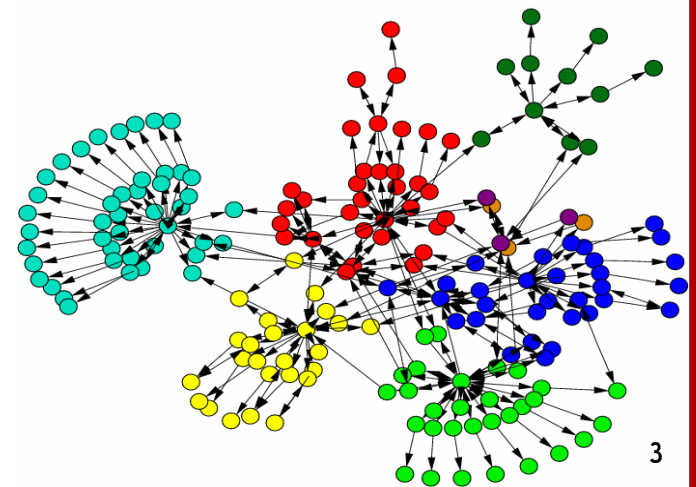
Introduction

- Why is JxNAP needed?
- What is JxNAP?
- Features
- System overview
- Employed Technologies



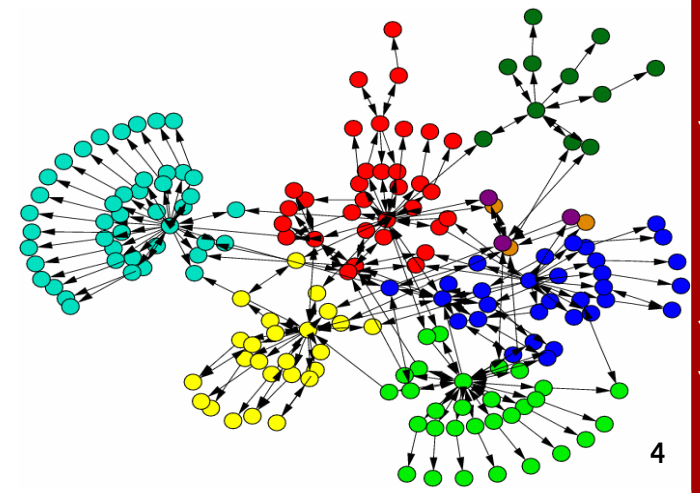
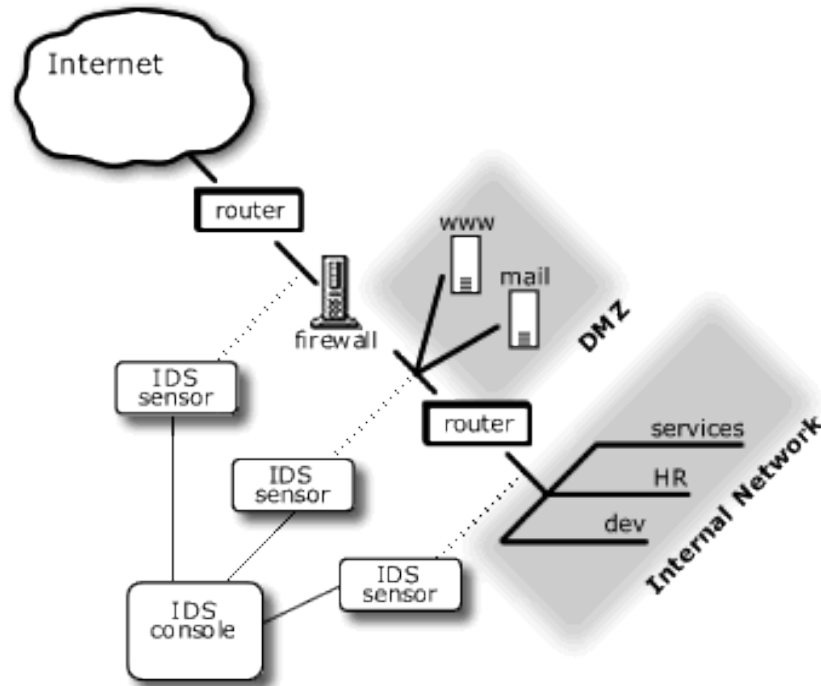
Why is JxNAP needed?

- No open source network monitoring platform
- Possible applications of Realtime Network Monitoring:
 - Network Asset Tracking
 - Low Bandwidth IDS
 - IDS Event Threat Level Estimation
 - Network Anomaly Detection
 - Roaming Client Tracking
- Breakdown of hard business edge



What Is JxNAP?

- A network monitoring platform
- Targeted network security specialists
- Passive and non destructive
- Modular and self maintaining



Features

- Hub

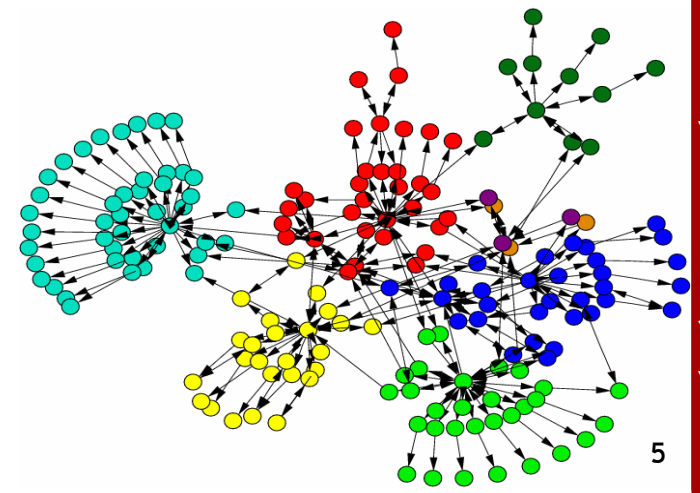
- Embeded MySQL Server and Manager
- Automatic Module Loading
- Automatic Failure Recovery
- Module Distribution
- Multicast Service Anouncements

- Node

- Automatic module loading
- Runtime re-configuration
- Dynamic Hub Discovery

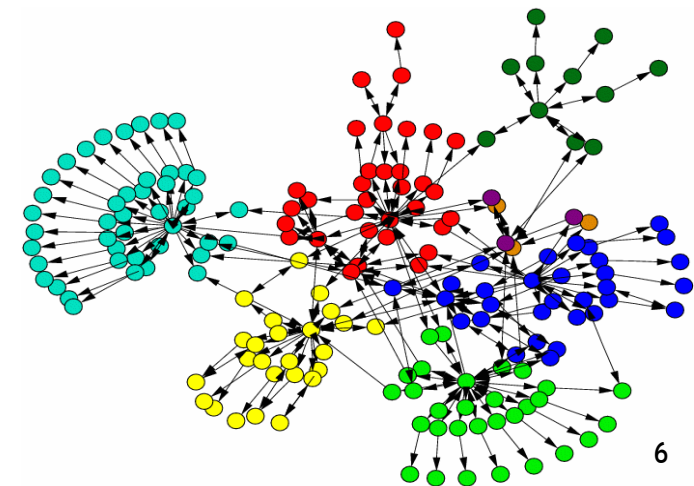
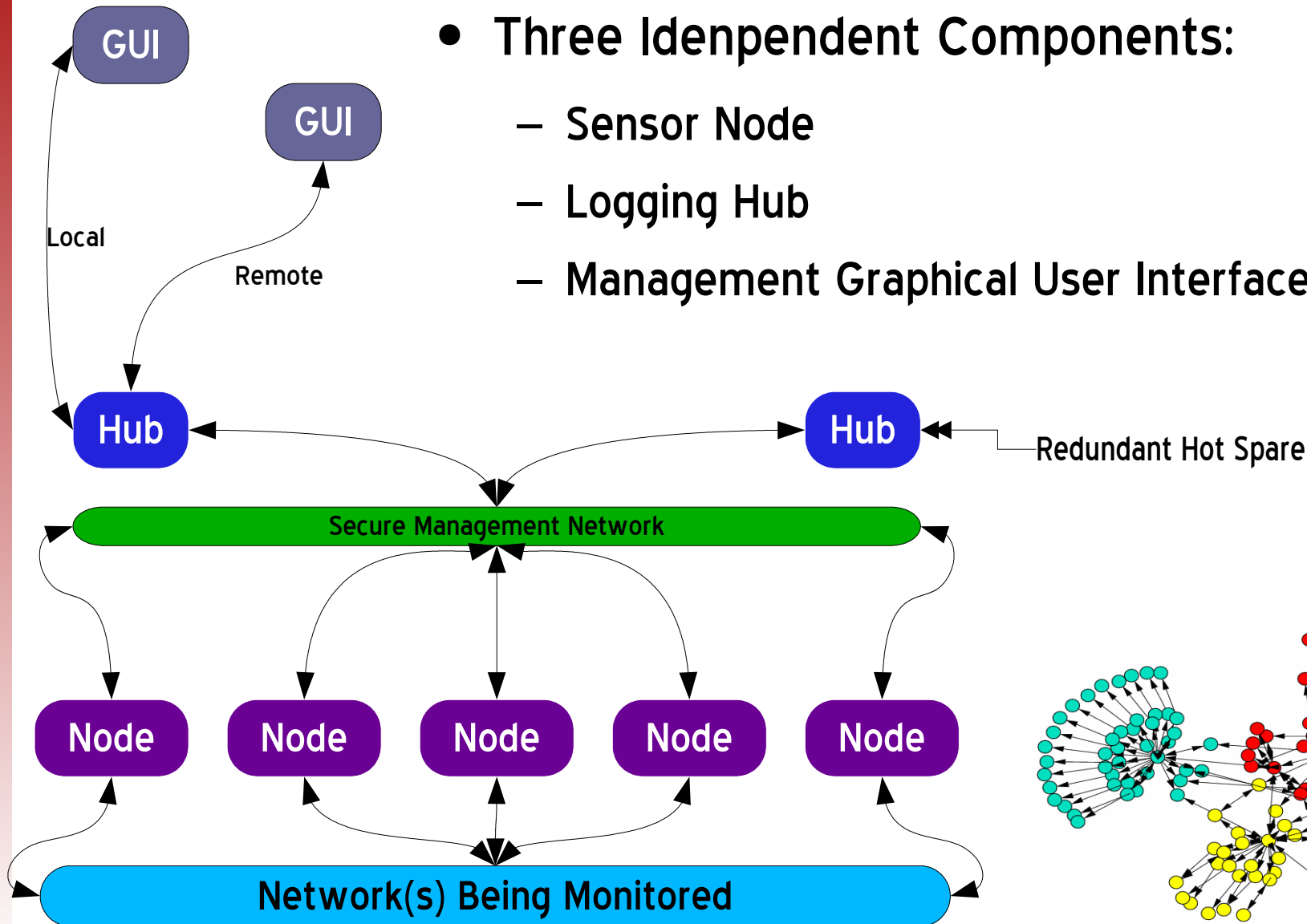
- Gui

- Automatic module loading

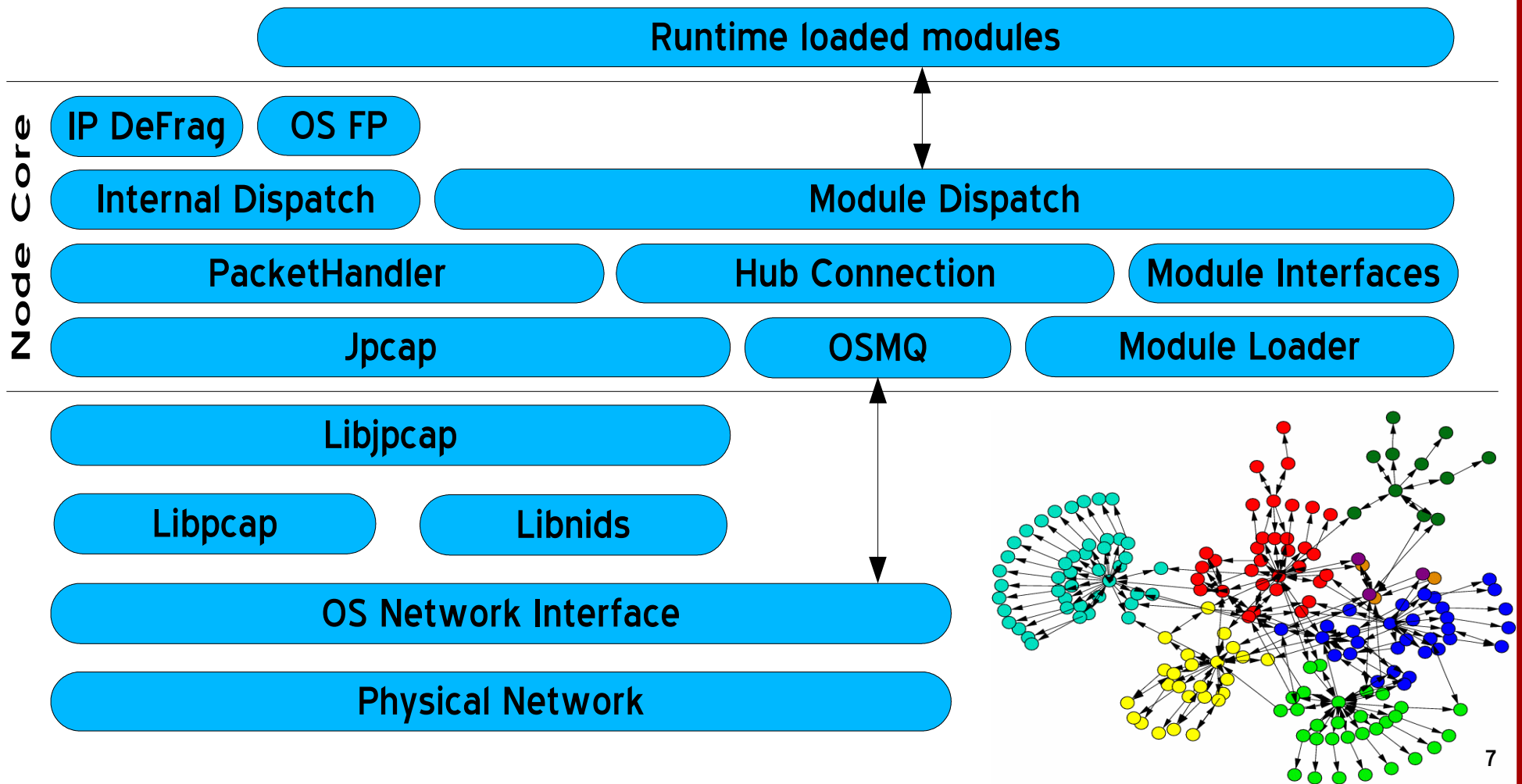


System Overview

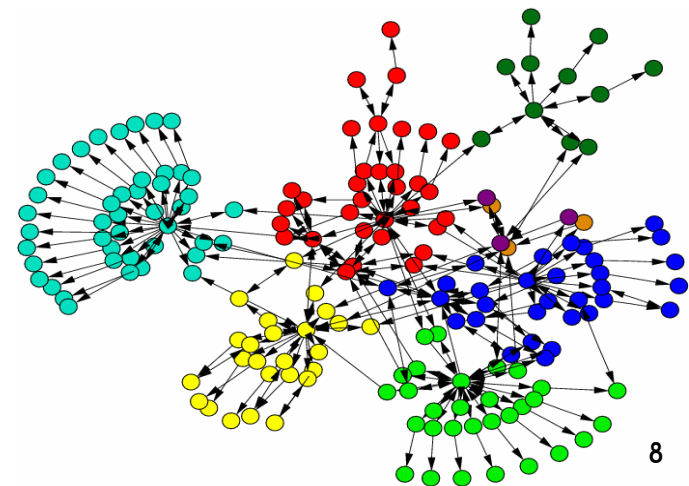
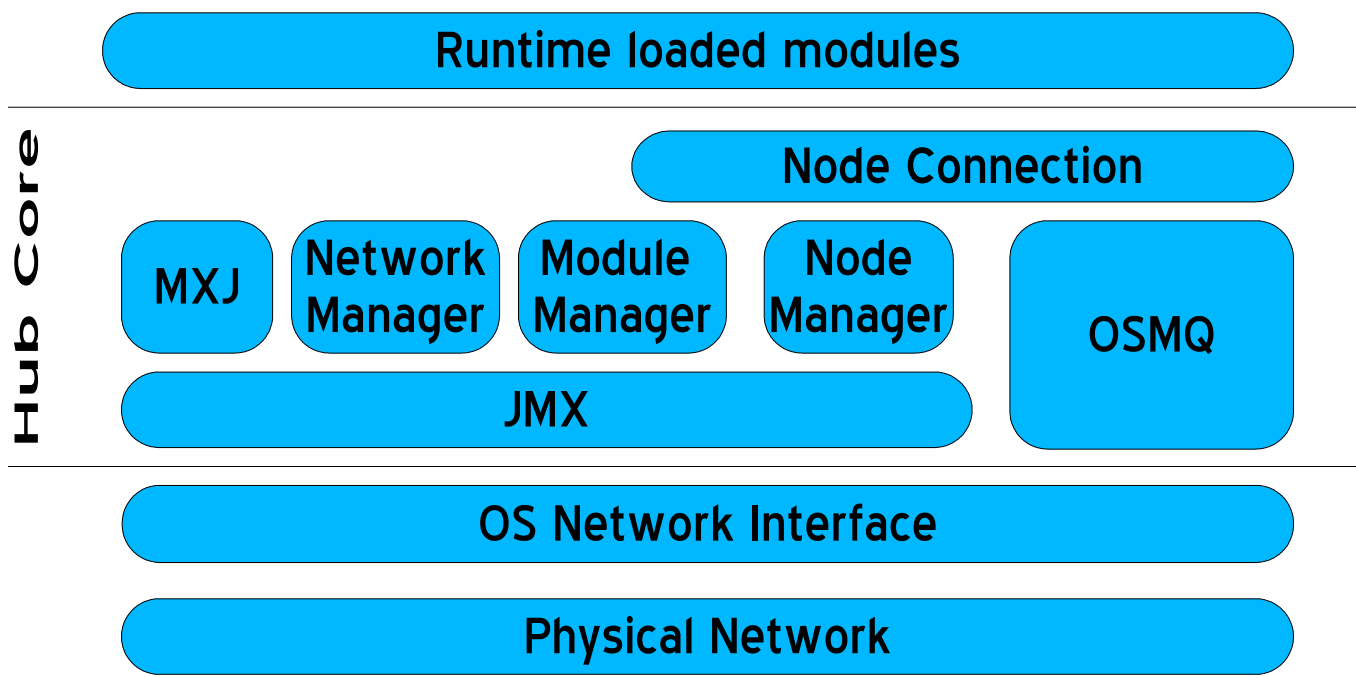
- Three Independent Components:
 - Sensor Node
 - Logging Hub
 - Management Graphical User Interface



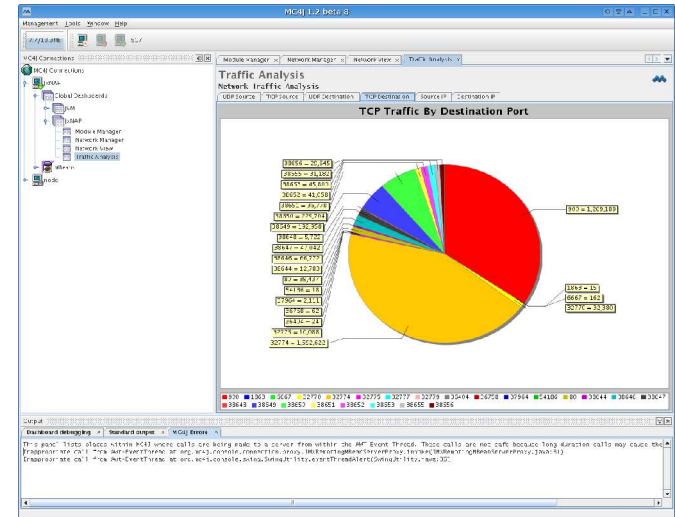
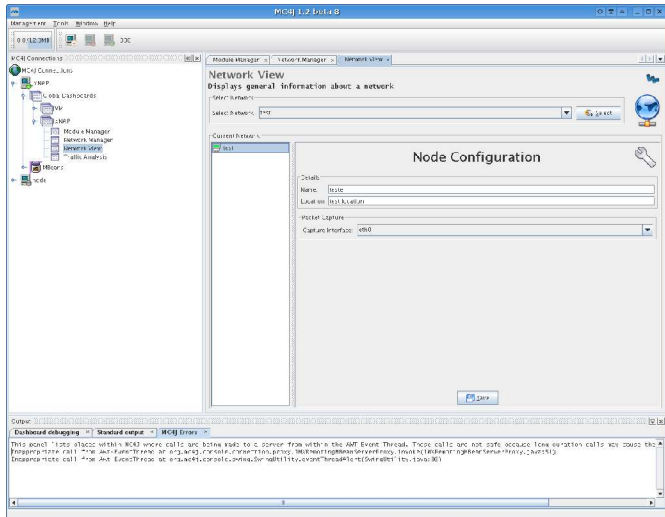
Node Overview



Hub Overview



GUI Overview



Core Dashboards

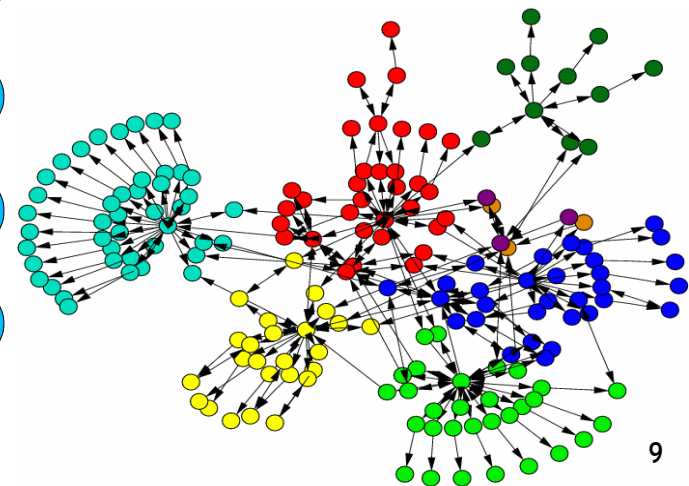
Module Dashboards

MC4J Platform

JMX

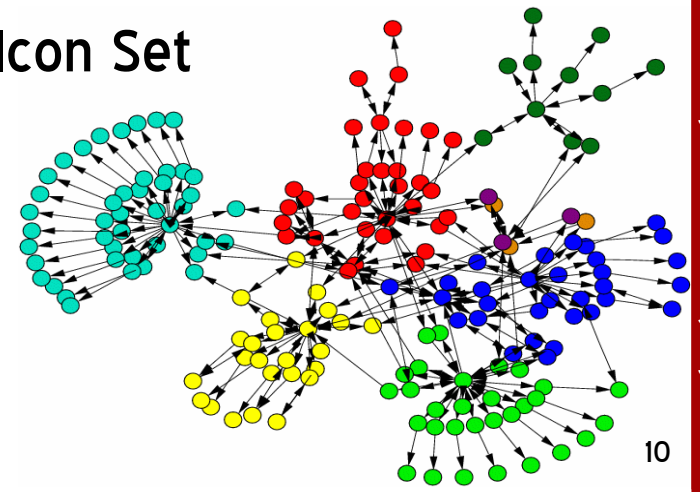
OS Network Interface

Physical Network

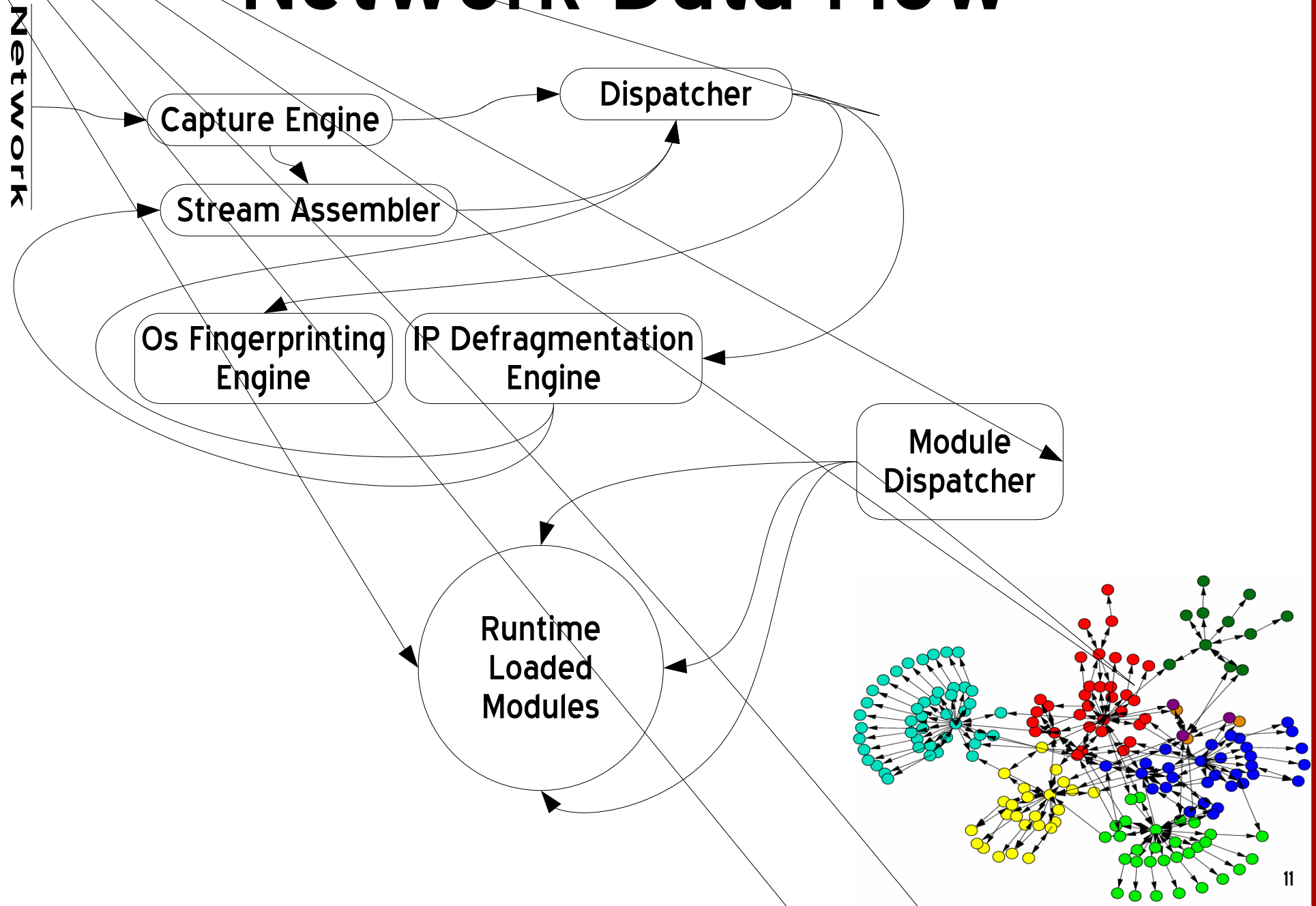


Employed Technologies

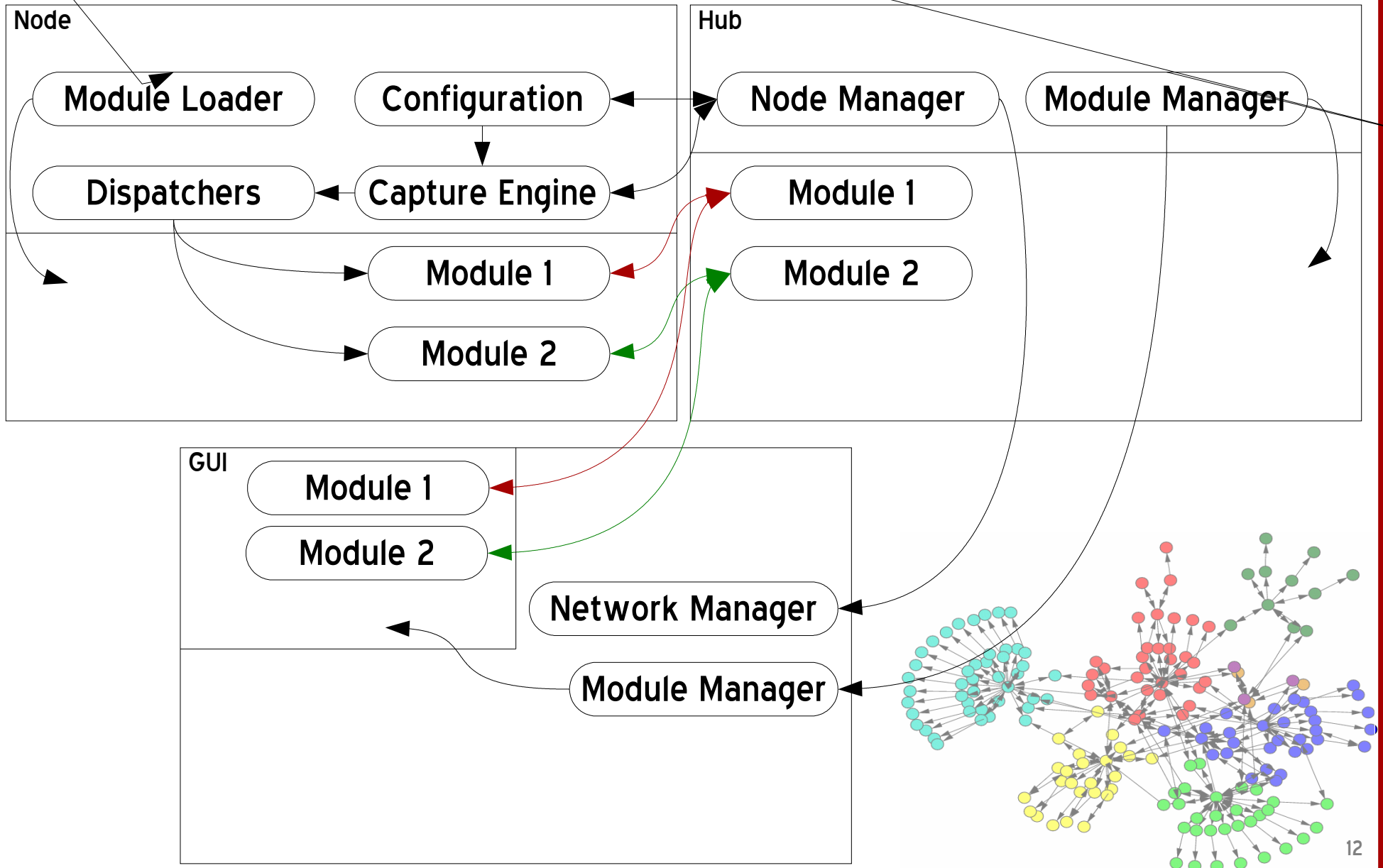
- Node
 - Jpcap
 - Libnids
- Common
 - Log4J
 - Open Source Message Queue (OSMQ)
 - jModuleLoader
- Hub
 - MySQL
 - Connector/J
 - Connector/MXJ
- GUI
 - MC4J
 - JFreeChart
 - Nuvola Icon Set



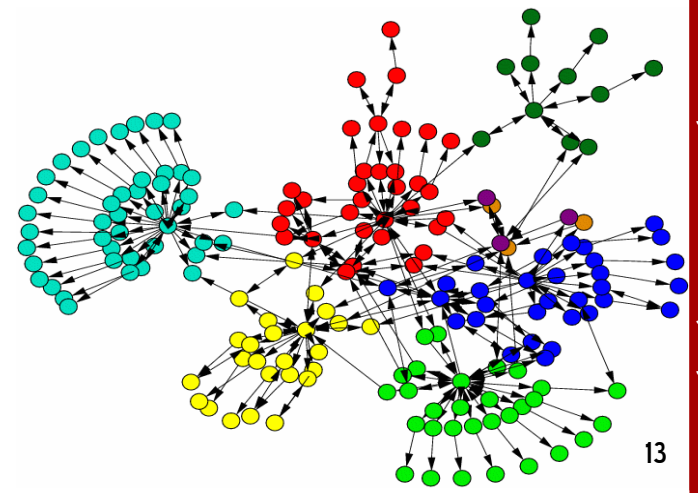
Network Data Flow



Event Data Flow



Demonstration



Are there any Questions?

