



# FY2001 ONR CIP/SW URI



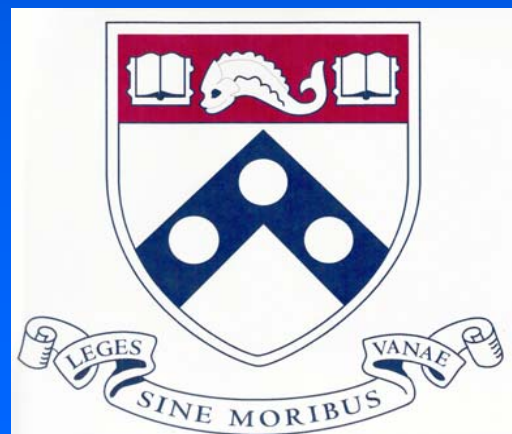
## Network Architecture Research in SPYCE CIP/URI Project



**Jonathan M. Smith**

University of Pennsylvania

<http://www.cis.upenn.edu/spyce>



# SPYCE Objective: Scalable Distributed Assurance



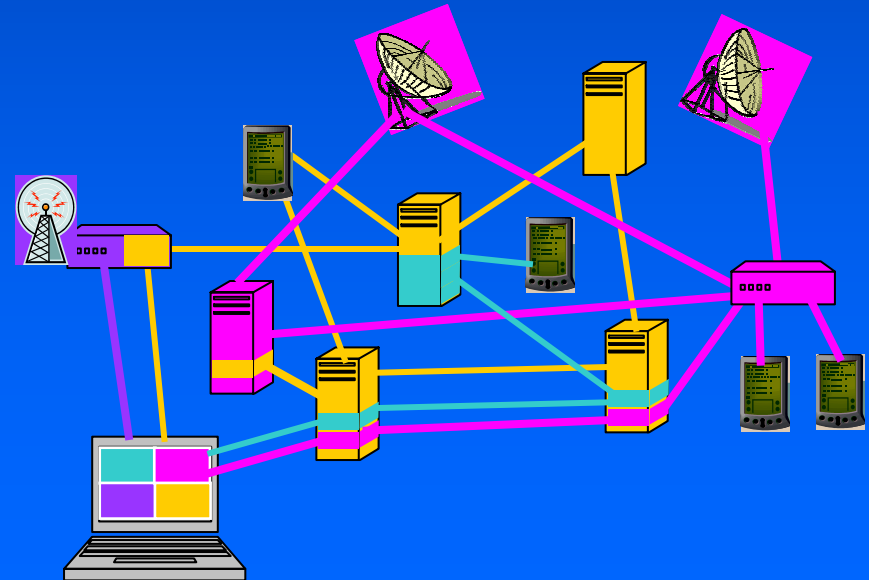
Develop fundamental understanding, models, algorithms, and network testbed, in order to reduce cost, improve performance, and provide higher reliability for networked operations across untrusted networks.

Incentives, Privacy, and Anonymity

Protocol Design and Analysis

Network Architecture

Trust Management

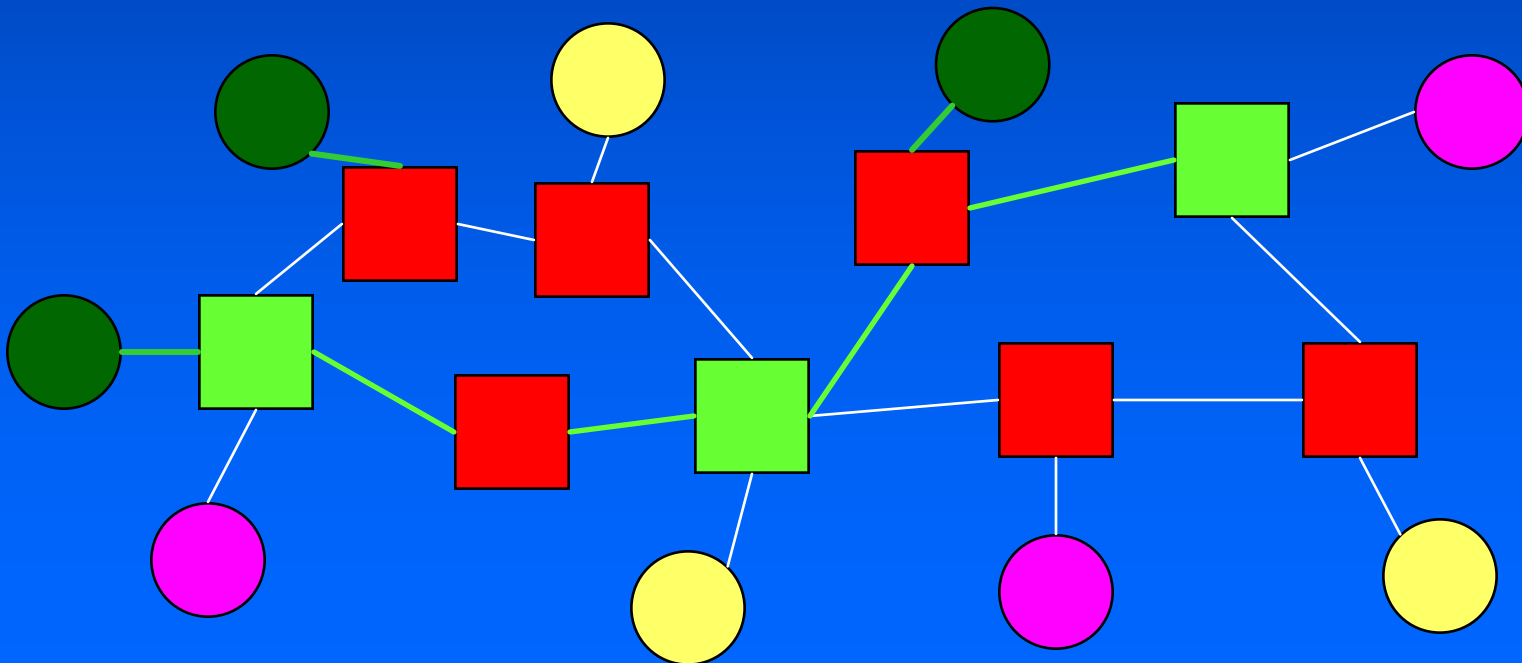


# Highlights: Network research

- FLAME: monitor & measure
- MPPW: Massively Populated Persistent Worlds; simulation
- CING network measurement system
- *Transcoding & proxies* to support *diffuse computing* on media streams and images in large-scale heterogeneous nets
- Growing SPYCELab software toolkit

# *The 70s Internet is no more!*

- New Roles for Hosts (Hosts, WWW, P2P)
- Routers \*plus\* RFC3234 "middleboxes"
- Other Diffuse Computing Elements



# Network Challenges and Diffuse Computing

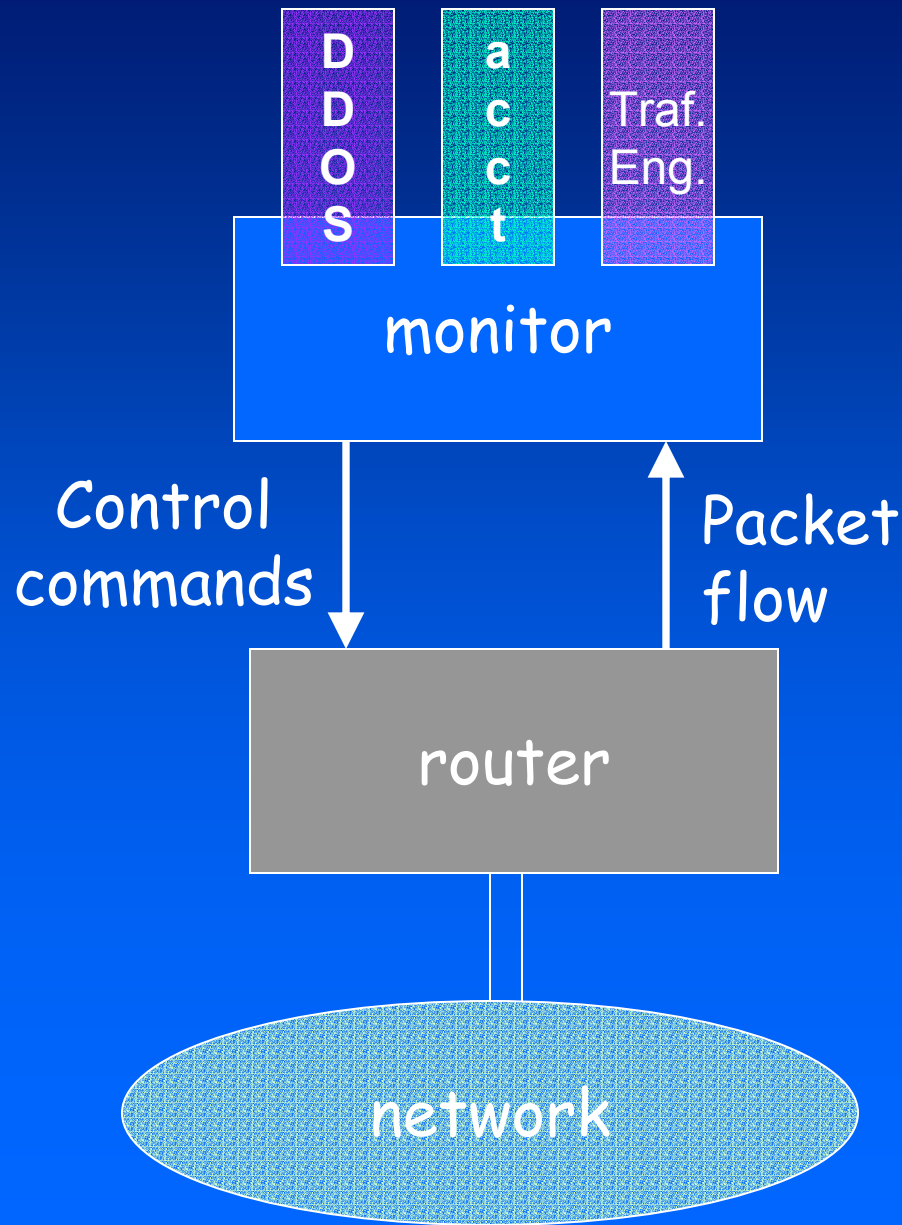
- **Diagnosis** in spite of complex network conditions, heterogeneity
- **Reconfigurability** for high availability
- Accommodating **new applications** (rapidly)
- Accommodating **new tech** rapidly (wireless)
- **Scalability**; Metcalfe's Law phenomenon
- Need for **global security** even *with* local failures and subversions

# Achievements/Prototypes

- **FLAME\*** active networking
  - fast/safe/extensible NW monitoring (NOMS 2002)
- **CING\*** network measurement tool
  - characterize Internet paths (Performance'02)
  - Indirect measurements (Infocom'03)
- **Transcoding proxies\***
  - Diffuse support for thin clients (TOIT 2003)
- **Massively Populated Persistent Worlds\***
  - Applications to distributed simulation (OSDI02 WIP)

\* Done with CIP/URI support

# Diagnosis: AN-based monitors:



Uses:

IDS

DDoS/virus detection

performance debug

traffic engineering

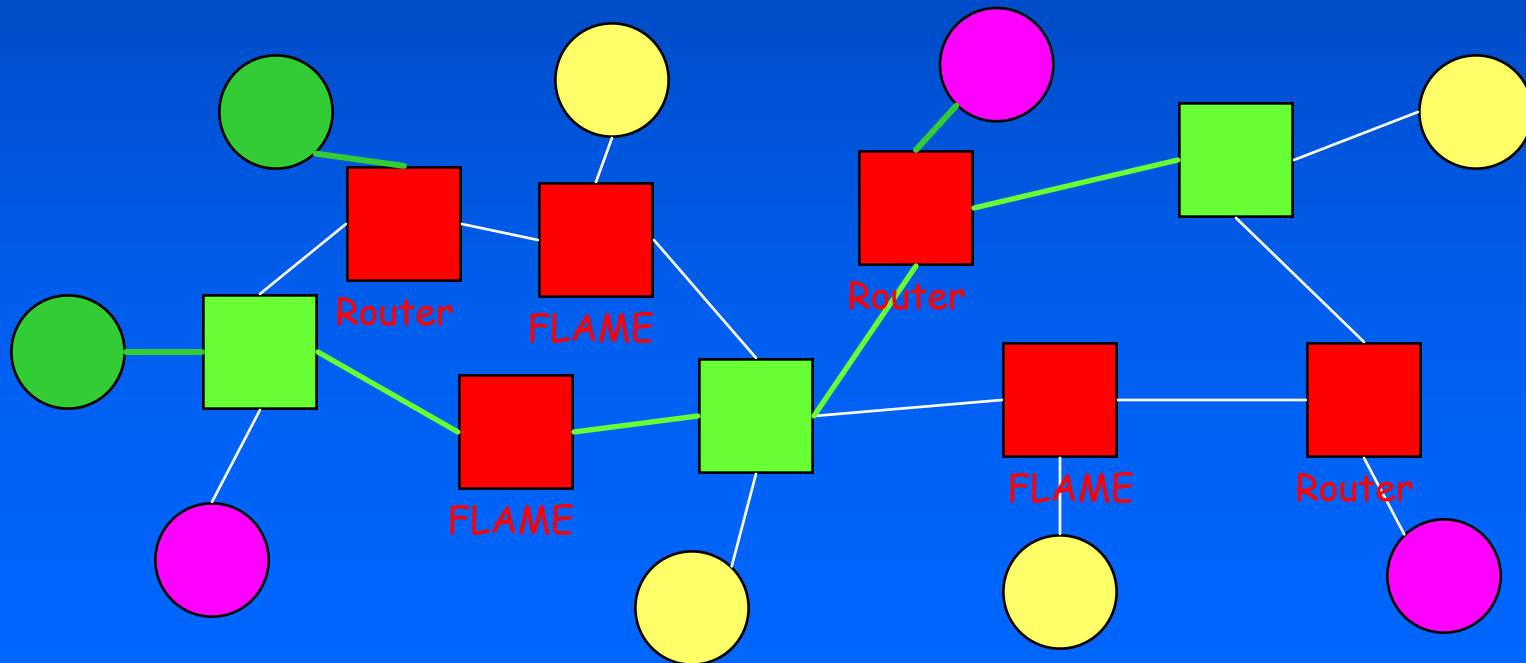
traffic measurement

Accounting

SPYCE platform

# FLAME: *Safe in-network* monitoring

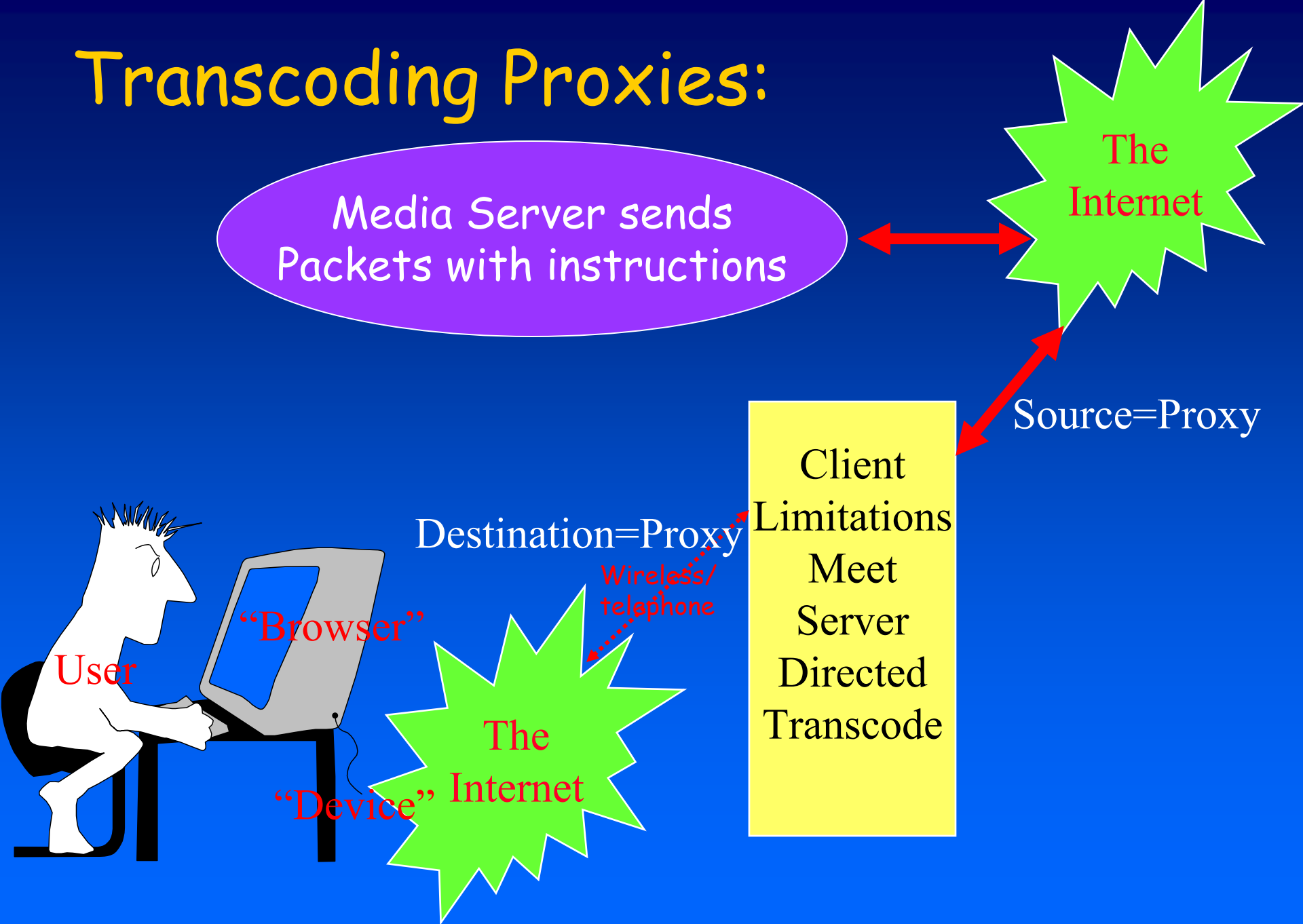
- Hosts of **various** types
- **Routers / FLAME nodes**
- Diffuse Computing Elements
- P2P participants



# Transcoding proxies

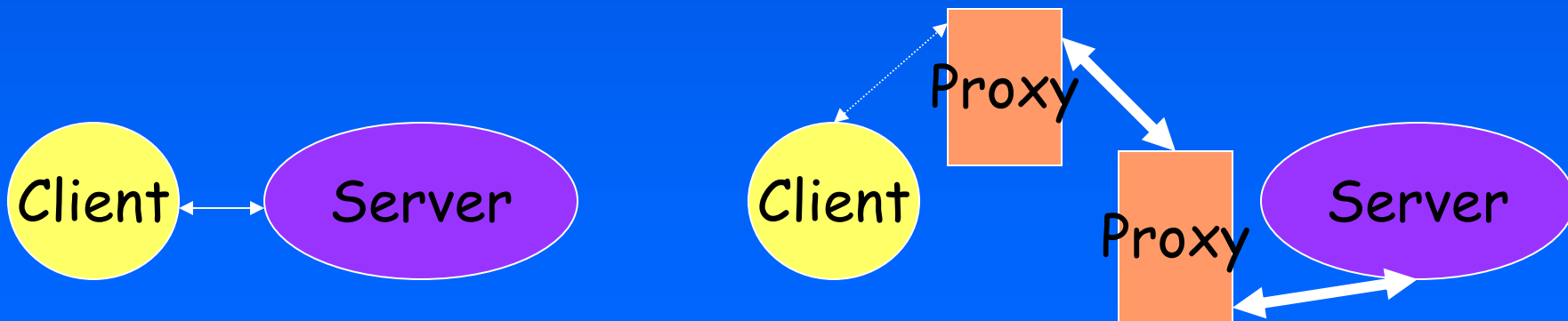
- Client/Server model too simplistic
  - “remote access” style of LAN-based distributed computing from 70s
- Diffuse computing allows a far more general approach
  - e.g., WWW (it's diffuse Remote Procedure Call..)
  - Diffuse transcoding to address heterogeneity in network and device capabilities
  - Proxies to address localized specialization and access control, e.g., interface to secure repository

# Transcoding Proxies:



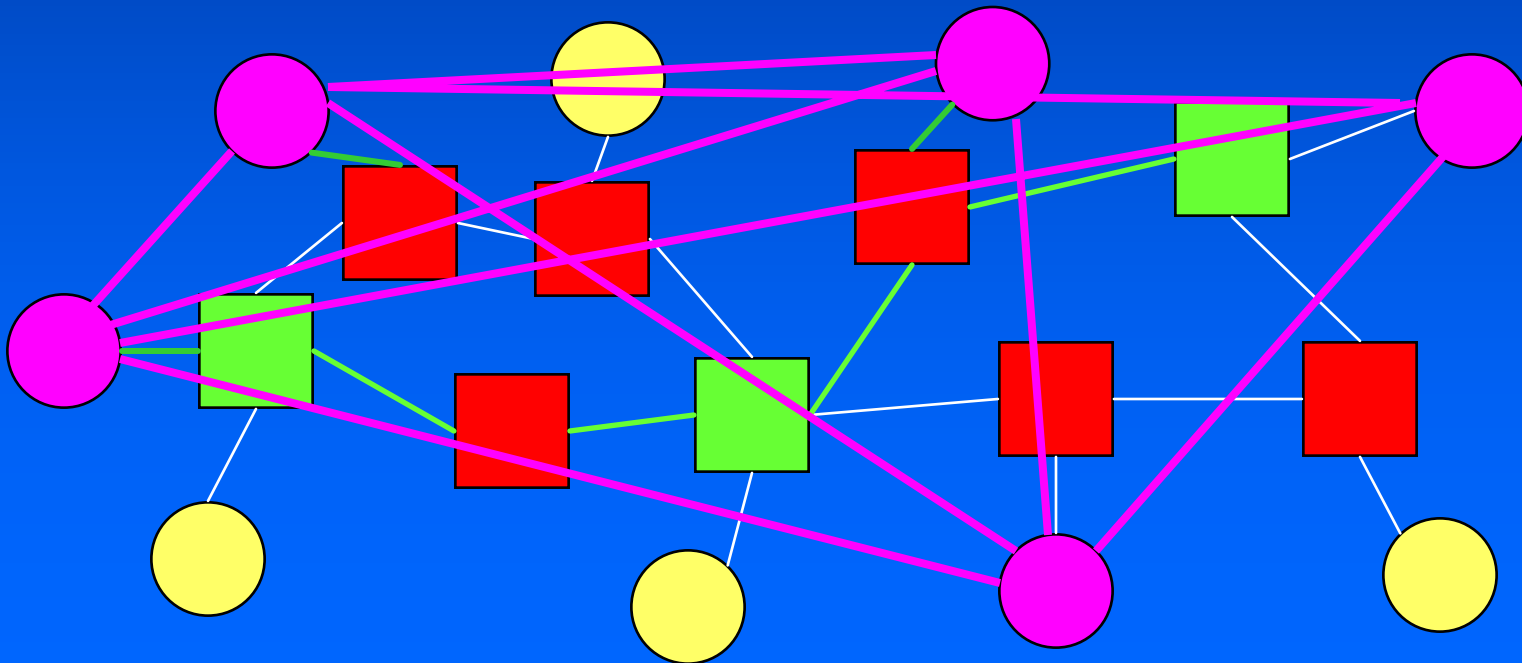
# Diffuse Computing issues addressed

- Distributes work
  - Easy (in fact desirable) to have multiple proxies
  - Load-balancing with anycast
  - Anycast is path to economics control
- Addresses scale
  - Copes with heterogeneous nets and devices
  - Localizes complexity
  - *Diffuse* complexity, not centralized at server



# Massively Populated Persistent Worlds

- Hosts - Participate Dynamically as Peers
- Routers
- Participating Nodes create an *overlay*

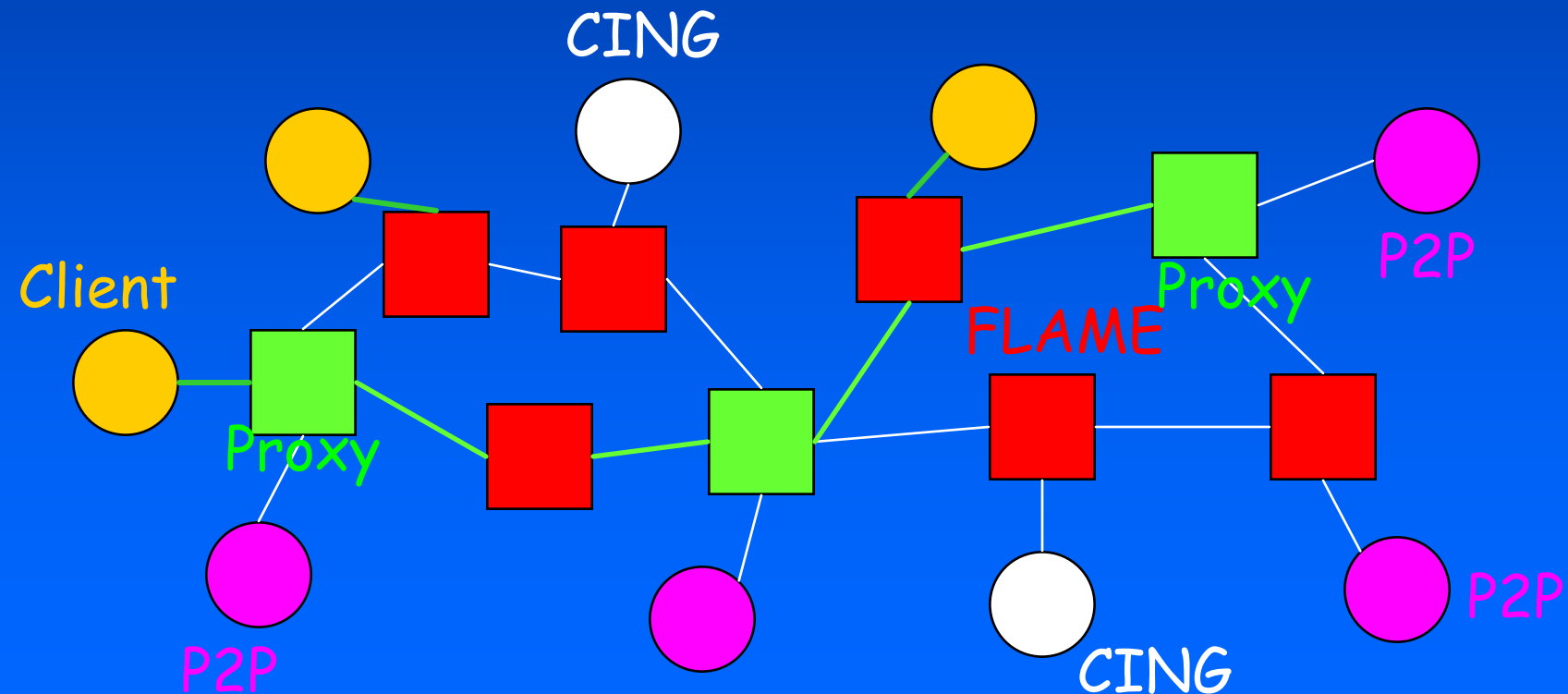


# Diffuse Computing issues addressed

- Ultra large scale via *dynamic* decentralized resource allocation model
  - *Global reliability* in face of *local failures*
  - Tight coupling of networking and distributed computing issues
- Ongoing work in interest management, w/good opportunities to introduce *incentives* for diffuse control (*e.g.*, for *dynamic* region construction)
- Great opportunity for DoD *tech transfer* (*viz.* 2002 ISAT study)

# MANY PLACES for Diffuse Computing!

- Hosts
- Routers
- Network Embedded Diffuse Computing Elements
- Peer-to-Peer (P2P) for MPPW



# Critical Infrastructure Protection

Many critical infrastructures, national and DoD-specific, are *diffuse computing systems*

- e.g, financial systems
- Today's networks have themselves become critical infrastructures!

*Research Question:* How to build large-scale, adaptive and robust next-generation systems?

*Approach:* New **Diffuse Computing** concept

- results with *extremely* loosely-coupled modules

# Assuring Software Quality

- Great decentralization yields high autonomy
  - Loose-coupling leads to natural “sandboxing”
- Pieces of system more robust in face of:
  - Failures / Disruptions
  - Partial Information
- New way of writing software
- *Result*. Software Engineering for highly decentralized, policy-controlled and networked world

# DoD Impact

- Joint Vision 2010 / Joint Vision 2020 of "Network Centric" operations
- *DoD network challenges* addressed:
  - Agile and rapidly evolving
    - ✦ CING measurements/Active Network deployment
    - ✦ Transcoding Proxies
  - Secure and Robust
    - ✦ FLAME A.N. approach - restricted but flexible
  - Scalable
    - ✦ Massively Populated Persistent Worlds concepts

# Plans for Option

- Kostas Anagnostakis Ph.D research:
  - **ITRUST** - Incentive TRust for Ultrascale Services and Techniques [P,Y,Columbia]
    - ✦ Ultrascale diffuse approach to distributed anomaly (*e.g.*, worm) detection
    - ✦ Ultrascale resource (*e.g.*, file) sharing
- Bjorn Knutsson Post-Doctoral research:
  - Experimental Validation of **MPPW** on PlanetLab (& new anomaly detection algorithms)
  - **DHARMA** - Distributed Home Agent for Reliable Mobile Access (diffuse approach for mobility; advanced adaptive configuration management)
- Continuing evolution of **SPYCELab**

# Notes:

- CING: Anagnostakis, Greenwald (Penn), Ryger (Yale)
- FLAME: K. Anagnostakis, *et al.* (Penn)
- Transcoding Proxy: Knutsson, Lu, Mogul (Compaq)
- MPPW: Knutsson, Lu, Wai
- DHARMA: Mao, Knutsson, Lu, deBruijn, JMS
- Papers + Software Distros at:  
<http://www.cis.upenn.edu/spyce>