Supernetworking: Virtual Address Resolution at the Edge

Christoph Schuba

Caronni, Chang, Kumar, Landau, Schuba, Scott
Security Research Group
Network&Security Center
Sun Microsystems Laboratories
901 San Antonio Road
USA − Palo Alto, CA 94303

Sun Microsystems Laboratories

Outline

- *Motivate and present* our model of secure virtual networking
- *Explain* requirements for addressing in global/virtual network, focus on edge
- *Describe* the prototype status quo and future work
- *Draw* conclusions

Public Utility Computing Model

- Secure Communication: ***Supernets***
- Secure Storage
- Secure Computing
- Security Management

Motivation for Public Utility Computing (PUC)

- Dependence on computer networking
- Requirement for ubiquitous access to data and services, e.g., e−commerce, sales staff, remote employees, etc.
- Desire for network security

  vs.

  Desire for open access

Motivation for PUC (cont.)

- IT expertise ≠ core business expertise
- Outsourcing of information infrastructure needs in a **secure** fashion
- Benefits through economies of scale:
  - cost effectiveness,
  - no provider lock−in,
  - leveraging today's technology,
  - access to new technologies

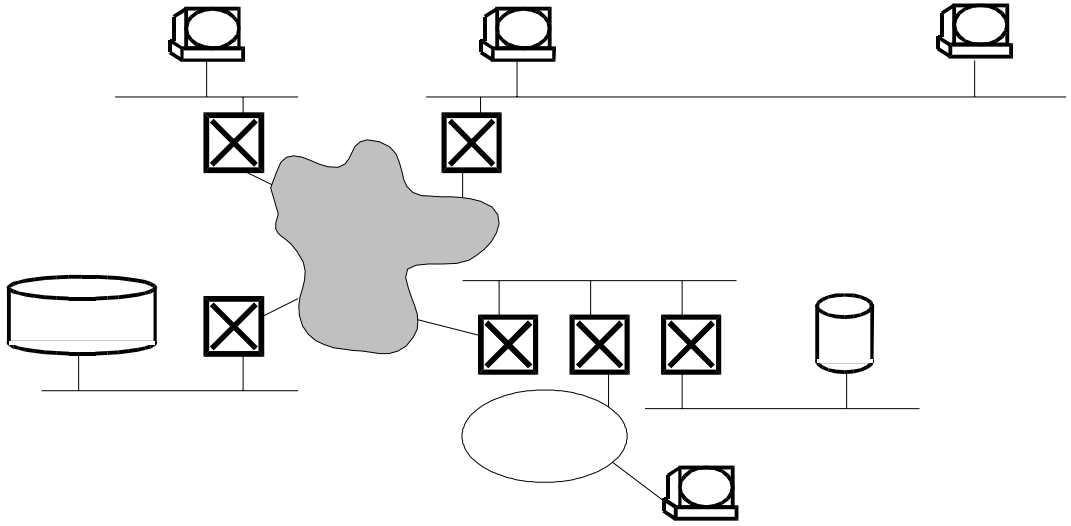
Motivation for PUC (cont.)

- Insufficient attempts at security problem:
  - Firewall technology
  - Virtual private networks
  - Reverse proxies, e.g., iPlanet (sun.net)
- Drawbacks and problems:
  - Inefficiencies in operation
  - Lack of flexibility for network creation/dissolution
  - Difficulty in maintainance and administration
  - High cost

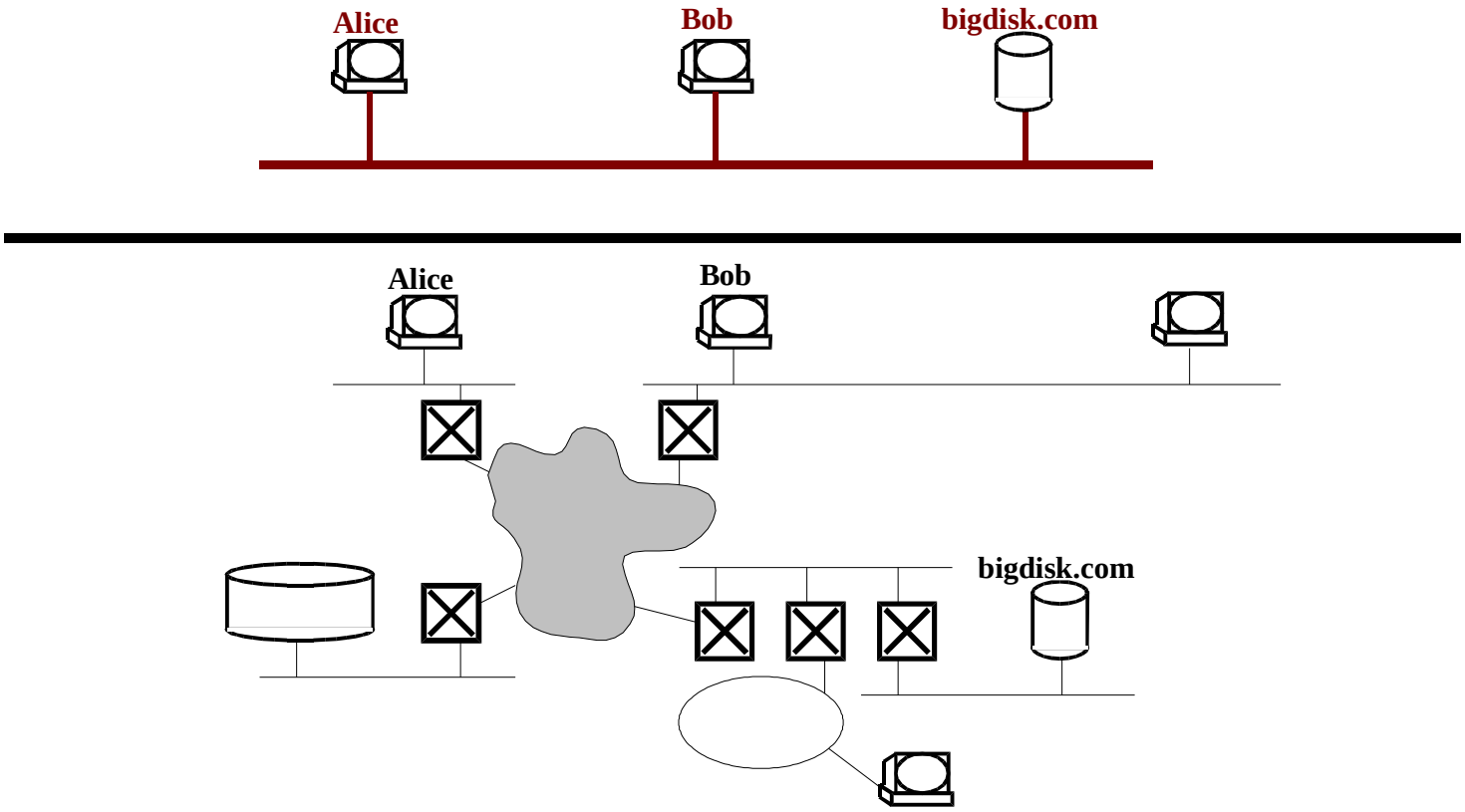
Articles of Faith

- Large number of network attached devices
- Security requirements
- Dynamic coalition capability
- Lifetime independence
- Reuse of existing applications
- Outsourcing of communication infrastructure

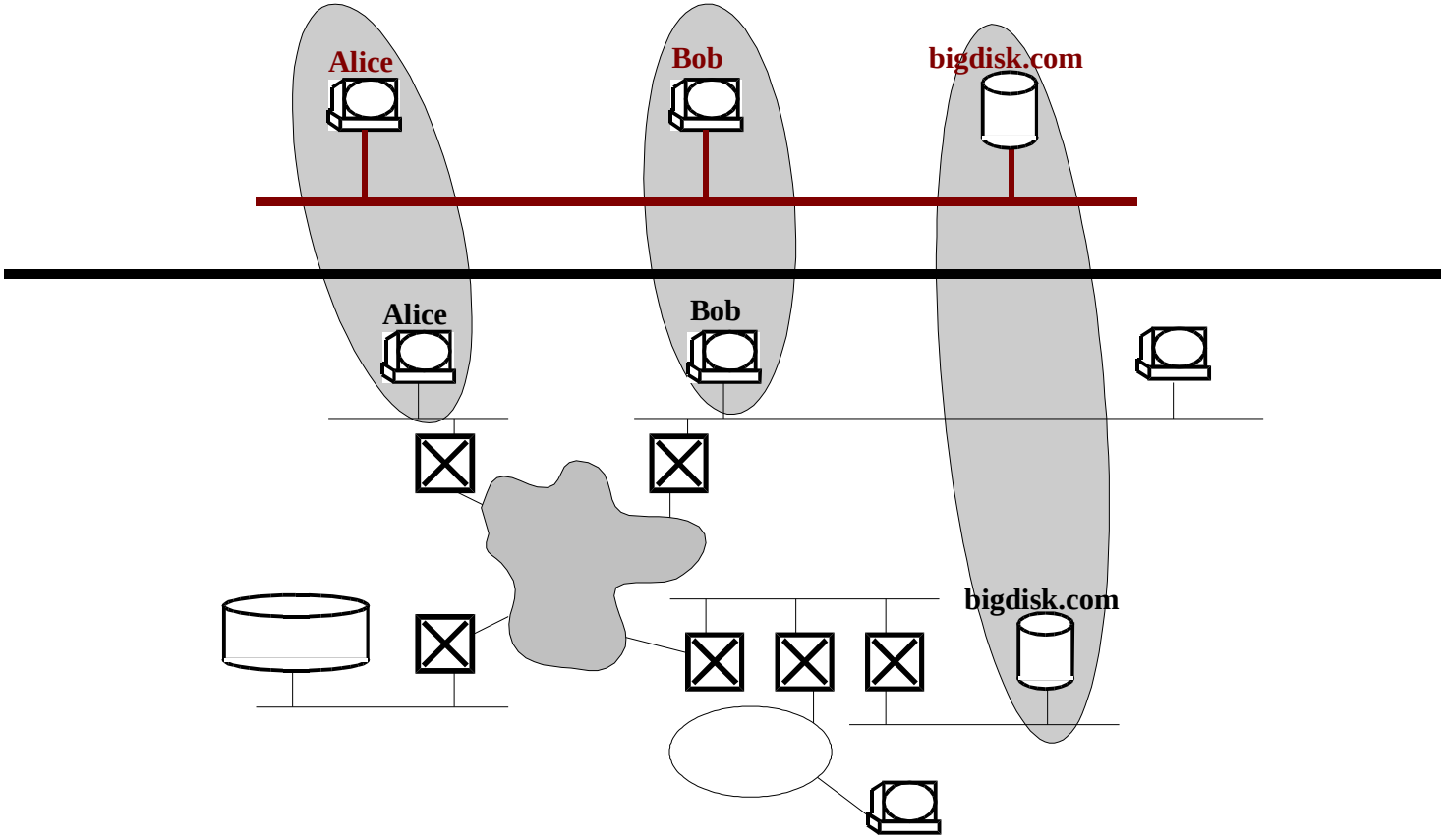
Today: Building Communities around Networks



Goal: Building Networks around Communities



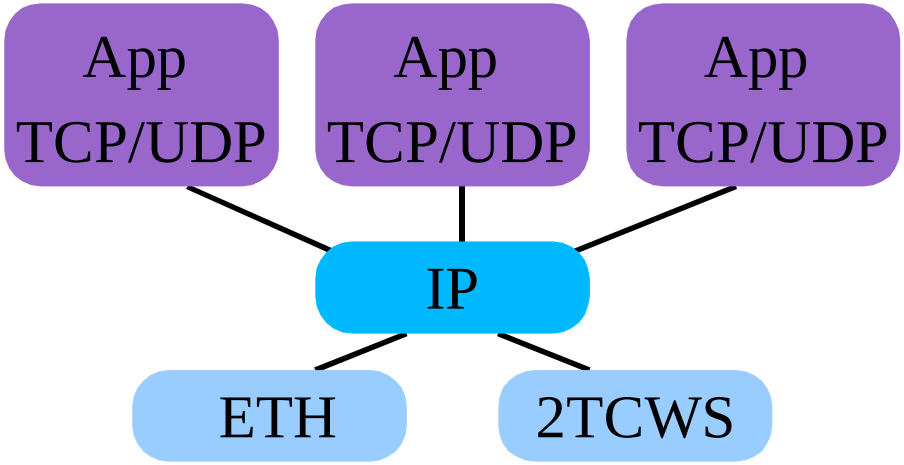
Goal: Building Networks around Communities



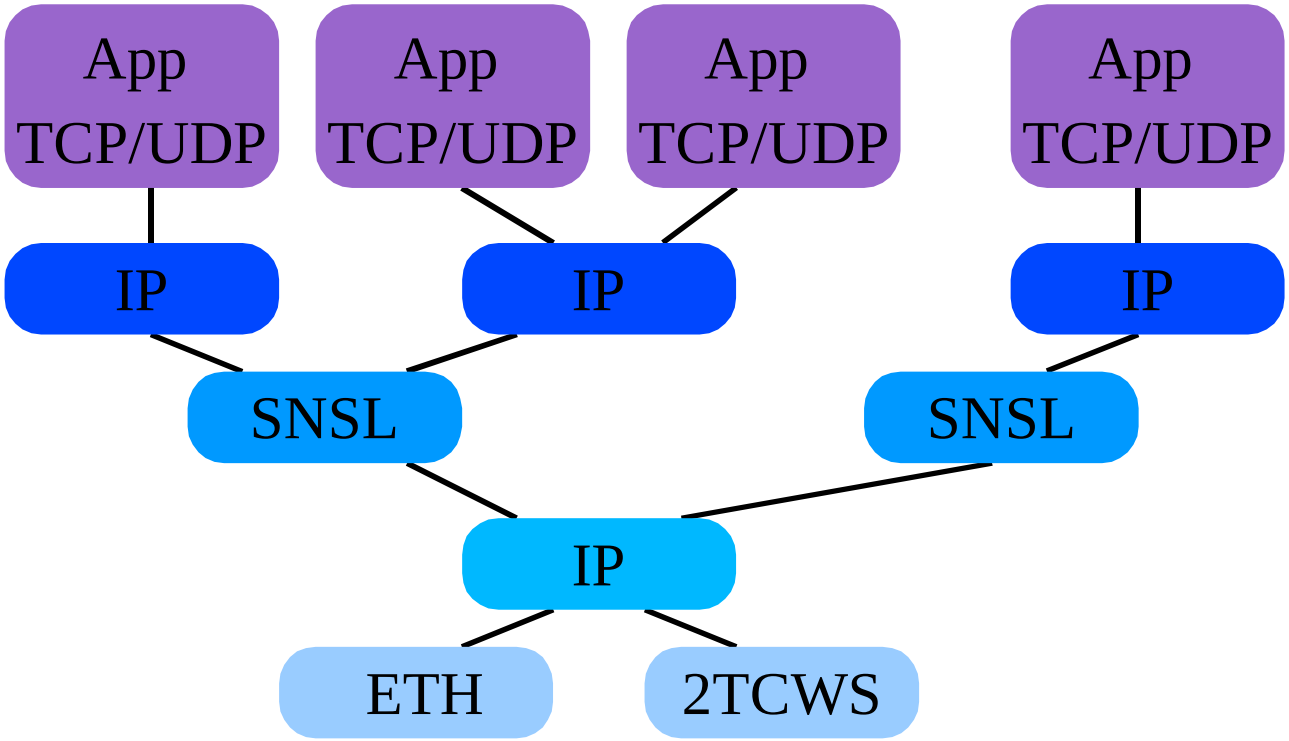
Addressing at the Edge

- Legacy:
  Lots of applications that use TCP/IP
- Desire:
  Independence of underlying transport (¬hw)
- Realization:
  IP is global *glue*

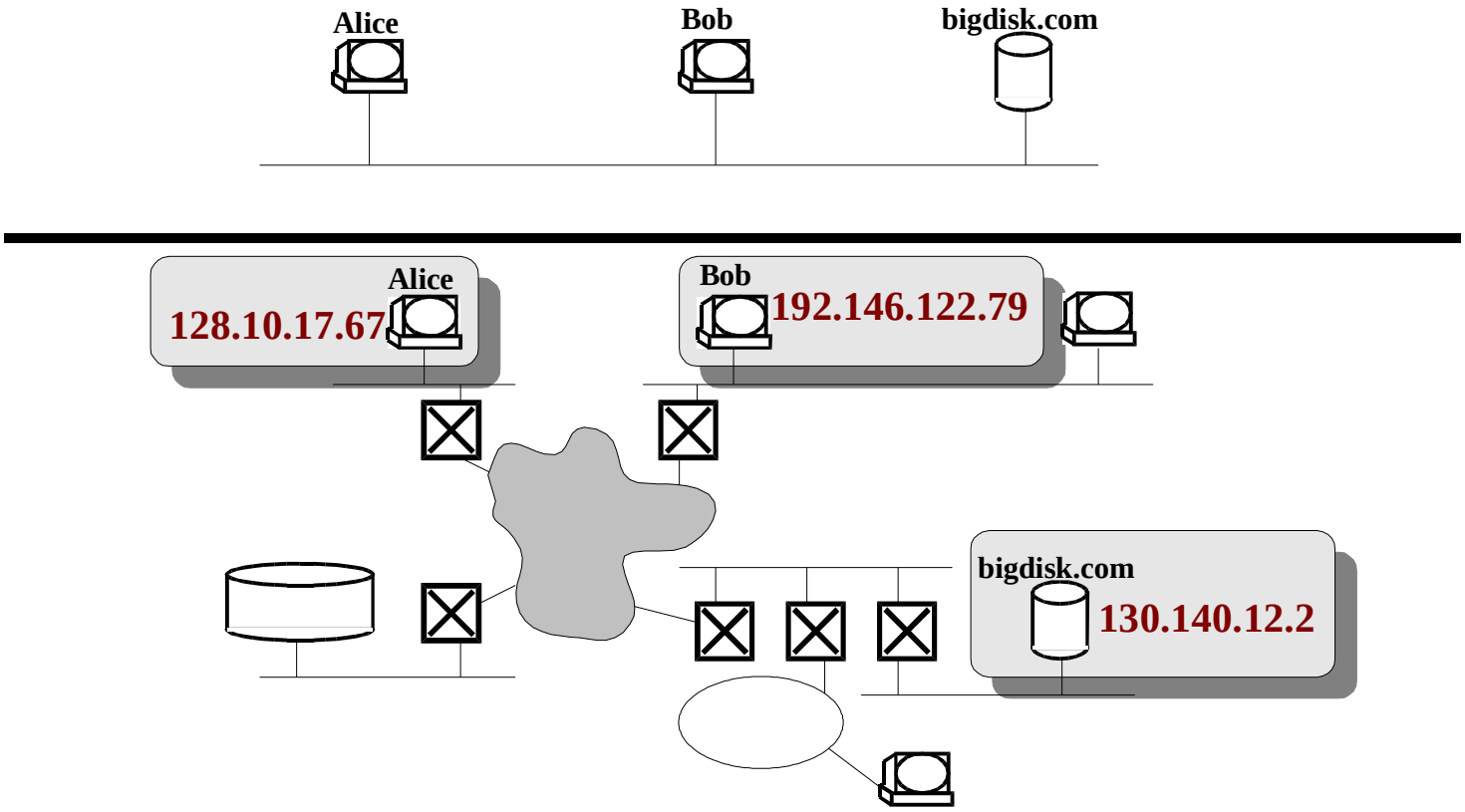
IP: Global Glue



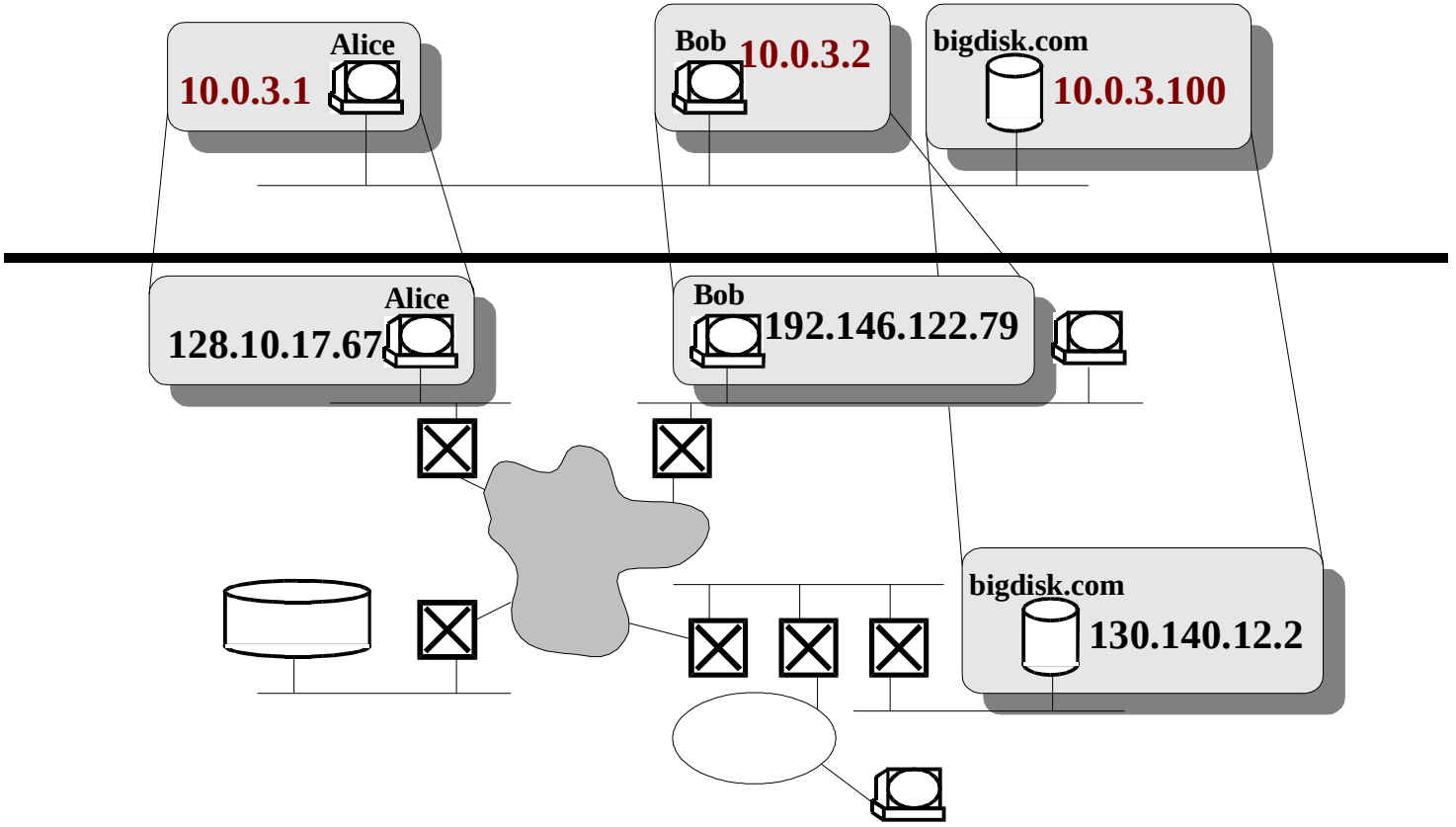
IP: Global Glue (cont.)



Addressing in Supernets



Addressing in Supernets (cont.)



Five Architectural Components

- Authentication and Admission Control
- Communication Security Services
- Key Management
- **Virtual Address Resolution (VARP)**
- OS−level Enforcement of Node Compartmentalization

Authentication and Admission Control: `sasd`, `snlogin`

- Multiple pluggable authentication mechanisms
- Policy encoding separate from enforcement
- Virtual IP address (vaddr) request

  vs.

  assignment in DHCP style
- **Node** = equivalent to a host in supernets (identified by a supernet id and IP address)

Communication Security Services: SNSL

- Network security services for
  - Confidentiality
  - Integrity
  - Authenticity
- IPSec encapsulation in tunnel mode
- Avoid IPSec NAT problem

Key Management: kms, kmc, kmd

- Groupkey management
- All group members share the same key: **Channel**
- Policy−based key revisions on events
  - join, leave, time interval
- Supernet channels are *small* enterprise networks that are secured against *outside*.

Virtual Address Resolution Protocol (VARP)

- Assume: Endpoint addressability:
  - Currently IPv4
  - Future: IPv6, DNS names, (RA,IRT), etc.
- Mapping between
  - Virtual IP addresses (vaddrs)
    and
  - IP address of computer hosting nodes

Virtual Address Resolution Protocol (cont.)

- Example:

```
0x00000123:10.0.3.2  –  192.146.122.79
```

- Localized scope (per supernet)
- Endpoint requirements:
  - VARP client functionality
  - Dynamic configuration of VARP service

OS–level Enforcement of Node Compartmentalization

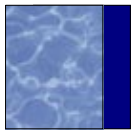
- OS enforcement of process encapsulation
- Inheritance of supernet membership on fork()
- Caching of address mappings and keying material

Status Quo

- Working prototype of communication component (on Sparc, and Redhat Linux, IPSec, C, Java).
  Limited availability as RedHat rpm
- Several design documents, white papers, presentations, related patents

In Progress + Future Work

- Prototyping of storage component (cnfs)
- Storage key management under development
- Secure Computing?
- Management Component?



Summary

- Create autonomous, secure networks around dynamically changing communities
- Requirements on infrastructure
  - Endpoint addressability
  - PUC enabling services: sas, varp, km
- Requirements on endpoints:
  - Address of admission control: DNS, config
  - Client sw for VARP, group key mgmt
  - SNSL layer

christoph.schuba@sun.com