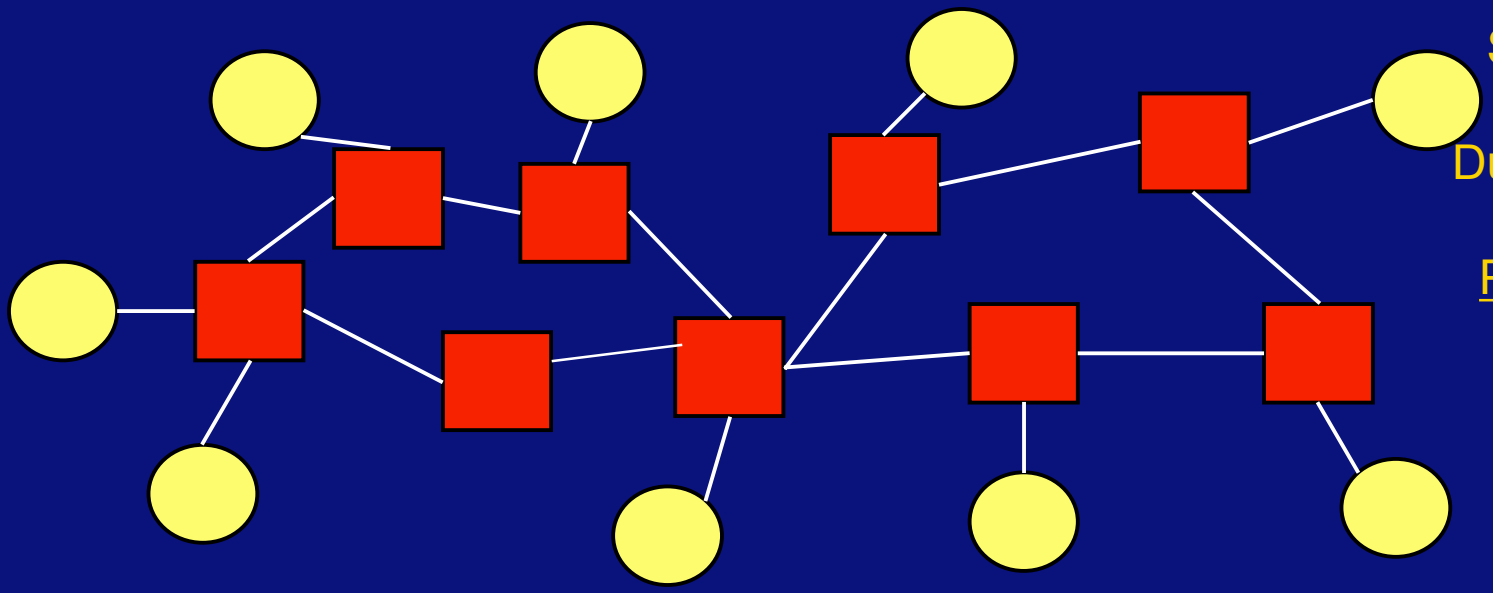
SwitchWare:
Lessons Learned, and Where Next?

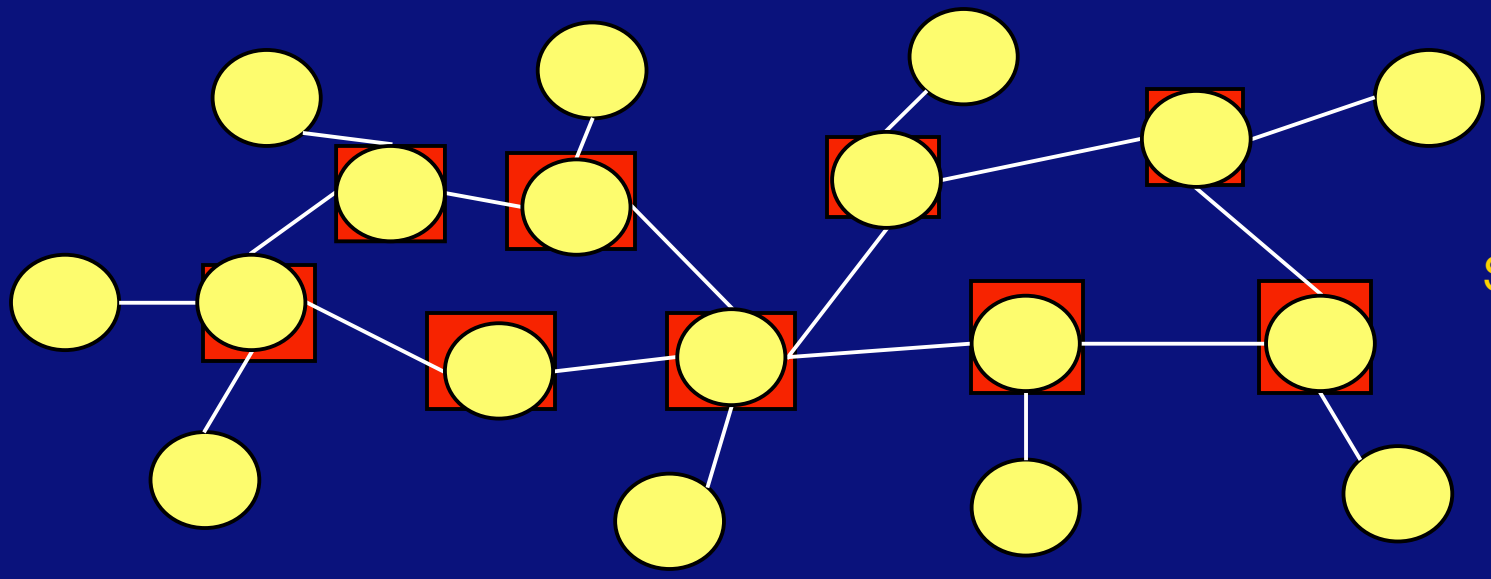
Microsoft Research, Redmond, WA
December 19th, 2006

Jonathan M. Smith
University of Pennsylvania
http://www.cis.upenn.edu/~jms

Active Networks enable new distributed systems



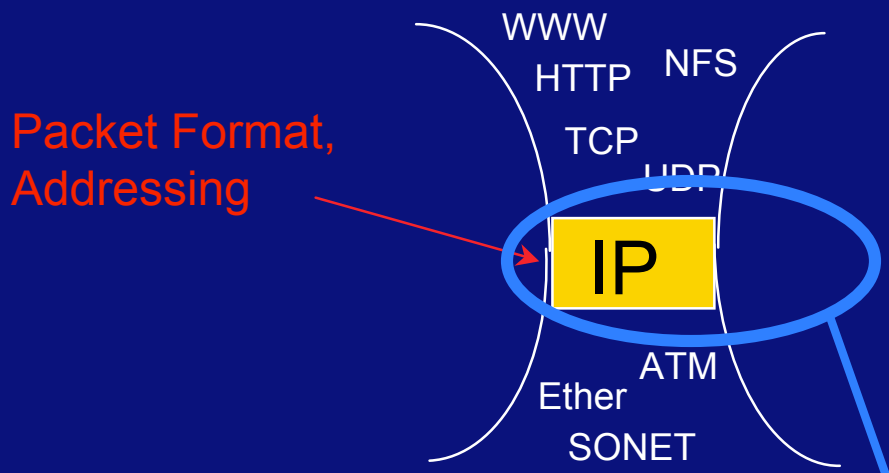
Smart Hosts
+
Dumb Switches
=
Passive Nets



Smart Hosts
+
Smart Switches
=
Active Nets

Virtual Infrastructures, e.g., IP

- IP is a network interoperability layer
- Interoperable through minimality:



Overlays (running at hosts)

Virtual Network Infrastructure
(runs globally)

Subnetworks (run IP locally)

Idea: Make waist *Programmable*

Accelerate Network Evolution

- Create *programmable* network nodes; standardize the programming model, not the nodes
- Change from Political Tempo (standards) to Technical Tempo (code)
- Balance Usability, Flexibility, Performance and Security

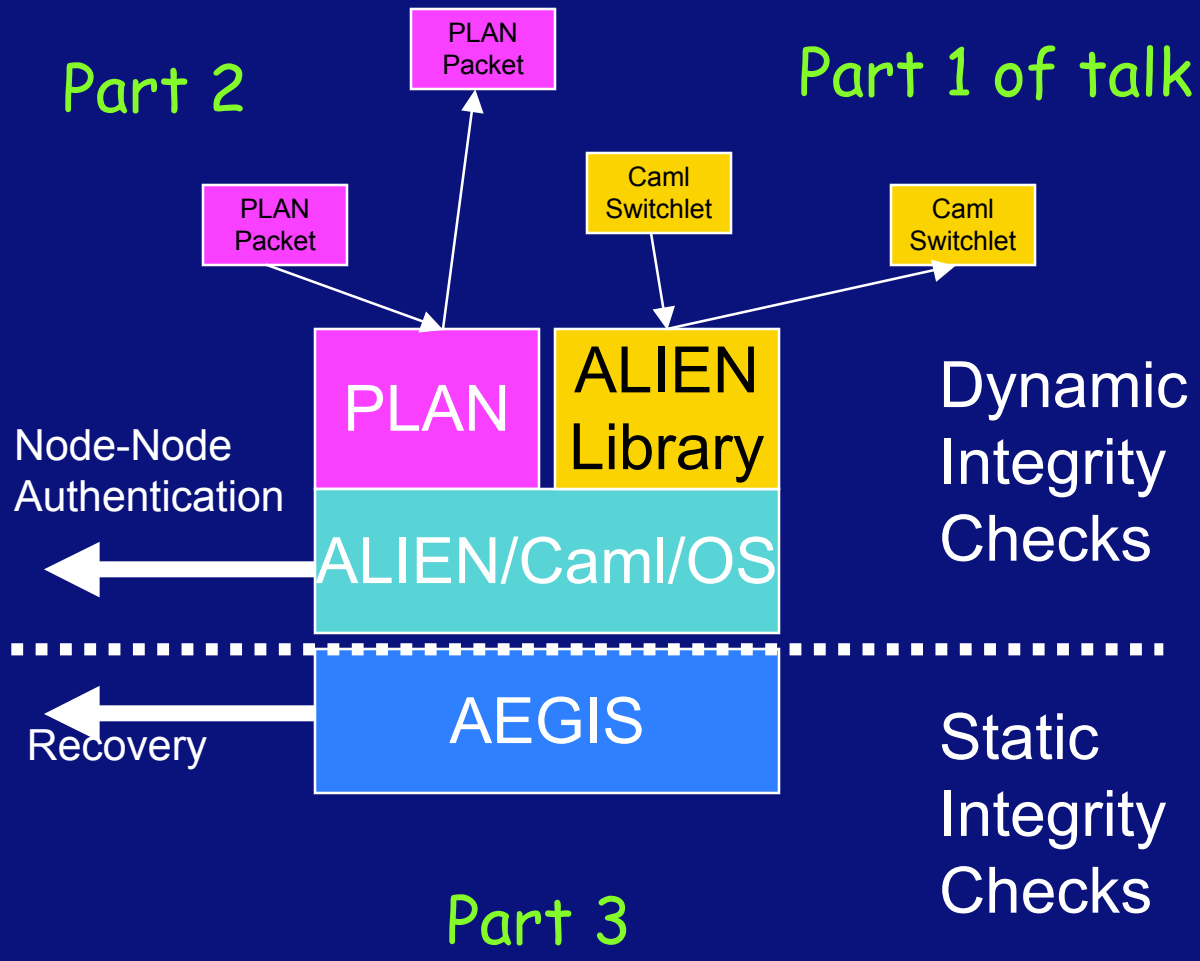
SwitchWare Approach

- Modern Programming Language technology can help with safety and security, maybe performance (cntxt X)?
- Build flexible node executing programs written in such languages
- Use P.L. typing to restrict programs for *safe multiplexing of node* in a network

A Language-Oriented Solution in 3 Parts

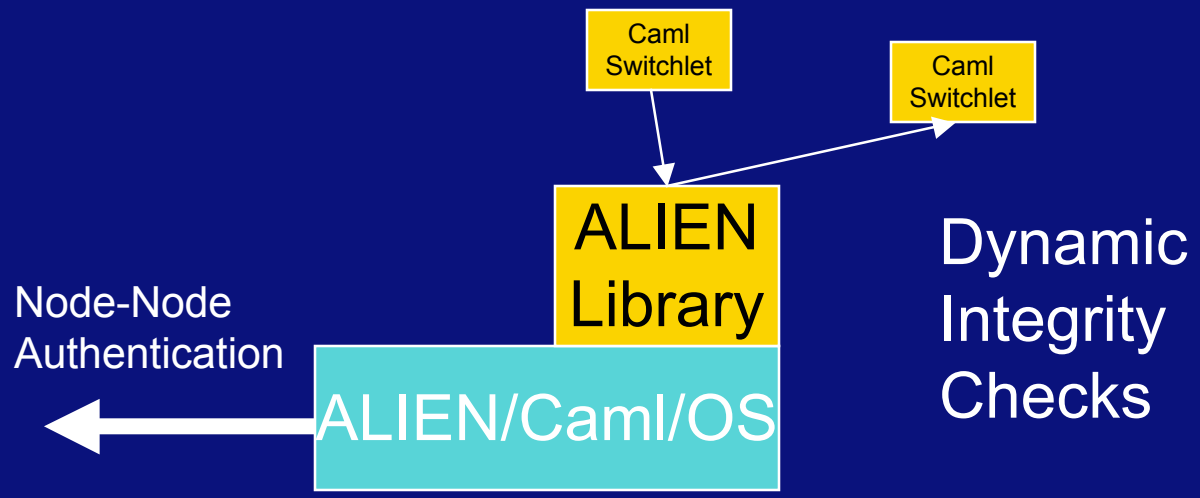
- *Switchlet Language* for users (SL)
  - →Formal semantics, restricted programs
  - →E.g, restricted CAML or Domain Specific Lang.
- *Wire Language* for communicating (WL)
  - →Enforce formal semantics across boundaries
  - →Cryptographic signatures + hashes
- *Infrastructure Language* for Virtual Machine (IL)
  - →formal semantics supported on metal: run-time
  - →Replace O.S. with P.L. runtime

SwitchWare Architecture



SwitchWare Architecture

Part 1

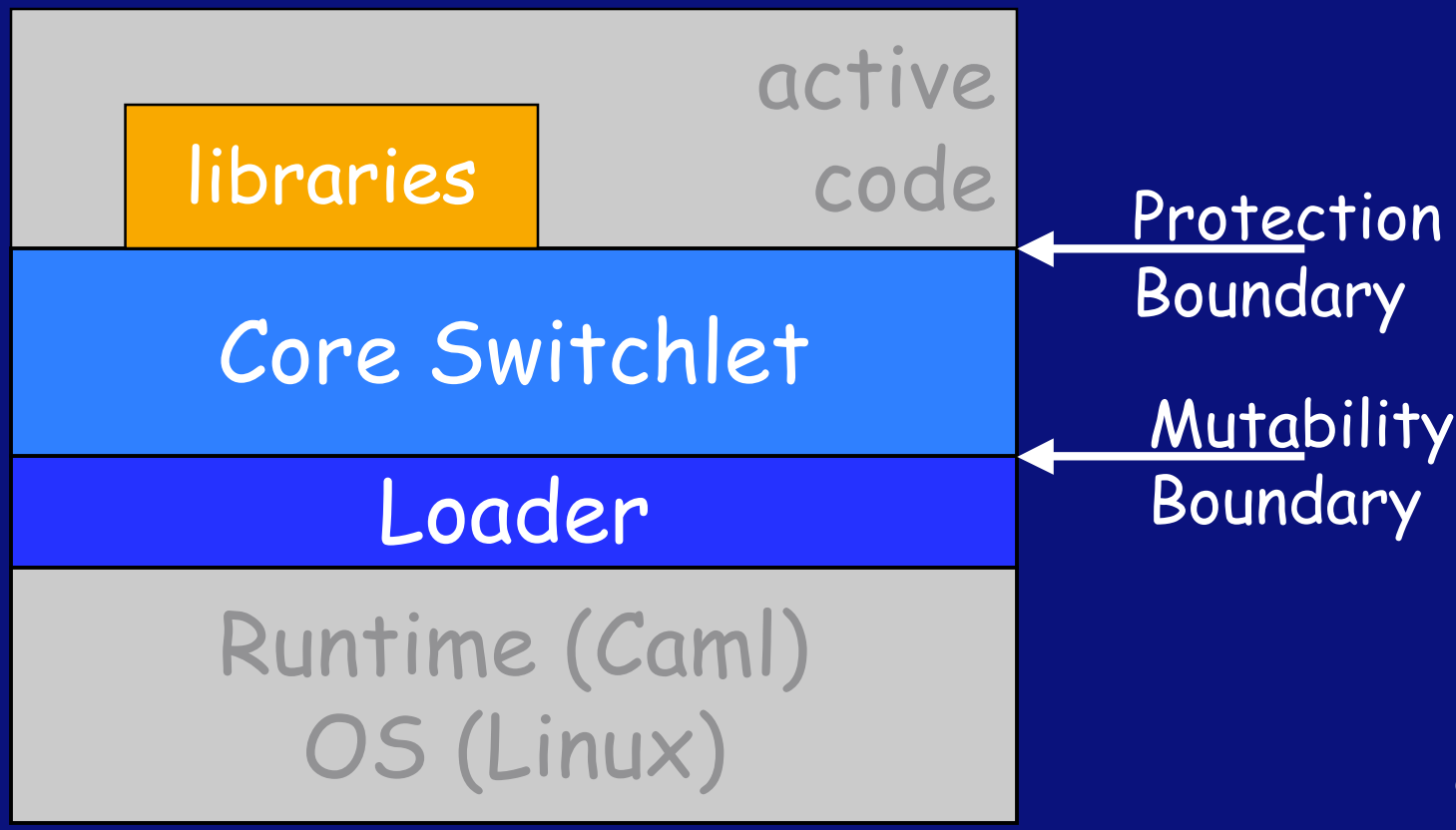


Dynamic Integrity Checks

Static Integrity Checks

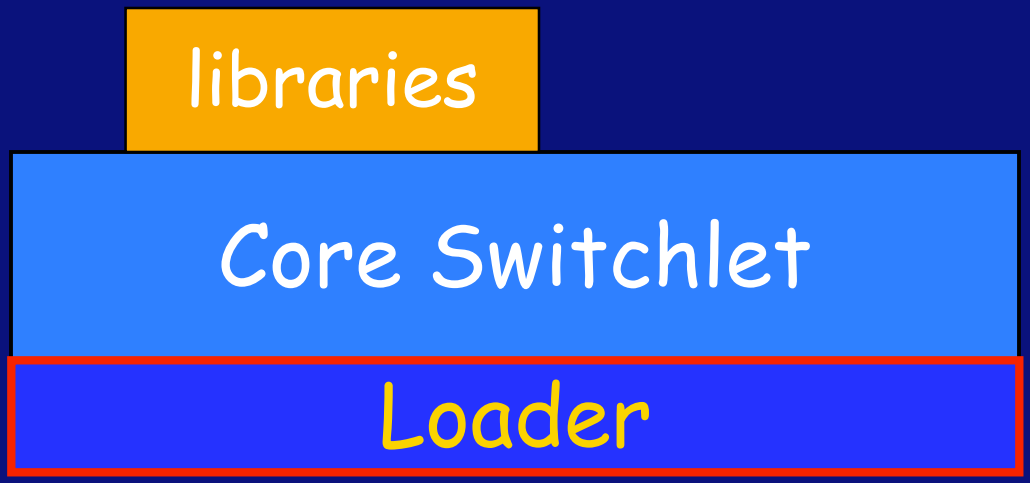
ALIEN Active Loader

- D. Scott Alexander's Ph.D. thesis



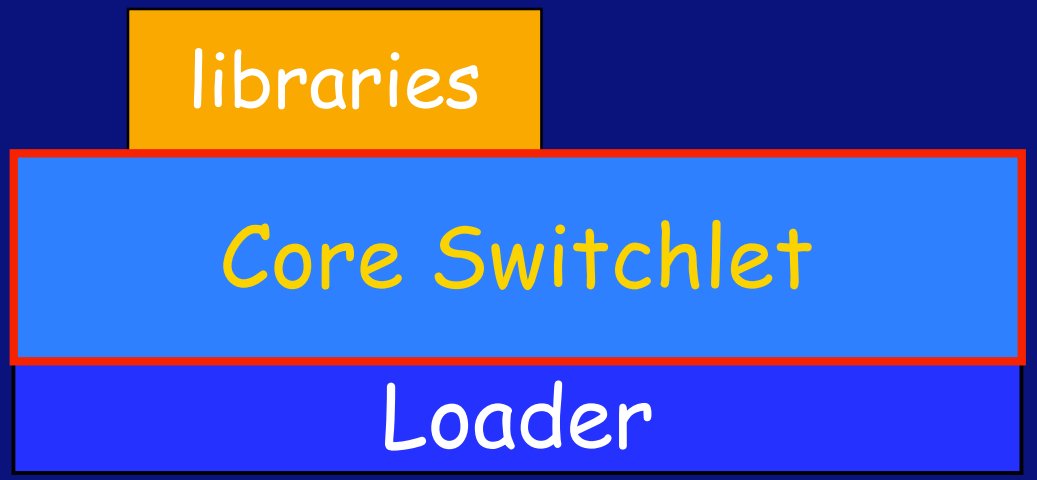
The ALIEN Loader

- startup routines
- active program loading
- system console
- mechanism only



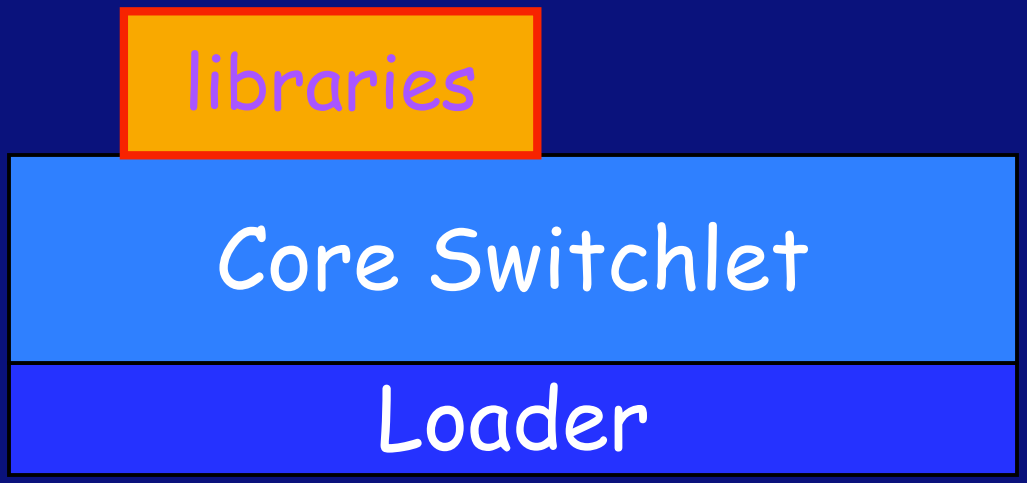
The Core Switchlet

- language primitives
- OS access
- network access
- thread access
- loading support
- message logging
- mechanism and policy



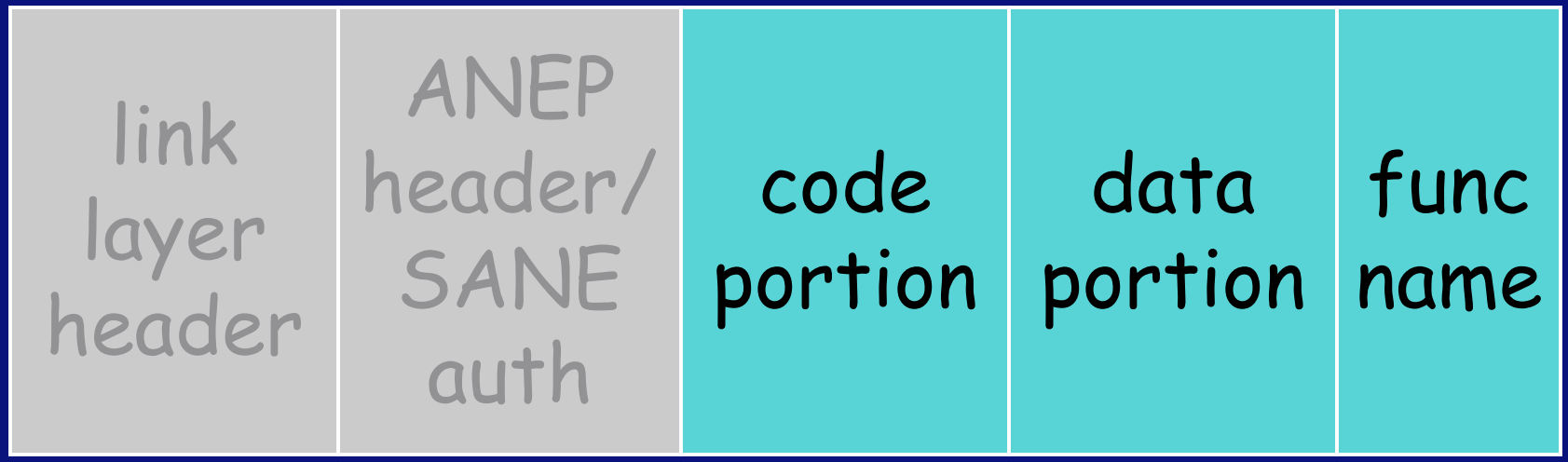
The Library

- "Everything else"
- IP
- UDP
- utility functions

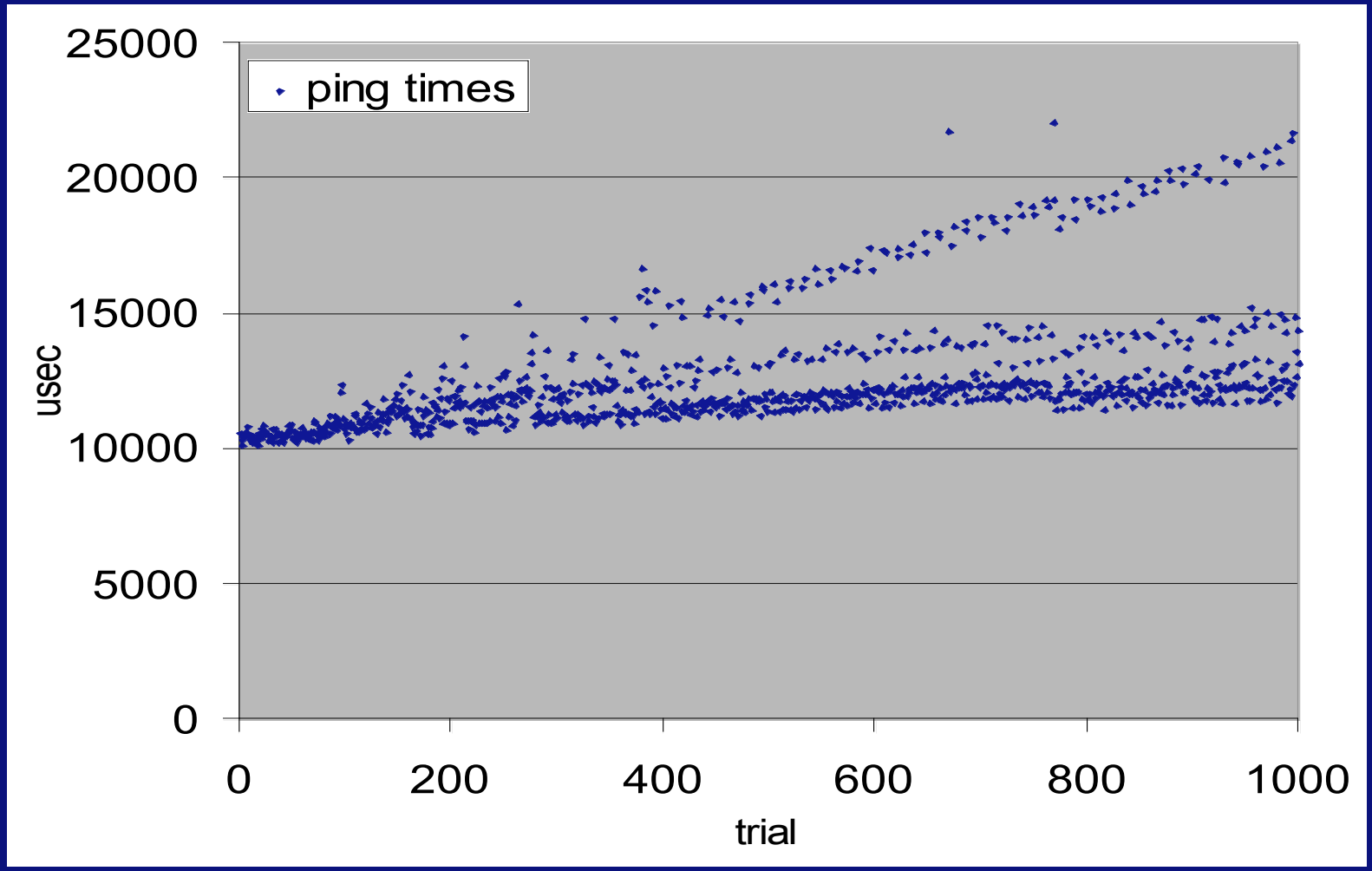


Active Packets in ALIEN

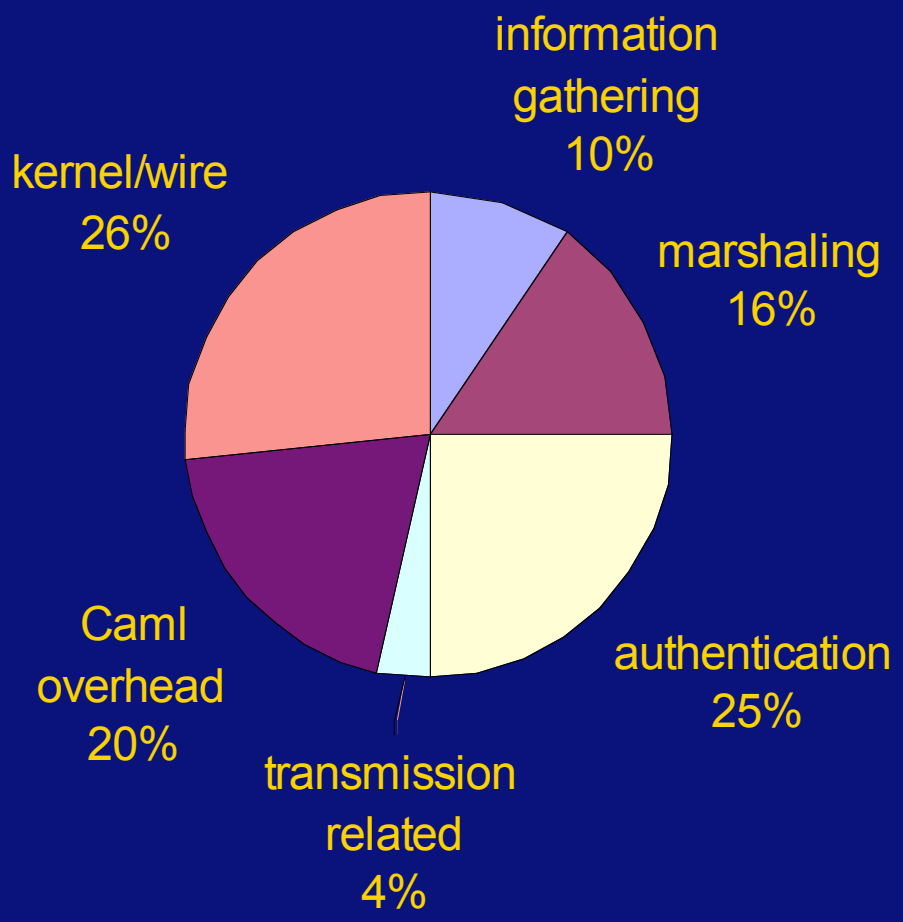
- If ANEP header indicates ALIEN
  - → SANE processing as part of ANEP
  - → Code portion is loaded
  - → *func* is called with code, data, and func name as arguments



saneping Performance (533 Mhz Alpha PC, 100M Ethernet)

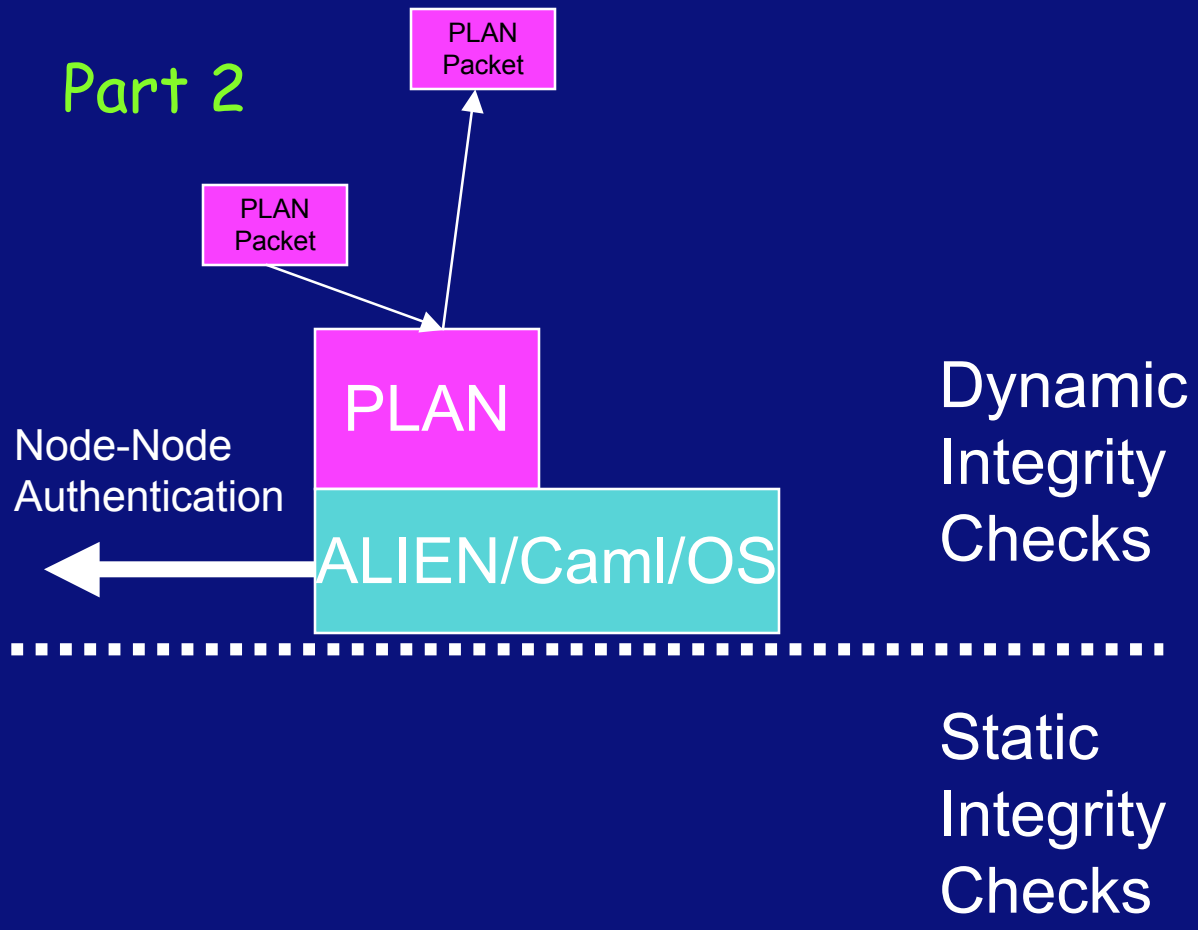


Breakdown of Costs in Alien



SwitchWare Architecture

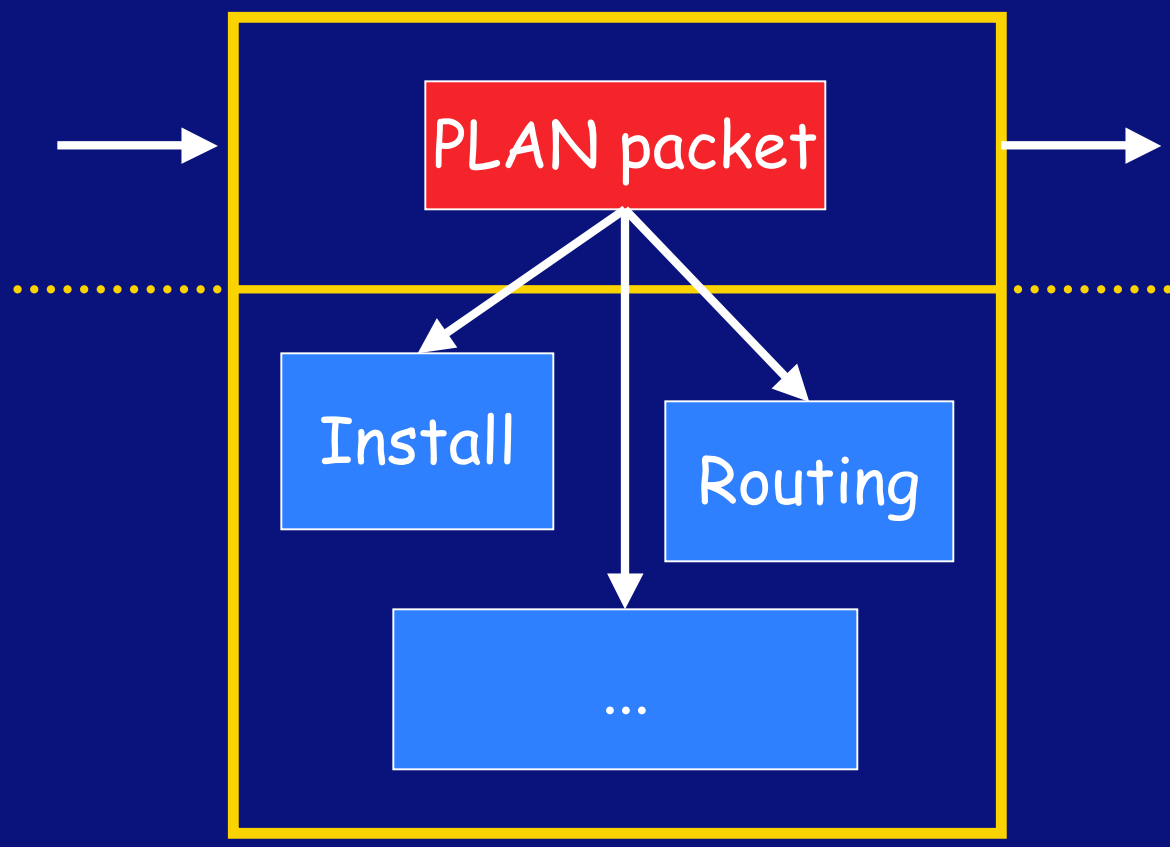
Part 2



Packet Language for Active Networks (PLAN)

- Hicks, Kakkar, Moore, Gunter, Nettles
- Active Packet-based approach
- Highly-restricted domain specific language (safe "glue" language, like the UNIX shell), extensible via ALIEN
- Active extensions for restricted ("privileged") things

PLANet: 2-level Architecture

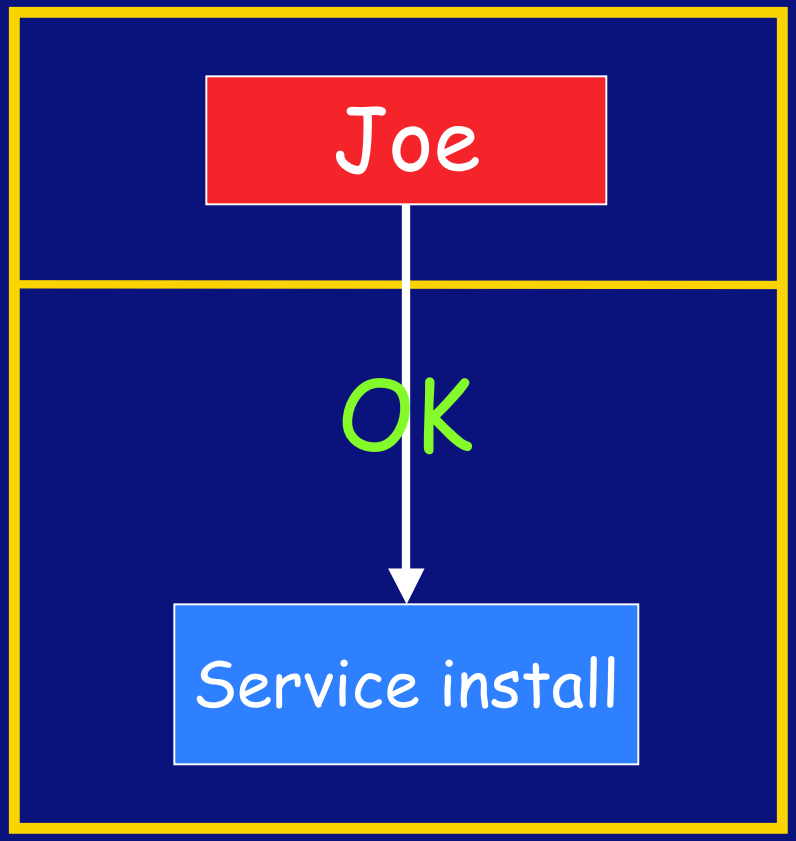


PLAN :
- safe
- in packet

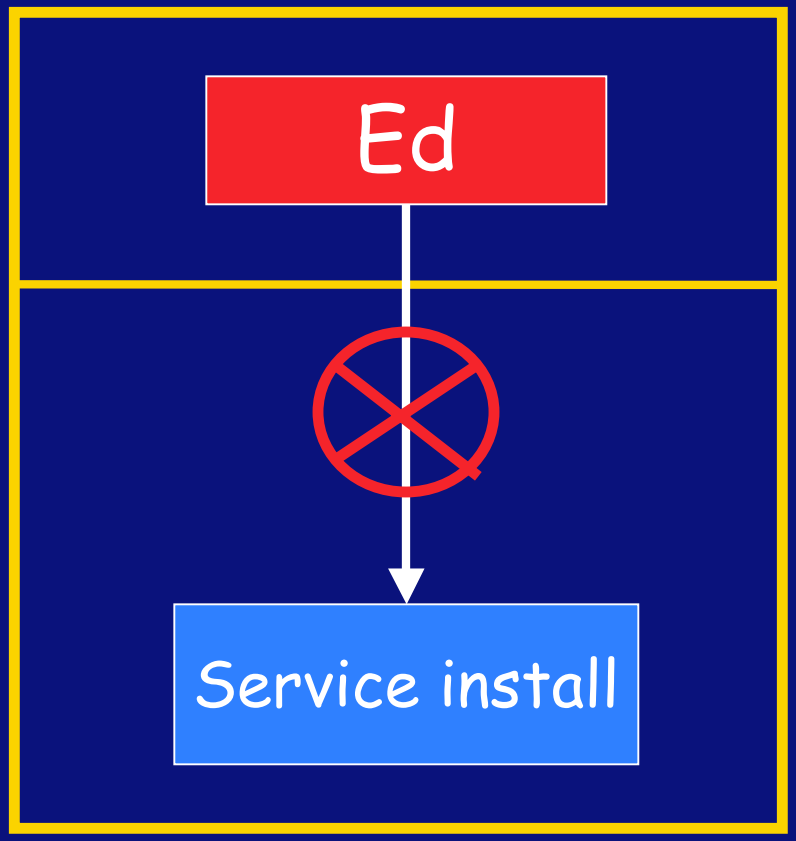
Services:
- general
- on router

(e.g., ALIEN)

Trust Management

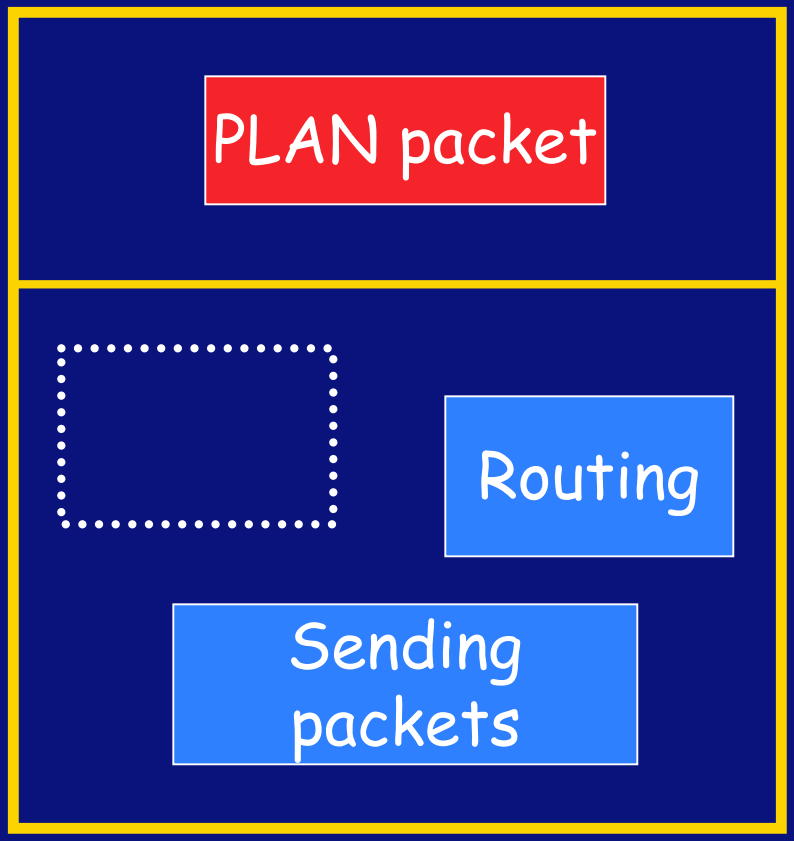


Trust Management



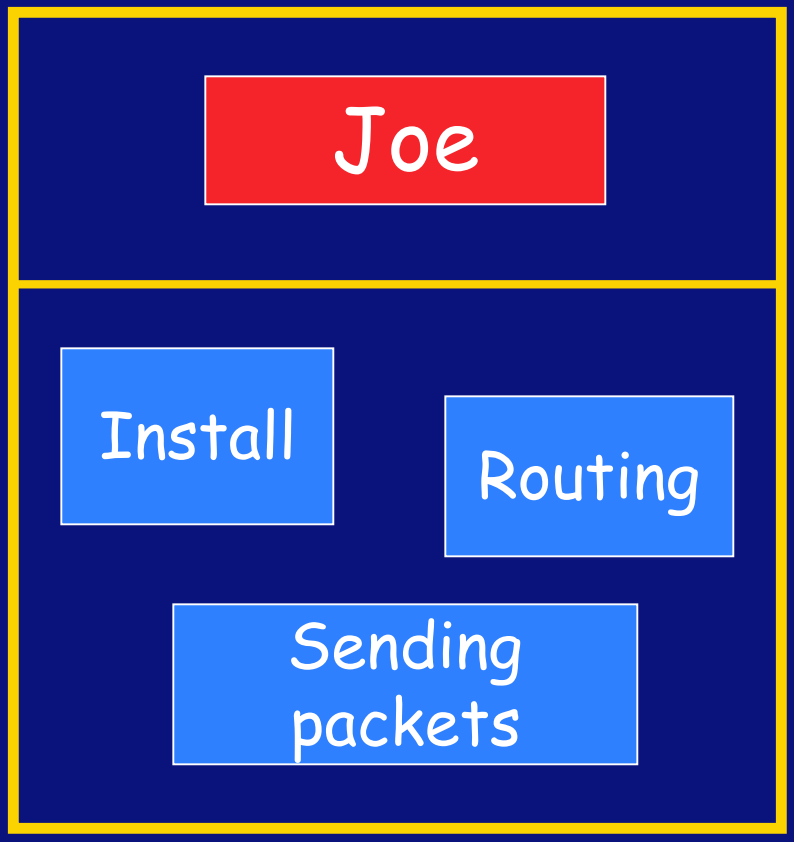
not allowed

Form of Service Policies: Access



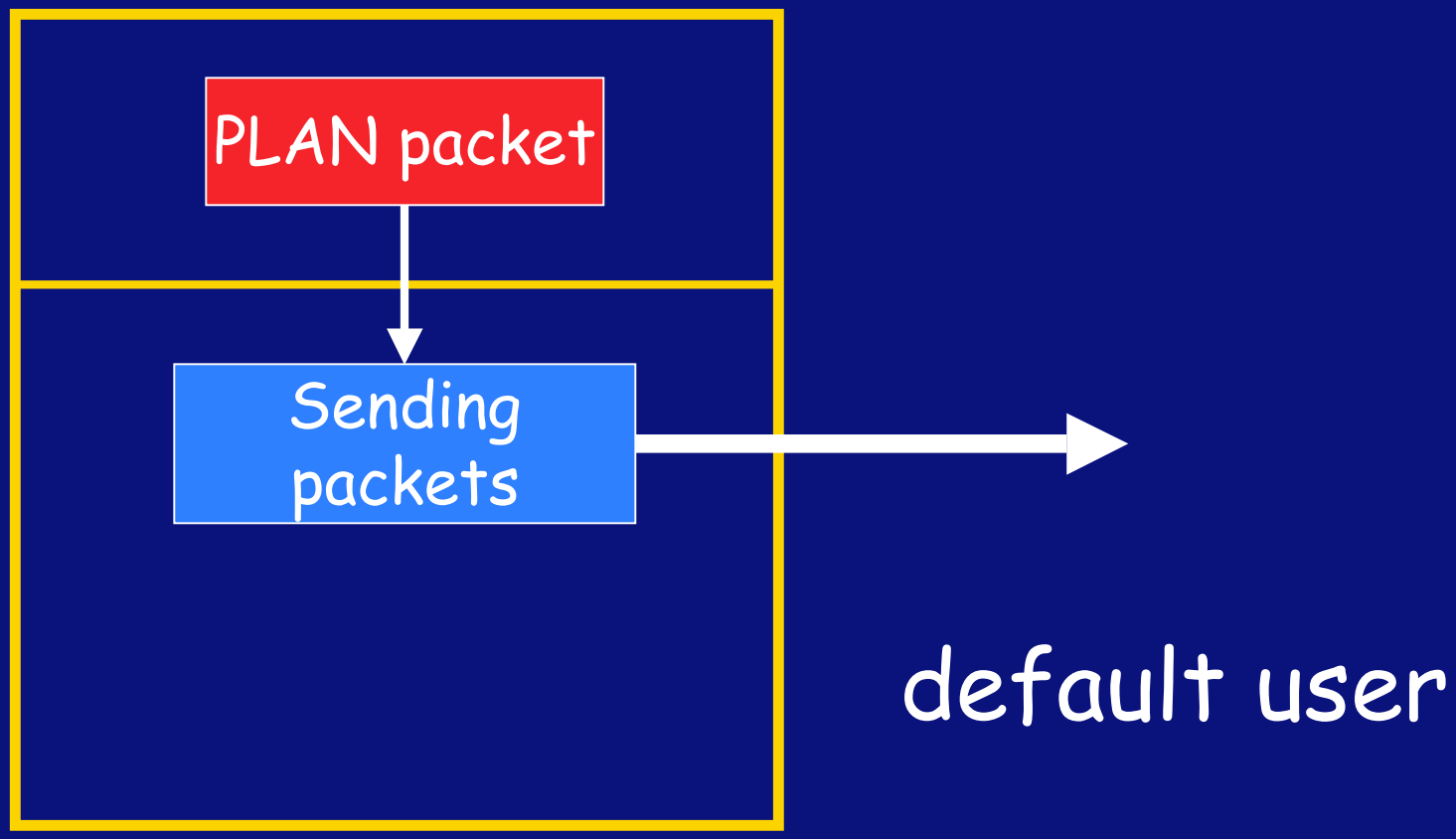
default user

Form of Service Policies: Access

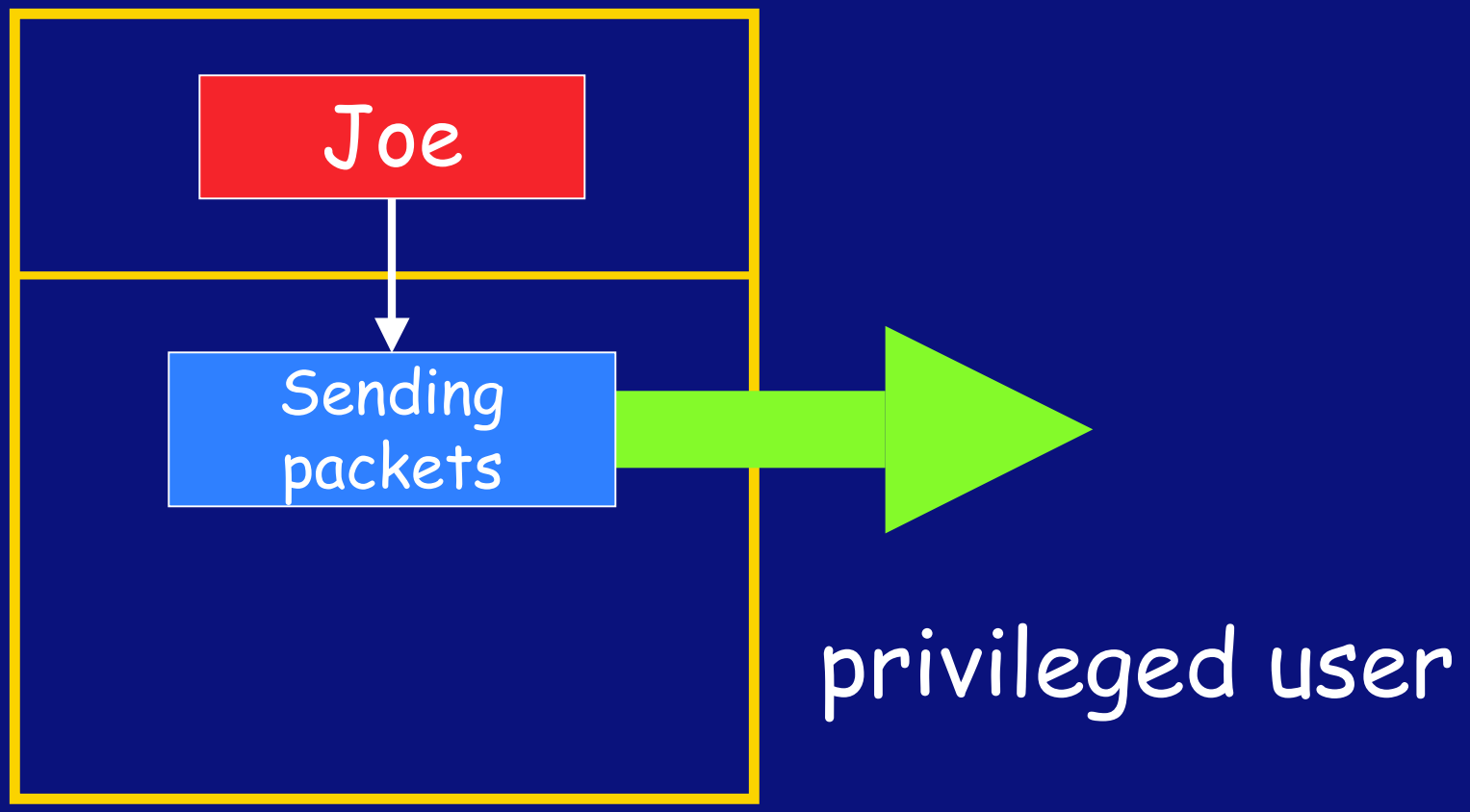


privileged user

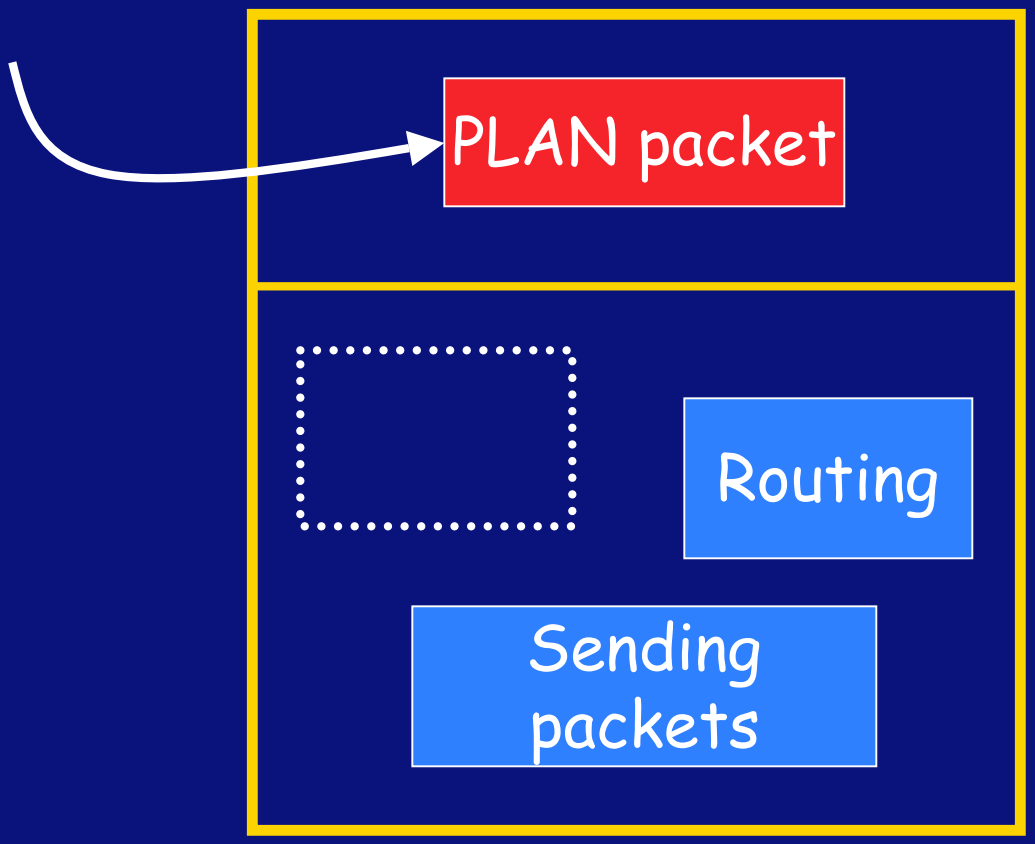
Form of Service Policies: Usage



Form of Service Policies:
Usage

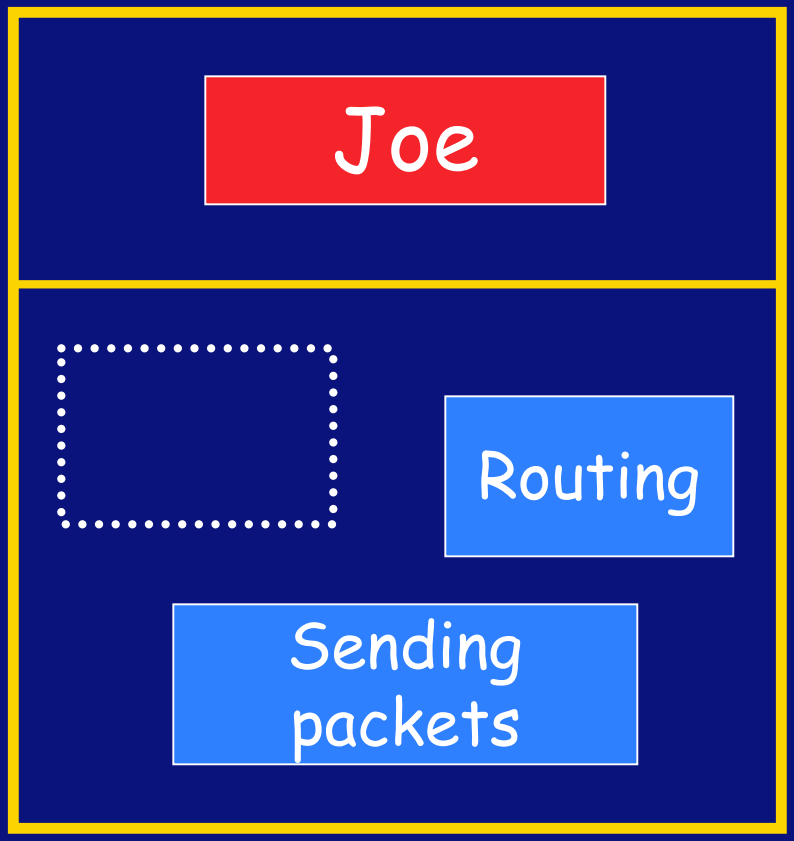


Security Procedure



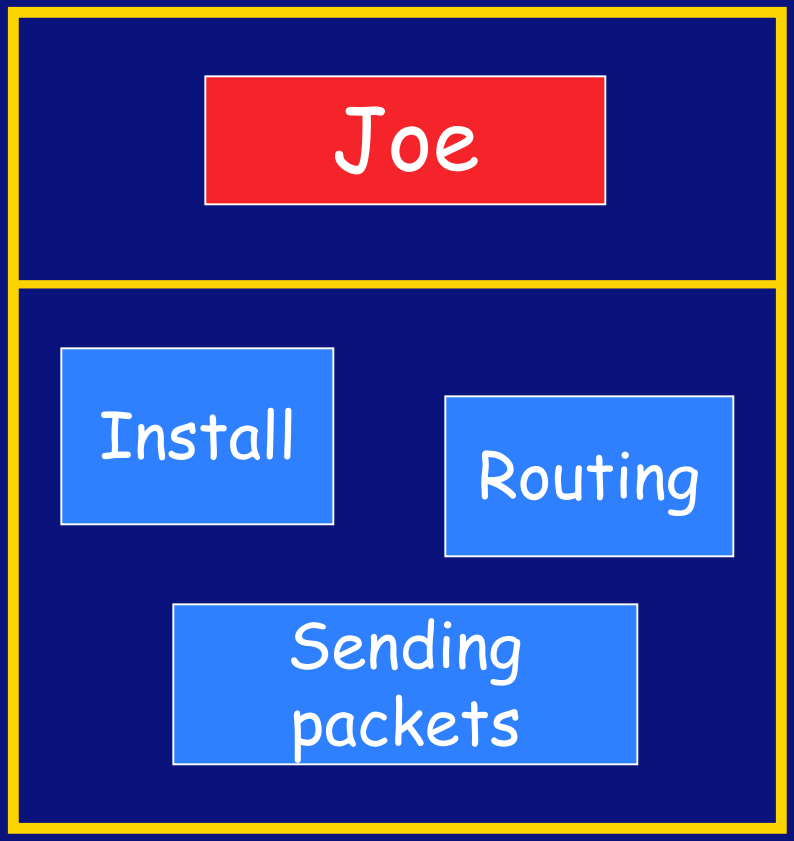
arrival
as default user

Security Procedure



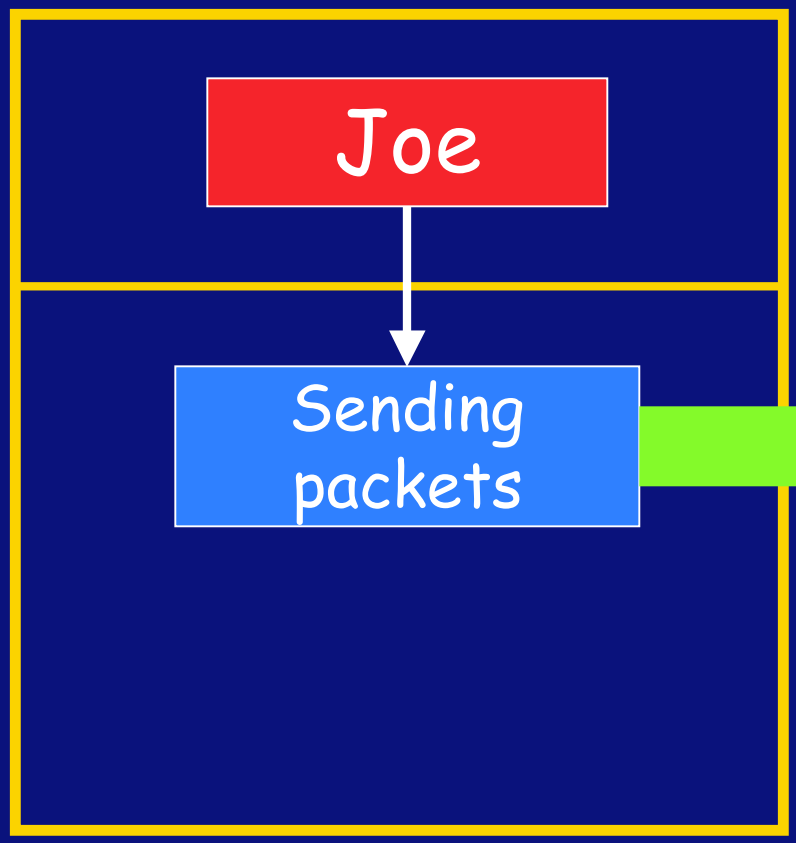
authentication

Security Procedure



namespace adjustment

Security Procedure



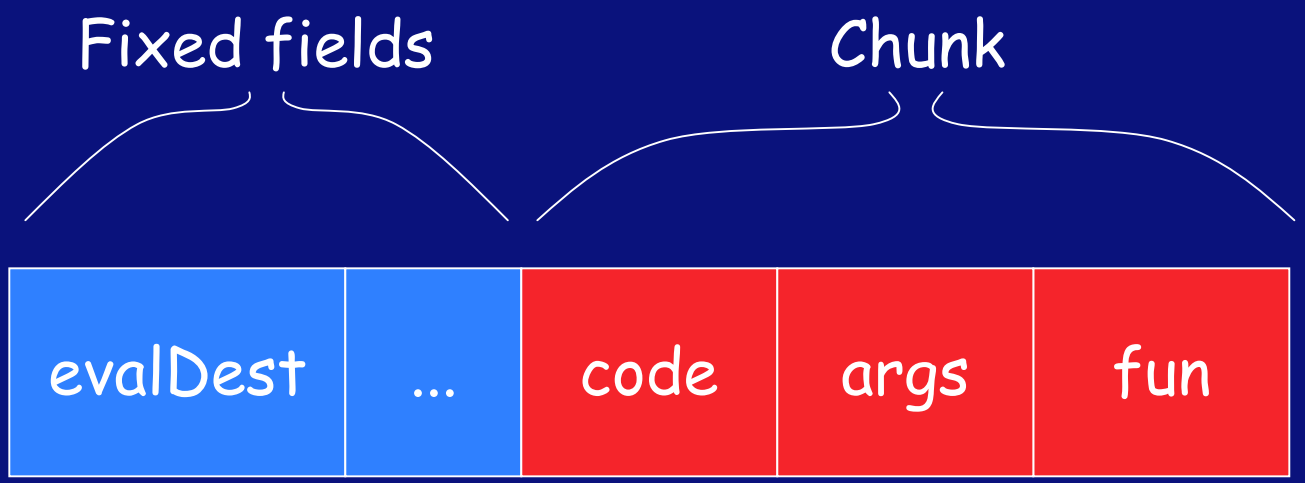

```
...
if Joe then
   more bandwidth
...
```

per-usage adjustment

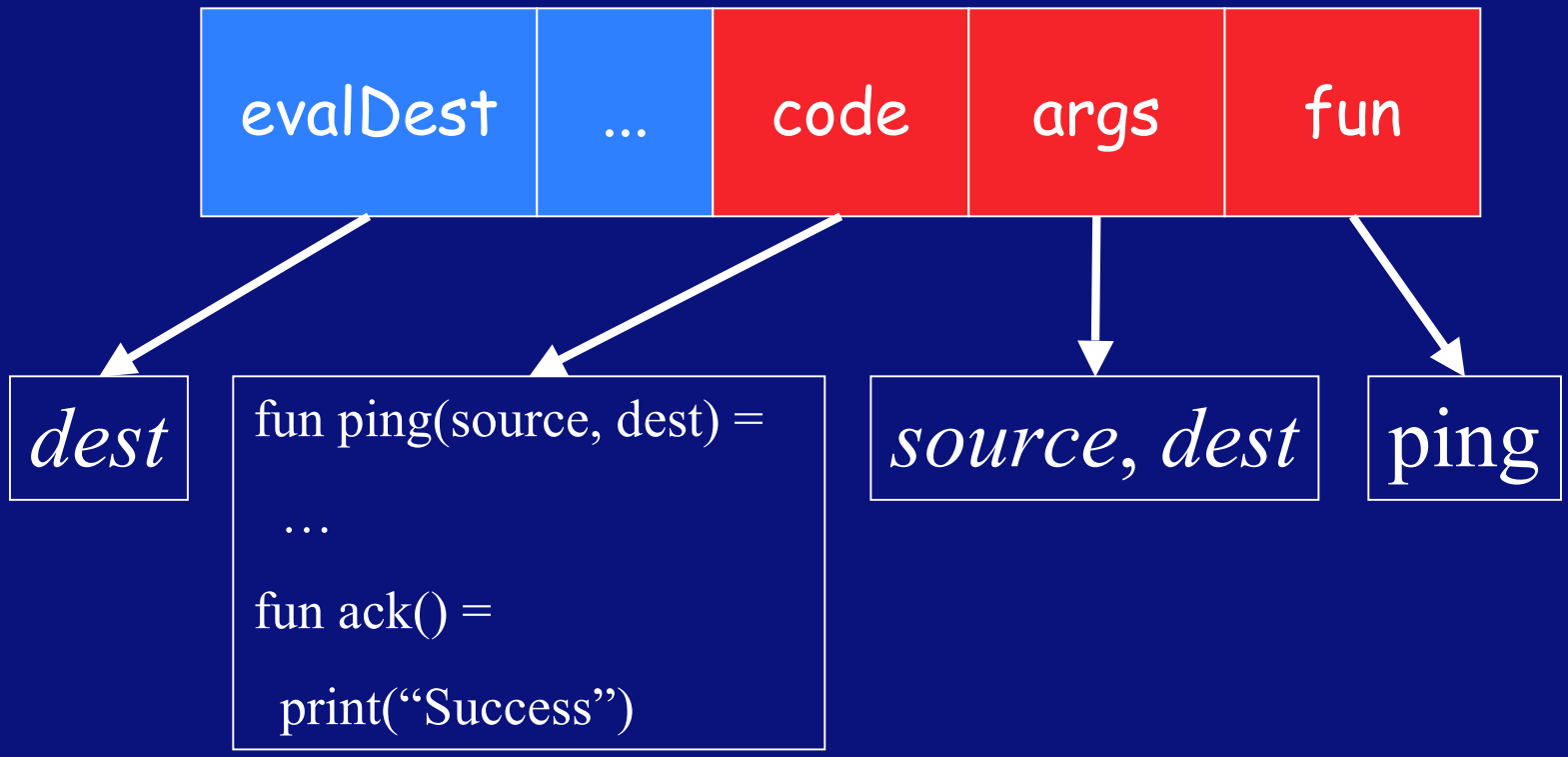
Chunks - units of authentication

- Unit of evaluation in PLAN
  - → like a suspended function call
- First-class
  - → can be manipulated as data within PLAN programs
- Useful programming construct
  - → encapsulation via `eval`

Chunks - in PLAN packets



Ping packet


evalDest
...
code
args
fun
dest
fun ping(source, dest) =
…
fun ack() =
print("Success")
source, dest
ping

Core Service

```
authEval: 'a chunk * sign -> 'a
```

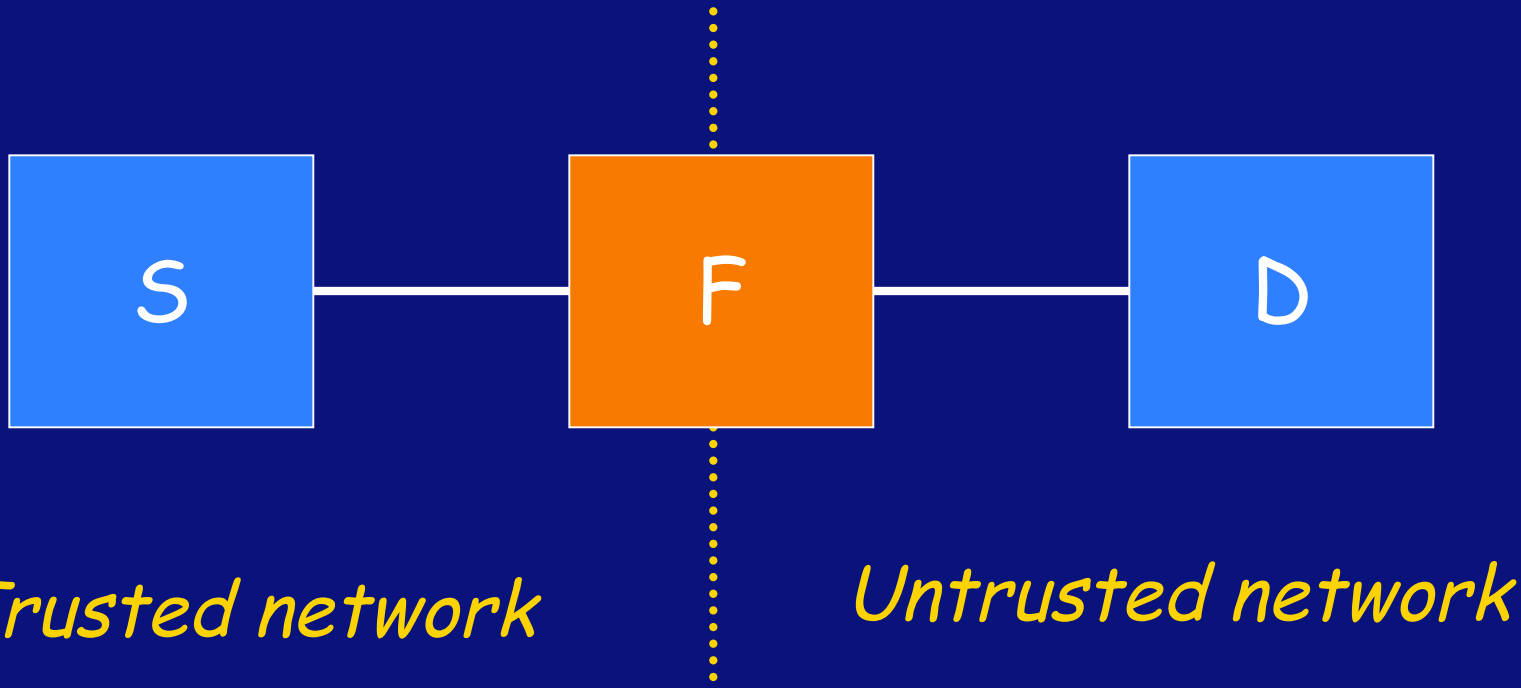
- takes a chunk and an HMAC digital signature and authenticates the chunk
  - → if successful, performs namespace adjustment and evaluates the chunk

Application: An Active Firewall

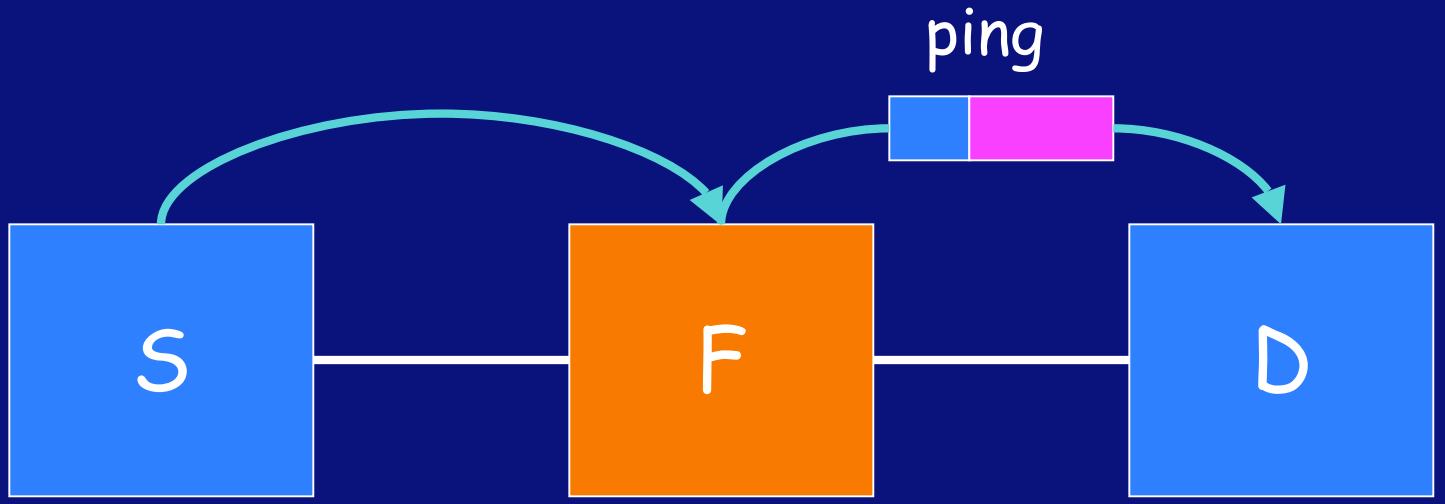
- Rather than *filter* external packets, *restrict their privilege*
- Accomplished by encapsulating incoming packets with service-restricting chunk

```
fun wrap(c,sign) =
   (zeroRB(); authEval(c,sign))
```

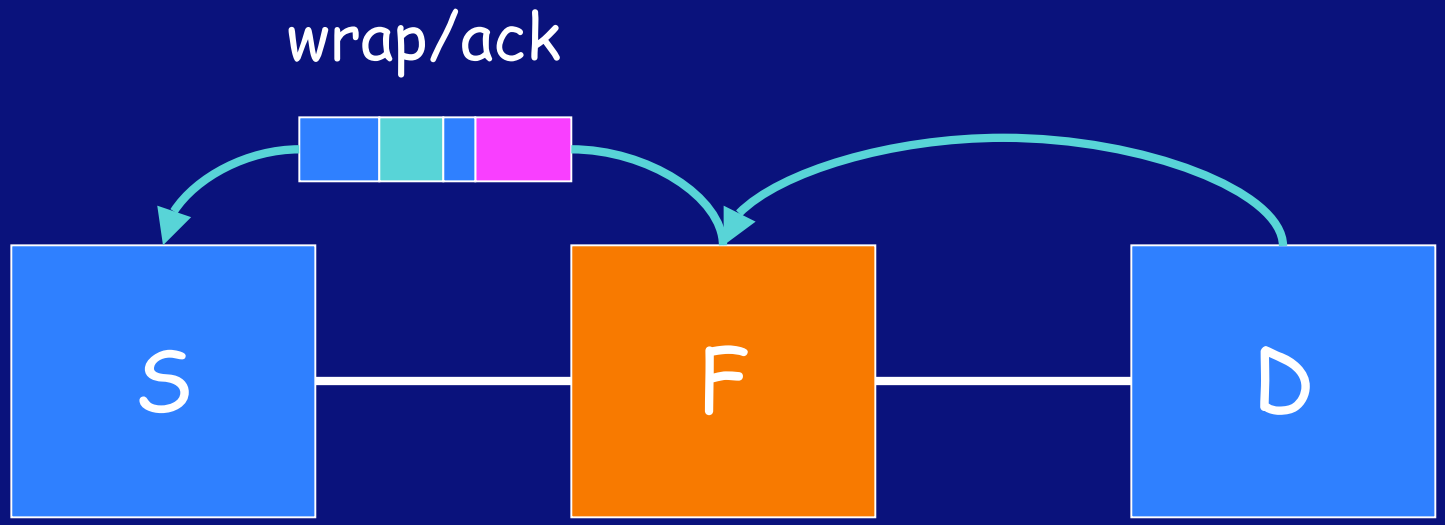
Experimental Setup



Outgoing Ping

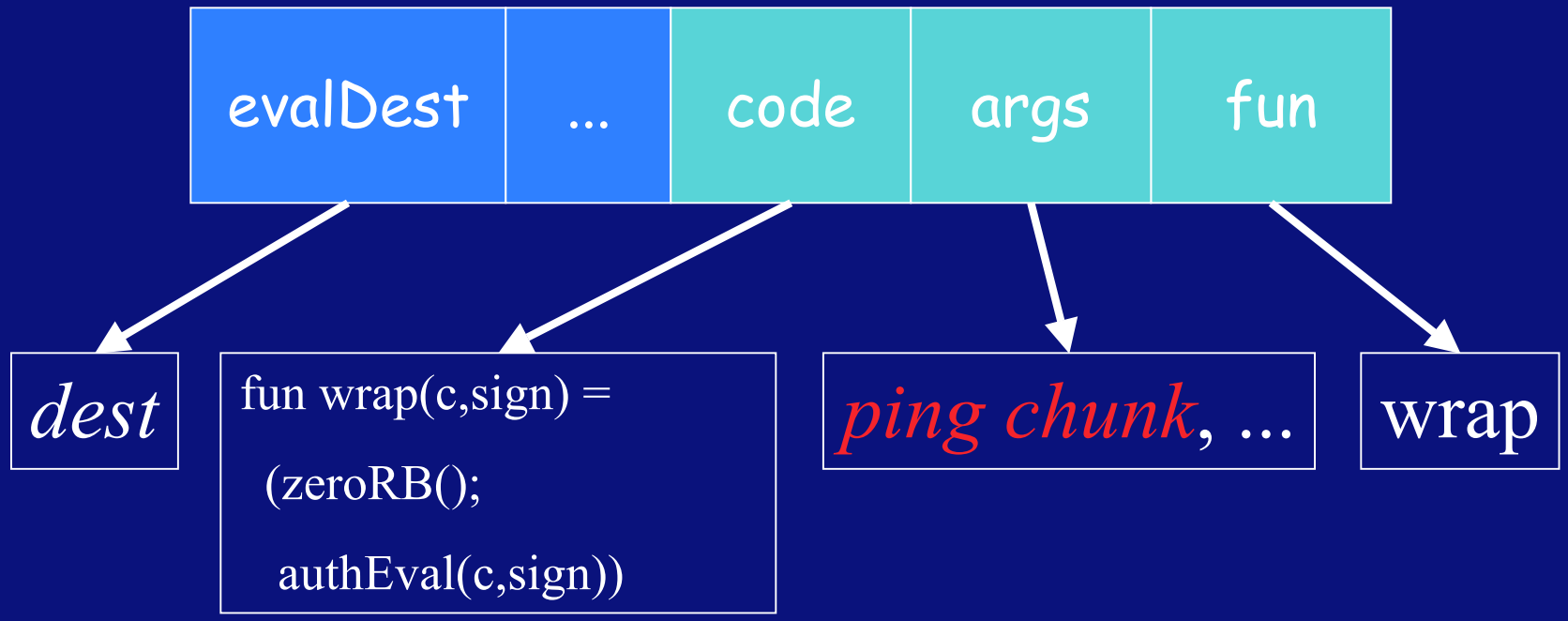


Returning Acknowledgement

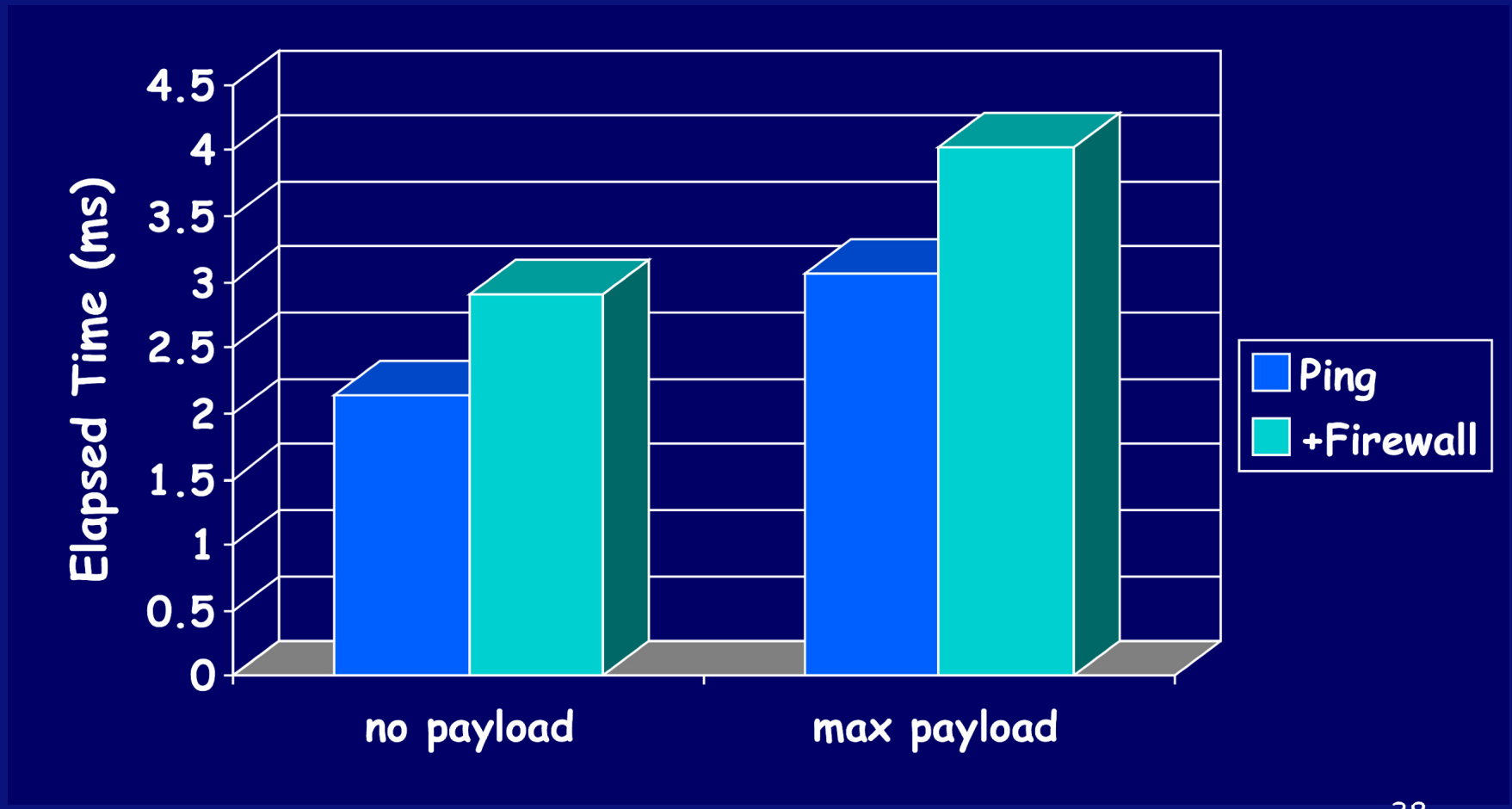


Firewall signs as and encapsulates packet chunk

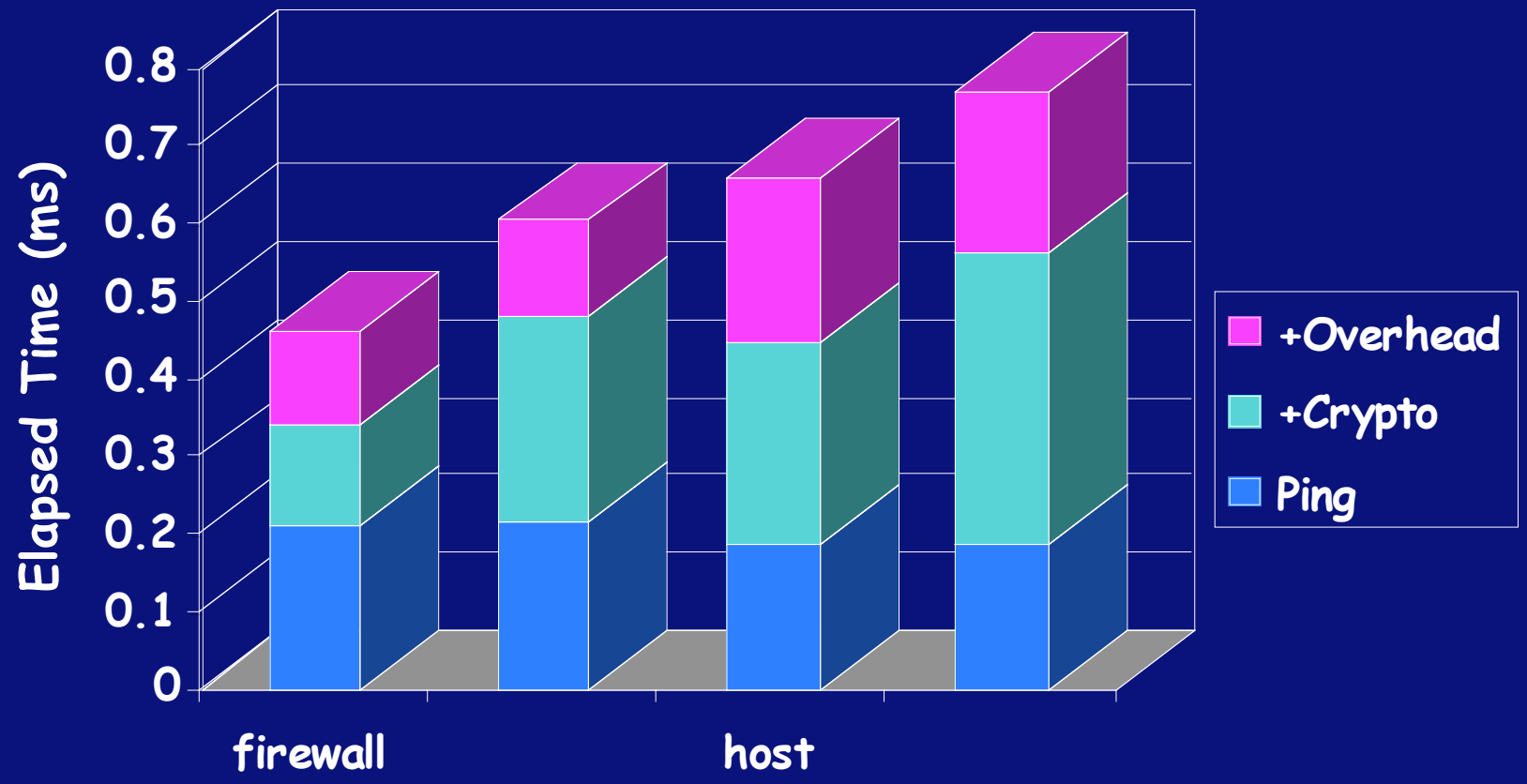
Firewall-wrapped Ping packet



Firewall Performance



Firewall Overhead Breakdown

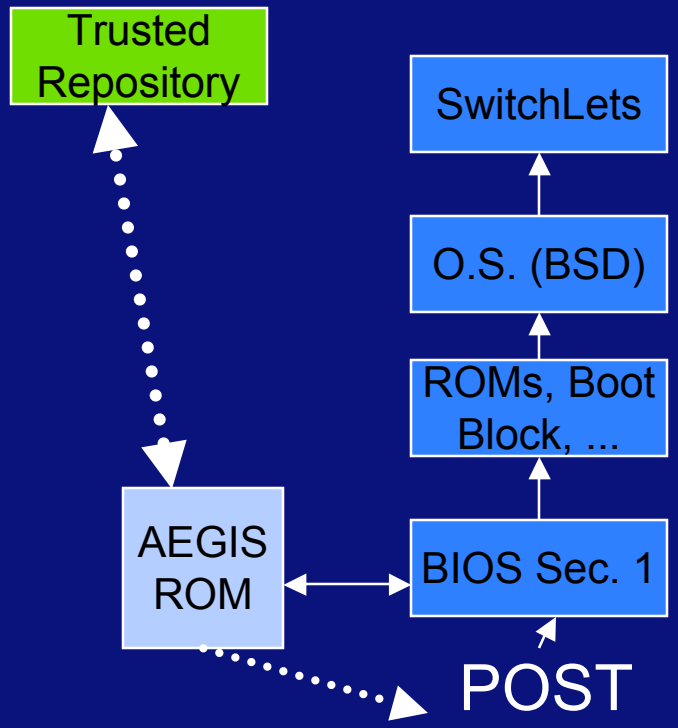


SwitchWare Architecture

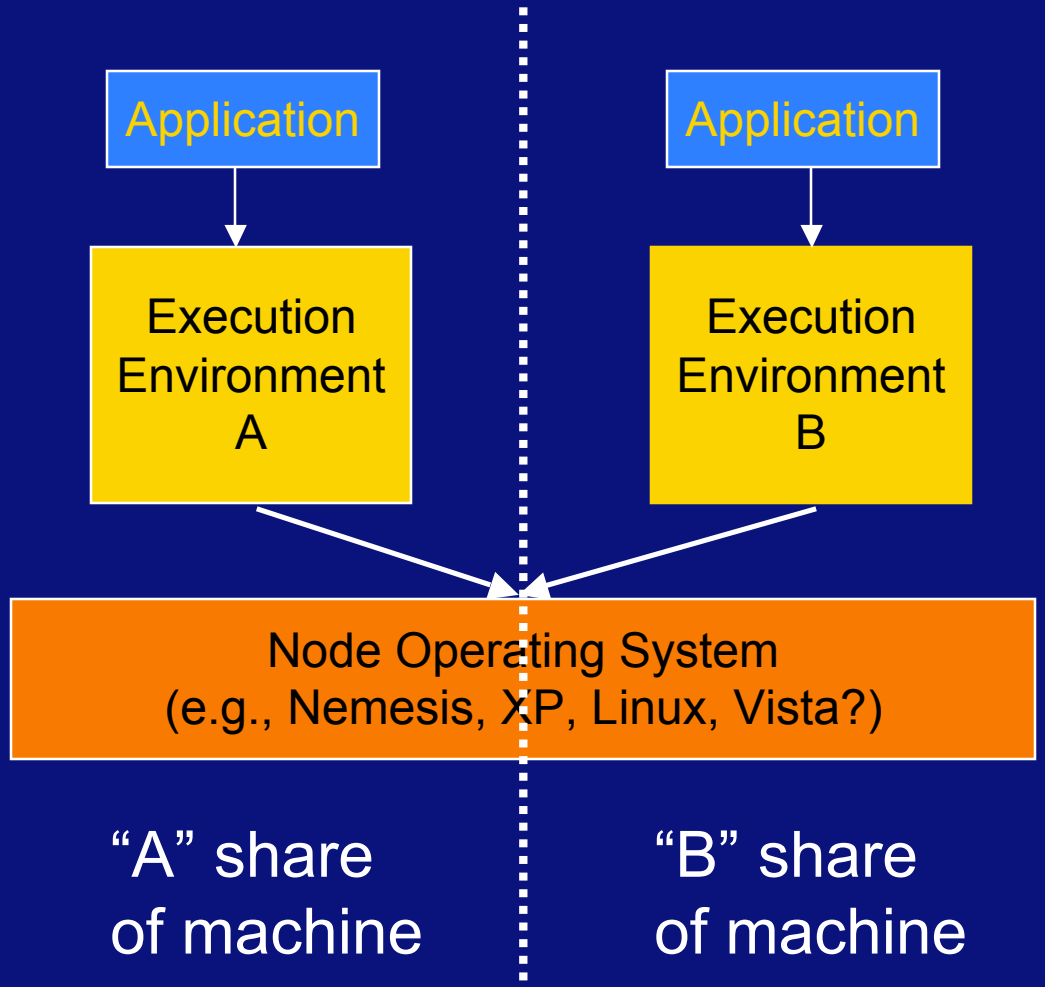
Part 3

Integrity of the Runtime/O.S.: AEGIS Secure Bootstrap

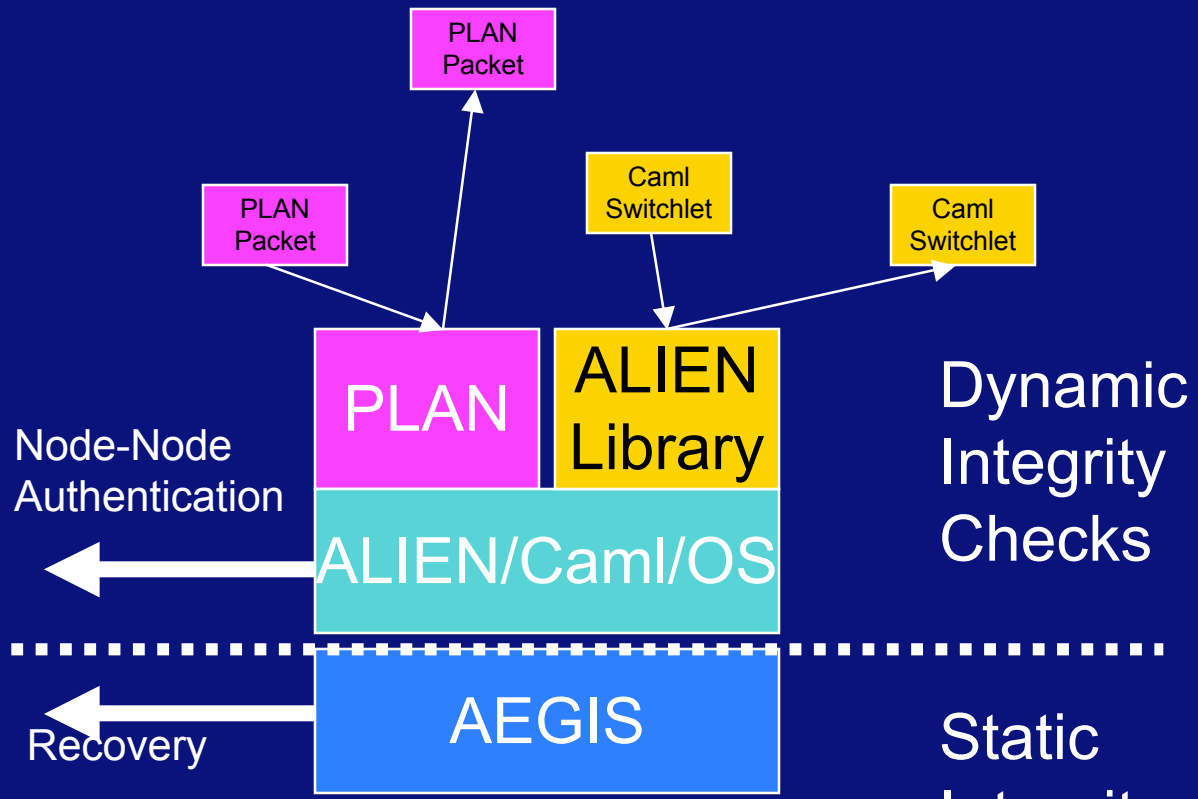
- Integrity Guarantees for Dynamic Integrity Checking



Resource Controlled AN Environment (RCANE):



SwitchWare Architecture

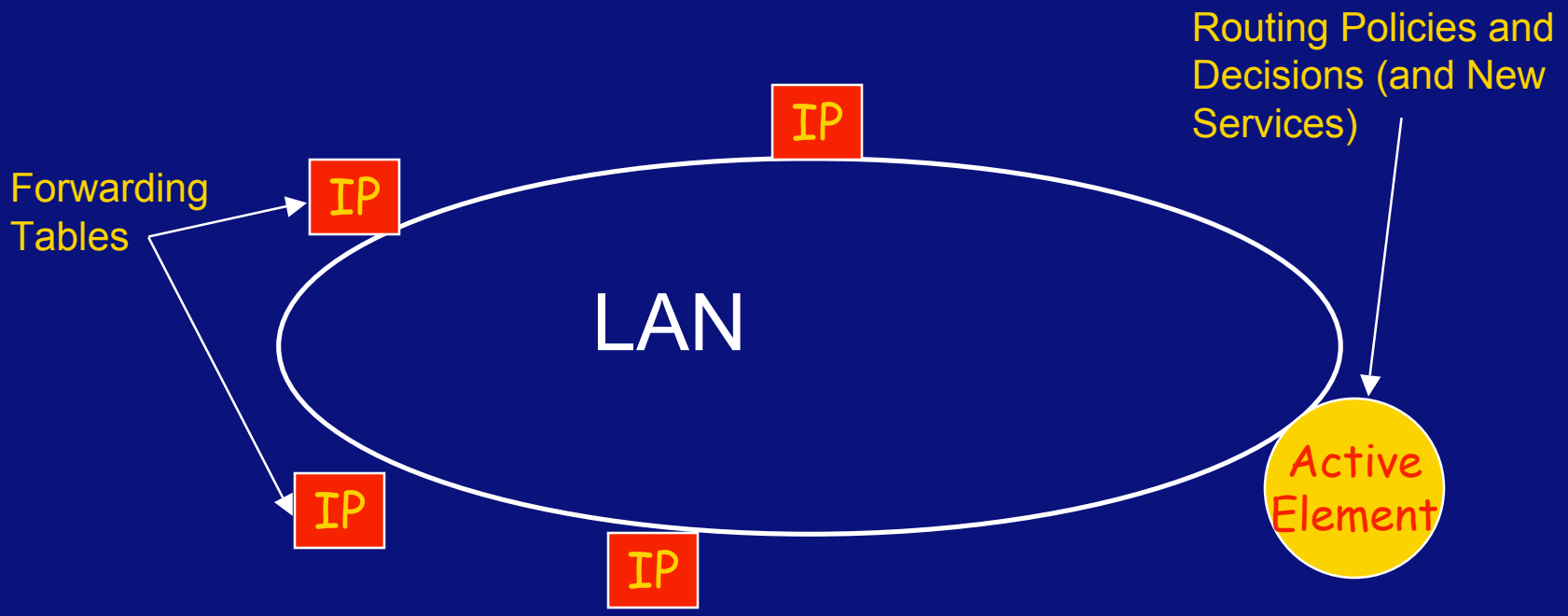


Lessons Learned

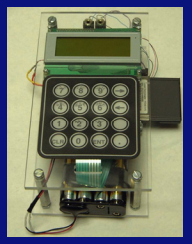
- Interoperability problems not removed; just moved.
- Performance acceptable for access networks
- CAML technical win, marketing lose
- Restricted language for packets a win
  - →May need to augment with cryptographic tools
- Did not allow enough time for network versus node work (should have been 5-6 year project, not 3+)
- Convincing (not ping) Active Applications hard

Next: Active Router Control (Active Border Gateways?)

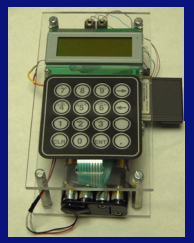
- IP Router/Forwarders co-located with Active Elements:



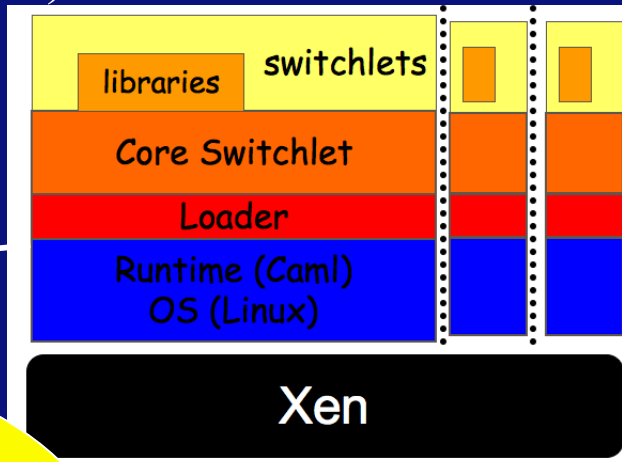
Xen Programmable Edge Router Technology (XPERT): flexible & sliceable



IMP Mobiles



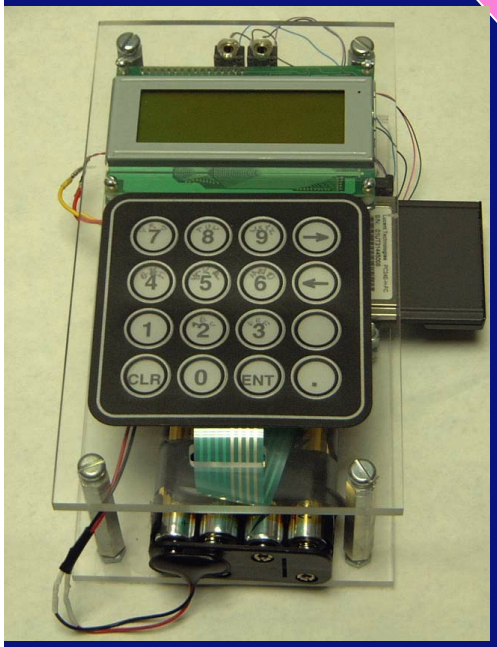
Penn Orbit



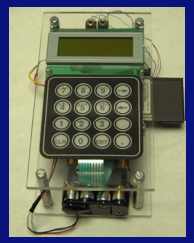
XPERT

Virtualized Transport Infrastructure

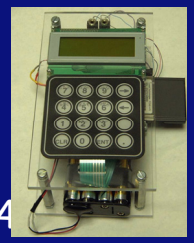
XPERT



Rutgers Orbit



IMP Mobiles



M. DeYoung, N. Henke, G. Wai, and J. Smith, "Rethinking Mobile Telephony with the IMP," in Proceedings, European Wireless, Barcelona, SPAIN (February, 2004), pp. 378-386.

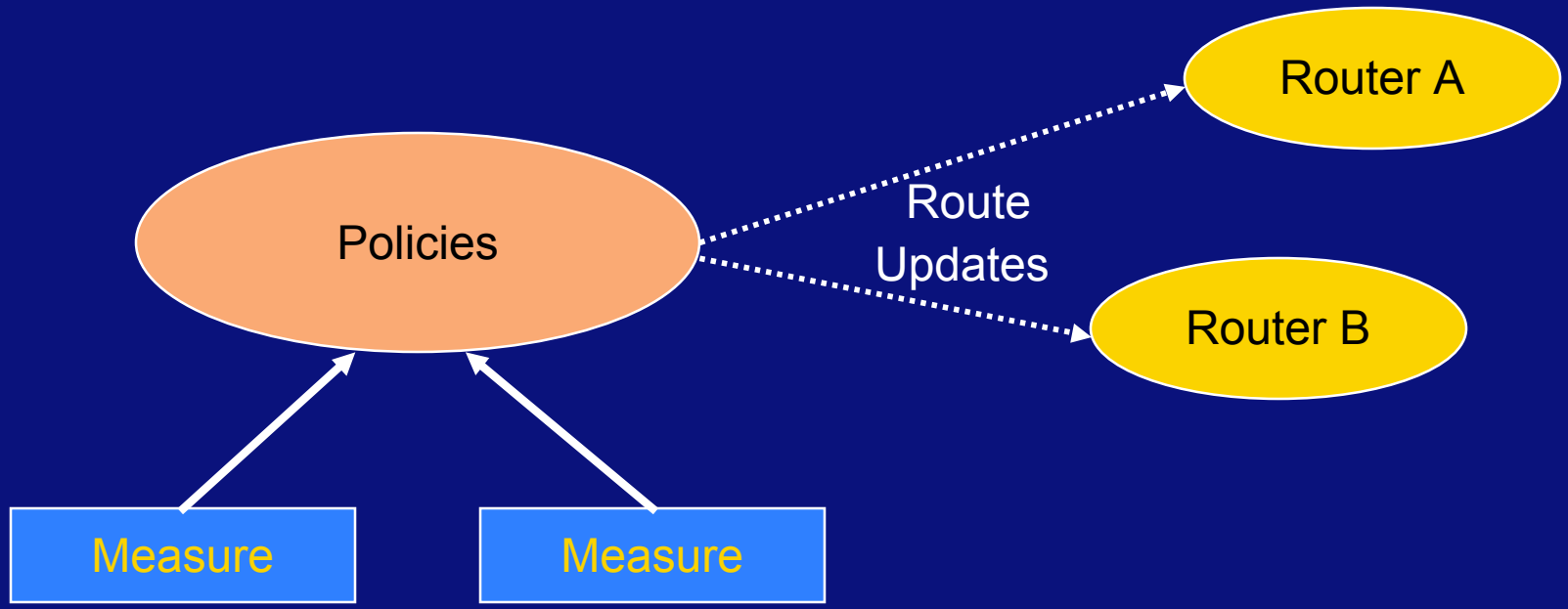
Acknowledgments:

- SwitchWare was a joint project of Penn and Telcordia, supported by DARPA
  - → Extensive literature
    - ✦ Responsible parties named there!
  - → RCANE was a collaboration with Cambridge University, described in Paul Menage's Ph.D., and supported at Penn by NSF
- Hewlett-Packard, Intel, 3Com & Nortel

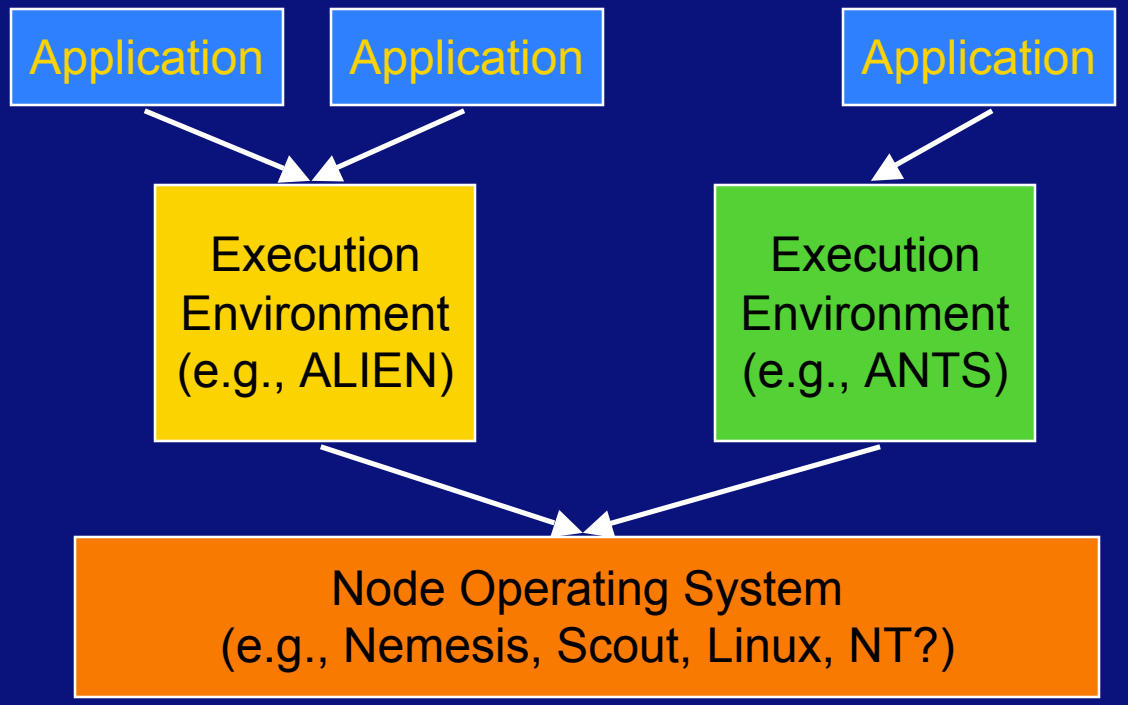
Questions and Discussion

Backup

ARC: Internet Control Plane



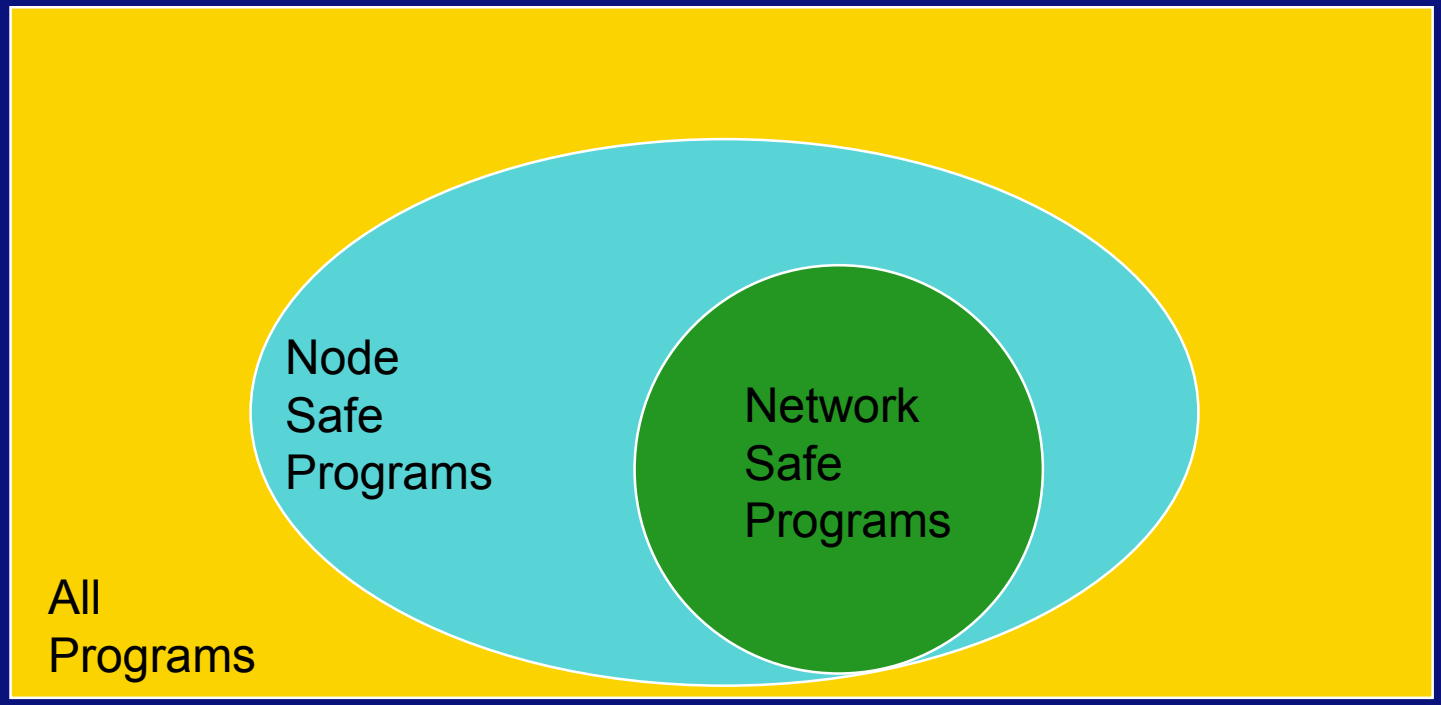
Active Network Architecture



(see April 1999 "IEEE Computer")

Research Issue: Restricting Programs in the Network

- Node safe versus network safe



Netwide Sense Data Selection

- Nets and computers improving exponentially. Humans not.
- Active nodes contain "delegates"
  - →select information (watching a million cameras at once……)
  - →forward towards you for consumption
  - →your senses extended into the network