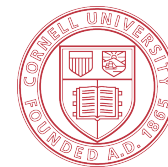
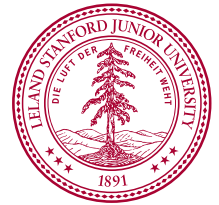


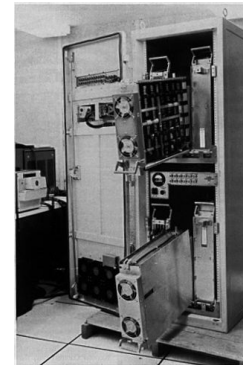
The NEBULA Future Internet Architecture



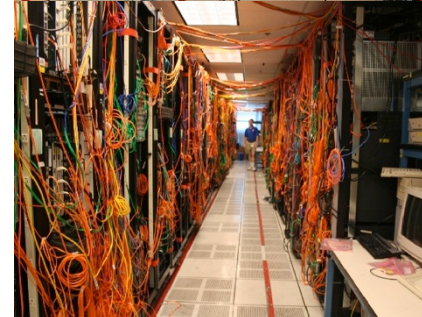
Cornell University

A Comprehensive Architecture

- Technology, Economics and Policy continue to evolve
- NEBULA is an architecture for the cloud-based *future* Internet
 - More secure and reliable
 - Deployable and evolvable
 - Truly clean slate
- Co-design Tech, Econ and Policy!



IMP



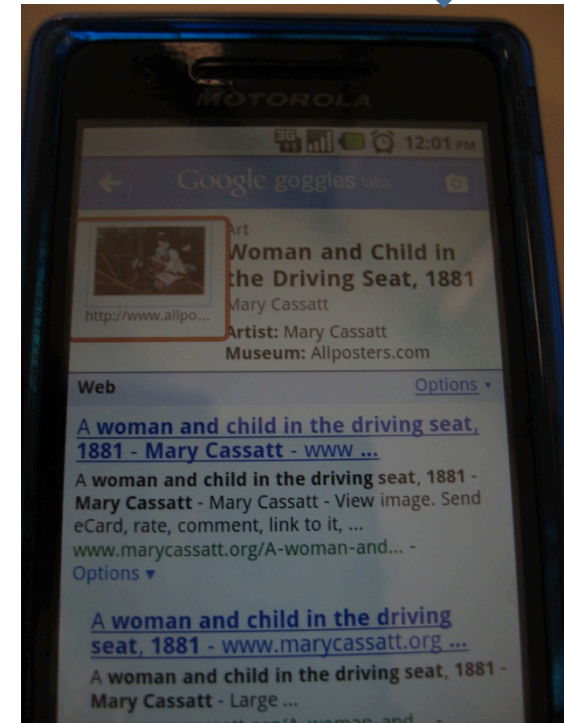
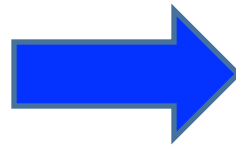
Front and Back, CRS-1

Motivation: Cloud Computing

- A 21st Century computing paradigm
 - Realization of long-desired “computing utility”
- Economic, energy and managerial advantages
- Possibly more secure, possibly less secure
 - Secure Future Internet Architecture is needed
now
- Excellent validation for NEBULA

Prelude: Personal Sensors + Data + Cloud

- The Internet is full of data on recipes, nutrition, caloric burn rates, medical advice, ...
- Cloud-based image matchers, e.g., Google Goggles!



Dietician, Coach, Nurse,... in cloud

- Monitor food intake as eating
 - Photos of food, menu...
- Monitor exercise with device or video (Kinect???)
- Monitor meds and conditions
 - after every checkup, etc.
- Cloud provides a daily report
 - Recommendations
 - Medication reminders
- **Sci-fi? Just *barely*...**

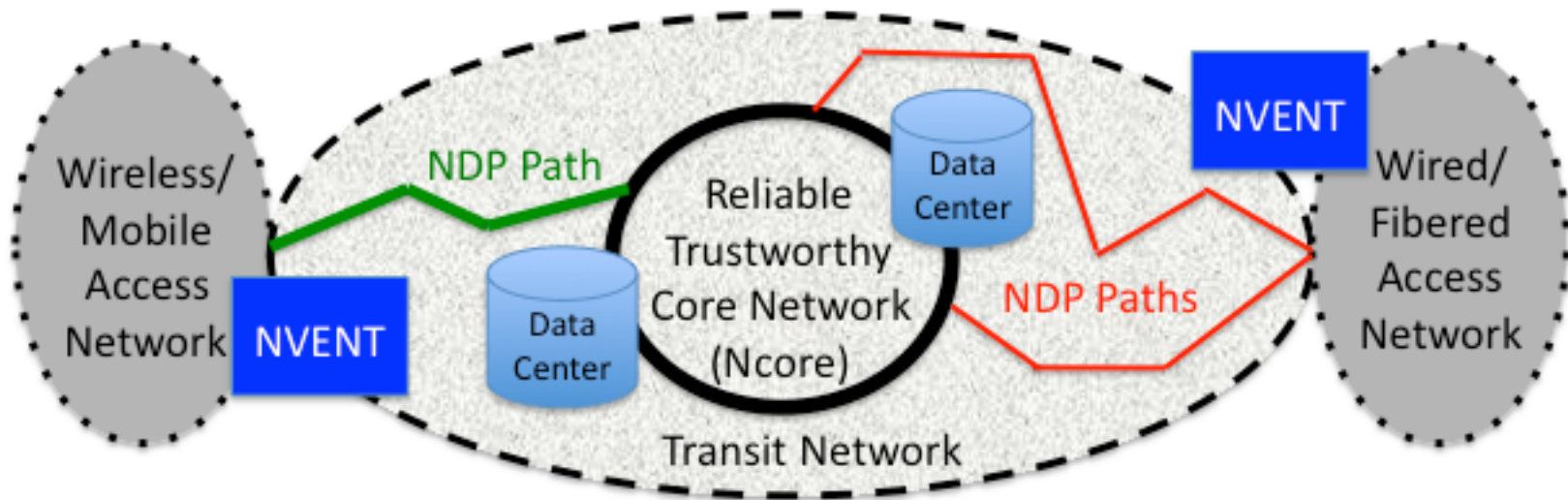


What's missing from this story?

- Health info is confidential; routes?
- Real-time medical; consistent latency and bandwidth, high reliability
- Diagnoses, advice, dosages?
 - Data quality needs: prevent, identify, clean, audit, repair
- Network & system architects need introspection tools
 - Attacks, performance bottlenecks, ...



NEBULA: A Network Architecture to Enable Security



NDP – NEBULA Data Plane – distributed path establishment with guarantees

NVENT - NEBULA Virtual and Extensible Networking Techniques – extensible control plane

NCore – NEBULA Core – redundantly connected high-availability routers

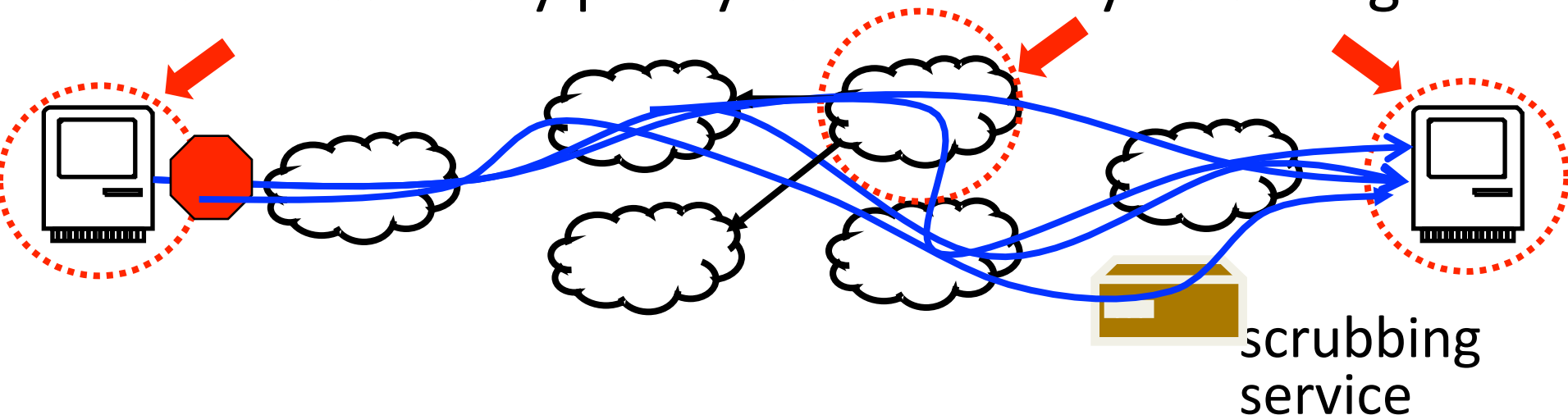
Network-layer security in NEBULA

- The “big I” Internet is *federated*:
 - Policies must be *enforced* across realms (e.g., DDoS)
- NEBULA addresses problems at right places:
 - Extensibility + Policy: new control plane (NVENT)
 - Policy Enforcement: new data plane (NDP)
 - Availability: high-performance, redundant-path core with high-availability core routers (NCORE)

Who should control communications?

What should they control?

- **Many stakeholders:** senders, receivers, transit providers, edge providers, middleboxes, ...
- Each has many policy- and security-related goals

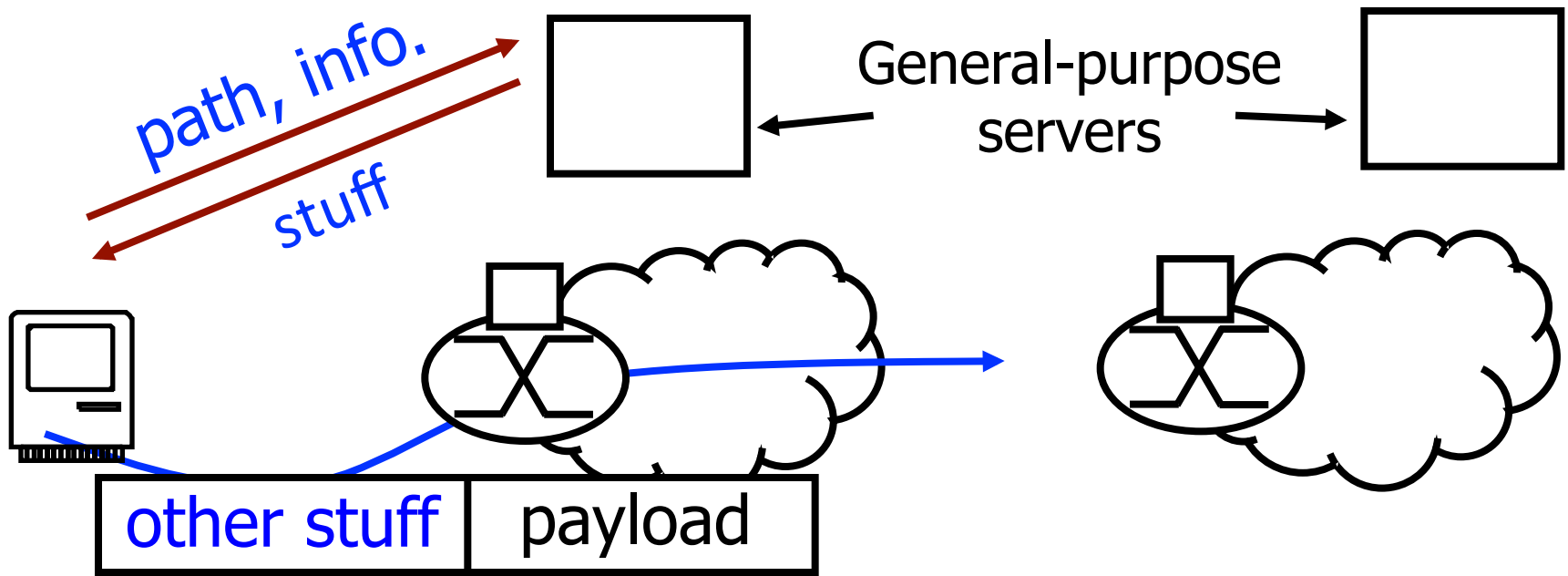


- **Each stakeholder has their own concerns!!!**

What are the technical challenges?

- Letting the control plane specify arbitrary policies
 - Requires new interface between control/data planes
- Enforcing policy decisions in the data plane
 - Requires new packet authentication techniques
- Delegating policy decisions
- Bootstrapping and migration

What should be the control/data plane interface?



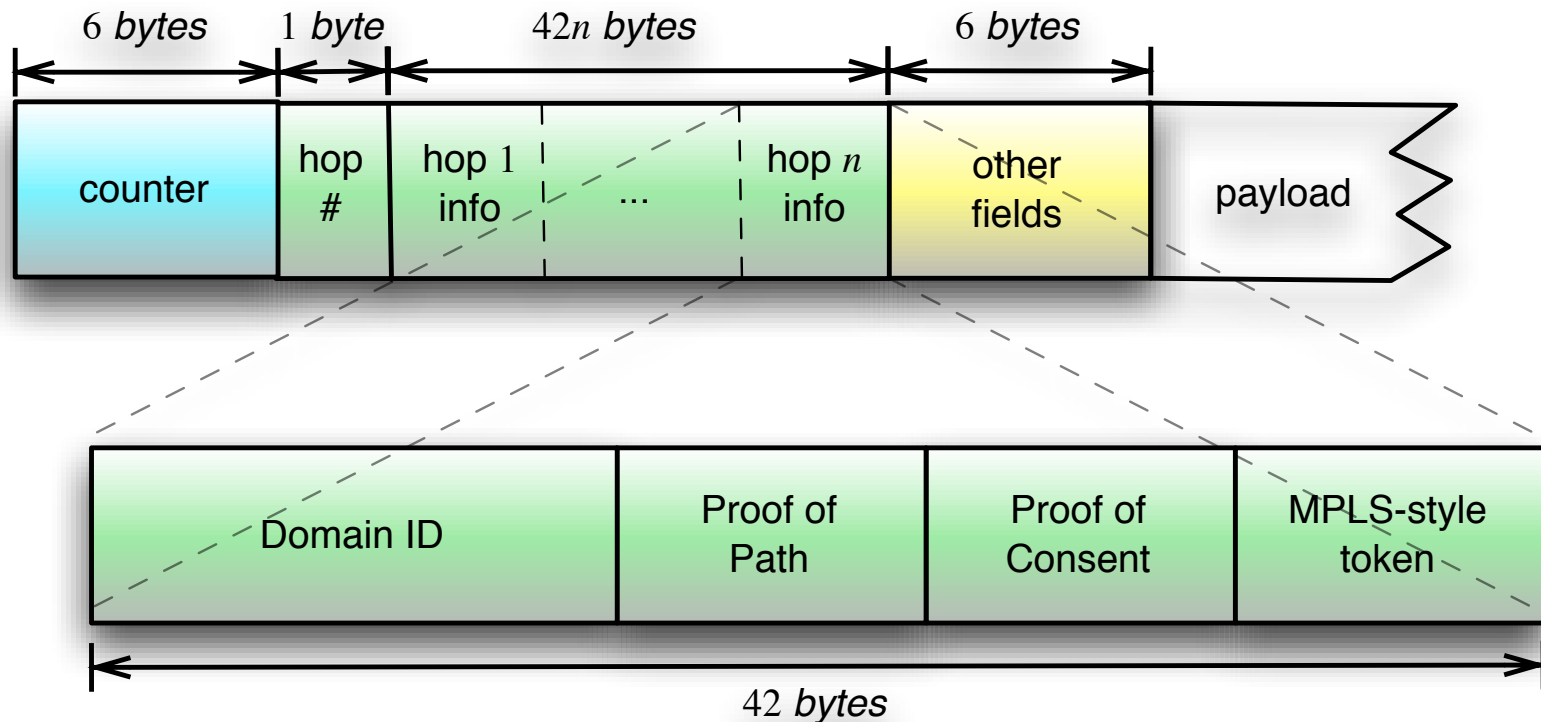
- Policy decisions need to be prior to packet flow
- So move policy from routers to **evolvable** servers
- Servers can delegate or abdicate their control
- **Enables new provider business models** (sell transit to anyone)

Enforcing policy at high speed?


- Data plane must check that path is **authorized**
- Data plane must check that path was **followed**
 - This is a hard technical problem
- Status quo not even close (BGP only advisory)
- Target environment rules out previous techniques
 - **Backbone speeds** preclude digital signatures
 - **Federated nature of Internet** precludes central root of trust, pre-configured shared secrets, etc.

NDP in a nutshell

- Use cryptography for:
 - Proof of consent (PoC) – route *authorized*?
 - Proof of path (PoP) – route *followed*?

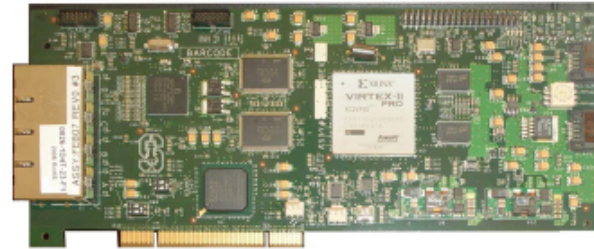


NDP is feasible (from prior work of PIs):

- Space overhead? 

- Average header: ~250 bytes
- Average packet size: ~1300 bytes [CAIDA]
- So, total overhead: ~20% more space

- What is the hardware cost?



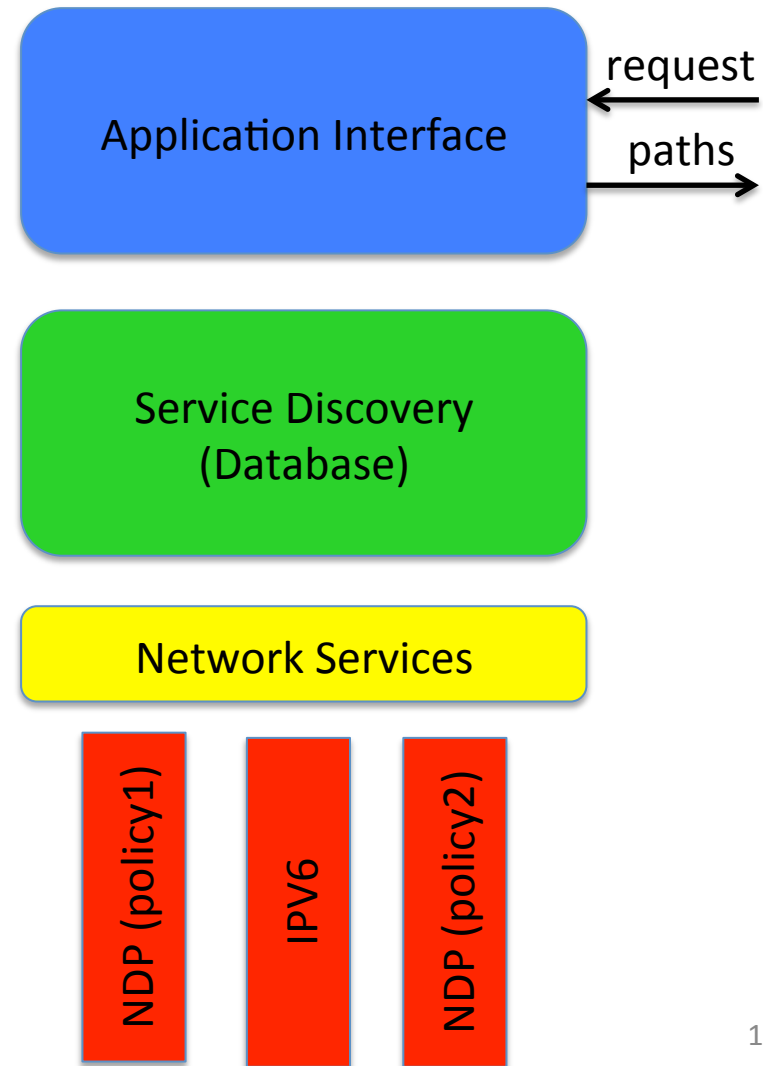
- NetFPGA gate counts: 13.4 M (IP is 8.7 M)
- NetFPGA forwarding speed: ~80% of IP
- Comparison to simple IP in gates/(Gbits/sec): ~2x

NDP Research Questions:

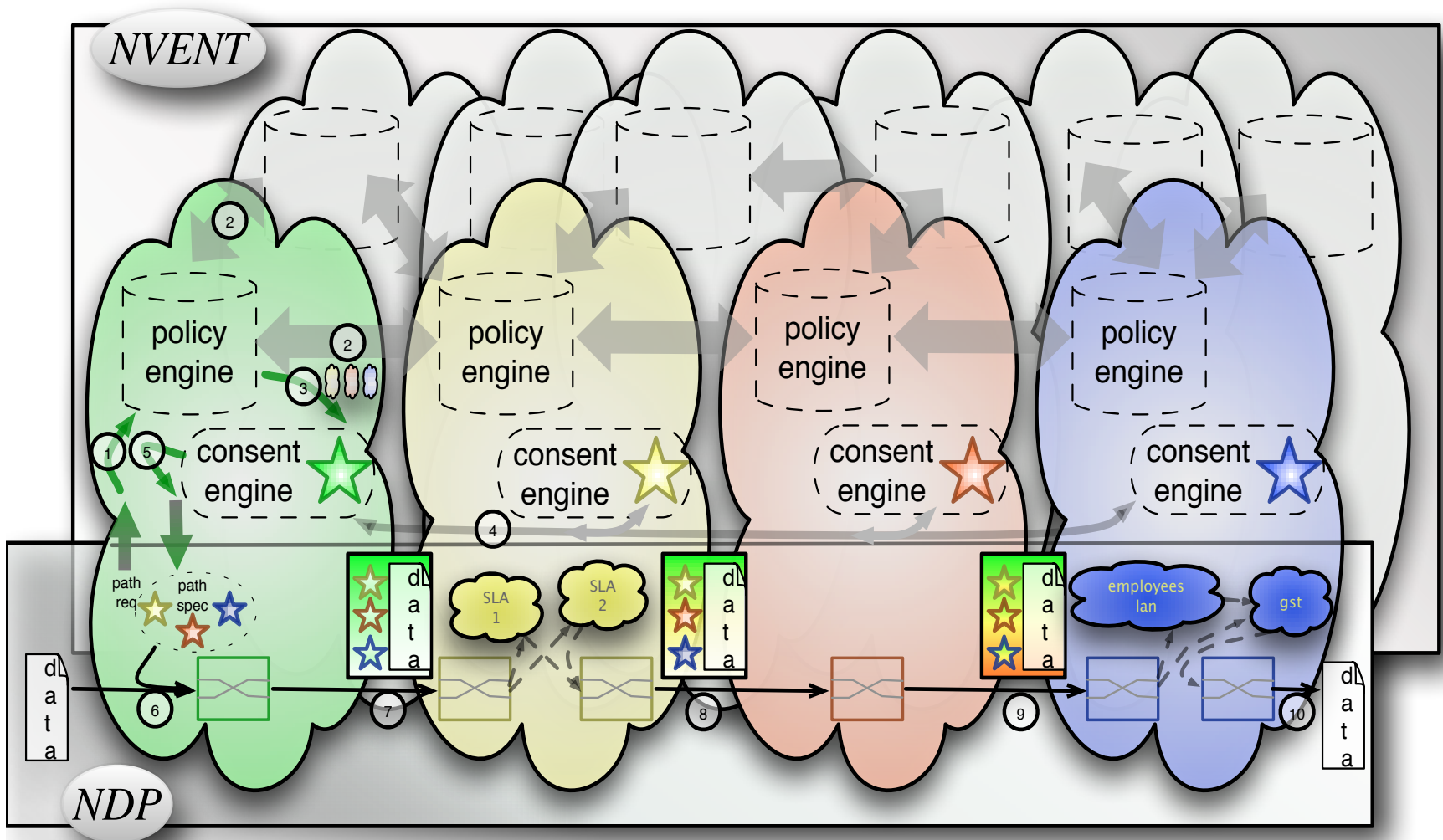
- Must NDP run on all paths?
- Realm management (roughly AS-like?)
- Mapping to intra-domain/inter-domain?
 - Economic implications?
- Public-key infrastructure challenges
- Control of enforcement

NEBULA Virtual and Extensible Network Techniques (NVENT)

- Secure control plane for naming, path exchange, etc.
- Service access
- New service injection
- Generalized path discovery for specifying policies, multiple paths and dynamic path construction via NDP



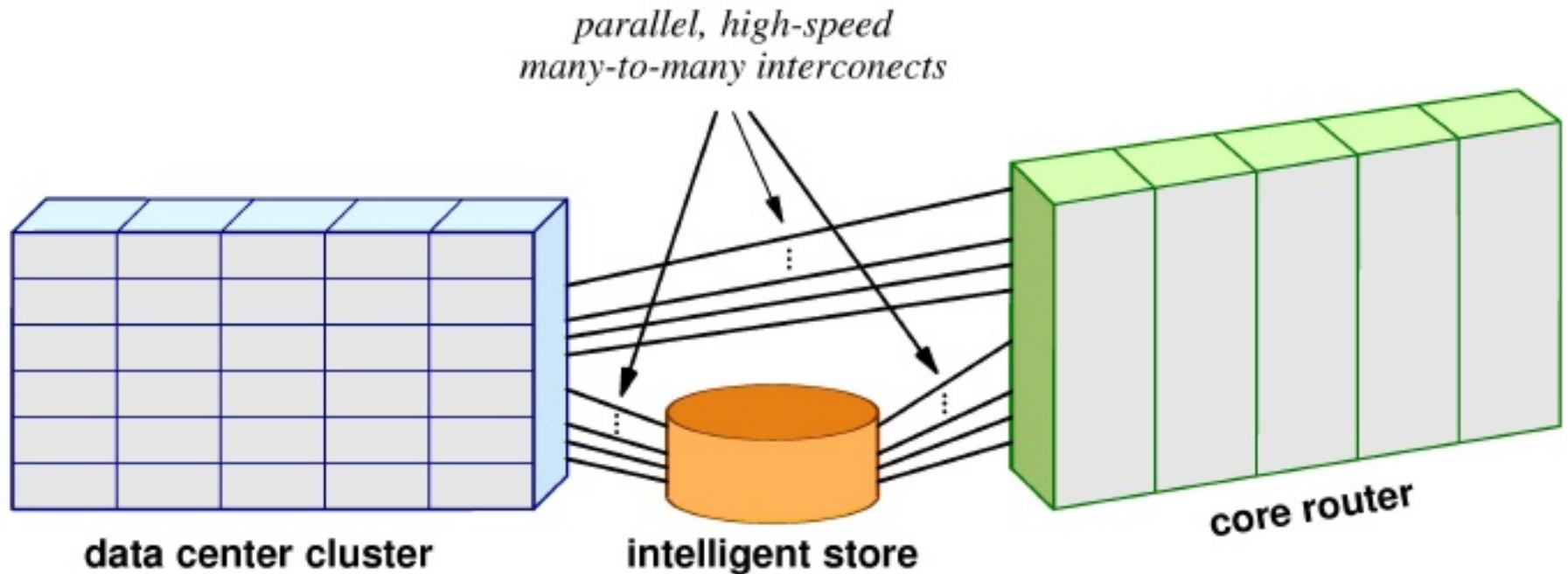
NDP and NVENT roles:



NVENT Research Questions:

- How do NVENT nodes peer?
- What is the right division between roles of NVENT: 1) API, 2) Policy/Consent server, 3) means for introducing and offering new services / slicing up services?
- Policy specification and management?
- (Soft)-state management versus dynamics?
- Changes in dynamics if routers more resilient?

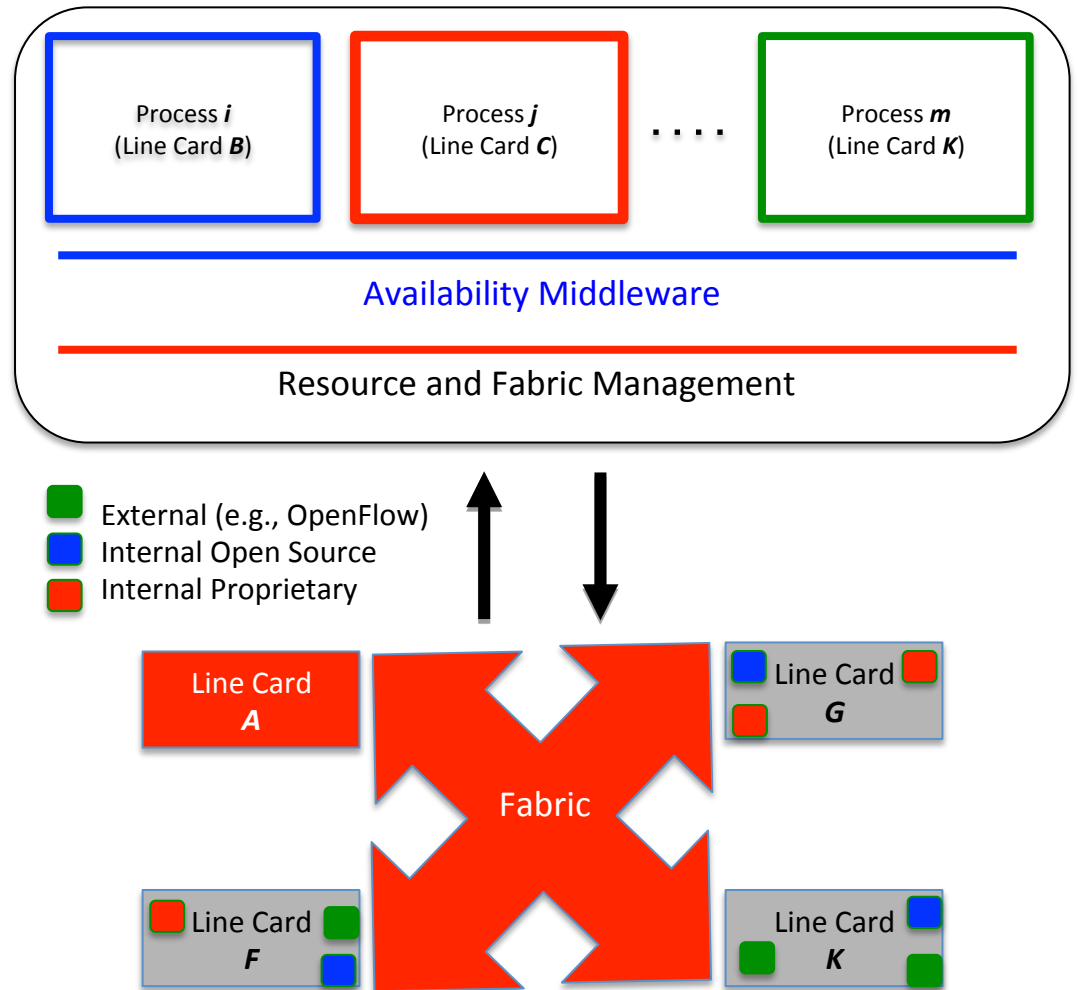
Ncore redundancy: paths



- High availability via redundant high-throughput links
- *A routing complex* from multiple chassis
- Sufficient capacity for easy VM replication/migration

Ncore redundancy: software

- High-availability router control software
- Ideas from distributed systems and cluster computing



Ncore Research Questions:

- What are the scalability barriers?
- What are the technical/economic tradeoffs among redundancy: 1) inside routers, 2) inside data centers and 3) between routers?
- Algorithms and Interfaces for path management
- Interfaces with NDP and NVENT

NEBULA Architectural Choices

Design Goal	NEBULA
Communication must continue despite loss of networks, links, or gateways.	NEBULA uses multiple dynamically allocated paths and reliable transport.
Allow host attachment and operation with a low level of effort	NVENT/NDP is as easy to automate and use as DHCP/IP.
Support secure communication (authentication, authorization, integrity, confidentiality) among trusted nodes.	Mutually suspicious NDP nodes self-select paths exhibiting cryptographic proofs of properties required for security.
Provide a cost-effective communications infrastructure	Ncore places resources where architecturally needed; regulatory/policy analysis.
Implement network and user policies	Policies implemented with NDP and NVENT.
The architecture must accommodate a variety of networks.	NDP sends packets by encapsulation, NVENT networks by virtualization
The architecture must permit distributed management of its resources.	NDP path establishment decentralized, NVENT

NEBULA Research Questions:

- Can we design the overall system for Byzantine Faults?
 - E.g., an entire nation's routers “go bad” ...
- Economic implications for (new?) industry?
 - Customer demand for NEBULA features?
- How does NEBULA interact with regulatory requirements?
- Nebula policies, versus, e.g., Net Neutrality?

The NEBULA Team

Tom Anderson

Ken Birman

Robert Broberg

Matthew Caesar

Douglas Comer

Chase Cotton

Michael Freedman

Andreas Haeberlen

Zack Ives

Arvind Krishnamurthy

William Lehr

Boon Thau Loo

David Mazieres

Antonio Nicolosi

Jonathan Smith

Ion Stoica

Robbert van Renesse

Michael Walfish

Hakim Weatherspoon

Christopher Yoo

