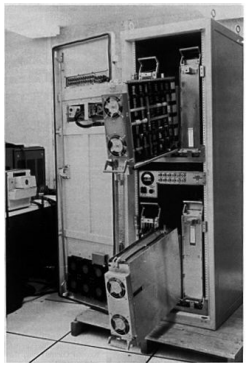
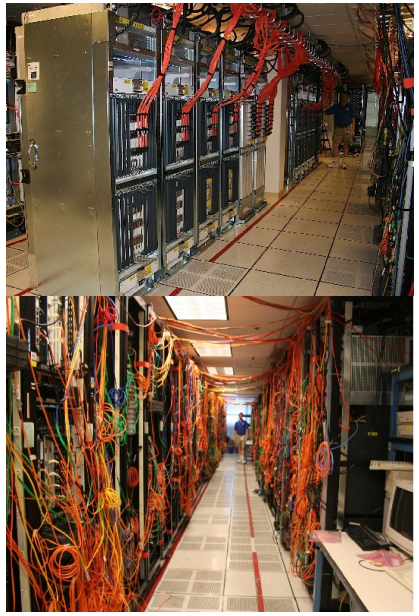
NEBULA: A Future Internet Architecture That Supports Trustworthy Cloud Computing

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
  - Economist and Lawyer on team



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 claims
- Potential broad applicability, e.g., Electronic Health Records (EHR)

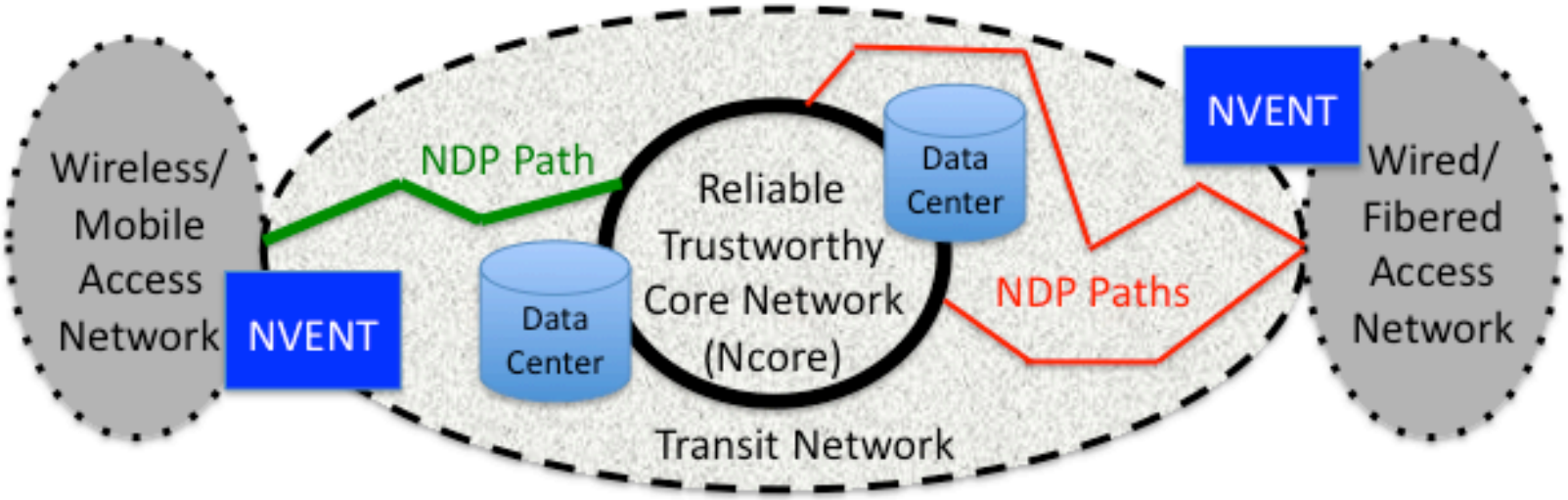
We need a new *architecture*

- Availability: At risk of network outages
- Security:
  - Poor endpoint authentication
  - HIPAA policy restrictions not expressible with existing routing protocols
- Consistency:
  - Communications end-point focused, not data focused
  - Cloud systems have embraced weak consistency (CAP Theorem)

Architecture and Principles

- Architecture:
  - Services provided by cloud data centers
  - Multiple cloud providers, that each use replication
  - Agreements for "roaming" allow user to connect to nearest center
  - Variety of access mechanisms (wired & wireless)
  - Transit networks to connect access to data centers
- Principles
  - Ultra reliable, high-speed core interconnecting data centers
  - Parallel paths between data center and core router
  - Secure access and transit
  - Policy-based path selection
  - Authentication during connection establishment

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

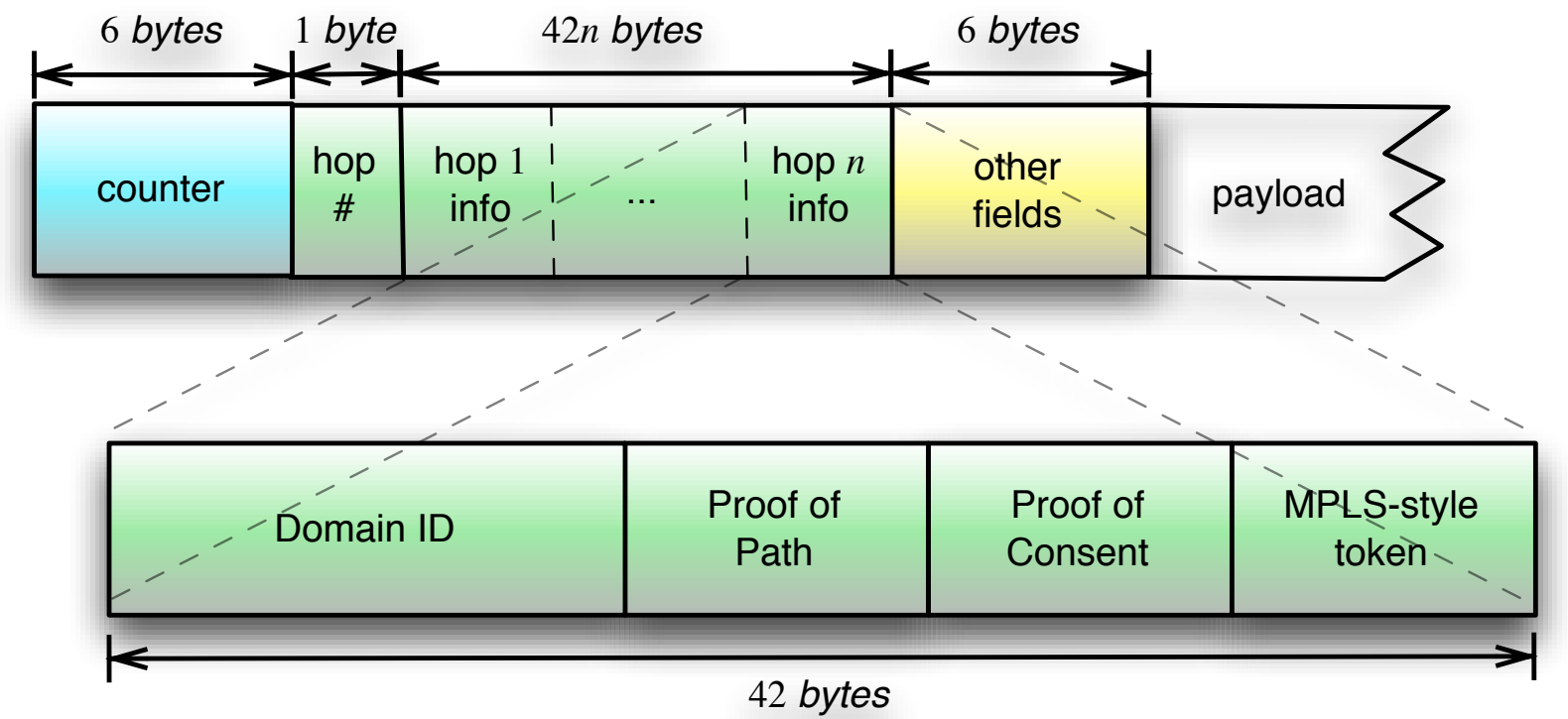
NCore – NEBULA Core – redundantly connected high-availability routers

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
  - Policy Enforcement: new data plane
  - Availability: high-performance, redundant-path core with high-availability core routers

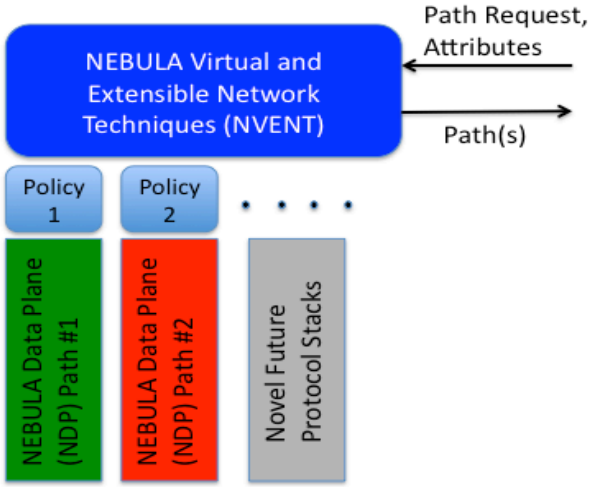
NDP in a nutshell

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



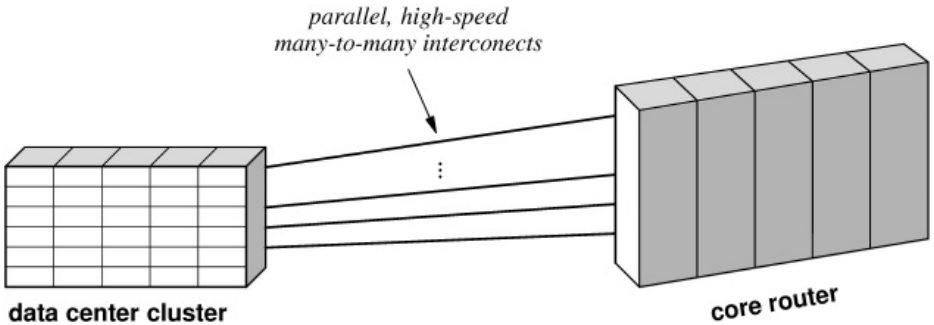
NEBULA Virtual and Extensible Network Techniques (NVENT)

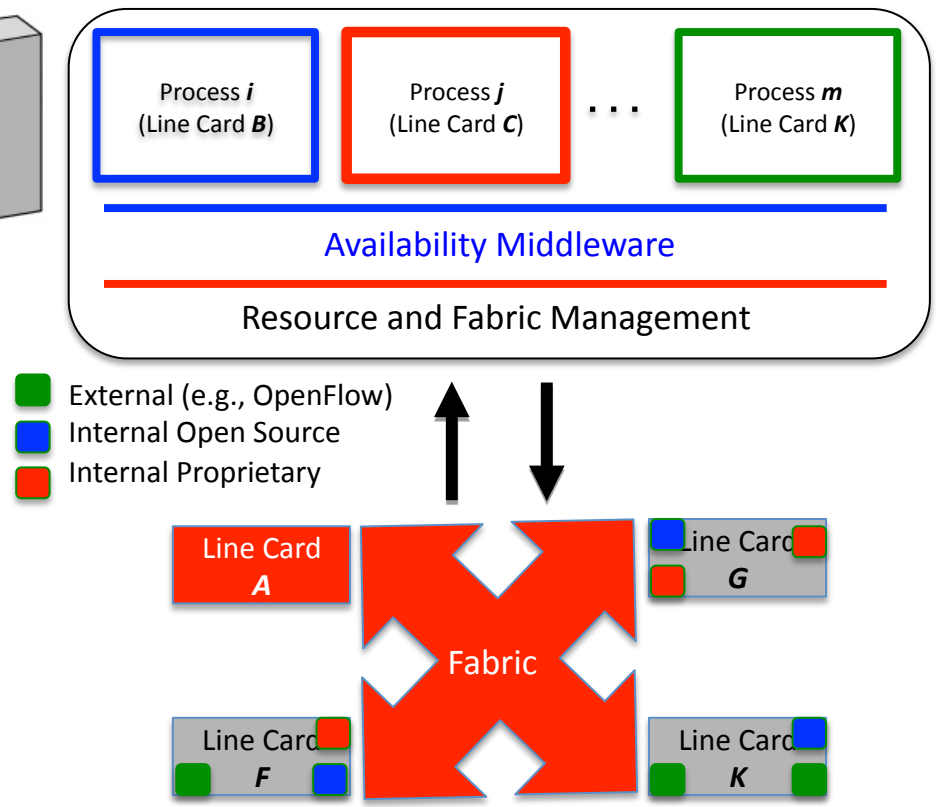
- Service discovery
- New service injection
- Secure control plane for naming, border gateways, etc.
- Generalized path discovery for specifying policies, multiple paths and dynamic path construction via NDP



Extensible: Paths over new substrates
Deployable: Linux implementation of reliable BGP

NEBULA Core (NCore)





- High availability via redundant high-throughput links and novel high-availability router control software
- Reliable distributed software builds a *routing complex* from multiple chassis

Architectural Criteria

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

A Comprehensive *Team*

Researcher	Expertise	NEBULA Focus
Tom Anderson	Distributed Systems, Architecture	NCore
Ken Birman*	Reliable Distributed Systems	All
Matthew Caesar	Reliable Distributed Systems	NCore
Douglas Comer*	Architecture, Protocols	All
Chase Cotton	Reliable Routers	NCore
Michael Freedman	Security, Distributed Systems	NVENT
Andreas Haeberlen	Architecture	NVENT
Zack Ives	Distributed Databases	NVENT
Arvind Krishnamurthy	Distributed Systems	NCore
William Lehr	Economics, Architecture	Economics
Boon Thau Loo	Protocol Verification, Security	NVENT
David Mazieres	Security	NDP
Antonio Nicolosi	Cryptography	NDP
Jonathan Smith*	Architecture, Security	All
Ion Stoica	Architecture	NDP
Robbert van Renesse	Reliable Distributed Systems	NVENT
Michael Walfish	Network Architecture	NDP
Hakim Weatherspoon	Architecture, Reliable Routers	NCore
Christopher Yoo	Regulation	Regulation