Issues of Access Control and Resource Trading for Inter-Domain Provision

A Proposal for Experiments

Admela Jukan
EMT-INRS, U of Quebec

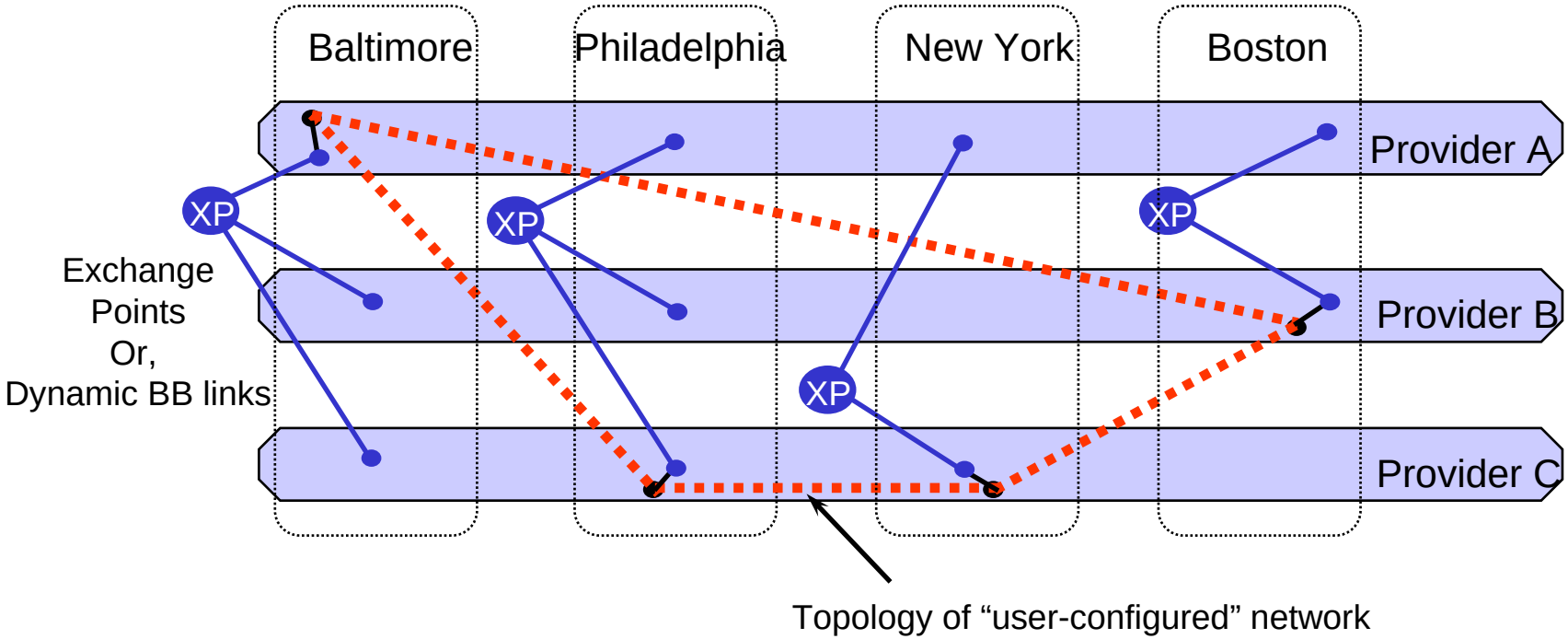
Vassilis Prevelakis
Drexel University

Feb 14, 2007

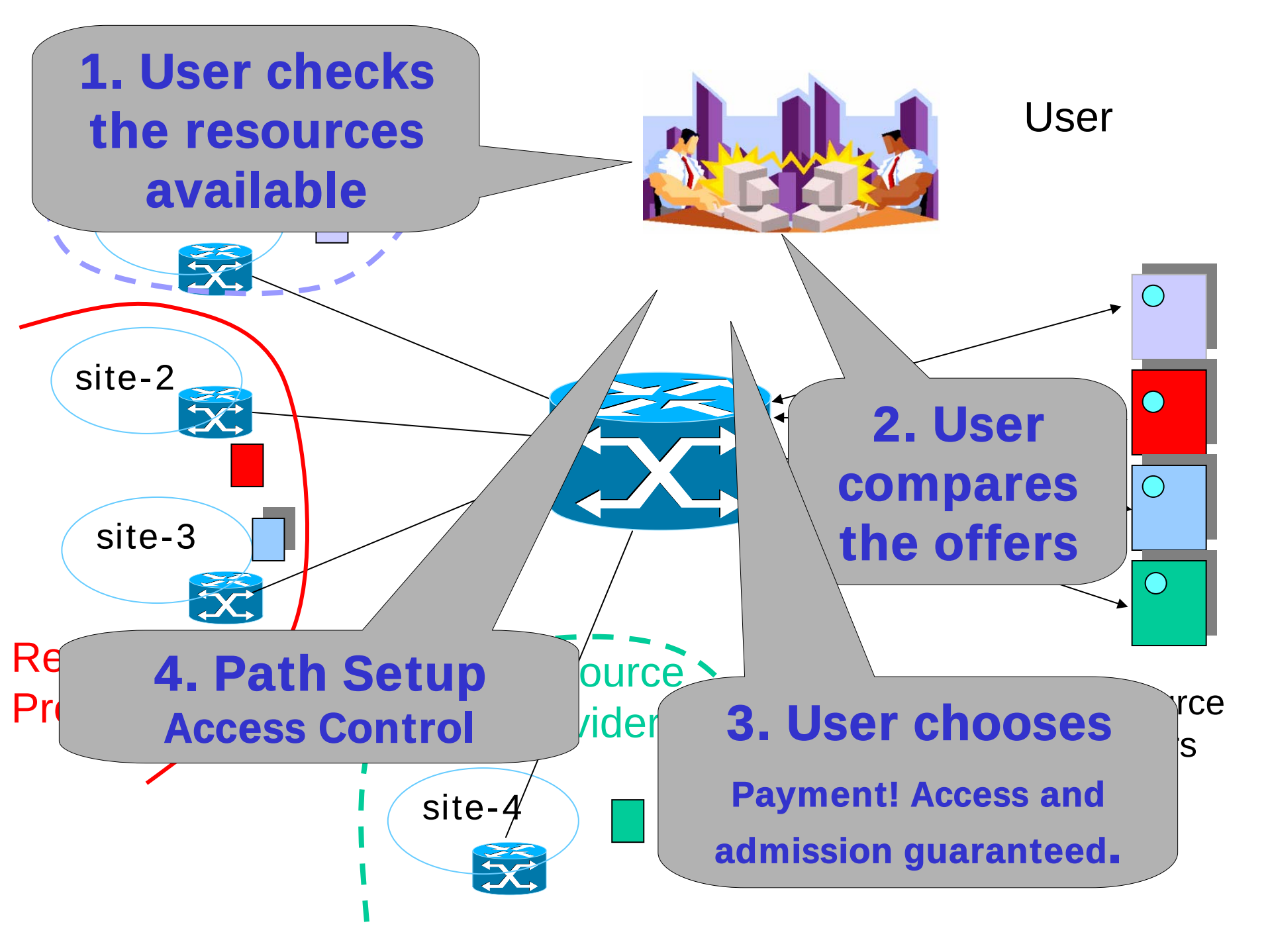
Outline

- Who are we?
  - Collaborators in network security and optical control plane
- Our current interests
  - Access Control (in the Phy Layer)
  - Trading (choice of owners)
  - Inter-Domain Issues (the right scenario to test)
- Experiments
  - GLIF Control Plane?

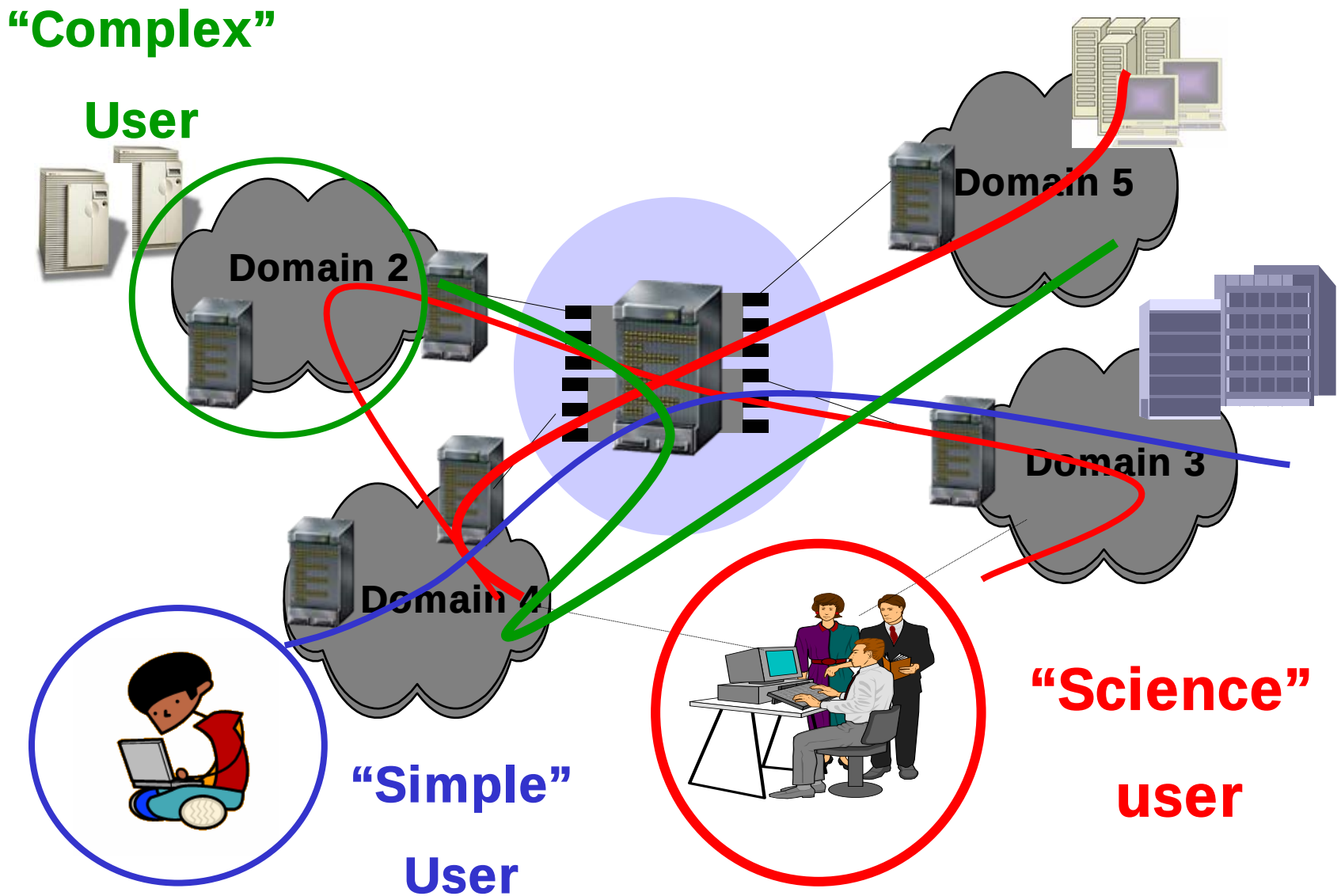
Reference Scenario



- Three providers (domains) & four cities
- Want to provision end-to-end circuits or whole networks (orange dots)


1. User checks the resources available
User
site-2
site-3
site-4
2. User compares the offers
4. Path Setup
Access Control
3. User chooses
Payment! Access and admission guaranteed.

What do we mean by "user"?



Trading

Resource Offers

Dark fiber

site-1

site-2

site-3

site-4

XP

Wavelengths

Dark Fiber

Diff Serv

- Resources becoming a commodity
- XP as a "broker"

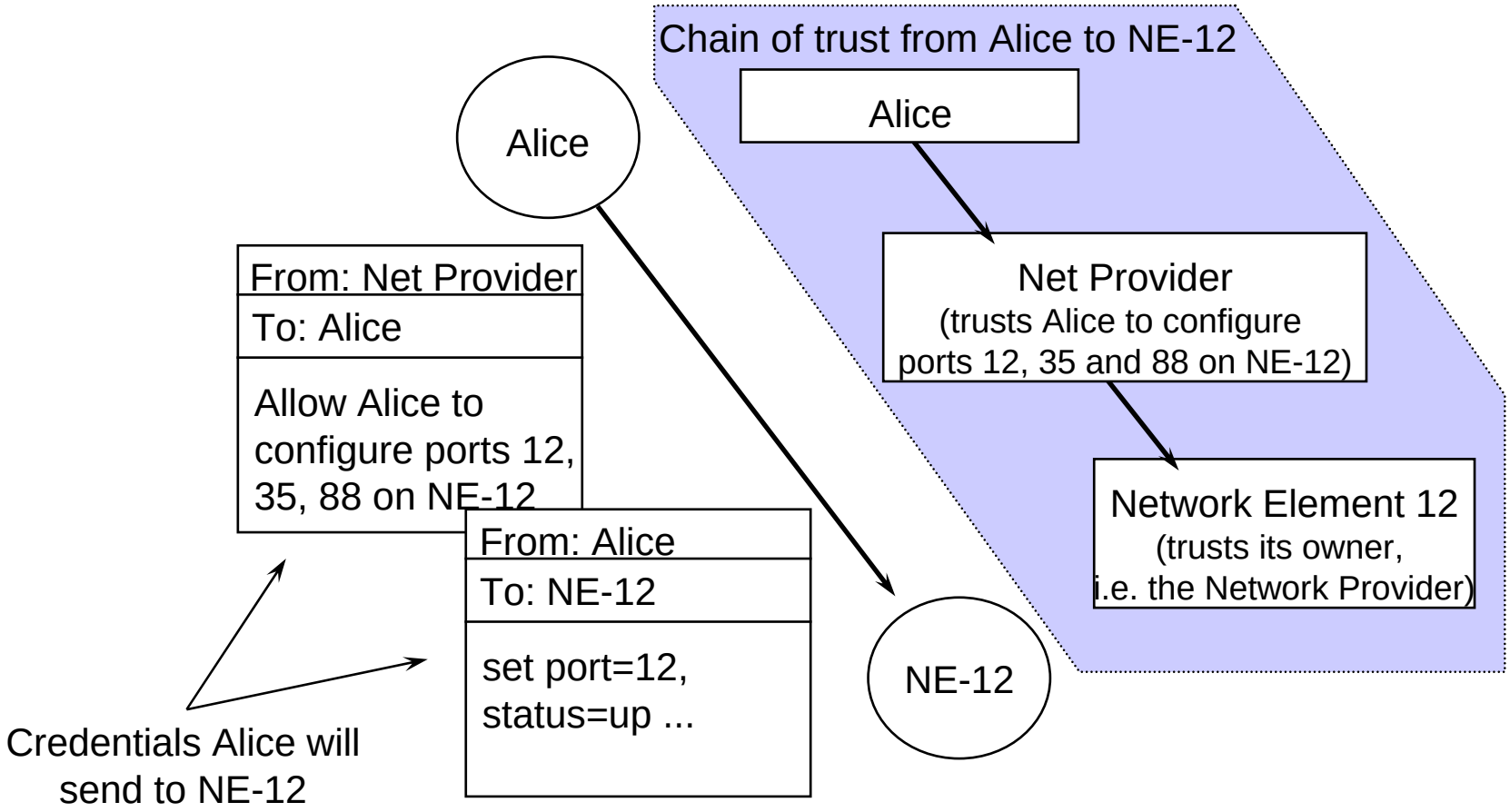
Why brokering?

- Users have one point of contact (broker) instead of contacting multiple providers
- SLAs are easier to compare in presence of multiple contracts
- Unused resources can return the investment, if offered on the free market
- Commoditized resources (i.e., fit for market) make multi-carrier interoperability possible
- Control plane enables fast and short-term resource set-up and reduces ($$) risks of longer contracts

Our Model

- Users submit commands to network elements (NEs)
- NEs verify rights (access control)
- Trust management framework allows subsets of rights to be delegated
- How does trust pass from provider to end-user or another provider?

Trust Model


Chain of trust from Alice to NE-12
Alice
Net Provider
(trusts Alice to configure
ports 12, 35 and 88 on NE-12)
Network Element 12
(trusts its owner,
i.e. the Network Provider)
Alice
From: Net Provider
To: Alice
Allow Alice to
configure ports 12,
35, 88 on NE-12
From: Alice
To: NE-12
set port=12,
status=up ...
NE-12
Credentials Alice will
send to NE-12

Big Picture

- Security framework has been demonstrated to work in:
  - reservations for IP-based networks (Bandex-X ISCC'05)
  - distributed file-access (DISCFS USENIX'04, PWC'03, WETICE'03, Fileteller FinCrypto'03)
  - access control at the library-call level (SecMod, SSN'06)
- Putting everything together we get a framework that supports resource reservations for Grid-class applications over optical network.

Discussion (1)

- Flexibility
  - users can create non-standard configurations to cope with incidents
  - users have better control of the resources they lease
  - provider's internal network becomes visible to users (not always desirable)
- Scalability
  - distributed access control (access rights are evaluated at point of enforcement)
  - each request carries with it all credentials need for access control
  - no access lists or user databases (state may be cached)

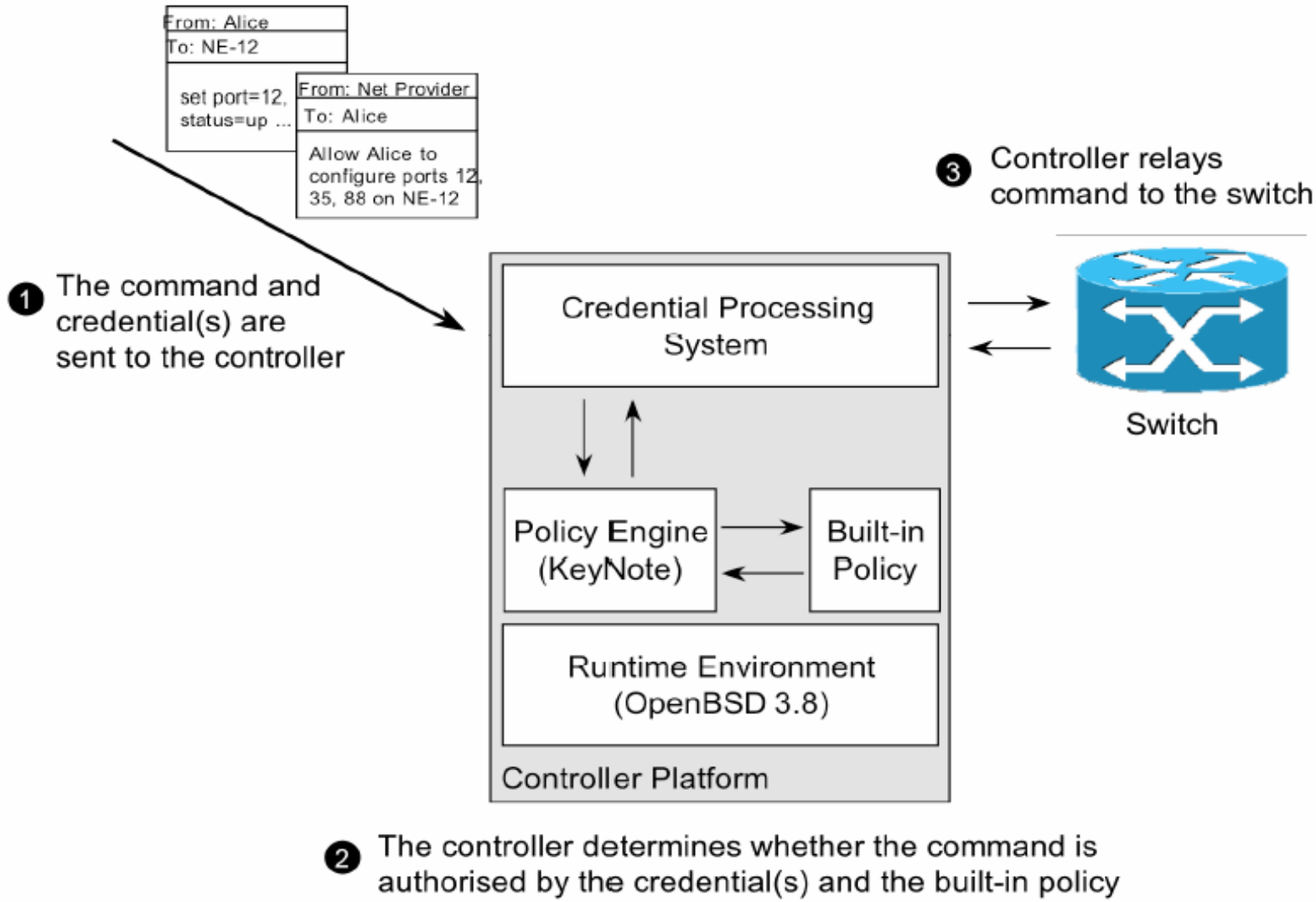
Discussion (2)

- Talked about access control, but how do we handle admission?
  - "offer database" allows resource trading
  - possession of offer implies admission
- Overlaying VPNs is a way to support virtual providers ("resource traders"), but
  - in layer 3, overlaying VPNs creates multiple layers of encapsulation.
  - in layer 2, overlaying VPNs creates multiple layers in the control plane.
- **By switching to the credential-based access control strategy, we eliminate the layers and replace them with credential chains.**

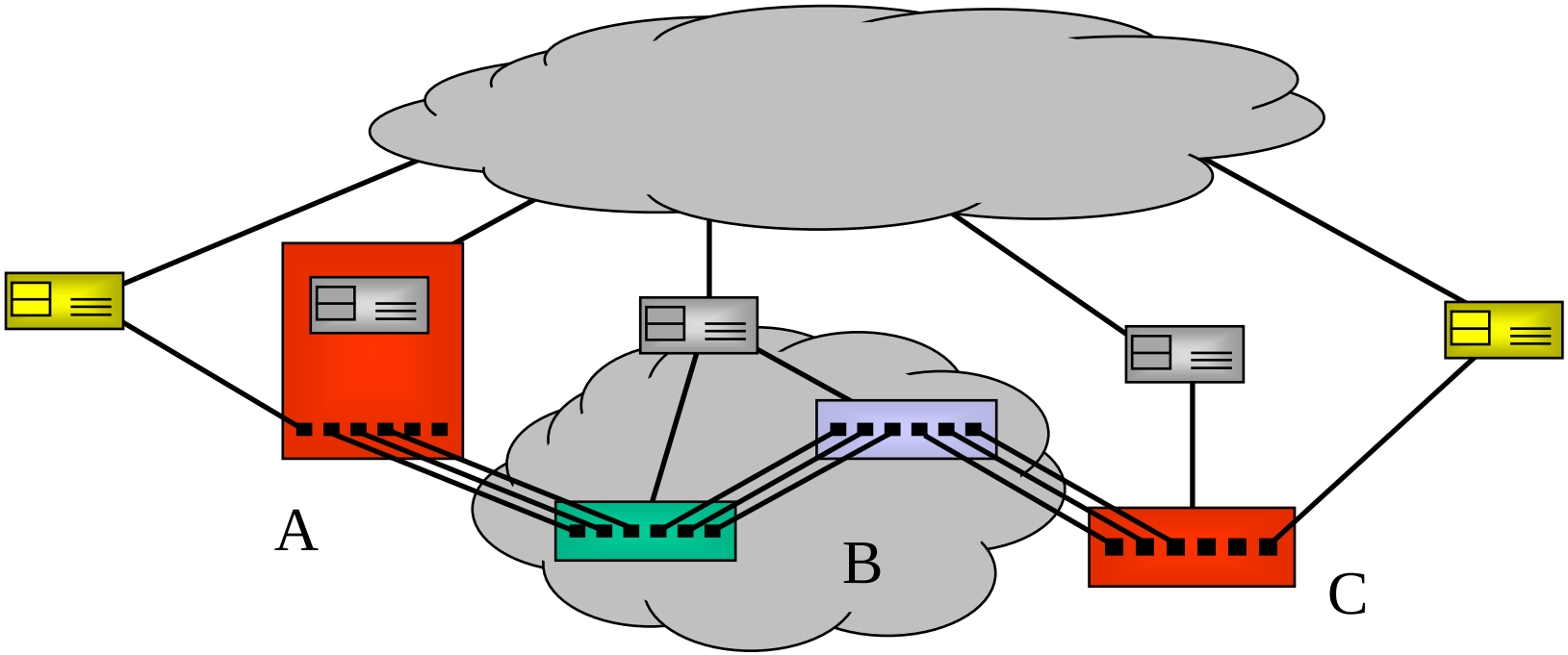
Implementation

- Addresses need to deploy framework in existing networks
  - two projects
    - experimentation within GMPLS or UCLPv2
    - "reference-implementation" using "buddy host"
      - Single board computer located next to NE
      - Requests must go though the SBC
      - Policy is evaluated at the SBC and relayed to NE via console interface, or SNMP
      - based on earlier work in secure monitoring and control of network elements (Usenix 1999)

Policy Enforcement Node

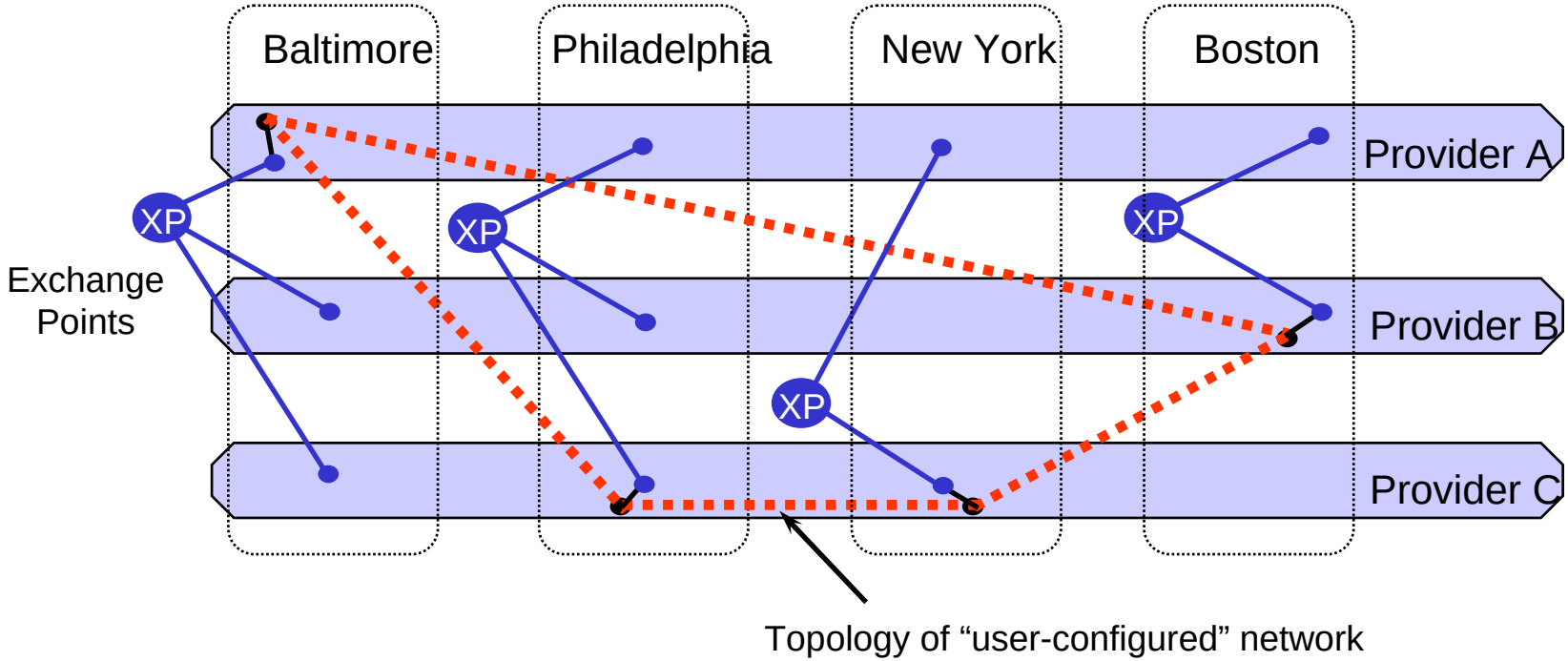


Three ways to implement Policy Nodes



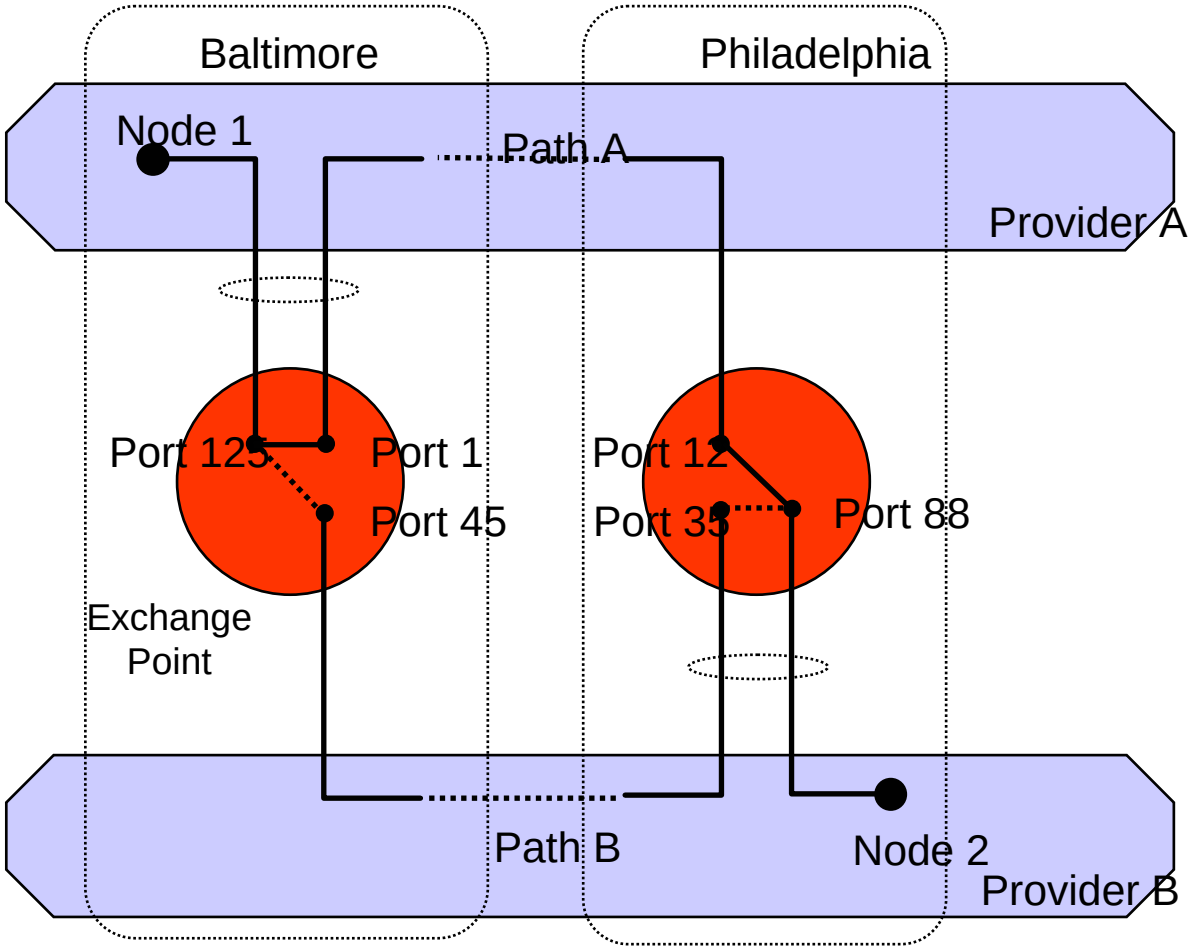
(A) NE contains the policy engine,
(B) External Switch Control Unit controls multiple switches, thus allowing "bundled" services to be offered.
(C) External Switch Control Unit controls single switch

Going back where we started,…



- Three providers (domains) & four cities
- Want to provision end-to-end circuits or whole networks (orange dots)

Controlled Access to NEs



- Consider earlier example
- User wants to configure interconnects to use backup link (Path B)

Final Remarks

- Configurable Exchange Points and Resource Brokers
  - Holy Grail of Inter-Domain Provisioning
  - Playgrounds for Access Control Experimentations
- Looking for large-scale experiments environment
  - To test policies and interactions between end-users and intermediaries
  - To integrate with control plane and network elements
- Test failure recovery scenario
  - If a failure happens on a "sold" resource how to recover? (research)

Thank you

vp@drexel.edu

jukan@emt.inrs.ca

Controlled Access to NEs (2)

- not a new concept, been using this in general-purpose computing environments for years
- e.g., Virtual Machines
  - create VM for user with access only to leased resources
  - run vendor's OS (e.g. Cisco's IOS) in a VM
  - users cannot "see" (and hence control) rest of hardware
  - but ...
    - management problems (VMs, guest OSs, etc.)
    - performance issues
    - not all resources fit this framework (e.g. CPU allocation can only be managed by the provider)

Reference Scenario 2

- Leasing resources to create user-controlled network (a.k.a. UCLP)
  - existing way
    - providers lease links ensuring QoS, fault recovery, etc.
    - "taxi cab" type of service
  - proposed way
    - controlled access to the network elements allows user to manage leased assets directly
    - "rental car" type of service