NewArch: A new architecture for an Internet

David D. Clark, Steve Bellovin,
Bob Braden, Noel Chiappa,
Ted Faber, Aaron Falk
Mark Handley, Scott Shenker,
Karen Sollins, John Wroclawski

What has changed?

- The Internet as an economic reality.
  - ISPs have to make money. Facilities are important.
- The erosion of trust.
  - Universal transparency is scary.
- The rise of third-party involvement.
  - A tussle of interests.
- A broader class of users.
  - DIY is not empowerment.
- New application requirements.
  - Quality of service, placement in the network, delegation.
- New technology features.
  - Mobility, embedded processing, location aware computing, etc.
- We did not fully understand any of these.

High level-examples

- Facilitate, and not impede, the deployment of new applications.
  - Old: End to end, transparent carriage. New:??
- Design so that failures in the network impair the end point activities no more than necessary.
  - Old: No state in net that end points depend on. New?
- Bursty traffic and aggregation are fundamental.
- Recognize that people and societal issues are a part of the Internet.
  - Technology shapes the balance of power.
  - Support the tussle.

° Thinking about “architecture”

- A future Internet architecture must:
  - Better preserve itself.
  - Be (more) tolerant of evolving requirements.
- Can we invent better design principles for architecture?

Some fundamentals

- Loss of trust--a basic change.
- The Internet as an economic entity.
- Dealing with increasing heterogeneity
- Routing--still fundamental after all those years.
- Resource management.

Trust--fundamentals

- Trust (among people) is assuming that another will act in our best interest even though not externally constrained.
  - The power and the risk is the lack of constraint.
  - Constraint is the opposite of trust.
- The Internet implies human trust.
- We no longer trust most of the people we meet on the Internet.

Trust-architecture

- Users want selective transparency, regulated by trust relationship.
  - A framework for identity is central.
  - Identity theft is destructive.
  - Need mechanisms for control of transparency.
    - Firewalls of the future--delegate trust.
    - Who, not just what.
    - Some support is “in” the network.
  - Enforce trust locally.
- Trust and constraint are dual approaches.
- Think “middle players”, not “middle boxes”.

Economics--fundamentals

- Internet service is provided by a set of players, some of which have economic motivations.
  - A number of entities with self interest.
  - E.g. ISPs want to make money.
- ISPs sit in the middle.
  - Transparency commoditizes them.
- How can we constrain the resulting tussle?
  - Architectural purity? Nope…
  - Architect to exploit self-interest.

Economics--architecture

- Payment for services is a necessary part of a competitive market.
  - Does not imply “simple” per-byte billing.
  - No single scheme, not just two-party.
- Competition is a tool to shape commercial practice, and encourage change.
  - Other tools include law and societal pressure.
  - We can design a marketplace, “they” cannot.
- Competition will only discipline the provider based on actual user preference.
  - Beware the “AOL trap”.

Economics-route selection

- Route selection defines an important competitive marketplace.
- Old: Users picks his access ISP. That ISP picks next ISP, and so on.
- Better: User can pick a path of providers.
  - Why? Insufficient competition in access.
  - Example: Force deployment of QoS.
  - Implication: pay for what you use.
- General principle: global change through local action.

Heterogeneity

- Technology heterogeneity.
  - Lossy wireless vs. fiber vs. ???
  - Both very fast and very slow.
- Traffic heterogeneity.
  - Single flows and aggregates are different.
    - “Duration” heterogeneity.
- Operational heterogeneity.
  - Among friends vs. hostile vs. costly.
    - Continuous, not point solutions.

Next Generation Application Architecture (NGAA)

- Transparency is not enough.
- Explicit talk about division of responsibility.
  - Naming, finding peers.
  - Identity framework.
  - Abstraction of network performance.
  - Application-level routing.
    - Application-defined transparency/conversion.
    - Controlled delegation.
      - Who do you trust?
      - Role of the third parties.

Architecture: Data carriage

- We must define transparency carefully.
  - Syntactic vs. semantic transparency.
  - Who controls conversion: net or application.
- User must be able to control transparency.
  - Data must be associated with identity.
  - Implies constraints on routing.
- User must be able to control routing at ISP level.
  - Data must carry info to support payment.
  - ISP must be able to validate service request.
    - Traffic policing.
  - Routing will also occur at application level.
- A clean separation between forwarding and other functions.
  - Balance what ISP, others can see.

Implications for data carriage

- Network must deal with a wider range of issues than in current Internet.
  - Trust, user-specified routes, accounting, etc.
- Require a new model for amortizing complexity/overhead/cost.
  - Not always pure datagrams.
  - Not mandatory connections.
  - Self-detection (caching, adaptive algs, etc.)?
  - Application guidance?

Balance of power

- User empowerment in the new world.
- Vs.: The employer as an ISP.
- Vs.: Governments and other third parties.
- Designing the trade-off.
  - What is visible to whom?
    - Hiding contents weakens power of third parties.
  - Who controls routing?
  - Who can attach a connection to a “region”?

Our list of design rules

- What should an architecture do?
  - Don’t design for rigid outcome, but to allow a tussle.
  - Design marketplaces to shape technology.
  - Design for competition, to discipline the market and drive change.
  - Mechanisms will come in pairs--trust and constraint.

Current projects

- Data transport abstraction.
- Location and rendezvous architecture.
- Role based architecture.
- Map/abstraction routing.
- Network projection of trust models.
- Economics framework (routing money?)