Trends in the evolution of the Internet Architecture

Bengt Ahlgren
SICS
Overview

- Background
- 1. Naming and addressing
- 2. The network as an entity
- 3. Overlays moving into the network
- 4. Controlled transparency
- 5. New link abstraction
- Summary
Background

- Internet huge success after 20 years of development
  - Was not designed for today's requirements
- The IETF is coming to the roads end with patches and ad-on mechanisms
  - Many of which are violating the original architecture
- No body has the task of evolving the Internet architecture in a consistent manner
  - Task for research community!
- Evolving is hard – perhaps think about replacement?
  - C.f. David Clark's effort to create funding program
  - Design replacement first – then look into migration?
- What should a replacement look like?
1. Naming and addressing

- *Naming* and *addressing* central to any network architecture

Main problem in the Internet:

⇒ IP addresses are used both for **node identity** and defining its **location**

⇒ Mobile IP is a hack that does not solve this fundamental problem

- Instead, **separation is needed!**

This is hard – many issues creep up, e.g.:

⇒ Can we afford to introduce a **new global namespace**?

⇒ Does the separation affect global routing?

⇒ We should at the same time create a solution to the IPv6 migration problem!
1. Naming and addressing

- HIP – *Host Identity Protocol* – is one such proposal
- Focus on *security*:
  - Uses *cryptographic host identifiers* based on public key cryptography
  - Node identities can be verified for each packet
- Transport layers see a representation of the host identity instead of IP address
  - Node can change IP address without breaking TCP connections
- Could also be made to bridge IPv4 and IPv6
- Hard issues remain on how to handle in DNS
2. The network as an entity

- Networking (Internet style) has a focus on the individual nodes – "you can't see the forest for all trees"

- I claim that there is a missing piece: The notion of a collection of nodes acting as ONE entity
  - Personal area networks, home networks, an operators network
  - Each under different administrative control
  - An individual node does not matter – it is the functions and services of the collection of nodes that matter

- Would be very useful in many scenarios:
  - Provides a basis for building trust and security
  - Provides a focus on the services, not the nodes
  - Provides a means for on-the-fly subscriptions and other flexible business models
2. The network as an entity

- Example from the EU Ambient Networks project
- The network entity is manifested by a common control space
- The control space has uniform interfaces:
  - Inter-network interface for negotiation of connectivity and services between networks
  - Service interfaces for using connectivity and providing service to applications
3. Overlays moving into the network

- Overlays has almost become a synonym with peer-to-peer
  - But overlays are more than that, including simple VPN tunnels and advanced distributed systems

- Important tool to *provide new services*
  - Opportunity for network operators to create added value for its customers

- Important tool to *experiment with new technology*
  - Opportunity for both researchers and industry to do what they want, not worrying about the operation of the rest of the network

- Overlay technology could be the migration tool needed to move to a new Internet architecture
4. Controlled transparency

- The Internet was designed to be **transparent**
  - A packet sent comes out *unaltered* at the other end
  - The network does not care about packet content
- **Benefit:** anyone can start new application services
  - Main factor behind Internet's success – *maximises innovation*
- **Drawback:** anyone can *abuse* the network
  - Spam, denial-of-service, ...
- Transparency *does not hold* today
  - Firewalls, address translation, routing and filtering based on application info (packet content), ...
- Not generally visible to the application/user
  - Hard to debug connectivity problems for an application
4. Controlled transparency

**Challenge:** Keep the network *open to new applications and services*, but at the same time *prevent abuse*

- Need the concept of **controlled transparency**
  - An application/user visible description of the offered service
  - Tightly coupled with trust relationship
  - But need to keep innovation power of transparency
5. New link abstraction

- Theory behind networking technology is *graph theory*
- *Fundamental assumption:*
  - A link either exists or does not exist
- Everything from routing protocols to applications are based on this all-or-nothing link abstraction
- OK abstraction for wired networks
  - but really just rubbish for wireless media
  - especially when you push the limits and invent new fancy antenna and radio things
  - radio is fundamentally not point-to-point
- *We need a new abstraction of “a link” which enable the network level to better handle and take advantage of wireless media*
Summary

- IETF at roads end with patches to current Internet architecture
- Need to work on complete replacement
  ⇒ Then think about migration
- Challenges for a replacement:
  ⇒ 1. Naming and addressing
  ⇒ 2. The network as an entity
  ⇒ 3. Overlays moving into the network
  ⇒ 4. Controlled transparency
  ⇒ 5. New link abstraction