Enhanced MILSA Architecture for Naming, Addressing, Routing and Security Issues in the Next Generation Internet

Jianli Pan, Subharthi Paul, **Raj Jain**
Washington University in Saint Louis
jain@cse.wustl.edu

Mic Bowman, Intel Corporation
Xiaohu Xu, Huawei Technologies
Shanzhi Chen, BUPT, China

Presentation at ICC 2009, June 16, 2009, Dresden, Germany

These slides and Audio/Video recordings of this talk are at:
http://www.cse.wustl.edu/~jain/papers/emilsa.htm

Outline

MILSA=Mobility and Multi-homing Supporting Identifier-Locator Split Architecture

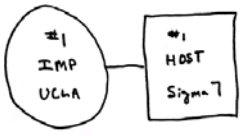
1. Internet 3.0 and our project
2. Problems with the current Internet
3. Our proposed solution: MILSA
4. Enhancements to MILSA

Internet 3.0: Next Generation Internet

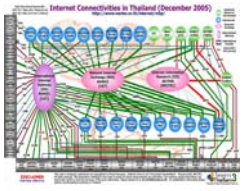
- Internet 3.0 is the name of the Washington University project on the Future Internet (inspired by NSF's FIND and GENI)
- Project supported by Intel and Huawei
- Named along the lines of "Web 2.0"
- Goal 1: Develop a *clean slate architecture* to overcome limitations of the current Internet
- Goal 2: Develop an *incremental approach* to implement the architecture

Internet Generations

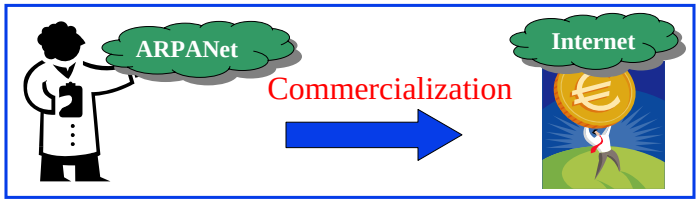
- **Internet 1.0** (1969 – 1989) – Research project
  - RFC1 is dated April 1969.
  - ARPA project started a few years earlier
  - IP, TCP, UDP
  - Mostly researchers
  - Industry was busy with proprietary protocols: SNA, DECnet, AppleTalk, XNS



- **Internet 2.0** (1989 – Present) – Commerce ⇒ new requirements
  - Security RFC1108 in 1989
  - NSFnet became commercial
  - Inter-domain routing: OSPF, BGP,
  - IP Multicasting
  - Address Shortage IPv6
  - Congestion Control, Quality of Service,…



Problems of Current Internet

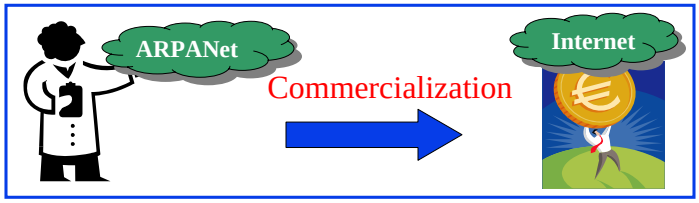


Security

1. Trusted ⇒ Un-trusted
2. Control, management, and data path intermixed
3. Perimeter based.
4. Difficult to represent organizational, administrative hierarchies and relationships.

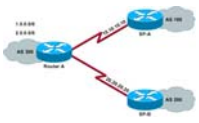
Trusted
Un-trusted

Problems of Current Internet



Security

Mobility

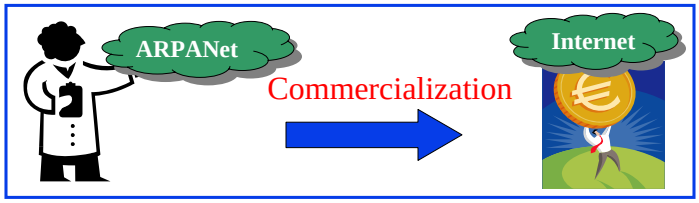


Multi-homing

Two type addresses
PI: Provider Independent
PA: Provider Aggregatable

1. Multi-homing is PI based
2. Easy for end-site, but put high burden to the routing system

Problems of Current Internet



Security

Mobility

Multi-homing

Scalability
Traffic Engg
Renumbering

See our Milcom 2006 Paper

Key Problem: Overloaded Semantics of IP Addresses

TCP: "I need it to be session identifier"

Routing System: "I need it to be routing locator"

Physical vs Logical Connectivity

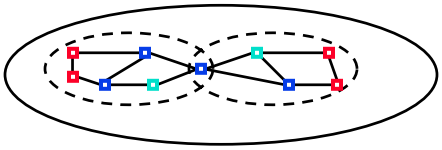
- Physically and logically connected:
  All computers in my lab
  = Private Network,
  Firewalled Network

- Physically disconnected but logically connected:
  My home and office computers

- Physically connected but logically disconnected: Passengers on a plane, Neighbors, Conference attendees sharing a wireless network, A visitor

Physical connectivity ≠ Trust

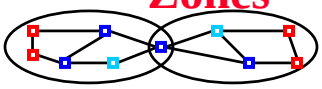
Realms



- Object names and Ids are defined within a realm
- A realm is a **logical** grouping of objects under an administrative domain
- The Administrative domain may be based on Trust Relationships
- A realm represents an organization
  - Realm managers set policies for communications
  - Realm members can share services.
  - Objects are generally members of multiple realms
- Realm Boundaries: Organizational, Governmental, ISP, P2P,…

Realm = Administrative Group

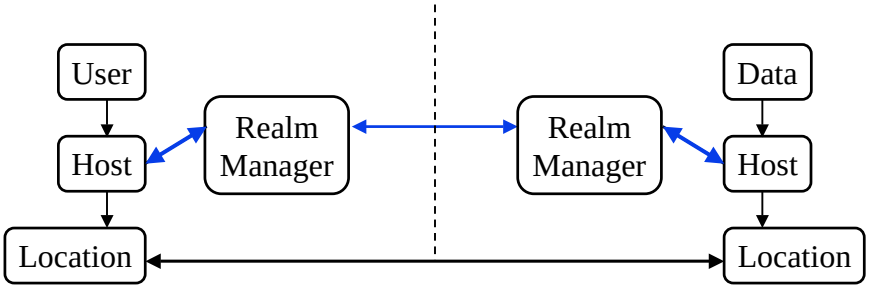
Zones



- Address of an object indicates its ***physical attachment point***
- Networks are organized as a set of ***zones***
- Zones are **physical** grouping of objects based on connectivity. Does not imply trust.

Zonal Hierarchy = Network Structure

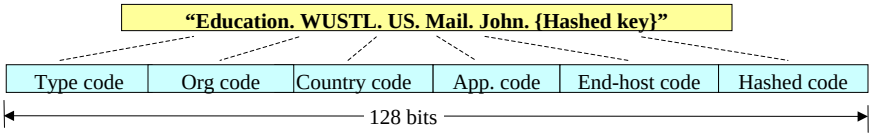
Id-Locator Split Architecture (MILSA)



- Realm managers resolve current location for a given host-ID ⇒ Provides privacy and organizational control
- Allows mobility, multi-homing
- Ref: Our Globecom 2008 paper [3]

MILSA: Key Features 1

- Hierarchical URI-like Identifiers (HUI): Example



- HUI can have same length as IPv6 address for transition benefit
- Realm Manager:
  Realm-Zone Bridging Server (RZBS)
- Provides the ID to locator translation
- Trust Relationship: Realm managers belong to a realm and have trust relationships with its clients and higher level realm managers. Set up trust relationship with other realm managers as needed.

MILSA: Key Features 2

- Control and data plane separation:
  Realm manager is used only in the control plane (Resolving Names/IDs to locators)
- A node can register multiple locators in multiple zones with a realm manager ⇒ Multihoming
- Object Delegation:
  A node can register other node or realm manager as proxy ⇒ Allows location privacy

Problems for the Current Internet

- Routing scalability
- Traffic engineering
- Mobility
- Multi-homing
- Renumbering
- Security
- Incremental deployment

Ref: [RFC4984] "Report from the IAB Workshop on Routing and Addressing," September 2007

Current Proposals

- Two possible approaches:

" ID/Locator Split "

Pros:
⇒ Clear
⇒Mobility, Multi-homing support
⇒ Trust, policy enforcements
Cons:
⇒ Need host modifications

"Core-edge separation"

Pros:
⇒ No host Modification
Cons:
⇒ Mobility, Multi-homing
⇒ Trust, policy enforcements

Current Proposals

- ***"Core-edge separation"*** mechanisms are to solve the routing scalability problems
  - *IP-in-IP tunneling*: LISP-ALT, LISP-NERD, APT, IVIP, TRRP, CRIO
  - *PI-PA indirection*: SIX/One
    PI = Provider Independent address
    PA = Provider Aggregatable address
- ***"Id/Locator Split"*** trying to solve other different parts of the problem space
  - HIP (mobility, security), Shim6(multihoming), I3(mobility, multicast), Hi3(mobility, security).

Enhanced MILSA Approach

- Hybrid design = Combines ***Core-edge separation*** and ***ID/Locator split***.
  ⇒ One solution for all problems identified by the routing research group (RRG)
  - Prevent PI addresses usage for global routing
  - *ID/Locator split* to gain benefits in mobility, multihoming, renumbering, security, etc.
  - New *Secure ID system* for naming: two different name spaces for two different purposes (not like currently overloaded IP addresses)
  - Support for future *integrated service architecture*
  - Support for *smooth transition* and *incremental deployment*

Hybrid Transition

- Allows coexistence, put the decision to future competence
  ⇒ reduce investment risk
- Allows evolvement in either direction
- Deploy incrementally, and reduce the global routing table size gradually
- Legacy hosts and new hosts coexist and can talk to each other

Ref: Our Globecom paper [3]

Summary

1. Internet 3.0 must be designed for commerce
   ⇒ Must represent multi-organizational structure and policies
2. Realm managers in Mobility and multi-homing supporting ID-locator split architecture (MILSA) enforce trust policies while allowing mobility, multi-homing, scalability, ...
3. Hybrid transition mechanism allowing both core-edge separation and id-locator split strategies to coexist and transit to either direction in the future
4. Incrementally deployable
   ⇒ Allows reducing the routing table size gradually

References

1. Jain, R., "Internet 3.0: Ten Problems with Current Internet Architecture and Solutions for the Next Generation," in Proceedings of Military Communications Conference (MILCOM 2006), Washington, DC, October 23-25, 2006, http://www.cse.wustl.edu/~jain/papers/gina.htm
2. Subharthi Paul, Raj Jain, Jianli Pan, and Mic Bowman, "A Vision of the Next Generation Internet: A Policy Oriented View," British Computer Society Conference on Visions of Computer Science, Sep 2008, http://www.cse.wustl.edu/~jain/papers/pona.htm
3. Jianli Pan, Subharthi Paul, Raj Jain, and Mic Bowman, "MILSA: A Mobility and Multihoming Supporting Identifier-Locator Split Architecture for Naming in the Next Generation Internet,," Globecom 2008, Nov 2008, http://www.cse.wustl.edu/~jain/papers/milsa.htm

References (Cont)

- Xiaohu Xu, Raj Jain, "Routing Architecture for the Next Generation Internet (RANGI)," IRTF RRG Internet Draft, March 2009, http://tools.ietf.org/html/draft-xu-rangi